Mobile Information Systems 6 (2010) 107–121
DOI 10.3233/MIS-2010-0095
IOS Press

Diffie-Hellman key based authentication in proxy mobile IPv6

HyunGon Kim[a] and Jong-Hyouk Lee[b,*]
[a]*Department of Information Security, Mokpo National University, Korea*
[b]*IMARA Team, INRIA, Paris, France*

Abstract. Wireless communication service providers have been showing strong interest in Proxy Mobile IPv6 for providing network-based IP mobility management. This could be a prominent way to support IP mobility to mobile nodes, because Proxy Mobile IPv6 requires minimal functionalities on the mobile node. While several extensions for Proxy Mobile IPv6 are being developed in the Internet Engineering Task Force, there has been little attentions paid to developing efficient authentication mechanisms. An authentication scheme for a mobility protocol must protect signaling messages against various security threats, e.g., session stealing attack, intercept attack by redirection, replay attack, and key exposure, while minimizing authentication latency. In this paper, we propose a Diffie-Hellman key based authentication scheme that utilizes the low layer signaling to exchange Diffie-Hellman variables and allows mobility service provisioning entities to exchange mobile node's profile and ongoing sessions securely. By utilizing the low layer signaling and context transfer between relevant nodes, the proposed authentication scheme minimizes authentication latency when the mobile node moves across different networks. In addition, thanks to the use of the Diffie-Hellman key agreement, pre-established security associations between mobility service provisioning entities are not required in the proposed authentication scheme so that network scalability in an operationally efficient manner is ensured. To ascertain its feasibility, security analysis and performance analysis are presented.

Keywords: PMIPv6, NETLMM, authentication, security

1. Introduction

While conventional mobility solutions have been developed based on host-based mobility management, the concept of network-based mobility management has been introduced in the Internet Engineering Task Force (IETF). Because conventional mobility solutions such as Mobile IPv6 (MIPv6) [8] and its extensions force a mobile node (MN) to have heavy functionalities for supporting its own mobility service, wireless communication service providers turn their gaze on network-based mobility management [3, 14,15]. Proxy Mobile IPv6 (PMIPv6) [21] is a recently developed mobility protocol from the concept of network-based mobility management wherein mobility service for an MN is provided by mobility service provisioning entities. The mobility service provisioning entities in the PMIPv6 domain manage all mobility signaling and data structures for the MN. Accordingly, an ordinary MN, which does not implement the mobility stack required in the conventional mobility solutions, achieves its mobility service in the given PMIPv6 domain [14,21].

In the IETF, extensions for PMIPv6 are being actively developed. Especially, several fast handover mechanisms proposed to minimize handover latency are introduced. Then, Fast Handovers for Proxy

*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.

Mobile IPv6 (FPMIPv6) [11] proposed by Yokota et al. has been selected and being standardized in the IETF. Even if FPMIPv6 has been well introduced how to reduce handover latency and packet loss while an MN moves different networks in the given PMIPv6 domain, it does not consider security issues. In other words, the MN must undergo its authentication procedure to have network access authorization when it attaches to a new network [2,13], but FPMIPv6 does not supply to reduce authentication latency occurred when the MN changes its access network.

In order to provide authenticated handover service for authorized MNs, an authentication, authorization, and accounting (AAA) architecture is a major security architecture [4,6,10] that has been widely being used in the networks of wireless communication service providers. Accordingly, it is naturally expected that PMIPv6 will be deployed in many networks with the AAA architecture [13]. However, the base specification of PMIPv6 has been developed with a limited understanding of secure authentication and actual deployment scenarios. For instance, 1) the impact of handover authentication is not addressed even if it contributes as an important performance metric, 2) the impact of the chosen integrity, confidentiality, and authentication methods is not addressed. We therefore need a secure handover scheme considering efficient secure authentication elements and deployment scenarios in order to deploy PMIPv6 mobility service within the AAA architecture successfully.

In this paper, we introduce a Diffie-Hellman (DH) key based authentication scheme that utilizes the low layer signaling to exchange DH variables and allows mobility service provisioning entities to exchange mobile node's profile and ongoing sessions securely. More precisely, the introduced DH key based authentication scheme has the following distinctive features compared to PMIPv6.

- DH key exchange operation is adopted to reduce the computation overhead.
- Relevant mobility service provisioning entities are supported to perform the context transfer and data packet forwarding.
- Pre-established security associations between mobility service provisioning entities are not required.

By utilizing the distinctive features, the DH key based authentication scheme achieves low handover latency while providing secure handover service for MNs in PMIPv6. The current specifications of PMIPv6 and FMIPv6 only provide the protocol operations without secure authentication concerns. Accordingly, the proposed DH key based authentication scheme would be a good direction for secure authentication for PMIPv6.

The remainder of this paper is organized as follows: Section 2 describes the specification of PMIPv6 and FPMIPv6 with the operation scenario within the AAA architecture. Then, in Section 3, the proposed DH key based authentication scheme is presented with the protocol operation and the security analysis. In Section 4, the results of performance evaluation are presented compared to existing authentication schemes. The conclusions of this paper are presented in Section 5.

2. Related work

In this section, we present the basic operation of PMIPv6 defined in [21]. Then, its extension, FPMIPv6 [11], is also described. PMIPv6 only defines the basic handover operation and data structure for network-based mobility management, whereas FPMIPv6 applies the concept of fast handover into PMIPv6 to improve handover performance.

2.1. Proxy Mobile IPv6

PMIPv6 is a network-based mobility management protocol reusing MIPv6 entities and concepts as much as possible. The core functional entities, i.e., mobility service provisioning entities, are the mobile access gateway (MAG) and the local mobility anchor (LMA). The MAG is usually located at the access router (AR) as software functionalities. The MAG detects the movement of an MN and then sends a proxy binding update (PBU) message to the LMA in order to register the location information of the MN. It means that mobility service for the MN is supported by the mobility service provisioning entities such as the MAG and the LMA. When the LMA receives the PBU message including essential information for the MN, the LMA recognizes that the MN has been attached to the access network managed by the MAG. As a response, the LMA sends back a proxy binding acknowledgement (PBAck) message including the home network prefix (HNP) for the MN. Then, the MAG sends a router advertisement (RA) message including the HNP to the MN. The LMA and the MAG establishes a bi-directional tunnel for the MN. Because that the LMA is responsible for maintaining the MN's reachability state and is the topological anchor point for the MN's HNP, all data packets sent from and to the MN are smoothly delivered through the established bi-directional tunnel for the MN.

As the MN receives the RA message sent from its MAG, the MN configures its address based on the HNP included in the RA message. Compared to MIPv6, this configured address is not a care-of address (CoA), which is changed when an MN changes its point of attachment in MIPv6, but it is treated as a home address (HoA). In other words, the MN continuously obtains and uses the same address called as a Proxy-HoA in the given PMIPv6 domain. This is because that the LMA continuously provides the same HNP for the MN.

In PMIPv6, each MN must be identified by its identifier, MN-ID. The MN-ID is used to obtain the MN's profile describing the allowed LMA's address (LMAA), i.e., MN-LMAA, assigned HNP, i.e., MN-HNP, permitted address configuration mode, roaming policy, and other parameters. Note that the MN's profile is an abstract term for referring to a set of configuration parameters configured for the given MN. The mobility service provisioning entities in the PMIPv6 domain are thus required to access these parameters in order to provide the mobility service for the MN. This information (profile) is typically stored in a policy store at an AAA server. Accordingly, upon completing the authentication procedure for the MN, this profile is retrieved and used to execute network-based mobility management for the MN.

Here, we give an actual example of the handover procedure of PMIPv6. Suppose that the MN has attached with the MAG_1 and changes its point of attachment to the MAG_2 in the same PMIPv6 domain managed by the home LMA (LMAh).

As illustrated in Fig. 1, there are several message exchanging between nodes. The detailed descriptions for the message exchanging are as follows:

1. De-registration Proxy Binding Update (De-Reg. PBU) message: By utilizing the L2 trigger, the MAG_1 detects that the MN will change its point of attachment. Then, the MAG_1 sends the De-registration Proxy Binding Update (De-Reg. PBU) message to the LMAh in order to inform the detachment of the MN on the access network. The binding and routing state for the MN is removed at the binding update list at the MAG.
2. De-registration Proxy Binding Update Acknowledgement (De-Reg. PBAck) message: Upon receiving the De-Reg. PBU message indicating that the MN has been detached from that access network, the LMAh checks its corresponding mobility session for the MN and accepts the De-Reg. PBU message if it is valid. Then, the LMAh waits for a pre-defined time to allow the MAG on the

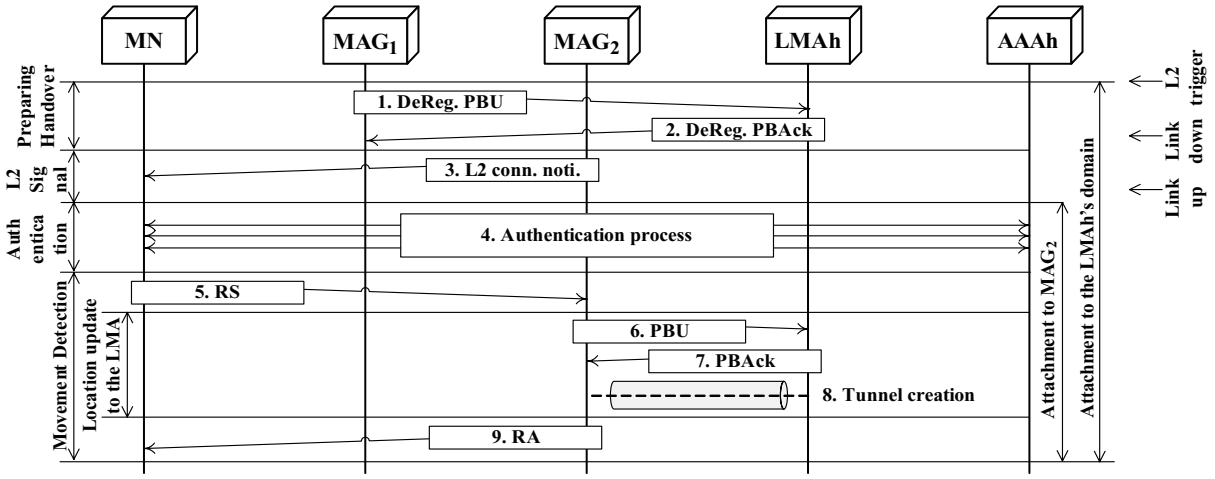


Fig. 1. The handover procedure of PMIPv6.

new access network to update the binding of the MN. That is, the LMAh waits for receiving a PBU message for the MN for a certain amount of time.

3. L2 Connection Notification: As the MN approaches the MAG_2, it receives the L2 connection notification. And then, the MN's wireless interface will be attached to the MAG_2.
4. Authentication Process: An authentication process for authorizing the MN in the new access network must be placed before the MN makes actual communication sessions. In Fig. 1, the exact authentication process it not presented, but a strong authentication mechanism must be applied when PMIPv6 is deployed in real network environments. For instance, the EAP-based authentication framework or public-key based framework with the AAA architecture can be used in here. Note that the AAA home server (AAAh) appears in this example.
5. Router Solicitation (RS) message: As soon as successful authentication of the MN, the MN sends the RS message in order to explicitly inform its attachment to the MAG_2 and to receive the RA message quickly.
6. Proxy Binding Update (PBU) message sent from the MAG_2: As receiving the RS message, the MAG_2 recognizes the presence of the MN and then sends the PBU message to the LMAh. In PMIPv6, the movement detection of the MN can be achieved in several ways. For instance, 1) by utilizing the L2/L3 signaling, MAGs can detect the movement of the MN and 2) by utilizing Authentication, Authorization and Accounting (AAA) signaling, MAGs can detect the movement of the MN as well as it obtains extra information of the MN. In [9,16], AAA operations and examples for PMIPv6 have been presented.
7. Proxy Binding Acknowledgement (PBAck) message: The LMAh on receiving the PBU message sent from the MAG_2 recognizes that the MN has been attached to the MAG_2. The LMAh sends the PBAck message including the same HNP that has been assigned to the MN at the previous access network of the MN.
8. Bidirectional Tunnel: As receiving the PBAck message indicating the success of the binding for the MN, a bidirectional tunnel between the LMAh and the MAG_2 is established for data packets forwarding for the MN.
9. Router Advertisement (RA) message: Because the LMAh assigns the same HNP for the MN, the MN is ensured to receive the same HNP compared to the previous one. The MN continuously finds

the same HNP in the RA message. The MN therefore configures and uses the same Proxy-HoA in the LMAh's domain.

Throughout the message exchanging, the MN is allowed to change its point of attachment without its actual involvement in mobility signaling actions, e.g., sending a message to register its new location. Compared to the previously developed mobility protocols such as MIPv6, PMIPv6 has a simple but devoted mobility support for the MN.

The limitations that the base PMIPv6 specification has are 1) route optimization (RO) support, 2) multihomed MN support, and 3) handover optimization. The recently chartered Network-Based Mobility Extensions (NETEXT) working group [19] are currently working on the issues of RO support and multihomed MN support in PMIPv6. Then, the issues of handover optimization is currently treated in Mobility for IP: Performance, Signaling and Handoff Optimization (MIPSHOP) working group [18]. FPMIPv6 [11] proposed by Yokota et al. has been being developed as a working group item in the MIPSHOP working group.

2.2. Fast proxy mobile IPv6

FPMIPv6 has been introduced in order to minimize the handover latency incurred while an MN performs its handover. The base specification of PMIPv6 does not cover this issues. As presented in [11], fast handover mechanisms introduced in MIPv6 called FMIPv6 [20] cannot be directly applied into PMIPv6 because that the MN cannot launch any mobility signaling to indicate its movement to ARs.

Similar to FMIPv6, FPMIPv6 operates in either the predictive mode and the reactive mode depending on the network circumstances. More precisely, if the MN does not have enough time to prepare its handover at the currently attached network, the reactive mode is activated, whereas the predictive mode is launched when the MN moves to the new access network after the completion of the context transfer between the relevant ARs. Obviously, the predictive mode can significantly reduce the handover latency compared to the reactive mode. The reactive mode hardly reduces the handover latency. Therefore we here focus on the predictive mode of FPMIPv6 because it actually achieves the goal of fast handover.

Figure 2 illustrates the message exchanging between nodes for the handover procedure of Predictive FPMIPv6. In Fig. 2, the MN prepares its handover at the currently attached network managed by the MAG_1 to the new network managed by the MAG_2. The detailed descriptions for the message exchanging are as follows:

1. L2 report: By utilizing the L2 trigger, the MN detects information of neighbor networks. Then, it reports information of the next network the MN will attach to with. This message is a access technology specific, but at least the MN-ID and network identification (NET-ID) must be provided to the MAG_1, where the MN is currently attached with.
2. Handover Initiate (HI) message: As receiving the L2 report sent from the MN, the MAG_1 recognizes that the MN will move to the specific network indicated by the NET-ID, i.e., the network managed by the MAG_2. Then, it informs the movement of the MN to the MAG_2 by sending the handover initiate (HI) message including the MN-ID,MN-HNP, MN-LMAA, MN's interface identification (MN-IID), etc.
3. Handover Acknowledge (HAck) message: The MAG_2 replies with the handover acknowledge (HAck) message indicating the success or failure for preparing of the MN's handover.
4. De-registration Proxy Binding Update (De-Reg. PBU) message: The MAG_1 sends the De-Reg. PBU message to the LMAh in order to inform the detachment of the MN on the access network. Depending on the actual implementation, the HI and De-Reg. PBU messages can be simultaneously sent, but in Fig. 2, it has been presented in stepwise.

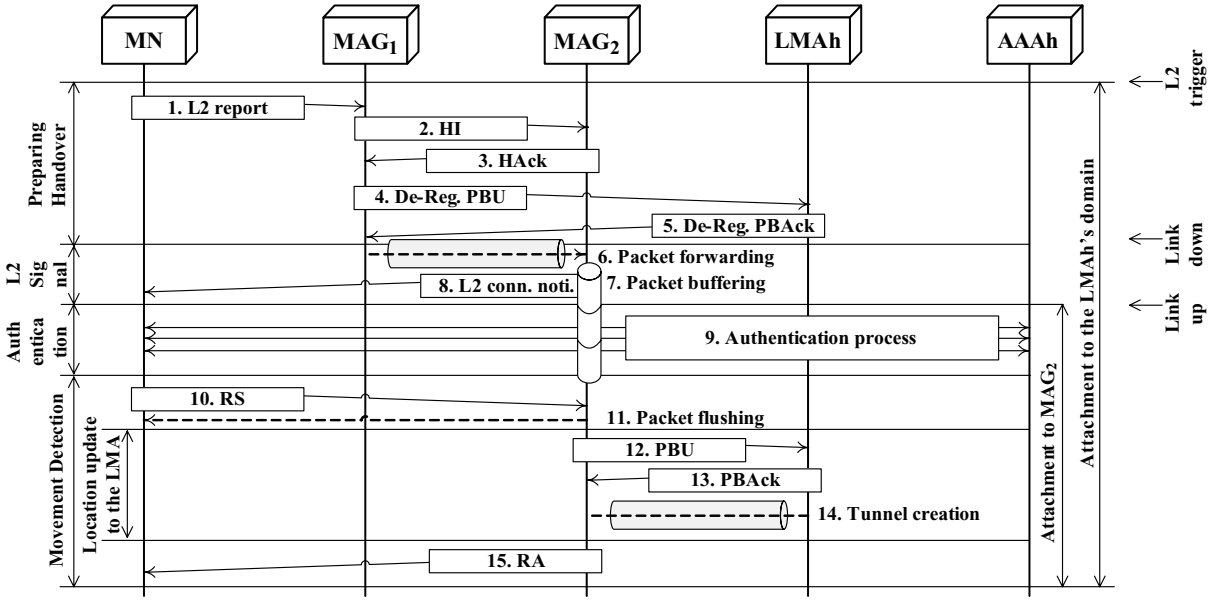


Fig. 2. The handover procedure of Predictive FPMIPv6.

5. De-registration Proxy Binding Update Acknowledgement (De-Reg. PBAck) message: Upon receiving the De-Reg. PBU message indicating that the MN has been detached from that access network, the LMAh checks its corresponding mobility session for the MN and accepts the De-Reg. PBU message if it is valid. Then, the LMAh waits for a pre-defined time to allow the MAG on the new access network to update the binding of the MN.
6. Packet Forwarding: The MAG_1 starts to forward data packets destined for the MN.
7. Packet Buffering: The data packets forwarded from the MAG_1 are being buffered at the MAG_2. The actual implementation and operation of packet forwarding and buffering can be different depends on the implementation details, but the goal of packet forwarding and buffering is to prevent packet loss.
8. L2 Connection Notification: As the MN approaches the network of MAG_2, it receives the L2 connection notification from the MAG_2. Then, the MN's wireless link is attached to the MAG_2.
9. Authentication Process: Similar to PMIPv6, the authentication process introducing unacceptable long latency is preformed if it is not optimized.
10. Router Solicitation (RS) message: As soon as successful authentication of the MN, the MN sends the RS message in order to explicitly inform its attachment to the MAG_2 and to receive the RA message quickly.
11. Packet Flushing: The MAG_2 immediately sends the data packets to the MN. However, this packet flushing can begin as the authentication process is done. This is, data packets can be sent before the MAG_2 receives the RS message if the MAG_2 explicitly knows the attachment of the MN at its access network throughout other information, i.e., the authentication success message for the MN sent from the AAAh server when it acts as an AAA client.

In Fig. 2, other message exchanging which has been not described here is similar with that of PMIPv6. Predictive FPMIPv6 obviously reduces the handover latency by allowing the MN prepares its handover before the MN performs its actual handover to the new access network. The HI and HAck message

presented in Fig. 2 are used to exchange the context transfer between the MAGs. Then, as the MN attaches to the new network managed by one of the MAGs, i.e., MAG_2, the buffered data packets for the MN are immediately sent to the MN.

Even if FPMIPv6 improves handover performance of PMIPv6, it cannot address the handover authentication latency occurred during the MN undergoes its authentication process. For instance, the required times for several message exchanging between the MN and the AAAh, and executing cryptography operation yield long latency. This long latency for handover authentication thus causes user-perceptible deterioration of handover performance even if FPMIPv6 is used. The objective of this paper is to reduce such long handover authentication latency.

3. Diffie-hellman key based authentication

In this section, we present the proposed DH key based authentication scheme. The followings are the design principles and assumptions of the DH key based authentication scheme.

- Minimizing the computation power consumption as well as the administrative cost imposed on the MN.
- Minimizing the number of keying material requests to the AAAh.
- Utilizing signaling messages defined in FPMIPv6 to improve handover performance.
- Utilizing L2 events to anticipate the handover of the MN.
- Utilizing L2 messages in order to carry DH variables.
- Protecting session keys against various attacks.
- Removing pre-established security associations between the MAGs.
- Removing additional signaling messages between the MAG and the LMA.

One of recent performance enhancement approaches is to use link-layer specific information. For instance, IEEE 802.21 (MIH) provides link-layer specific information to upper layers. Especially, some information provided by IEEE 802.21 such as available network list, link identification, link status, etc, can be used to facilitate the handover decision and detection of the MN [1,7]. In this paper, we assume that the MN and network entities are aware of MIH functionalities.

3.1. Protocol operation

Figure 3 depicts the message exchanging between nodes for the handover procedure of the proposed DH key based authentication scheme. For variant DH key exchange operations, MAGs choose a large prime number n, generate $g \in Z_n$ and $y \in Z_{n-1}$ at random, and compute $g^y \in Z_n$ in advance. The detailed descriptions are as follows:

1. L2 signal ($g_{old}^{y'}$, g_{old}, n_{old}) from the MAG_1: As a beacon signaling, the MAG_1 sends the L2 signal. This message contains $g_{old}^{y'}$, g_{old}, and n_{old}. In addition, this message includes the available network list, link identification, link status, etc.
2. L2 signal (g_{new}^{y}, g_{new}, n_{new}) from the MAG_2: Similarly, the MAG_2 sends the L2 signal containing g_{new}^{y}, g_{new}, and n_{new}.
3. L2 report (g_{new}^{y}, $g_{old}^{y'}$, g_{new}, n_{new}): The MN sends the L2 report including g_{new}^{y}, $g_{old}^{y'}$, g_{new}, and n_{new}. In addition, this message includes at least the MN-ID and NET-ID. As receiving this message, the MAG_1 recognizes that the MN is going to attach with the network managed

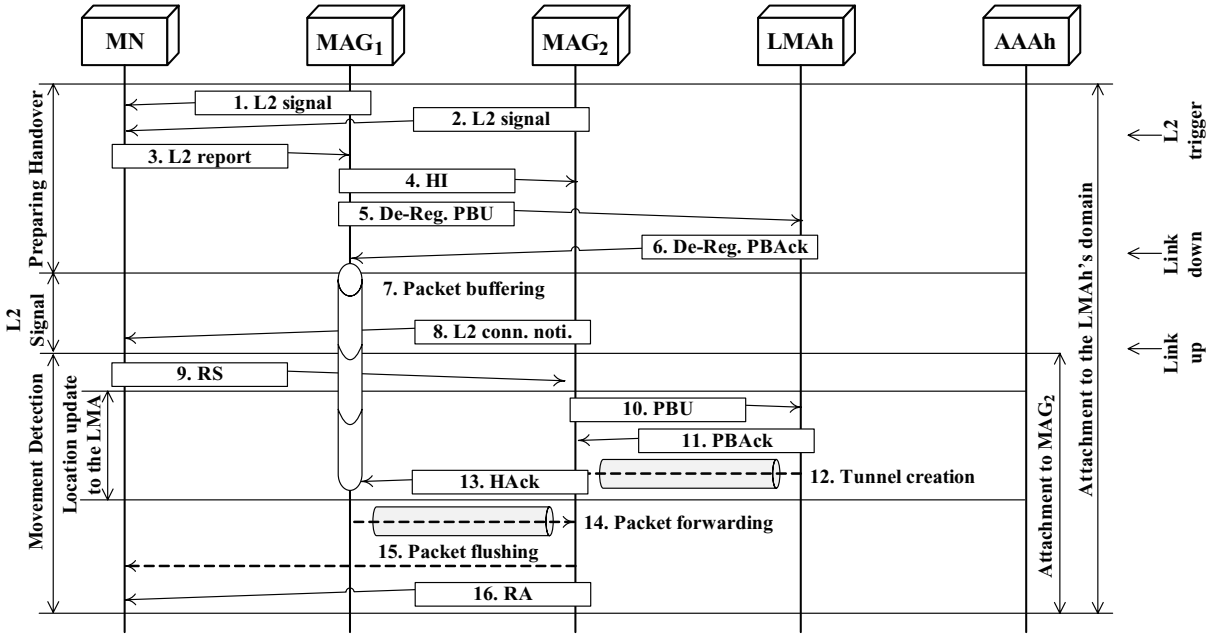


Fig. 3. The handover procedure of the proposed scheme.

by the MAG_2. Now, the MAG_1 computes $x = <g_{new}^{y}, g_{old}^{y'}> S_{MAG-LMA} (\mathtt{mod} n_{new-1})$ and creates $g_{new}^{x} \in Z_{n_{new}}$. Also, the MAG_1 creates a session key $K_{MAG_1-MAG_2} = (g_{new}^{y})^{x} = g_{new}^{xy} \in Z_{n_{new}}$. Finally, the MAG_1 encrypts $C = [S_{MN-MAG}, S_{MAG-LMA}] K_{MAG_1-MAG_2}$ and $C^{'} = [M_{\rho}, K_{\chi}] K_{MAG_1-MAG_2}$, where M_{ρ} is the profile's MN and K_{χ} is the ongoing mobility session key for the MN.

4. Handover Initiate (HI) message (C, C', g_{new}^{y}, $g_{old}^{y'}$): As receiving the HI message including C, C', g_{new}^{y}, and $g_{old}^{y'}$, the MAG_2 validates g_{new}^{y} and stores C. Then, it retrieves g_{new}^{y}, g_{new}, and n_{new}.
5. De-registration Proxy Binding Update (De-Reg. PBU) message: As a default operation defined in [21], this message is sent to the LMA in order to inform the detachment of the MN.
6. De-registration Proxy Binding Update Acknowledgement (De-Reg. PBAck) message: As a response to the De-Reg. PBU message, it is sent from the LMAh to the MAG_1.
7. Packet Buffering: The MAG_1 starts to buffer data packets destined for the MN. This packet buffering is continued until the MAG_1 receives the HAck message.
8. L2 Connection Notification: As the MN approaches the network of MAG_2, it receives the L2 connection notification.
9. Router Solicitation (RS) message: The MN sends the RS message in order to explicitly inform its attachment to the MAG_2 and to receive the RA message quickly.
10. Proxy Binding Update (PBU) message (g_{new}^{y}, $g_{old}^{y'}$, g_{new}, n_{new}): As receiving the RS message, the MAG_2 knows the attachment of the MN. Then, it sends the PBU message including g_{new}^{y}, $g_{old}^{y'}$, g_{new}, n_{new} to the LMAh. In addition, it computes $x = <g_{new}^{y}, g_{old}^{y'}> S_{MAG-LMA} (\mathtt{mod} n_{new-1})$ and creates $g_{new}^{x} \in Z_{n_{new}}$.
11. Proxy Binding Acknowledgement (PBAck) message (g_{new}^{x}): Once the LMAh successfully processes the PBU message, it replies the PBAck message including g_{new}^{x}. The MAG_2 decrypts C and then obtains S_{MN-MAG} and $S_{MAG-LMA}$. In addition, it decrypts $C^{'}$ and then obtains

M_ρ and K_χ. Accordingly, the MAG_2 now obtains all materials for serving the MN at its access network.

12. Bidirectional Tunnel: The bidirectional tunnel is established for the MN.
13. Handover Acknowledge (HAck) message: The MAG_2 sends the HAck message indicating its successful handover authentication.
14. Packet Forwarding: The MAG_1 now starts to forward data packets destined for the MN if the HAck message indicates the success of the handover authentication.
15. Packet Flushing: The MAG_2 immediately forwards the data packets to the MN.
16. Router Advertisement (RA) message: The RA message including the same HNP compared to the previous one is sent to the MN.

In the proposed scheme, the previously assigned session keys S_{MN-MAG} and $S_{MAG-LMA}$ are reused to reduce the key generation time and the key delivery time. This feature the proposed scheme has avoids the contact with the AAAh for authentication of the MN every time the MN changes its point of attachment. To ensure the confidentiality and integrity of these session keys, they are encrypted and decrypted under a short-term secret key $K_{MAG_1-MAG_2}$. In order to provide mobility service for the newly attached MN, the network must obtain related information for the MN. In the proposed scheme, M_ρ and K_χ are also forwarded from the previous network to the new network. To minimize the MN's computing power consumption, the MAGs create n and $g \in Z_n$. Since the MAGs use n and g for only a short period, at most 512 bits prime n should be large enough. It results in reducing the computational overhead for g^x and g^y.

3.2. Security analysis

In this section, we present security analysis results on the proposed DH key based authentication scheme.

The proposed scheme reuses the previously assigned session keys to achieve low handover latency. However, security weaknesses about this key reuse must be addressed. Accordingly, we point out a possible session-stealing attack on the proposed scheme. In order to re-use the session keys, however, they have to be taken over in a secure fashion between the relevant MAGs. Especially, $S_{MAG-LMA}$ is a random value of at least 64 bits and is not hashed. Unfortunately, if an attacker spoofs at the new network managed by the MAG_2, he can acquire the keys in the phase of key exchange between the MAG_1 and the MAG_2, and then the current session can be derived from that key. Because of this security weakness, the confidentiality of the session keys must be provided in the phase of key exchange. For a similar purpose, the solution proposed by Jacobs and Belgard [22] can be viewed as a further attempt to provide confidentiality of session keys based on public key cryptography. However, it is impractical because that each MAG must perform public key cryptography operations that suffer from a long delay during the handover authentication for the MN. The lifetime of the session keys is enough to avoid too-frequent AAA related transactions since each invocation of this process is likely to cause lengthy delays. Once the keys have been distributed by the AAAh, the MAG_1 obtains two session keys: S_{MN-MAG} and $S_{MAG-LMA}$. If the MN attaches with the MAG_2, the PBU message is launched to update the location of the MN by the MAG_2. Since the MAG_2 has no session keys, re-authentication is required and new session keys should be assigned by the AAAh, which leads to long signaling delay. The proposed scheme thus uses existing session keys when there is enough key lifetime remaining in the existing binding update. This can eliminate the time required for re-authentication by the AAAh.

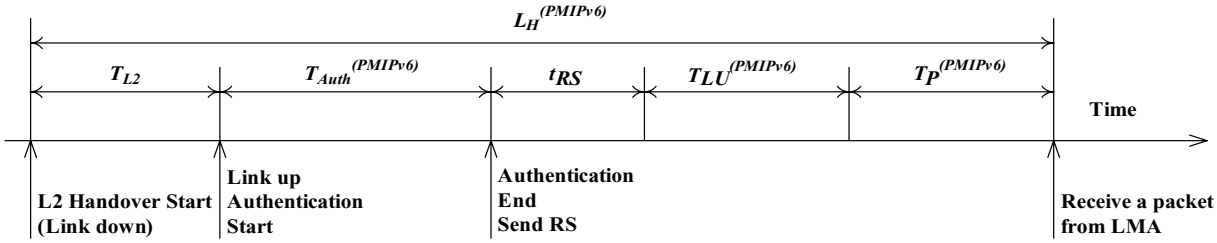


Fig. 4. The timing diagram for PMIPv6 handover.

Let us consider some scenarios considering possible session-stealing attacks from a session-stealing attacker's point of view: First, suppose an attacker intercepts the L2 report including g_{new}^{y}, $g_{old}^{y'}$, g_{new} and n_{new}. The attacker can obtain the encrypted message C and g^y, but cannot decrypt C since he does not have $K_{MAG_1-MAG_2}$. Furthermore, the attacker cannot compute $K_{MAG_1-MAG_2} = g^{xy}$ since he does not know x, even if he knows g^y. Second, suppose that an attacker intercepts the HI message including C, C', g_{new}^{y} and the PBAck message including g_{new}^{x}. Then, he only knows C, g^x and g^y so that he cannot compute $K_{MAG_1-MAG_2} = g^{xy}$ from g^x and g^y within the lifetime of the session keys since the DH problem is computationally infeasible. Therefore, we can assert that the proposed scheme provides confidentiality and integrity of ongoing session keys and enables MN's profile to be exchanged securely.

4. Performance analysis

In this section, we develop an analytical model to investigate the handover latency and the handover blocking probability. Then, we present the numerical results.

4.1. Handover latency

We define the handover latency as the time interval during which an MN cannot send or receive any packets while it performs its handover between different networks.

Figure 4 illustrates the timing diagram for PMIPv6 handover. PMIPv6 manages the movement of an MN in a localized manner, but the handover authentication for the MN must be performed for every time the MN changes its point of attachment in the given PMIPv6 domain.

Suppose $L_H^{(PMIPv6)}$ is the handover latency of PMIPv6. Then it is expressed as follows.

$$L_H^{(PMIPv6)} = T_{L2} + T_{Auth}^{(PMIPv6)} + t_{RS} + T_{LU}^{(PMIPv6)} + T_P^{(PMIPv6)}, \tag{1}$$

where T_{L2} is the link-layer handover latency. This latency varies among different implementation chipsets. $T_{Auth}^{(PMIPv6)}$ is the handover authentication latency that can be estimated the transmission latency between the serving MAG for the MN and the AAAh. In the paper, the computation times for generating and verifying keys are assumed to be negligible. The transmission latency for delivering required keys from the AAAh is assumed to be a main factor for authentication latency. t_{RS} is the required time for receiving the RS message sent from the MN so that it can be rewritten as t_{MAG-MN}, where t_{MAG-MN} is the one-way transmission latency between the MAG and the MN. $T_{LU}^{(PMIPv6)}$ is the location update latency for the MN. It can be expressed as $2t_{MAG-LMA}$, where $t_{MAG-LMA}$ is the one-way transmission latency between the MAG and the LMA. $T_P^{(PMIPv6)}$ is the time required that

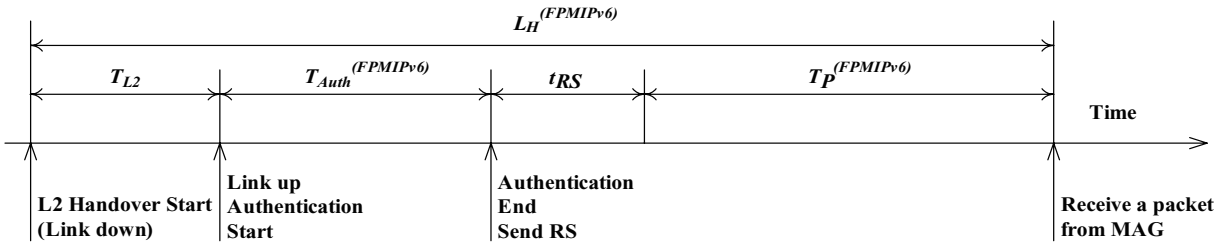


Fig. 5. The timing diagram for Predictive FPMIPv6 handover.

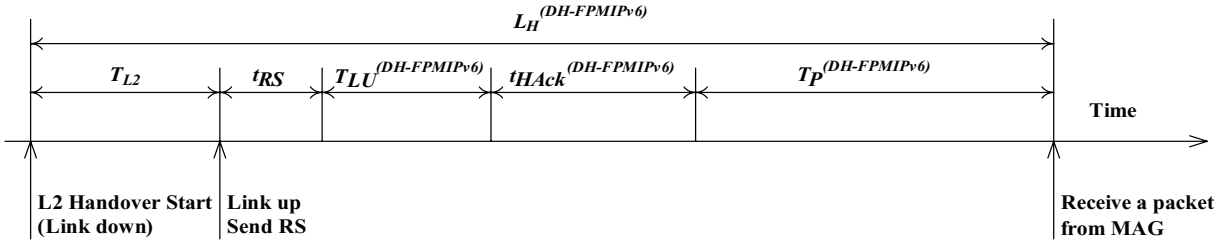


Fig. 6. The timing diagram for the proposed scheme's handover.

the first packet destined for the MN is arrived from the LMA to the MN. Then, it can be expressed as $t_{MAG-LMA} + t_{MAG-MN}$.

Figure 5 illustrates the timing diagram for Predictive FPMIPv6 handover. FPMIPv6 enables an MN prepares its handover before the MN performs its actual handover. Accordingly, the handover performance compared to that of PMIPv6 is improved. However, Predictive FPMIPv6 does not optimize the handover authentication. Accordingly, similar to PMIPv6, the handover authentication for the MN must be performed for every MN's handover.

Suppose $L_H^{(FPMIPv6)}$ is the handover latency of Predictive FPMIPv6. Then it is expressed as follows.

$$L_H^{(FPMIPv6)} = T_{L2} + T_{Auth}^{(FPMIPv6)} + t_{RS} + T_P^{(FPMIPv6)}, \tag{2}$$

$T_{Auth}^{(FPMIPv6)}$ is the handover authentication latency of Predictive FPMIPv6 which is not different with that of PMIPv6 so that $T_{Auth}^{(FPMIPv6)}$ is the same with $T_{Auth}^{(PMIPv6)}$. $T_P^{(FPMIPv6)}$ is the time which the first data packet sent from the new network, i.e., MAG_2, arrives at the MN. The data packets destined for the MN have been buffered at the MAG_2 before the MN attaches with the MAG_2. As the MAG_2 recognizes the attachment of the MN by receiving the RS message, it immediately sends the buffered data packets to the MN. Accordingly, $T_P^{(FPMIPv6)}$ can be rewritten as t_{MAG-MN}.

Figure 6 illustrates the timing diagram for the proposed scheme's handover. In the proposed scheme, the authentication process can be done as the MAG_2 receives the PBAck message sent from the LMAh. In addition, the proposed one utilizes the buffering mechanism used in FPMIPv6 so that data packets being buffered at the MAG_1 in the previous network are forwarded as the MAG_1 receives the HAck message sent from the MAG_2.

Suppose $L_H^{(DH-FPMIPv6)}$ is the handover latency of the proposed scheme. Then it is expressed as follows.

$$L_H^{(DH-FPMIPv6)} = T_{L2} + t_{RS} + T_{LU}^{(DH-FPMIPv6)} + t_{HAck}^{(DH-FPMIPv6)} + T_P^{(DH-FPMIPv6)}, \tag{3}$$

where $T_{LU}^{(DH-FPMIPv6)}$ is the location update latency that can be expressed as $2t_{MAG-LMA}$. $t_{HAck}^{(DH-FPMIPv6)}$ is the time which the HAck message sent from the MAG_2 arrives at the MAG_1. Then, it can be expressed as $t_{MAG-MAG}$, which is the one-way transmission latency between the MAGs. As receiving the HAck message, the MAG_1 immediately forwards data packets to the MAG_2 where the forwarded data packets for the MN are also sent to the MN. Accordingly, $T_P^{(DH-FPMIPv6)}$ is expressed as $t_{MAG-MAG} + t_{MAG-MN}$.

4.2. Handover blocking probability

The handover event will be failed due to several reasons. In this paper, we only consider the handover latency as a handover blocking factor. Then, the handover failure event can be expressed as the event which an MN cannot complete its handover when the network residence time is less than the handover latency.

Suppose $E[L_H^{(\cdot)}]$ is the mean value of $L_H^{(\cdot)}$, where $(\cdot)$ is a protocol indicator. For the sake of simplicity, we assume that $T_H^{(\cdot)}$ is exponentially distributed with its cumulative function $F_T(t)$. Then, the handover blocking probability $\rho_b^{(\cdot)}$ can be expressed as follows [12,23].

$$\rho_b^{(\cdot)} = Pr(L_H^{(\cdot)} > T_R) = \int_0^\infty (1 - F_T^{(\cdot)}(u)) f_R(u) du = \frac{\mu_c E[L_H^{(\cdot)}]}{1 + \mu_c E[L_H^{(\cdot)}]}, \tag{4}$$

where T_R is the network residence time and its probability density function is $f_R(t)$. μ_c is the border crossing rate for the MN. Assuming that the AR's coverage area is circular, then μ_c is calculated as follows [5].

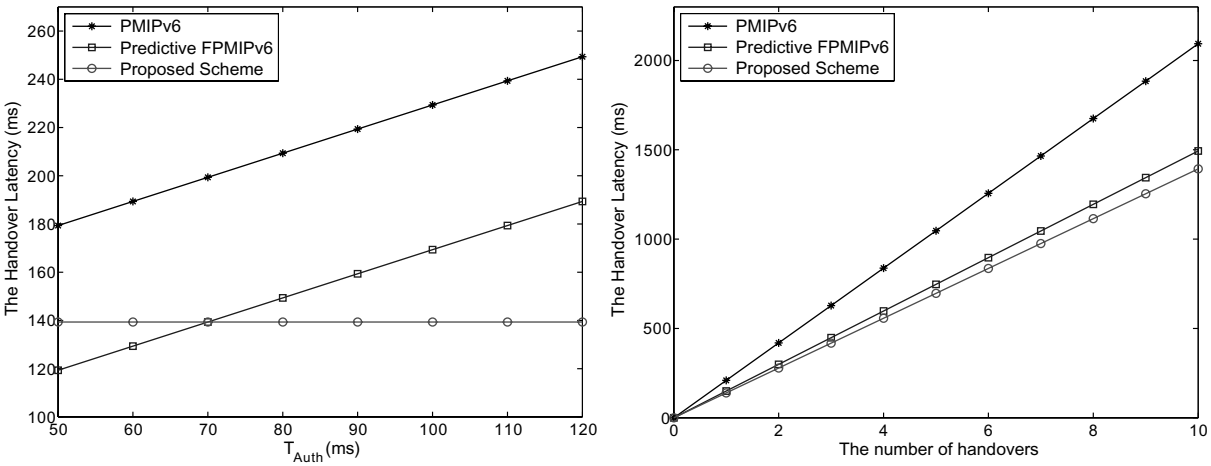
$$\mu_c = \frac{2\nu}{\pi R}, \tag{5}$$

where ν is the average velocity of the MN and R is the radius of the AR's coverage area.

4.3. Numerical results

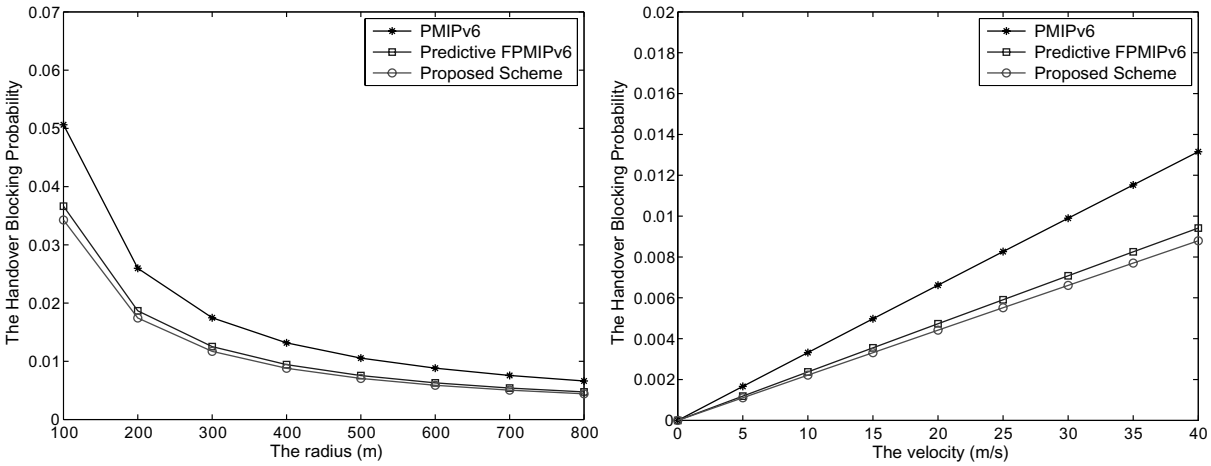
For the numerical analysis, we use the following system parameters obtained from the previous works [13,17]: $T_{L2} = 45.35$ ms, $t_{MAG-MN} = 12$ ms, $t_{MAG-MAG} = 15$ ms, and $t_{MAG-LMA} = 20$ ms.

In Fig. 7, we investigate the variation of the handover latency. As functions for the variation of the handover latency, we use T_{Auth} and the number of handovers n. Figure 7(a) presents the variation of the handover latency as a function of T_{Auth}. From the presented results in Fig. 7(a), we can find that the proposed authentication scheme is not affected by T_{Auth}, but other schemes are affected. This is because that the proposed authentication scheme reuses the previously assigned session keys for an MN when the MN performs its handover from the previous network to the new network. The session keys used in the previous network are securely transferred to the new network. In other words, the proposed authentication scheme does not require to contact with the AAAh in order to authenticate the MN. Moreover, as we can see in Fig. 7(a), when T_{Auth} is enough small value, Predictive FPMIPv6 outperforms other schemes, but as T_{Auth} increases, the proposed authentication scheme shows the best performance compared to others. Next, we vary n from 0 to 10 and fix T_{Auth} as 80 ms. Then, we see



(a) L_H versus T_{Auth} (b) L_H versus n

Fig. 7. The variation of the handover latency.



(a) μ_c versus R (b) μ_c versus v

Fig. 8. The variation of the handover blocking probability.

the variation of the handover latency as a function of n in Fig. 7(b). As the MN performs its handover continuously, the handover latency cumulatively increases and this phenomenon obviously shows that the proposed scheme requires lower handover latency due to its reduced handover authentication time.

In Fig. 8, we investigate the variation of the handover blocking probability. As functions for the variation of the handover blocking probability, we use R and ν. We fix T_{Auth} and ν as 80 ms and 40 m/s, respectively. Then, we see the variation of the handover blocking probability as a function of R in Fig. 8(a). In the small size of network, the MN quickly moves out to other network so that its handover must be completed in a short time. Accordingly, all schemes show low performance in the small size of network. Next, we vary ν from 0 to 40 m/s with $R = 400$ m. Then, we see the variation of the handover blocking probability as a function of ν in Fig. 8(b). Similarly, the MN quickly moves out to other network as its velocity is high. Accordingly, all schemes show low performance in the high

velocity environments. From the results presented in Fig. 8, we can confirm that Predictive FPMIPv6 and the proposed authentication scheme provide better performance compare to PMIPv6 due to the reduced handover latency. In addition, the proposed authentication scheme also outperforms others.

5. Conclusions

The proposed authentication scheme adopts a variant of the DH key agreement that does not require to have pre-established security associations between relevant MAGs. By avoiding such fixed security associations, the proposed DH key based authentication scheme also improves the scalability of PMIPv6. In addition, the proposed scheme reuses the previously assigned session keys for an MN when the MN changes its point of attachment. Accordingly, in the proposed scheme, the number of authentication and session key generation queries to the AAA server is minimized. We presented the protocol operation and security analysis of the proposed scheme. Then, we have developed the analytical model to investigate the handover latency and the handover blocking probability. The numerical results corroborate that the proposed scheme reduces the handover authentication latency and it outperforms PMIPv6 and Predictive FPMIPv6 in terms of handover latency and handover blocking probability.

References

[1] A.D.L. Oliva, A. Banchs, I. Soto, T. Melia and A. Vidal, An overview of IEEE 802.21: media-independent handover services, *IEEE Wireless Communications* **15**(4) (2008), 96–103.
[2] A. Durresi, M. Durresi1 and L. Barolli, Secure authentication in heterogeneous wireless networks, *Mobile Information Systems*, **4**(2) (2008), 119–130.
[3] 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.
[4] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht and D. Spence, Generic AAA Architecture, *RFC 2903* (2000).
[5] C. Makaya and S. Pierre, An Analytical Framework for Performance Evaluation of IPv6-Based mobility Management Protocols, *IEEE Transactions on Wireless Communications* **7**(3) (2008), 972–983.
[6] C. Perkins and P. Calhoun, Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4, *RFC 3957* (2005).
[7] D. Griffith and R. Rouil and N. Golmie, Performance Metrics for IEEE 802.21 Media Independent Handover (MIH) Signaling, *Wireless Personal Communications*, DOI: 10.1007/s11277-008-9629-4, 2009.
[8] D. Johnson, C. Perkins and J. Arkko, Mobility Support in IPv6, *RFC 3775* (2004).
[9] F. Xia, B. Sarikaya, J. Korhonen, S. Gundavelli and D. Damic, RADIUS Support for Proxy Mobile IPv6, *draft-xia-netlmm-radius-04* (*work in progress*) (2009).
[10] G. Giaretta, J. Kempf and V. Devarapalli, Mobile IPv6 Bootstrapping in Split Scenario, *RFC 5026* (2007).
[11] H. Yokota, K. Chowdhury, R. Koodli, B. Patil and F. Xia, Fast Handovers for Proxy Mobile IPv6, *draft-ietf-mipshop-pfmipv6-09* (*work in progress*) (2009).
[12] J. McNair, I.F. Akyildiz and M.D. Bender, An Inter-System Handoff Technique for the IMT-2000 System, In *Proceedings of IEEE Annual Joint Conference of the IEEE Computer and Communications Societies* (*INFOCOM*) (2000).
[13] 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*, DOI: 10.1002/wcm.895, 2009.
[14] J.-H. Lee, H.-J. Lim and T.-M. Chung, A competent global mobility support scheme in NETLMM, *International Journal of Electronics and Communications* **63**(11) (2009), 950–967.
[15] J.-H. Lee, Y.-H. Han, S. Gundavelli and T.-M. Chung, A comparative performance analysis on Hierarchical Mobile IPv6 and Proxy Mobile IPv6, *Telecommunication Systems* **41**(4) (2009), 279–292.
[16] J. Korhonen, J. Bournelle, K. Chowdhury and A. Muhanna, Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server, *draft-ietf-dime-pmip6-04* (*work in progress*), 2009.
[17] K.-S. Kong, W. Lee, Y.-H. Han and M.-K. Shin, Handover Latency Analysis of a Network-Based Localized Mobility Management Protocol, In *Proceedings of IEEE International Conference on Communications* (*ICC*) (2008).
[18] MIPSHOP working group, http://tools.ietf.org/wg/mipshop/, Accssed 2009.

[19] NETEXT working group, http://tools.ietf.org/wg/netext/, Accssed 2009.
[20] R. Koodli, Mobile IPv6 Fast Handovers, *RFC 5268* (2008).
[21] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, Proxy Mobile IPv6, *RFC 5213* (2008).
[22] S. Jacobs and S. Belgard, Mobile IP Public Key Based Authentication, *draft-jacobs-mobileip-pki-auth-03* (*work in progress*) (2001).
[23] S. Yang, H. Zhou, Y. Qin and H. Zhang, SHIP: Cross-layer mobility management scheme based on Session Initiation Protocol and Host Identity Protocol, *Telecommunication Systems*, DOI: 10.1007/s11235-009-9164-y, 2009.

HyunGon Kim received the B.S and M.S. degrees in electrical engineering from the KumOh National University, and the Ph.D. degree in computer science from the ChungNam National University, South Korea. He is currently an assistant professor in Department of Information Security at the Mokpo National University, South Korea. He has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea, as a senior member of engineering staff for 11 years. His research interests include wireless sensor network security, telecommunications network security, and vehicle communication security. He has published more than 45 papers in referred journals and conference proceedings. He is a member of IEEE and served as program committee member in several international conferences.

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.