Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 14(2): 89-96, Jun. 2016 **Regular paper**

Secure Pre-authentication Schemes for Fast Handoff in Proxy Mobile IPv6

Jaejong Baek*, ***Member, KIICE***

Naval Information and Communication School, Naval Education and Training Command, Changwon 51699, Korea

Abstract

In mobile communication, there are various types of handoff for the support of all forms of mobility. Proxy mobile IPv6 (PMIPv6) enables local network-based mobility management of a mobile node without any effect of mobility-related signaling. Recently, PMIPv6 has been considered for supporting mobility management in LTE/SAE-based mobile networks. To support seamless mobility in heterogeneous mobile networks, the overall cost of handoffs needs to be minimized and the procedure should be guaranteed to be secure. However, the reduction of the authentication cost has not been fully investigated to provide seamless connectivity when mobile users perform a handoff between the PMIPv6 domains. This paper proposes secure pre-authentication schemes, completing an authentication procedure before performing a handoff, for a fast handoff in PMIPv6. Analytic models have been used for measuring the authentication latency and for the overhead cost analysis. In addition to providing fast authentication, the proposed pre-authentication schemes can prevent threats such as replay attacks and key exposure.

Index Terms: AAA, Authentication, Handoff, MIP, Mobile IP, PMIP

I. INTRODUCTION

Proxy mobile IPv6 (PMIPv6) has been standardized by the NETLMN Working Group; it enables local network-based mobility management for meeting the needs of a heterogeneous handoff (HO) environment where client mobility can be performed without the use of another mobility management operation [1]. However, PMIPv6 cannot directly support global mobility and any specific authentication approach between different domains because it was originally designed for local mobility in a single domain. Because of these security issues, authentication is the fundamental security technology and has become the focus of security research [2].

Recently, some research has been conducted on the domain-level mobility of the PMIPv6 authentication method. This paper proposes secure pre-authentication and key management schemes for fast HO in PMIPv6. In addition to providing pre-authentication, the proposed authentication method can prevent threats such as replay attacks and key exposure. Further, analytic models have been used for measuring the authentication latency and for cost analysis. Then, the effects of mobility and traffic parameters on the authentication cost and latency, respectively, are analyzed.

II. RELATED WORKS

In [3], Zhou et al. proposed a PMIPv6 authentication scheme based on diameter protocol, utilizing a pre-shared

Received 01 April 2016, **Revised** 05 April 2016, **Accepted** 25 April 2016
***Corresponding Author** Jaejong Baek (E-mail: jjbaek35@gmail.com, Tel: +82-55-549-6750)
Naval Information and Communication School, Naval Education and Training Command, Changwon 51699, Korea.

Open Access **http://dx.doi.org/10.6109/jicce.2016.14.2.089** print ISSN: 2234-8255 online ISSN: 2234-8883

key between the AAA sever and the proxy mobile entities. They suggested that the interactions between the AAA sever and a proxy mobile entity can reduce the access efficiency. However, they do not mention sharing the key in advance. In [4], Zhang et al. proposed a certificateless signcryption scheme in the authentication process to solve the key management issue in a wireless environment during key negotiations with the AAA server, leading to an increase in the AAA server's cost, and the scheme did not mention how to deal with handoff authentication. In [5], Gao et al. proposed an authentication scheme for PMIPv6 on the basis of a two-level identity-based signature scheme, which is a mutual access authentication protocol, for eliminating the interactions between the home network and an access network and thereby improving authentication efficiency and reducing cost. Nevertheless, their scheme is restricted to mobile access gateways (MAGs) in the same domain and does not consider a reduction in the authentication delay as in the case of the pre-authentication.

III. PROPOSED SCHEME

A. Authentication Architecture

We use EAP-AKA, RADIUS, and the L2 triggers defined in IEEE 802.21 MIH for supporting a secure key distribution, mutual authentication, and inter-local mobility anchor (LMA) HO when a mobile node (MN) crosses the boundaries of a MAG within a PMIPv6 domain. We presume that the MAG and the LMA take charge of the authentication routine for a visiting MN. The AAA client is located at MAG and LMA. When the MN initiates a new session, the MN needs to be authenticated (i.e., initial authentication). In the standard EAP-AKA, the MN and the AAA must generate a master session key (MSK) and an extended MSK (EMSK) after successful authentication [6]. An MSK is delivered to the access point (AP) to be used in generating a transient session key (TSK). An EMSK is generated, but its use is not determined. We propose the use of an EMSK to derive additional keys in order to achieve secure pre-authentication without compromising security. We extend the key hierarchy in the EAP-AKA protocol by introducing MAG domain-level and local-level keys derived from the MSK and the EMSK as shown in Fig. 1. Global-level keys are unique keys derived by the AAA and the MN for a PMIPv6 domain. Local-level keys are unique keys derived by the LMA and the MN for an AP within the MAG domain. Session keys are unique keys derived by the MAG and are later used for deriving TSKs. MSK is used for deriving additional keys for the MN's re-authentication operations without HO. Further, we propose the use of the EMSK as the root key for HO pre-authentications.

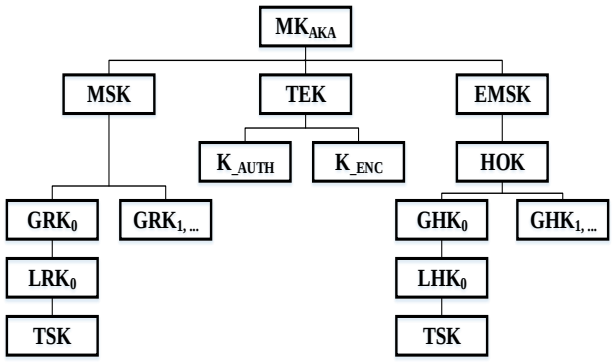

Fig. 1. Key hierarchy of proposed schemes.

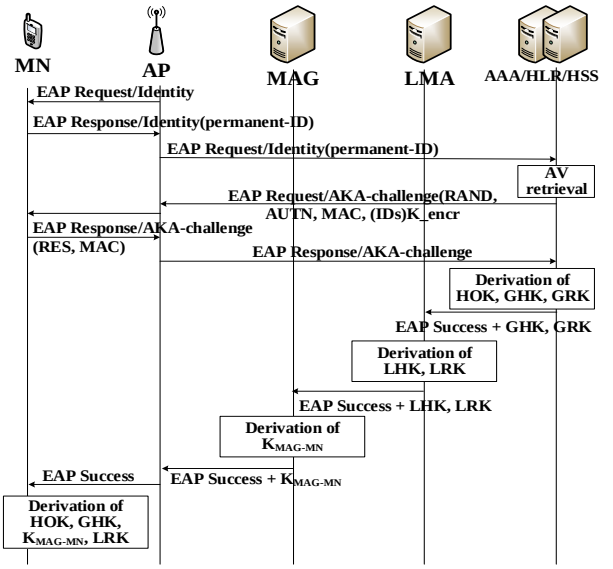

Fig. 2. Modified key initiation procedure of EAP-AKA.

The keys derived from the EMSK are the HO root key (HOK), the global-level HO key (GHK), and the local-level HO key (LHK). LHK is ultimately used for deriving TSK in intra- and inter-MAG HO.

B. Intra/Inter-LMA HO Authentication Procedure

When an MN initiates a new session in a PMIPv6 domain, an authentication procedure is started. To derive the required additional keys, we suggest the following modifications to the EAP-AKA message flow as depicted in Fig. 2. After the EAK-APA protocol is successfully performed, six new keys are generated. The HOK, that is, the root HO key is derived from the EMSK by the AAA and the MN. Both nodes use a special pseudo random function (PRF) similar to the one used in generating the MSK in the standard EAP-AKA protocol.

$$HOK = PRF(EMSK, EAP-AKA_{sessionID} \mid AAAID \mid MN\#, 256), \quad (1)$$

where "|" denotes concatenation and MN# represents the MN address in the medium access control layer. AAAID indicates the identity of the AAA server.

$$EAP-AKA_{sessionID} = (EAP_{typecode} \mid RADN \mid AUTN). \quad (2)$$

The global-level HO key, GHK, is derived from HOK by the AAA and the MN.

$$GHK = PRF(HOK, nonce \mid LMAID \mid MN\#, 256), \quad (3)$$

$$LHK = PRF(HOK, nonce \mid MAGID \mid MN\#, 256), \quad (4)$$

where LMAID and MAGID denote the identity.

The global-level and local-level re-authentication keys, GRK and LRK, are derived from the MSK and the GRK by the AAA and the LMA, respectively.

$$GRK = PRF(MSK, nonce \mid LMAID \mid MN\#, 256), \quad (5)$$

$$LRK = PRF(GRK, nonce \mid MAGID \mid MN\#, 256). \quad (6)$$

A key used for securing traffic between the MN and the AAA, K_{MAG-MN}. This key is exclusively inferred by the MN and the MAG.

$$K_{MAG-MN} = PRF(LHK \oplus LRK \mid MAGID \mid MN\#, 256). \quad (7)$$

Secure delivery of GRK, GHK and TMAGID is performed by the AAA to the LMA. Secure delivery of LRK is performed by LMA to the MAG. The derivation of HOK, GHK, LHK, GRK, LRK, and K_{MAG-MN} by the MN.

C. Intra/Inter-LMA Pre-authentication Procedure

An MN roams to a neighbor AP when experiencing the low signal intensity level of the current AP (CAP). The target AP (TAP) may be in the same LMA domain or belong to a different LMA domain. Because of the lack of an LMA HO authentication protocol in the PMIPv6 domain and the inadaptability of existing MIPv4/MIPv6 authentication protocols, we have designed intra and inter-LMA HO pre-authentication protocols to minimize the authentication delay and the signaling overhead. The proposed protocols utilize the EAP-AKA messages and can efficiently operate in the PMIPv6 domain. The intra-LMA HO is locally carried out when the CAP and the TAP reside in the same LMA domain. Further, the inter-LMA HO is executed when the CAP and the TAP reside in different LMA domains. The intra/inter-LMA HO minimizes the dependency on the HSS and the HAAA to authenticate the MN and thus results in improved performance without compromising security.

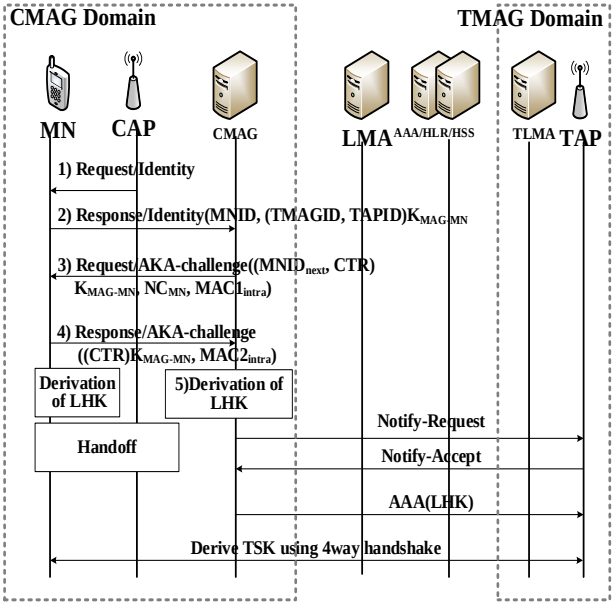

Fig. 3. Inter-MAG HO authentication.

The MN needs to supply the identities of the TAP and the TMAG that it requires to execute an HO to TAPID and TMAGID, respectively. Thus, we propose an adjustment of the IEEE 802.11 probe response management frames sent by the TAP to include its identity and the identity of the MAG associated with it as the information elements (IEs). A part of the IEs is set aside for future use and can be utilized for this purpose [7]. Do note that HO-related decisions such as HO triggers and the best TAP selection are out of the scope of this paper. Further, Fig. 3 depicts the inter-MAG HO authentication operation; here, the MAG controls the MN authentication instead of the HSS and the HAAA. The inter-MAG HO authentication protocol proceeds as follows:

1) When the MN recognizes the need for HO, it sends an EAPoL-start message to the CAP. The AP replies with an identity request message.
2) The MN responds to the request with MNID, TAPID, and TMAGID.
3) Receiving the TMAGID and TAPID indicates an HO pre-authentication request. The MAG classifies this request as an inter-MAG HO if the received TMAGID matches its identity and the TAPID matches the identity of one of the APs in the MAG domain. The MAG then prepares a challenge message that includes a fresh nonce, NC, and the next MNID as well as a counter CTR. The challenge message $MAC1_{Intra}$ can be calculated using K_{MAG-MN} as follows:

$$MAC1_{Intra} = SHA1(K_{MAG-MN}, CTR \mid MNID \mid NC), \quad (8)$$

where SHA1 denotes the secure hash algorithm.

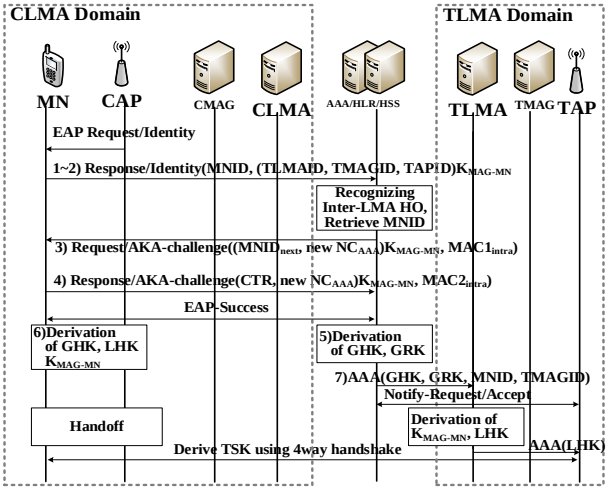

Fig. 4. Inter-LMA HO authentication.

4) At the MN's side, the CTR stored in the MN's memory is matched with the recently received CTR. Then, a new $MAC1_{Intra}$ is calculated and compared with the received $MAC1_{Intra}$. If both the checks are positive, the MN stores MNID and replies with CTR and $MAC2_{Intra}$.

$$MAC2_{Intra} = SHA1(K_{MAG-MN}, CTR | NC). \quad (9)$$

5) The MAG then derives a local-level HO key, LHK, from GHK as follows:

$$LHK = PRF(GHK, CTR | TAPID | TMAGID | MN\#, 512). \quad (10)$$

The MAG also increments CTR and sends an EAP success message to the MN. Consequently, the MN derives LHK and increments CTR. CMAG and TMAG exchange a notify-request and notify-accept RADIUS AAA message to confirm the HO operation. Finally, LHK is sent to the TAP in the RADIUS access-accept messages with the MS-MPPE-Recv-Key attribute [8].

In the inter-LMA HO, the authentication procedure is completed without the need to retrieve security keys from the HSS, as shown in Fig. 4. The protocol procedure is as follows:

1) The MN replies to the identity request message with MNID, TLMAID, TMAGID, and TAPID.
2) The HO pre-authentication request is classified as inter-LMA by the MAG if the TMAGID does not match its identity and TAPID does not match any of the AP identities in the MAG domain. The MAG retrieves the MN permanent ID and forwards it along with the TAPID, TMAGID, and TLAMID to the AAA.
3) Upon receiving the IDs, the AAA recognizes that an inter-LMA HO is requested and prepares an authentication challenge. The challenge includes the next MNID ($MNID_{next}$), NC_{MN}, and the newly generated NC_{AAA}. $MAC1_{Inter}$ can be calculated as follows:

$$MAC1_{Inter} = SHA1(K_{auth}, NC_{MN} | MNID | NC_{AAA}), \quad (11)$$

where NC_{MN} was previously received by the AAA in the modified EAP-AKA protocol.
4) Upon receiving the authentication challenge, the MN checks NC_{MN}, calculates a new $MAC1_{Inter}$, and compares it with the received $MAC1_{Inter}$. If all verification returns positive, $MNID_{next}$ is stored and a reply message is prepared. The reply message includes the new NC_{AAA}, newly generated NC_{MN}, CTR, and $MAC2_{Inter}$,

$$MAC2_{Inter} = SHA1(K_{auth}, newNC_{MN} | CTR | lastNC_{AAA}). \quad (12)$$

5) Upon receiving the message, the AAA confirms CTR and verifies $MAC2_{Inter}$. If all verifications are positive, the AAA validates the HOK lifetime and derives a new GHK and GRK, and an EAP success message is sent to the MN.
6) Upon receiving the EAP success message, the MN derives a new GHK, GRK, $K_{TMAG-MN}$, and LHK. It also increments CTR.
7) An AAA message that includes GHK, GRK, CTR, MN permanent ID, $MNID_{next}$, and TAPID is sent to the TMAG by the AAA. As a result, $K_{TMAG-MN}$ and LHK are generated and CTR is incremented by TMAG. Lastly, TMAG confirms HO with TAP by exchanging the RADIUS AAA notify-request and notify-accept messages and forwards LHK in the access-accept message. The MAG also increments CTR and sends an EAP success message to the MN. Therefore, the MN derives LHK and increments CTR. CMAG and TMAG exchange the notify-request and notify-accept RADIUS AAA messages to confirm the HO operation [9]. Finally, LHK is pushed to the TAP in the RADIUS access-accept message with the MS-MPPE-Recv-Key attribute.

At the conclusion of a successful intra- or inter-LMA HO, a fresh LHK is retained by the MN and the TAP. The LHK is used for deriving TSK, which is then applied to generate additional keys that are demanded to secure the channel between the MN and the TAP.

IV. PERFORMANCE ANALYSIS

A. Analysis of Average Authentication Cost

We define the authentication cost as the amount of signaling load and processing load during each authentication procedure. Then, the initial authentication cost, C_i, can be represented as follows:

$$C_i = 2(N_h + 3)C_t + 2C_v + 3C_{ed} + 12C_k . \quad (13)$$

where N_h denotes the number of hops between the MN and the AAA server. The first item is the signaling cost, and the other items are the processing costs. The cost parameters C_t, C_v, C_{ed}, and C_k denote the transmission cost on one hop, the verification cost of the AAA server, a pair of encryption and decryption costs for a value, the key generation cost, respectively. As shown in Fig. 2, an MN needs to request identity from the MAG first. The distance that the messages traverse is 2 in this step. Then, the authentication messages need to reach the AAA. The distance between the MN and the AAA is assumed to be N_h hops. Since no security association (SA) exists between the MAG and the LMA, a mutual authentication process to the LMA is needed, which requires the messages to traverse four more hops in a round-trip transmission. Thus, the total number of hops that the authentication messages traverse in the round-trip transmission is $2 + 2N_h + 4 = 2(N_h + 3)$. In this authentication process, the challenge/response values are verified twice at the AAA and the MN for mutual authentication. Thus, the coefficient for C_v is 2. In this process, three pairs of encryption and decryption costs are needed. The first pair is for encrypting and decrypting the challenge/response values between the MN and the AAA; the second is for encrypting and decrypting the session key between the AAA and the LMA; and the third is for encrypting and decrypting the session key between the AAA and the MAG. Thus, the coefficient for C_{ed} is 3. Because the AAA needs to generate a dynamic key for the LMA, the MAG, and the MN, the coefficient for C_k is 12. As shown in Fig. 3, we can determine the inter-MAG HO authentication cost, C_{mh}, as follows:

$$C_{mh} = 2(N_h + 1)C_t + 2C_V + 3C_{ed} + 4C_k + 2N_m C_t , \quad (14)$$

where the last processing cost, $2N_mC_t$, is the transmission cost for the notify-request, notify-accept, and AAA messages between the CMAG and the TMAG. The cost parameter N_m denotes the number of hops between the CMAG and the TMAG. The average authentication cost is defined as the sum of the authentication cost over a number of ARs per unit time, which can be written as follows:

$$\overline{C}_{mh} = \lambda_\mu C_i + \lambda_\mu MAX(N_m - 1,0)C_{mh} \quad (15)$$

where C_i and C_{mh} represent the initial and the HO authentication cost expressed in Eqs. (13) and (14), respectively, and λ_μ denotes the call arrival rate. As shown in Fig. 4, we can determine the inter-LMA HO authentication cost, C_{lh}, as follows:

$$C_{lh} = 2(N_h + 1)C_t + 2C_V + 3C_{ed} + 8C_k + 4N_m C_t \quad (16)$$

where the last processing cost, $4N_mC_t$, is the transmission cost for the notify-request, notify-accept, and two AAA messages between the CLMA and the TLMA. The cost parameter N_m denotes the number of hops between the CLMA and the TLMA. The average authentication cost is defined as the sum of the authentication cost over a number of ARs per unit time, which can be written as follows:

$$\overline{C}_{lh} = \lambda_\mu C_i + \lambda_\mu MAX(N_m - 1,0)C_{lh} , \quad (17)$$

where C_i and C_{lh} denotes the initial and the HO authentication cost in Eqs. (13) and (16), respectively, and $\lambda\mu$ represents the call arrival rate.

B. Analysis of Average Authentication Delay

We define authentication delay as the time from when an MN sends out an AR to when the MN receives the authentication reply (i.e., the EAP success message). Then, the delay per initial authentication, T_i, can be written as follows:

$$\begin{aligned} T_i = {} & 2(N_h + 3)(T_{pr} + T_{tr}) + 4T_{wm} \\ & + 2T_{wa} + 2T_v + 3T_{ed} + 12T_k \end{aligned} , \quad (18)$$

where the time parameters T_{pr}, T_{tr}, T_{wm}, T_{wa}, T_{ed}, T_v, and T_k represent the message propagation time on one hop, the message transmission time on one hop, the AR service and waiting time at the MAG, the AR service and waiting time at the AAA, a pair of encryption and decryption times for a value, the verification time at the MN/the AAA, and the key generation time at the AAA, the LMA, the MAG and the MN, respectively. The coefficients in front of the time variables in T_i denote the number of time variables for each authentication. Similar to the analysis in Eq. (13), we can calculate the number of hops that the round-trip signaling messages traverse in the authentication process to be $2(N_h + 3)$. Then, the coefficient in front of $T_{pr} + T_{tr}$ is $2(N_h + 3)$. Since the authentication process needs to pass the MAG four times, the coefficient of T_{wm}, i.e., the AR service and waiting time, is 4. Because the authentication message traverses the AAA twice, the coefficient of T_{wa}, i.e., the AR service and waiting time at the AAA, is 2. Similar to the coefficient analysis in front of C_{ed} and C_k in Eq. (13), we can calculate the coefficient of T_{ed} to be 3 and the coefficient of T_k to be 12. As shown in Fig. 3, the delay per inter-MAG HO authentication, T_{mh}, can be expressed as follows:

$$\begin{aligned} T_{mh} = {} & 2(N_h + 1)(T_{pr} + T_{tr}) + 4T_{wm} + 3T_{wm} \\ & + 3T_{ed} + 2T_V + 4T_k + 2N_m(T_{pr} + T_{tr}) \end{aligned} , \quad (19)$$

where the time parameter N_m denotes the number of hops between the PMAG and the TMAG. The average authentication delay is defined as the sum of an authentication delay over a number of ARs in unit time, which can be expressed as follows:

$$\overline{T}_{am} = \lambda_{\mu} T_i + \lambda_{\mu} MAX(N_m - 1,0) T_{mh} \quad , \tag{20}$$

where T_i and T_{mh} denote the delay per initial and inter-MAG HO authentication expressed in Eqs. (18) and (19), respectively, and λ_{μ} represents the call arrival rate. As shown in Fig. 4, the delay per inter-LMA HO authentication, T_{lh}, can be expressed as follows:

$$\begin{aligned} T_{lh} = {} & 2(N_h + 1)(T_{pr} + T_{tr}) + 4T_{wm} + 3T_{wa} \\ & + 3T_{ed} + 2T_V + 8T_k + 2N_m(T_{pr} + T_{tr}) \end{aligned} \quad , \tag{21}$$

where the time parameter N_m denotes the number of hops between the previous LMA (PLMA) and the target LMA (TLMA). The average authentication delay is defined as the sum of an authentication delay over a number of ARs in unit time, which can be expressed as follows:

$$\overline{T}_{al} = \lambda_{\mu} T_i + \lambda_{\mu} MAX(N_m - 1,0) T_{lh} \quad , \tag{22}$$

where T_i and T_{lh} represent the delay per initial and inter-LMA HO authentication shown in Eqs. (18) and (21), respectively, and λ_{μ} represents the call arrival rate.

C. Analysis of Results

The parameters to evaluate the authentication cost and delay are shown in Table 1. Some parameter values for the analysis have been taken from [3]. The authentication cost in Eqs. (13), (14), and (16) can be calculated using the number of messages [10]. We utilize the ratio of the processing times to obtain the authentication cost because the time required to complete an operation represents the payload of the server to complete it [11]. The key generation cost, C_k, is normalized to a cost unit because it is the lightest load compared to the other costs. The values of the other costs are determined by a comparison with C_k using the time taken to complete the procedure. In Eqs. (13), (14), and (16), we only consider T_{wm}, T_{wa}, and T_v to be the random variables because the variance of the other time variables is small. T_{pr} is a function of the distance between two points, T_{tr} is determined by the message length and the link speed, T_{ed} is mainly related to the performance of the computer and the message length, and T_k is directly related to the computer performance. In practice, the distance between two points, the message length, the link speed, and the computer performance are all fixed. Therefore, we do not consider T_{pr}, T_{tr}, T_{ed}, and T_k random variables in this work. However, T_{wm}, T_{wa} and T_v are all related to the traffic load, queue length, and service time, which are varied from time to time and have a large variance. For the sake of simplification, we consider that the M/M/1 queues are applied at the MAGs, LMAs and the AAA and that the PDFs of T_{wm}, T_{wa}, and T_v are independent, identical distributions. The effects of the mobility and the traffic pattern on the average authentication cost and delay are shown in Figs. 5–12. In Figs 5 and 6, the average authentication costs decrease with an increase in the residence time of an MN in a MAG because the longer an MN stays in the MAGs, the lower is the handoff AR. Thus, if the residence time of an MN approaches infinity, the authentication cost will be stable and will be the same as the initial authentication cost because only the initial authentication exists in this case. Conversely, when the residence time approaches 0, most of the authentications are handoff authentications and the average authentication cost approaches infinity. However, for the sake of clarity, this is not depicted in Figs. 5 and 6. Figs. 7 and 8 show that the average authentication costs increase with an increase in the call arrival rate of an MN. As shown in Eqs. (15) and (17), the authentication cost is proportional to the call arrival rate λ_{μ}.

Figs. 5–8 show that the average authentication cost increases with an increase in the number of hops between the AAA servers. This is attributed to the fact that a relatively high transmission cost will be needed in such a case. Figs. 9 and 10 show the effect of the residence time on the average authentication delay. As we can see, the authentication delay decreases with an increase in the residence time of an MN in a MAG. As in the case of the authentication cost, this trend is attributed to the decrease in the handoff AR. Thus, if the residence time of an MN approaches infinity, the authentication delay will be the same as the initial authentication delay. In contrast, when the residence time approaches 0, most of the authentications are handoff authentications and the average

Table 1. Parameters for evaluation

Parameter	Value	Parameter	Value
C_t	5	T_{pr}	20 μs
C_v	10	T_{tr}	10 ms
C_{ed}	1	T_{um}	10^{-1} s
C_k	1	T_{wa}	10^{-1} s
N_h	4	T_v	10^{-1} s
N_m	1	T_{ed}	5 ms
T_k	5 ms	λ_{μ}	0.2^{-1} min
η	0.5 min^{-1}	μ_{γ}	$(1/2)^{-1}$ min

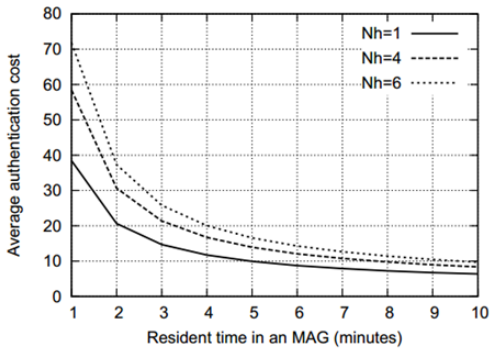

Fig. 5. Authentication cost versus residence time in inter-MAG HOs.

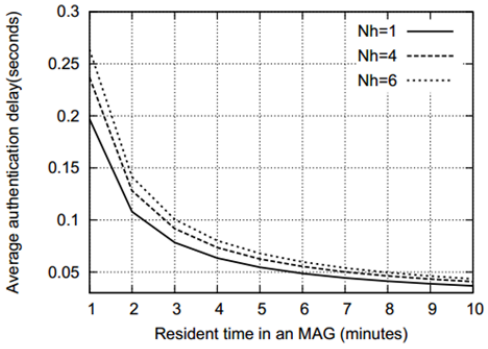

Fig. 9. Authentication delay versus residence time in inter-MAG HOs.

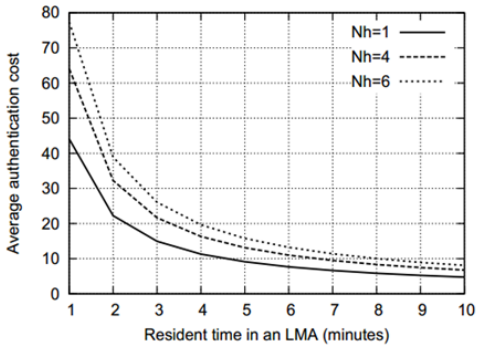

Fig. 6. Authentication cost versus residence time in inter-LMA HOs.

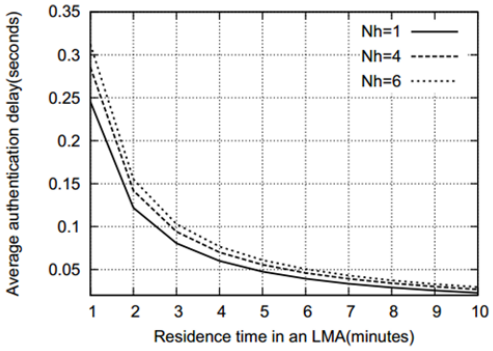

Fig. 10. Authentication delay versus call arrival rate at inter-MAG HOs.

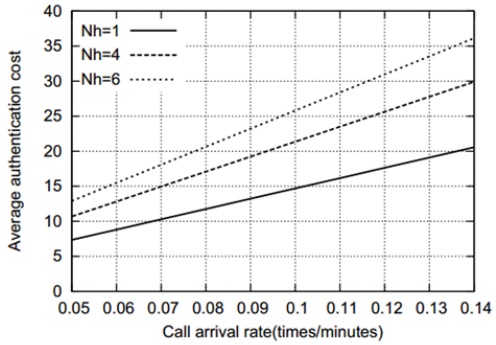

Fig. 7. Authentication cost versus call arrival rate in inter-MAG HOs.

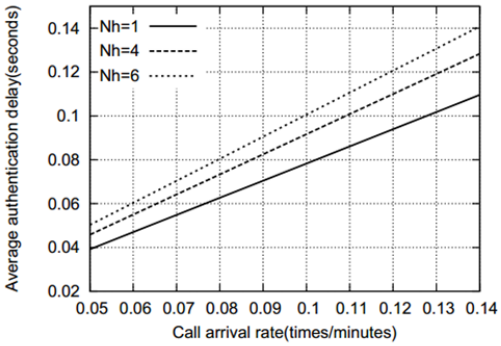

Fig. 11. Authentication delay versus call arrival rate at inter-MAG HOs.

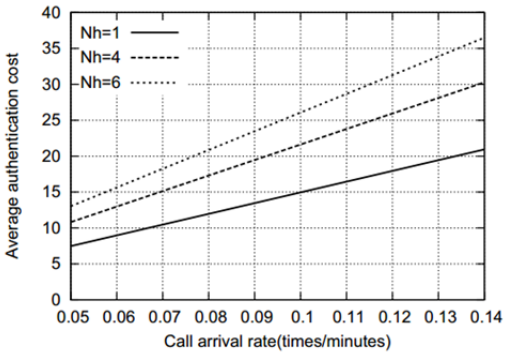

Fig. 8. Authentication cost versus call arrival rate at inter-LMA HOs.

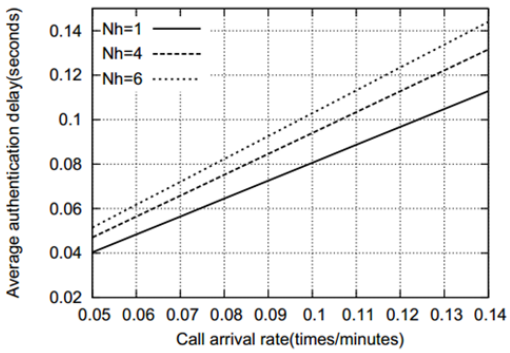

Fig. 12. Authentication delay versus call arrival rate at inter-LMA HOs.

authentication delay approaches infinity. However, for the sake of clarity, this is not shown in Figs. 9 and 10. Figs. 11 and 12 show that the average authentication delay increases with an increase in the call arrival rate of an MN. As shown in Eqs. (20) and (22), the authentication delay is proportional to the call arrival rate λ_{μ}. Figs. 9–12 show that the average authentication delay increases with an increase in the number of hops between the MN and the AAA server as more message propagation time and message transmission time are needed.

V. CONCLUSION

In this paper, we proposed a pre-authentication method for the PMIPv6 protocol, which invokes the EAP-AKA signaling messages towards the AAA system. The proposed secure pre-authentication method prevents threats such as replay attacks and key exposure. We also conducted a performance analysis of the authentication cost and delay with respect to the mobility and traffic patterns. Therefore, this scheme presents a further understanding of the authentication mechanism in PMIPv6 networks. In the future, we plan to improve the proposed authentication method with a more detailed security analysis and better comparisons with other new authentication mechanisms in a PMIPv6-based network.

REFERENCES

[1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," The Internet Engineering Task Force, Fremont, CA, RFC 5213, 2008.

[2] S. Wie and J. Jang, "Tunnel-free scheme using a routing table in a PMIPv6-based nested NEMO environment," *Journal of Information and Communication Convergence Engineering*, vol. 11, no. 2, pp. 82-94, 2013.

[3] H. Zhou, H. Zhang, and Y. Qin, "An authentication method for proxy mobile IPv6 and performance analysis," *Security and Communication Networks*, vol. 2, no. 5, pp. 445-454, 2009.

[4] L. Zhang, T. Mo, and L. Zhao, "Authentication scheme based on certificateless signcryption in proxy mobile IPv6 network," *Application Research of Computers*, vol. 29, no. 2, 2012.

[5] T. Gao, L. Tan, P. Qiao, and K. Yim, "An access authentication scheme based on Hierarchical IBS for proxy mobile IPV6 network," *Intelligent Automation & Soft Computing*, vol. 22, no. 3, pp. 389-396, 2016.

[6] 3GPP, "3G security; Wireless Local Area Network (WLAN) interworking security," 3GPP TS 33.234 (v8.1.0), 2008.

[7] 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: Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE SA 802.11i-2004, 2004.

[8] J. Arkko and H. Haverinen, "Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)," The Internet Engineering Task Force, Fremont, CA, RFC 4187, 2006.

[9] W. Arbaugh and B. Aboba, "Handoff extension to RADIUS," draft-irtf-aaaarch-handoff-04.txt, 2003 [Internet], Available: https://www.ietf.org/archive/id/draft-irtf-aaaarch-handoff-04.txt.

[10] S. Baek, S. Pack, T. Kwon, and Y. Choi, "A localized authentication, authorization, and accounting (AAA) protocol for mobile hotspots," in *Proceedings of 3rd Annual Conference on Wireless On-demand Network Systems and Services (WONS2006)*, Les Menuires, France, pp. 144-153, 2006.

[11] W. Liang and W. Wang, "On performance analysis of challenge/response based authentication in wireless networks," *Computer Networks*, vol. 48, no. 2, pp. 267-288, 2005.

Jaejong Baek
received his B.S. in Computer Science from Hanbat National University, Daejeon, Korea, in 1992 and his M.S. and Ph.D. in Computer Science from Yonsei University, Seoul, Korea, in 2001 and 2011, respectively. He has worked as an adjunct professor in the department of Defense Science and Technology at Howon University from 2015. His research interests include handover authentication, network security, cyber warfare, and NCW.