An Efficient Handover Authentication Scheme Based on HMAC for Proxy Mobile IPv6 Network

Tianhan Gao[1]*, Ling Tan[1], Peiyu Qiao[1], and Kangbin Yim[2]
[1]Faculty of Software College, Northeastern University, No.11
the 3rd Lane,Wenhua Road, Heping District, Shenyang, 110819, China
gaoth@mail.neu.edu.cn, moonweak@163.com, qpy_11@sina.com
[2]Faculty of Information Security Engineering, Soonchunhyang University,336745 Asan, Korea
yim@sch.ac.kr

Abstract

Proxy mobile IPv6 plays a significant role in optimizing the performance of mobile IPv6 and achieving the support for network mobility management. But the open nature and lack of security consideration result in potential threat. The requirement of the real-time application of mobile node leads us to develop a handover authentication scheme which satisfies certain security and efficiency needs. In this paper, based on the 2-HIBS scheme, the handover authentication scheme is implemented by utilizing hash-based message authentication code (HMAC). The proposed scheme makes an excellent combination between initial access authentication and handover authentication procedures. We also evaluate the handover authentication latency between our scheme and other authentication schemes. The results show that our scheme has higher efficiency and lower communication cost than existing ones.

Keywords: Proxy Mobile IPv6, access authentication, handover authentication

1 Introduction

Proxy Mobile IPv6 protocol[7] (PMIPv6) supports the mobility of IPv6 nodes by extending the signal between mobile node (MN) and home agent (HA) in Mobile IPv6 protocol[3](MIPv6), which eliminates the signal interaction between MN and HA. PMIPv6 plays a significant role in optimizing the performance of Mobile IPv6 and achieving the support for network mobility management. Although NETLMN presents the official standard of PMIPv6, which only ensures the continuous communication of mobile users, the open nature and lack of security consideration result in potential threat. The security of PMIPv6 is based on access security[9]. When MN accesses foreign network, mutual authentication between MN and the proxy mobile entities is necessary. To satisfy the requirement of the real-time application of MN, handover and authentication must occur simultaneously and possess high efficiency. Thus, more efficient handover authentication schemes become a popular research issue.

In the existing research of PMIPv6 access authentication, [6] proposed a packet lossless PMIPv6 (PL-PMIPv6) which uses a buffer mechanism to prevent packet loss during handover, but the scheme results in long handover latency. [5] proposed a certificated-based authentication scheme to provide security for PMIPv6 (C-PMIPv6). Although this scheme ensures the security of the handover procedure, it does not improve the situation of long handover latency and suffers from the packet loss problem. [11] proposed a PMIPv6 authentication scheme based on Diameter protocol[4] where access authentication is

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 4 (January 15, 2015)

*Corresponding author: Department of Software college, Northeastern University, No.11, the 3rd Lane, Wenhua Road, Heping District, Shenyang, 110006, China, Tel: 8624-83681822 achieved by pre-sharing the key between AAA[1] sever and proxy mobile entities. But the enhancement of signal interaction between AAA sever and proxy mobile entities also reduces MN access efficiency. [2] proposed a 2-HIBS scheme based on identity-based cryptography which efficiently eliminates the signal interaction between access network and home network. However, it only presented an initial access authentication scheme, no consideration of handover authentication issue.

In this paper, based on the 2-HIBS scheme, we propose a handover authentication scheme by utilizing hash-based message authentication code (HMAC). The scheme eliminates the complicated calculation process of bilinear pairing and makes an excellent combination between initial access authentication and handover authentication procedures that contributes to achieving higher efficiency and lower communication cost. In addition, we also evaluate the handover authentication latency between our scheme and other handover authentication schemes, which shows that our scheme owes excellent performance in access authentication efficiency.

The rest of this paper is organized as follows. Section 2 briefly describes PMIPv6 and 2-HIBS scheme proposed in [2]. Section 3 shows initial access authentication scheme proposed in [2] and introduces a handover authentication scheme based on HMAC. Section 4 evaluates the handover authentication latency between our scheme and other authentication schemes. Finally, we make a conclusion about this paper in section 5.

2 Preliminaries

2.1 PMIPv6

All control messages and system status of PMIPv6 is managed and sustained by two news core entities in the network. One is local mobility anchor (LMA). LMA is the topological anchor of the home network prefix of MN and manages the binding status about MN. The other entity is mobile access gateway (MAG). MAG is implemented on access router and executes mobility management instead of MN, so that MN can gain mobility support without any configuration of mobility management protocol. Thus, the complexity of MN's protocol stack is reduced.

As shown in Figure. 1, network is divided into home domain and foreign domain. HLMA represents home domain authentication sever while FLMA represents foreign domain authentication sever.

2.2 2-HIBS scheme

Proposed in [2], 2-HIBS is organized by five algorithms including Root-PKG Setup, Level-1-PKG Extract, Level-2-PKG Extract, Sign and Verify. The scheme owes two level of users. The first level user's identity is $ID_{1=\{I_1\}}$ and the second level user's identity is $ID_{2=\{I_1,I_2\}}$, where$I_1, I_2 \in \{0,1\}^*$. The main idea about 2-HIBS is illustrated as below.

1. Root-PKG Setup
   Generating the public parameters of the system;

2. Level-1-PKG Extract
   Generating private key for the first level PKG such as FLMA and HLMA by using its own identity information;

3. Level-2-PKG Extract
   The first level PKG generates private key for the second level PKG such as MN and MAG, by using the identity information of the second level PKG;

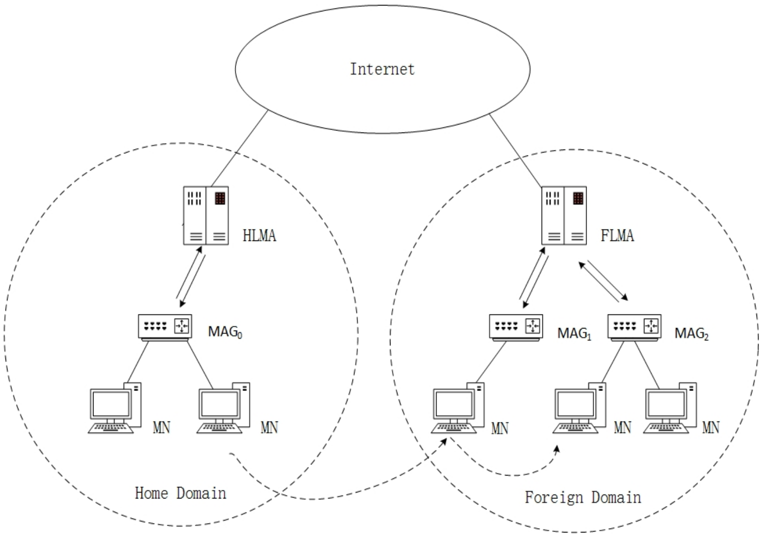

Figure 1: Network architecture of PMIPv6

4. Sign
   Signing message M in different ways in terms of signers' identity;

5. Verify
   Once receiving the signature of the message M under identity $ID_{i(i\in\{1,2\})}$, the verification process is started.

3 Access authentication scheme for PMIPv6

3.1 Notations and descriptions

To simplify the illustration of our scheme, some notations and descriptions are presented in Table. 1.

3.2 Initial access authentication scheme

As shown in Figure. 1, once MN leaves home domain and initially accesses MAG_1 in foreign domain, the initial access authentication will be triggered. The specific steps proposed in [2] are shown in Fig. 2.

1. $MN \rightarrow MAG_1 : [g^a, MN_{Info}, TS_1, \sigma_1]$
   MN randomly chooses $a \in Zq^*$, then generates the key agreement parameter g^a and utilizes 2-HIBS scheme to obtain the private key $d_{ID_{MN}}$ to calculate the signature $\sigma_1 = Sign_{MN\_d_{ID_{MN}}}(g^a \| MN_{Info} \| TS_1)$. g^a, MN_{Info}, TS_1 and σ_1 are assembled into an authentication request message REQ and is sent to MAG_1.

2. $MAG_1 \rightarrow FLMA : \{HNP_{MN} \| g^a\}$
   After receiving REQ, MAG_1 first verifies the freshness of TS_1, if it is fresh, the identity information $ID_{MN} = (I_{HLMA}, I_{MN})$ is extracted from MN_{Info}. According to the system parameter and ID_{MN}, MAG_1 verifies the signature: $Verify_{MAG_1\_ID_{MN}}(\sigma_1)$, if verification is done successfully, then MN is regarded as a legal user. MAG_1 extracts HNP_{MN} from MN_{Info}, then sends HNP_{MN} through PBU to FLMA.

Table 1: Notations and description

Notations	**Descriptions**
ID_A	The identity of entity A
I_A	Network access identifier of entity A
MN_{Info}	Configuration information of MN
$sign_{A\_SK}(M)$	Singer A use 2-HIBS algorithm to generate signature under private key SK on message M
$Verify_{A\_ID_B}(\sigma)$	Singer A use 2-HIBS algorithm to verify signature σ under the identity of $B(ID_B)$
K_{A-B}	The shared key between A and B
$HMAC_{K_{A-B}}(M)$	Using the shared key between A and B calculates message M under HMAC
$VerifyH_{K_{A-B}}(\theta)$	Using the shared key between A and B verifies result θ under HMAC
$A \to B\{M\}$	A sends message to B through security channel
$A \to B[M]$	A sends message to B through public channel
HNP_{MN}	Home network prefix of MN
PF_{MN}	Address configuration policy file of MN, including HNP_{MN} and related address configuration
TS	The current timestamp
$\|\|$	Concatenate two messages

3. $FLMA \to MAG_1 : \{PF_{MN}, g^b\}$
   After receiving PBU, FLMA extracts HNP_{MN} and checks whether this HNP_{MN} is in the binding cache entry (BCE), if HNP_{MN} already exists in BCE and the corresponding MN is different from the request one, MAG_1 sends PBA message to reject this access. Otherwise, FLMA randomly chooses $b \in Zq^*$, calculates key negotiation parameter g^b and the shared key $K_{FLMA-MN} = g^{ab}$, then saves $K_{FLMA-MN}$ to the local BCE. Finally, FLMA stores the network prefix distributed to MN and the address configuration strategy PF_{MN}. FLMA sends PF_{MN}, g^b through the PBA message back to MAG_1.

4. $MAG_1 \to MN : [PF_{MN}, ID_{MAG_1}, g^b, TS_2, \sigma_2]$
   After receiving PBA, MAG_1 extracts PF_{MN} and g^b, calculates the shared key $K_{MN-FLMA} = g^{ab}$ and keeps it locally. Then MAG_1 generates the signature $\sigma_2 = Sign_{MAG_1\_d_{ID_{MAG_1}}}(g^b \| PF_{MN} \| ID_{MAG_1} \| TS_2)$. Finally, $PF_{MN}, ID_{MAG_1}, g^b, TS_2$ and σ_2 are assembled into routing announcement message RA and is sent to MN.

5. MN
   Upon receiving RA, MN first checks the freshness of TS_2, if it is fresh, MN extracts information

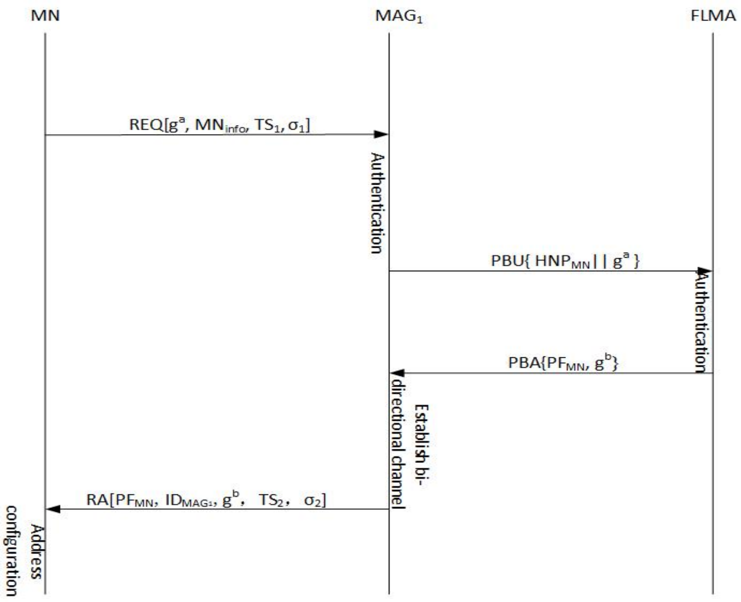

Figure 2: Initial access authentication procedure

from RA and verifies signature σ_2 according to ID_{MAG_1} and system parameter:$Verify_{MN\_ID_{MAG_1}}(\sigma_2)$. If the verification success, MN makes sure to access a legal MAG and configures its IPv6 address according to PF_MN. Meanwhile, MN calculates $K_{MN-FLMA} = g^{ab}$ and saves the results in terms of g^b to complete the mutual authentication.

3.3 Handover authentication scheme

As shown in Figure. 1, while MN roams to MAG_2 from MAG_1 in foreign domain, handover authentication is triggered. We propose a handover authentication scheme based on HMAC by using the shared key between MN and FLMA which is generated from the initial access authentication procedure. The specific steps are shown in Figure. 3:

1. $MN \rightarrow MAG_2 : [MN_{Info}, TS_3, \sigma_3]$
   Using HMAC algorithm, MN calculates $\sigma_3 = HMAC_{K_{MN-FLMA}}(MN_{Info} \| TS_3)$ by utilizing MN_{Info}, TS_3 and the shared key $K_{MN-FLMA}$ generated during initial authentication phase. Then, MN_{Info}, TS_3 and σ_3 are assembled into an authentication request message REQ which is sent to MAG_2.

2. $MAG_2 \rightarrow FLMA : \{HNP_{MN}\}$
   After receiving REQ, MAG_2 first verifies the freshness of TS_3. If it is fresh, HNP_{MN} is extracted from MN_{Info}. Then, MAG_2 sends HNP_{MN} through PBU to FLMA and requests the shared key $K_{MN-FLMA}$.

3. $FLMA \rightarrow MAG_2 : \{PF_{MN}, K_{FLMA-MN}\}$
   After receiving PBU, FLMA extracts HNP_{MN} from PBU and removes the shared key $K_{MN-FLMA}$ from BCE. Then, FLMA sends PF_{MN} and $K_{MN-FLMA}$ through the PBA message back to MAG_2. At the same time, the access router information of MN stored in BCE is updated.

4. $MAG_2 \rightarrow MN : [PF_{MN}, TS_4, \sigma_4]$
   After receiving PBA, MAG_2 verifies σ_3: $Verify_{K_{FLMA-MN}}(\sigma_3)$ by using $K_{MN-FLMA}$ extracted from

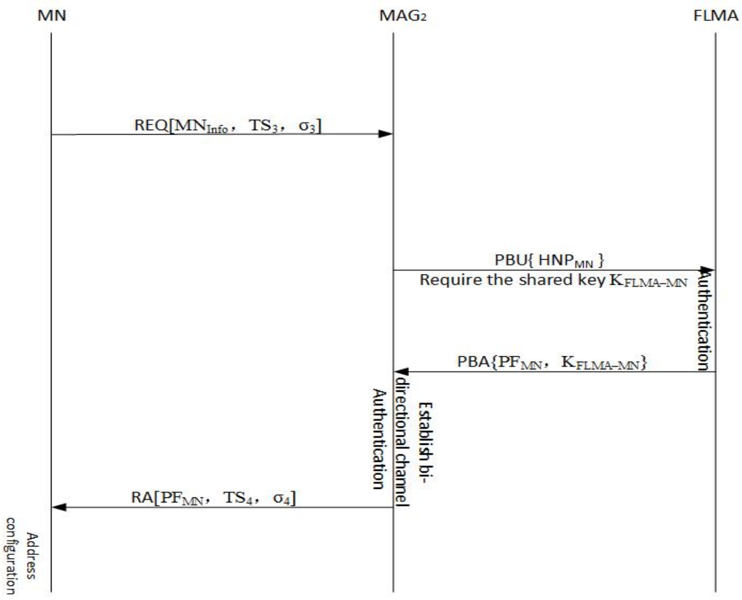

Figure 3: Handover authentication procedure

PBA. if the verification is done successfully, MN is regarded as a legal user .Then, MAG_2 calculates σ_4: $\sigma_4 = HMAC_{K_{FLMA-MN}}(PF_{MN} \| TS_4)$. Finally, PF_{MN}, TS_4, σ_4 are assembled into routing announcement message RA and is sent to MN. At the same time, $K_{MN-FLMA}$ is stored locally.

5. MN
   Upon receiving RA, MN checks the freshness of TS_4. If it is fresh, MN verifies $\sigma_4 : Verify_{K_{FLMA-MN}}(\sigma_4)$ by using $K_{MN-FLMA}$. If the verification success, MN makes sure to access legal MAG_2 and configures its IPv6 address according to HNP_{MN} in PF_{MN}.

4 Performance analysis

Authentication latency is defined as the interval from that MN received the first broadcast message after accessing foreign domain to that the mutual authentication between MN and access network is finished. In addition, authentication latency plays a significant role in the performance of mutual access authentication schemes. In the existing access authentication schemes for PMIPv6, the authentication information of MN is stored in home domain or remote sever: AAA sever. In order to achieve access authentication, MN must interact with home domain or remote sever which increases authentication latency in pace with the enhancement of distance between home domain and foreign domain. Consequently, the number of interactions among MAG, LMA and AAA sever becomes the important factor to affect the authentication latency.

As shown in Table. 2, T_{ma} refers the number of interactions between MAG and AAA sever; T_{la} means the number of interactions between LMA and AAA sever; T_{ml} means the number of interactions between MAG and LMA sever. HLMA in OTK[8] severs as AAA sever that authenticates MN. Compared with other schemes such as APFP[11],CSS[10],OTK in terms of T_{ma}, T_{la} and T_{ml}, our handover scheme achieves local authentication and eliminates communication latency cost between itself and remote sever. Thus, our scheme presents excellent performance in authentication latency than other ones.

Table 2: Comparative results of authentication efficiency among different schemes

Authentication Scheme	T_{ma}	T_{la}	T_{ml}
APFP	2	2	2
CSS	2	0	2
OTK	0	2	2
This paper	0	0	2

5 Conclusions

Access authentication is an essential and necessary approach to address the security problem of PMIPv6 in the situation that authentication is triggered simultaneously with handover. In this paper, we propose a handover authentication scheme to eliminate the interactions between access network and home network. Compared with other similar schemes, our scheme efficiently improves the efficiency of handover authentication.

In the future research, we will optimize the details of our scheme to further enhance the authentication efficiency.

Acknowledgements

This work was supported by Major National Scientific & Technological Projects of China under Grant No. 2013ZX03002006

References

[1] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence. Generic AAA Architecture. IETF Internet-draft (work in progress), August 2000. `https://datatracker.ietf.org/doc/rfc2903/`.

[2] T. Gao and P. Qiao. An access authentication scheme based on 2-hibs in proxy mobile ipv6 network. *International Journal of Security and Its Applications*, November 2014.

[3] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. IETF RFC 3775, June 2004. `http://www.ietf.org/rfc/rfc3775.txt`.

[4] F. Le, B. Patil, C. E. Perkins, and S. Faccin. Diameter mobile ipv6 application. IETF Internet-draft (work in progress), November 2004. `http://www.ietf.org/archive/id/draft-le-aaa-diameter-mobileipv6-04.txt`.

[5] T. Ling and H. Di. A certificated-based binding update mechanism for proxy mobile ipv6 protocol. In *Proc. of the 2009 Asia Pacific Conference on Postgraduate Research in Microelectronics & Electronics (PrimeAsia'09), Shanghai, China*, pages 333–336. IEEE, January 2009.

[6] S. Ryu, G.-Y. Kim, B. Kim, and Y. Mun. A scheme to reduce packet loss during pmipv6 handover considering authentication. In *Proc. of the 2008 International Conference on Computational Sciences and Its Applications (ICCSA'08), Perugia, Italy*, pages 47–51. IEEE, July 2008.

[7] E. S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil. Proxy Mobile IPv6. IETF RFC 5213, August 2008. `http://www.ietf.org/rfc/rfc5213.txt`.

[8] J. Song and S. Han. One-time key authentication protocol for pmipv6. In *Proc. of the 3rd International Conference on Convergence and Hybrid Information Technology (ICCIT '08), Busan, Korea*, volume 2, pages 1150–1153. IEEE, November 2008.

[9] C. Vogt and J. Kempf. Security Threats to Network-Based Localized Mobility Management (NETLMM). IETF RFC 4832, April 2007. `http://www.ietf.org/rfc/rfc4832.txt`.

[10] L. Zhang, T. Mo, and L. Zhao. Authentication scheme based on certificateless signeryption in proxy mobile ipv6 network. *Application Research of Computers*, 29(2):411–414, February 2012.

[11] H. Zhou, H. Zhang, and Y. Qin. An authentication protocol for proxy mobile ipv6. *Acta Electronica Sinica*, 36(10):1873–80, October 2008.

Author Biography

Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained an early promotion to an associate professor in January 2010. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He is the author or co-author of more than 30 research publications. His primary research interests are next generation network security, MIPv6/HMIPv6 security, wireless mesh network security, Internet security, as well as security and privacy in ubiquitous computing.

Peiyu Qiao is a master's degree student majoring in Software Engineering at Northeastern University in China. His primary research interests are mobile computing and network security.

Ling Tan is an undergraduate student majoring in Information Security at Northeastern University in china. Her primary research interests are mobile computing and network security.

Kangbin Yim received his B.S. M.S. and Ph.D. from Ajou University, Suwon, Republic of Korea in 1992, 1994 and 2001, respectively. He has joined the Department of Information Security Engineering, Soonchunhyang University as a professor since 2003 and he is currently running the Lab. of Information Systems Security Assurance. His research interests include security protocols and access control mechanism, secure hardware design, vulnerability assessment, offensive security analysis and security issues on cyber physical systems and embedded realtime systems.