International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.389-396
http://dx.doi.org/10.14257/ijsia.2014.8.6.33

An Access Authentication Scheme Based on 2-HIBS in Proxy Mobile IPv6 Network

Tianhan Gao

Faculty of Software College, Northeastern University,
110819 Shenyang, China
gaoth@mail.neu.edu.cn

Abstract

Proxy Mobile IPv6 is a network-based mobility management protocol. The access authentication security plays the primary role in maintaining network security of proxy mobile IPv6. In this paper, we constructed an authentication framework, which is suitable for proxy mobile IPv6 and has eliminated the interaction between the access network and the home network. We implemented a mutual authentication between users and the access network by using hierarchical identity-based signature (HIBS) schemes and combining the identity-based signature and the real network environment based on proxy mobile IPv6. Also, we have enhanced the function of LMA to make it able to optimize the authentication function of proxy mobile IPv6 protocol by reusing historical authentication information. By results from security analysis, this scheme is secure.

Keywords: *Proxy mobile IPv6, Hierarchical identity-based signature, Access authentication*

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [1] protocol supports the mobility of IPv6 nodes by extending the signal between mobile node (MN) and home agent (HA) based on mobile IPv6 [2] protocol. The mobile agents in PMIPv6 network handle the signal interaction between MN and HA, and participates in the mobility management on behalf of MN. Since it is not necessary for PMIPv6 to do extra configuration for MN, PMIPv6 thus becomes an important mobility supporting protocol in next generation networks. The open nature and lack of security considerations brings potential risk for PMIpv6 during its deployment. Mutual access authentication between MN and proxy mobile entities is mandatory when MN gets access to the foreign network. The mutual access authentication is a fundamental requirement for the security of PMIPv6. In addition, since handover and authentication often occur simultaneously, authentication operations should be synchronized with handover, to ensure the real-time application and handover efficiency.

In the literature research of PMIPv6 access authentication, [3] proposed a PMIPv6 authentication scheme based on Diameter protocol. Access authentication is achieved by pre-sharing the key of AAA server, MN, and mobile agent entity, which increases delay between the AAA server and the proxy mobile entity. [4] solves the key management security issue in the wireless environment by adopting certificate-less sign cryption mechanism in the authentication process of PMIPv6, but this method incurs heavy load on the AAA server due to the interaction between key negotiation process and the AAA server [5] gives a better way to optimize the authentication efficiency of proxy mobile entity handover, it increases the communication cost due to long distance and communication delay among proxy mobile

ISSN: 1738-9976 IJSIA

entities which reduces the efficiency of the switch authentication moreover it requires frequent replacement of the key of related entities. To sum up, the current PMIPv6 access authentication schemes have large system cost, low authentication efficiency and poor handover authentication performance.

Proxy Mobile IPv6 is a network-based mobility management protocol. The access authentication security plays the primary role in maintaining network security of proxy mobile IPv6. In this paper, we constructed an authentication framework, which is suitable for proxy mobile IPv6 and has eliminated the interaction between the access network and the home network. We implemented a mutual authentication between users and the access network by using HIBS schemes and combining the identity-based signature and the real network environment based on proxy mobile IPv6. Also, we have enhanced the function of LMA to make it able to optimize the authentication function of proxy mobile IPv6 protocol by reusing historical authentication information. By results from security analysis, this scheme is secure.

Section 1 of this paper briefly describes the PMIPv6 protocol and identity-based signature technology. Section 2 presents a new authentication protocol, which utilizes HIBS technology. Section 3 shows the performance analysis. Section 4 gives conclusions.

2. Preliminaries

2.1. Proxy MIPv6

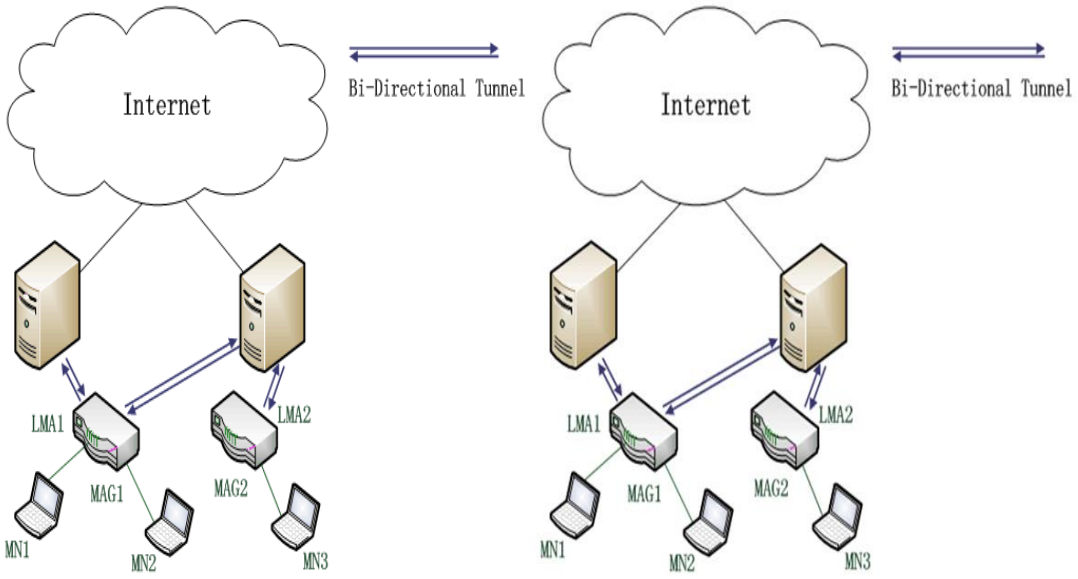

Figure 1. Network Architecture of PMIPv6

As shown by Figure 1, two new functional entities are introduced in the PMIPv6: Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). LMA is equivalent to the home agent in mobile IPv6. Since LMA extends the functions of the home agent, it becomes the topological anchor node of the MN's home network prefix and manages the state of the MN's binding. MAG is implemented on the access router. MAG participates in mobility management on behalf of MN, so that MN can acquire mobility support without any configuration from mobility management protocol.

When MN accessing the PMIPv6 domain, MAG gets MN configuration file first. This configuration file contains the user identity, the LMA address that provides services. Then MAG sends the Proxy Binding Update (PBU) message to the designated LMA on the behalf on MN. Once LMA receives PBU, it feedbacks the Proxy Binding Acknowledge (PBA) message containing the MN's Home Network Prefix (HNP) meanwhile generates a binding cache (BCE) for storing the registration information of accessing MN. After MAG receives PBA, it establishes a bi-directional tunnel between itself and LMA, through which MAG sends announcement messages to MN to inform the prefix of MN home network. MN is able to configure a global IPv6 address based on that prefix. Finally, MN establishes the communication with its correspondent node (CN) by the bi-directional tunnel between the MAG and the LMA.

2.2. Bilinear Pairings

Let G_1 and G_2 be an addition cyclic group and a multiplicative cyclic group with an order of prime q respectively. We call ê a bilinear pairing, if the mapping ê: $G_1 \times G_1 \rightarrow G_2$ satisfies the following properties [6]:

- Bilinearity: For any P, $Q \in G_1$ and a, $b \in Z_q^*$, we have $\hat{e}(aP,bQ)= \hat{e}(P,Q)^{ab}$.
- Non-degeneracy: There exists P, $Q \in G_1$, such that $\hat{e}(P,Q) \neq I_{G2}$, where I_{G2} is the generator of G_2.
- Computability: For any P, $Q \in G_1$, there exists an algorithm that calculates ê(P,Q) .

In modern cryptography, by using bilinear paring, we can construct many security mechanisms which cannot be implemented by other mathematical methods, such as the Tate Pairing and the Weil Pairing over elliptic.

3. Access Authentication Scheme Based on 2-HIBS

3.1. 2-HIBS Scheme

In order to adapt to the network structure of PMIPv6, in this paper, we construct a new 2-HIBS scheme by incorporating the HIBS mechanism [7]. Our 2-HIBS scheme consists of five algorithms: Root-PKG Setup, Level-1-PKG Extract, Level-2-PKG Extract, Sign and Verify .Two levels of users are involved. 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 detail of 2-HIBS scheme is described as below:

- Root-PKG Setup

Root-PKG generates cyclic group G and G_T with the prime order q based on the security parameter k, and bi-linear pairings ê: $G \times G \rightarrow G_T$. Randomly chooses $\alpha \in Z_q^*$, generator $g \in G$, calculates $g_1=g^{\alpha}$. Chooses $g_2, g_3 \in G$, vector $U=(u_1, u_2)$, where $u_1, u_2 \in G$ together with hash function $H_1:\{0, 1\}^* \rightarrow Z_q^*$.Publishes the system parameter $param=(G, G_T, \hat{e}, g, g_1, g_2, g_3, U, H_1)$, message space $M=\{0,1\}^*$, signature space $\sigma=G^2$, master key $msk=g_2^{\alpha}$.

- Level-1-PKG Extract

To generate private key d_{ID1} of level-1 PKG user ID_1, Root-PKG randomly chooses $r_1 \in Z_q^*$, calculates private key of level-1 PKG: $d_{ID1}= (g_2^{\alpha}(u_1^{H1(I1)}g_3)^{r1}, g^{r1}, u_2^{r1})$.

- Level-2-PKG Extract

To generate private key d_{ID2} of level-2 PKG user. Let $d_{ID1}=(a_0, a_1, b_2)$, level-1 PKG randomly chooses $r_2 \in Z_q^*$, calculates private key of level-2 PKG: $d_{ID2}=(a_0 b_2^{I2}(u_1^{H1(I1)} u_2^{H1(I2)} g_3)^{r2}, a_1 g^{r2})$.

- Sign

In order to sign the message M, the signer (ID_i) first calculates the signer $m=H_1(ID_i, M)$, i=1or 2, randomly chooses $t \in Z_q^*$.

If the signer is level-1 PKG. Then calculates: $C_1=g^t$, $C_2=a_1=g^{r1}$, $C_3=a_0 \cdot (g^m)^t = msk(u_1^{H1(I1)} g_3)^{r1}(g^m)^t$.

Finally, outputs signature $\sigma=(C_1, C_2, C_3)$.

If the signer is level-2 user. Then calculates: $C_1'=g^t$, $C_2' = a_1 g^{r2}$, $C_3'= a_0 b_2^{I2}(u_1^{H1(I1)} u_2^{H1(I2)} g_3)^{r2} \cdot (g^m)^t$.

Finally, outputs signature $\sigma'=(C_1', C_2', C_3')$.

- Verify

Once the verifier receives the signature of the message M in terms of identity ID_i, the verification is as below.

Level-1 PKG signature verification

Checks the equation: $\hat{e}(C_3, g)=?\hat{e}(g_1, g_2)\hat{e}(C_2,(u_1^{H1(I1)} g_3))\hat{e}(C_1, g)^m$, if the equation holds, then outputs True, otherwise, outputs False.

Level-2 user signature verification

Checks the equation: $\hat{e}(C_3', g)=?\hat{e}(g_1, g_2)\hat{e}(C_2', (u_1^{H1(I1)} u_2^{H1(I2)} g_3))\hat{e}(C_1', g)^m$, if the equation holds, then output True, otherwise, output False.

3.2. Network Architecture

As shown in Figure 2, 3-level network architecture is designed for PMIPv6. The first level consists of Trust Third Party (TTP) acting as the root PKG. TTP is responsible for generating the system parameters and the private key for level-1 PKG. According to MN affiliation, PMIPv6 domain is divided into the Home Domain and Foreign Domain. HLMA is the authentication server in the home domain, while FLMA is the authentication server in the foreign domain. The second level consists of FLMA and HLMA, *i.e.*, level-1 PKG. The third level is composed of MAG and MN. When MN roaming and accessing a foreign domain. Access authentication is invoked. In this paper, our 2-HIBS scheme achieves localized mutual authentication for MN, which greatly improves the efficiency of access authentication.

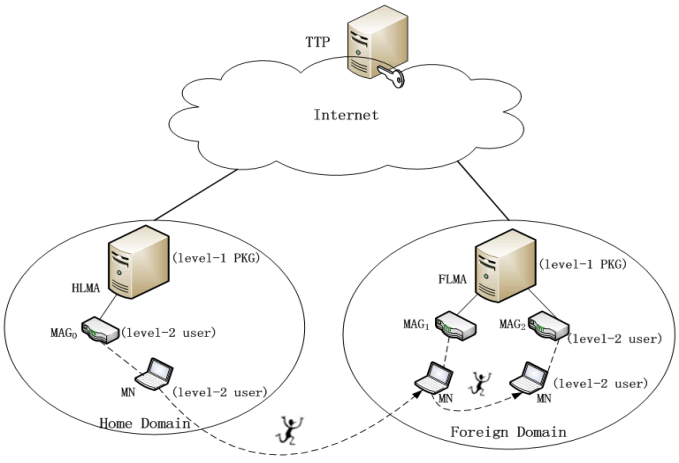

Figure 2. Hierarchical Network Architecture for PMIPv6

To simplify the description of the follow-up scheme, related operations and instructions are presented by Table 1.

Table 1. Identification and Description

Identification	Description
ID_A	The identity of entity A
I_A	Network access identifier of entity A
MN_{Info}	Configuration information of MN
$Sign_{A\_SK}(M)$	Signer A uses 2-HIBS algorithm to generate signature under private key SK on message M
$Verify_{A\_IDB}(\sigma)$	Verifier A uses 2-HIBS algorithm for verifying signature σ by ID_B
K_{A_B}	The shared key between entity A and entity B
A→B:{M}	Entity A sends message M to entity B through secure channel
A→B:[M]	Entity A sends message M to entity 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 parameters
TS	The current timestamp
||	Concatenate two messages

3.3. System Initialization

We make assumptions first for the various functional entities in the network architecture as follows:

- All entities support 2-HIBS mechanism in the network architecture;
- A secure channel has been established in advance between MAG and FLMA (HLMA) ;
- The format of configuration information of MN (MN_{Info}) is shown as Table 2;

Table 2. Configuration Information of MN

HNP_{MN}	I_{HLMA}	I_{MN}

- To resist replay attack, the entire signature must include the current timestamp.

The system is initialized with the help of 2-HIBS mechanism:

- Root-PKG generates system parameters param = (G, G_T, $\hat{e}$, g, g_1, g_2, g_3, U, H_1), and distribute private keys according to identity information of level-1 PKG ;
- Level-1 PKG assigns private keys based on identity information of level-2 user.

3.4. Mutual Authentication Protocol

While MN leaving home domain and accessing to MAG_1 of foreign domain, the mutual authentication is triggered. The specific steps are shown in Figure 3.

- MN→MAG_1: [g^a, MN_{Info}, TS_1, σ_1]

MN randomly chooses $a \in Z_q^*$, then generates the key agreement parameters g^a; utilizes 2-HIBS scheme to obtain the private key d_{IDMN} to calculation the signature σ_1= $Sign_{MN\_dIDMN}(g^a||MN_{Info}||TS_1)$; g^a, MN_{Info}, TS_1 and σ_1 are assembled into an authentication request message REQ and is sent to MAG_1.

- MAG_1→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}) will be extracted from MN_{Info}. According to the system parameter and ID_{MN}, MAG_1 verifies the signature: $Verify_{MAG1\_IDMN}(\sigma_1)$, if verification is done successfully, then MN is regarded as a legal user, MAG_1 extracts HNP_{MN} from MN_{Info}, then will sends HNP_{MN} through PBU to FLMA.

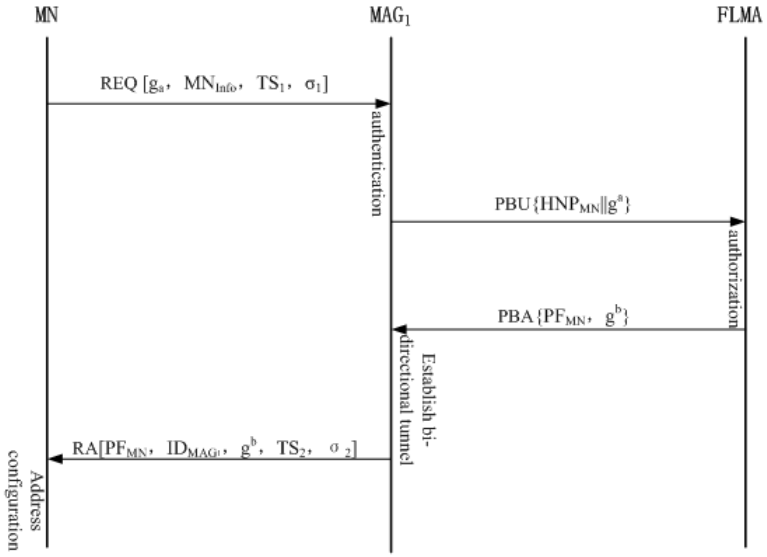

Figure 3. Flow Chart of Mutual Authentication Protocol

- FLMA→MAG_1: {PF_{MN}, g^b}

After receiving PBU, FLMA extracts HNP_{MN} and checks whether there exists this HNP_{MN} in the BCE, if HNP_{MN} already exists in BCE and the corresponding MN is different from the request one, then MAG_1 sends PBA message to reject its access. Otherwise, FLMA randomly chooses $b \in Z_q^*$, calculates key negotiation parameter g^b and 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 PBA message back to MAG_1.

- MAG_1→MN: [PF_{MN}, ID_{MAG1}, g^b, TS_2, σ_2]

After receiving PBA, MAG_1 extracts PF_{MN} and g^b, calculates the shared secret $K_{MN\_FLMA} = g^{ab}$ and keeps it locally. Then MAG_1 generates the signature $\sigma_2=Sign_{MAG1\_}d_{IDMAG1}(g^b||PF_{MN}||ID_{MAG1}||TS_2)$. Finally, PF_{MN}, ID_{MAG1}, g^b, TS_2 and σ_2 are assembled into routing announcement message RA and is sent to the MN.

- Upon receiving RA, MN first checks the freshness of TS_2, if it is fresh, MN extracts information from RA and verities signature σ_2 according to ID_{MAG1} and system parameter: $Verify_{MN\_IDMAG1}(\sigma_2)$. If the verification success, MN makes sure to access a legal MAG and according PF_{MN} configures IPv6 address. At the same time, MN calculates $K_{MN\_FLMA=}g^{ab}$ and save the results in terms of g^b. To complete the mutual authentication.

4. Security Analysis

We analysis the security of our proposed scheme in three aspects [8]: private key confidentiality, signatures unforgeability and key escrow free.

- Private key confidentiality

In 2-HIBS scheme, the private key d_{ID2} of any level-2 user $ID_2 = (I_1, I_2)$ is calculated from its private key d_{ID1} and randomly selected r_2 by $d_{ID2} = (a_0 b_2^{I2} (u_1^{H1(I1)} u_2^{H1(I2)} g_3)^{r2}$, $a_1 g^{r2})$. Although root-PKG generates the private key of PKG_1, it cannot obtain a random number r_2. Through its own private key, so cannot get d_{ID2}. Since the calculation of the DH problem on group G is difficult, for other level-1 PKG except PKG_1, they cannot get the system master key msk and r_1 through its own private key d_{ID1}', and therefore cannot get d_{ID1} and r_2, therefore they are unable to calculate d_{ID2}. Similarly ID_2's peer user ID_2' cannot get d_{ID2}. In summary, the private key of any entity is only known by his father entity rather than other entities.

- Signatures unforgeability

Adversary may forge 2-HIBS signatures in two different ways: The first is replay attack through collecting used signatures. The second is trying to break 2-HIBS itself to achieve the purpose of forgery. First, the proposed mutual authentication protocol introduces is in the message signature. Verifier can determine the validity of the signature by checking freshness of TS to effectively prevent replay attacks. Second, 2-HIBS scheme adopts l-HIBS scheme as building block proved l-HIBS scheme secure under *l*-DHI difficulties assumption so that chosen identity attack and chosen message attack are not effective. Therefore adversary cannot forge signature by breaking 2-HIBS scheme.

- Key escrow free

It has been analyzed in the private key confidentiality that level-2 user's private key is only known by himself and his father (HLMA), any other entity is unable to get the private key. Thus in a wireless mobile environment, when MN accessing a foreign domain, any entity in foreign domain cannot impersonate MN to finish access authentication or monitor encrypted communication of MN. Thus within foreign domain, 2-HIBS scheme is key escrow free. As for the key escrow problem between HLMA and MN, it can be solved by combing 2-HIBS and CBS, which will be a main task of our future work.

4. Conclusions

In this paper, we propose a new access authentication scheme for PMIPv6 based on 2-HIBS mechanism, then analysis the security. By results of analysis this scheme satisfy security requirement of three aspects: private key confidentiality, signatures unforgeability and key escrow.

In the further task, we will do a detailed performance analysis and compare the time with the other scheme.

Acknowledgements

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

References

[1] Z. Hua-chun, Z. Hong-ke and Q. Ya-juan, "An Authentication Protocol for Proxy Mobile IPv6", Chinese Journal of Electronics, vol. 36, no. 10, **(2008),** pp. 1873-1880.
[2] Z. Long-jun, M. O. Tian-qing and Z. Li-yi, "Authentication Scheme based on Certificate less Signcryption in Proxy Mobile IPv6 Network", Application Research of Computers, vol. 29, no. 2, **(2012),** pp. 411-414.
[3] A. Shamir, "Identity-base cryptosystems and signature schemes", Advances in Cryptology-Crypto'84. LNCS, vol. 196, **(1984),** pp. 47-53.
[4] S. Hua, W. Ai-min and Z. Xue-feng, "Efficient Hierarchical Identity-based Signature Scheme", Computer Science, vol. 39, no. 8, **(2012),** pp. 67-69.
[5] J. Song and S. Han, "One-Time Key Authentication Protocol for PMIPv6", Third 2008 International Conferences on Convergence and Hybrid Information Technology, **(2008),** pp. 1150-1153.
[6] G. Iapichino and C. Bonnet, "Experimental Evaluation of Proxy Mobile IPv6: An Implementation Perspective", Wireless Communications and Networking Conference (WCNC), **(2010),** pp. 1-5, 18-21.
[7] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy Mobile IPv6", Internet Draft, RFC 5213, **(2008)**.
[8] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", Internet Draft, RFC 3775, **(2004)**.

Author

Tianhan Gao, he 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.

