Secure Mobility Management for MIPv6 with Identity-Based Cryptography

Nan Guo, Fangting Peng, Tianhan Gao

Secure mobility management for MIPv6 with identity-based cryptography

Nan Guo, Fangting Peng, and Tianhan Gao

Northeastern University,
NO.3-11,Wenhua Road, Heping District, Shenyang, P.R.China
{guonan,pengft,gaoth}@mail.neu.edu.cn

Abstract. Mobile IPv6 is an improvement of the original IPv6 protocol, and provides mobility support for IPv6 nodes. However, the security of mobility management is one of the most important issues for MIPv6. Traditional MIPv6 uses IPSec to protect the mobility management, while the dependence on the mechanism of the pre-shared key or certificate limits its applicability. This paper proposes an improved scheme for the original method based on IBC, to protect the mobility management signaling for MIPv6.
Keywords: Mobile IPv6, IPSec, IBC, Mobility Management

1 Introduction

The development of IPv6[11] has leaded to the rapid popularization of Mobile IPv6 (MIPv6). MIPv6 is a protocol to provide mobile support for IPv6, and it was standardized by IETF in 2004. The security problem has been exposed at the devising of MIPv6. The primary threat comes from fake binding update messages, replay attack and route attack which mainly manifest in the mobility management procedure[1, 10]. The main reason derives from no efficient authentication approach between the communication entities. In this paper, we propose a novel encryption and authentication scheme to guarantee the security of MIPv6 mobility management.

In the literatures, [2] shows that MIPv6 adopts IPSecurity(IPSec) protocol and Internet Key Exchange(IKE) protocol to protect mobile management signaling between mobile node and home agent. However, the method is not efficient as required. [3] shows that pre-shared key or certificate adopted by the first stage of IKE is not suitable under the mobile environment. It is not realistic to build the infrastructure to satisfy IKE. Besides, using IPSec with IKE would add extra burden for mobile nodes. To solve the problem, [4] utilizes multilevel IPSec in MIPv6 to protect mobility management procedure; [5] suggests that a secure association between mobile node and home agent should be built in advance. However, this will bring more cost of security management. Thus, the efficiency of the above schemes still need to be improved.

In traditional public key cryptography, the public key is a string of random characters without any practical information. The Certificate Authority(CA) in

PKI infrastructure takes the responsibility of publishing certificates. As a result, the expense of release, storage, verification and revocation is enormous. To solve the problem, the Identity-Based Cryptography(IBC) uses IP address, Email address or any other string that represents the users identity as public keys. Shamir first proposed Identity-Based Encryption(IBE) in 1984. Then in 2001, Boneh and Franklin proposed BF-IBE scheme [7]. Later, Identity-Based Signature(IBS) was proposed. In IBS, every communication entity owns a pair of public key and private key. Public key is the identity of the entity and private key is generated and allocated by the trusted third party, Private Key Generator(PKG). Certificate is not necessary during communication, which relieves the computation and storage cost in encryption and authentication. IBC is thus suitable for the security of mobile network [9].

In this paper, we discuss the typical security protocols in MIPv6 and propose a novel identity-based security scheme for MIPv6 mobility management. The scheme can protect the mobility management signaling among mobile node, home agent and correspondent node in an efficient way.

2 Preliminaries

2.1 MIPv6 Protocol

According to the standardization document RFC3775, MIPv6 protocol is the mobility extension solution for IPv6. It is composed of four entities, Mobile Node(MN), Home Agent(HA), Correspondent Node(CN) and Access Router(AR). MN is allocated a permanent address, i.e. Home of Address(HoA) at the home network, and will get a temporary address, i.e. Care-of Address(CoA), from AR and register it to HA when moving to a foreign network[6].

2.2 IPSec Protocol

IPSec protocol provides confidentiality, data integrity, data authentication and anti-replay services at IP layer. It is an open framework applied widely in a variety of operating environments including mobile network. IPSec supports IKE protocol, which means that key negotiation can be implemented. Besides, encryption and authentication in IPSec guarantee the security of IP data packet. As shown in Fig.1, IPSec owns a set of approaches for data security such as Authentication Header(AH), Encapsulating Security Payload(ESP), as well as the related cryptography algorithms.

2.3 Identity-Based Cryptography

An IBE scheme is generally defined as follows.

IBE.Setup: given a security parameter k as input, output PKG's public key mpk and private key msk.

IBE.Extract: given msk and user's id as input, output user's private key usk.

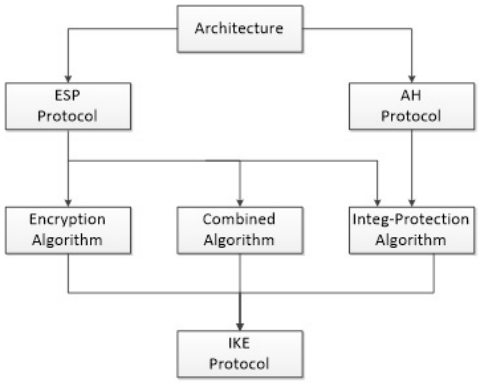

Fig. 1. The architecture of IPSec

IBE.Encrypt: given msk, id, and message m as input, output the encryption δ on m.

IBE.Decrypt: given usk and δ as input, output 1 if δ is valid or 0 otherwise.

In an IBS scheme, IBS.Setup and IBS.Extract are identical to IBE.Setup and IBE.Extract respectively. The other algorithms are defined as follows.

IBS.Sign: given usk and message m as input, output the signature σ on m.

IBS.Verify: given mpk, id, m and σ as input, output 1 if σ is valid or 0 otherwise.

3 Our Solution

In this chapter, we propose a secure mobility MIPv6 management scheme based on BF-IBE scheme[7] and BF-IBS Scheme[8]. The network architecture and intra-domain security management solution are given in detail.

3.1 Network Architecture

In our scheme, the security of the mobility management signaling among MN, CN and HA is guaranteed by IBC. NAI acts as the identifier for every entity. The format of NAI is as user@domain, which would be kept fixed even when the location of MN has changed.

As shown in Fig.2, the proposed network architecture can be divided into several domains according to the trajectories of MN's roaming. The architecture is composed of CA, PKG, MN, HA and CN. CA is in charge of issuing certificates for PKGs and providing identity authentication service for the communication among them. PKG takes the responsibility of security management in each domain. It maintains public parameters and generates private keys for entities in its domain.

In order to simplify the descriptions of the relevant protocol, Table 1. shows the notations and explanations used in our scheme.

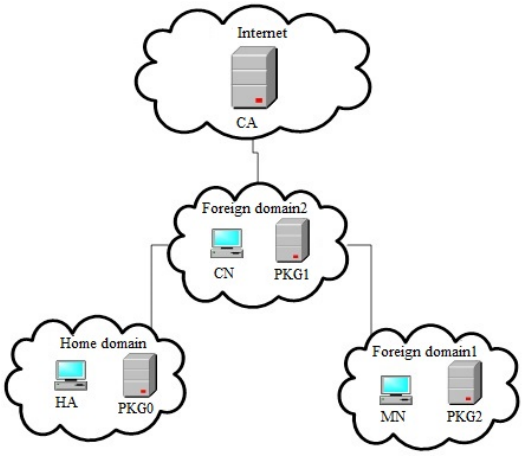

Fig. 2. Network Architecture

Table 1. Notations and Explanations

Notations	Explanations
$Msg_1 \| \| Msg_2$	Msg_1 connects to Msg_2
$S_{x,y}$	Entity X's private key generated by PKG_Y
$SK_{x,y}$	Symmetric key between entity X and entity Y
ID_x	Entity X's ID
$Enc(Msg, ID_x)$	Msg is encrypted by Entity X's public key ID_x by BF-IBE
$Sig(Msg, S_{x,y})$	Msg is signed by Entity X's private key $S_{x,y}$ by BF-IBS
$Code$	Global unique message type for message handling
$Source$	The source of message
$Destination$	The final destination of message
$Payload$	The load of message
$Time$	The message's generation time and allowable maximum delay

3.2 Secure Mobility Management Scheme

There are two states in our scheme in terms of MN's location: When MN is at home domain, the scheme is on the initial state, and when MN moves to foreign domain, the scheme is on the mobile state.

As shown in Fig.3. MN and HA execute Diffie-Hellman key exchange to negotiate the shared symmetric key, which is the same as IKE key agreement that can provide encryption key for IPSec.

At the initial state, key negotiation is relatively simple and there are only two messages because MN and HA are both at the home domain.

(1)MN → HA: Key Exchange Request

Message format in detail:

$Code||MN||HA||Enc(Sig(g^m, S_{MN,0}), ID_{HA})||Time$

Key Exchange Request is generated by MN and sent to HA. *Code* is the message type. MN is *Source* and HA is *Destination*. g^m is the parameter of Diffie-Hellman key exchange in the *Payload*, where g is public parameter in the home domain and m is the secret value chosen by MN. After sending the message, MN expects to get reply within *Time*.

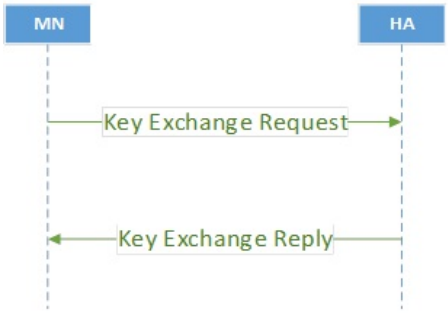

Fig. 3. Intra-domain Secure Mobile Management Scheme

(2)HA → MN: Key Exchange Reply

Message format in detail:

$Code||MN||HA||Enc(Sig(g^h, S_{HA,0}), ID_{MN})||Time$

Key Exchange Reply is generated by HA and acts as the reply for MN's Request. *Code* is the message type. HA is *Source* and MN is *Destination*. g^h is the parameter of Diffie-Hellman key exchange in the *Payload*, where h is the secret value chosen by HA.

After the exchange of the above two messages, MN and HA have achieved Diffie-Hellman key exchange through IBC. They compute the same symmetric

key respectively, $SK_{MN,HA} = SK_{HA,MN} = (g^m)^h = (g^h)^m$. The symmetric key can work for the following IPSec stage.

4 Conclusion and Future Work

In this paper, we first analyze a series of threats on MIPv6, then propose a secure mobility management scheme based on IBC to protect the signaling among MN, HA and CN. The details of the scheme are explained.

For the next step, we plan to discuss inter-domain secure mobile management scheme and add a new method Return Routability to guarantee the security of MIPv6. Further security analysis is also required to demonstrate the robustness of our scheme.

Acknowledgments This work was supported by National Natural Science Foundation of China under [Grant Number 61402095] and [Grant Number 61300196], China Fundamental Research Funds for the Central Universities under [Grant Number N120404010] and [Grant Number N130817002].

References

1. Tian Y, Zhang Y, Zhang H, et al. Identity-based hierarchical access authentication in mobile IPv6 networks[C]. Communications, 2006. ICC'06. IEEE International Conference on. IEEE, 2006, 5: 1953-1958.
2. Elgoarany K, Eltoweissy M. Security in Mobile IPv6: A survey[J]. Information Security Tech Report, 2007,12(1):32C43.
3. Aura T, Roe M. Designing the Mobile IPv6 Security Protocol[J]. Annales Des Tlcommunications, 2006, 61(3-4):332-356.
4. Choi H, Song H, Cao G, et al. Mobile multi-layered IPsec[J]. Wireless Networks, 2005, 3(6):1929 - 1939.
5. You Yebin, Wang Qingxian, Luo Junyong, Huangfu Luzi. Optimized Method of Constructing IPSec SA between MN and HA in MobileIPv6[J]. Journal of Information Engineering University,2008, (2):222-224.
6. Conta A, Deering S. Generic Packet Tunneling in IPv6 Specification, RFC 2473[J]. OverDRiVE 102 Description and Validation of Mobile Router and Dynamic IVAN Management,3/31/04 OverDRiVE WP3 D17, 1998.
7. Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing[J]. Siam Journal on Computing, 2001, 32(3):213-229.
8. Barreto P S L M, Kim H Y, Lynn B, et al. Efficient algorithms for pairing-based cryptosystems[M]. Advances in cryptologyCRYPTO 2002. Springer Berlin Heidelberg2002: 354-369.
9. Kyoungjae Sun, Younghan Kim. Flow Mobility Management in PMIPv6-based DMM (Distributed Mobility Management) Networks[J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA),Vol. 5, No. 4, pp. 120-127, December 2014.
10. Karl Andersson, Muslim Elkotob. Rethinking IP Mobility Management[J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol. 3, No. 3, pp. 41-49, September 2012.

11. Antonio J. Jara, Latif Ladid, and Antonio Skarmeta. The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities[J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol. 4, No. 3, pp. 97-118, September 2013.