A security registration based on IPSec for mobile IPv6 fast handoff

Lei Zhao[1] Xiaoping Li [1]
1. The School of meno-electronic engineering, Xidian University,
Xi'an, China
bohe314@sina.com

Qingkuan Dong [2] Lei Shi [1]
2. State Key Lab. Of Integrated Services Networks,
Xidian University,
Xi'an, China
xpli@xidian.edu.cn

***Abstract*—At present, many studies focus on the efficiency of handoff among different networks, while research on how to maintain the safety during registration process of handoff is not enough. Unfortunately, mobile node is vulnerable to various security threats and attacks when handover for being lack of protection. A security scheme based on the IPSec protocol which was combined with fast handoff signaling was given in this paper. The mutual handover authentication between mobile nodes and access routers was obtained through improved handoff signaling, and IPSec security association was used to protect the handoff process without lowering its efficiency.**

Keywords- mobile register；IPSec；Mobile IPv6；Handoff Authentication

I. Introduction

As the growth of ubiquitous network technologies and services, users can access the Internet from anywhere at any time by using wireless devices. As to support mobility of various applications and services, IETF proposed mobile IPv6 protocols [1] in 2004. However, wireless environment is characterized by openness, which makes it vulnerable to the threat of attacks, and also does MIPv6. MIPv6 signaling are easy subject to attacks, such as man-in-the-middle attack, replay attack, flooding attack, code attacks, DOS attack and so on. Redirection attacks, middle attacks, denial of service attacks will be occur especially during the handover process of mobile nodes for lacking of strong protection measures to the signaling interactions. Additionally, Mobile IPv6 may also be subjected to other security attacks, such as the lack of effective authentication mechanism, which may be the root of many attacks. Mobile IPv6 authentication protocol make mobile nodes get certified in their respective certification entities by using IPSec Security Association(SA) between mobile nodes and home agent or AAAH[2] server when mobile nodes access to a new network. However, the authentication protocol just applied to MN-HA, mutual certification between MN-CN still cannot be made effectively, thus the risk of eavesdropping or intermediary attacking increase if malicious node access to network fake normal node.

II. Related Works

Several mechanisms [3-7] have been proposed to solve security problems in handoff process. The related works are discussed here and their drawbacks are pointed out as sequel.

In [3], Hu Wang and Anand R. Prasad proposed a method of fast authentication for inter administrative domain handoff between two foreign mobile or wireless communication network domains. In this method, Serving Network (SN) and Target Networks (TN) must be a relationship of mutual trust. When MN handoff from SN to TN, MN send a handoff decision to SN, then SN calculates a shared key for MN and TN， and sends it to MN and TN respectively. Then MN sends a fast authentication request asking to TN after receiving the key, and MN can be accessed to TN when authentication finish. Such an approach, however, faces the following challenges: First, if the trusted third-party introduced for distributing the pre-shared key to authentication entities is under attack, there is no security to speak of in authentication process. Secondly, the introduction of a trusted third-party will be an additional signaling overhead. Finally, binding update process is also lack of effective protection after handoff.

In[6], a fast authentication mechanism using identity-based signature (IBS) was proposed. Its primary idea is the effective combination of fast handover and access authentication. New access router (NAR) and NAAA server ask for the signature parameters of MN from AAAh of MN when handover initials. MN accomplish access authentication with only one interaction with AAAv server and complete binding update process with HA simultaneously. Similar researches on the combination of Mobile IP and AAA mechanism solving the authentication issues of MN in handover process are presented in [4-7]. But such approaches need a great deal of signaling interactions with the home network each handoff happens, which lead to a large handover delay and considerable signaling overhead.

Even though these methods can solve the security treats in handoff process to a certain extent, there are still many defects, such as more packets overhead, the security issue of message and signals protection which was rarely take into

978-1-4244-3709-2/10/$25.00 ©2010 IEEE

account in the handover process, and poor performance when mobile node far away from home networks.

III. Proposed Scheme Protocol

The underlying security problem of handoff is the lack of effective authentication of mobile nodes as well as security protection of handover signals. In this paper, we propose a novel registration of fast handoff, which is based on IPSec protection. Its basic mind is using IKEv2 protocol [8] to achieve pre-authentication of mobile nodes in fast handoff process, and the Security Association (SA) generated by IKEv2 also utilized to provide protection for handover signaling. We illustrate the method of registration in handover procedure as Fig.1 shows.

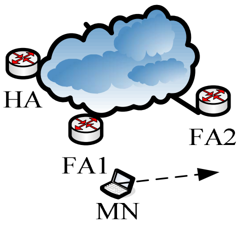

Figure 1. Handover procedure.

The scenario as this: there are two foreign networks, the local fixed node FA1 is a Foreign Agent of MN in foreign network 1, and FA2 is the agent of MN in link 2. When MN move to foreign network 2, two prerequisites should be satisfied in order to achieve security handover, one is that the tunnel between FA1 and FA2 should be existed, and the other is that IPSec protection is used between MN and FA1 in the domain of FA1. Furthermore, all the signaling must be transmitted via encryption. Fig.2 presents detailed steps and specific implementation processes are described below:

(1) MN->FA1
$M1 = RtSol\Pr,\{SAi, KEi, CERT_{MN}, Ni\}Sig_{MN}$

MN sent Router Solicitation for Proxy Advertisement (RtSolPr) message to FA1 that carrying mobile node's certificate, random number Ni, as well as security association request message through tunnel that has been established when it predict handoff is to take place. The certification and random number are signed by private key of mobile node.

(2) FA1->FA2 $M2 = HI,\{SAi, KEi, CERT_{MN}, Ni\}Sig_{MN}$

FA1 forward MN's certificate and random number with Handover Initiate(HI) message to FA2 after receiving the message, FA2 extract public key in MN certificate to verify the signature. If the message authentication show that it indeed from MN and real, FA2 will create a binding cache for MN, and FA2 itself generate a random number Nr, which is used to figure out g^{ir} together with Ni, then a secret key is to calculate by an algorithm selected, i.e. $SK = prf(Ni \mid Nr, g^{ir})$.

(3) FA2->FA1
$M3 = HACK,\{SAr, KEr, CERT_{FA2}, Nr\}Sig_{FA2}$

FA2 signature its own certificate, random number Nr and then sent them to FA1 along with Handover Acknowledge(HACK) security association proposal, and Diffie-Hellman parameters Ker.

(4) FA1->MN
$M4 = \Pr RtAdv,\{SAr, KEr, CERT_{FA2}, Nr\}Sig_{FA2}$

FA1 extract the information of FA2 and forwarding it with Proxy Router Advertisement(PrRtAdv) message to MN, from which MN can get a new Care-of Address (NCoA). Then MN extract public key in FA2 certificate to verify the signature in message, if it is prove to be validate , MN also use random numbers to calculate a SK. So far, both sides complete the authentication process, and negotiate out a KEY SEED.

(5) Fast binding update message was sent to FA1 from MN, which notify FA1 binding the Home Address and new care-of address for MN. FA1 create a cache for MN which memory the packet belong to MN before sending fast back acknowledgement. Then MN disconnects with FA1 and move into a new network 2.

(6) Packets belongs to MN are forwarded from FA1 to FA2.

(7) MN registers to its home agent (HA) using binding update message, which is protected by IPSec [10].

(8) HA return binding update acknowledge message.

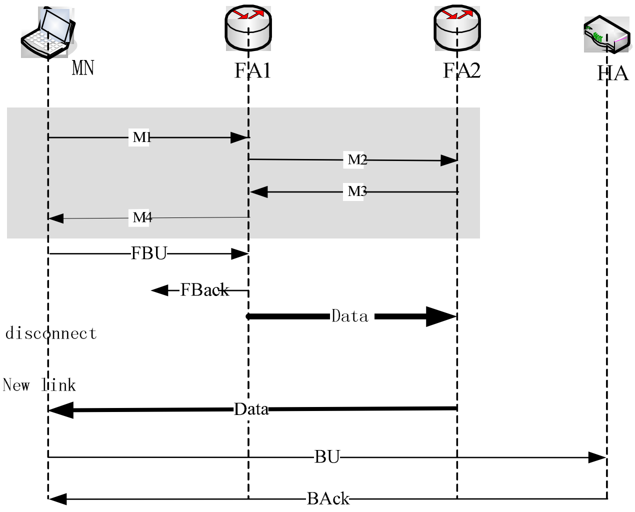

Figure 2. Handoff registration processes.

IV. Performance Analysis

The performance of the proposed scheme will be evaluated in this section. In order to analyze the handover performance, we will check two key aspects: authentication delay and security.

A. Handoff Delay

We compared our proposed scheme with the IBS-FAMIPv6 [7], which using math model describe as [7]. The parameters are show in Table 1.

TABLE I. PARAMETERS FOR PERFORMANCE EVALUATION

Parameter	Notes
t_p	Transferring and node processing time
t_{RSA}	RSA signature mechanism a "Signature + verification" time-consuming
a	Wireless Transmission Delay
b	Transmission delay between two nodes within the same domain
d	Adjacent inter-domain transmission delay
c	Adjacent inter-domain transmission delay

Costs of various methods are listed below:

$$T_{FAMIPv6} = 4a + 3b + d + 14t_p + t_{RSA} + 4c$$
$$T_{IBS-FAMIP6} = 2a + 2b + d + 8t_p + 2t_s + \max(t_v, 2c + t_p)$$
$$T_{IPSec-FMIPv6} = 2a + 2d + 4t_p + 2t_{RSA} + 2c$$

We assume that c obey the uniform distribution of $[b, H]$, and their mathematical expectation are [7]:

$$E[T_{FAMIPv6}] = 4a + 5b + d + 14t_p + t_{RSA} + 2H$$
$$E[T_{IBS}] = 2a + 2b + d + 8t_p + 2t_s + E[\delta_1] \quad ,$$
$$E[\delta_1] = \begin{cases} t_v, & t_v > 2H + t_p \\ \dfrac{(t_v - t_p)^2 + 4H + 4Ht_p - 4t_v b}{4(H-b)}, & t_v < 2H + t_p \end{cases}$$
$$E[T_{IPSec}] = 2a + 2d + 4t_p + 2t_{RSA} + b + H$$

In order to facilitate subsequent analysis，we set specific parameter values as follows：$a = 4ms$, $b = d = 2ms$, $t_p = 0.5ms$, $t_{RSA} = t_s$ ， $t_v = 5t_s$. Then Mathematical expectations are:

$$E[T_{FAMIPv6}] = 35 + t_s + 2H$$
$$E[T_{IBS}] = \begin{cases} 18 + 7t_s, H \le \dfrac{5t_s - 0.5}{2} \\ 20.5 + 2t_s + H + \dfrac{25t_s^2 - 45t_s + 20.25}{4(H-2)}, H > \dfrac{5t_s - 0.5}{2} \end{cases}$$
$$E[T_{IPSec}] = 14 + 2t_s + \text{H+2}$$

Mathematical expectations of the total handoff delay distribution are shown in Fig.3 and Fig.4 for t_s equals to 8ms and H equals to 20ms respectively. In figure 3, it can be see that FAMIPv6 and IBS-FAMIPv6 is more time-consuming with the increase of H than that we proposed when the total time of signature and verification algorithm is determined. Likewise, the total handoff delay with the growth of t_s in our scheme is less than [7] when the transmission delay is deterministic. Moreover, this advantage will still exist as the processing power of mobile nodes increase.

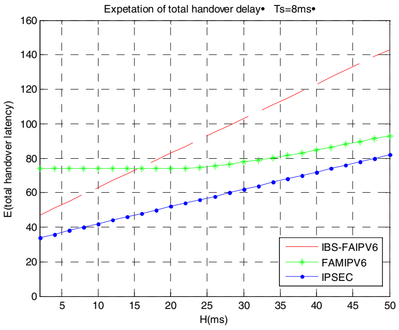

Figure 3. Mathematical expectation of total handoff delay distribution (Ts=8ms)

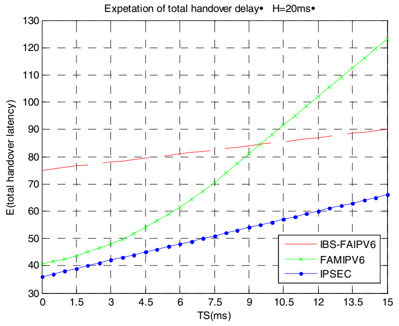

Figure 4. Mathematical expectation of total handoff delay distribution (H=20ms)

From the analysis of Fig.3 and Fig.4, we draw a conclusion that the scheme we proposed can reduce the signaling interaction with home network for the mobile node, what's more, pre-authentication low the handoff delay considerably.

In addition, in order to test the feasibility of our scheme, we use NS-2 to simulation the proposed scheme. The whole simulation process involves two handoff processes as depicted in Fig. 1: first from home network to the foreign network 1; and then to foreign network 2. For the integrity of analysis, Fast handover for Mobile IPv6 (FMIPv6) is also simulated for comparison. Fig. 5, Fig. 6 shows the handover delay simulated via NS2.

In Fig. 5 and Fig. 6, there is a slight increase in packet delay after adding IPSec. IPSec processing delay is zero since IPSec does not contain encryption and decryption operations during simulation, and thus the packet delay increases just a little. The jitter conditions have also been improved.

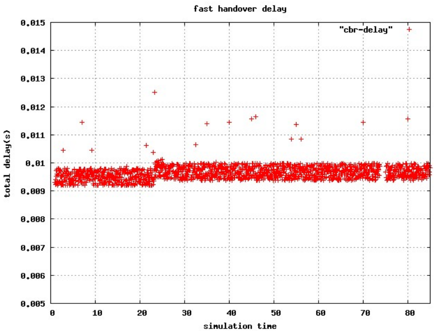

Figure 5. Simulation of FMIPv6 delay

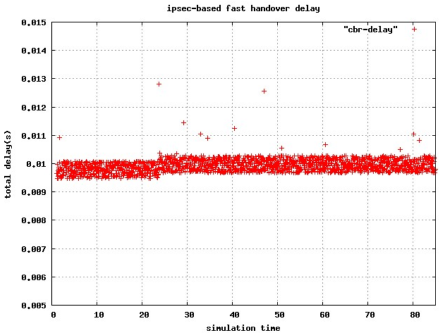

Figure 6. Simulation of IPSec-FMIPv6 delay

B. *Security and scalability analysis*

This scheme can achieve good security by using IPSec protection. As respect to attacks that handover process usually suffered includes man-in-the-middle attack, replay attack, flooding attack, code attacks, and denial of service attack. In Fig.2, it can be seen from step 1 to step 4 that the realization of authentication messages M1-M4 were encrypted by the SAs between the two entities, which means no one could obtain the content of these message except FA1. At the same time, FA1 is a trustable entity for MN and FA2. We assume that FA1 is under control of attacker and FA1 try to falsify message that from MN to FA2, however, FA1 cannot make man-in-the-middle attack for the reason that the message $M1 = RtSol\Pr, \{SAi, KEi, CERT_{MN}, Ni\} Sig_{MN}$ from MN to FA2 is protected by MN signature which is unforgeable. MN and FA2 are without IPSec protection between when MN just access to FA2, so there is occasions that someone want to use this bug to launch attack. According to message 1-4, MN register to FA2 would use a random number and security association parameters to figure out a shared key SK, while message signature can not be forged guarantee that SK are only known to MN and FA2. Thus an attacker can not get SK and eavesdropping signaling between MN and FA2. The scheme has good ability of anti-intermediary attacks.

Due to the serial number in IPSec protocol is the non-repetitive and the confidentiality and integrity protection of IPSec data, IPSec-FMIPv6 can effectively block these three types of attacks: replay attacks, flooding attacks and code attacks. But the attacker may take advantage of the node's signature and verify process to send a large number of spam operations for DOS attack, which means that policy configuration must choose right algorithm to reduce the likelihood of attack. Support for scalability is mainly reflected in the scheme on inter-handover under the hierarchical mobile IPv6 domain management, and have better switch performance.

V. CONCLUSIONS

This paper propose a novel security register scheme based on IPSec combining with FMIPv6 signaling and adopting pre-authentication mechanism ,which realizing authentication before handover and reducing time delay brought in by authentication after handover greatly. Analysis indicating that IPSec-FMIPv6 scheme has the advantage of low delay and gentle expenses of packet overhead as well as good characteristics in such aspects as security and expansibility support comparing to the authentication scheme of AAA. Certainly, some details need to be done further, for example selection of encrypt algorithms and time consuming that needed in the course have not been in consider, which will be further researched in our follow-up work.

ACKNOWLEDGMENT

This paper is supported by the National Natural Science Foundation of China (No. 60603010) and State Key Lab. of Information Security (No. k03-06).

REFERENCES

[1] C. E. Perkins, D. B. Johnson. Mobility Support in IPv6. RFC 3775, June 2004

[2] C.de Laat,G.Gross, L.Gommans, J.Vollbrecht, D.Spence. Generic AAA Architecture. RFC 2903, August 2000

[3] Hu Wang, Anand R..Prasad. Fast Authentication for Inter-domain Handover. J.N. de Souza et al. (Eds.): ICT 2004, LNCS 3124, 2004.Springer-Verlag Berlin Heidelberg 2004 .pp. 973–982,

[4] C Kim , Y S Kim , E N Huh , *et al* . Performance improvement in mobile IPv6 using AAA and fast handoff [C] . In : Proc of t he ICCSA 2004 , LNCS 3043. Berlin :Springer-Verlag , 2004.p. 738-745

[5] Paal. Engelstad, Thomas. Haslestad, Frederic. Paint. Authenticated Access for IPv6 Supported Mobility. Eighth IEEE International Symposium on Computers and Communication, 2003

[6] Zhang Hanwen , Zhang Yujun , Tian Ye , *et al* . Hierarchical access authentication method in mobile IPv6 networks [J] .Journal of Computer Research and Development , 2007 , 44(1) pp: 51-57 (in Chinese)

[7] Tian Ye , Zhang Yujun , Liu Ying , *et al* . A fast authentication mechanism using identity based signature in mobile IPv6 network [J] . Journal of Software , 2006 , 17 (9)pp :1980-1988

[8] Kaufman, C., Ed.. Internet Key Exchange (IKEv2) Protocol. RFC 4306, December 2005、

[9] R Koodli. Fast handovers for mobile IPv6 [S] . IETF RFC 4068 , 2005

[10] J. Arkko, V. Devarapalli, F. Dupont,Using IPSec to protect mobile IPv6 signaling between mobile nodes and home agent[S]. IETF RFC 3776, 2004