

A Secure Hierarchical Identify Authentication Scheme Combining Trust Mechanism in Mobile IPv6 Networks

Zhang Zhi

1 College of Computer,
Huazhong University of Science & Technology

2 College of Computer,
Wuhan Institute of Technology
Wuhan, Hubei, 430074, China
Amice_zhang@yahoo.com.cn

Guohua Cui

College of Computer,
Huazhong University of Science & Technology
Wuhan, Hubei, 430074, China
Amice_zhang@163.com

Abstract—During the last few years, it has become more and more compeling in mobile applications, mobile IPv6 technology is convenient, but also produces a series of security compromise. Identify authentication is an important part of the network security. In this paper, we proposed a secure identify authentication scheme combining reputation mechanism, which considers inters domain trust relationship between mobile node home domain and the access domain in the pre-handoff procedure and realizes effective mutual authentication between mobile node(MN) and the access domain. A dynamic reputation maintenance mechanism for inter domain relationship is also designed. Based SMC signature, a hierarchical signature and verification scheme is designed in one round mutual authentication. Theoretical analysis and numerical results show that proposed scheme is more effective in reducing total authentication and handoff delay and the signaling overhead than relative schemes. Security analysis shows, basing on the security of SMC-IBS, the proposed scheme is sufficient for private key privacy, signature unforgeability. Moreover, our scheme first provide public key revocation and key escrow problem in mobile IPv6 networks' access authentication.

Index Terms— MIPv6; handover performance; SMC-IBS; Mutual authentication;

I. INTRODUCTION

During the last few years, it is arising an increasing concern to mobile applications, mobile IPv6 technology brings us convenient but also produces a series of security issues. As a direct consequence of these facts, several security technologies have recently emerged in order to provide security services in wireless networks, authentication is used as an initial process to authorize a mobile node (MN) for communication through secret credentials such as authentication, authorization, and accounting (AAA) architecture [1], [2]. Currently, the AAA architecture for the Mobile IPv6 relies on frequently consulting the home network to authenticate the MN when the MN roams to a foreign network, the foreign network has to send back an authentication request to the home network to be verified. This procedure causes long handoff delays and may not be feasible for real-time applications [3], [4].

To minimize the authentication delay is very important for real-time applications in wireless mobile networks. Many solutions have been proposed [2-4]. All of the solutions only append authentication procedure into the handover procedure,

but don't consider reputation relationship in the domains. Authentication failure caused by the adversaries is not detected until the entire authentication procedure is over. Lecture [6] first propose authentication scheme combining trust mechanism with poor performance.

In this paper, we propose a hierarchical identify authentication scheme combining trust mechanism for wireless mobile IPv6 networks is proposed, which considers inter-domain trust relationship between MN's home domain and the access domain in the pre-handoff procedure and realizes effective mutual authentication between mobile user and the access domain in one round trip. A dynamic maintenance mechanism for inter-domain trust relationship is also designed. Based on the combined SMC algorithm, a signature and verification scheme is designed for network entities, which accelerates mutual authentication process. Theoretical analysis and numerical results show that the proposed method is more effective in reducing total authentication and handoff delay and the signaling overhead than relative methods. Also, based on the security of SMC-IBS algorithm; the method is sufficient for privacy and unforgeability in realizing mutual authentication in mobile IPv6 networks. Moreover, our scheme first provides public key revocation and key escrow problem in mobile IPv6 networks' access authentication. The rest of the paper is organized as follows. Section II introduces the related work. Section III defines two heterogeneous network models. In Section IV, we describe the SMC-HAMIPv6 protocol. In Section V, our protocol is simulated and analyzed. We conclude our work in Section VI.

II. PRELIMINARIES

A. Bilinear Map

Bilinear map was proposed by Boneh and Franklin [2], and it was used to build some well known and efficient IBE schemes.

Definition 1. Let G_1 and G_2 be two groups of the large prime order q . The bilinear map is a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ between these two groups, and the map must satisfy the following three properties:

1) Bilinear: We say that a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ is bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in \mathbb{Z}$.

2) Non-degenerate: if P is a generator of G_1 then $\hat{e}(P, P)$ is a generator of G_2 .

3) Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for $\forall P, Q \in G_1$.

B. DLP Assumption

Definition 2. Discrete Logarithm Problem (DLP). The DLP is the problem of finding a given (p, q, g, g^a) with uniformly random choices of $a \in \mathbb{Z}_q^*$ and $g \in \mathbb{Z}_p^*$. The DL assumption states that there is no polynomial time algorithm with a non-negligible advantage in solving the DLP.

C. Identity-Based Mediated Certificateless Cryptography

The concept of Identity-Based Signature (IBS) was first introduced by Shamir, the motivation is to simplify a certificate management and the essential idea of the IBE is that any string such as email or IP address can be used as public key for encryption or signature verification. In [6] Mediated cryptography was introduced by Boneh, Ding and Tsudik [7] as a method to allow immediate revocation of public keys. In PKC 2006, Chow, Boyd and Gonzalez Neito designed the notion of security mediated certificateless (SMC) cryptography. SMC cryptography provides certificateless cryptography with instantaneous revocation.

III. HIERARCHICAL AUTHENTICATION SCHEME COMBINED REPUTATION

A. Signature Algorithm

In this section, we briefly recall some of the properties of bilinear pairings, and recall an SMC signature [8], which is the basis of our proposed scheme. The signature and verification Algorithm include parameter establishment, signature and verification [8].

Setup: Given the security parameter k , the KGC performs the following.

1) The KGC chooses group G_1, G_2 prime order q , P is generator in G_1 , map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ and chooses the hash functions where $H_0: \{0,1\}^* \rightarrow \{0,1\}^l$, $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and $H_2: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

2) Generate two primes p and q such that $q|p-1$.

3) The system parameters are $params = \langle p, q, G_1, G_2, e, Y, H_0, H_1, H_2 \rangle$ and the master key is s .

KeyGen: The user performs the following.

1) Randomly select $x_{ID} \in \mathbb{Z}_q^*$ as the user private key.

2) Corresponding compute $P_{ID} = g^{x_{ID}} \in \mathbb{Z}_q^*$ as the user public key.

Register: Now user ID wants to register a public key P_{ID} :

1) The KGC authenticates and registers (ID, P_{ID}) , randomly pick $w \in \mathbb{Z}_q^*$.

2) The KGC computes $W = g^w$ and $d = w + sH_1(ID || W)$.

3) The KGC sends the SEM private key $D_{ID} = \langle W, d \rangle$ and the (ID, P_{ID}) pair to the SEM over a secret channel.

Sign: Suppose the user ID wants to get the signature of message m , the SEM checks whether ID is revoked; if not, the interaction between the signer and the SEM is as follows (I denotes the first part and II denotes the second):

1) User-Sign(I): randomly chooses $r_U \in \mathbb{Z}_q^*$ sends $R_U = g^{r_U}$ to the SEM.

2) SEM-Sign(I): randomly chooses $r_S \in \mathbb{Z}_q^*$, computes $R_S = g^{r_S}$, computes $R = R_S \cdot R_U$, $h_S = H_2(ID || W || 0 || P_{ID} || R || m)$, $t = r_S + d \cdot h_S$, sends back $\sigma_1 = \langle R_S, t \rangle$ and $c = H_0(R_S)$ to the user.

3) User-Sign (II): checks if $c = H_0(R_S)$; if they are equal, computes $R = R_S \cdot R_U$, $h_U = H_2(ID || W || 1 || P_{ID} || R || m)$, $V = r_U + x_{ID} \cdot h_U + t$. The final signature is $\sigma = \langle R, V, (ID || P_{ID} || W) \rangle$.

Verify: The verifier receives the signature and confirms as follows:

1) Get user's public key P_{ID} from *KeyGen* algorithm.

2) Compute

$$R = g^V P_{ID}^{-H_2(ID || P_{ID} || 1 || W || R || m)} (W \cdot Y^{H_1(ID || W)})^{-H_2(ID || P_{ID} || 0 || W || R || m)}$$

3) Verify the formula:

$$\begin{aligned} R' &= g^V P_{ID}^{-h_U} (W \cdot Y^{H_1(ID || W)})^{-h_S} \\ &= g^{r_S + r_U + d \cdot h_S + x_{ID} \cdot h_U} g^{-x_{ID} \cdot h_U} (g^w \cdot g^{sH_1(ID || W)})^{-h_S} \\ &= g^{r_S + r_U + d \cdot h_S} (g^{w + sH_1(ID || W)})^{-h_S} \\ &= g^{r_S + r_U + d \cdot h_S} g^{(d) \cdot (-h_S)} \\ &= R \end{aligned}$$

If established, the output T; Otherwise output F.

B. Hierarchical Authentication Architecture

In the current authentication methods, authentication must be accomplished between a user and its home AAA server. Authentication latency will increase considerably while MN moves far from its home network. According to the IBS characteristic, each MN that obtains prams can implement Sign and Verify. Therefore the authentication can be accomplished with the access network directly. Then the communication cost between the visited network and the home network is eliminated. We propose the hierarchical authentication framework. It consists of HA act as root KGC, several Level-one SEM, include Maps, and many Level-two users, include AR and MN.

In MIPv6 network, different access domain of the coverage may overlap, MN need to choose the right relationship of trust between the access domains. Each MN need to protect information form an AR (AR information table, ARIT), used to store AR can access the relevant information. ARIT maintain the following records: HA, AR and its reputation value. As shown in Table I.

TABLE I. AR INFORMATION TABLE

Type	ID	Reputation value
HA	7	16
AR ₄	17	9

For each AR, need to preserve a domain mobile nodes information form (MNIT), preserves of the current MNs information. MNIT the following fields: mobile node ID, reputation value and access time. As shown in Table II.

TABLE II. MOBILE NODES INFORMATION TABLE

ID	Reputation value	Access time
7	0.9	2008-7-30 10 : 22 : 40
17	0.7	2008-7-31 12 : 42 : 10

Hierarchical authentication scheme includes pre-handover and verification in two stages, the specific process shown in Figure 1 handover procedure described in detail:

- 1) $MN \rightarrow PAR : RtSolPr$;
- 2) $PAR \rightarrow all\ ARs : TrVaReq(IP_{PAR}, IP_{NAR}, LLA_{MN}, PCoA, NCoA, ID_{MN}, checksum)$
PAR sent t reputation search request to all ARs.
- 3) $NAR \rightarrow PAR : TrVaRsp(IP_{PAR}, IP_{NAR}, NCoA, TV_{MN+NAR}, checksum)$

NAR lookup credibility of the list and returned to the query results;

- 4) $PAR \rightarrow MN : PrRtAdv$

Given reputation parameter R , NAR response to the request T_{REQ} $\varphi = \frac{R}{T_{REQ}}$ (1)

As shown in formula (1), NAR is decided by parameter φ .

- 5) $MN \rightarrow PAR : FBU + AS$
- 6) $PAR \rightarrow NAR : RfTrReq(IP_{PAR}, IP_{NAR}, ID_{MN-NAR}, checksum) / HI+AS$

PAR send message to NAR with the highest φ . If there has none reputation value in his hometown domain, send message to the fastest response NAR .

- 7) $NAR \rightarrow PAR : RfTrRsp(IP_{PAR}, IP_{NAR}, ID_{MN-NAR}, TV_{MN-NAR}, checksum) / Hack + AA$

If success, update reputation value and return $RfTrRsp$ and update the list of AR reputation. Otherwise, return Hack .

- 8) $PAR \rightarrow MN : < BA_{HA} || TS\{BU_{HA} || R_{MN} || RrVa\}Sign_{HA} >$

When MN ready to move the new sub-network, randomly chooses $r_U \in Z_q^*$ sends $R_U = g^{r_U}$ to the HA. . HA checks whether MN's identify is revoked. If not, generate bundled

home the updated registration confirmation message BU, the reputation value of the MN in the list of MN reputation, send verification $\sigma_1 = < R_S, t >$ and $c = H_0(R_S)$ to the MN. Otherwise, send the wrong message.

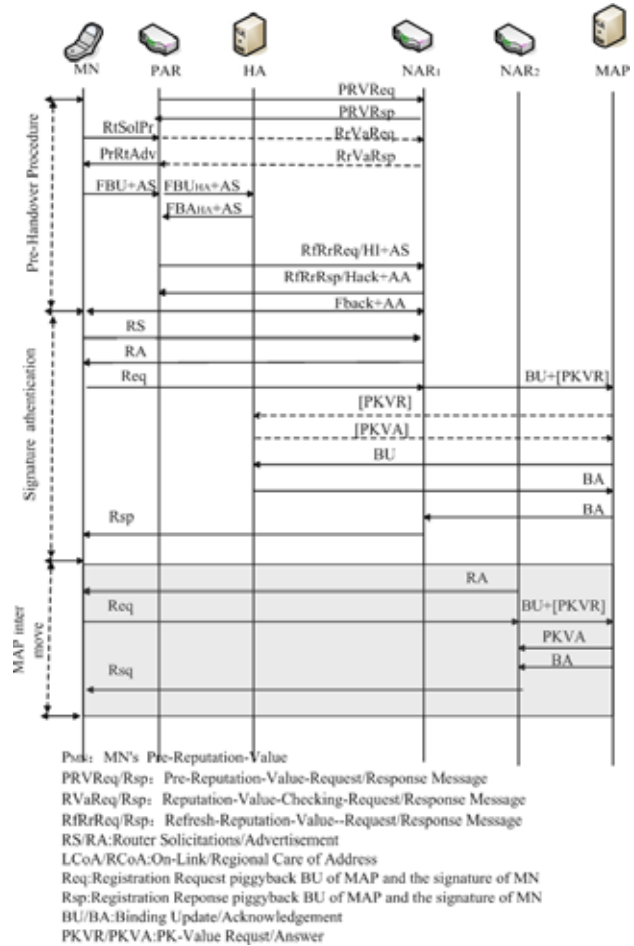


Figure 1. Hierarchical Authentication Protocol using IBS and CPK.

- 9) $MN \rightarrow NAR : Req = < BU_{HA} || TS || \{BU_{HA} || TS\}Sign_{MN+HA} || PK_{MN} || ID_{MN} >$

When MN reach new sub-network, according to NAR received news sent the router declared build BU_{HA} after it obtains the LCoA and the RCoA. Then it generates the signature for BU using share prams, sign binding update with MN's semi-signature, and news updates bundled together with both MN's semi-signature and HA's semi-signature and identity of information sent to the NAR.

- 10) $NAR_1 \rightarrow MAP : < BU_{MAP}, BU_{HA}, [PKVR] >$

AR_1 queries the PK_{ID} firstly. If the result is PK_{ID} , it can verify the signature $NAR \rightarrow MAP : < BU_{MAP}, BU_{HA}, [PKVR] >$ with PK_{ID} . If verification is success, authenticating MN is completed. Then sends $MAP : < BU_{MAP}, BU_{HA}, [PKVR] >$ [QVR], verifies the signature. Thus the BU procedure and verify can be parallel.

- 11) $MAP \rightarrow NAR : < \{BA_{MAP}\}ID_{MAP} >$

After MAP verified MN the signatures, convinced news binding updating message are signed by the HA and the MN, then registered the MN's location LCoA, and signed BA_{MAP} with MAP identity ID_{MAP} .

12) $NAR \rightarrow MN : ARsp = \langle BA_{MAP} || TS_1 || TS_2 || \{BA_{MAP} || TS_1\}Sign_{MAP} || \{BA_{MAP} || TS_2\}Sign_{NAR_1} \rangle$

a) NAR generates the signature for BA using params and its private key. Then it builds $ARsp$ message and sends it to the MN.

b) The MN verifies $\{BA_{MAP} || TS_1\}Sign_{MAP}$. Then it verifies $\{BA_{MAP} || TS_2\}Sign_{NAR_1}$. If verification is success, authenticating network is completed, so mutual authentication is finished.

c) In order to reduce latency greatly, the MN firstly resumes transmission with CN. Then it verifies the signature and updates the public key value list.

IV. REPUTATION SYSTEM

In this reputation mechanism, to ensure mutual reputation authentication between AR and the MN, each AR and MN keeps a reputation list. Each MN node maintains a list of ARs reputation value. Accordingly, each AR maintain an reputation value list of the MNs. The reputation list is composed of two parts: direct reputation and indirect credibility.

A. Direct reputation

Direct reputation is the list that MN maintains AR_j 's reputation information from them own history records.

1) MN 's direct reputation value R^d_{MN}

$R^d_{MN \rightarrow AR_j}$ expresses MN direct trust AR_j value. MN checks the validity of signature of the AR_j . If valid, direct reputation increases α . Otherwise, reduces α . If the value of the $R^d_{MN \rightarrow AR_j}$ below the threshold value R_T , AR_j should be deleted from the list;

2) AR_j 's direct reputation value $R^d_{AR_j}$

$R^d_{MN \rightarrow AR_j}$ expresses AR_j direct trust MN value. AR_j checks the validity of signature of the MN. If valid, direct reputation increases α . Otherwise, reduces α . If the value of the $R^d_{MN \rightarrow AR_j}$ below the threshold value R_T , AR_j should be deleted from the list;

B. Indirect reputation R^i

1) MN 's indirect reputation value R^i_{MN}

When MN received AR_j 's reputation information from other AR, checks the reputation of the AR. If it is credible, updates R^i_{MN} . Suppose MN received AR_j 's reputation information from AR_i . MN checks the reputation value of the AR_i , if it is node MN is bigger than the credible threshold value R_T , updates R^i_{MN} .

$$R^c_{MN,AR_i} = R^c_{MN,AR_j} + (R_{AR_i,AR_j} - R^c_{MN,AR_j}) * R_{MN,AR_i} \quad (2)$$

2) AR_j 's indirect reputation value $R^i_{AR_j}$

When AR_j received MN's reputation information from other AR, checks the reputation of the AR. If it is credible, updates R^i_{MN} . Supposes AR_j to receive MN's reputation information from AR_i . MN checks the reputation value of the AR_i , if it is node MN is bigger than the credible threshold value R_T , updates R^i_{MN} .

$$R^c_{AR_i,MN} = R^c_{AR_j,MN} + (R_{AR_i,AR_j} - R^c_{AR_j,MN}) * R_{MN,AR_i} \quad (3)$$

V. ANALYSIS

A. Performance Analysis

In this section we propose an analytical model to evaluate the handover latency among DAMIPv6 [3], HAMIPv6[5], 2-IBS-HAMIPv6 and our SMC-IBS-HAMIPv6.

Note that the handover latency is the period time from a MN receiving the first RA packet in the new sub-network to it receiving BA from HA. FAMIPv6[1] combines HMIPv6 signals with Diameter signals. The challenge of visited AAA server (AAAv) is piggybacked in the MAP's RA message to reduce the number of RTs. So unilateral authentication will only take one RT between the MN and its home network, and one more RT with AAAh for mutual authentication. IBS-FAMIPv6 [2] combines MIPv6 authentication with IBS signature to implement the mutual authentication, and optimizes the access authentication and the home registration. In the solution, the access authentication can be accomplished in the visited network instead of the home network, which can eliminate the transport latency arose by the interaction with the home network in the access authentication. Also signing or verifying the home can accomplish the authentication registration messages, and then the handover procedure-integrating authentication only needs one round trip. So the additional load arose by authentication can be minimized. We prove that the access authentication and home registration process handover latency of ours is better than that of the existing solution and our solution satisfies the mutual authentication security.

The transport latency can be categorized into three parts: first is wireless latency a, second is intra-domain latency b, and third is inter-domain latency c. We suppose a and b are fixed values. While c is a variable because of the changeable distance between two sub networks. Let $a > b$ and $b \geq c$. Besides the transport latency and the node processing time t_p , the more important cost is the processing time for authentication t . This cost is correlative to the specified algorithm and the node processing capability. So there are two variables: the transport latency c and the processing time t. Let t_{RSA} be the total processing time required to signature plus verification in RSA algorithm.

There are several dominant cost operations in SMC-IBS. One is the operations in group G_1 or G_2 , such as multiplication in G_1 , scale multiplication and point addition in G . Another is the bilinear pairing. According to the introduction in Section III, we can draw the following results, which are shown in Table III.

TABLE III. PERFORMANCE ANALYSIS FOR SMC-IBS

Operation type	Bilinear Pairings	Exp	MtP
Signing	0	2	0
Verification	0	4	0
ACGA Signing 1	0	1	0
ACGA Verify	0	2	0

① When MN moves between neighboring domains frequently, pre-calculation is performed to reduce the number of point, multiplication operations. Supposes random variable N to express an effective authentication needs the complete interactive number of times, passes through the time completely alternately to obtain the effective authentication the probability is:

$$Pr ob(N = i) = (p)^{i-1} \times (1 - p) \tag{4}$$

A MN effective authentication time average interactive number of times for is the $1, 2, \dots, N$ mathematic expectation, and MN most initiates n authentication to request, therefore $K = n$, therefore:

$$E(N) = \sum_{i=1}^n Pr ob(N = i) = \sum_{i=1}^n i(p)^{i-1} (1 - p) \tag{5}$$

According to [9][10], the cost of computing a 512-b Tate pairing plus two SMs and one hash function is about 3.5 times that of computing a 1024-b modular exponentiation. In addition, the cost of one SM with 160-b p is approximate to that of one modular exponentiation with 1024-b RSA modulus n . We can get the following conclusions, combined specific process of the schemes we get results:

$$T_{FAMIPV6} = E[N] \times T_{FAMIPV6} = \sum_{i=1}^n i(p)^{i-1} (1 - p) \times [6a + 8b + 6c + 21tp + 2tRSA] \tag{6}$$

$$T_{IBS-FAMIPV6} = E[N] \times T_{IBS-FAMIPV6} = \sum_{i=1}^n i(p)^{i-1} (1 - p) \times [\max(18 + 7t, 20.5 + 2t + H + \frac{25t^2 - 45t + 20.25}{4(H - 2)})] \tag{7}$$

$$T_{SMC-HAMIPV6} = \sum_{i=1}^n i(p)^{i-1} (1 - p) \times [2a + 2b + 6t_p + t_{verify} + 2c] \tag{8}$$

In order to estimate these solutions, Let $a = 4ms$, $b = 2ms$ $tp = 0.5ms$ and $t_{RSA} = t$, then

$$T_{FAMIPV6} = 56.5 + 2t + 3H \tag{9}$$

$$T_{IBS-FAMIPV6} = E[N] \times T_{IBS-FAMIPV6} = \sum_{i=1}^n i(p)^{i-1} (1 - p) \times [\max(18 + 7t, 20.5 + 2t +$$

$$H + \frac{25t^2 - 45t + 20.25}{4(H - 2)})] \tag{11}$$

$$T_{SMC-HAMIPV6} = 17 + t + H$$

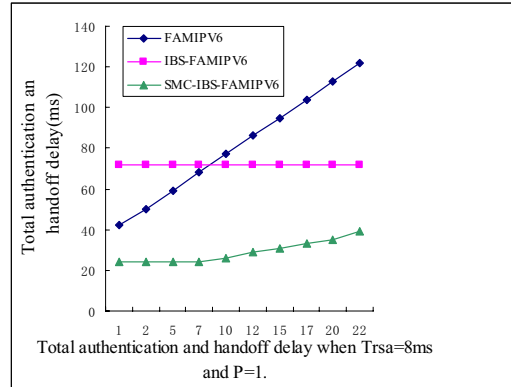


Figure 2 Total authentication and handoff delay when $n = m$

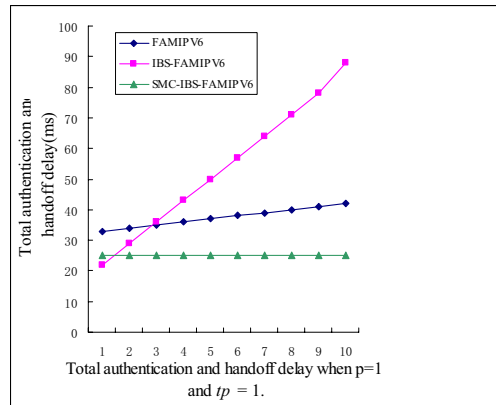


Figure 3 Total authentication and handoff delay when $t_p = 1$ and $p=1$.

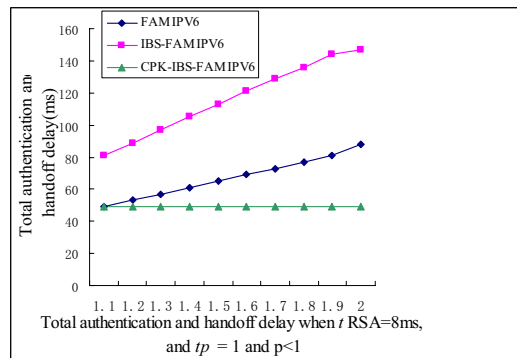


Figure 4 Total authentication and handoff delay when $t_{RSA} = 8ms$, $t_p = 1$ and $p < 1$.

Fig2 and Fig3 reveals the handover latency when $p=1$. As shown in Figure that F that get the minimum as t_p is small, but increases its along with t_p the growth rate to be also biggest, causes t_p increases after the certain extent IBS/SMC-IBS is always below F; Shown in Figure 4, t_{RSA} is small when SMC-IBS is smallest, increases the IBS-F growth rate along with t_{RSA} to be biggest, but enhances the computer

processing performance through to cause tRSA to reduce is the inevitable trend. In two chart has SMC-IBS is always smaller than IBS-F; shown in Figure 3, tRSA smaller SMC-IBS The smallest, with the increase of IBS2F tRSA largest increase, by Improve the performance of the computer processing is an inevitable trend of decreasing tRSA. In Figure 3 and Figure 4, SMC-IBS always smaller than IBS-F.

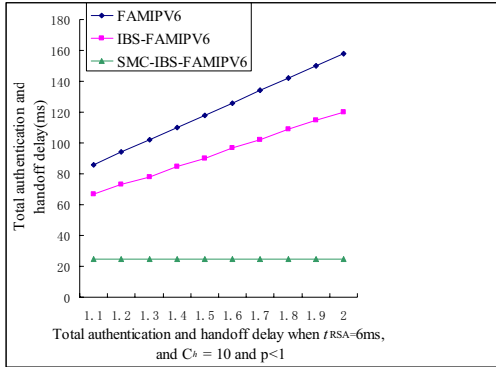


Figure 5 Total authentication and handoff delay when tRSA= 6ms, tp = 10 and p<1.

Given $t_{RSA} = 8ms$, $C_h = 1$ and $t_{RSA} = 6ms$, $t_p = 10$ respectively in figure 4 and figure 5. The handover latency, representing MN domain close to home and far away from the access domain two typical cases. It is easy to know that assigns tRSA and Ch, SMC-IBS is the constant independent of E[8], but other two kind of scheme increase along with E [8] increase; When tRSA is small, and t_p is big time SMC-IBS surpasses F obviously, and in the majority situations the SMC-IBS performance is most superior.

B. Security Analysis

In this section, we consider the following security notions.

1) Privacy

In SMC mechanism, in accordance with section 3 key Generation mechanism we can see that the private key divide into the two parts, kept by HA and MN respectively. Although the HA has semi-private key, but can not get part of the MN's private key and can not fabricate the signature. For the other nodes, the only publicly known parameters, but the calculation of group G as the DH on the issue is difficult, the other nodes cannot calculate. Therefore, only the private key of an entity PKG aware that other entities, including the HA cannot access.

2) Unforgeability

Our SMC-HAMIPv6-IBS scheme can be regarded as an identity based signature scheme with multiple PKGs, each PKG is associated with a role. In order to activate role set AR={rj,...,rk}, a user has to generate a valid signature using the sum of assigned keys corresponding to all the roles of AR on the user's ID. We use similar method as in [7] to prove the unforgeability of our scheme. Suppose the hash functions H1 and H2 are random oracles.

The following attack model appropriate to SMC-HAMIPv6 scheme is secure against the existential forgery on adaptive chosen message and identity attacks (EUF-SMC-HAMIPv6-

CMIA) against adversary $A = \langle A_I, A_{II} \rangle$, where adversary A_I acts as a dishonest MN and adversary A_{II} acts as acts as a malicious HA.

SMC Signatures Type I Adversary: Adversary A_I does not have access to the master key. On the other hand, A_I may request and replace the public keys, extract the SEM private key and the user private key and make the sign queries.

Here are several natural restrictions on the Type I adversary:

- (1). A_I cannot extract the SEM private key of the challenge identity ID^* .
- (2). A_I has not issued any SEM-Sign query on the forged message m for the challenged identity ID^* .
- (3). A_I cannot make a Complete-Sign query on the forged message m for the challenged identity ID^* .

SMC Signatures Type II Adversary: Adversary A_{II} does have access to the master key, but cannot replace the public keys of entities. Adversary A_{II} can compute the SEM private key itself, request the public keys, extract users' private key and make the sign queries, all for the identities of its choice. The restrictions on Type II Adversary are: (1) A_{II} cannot replace the public keys of the challenge identity ID^* . (2) A_{II} cannot extract the user private key for ID^* at any point.(3) A_{II} cannot make an User-Sign query on the forged message m for the challenged identity ID^* .(4) A_{II} cannot produce a Complete-Sign query on the forged message m for the challenged identity ID^* .

Definition 3 (UF-SMC-HAMIPv6-CMA): We say that our SMC-SMCHAMIPv6 scheme based on SMC signature is secure against EUF-CMIA if there is no efficient adversary in the above game with a non-negligible advantage against challenger C for both types of adversary in the following game:

If no polynomial time algorithm A has a non-negligible advantage against a challenger C in the following game:

1. Setup: C takes as input 1^k , runs the Setup algorithm, and gives A the resulting params. The master key is given to A if it is a Type II adversary.
2. Attack: A issues a sequence of requests, each request being either a query of Create, Replace, SEM-Extract, User-Extract, SEM-Sign, User-Sign or Complete-Sign for a particular entity.
Create queries create users by either registering the user public key when playing against A_I , or executing the Key-Gen algorithm for A_{II} . Replace queries let A_I to change user public key at its wish. Two Extract queries return the SEM and user private key respectively. Sign queries are to be explained shortly. These queries may be asked adaptively, subjected to the rules on adversary behaviors to be defined below.
3. Forgery: A outputs a signature σ on message m signed by user ID with public key P_{ID} . The only restriction is that (m, ID) does not appear in the set of previous Sign queries.

A wins the game if Verify ($params, \sigma, m, ID, P_{ID}$) is true. The advantage of A is defined as the probability that it wins.

Our SMC-HAMIPv6 scheme is based on SMC identity-based signature scheme, and SMC scheme is completely secure against existential forgery under adaptively chosen message and ID attack [8] in the random oracle model assuming the hardness of DLP. The security proof of SMC scheme is given in [8].

Theorem 1. If SMC identity-based signature scheme is secure against the Type I adversary under random oracle model, then our SMC-HAIPv6 scheme is secure against the attack model UF-SMC-HAMIPv6-CMA.

Proof. Suppose there exists a polynomial-time adversary A_I be a forger that breaks the proposed signature scheme under adaptive chosen message and identity attack. A_I can attack our scheme in the game described in Definition 2 with a non-negligible advantage $Adv(A_I)$. Our main idea is to construct an adversary B that uses A_I to gain advantage $Adv(A_I) > Adv(A_I)$ against SMC scheme solve the DLP instance (p, q, g, g^a).

B works by simulate A_I 's environment as lecture[8].

The simulation fails if $H_0(R_S) = c_I$, but no R'_S can be found or $R'_S \neq R_S$. For the first case, the probability that AI can predict $H_0(R_S) = c_I$ without asking the random oracle is at most $1/2^l$. For the second case, collision must have occurred and the probability for this is at most $((q_H + q_S)(q_H + q_S + 1)/2)/2^l \leq (q_H + q_S + 1)2/2^l$. We just assume A asked for $H_2(ID_I \| P_I \| 1 \| W_I \| R_U \| R_S \| m)$. If R'_S was not found since A knew the value of R_S before B .

(4). Complete-Sign: If both the SEM private key and the user private key are available, signing is trivial. If either one of them is unavailable, this request can be simulated faithfully as a combination of the above two simulation, but much easier since we no longer need the technicality to solve the problem that either one of the R_S and R_U is unknown.

Forgery: According to the forking lemma in [7], suppose $\langle R^*, V^* \rangle$ be a forgery of a signature on message m^* with respect to (ID^*, PID^*, W^*) that is output by A_I at the end of the attack. If A_I does not output $ID^* = ID_I$ as a part of the forgery then B aborts (the probability that B does not abort the simulation is $O(1/qH_1)$).

Consider the case that W^* has not been replaced, i.e. $W^* = W_I = g^a Y^{-e_I}$ where $e_I = H_1(ID_I \| W_I)$. B then replays A_I with the same random tape but different H_2 after the point $(ID^* \| W^* \| 0 \| P_{ID}^* \| R^* \| m^*)$. Suppose H_2 outputs h_S and h'_S in the first round and the second round respectively, where $h_S \neq h'_S$. Note the special step in the simulation of

H_2 ensures $H_2(ID^* \| P_{ID}^* \| 1 \| W^* \| R^* \| m^*)$ remains the same after forking. Moreover, since $e_I = H_1(ID^* \| W^*)$ is defined at the very beginning of the game, it remains the same as well.

So we get another valid forgery $\langle R^*, V^* \rangle$.

$$R^* = g^{V'} PK_{ID}^{-H_2(ID \| P_{ID} \| 1 \| W \| R \| m)} (W \cdot Y^{H_1(ID \| W)})^{-h_S}$$

$$R' = g^{V'} PK_{ID}^{-H_2(ID \| P_{ID} \| 1 \| W \| R \| m)} (W \cdot Y^{H_1(ID \| W)})^{-h'_S}$$

B thus gets $V^* - ah_S = V' - ah'_S$. DLP's solution is $a = (V^* - V') / (h_S - h'_S)$.

In the second case, W^* is replaced. We would like to apply forking lemma so that $H_1(ID^* \| W^*)$ changes from h to h' after forking, but H_2 queries related to W^* remain the same. Since W^* never appears in Sign query of any kind, it is thus safe to rearrange all those H_2 queries before the forking, without affecting the adversary's view. After forking, we get another valid forgery $\langle R^*, V^* \rangle$ where

$$R^* = g^{V'} P_{ID}^{-H_2(ID^* \| P_{ID}^* \| 1 \| W^* \| R^* \| m^*)} (W^* \cdot Y^h)^{-H_2(ID^* \| P_{ID}^* \| 0 \| W^* \| R^* \| m^*)} \quad (1)$$

$$R' = g^{V'} P_{ID}^{-H_2(ID^* \| P_{ID}^* \| 1 \| W^* \| R^* \| m^*)} (W^* \cdot Y^{h'})^{-H_2(ID^* \| P_{ID}^* \| 0 \| W^* \| R^* \| m^*)} \quad (2)$$

$$\frac{R^*}{R'} = \frac{g^{V'} P_{ID}^{-H_2(ID^* \| P_{ID}^* \| 1 \| W^* \| R^* \| m^*)} (W^* \cdot Y^h)^{-H_2(ID^* \| P_{ID}^* \| 0 \| W^* \| R^* \| m^*)}}{g^{V'} P_{ID}^{-H_2(ID^* \| P_{ID}^* \| 1 \| W^* \| R^* \| m^*)} (W^* \cdot Y^{h'})^{-H_2(ID^* \| P_{ID}^* \| 0 \| W^* \| R^* \| m^*)}} \quad (3)$$

B solves the DLP by $a = (V^* - V') / (H_2(ID^* \| W^* \| 0 \| P_{ID}^* \| R^* \| m^*)(h - h'))$.

Theorem 2. If SMC identity-based signature scheme is secure against the Type II adversary under random oracle model assuming the DLP in G is hard, then our SMC-HAIPv6 scheme is secure against the attack model UF-SMC-HAMIPv6-CMA.

Proof. Suppose there exists a polynomial-time adversary A_{II} be a forger that breaks the proposed signature scheme under adaptive chosen message and identity attack. A_{II} can attack our scheme in the game described in Definition 2 with a non-negligible advantage $Adv(A_{II})$. Our main idea is to construct an adversary B that uses A_{II} to gain advantage $Adv(A_{II}) > Adv(A_{II})$ against SMC scheme solve the DLP instance (p, q, g, g^a).

Under the UF-SMC-HAMIPv6-CMA model described in Definition 3, A has access to the random H_0, H_1 and H_2 , A issues a sequence of requests, each request being either a query of Create, Replace, SEM-Extract, User-Extract, for a particular entity, which are taken from SMC's scheme, for every query made by A to random oracles H_0, H_1 and H_2 , B forwards it to its challenger and sends the answer back to A . B simulates the Activate oracle as lecture[8].

The simulation fails if $H_0(R_S) = c_I$, but no R'_S can be found or $R'_S \neq R_S$. For the first case, the probability that AI can predict $H_0(R_S) = c_I$ without asking the random oracle

is at most $1/2^l$. For the second case, collision must have occurred and the probability for this is at most $((q_H + q_S)(q_H + q_S + 1)/2)/2^l \leq (q_H + q_S + 1)2/2^l$.

We just assume A asked for $H_2(ID_I || P_I || 1 || W_I || R_U || R_S || m)$. if R'_S was not found since A knew the value of R_S before B .

(4). Complete-Sign: If both the SEM private key and the user private key are available, signing is trivial. If either one of them is unavailable, this request can be simulated faithfully as a combination of the above two simulation, but much easier since we no longer need the technicality to solve the problem that either one of the R_S and R_U is unknown.

Forgery: According to the forking lemma in [11], suppose $\langle R^*, V^* \rangle$ be a forgery of a signature on message m^* with respect to (ID^*, PID^*, W^*) that is output by A_{II} at the end of the attack. If A_{II} does not output $ID^* = ID_I$ as a part of the forgery then B aborts (the probability that B does not abort the simulation is $O(1/qH_1)$).

B then replays A_{II} with the same random tape but different H_2 after the point $(ID^* || W^* || 0 || P_{ID}^* || R^* || m^*)$. Suppose H_2 outputs h_U and h'_U in the first round and the second round respectively, where $h_U \neq h'_U$. Note the special step in the simulation of H_2 ensures $H_2(ID^* || P_{ID}^* || 1 || W^* || R^* || m^*)$ remains the same after forking.

So we get another valid forgery $\langle R', V' \rangle$.

$$R^* = g^{V^*} P_{ID}^{-H_2(ID || P_{ID} || 0 || W || R || m)} (W \cdot Y^{H_1(ID || W)})^{-h_U}$$

$$R' = g^{V'} P_{ID}^{-H_2(ID || P_{ID} || 1 || W || R || m)} (W \cdot Y^{H_1(ID || W)})^{-h'_U}$$

Since $P_{ID} = g^a$, B thus gets $V^* - ah_S = V' - ah'_S$. DLP's solution is $a = (V^* - V') / (h_U - h'_U)$.

3) Escrow problem.

A major drawback of all identity-based and security mediated cryptosystems so far proposed is that they require a trusted third party to generate keys for all entities. This is widely known as the escrow problem. The SMC signature, in accordance with section 3 Key Generation mechanism we can see that dispense with certificates, the key escrow of a user's private key is inherent in the identity-based signature scheme a trusted third party called the PKG (Private Key Generator) manages the generation and distribution of the users' private keys. Although the PKG has part private key, but can not get part of the MN's private key and can not fabricate the signature. For the other nodes, the only publicly known parameters. Therefore, only the private key of an entity PKG aware that other entities, including the SMC cannot access.

4) Public key revocation.

The need to be able to revoke public keys was recognized early in the development of public key infrastructure. Private keys will be compromised and in such a case it is no longer safe to use the corresponding public key. Initial solutions

relied on certificate revocation lists (CRLs) similar to the idea of black lists for credit cards. The difficulty of managing CRLs has led to alternative revocation solutions [8], many of which rely on some on-line checking. As modern networks become more reliable, use of on-line servers becomes much more realistic than it was several years ago. Mediated signature was designed as a method to revoke a key when a user suspects key compromise, or when a user is removed from a position of authority. The SMC signature is to use an on-line mediator for every transaction. This on-line mediator is referred to as a HA(SEM) since it provides a control of security capabilities. If the SEM does not cooperate then no transactions with the public key are possible any longer. Once the HA(SEM) is notified that a user's key is to be revoked its use can be immediately stopped.

VI. CONCLUSION

It is an important issue to reduce handover latency integrating authentication in wireless mobile networks. In this paper, we propose the hierarchical authentication scheme for mobile IPv6 networks. Instead of using certificate to achieve mutual authentication, we adopt SMC-IBS. Compared to PKI based schemes, there is no heavy operation or communication overhead for certificate in MN. In addition, our solution combines handover with authentication procedure, and utilizes the SMC-IBS characteristic to reduce the alternation between the visited network and the home network.

REFERENCES

- [1] C. Kim, YS Kim, EN Huh, and YS Mun, "Performance Improvement in Mobile IPv6 Using AAA and Fast Handoff," in Proc. ICCSA, Springer-Verlag LNCS 3043, pp. 738-745, 2004.
- [2] P. Engelstad, T. Haslestad, and F. Paint, "Authenticated Access for IPv6 Supported Mobility," in Proc. IEEE International Symposium on Computers and Communication. Kemer-Antalya, pp. 569-575, 2003.
- [3] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," RFC 2716, October 1999.
- [4] A. Shamir, "Identity-base cryptosystems and signature schemes," Advances in Cryptology - Crypto, Springer-Verlag LNCS 196, pp. 47-53, 1984.
- [5] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairings," Advances in Cryptology - Crypto, Springer-Verlag LNCS 2139, pp. 213-229, 2001.
- [6] Zhang Jiao, Zhang Yujun, Zhang Hanwen, Li Zhongcheng, "A Fast Inter-Domain Authentication Method Combining Trust Mechanism in Mobile IPv6 Networks" Journal of Computer Research and Development. Vol.45 (6), 2008, pp.951~959.
- [7] X. Nan, Z. Cheng. "Profile to network security techniques". Beijing: National defense industry press, 2003.
- [8] Wun-She Yap, Sherman S.M. Chow, Swee-Huay Heng, and Bok-Min Goi, "Security Mediated Certificateless Signatures", Springer-Verlag, ACNS 2007, LNCS 4521, pp. 459-477, 2007.
- [9] PSLM. Barreto, HY Kim, B. Lynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," Advances in Cryptology - Crypto, Springer-Verlag LNCS 2442, 2002, pp. 354-368
- [10] SD.Galbraith, K.Harrison and D.Soldera. "Implementing the Tate Pairing". In Proc. of Algorithmic Number Theory Symposium, ANTS V. LNCS 2369, Heidelberg: Springer-Verlag, 2002, pp.324-337.
- [11] D.Pointcheval and J.Stern. "Security proofs for signature scheme". Advances in Cryptology--Eurocrypt 1996. LNCS 1070, Heidelberg: Springer-Verlag, 1996, pp.387-398.