DOI: 10.2298/CSIS121114041G

# A Hybrid Approach to Secure Hierarchical Mobile IPv6 Networks

Tianhan Gao[1], Nan Guo[2, *], Kangbin Yim[3]

[1] Faculty of Software College, Northeastern University,
110819 Shenyang, China
gaoth@mail.neu.edu.cn
[2] Faculty of Information Science and Engineering College, Northeastern University,
110819 Shenyang, China
guonan@ise.neu.edu.cn
[3] Faculty of Information Security Engineering, Soonchunhyang University,
336745 Asan, Korea
Yim@sch.ac.kr

**Abstract.** Establishing secure access and communications in a hierarchical mobile IPv6 (HMIPv6) network, when a mobile node is roaming into a foreign network, is a challenging task and has so far received little attention. Existing solutions are mainly based on public key infrastructure (PKI) or identity-based cryptography (IBC). However, these solutions suffer from either efficiency or scalability problems. In this paper, we leverage the combination of PKI and certificate-based cryptography and propose a hierarchical security architecture for the HMIPv6 roaming service. Under this architecture, we present a mutual authentication protocol based on a novel cross-certificate and certificate-based signature scheme. Mutual authentication is achieved locally during the mobile node's handover. In addition, we propose a key establishment scheme and integrate it into the authentication protocol which can be utilized to set up a secure channel for subsequent communications after authentication. As far as we know, our approach is the first addressing the security of HMIPv6 networks using such a hybrid approach. In comparison with PKI-based and IBC-based schemes, our solution has better overall performance in terms of authenticated handover latency.

**Keywords:** hierarchical mobile IPv6, mutual authentication, identity-based cryptography, certificate-based cryptography, cross-certificate

## 1. Introduction

MIPv6 [1], developed by Internet Engineering Task Force (IETF), has been recognized as the best solution for linking different mobile networks. More

[*] Corresponding author. Tel.: +8624-83681822. E-mail: Guonan@ise.neu.edu.cn

specifically HMIPv6 extends MIPv6 [2] by introducing local mobility management. However, HMIPv6 does not specify nor endorse any particular security mechanisms which may thus result in a variety of threats such as redirection, denial of service (DoS), man in the middle attacks, and resource misuse [3, 4]. Consequently, how to secure HMIPv6 network is currently the focus of intense attention in the research community.

In order to securely deploy HMIPv6 services, mutual authentication between mobile nodes and access points in the visited networks is essential. Moreover, it is crucial that secure channels be dynamically set up with respect to key establishments among participants for subsequent communications after a successful authentication.

The general approach for achieving mutual authentication and secure channels is based on the use of a public key infrastructure (PKI) [5]. In this approach, mutual authentication between the mobile node and the access point is performed by verifying the other party's digital signature and public key certificate (PKC) issued by a certificate authority (CA). Communications can also be protected via public key cryptography. As a result, no shared keys or security associations are needed for the mobile node and the access point. They only need to have their own private and public key pair. However, the major drawback of a PKI solution is that if the mobile node and the access point belong to different trust domains that have different CAs, they have to piggyback and verify a long PKC chain which typically results in a heavy burden on each side and affects performance. Another obstacle that impedes PKI's employment in HMIPv6 networks is the overhead due to the transmission and storage of PKC. Frequent changes in network topology make the management of PKC even harder.

Some of the drawbacks of PKI have been addressed by identity-based cryptography (IBC) [13]. The use of IBC protocols greatly simplifies the key management procedures of conventional PKI and eliminates the need for PKC. Therefore, several schemes [8-11] have been proposed to integrate IBC into HMIPv6 network for authentication and key management services. In such schemes, the private key generator (PKG) introduced by IBC is used for distributing secret keys to all entities in a HMIPv6 network. Mutual authentication and secure communications are then directly implemented between mobile nodes and access points through IBC-based signature and encryption mechanisms without the help of PKI. However these schemes are based on the assumption that the PKG is trusted by all the participants, which makes them only suitable for small scale mobile networks. Moreover, the IBC protocols adopted by these schemes have also some intractable problems, such as the secret key escrow and distribution problems as well as the computational costs incurred by pairing-based operations.

In general, although PKI suffers from a heavy maintenance workload, it has been widely deployed in real world and can support authentication even for large scale, hierarchical groups. On the other hand, IBC supports an efficient key management but is only suitable for a closed organization where the PKG is completely trusted by every entity. Consequently, a promising approach is to concatenate these two techniques in order to gain the benefits from both. This combination can support secure communications between group managers already in possession of certificates, as well as between individual users without certificates. Therefore a few approaches have been proposed that combine PKI and IBC [14-16]. Their focus is however on scalability and they do not address security in HMIPv6 networks. It is thus crucial to develop a hybrid PKI and IBC scheme for securing HMIPv6 networks.

In this paper, we present an authentication protocol for HMIPv6 roaming service based on the combination of PKI and IBC. A novel signature scheme based on cross-certificate [24] and certificated-based signature [22, 23] is proposed as building block for our protocol. Mutual authentication is achieved locally within the access network. The proposed protocol presents a more efficient PKC management because of the cross-certificate mechanism. Also the secret key escrow and distribution problems inherited from IBC are addressed by the use of certificate-based cryptography. A key establishment scheme is also incorporated into our protocol to build a secure channel for subsequent communications. To further improve the efficiency of our protocol, we integrate the authentication operations into the HMIPv6 mobility management process. Performance analysis demonstrates that our proposed protocol outperforms existing ones in terms of handover latency during authentication.

The rest of this paper is organized as follows. Section 2 presents the HMIPv6 and certificate-based cryptographic primitives. We describe our proposed hybrid security architecture in Section 3 as well as the mutual authentication and key establishment scheme for HMIPv6 roaming service in Section 4. Performance analysis of our scheme is elaborated in Section 5. In section 6, we assess how our scheme satisfies the security requirements of HMIPv6 networks. Section 7 discusses the related work. Finally, we conclude the paper in Section 8.

## 2. Background

In this section, we provide an overview of the HMIPv6 protocol and certificate-based cryptography for readers to better understand our constructions.

### 2.1. HMIPv6 networks

To alleviate the latency and the amount of the signaling messages occurring during handover, HMIPv6 has been adopted by IETF as the hierarchical mobility management enhancement for MIPv6. A new entity, called mobile anchor point (MAP), is introduced, which is a mobility agent in charge of certain access routers (ARs). The MAP and these routers form an administrative MAP domain. According to HMIPv6, each mobile node (MN) is addressable by two types of address on the visited link: the on-Link Care-of Address (LCoA), and the Regional Care-of Address (RCoA). The LCoA is configured based on the mobile node's interface, whereas the RCoA is an address on the MAP's subnet. As shown in Fig.1, a mobile node entering a MAP domain will receive a router advertisement (RA) with which it can configure its RCoA and LCoA. Thereafter, the mobile node sends a remote binding update (RBU) to its home agent (HA) in its home domain and its correspondent nodes whereby to bind its RCoA with its home address. In the meantime, the mobile node registers its LCoA with the MAP through a local binding update (LBU). The home agent intercepts the initial packets and tunnels them to the mobile node's RCoA. Function as a local home agent, the MAP will receive all the packets on behalf of the mobile node and will then encapsulate and forward them to the mobile node's current LCoA. The subsequent packets will directly hit the mobile node's RCoA by means of route optimization. If the mobile node moves within the MAP domain, only the LBU should be sent to the MAP in order to register its new LCoA. The RCoA remains unchanged as long as mobile node stays in the current MAP domain. As a consequence, the delays and signaling overhead induced by the RBU can be considerably reduced through such local mobility management strategy. With this salient feature, HMIPv6 is expected to become the fundamental support for next generation mobile networks.

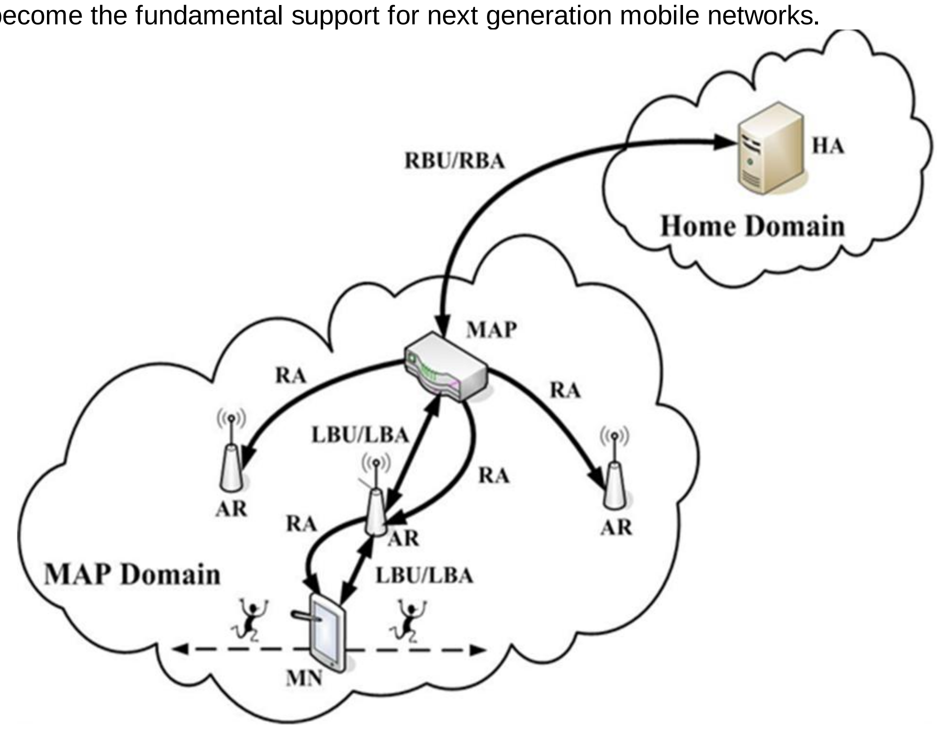



**Fig 1** HMIPv6 network

## 2.2. Bilinear pairings

Let G be an additive group and $G_T$ be a multiplicative group of the same prime order q. Let $I_G$ and $I_{GT}$ be the generator of G and $G_T$ respectively. Assume that the discrete logarithm problem [21] is hard in both G and $G_T$. A mapping $\hat{e}: G \times G \rightarrow G_T$ which satisfies the following properties is called bilinear pairing:

(1) *Bilinear*: *For all* $P, Q \in G$ *and* $a, b \in Z_q^*$, $\hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(P, Q)^{ab}$, *where* $Z_q^* = \{1, 2, \ldots q-1\}$;

(2) *Non-degenerate*: $\hat{e}(P, Q) \neq I_{GT}$;

(3) *Computable*: *For all* $P, Q \in G$, *there is an efficient approach to compute* $\hat{e}(P, Q) \in G_T$.

The Weil and Tate pairing [20] on supersingular elliptic curves can be modified to construct such bilinear pairing. Most literature IBC-based schemes employ these pairings as primitives [35].

## 2.3. Certificate-based Cryptography

In 1984, Shamir proposed the concept of identity-based cryptography (IBC) [13] which significantly reduced the system complexity and the cost for managing the public key compared with PKI. However, a major drawback of IBC is that the PKG can access all the communications among users, and thus can yield any user's secret key. Secret key escrow problem is inherent and in addition the secret keys must be sent over secure channels, making key distribution difficult.

To fill the gap between traditional PKI and IBC, the notion of certificate-based encryption (CBE) [21] was proposed by Gentry in 2003. Certificate-based Cryptography (CBC) combines PKI and IBC and consists of a CA and a set of users. Each user generates its own private and public key pair and requests a certificate from the CA. The CA uses the private key generation algorithm of the Boneh-Franklin IBE scheme [17] as well as the BLS scheme [20] to generate certificates for the users. Such approach provides an implicit certification by the fact that the signing key is composed of the certificate and the secret key generated by user. Moreover, it solves the inherent key escrow problem of IBC. Although the CA knows the certificate of user, it yet cannot forge the signature since it does not know the user's secret key.

Certificate-based signature (CBS) [22, 23], a fundamental branch of CBC, can provide high level of trust along with the shorter length and more efficient verification. It is especially useful in those environments where the computation power is very limited, or communication bandwidth is very expensive. Mobile networks are a good example of such environments. As the verification is efficient, the impact of verification on energy consumption is very low. In addition, the elimination of certificates from the verification process reduces the amount of information that needs to be transmitted thus reducing the communication overhead. In the case of wireless mobile networks, communication bandwidth is a very expensive resource. The formal CBS scheme that we adopt in our work is specified as following algorithms.

CBS_Setup.

The CA takes as input a security parameter $1^{k1}$ and returns $SK_C$ (the CA's master secret) as well as the public parameters params that include the CA's public key $PK_C$.

CBS_GenCert.

The user takes as input a security parameter $1^{k2}$ and returns a private key $SK_U$ and a public key $PK_U$ (the user's private and public key pair). The CA uses $SK_C$, params, i, $PK_C$ and $PK_U$ at the start of time period i to create $Cert_i'$ which is sent to the user. Then the user computes $Cert_i$ using params, i, $Cert_i'$ and (optionally) $Cert_{i-1}$ at the start of time period i.

CBS_Sign.

To sign a message *m* with params, $Cert_i$, $SK_U$ in time period i. The signer computes the temporary signing key SK = *f* ($SK_U$, $Cert_i$) where *f* is a public algorithm, and outputs a signature σ.

CBS_Verify.

To verify σ, the verifier takes σ, m, i, $PK_C$, $PK_U$ as input and outputs a binary value 0 (invalid) or 1 (valid).

## 3. Network architecture and novel signature scheme

In this section we present the details of our approach. We first introduce our hierarchical security architecture for HMIPv6 networks which concatenates PKI and CBC. Then we propose a novel PKI-CBS-based signature scheme (PCS) under the proposed architecture in order to achieve mutual authentication for HMIPv6 networks.

### 3.1. Concatenated security architecture

As shown in Fig.2, our proposed architecture has three tiers. The top tier comprises the CAs and the repositories forming the trust infrastructure. The CAs are the trust authorities for the domain managers, while the repository stores the PKCs of CAs. Each CA can set up trust relationships with other CAs through cross-certificates as long as the underlying domains have roaming agreements. For example, consider Fig.2 and assume that the home agent (denoted by HA in Fig.2) has a roaming agreement with MAP1.Then CA1 can issue a PKC for CA2 and register it into the repository, and vice versa. Domain managers reside in the second tier. From the CA point of view, domain managers are PKI-aware users with PKCs issued by CAs. Nonetheless, from the domain perspective, domain managers are trust anchors of end-users (that is, mobile nodes and access routers) inside domains which form the bottom tier of the architecture. We assume that all nodes within each domain support CBC operations. This implies that the domain managers also have identity-based key pairs and are able to issue certificates to end-users based on CBC. Moreover, as the signing and verifying operations in CBS depend on the same set of public parameters, the public parameters derived from different domains must be certified, which in our scheme is achieved by embedding the parameters into the domain manager's PKC.

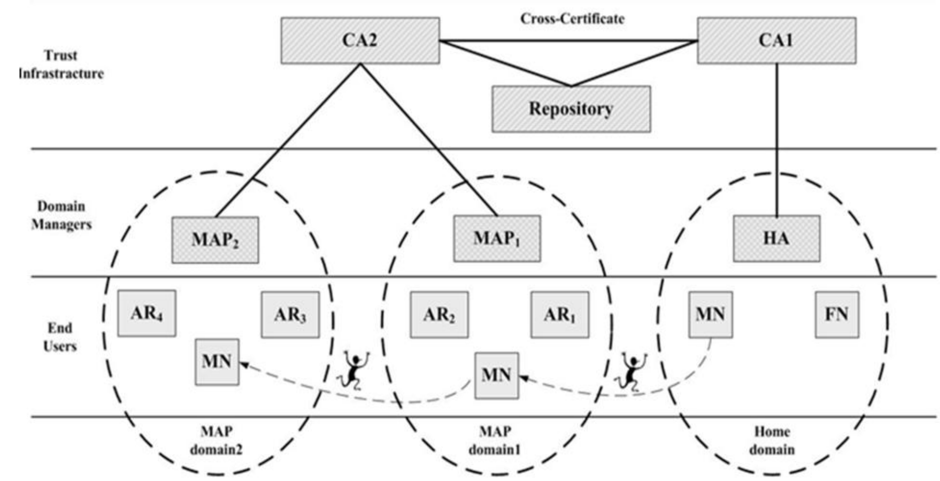



**Fig 2** Concatenated security architecture

In short, the cross-domain trust of our architecture relies on cross-certificate between CAs at the trust infrastructure level which makes the architecture appropriate for large scale deployment, whereas the trust relationship inside each domain is achieved through CBC that is simple from the management point of view and suitable for bandwidth-limited wireless networks as well as computational constrained mobile nodes. We also assume that domain managers and their own end-users pre-share a symmetric key to build secure channels for subsequent communications. For the purpose of clarity, the notations and acronyms, used in the rest of the presentation, are listed in Tab.1.

**Tab.1.** Notations and acronyms

| Notations | Meaning |
|---|---|
| DM | Domain manager, includes home agent (HA) and MAP |
| Domain_DM | Administrative domain managed by DM |
| User | End-user within Domain_DM, includes mobile node (MN) and access router (AR) |
| PKC_A | X.509 format PKC of entity A |
| Cert_User | CBC-based certificate of user issued by DM |
| $ID_A$ | Identity information of entity A |

| | |
|---|---|
| $PK_A$ | Public key of entity A |
| $SK_A$ | Private key of entity A |
| $PARA_{DM}$ | Public parameters of Domain_DM |
| $User_{INFO}$ | Related information of user, includes $ID_{User}$, $PK_{User}$ and PKC_DM |
| $P_{User}$ | Hash value of $User_{INFO}$ |
| $\{M\}_{\alpha\_Sign\_Signer}$ | Signer signs message M with algorithm α |
| $\{\sigma\}_{\beta\_Verify\_Verifier}$ | Verifier verifies signature σ with algorithm β |
| $K_{A\text{-}B}$ | Shared key between entity A and entity B |
| $SEK_{A\text{-}B}$ | Session key between entity A and entity B |
| TS | Timestamp |
| TP | Time period |
| A→B:[M] | Entity A sends message M to entity B through unsecure channel |
| A⇨B:[M] | Entity A sends message M to entity B through secure channel |
| M1,M2 | Concatenation of two messages, M1 and M2 |

### 3.2. PKI-CBS-based signature scheme (PCS)

Roughly speaking, PCS is constructed by merging cross-certificates and CBS. The scheme consists of the following algorithms.

PCS_Setup.

DM initializes the following system parameters:

Additive group $G_1$ and multiplicative group $G_2$ of the prime order q, as well as a bilinear pairing $\hat{e}: G_1 \times G_1 \to G_2$;

Arbitrary $P \in G_1$, $SK_{DM} \in Z_q^*$ and $PK_{DM} = SK_{DM} \cdot P$;

Hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \times G_1 \to Z_q^*$, $H_3 : \{0,1\}^* \to Z_q^*$, $H_4 : G_2 \to \{0,1\}^*$;

Time period $TP_i$.

DM publishes $PK_{DM}$ and $PARA_{DM} = (G_1, G_2, \hat{e}, P, TP_i, H_1, H_2, H_3, H_4)$, where $H_3$, $H_4$ are used for the mutual authentication protocols (described in the following sections).

PCS_Cross-certificate.

CA first generates a public and private key pair ($PK_{CA}$ and $SK_{CA}$). If two DMs ($DM_i$ and $DM_j$) have roaming agreement, their CAs ($CA_i$ and $CA_j$) issue a PKC to each other as below:

*$CA_i$ exchanges PKC with $CA_j$*;

*$CA_i$ issues PKC _$CA_j$ which includes $PK_{CAj}$ and registers it to repository*;

*$CA_j$ issues PKC _$CA_i$ which includes $PK_{CAi}$ and registers it to repository*.

**PCS_PKI-cert.**

CA checks DM's identity ($ID_{DM}$) and issues PKC_DM to DM which includes $ID_{DM}$, $PK_{DM}$ and $PARA_{DM}$.

PCS_CBC-cert.

User chooses the secret key $SK_{User}$ and computes $PK_{User}=SK_{User} \cdot P$. DM checks User's identity ($ID_{User}$) and issues $User_{INFO}$= ($ID_{User}$, $PK_{User}$, PKC_DM) as well as Cert_User= $SK_{DM} \cdot P_{User}$ to User, where $P_{User} = H_1(TP_i, User_{INFO})$. Afterwards, User computes its signing key, $SK_{sign\_User}$= Cert_User + $SK_{User} \cdot P_{User}$.

To deal with the certificate revocation problem, the time period $TP_i$ is added into Cert_User to avoid the use of the current certification status.

PCS_Sign.

To sign message *m* with *Sign* algorithm, signer A in Domain_DM$_i$ selects a random *r* and outputs a signature σ = (U, V), where U= $r \cdot P_A$, h= $H_2$ (m, U), V=$(r+h) \cdot SK_{sign\_A}$. Signer A then sends σ, $A_{INFO}$ to verifier.

PCS_Verify.

Verifier B in Domain_DM$_j$ uses following algorithm to verify σ.

If B is DM then
  B requests $PKC\_CA_i$ from repository;
  B verifies $PKC\_CA_i$ with $PK_{CAj}$;
  B verifies $PKC\_DM_i$ in $A_{INFO}$ with $PK_{CAi}$ in $PKC\_CA_i$;
If B is User then
  B asks its DM to verify $PKC\_DM_i$ in $A_{INFO}$;
  B picks $PK_{DMi}$ and $PARA_{DMi}$ from $PKC\_DM_i$;
With parameters in $PARA_{DMi}$, B checks whether $\hat{e}(PK_{DMi} + PK_A, U + h \cdot P_A) == \hat{e}(P, V)$, where $h = H_2(m, U)$, if the equation holds, outputs 'Valid', otherwise outputs 'Invalid'.

## 4. The proposed scheme

We now present a key establishment and mutual authentication scheme based on the concatenated architecture and PCS. We further integrate mutual authentication into the mobility management procedure to improve authentication and handover efficiency.

We consider the scenario in Fig.2 as roaming scenario. Before MN starts roaming, each entity should run *PCS.Setup* to configure the relative parameters. Afterwards, MN leaves the home domain and accesses the AR1 of MAP domain1, then handovers from AR1 to AR2 within the same MAP domain. Finally, MN roams to MAP domain2.

### 4.1. Key establishment scheme (KES)

In order to secure the communications during authentication procedure, a key establishment scheme (KES) is necessary to build security channel between

MN and MAP or AR. As such, we propose a novel KES, in this section, which can be integrated into the later proposed mutual authentication protocol.

To establish a common shared key, two messages need to be exchanged between MN and MAP as shown in Fig.3. MN first sends a message to MAP that includes $MN_{INFO}$ (message K1 in Fig.3). Upon receiving this message, MAP picks $PARA_{HA}$ from PKC_HA in $MN_{INFO}$ and selects a time period $TP_j$. Afterwards, MAP computes $P'_{MN}=H_1(TP_j, MN_{INFO})$, as well as $PK'_{MAP}=SK_{MAP}\cdot P$ using the parameters in $PARA_{HA}$ and sends $TP_j$, $PK'_{MAP}$, $MAP_{INFO}$ back to MN (message K2 in Fig.3). Upon receiving this message, MN picks $PARA_{MAP}$ from PKC_MAP in $MAP_{INFO}$ and checks whether $\hat{e}(PK'_{MAP}, P') == \hat{e}(PK_{MAP}, P)$ holds to verify the validity of $PK'_{MAP}$. If the validity verification is successful, MN computes $P'_{MN}=H_1(TP_j, MN_{INFO})$.

(K1) $MN \rightarrow MAP$: [$MN_{INFO}$],
(K2) $MAP \rightarrow MN$: [$TP_j$, $PK'_{MAP}$, $MAP_{INFO}$]

**Fig.3.** Key establishment scheme

With all these parameters, MN computes $K_{MN\text{-}MAP} = \hat{e}(SK_{MN}\cdot P'_{MN}, PK'_{MAP})$, MAP computes $K_{MAP\text{-}MN} = \hat{e}(SK_{MAP}\cdot P'_{MN}, PK_{MN})$. It can be easily proved that $K_{MN\text{-}MAP} = \hat{e}(SK_{MN}\cdot P'_{MN}, PK'_{MAP}) = \hat{e}(SK_{MN}\cdot P'_{MN}, SK_{MAP}\cdot P) = \hat{e}(SK_{MN}\cdot P, SK_{MAP}\cdot P'_{MN}) = \hat{e}(SK_{MAP}\cdot P'_{MN}, PK_{MN}) = K_{MAP\text{-}MN}$.

It should be noted that, for the security and convenience in the exchange of the time period $TP_j$, DM can use the time period $TP_i$ chosen during *PCS.Setup*, instead of $TP_j$.

## 4.2. Mutual authentication protocol with KES (PCS-K-HMIPv6)

We incorporate the previous KES into our proposed mutual authentication protocol (PCS-K-HMIPv6), and presents the details of inter-domain as well as intra-domain authentication procedures in the following subsections.

### 4.2.1. Inter-domain authentication of PCS-K-HMIPv6

In our roaming scenario, inter-domain authentication occurs when MN first enters MAP domain1 and accesses AR1. Fig.4 shows the messages that are exchanged as part of the authentication procedure of PCS-K-HMIPv6.

(C1) AR1→MN: [RA, $AR1_{INFO}$]
(C2) MN→AR1: [LBU, RBU, CVR(PKC_MAP), $MN_{INFO}$, $TS_1$, $\sigma_1$, $\sigma_2$ ]
(C3) AR1⇨MAP: [LBU, CVR(PKC_HA), RBU, CVR(PKC_MAP), $MN_{INFO}$, $TS_1$, $\sigma_2$]
(C4a) MAP→ Repository: [CVR(PKC_CA1)]
(C4b) MAP →HA: [RBU, CVR(PKC_MAP), $TS_1$, $\sigma_2$]
(C5) HA→ Repository: [CVR(PKC_CA2)]
(C6) Repository→ HA: [CVA(PKC_CA2)]
(C7a) HA→MAP: [RBA, CVA(PKC_MAP), $TS_2$, $\sigma_3$]
(C7b) Repository→ MAP: [CVA(PKC_CA1)]
(C8) MAP ⇨ AR1: [LBA, CVA(PKC_HA), RBA, CVA(PKC_MAP), $TS_2$, $\sigma_3$, $TP_j$,
$PK'_{MAP}$, $SEK_{MN\text{-}MAP}$].
(C9) AR1→MN: [LBA, RBA, CVA(PKC_MAP), $TS_2$, $\sigma_3$, $TS_3$, $\sigma_4$, $TP_j$, PK□'$_{MAP}$]

**Fig.4.** Inter-domain authentication of PCS-K-HMIPv6

AR1 periodically broadcasts a message (message C1 in Fig.4) to its coverage area through router advertisement (RA) which carries $AR1_{INFO}$. Upon receiving this message, MN starts the mobility registration procedure. In order to protect registration signaling, MN signs LBU with *PCS.Sign* and outputs $\sigma_1$={LBU, $TS_1$}$_{PCS\_Sign\_MN}$, where $TS_1$ is the current timestamp. MN also signs RBU by using HMAC [34] and outputs:

$\sigma_2$={RBU,CVR(PKC_MAP),$TS_1$}$_{HMAC\_Sign\_MN}$

=$H_3$(RBU,CVR(PKC_MAP),$TS_1$,$K_{MN\text{-}HA}$)

where CVR (certificate verification request) is a new message introduced by PCS-K-HMIPv6, to request a valid PKC from DM. Without the ability of verifying PKC_MAP in $AR1_{INFO}$, MN should send the CVR to its DM (HA) to request a valid PKC_MAP. MN combines registration signaling (together with signature and timestamp), CVR and $MN_{INFO}$ into one message (message C2 in Fig.4) and sends it to AR1. AR1 checks the freshness of $TS_1$ to protect against replay attacks and forwards the message (message C3 in Fig.4) to MAP through a secure channel. As AR1 is not DM, this message also includes a CVR to MAP to verify the PKC_HA. After receiving this message, MAP requests the PKC_CA1 (message C4a in Fig.4) from the repository in order to verify PKC_HA. In the meantime, MAP forwards RBU, CVR to HA (message C4b in Fig.4). Upon receiving this message, HA executes the following steps:

(1) It verifies $\sigma_2$ with HMAC, {$\sigma_2$}$_{HMAC\_Verify\_HA}$. If the signature is verified, HA updates its binding cache.

(2) It requests PKC_CA2 (message C5 in Fig.4) from the repository the public key ($PK_{CA2}$) in order to verify PKC_MAP. The repository then returns HA PKC_CA2 (message C6 in Fig.4) through a certificate verification acknowledgement message (CVA) which is the response to the CVR.

(3) It verifies PKC_CA2 with $PK_{CA1}$, and then verifies PKC_MAP with $PK_{CA2}$.

(4) It returns RBA, CVA (message C7a in Fig.4) to MN together with the HMAC signature, where $\sigma_3$= $H_3$ (RBA, CVA, $TS_2$, $K_{MN\text{-}HA}$).

As a reply to message C4a, the repository sends PKC_CA1 to MAP (message C7b in Fig.4). In order to establish a common key between MN and MAP, upon receiving message C7a from HA, MAP executes the following steps:

(1) It verifies PKC_CA1 with $PK_{CA2}$, and then verifies PKC_HA with $PK_{CA1}$.

(2) It executes protocol KES using $PARA_{HA}$ in PKC_HA in order to generate $K_{MAP\text{-}MN}$.

(3) It computes the session key $SEK_{MN\text{-}MAP}$= $H_3(TS_1, H_4(K_{MAP\text{-}MN}))$.

(4) It records the relationship of $TP_j$, $MN_{INFO}$ and $K_{MAP\text{-}MN}$.

(5) It inserts LBA, CVA, $TP_j$, $PK'_{MAP}$ and $SEK_{MN\text{-}MAP}$ into a message (message C8 in Fig.4), and then sends this message to AR1 through a secure channel.

Upon receiving such message, AR1 executes the following steps:

(1) It signs LBA with HMAC instead of *PCS.Sign* using $SEK_{MN\text{-}MAP}$ in (C8) and outputs $\sigma_4$= $H_3$ (LBA, $TS_3$, $SEK_{MN\text{-}MAP}$).

(2) It sends a message (message C9 in Fig.4) to MN that includes $\sigma_4$ and other information from message C8.

(3) It uses a valid $PK_{HA}$ and $PARA_{HA}$ in PKC_HA to verify $\sigma_1$ with *PCS.Verify,* $\{\sigma_1\}_{PCS\_Verify\_AR1}$.

After receiving the message from AR1, MN first checks the freshness of $TS_3$. It then executes KES using $TP_j$, $PK'_{MAP}$ in (C9) to generate $K_{MN\text{-}MAP}$. MN computes the session key $SEK_{MN\text{-}MAP}$=$H_3(TS_1, H_4(K_{MN\text{-}MAP}))$ and uses this key to verify $\sigma_4$ with HMAC, $\{\sigma_4\}_{HMAC\_Verify\_MN}$. If the verification is successful, the mutual authentication between MN and AR1 is completed.

It should be noted that the implementation of timestamp is a critical factor. We suggest using 'Mobility Message Replay Protection Option' in [25] to carry timestamp and utilize NTP [26] for time synchronization among the participants.

### 4.2.2. Intra-domain authentication of PCS-K-HMIPv6

Fig.5 shows the messages that are exchanged as part of the intra-domain authentication process when MN moves from AR1 to AR2 within the same MAP domain.

When accessing AR2, MN receives a message (message W1 in Fig.5) from AR2 which carries $AR2_{INFO}$. For the sake of intra-domain handover, only the LBU should be sent to MAP according to HMIPv6. MN signs the LBU with *PCS.Sign* and outputs $\sigma_5$={LBU, $TS_4$} $_{PCS\_Sign\_MN}$. MN sends a message (message W2 in Fig.5) to AR2 that includes the LBU, the current timestamp ($TS_4$), $MN_{INFO}$, $\sigma_5$. AR2 first checks the freshness of $TS_4$ to protect from replay attacks; then it sends a CVR to MAP to request valid PKC_HA (message W3 in Fig.5). To achieve an efficient KES with MN, upon receiving message W3 from AR2, MAP checks the freshness of time period $TP_j$ which was recorded during inter-domain authentication. If the time period is fresh, MAP computes the new session key $SEK'_{MN\text{-}MAP} = H_3(TS_4, H_4(K_{MAP\text{-}MN}))$. Otherwise, MAP must re-execute a KES protocol with MN. MAP then sends a message to AR2 together with $SEK'_{MN\text{-}MAP}$ through a secure channel (message W4 in Fig.5). AR2 signs LBA with HMAC using $SEK'_{MN\text{-}MAP}$ and outputs $\sigma_6 = H_3(LBA, TS_5, SEK'_{MN\text{-}MAP})$. AR2 sends a message (message W5 in Fig.5) to MN that includes LBA, $\sigma_6$, and the current timestamp ($TS_5$). After receiving this message, MN first checks the freshness of $TS_5$ and also computes $SEK'_{MN\text{-}MAP} = H_3(TS_4, H_4(K_{MAP\text{-}MN}))$. Then MN verifies $\sigma_6$ with HMAC using $SEK'_{MN\text{-}MAP}$, $\{\sigma_6\}_{HMAC\_Verify\_MN}$. If the verification is successful, the mutual authentication between MN and AR2 is completed.

(W1 ) AR2→MN: [RA, $AR2_{INFO}$]
(W2 ) MN→AR2: [LBU, $TS_4$, $MN_{INFO}$, $\sigma_5$]
(W3 ) AR2 ⇨ MAP: [LBU, CVR(PKC_HA), $MN_{INFO}$]
(W4) MAP ⇨ AR2: [LBA, CVA(PKC_HA), $SEK'_{MN\text{-}MAP}$]
(W5) AR2→MN: [LBA, $TS_5$, $\sigma_6$]

**Fig.5.** Intra-domain authentication of PCS-K-HMIPv6

When MN roams to MAP domain2, the same operations are executed as the ones executed in the inter-domain authentication. It should be noted that, after the mutual authentication, MN and MAP/AR can set up secure channel for their subsequent communications using the shared SEK generated as part of the PCS-K-HMIPv6 protocol.

### 4.3. Compatibility of the scheme

Recently another novel local mobility management protocol, proxy mobile IPv6 (PMIPv6 [36]), is proposed by IETF and receives comprehensive attentions in research community. PMIPv6 is intended for providing network-based mobility management support to a MN without requiring MN's participation in any IP mobility-related signaling. Two functional entities are introduced in PMIPv6: local mobility anchor (LMA) and mobile access gateway (MAG). LMA is the home agent for the MN in the home network. MAG, located at the visiting network, is responsible for managing the mobility-related signaling by the deputy of the MN that is attached to its managed ARs. In spite of the increasing focus on the efficiency and deployment issues of PMIPv6, few security concerns have been conducted [37].

Fortunately, our proposed concatenated security architecture and mutual authentication protocol can be well adapted to PMIPv6 to address the security problem. Similiar as HA and MAP, LMA and MAG may also act as domain managers in our security architecture. They are in charge of issuing certificates to the managed MNs and ARs respectively through *PCS*. MN and accessing AR are thus able to generate the correspoding signing keys and further perform the mutual authentication as well as key establishment operations according to the scheme described in section 4.1 and 4.2. However, some revisions are still necessary for the compatibility to PMIPv6 since both topology and signalings are quite different between PMIPv6 and HMIPv6, which will be left for the further research work.

# 5. Performance analysis

We evaluate the authenticated handover latency of MN for the following protocols: PKI-HMIPv6 [6], 2-IBS-HMIPv6 [10], and PCS-K-HMIPv6. The authenticated handover latency refers to the interval from the time when MN enters a new MAP domain or different ARs in the same MAP domain to the time when the mutual authentication and mobility registration are completed.

## 5.1. Analytical model

From the definition of authenticated handover latency ($T_{ah}$) we can see that the latency is incurred during the mutual authentication and mobility management procedure. $T_{ah}$ consists of transport latency ($T_t$), authentication cost ($T_c$), and node processing time ($T_p$).

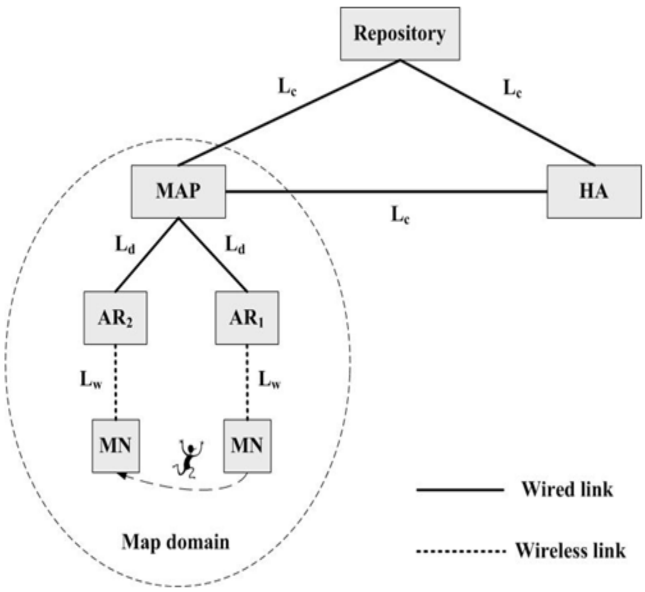



**Fig.6.** System model for transport latency analysis

$$T_{ah}=T_t+ T_c +T_p \quad (1)$$

We adopt the system model shown in Fig.6 to analyze $T_t$ first. The transport latency can be categorized into three types: wireless link latency ($L_w$), intra-domain wired link latency ($L_d$), and inter-domain wired link latency ($L_c$). In most cases we have that $L_c > L_w > L_d$. $L_w$ and $L_d$ are fixed when the link type is determined. $L_c$ is a variant with respect to the changeable distance between two administrative domains. We can treat $L_c$ as multi-hop of $L_d$:

$$L_c=h\times L_d+(h-1)\times T_p \quad (2)$$

where $h$ is the number of hops between two administrative domains, and $T_p$ is the processing time of intermediate routers which is also fixed as long as the node type is determined. Consequently, we have that:

$$T_t = L_w+(h+1)\times L_d+(h-1)\times T_p \quad (3)$$

$T_c$ is another variable which is primarily determined by the adopted authentication algorithm. Without loss of generality, we assume the classic RSA signature [27] is adopted for the verification of PKCs in PKI-HMIPv6 and PCS-K-HMIPv6. Compared with that, the computational cost of identity-based or certificate-based signature schemes in 2-IBS-HMIPv6 and PCS-K-HMIPv6 is higher. The involved operations consist of scale multiplication (SM), point addition (PA), bilinear pairing (BP), multiplication in group (MG), map to point function (MTP), and hash function (Hash).

We report the cost analysis of these operations in Tab.2. Let $t_x$ denotes the computational cost of operation x. According to [28,29], $t_{PA}$, $t_{MG}$, $t_{Hash}$ and $t_{RSAv}$ are negligible compared with $t_{BP}$ ,$t_{MTP}$, $t_{SM}$ and $t_{RSAs}$. Note that $t_{RSAs}$ and $t_{RSAv}$ denote the computational cost of RSA sign and RSA verification, respectively.

**Tab.2.** Computational cost of the operations in the different schemes

| | SM | PA | BP | MG | MTP | Hash |
|---|---|---|---|---|---|---|
| $2\text{-}IBS_{1\text{-}s}$ | 1 | 1 | N/A | N/A | N/A | 1 |
| $2\text{-}IBS_{1\text{-}v}$ | N/A | N/A | 2 | 1 | N/A | 1 |
| $2\text{-}IBS_{2\text{-}s}$ | 1 | 1 | N/A | N/A | N/A | 1 |
| $2\text{-}IBS_{2\text{-}v}$ | N/A | N/A | 3 | 2 | N/A | 1 |
| $PCS_s$ | 2 | N/A | N/A | N/A | N/A | 1 |
| $PCS_v$ | 1 | 2 | 2 | N/A | N/A | 1 |
| KA_MAP | 2 | N/A | 1 | N/A | 1 | N/A |
| KA_MN | 1 | N/A | 2 | N/A | 1 | N/A |

Note that:

$2\text{-}IBS_{1\text{-}s/v}$: It denotes the signature and verification algorithm used by first tier PKG in 2-IBS-HMIPv6;

$2\text{-}IBS_{2\text{-}s/v}$: It denotes the signature and verification algorithm used by second tier users in 2-IBS-HMIPv6;

$PCS_{s/v}$: It denotes the signature and verification algorithm in PCS;

KA_MAP: It denotes the key agreement operations at the MAP side;

KA_MN: It denotes the key agreement operations at the MN side.

From expressions (1), (2), (3) we can conclude that:

$$T_{ah}=aL_w+bL_d+cL_c+T_p+T_c=aL_w+(b+c\times h)L_d+(c\times h-c+1)T_p+T_c \quad (4)$$

where a, b, c are the number of messages in each type of link. We define three types of authenticated handover latency: inter-domain authenticated handover latency, intra-domain authenticated handover latency and total authenticated handover latency. Each of these is evaluated in the following sections.

### 5.2. Inter-domain authenticated handover latency analysis

The inter-domain authenticated handover latency ($T_{ah\_IRD}$) refers to the interval from the time MN receives the first RA in the access MAP domain to the end time of the remote mobility registration.

In PKI-HMIPv6, mutual authentication and mobility registration are executed separately. Both remote and local registration will occur after the successful mutual authentication, and the negotiation of security association between MN and AR is mandated to set up IPSec channel for mobility registration messages. $T_{ah\_IRD}$ of PKI-HMIPv6 can be evaluated as follows:

$$\begin{aligned} T_{ah\_IRD}\left(PKI-HMIPv6\right) &= 5L_w+4L_d+4L_c+14T_p+t_{RSAs}+3t_{RSAv} \\ &= 5L_w+\left(4h+4\right)L_d+\left(4h+10\right)T_p+t_{RSAs} \end{aligned} \quad (5)$$

In 2-IBS-HMIPv6, mutual authentication is integrated into the mobility registration procedure. A round trip message delivery between MN and HA is thus required to achieve both authentication and registration. Therefore we can evaluate $T_{ah\_IRD}$ of 2-IBS-HMIPv6 as follows:

$$\begin{aligned} T_{ah\_IRD}\left(2-IBS-HMIPv6\right) &= 2L_w+2L_d+2L_c+7T_p+t_{2-IBS1-v}+2t_{2-IBS2-s}+2t_{2-IBS2-v} \\ &= 2L_w+2t_{SM}+\left(2h+2\right)L_d+(2h+5)T_p+8t_{BP} \end{aligned} \quad (6)$$

PCS-K-HMIPv6 also incorporates mutual authentication with mobility registration procedure and there are additional queries of PKC between the domain managers (HA, MAP) and the repository. In addition, PCS-K-HMIPv6 has a key establishment between MN and MAP. We can evaluate $T_{ah\_IRD}$ of PCS-K-HMIPv6 as below:

$$\begin{aligned} & T_{ah\_IRD}\left(PCS-K-HMIPv6\right) = 2L_w+2L_d+4L_c+9T_p+t_{PCSs}+t_{PCSv}+ \\ & t_{KA\_MAP}+t_{KA\_MN} = 2L_w+\left(4h+2\right)L_d+\left(4h+5\right)T_p+5t_{BP}+6t_{SM}+2t_{MTP} \end{aligned} \quad (7)$$

### 5.3. Intra-domain authenticated handover latency analysis

The intra-domain authenticated handover latency ($T_{ah\_IAD}$) refers to the interval between the time of the MN handover to another AR within the same MAP domain and the end time of the local mobility registration.

In terms of local handover, only the local mobility registration should be undertaken and no PKC verification and key establishment are needed since these have been executed during the inter-domain handover. Authenticated handover latencies of the schemes are given by expressions (8), (9), and(10) .

$$T_{ah\_IAD}\left(PKI-HMIPv6\right)=5L_w+4L_d+10T_p+t_{RSAs} \tag{8}$$

$$\begin{aligned}T_{ah\_IAD}\left(2-IBS-HMIPv6\right)&=2L_w+2L_d+5T_p+2t_{2-IBS2-s}+2t_{2-IBS2-v}\\&=2L_w+2L_d+5T_p+6t_{BP}+2t_{SM}\end{aligned} \tag{9}$$

$$\begin{aligned}T_{ah\_IAD}\left(PCS-K-HMIPv6\right)&=2L_w+2L_d+5T_p+t_{PCSs}+t_{PCSv}\\&=2L_w+2L_d+5T_p+2t_{BP}+3t_{SM}\end{aligned} \tag{10}$$

## 5.4. Total authenticated handover latency analysis

HMIPv6 is designed for a scenario where MN handovers frequently within a domain far away from its home domain. Accordingly the total authenticated handover latency ($T_{ah\_TOT}$), which is the sum of $T_{ah\_IRD}$ and all $T_{ah\_IAD}$, must be taken into consideration. This sum is computed as:

$$T_{ah\_TOT}= T_{ah\_IRD} +\rho\ T_{ah\_IAD} \tag{11}$$

where ρ is the handover frequency of MN within the MAP domain.

Based on expressions (5)-(11), we have:

$$\begin{aligned}T_{ah\_TOT}\left(PKI-HMIPv6\right)&=(5\rho+5)L_w+(4\rho+4h+4)L_d\\&+(10\rho+4h+10)T_p+(\rho+1)t_{RSAs}\end{aligned} \tag{12}$$

$$\begin{aligned}T_{ah\_TOT}\left(2-IBS-HMIPv6\right)&=(2\rho+2)L_w+(2\rho+2h+2)L_d\\&+(5\rho+2h+5)T_p+(6\rho+8)t_{BP}+(2\rho+2)t_{SM}\end{aligned} \tag{13}$$

$$\begin{aligned}T_{ah\_TOT}\left(PCS-K-HMIPv6\right)&=(2\rho+2)L_w+(2\rho+4h+2)L_d\\&+(5\rho+4h+5)T_p+(2\rho+5)t_{BP}+(3\rho+6)t_{SM}+2t_{MTP}\end{aligned} \tag{14}$$

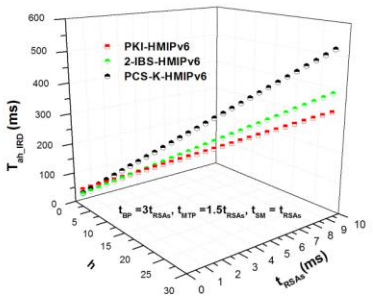
## 5.5. Numerical results and discussions

This section presents the performance differences of the above schemes through numerical results and discussions.

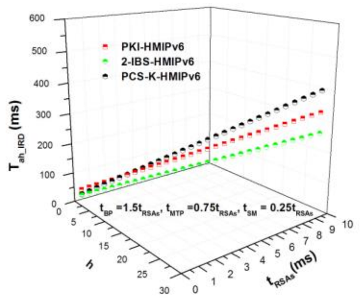
Based on the comprehensive analysis of the experimental results in [29-33], $t_{RSAv}$ can be omitted as it is negligible compared with $t_{RSAs}$. We also get following conclusions:

$$t_{BP} =1.5\sim3\ t_{RSAs},\ t_{MTP} = 0.75\sim1.5\ t_{RSAs},\ t_{SM} = 0.25\sim1\ t_{RSAs} \tag{15}$$

In order to analyze the performance differences, we select two groups of performance parameters: { $t_{BP} =3\ t_{RSAs}$, $t_{MTP} = 1.5\ t_{RSAs}$, $t_{SM} = 1\ t_{RSAs}$ } and { $t_{BP} =1.5t_{RSAs}$, $t_{MTP} = 0.75t_{RSAs}$, $t_{SM} = 0.25\ t_{RSAs}$ } for our analysis, where the two groups indicate the worst and best performance of the authentication operations respectively under the constrains of expression (15). Moreover, we set $L_w$=4ms， $L_d$=2ms， $T_p$=0.5ms, which we called fixed parameters according to [10].




(a) $T_{ah\_IRD}$ vs. h and $t_{RSAs}$ with {$t_{BP}$ =3$t_{RSAs}$, $t_{MTP}$ =1.5$t_{RSAs}$, $t_{SM}$ =1 $t_{RSAs}$ }



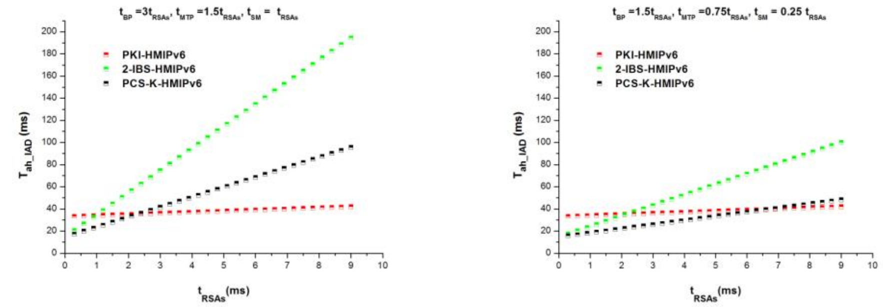

(b) $T_{ah\_IRD}$ vs. h and $t_{RSAs}$ with {$t_{BP}$=1.5$t_{RSAs}$,$t_{MTP}$=0.75$t_{RSAs}$,$t_{SM}$=0.25$t_{RSAs}$ }

**Fig.7.** Numerical results for inter-domain authenticated handover latency

Fig.7-9 plot the results of $T_{ah\_IRD}$, $T_{ah\_IAD}$, and $T_{ah\_TOT}$ for each scheme in light of expressions (5)-(14) based on different groups of performance parameters.

As shown in Fig.7, although the authentication and mobility registration are separated，PKI-HMIPv6 only requires few RSA signatures and verifications to achieve mutual authentication. Therefore $T_{ah\_IRD}$ of PKI-HMIPv6 is lower than the other schemes which involve more expensive authentication operations such as BP, MTP or SM as shown in Fig.7 (a). PCS-K-HMIPv6 has the highest $T_{ah\_IRD}$ since it requires not only authentication operations but also KES operations during inter-domain handovers. However, with the performance enhancement for the authentication operations ($t_{BP}$ $=1.5t_{RSAs}$, $t_{MTP}$ $= 0.75t_{RSAs}$, $t_{SM}$ $= 0.25$ $t_{RSAs}$) (see Fig.7 (b)), the $T_{ah\_IRD}$ of each scheme drops obviously except for PKI-HMIPv6.

As there are no interactions among the MAP domain, the home domain, and the repository during the intra-domain handover, the parameter *h* has no impact. $T_{ah\_IAD}$ mainly depends on the performance of the authentication operations. As a consequence, 2-IBS-HMIPv6 has the highest $T_{ah\_IAD}$ among the three schemes because of more heavy BP computations. Our PCS algorithm mitigates such heavy operations in both signature and verification processes compared with the scheme in [10]. Thus $T_{ah\_IAD}$ of PCS-K-HMIPv6 is lower than 2-IBS-HMIPv6. As shown in Fig.8 (b), with the performance enhancement to the authentication operations ($t_{BP}$ $=1.5t_{RSAs}$, $t_{MTP}$ $= 0.75t_{RSAs}$, $t_{SM}$ $= 0.25$ $t_{RSAs}$), $T_{ah\_IAD}$ of PCS-K-HMIPv6 is even lower than PKI-HMIPv6 when $t_{RSAs}$< 6.6ms.

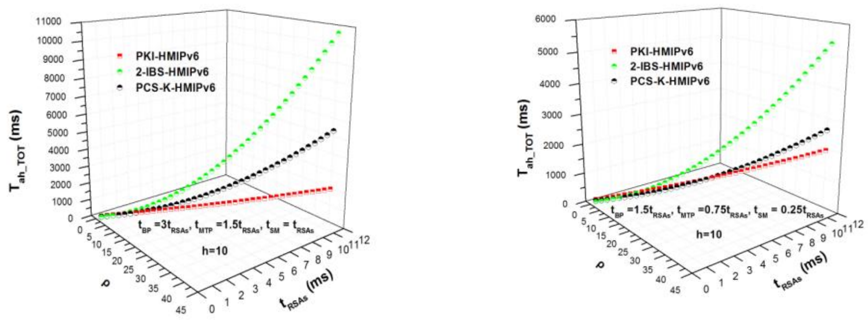



(a) $T_{ah\_IAD}$ vs. $t_{RSAs}$ with
{ $t_{BP} = 3t_{RSAs}$, $t_{MTP} = 1.5\ t_{RSAs}$, $t_{SM} = 1\ t_{RSAs}$ }

(b) $T_{ah\_IRD}$ vs. $t_{RSAs}$ with
{$t_{BP} = 1.5t_{RSAs}$, $t_{MTP}=0.75\ t_{RSAs}$, $t_{SM}=0.25\ t_{RSAs}$ }

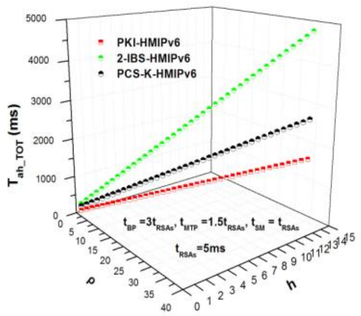
**Fig.8.** Numerical results for intra-domain authenticated handover latency

$T_{ah\_TOT}$ is important as it reflects the overall performance of each scheme. We first set h=10 to observe how $T_{ah\_TOT}$ is affected by ρ and tRSAs. From Fig.9 (a) and (b), we can see that 2-IBS-HMIPv6 performs worst. The reason is that 2-IBS-HMIPv6 requires more expensive authentication operations during both inter-domain and intra-domain handovers. In contrast, although PCS-K-HMIPv6 requires similar authentication and KES operations during inter-domain handover, these operations are eliminated or their costs are greatly mitigated in terms of intra-domain handovers. As shown in Fig.9 (b), $T_{ah\_TOT}$ of PCS-K-HMIPv6 is lower than PKI-HMIPv6 when $t_{RSAs}<6.3$ms. On the other hand, we set $t_{RSAs}$=5ms to see how $T_{ah\_TOT}$ is affected by ρ and h. A similar result is obtained. As shown in Fig.9 (d), $T_{ah\_TOT}$ of PCS-K-HMIPv6 is lower than the other two schemes when ρ>6.

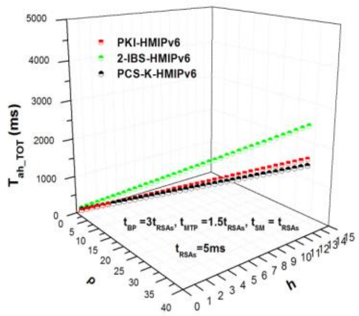



(a) $T_{ah\_TOT}$ vs. ρ and $t_{RSAs}$ with
{ $t_{BP} = 3t_{RSAs}$, $t_{MTP} = 1.5\ t_{RSAs}$, $t_{SM} = 1\ t_{RSAs}$ }

(b) Tah_TOT vs. ρ and tRSAs with
{ tBP =1.5tRSAs, tMTP = 0.75 tRSAs, tSM = 0.25 tRSAs }




(c) $T_{ah\_TOT}$ vs. ρ and h with { $t_{BP}$ =$3_{tRSAs}$, $t_{MTP}$ = 1.5 $t_{RSAs}$, $t_{SM}$ =1 $t_{RSAs}$ }




(d) $T_{ah\_TOT}$ vs. ρ and h with { $t_{BP}$ =$1.5_{tRSAs}$, $t_{MTP}$ =0.75 $t_{RSAs}$, $t_{SM}$ =0.25$t_{RSAs}$ }

**Fig.9.** Numerical results for total authenticated handover latency

To summarize, PCS-K-HMIPv6 has better overall performance when the MN frequently handovers (higher ρ) in remote MAP domains with efficient authentication operations (lower $t_{RSAs}$).

## 6. Security analysis

In this section, we analyze the security of our proposed scheme with respect to key, signature, as well as mobility registration procedure**.**

### 6.1. Key security

There are three types of key in our proposed schemes: long-term shared key or self-generated key, mid-term singing key or agreed key, as well as short-term session key. Security of all these keys is critical.

(1) We assume that the long-term shared keys (e.g. $K_{MN\text{-}HA}$, $K_{AR\text{-}MAP}$) are pre-shared between two parties and the long-term self-generated keys (e.g. $SK_{DM}$, $SK_{User}$) are securely kept by their owners.

(2) User's mid-term signing key is generated as $SK_{sign\_User}$=Cert_User+$SK_{User}$ · $P_{User}$, where Cert_User is openly issued by DM. However, $SK_{User}$ is randomly generated and securely kept by User. Hence no one but User can generate $SK_{sign\_User}$. In addition, our scheme does not have the key escrow problem of IBC since DM cannot create $SK_{sign\_User}$ either. The mid-term agreed key (e.g. $K_{MN\text{-}MAP}$) is produced through the KA scheme. Although some information (*PK'*$_{MAP}$) will be exchanged openly between participants, the adversary has no means for getting $SK_{MN}$ or $SK_{MAP}$, so it is unable to compute $K_{MN\text{-}MAP}$ by $\hat{e}$ ($SK_{MN}$·$P'_{MN}$, $PK'_{MAP}$) or $\hat{e}$ ($SK_{MAP}$·$P'_{MN}$,

$PK_{MN}$). Moreover, in order to avoid malicious modifications, $PK'_{MAP}$ is also verified by MN by checking whether $\hat{e}(PK'_{MAP}, P') == \hat{e}(PK_{MAP}, P)$.

(3) The short-term session key (e.g. $SEK_{MN\text{-}MAP}$) is derived from the agreed key ($K_{MN\text{-}MAP}$) and a valid timestamp by $SEK_{MN\text{-}MAP}=H_3(TS_1, H_4(K_{MN\text{-}MAP}))$. The security of $K_{MN\text{-}MAP}$ ensures that only MN and MAP can create this session key and the timestamp guarantees the freshness of the session key when MN handovers within the MAP domain.

### 6.2. Signature security

Our proposed scheme provides secure mutual authentication between MN and the MAP domain being visited based on PCS. Consider the following impersonation and modification attack scenarios:

(1) The adversary forges a valid signature to impersonate as legitimate User. As *PCS.sign* and *PCS.verify* are based on CBS which has been proved to be secure [23] under the condition of CDHP (computational Diffie-Hellman problem) difficulty in random oracle model [35], the only way by which an adversary can forge the signature is via stealing the signing key of legitimate User. However, as we discussed in section 6.1, User's signing key is secure to against such attack.

(2) The adversary collects a used signature to launch a replay attack. In our mutual authentication scheme, all the signatures are equipped with timestamps. Hence replay attacks can be easily detected by verifying the freshness of timestamps.

(3) The adversary modifies the public parameters so as to compromise the verification procedure. According to *PCS.verify,* the verifier must possess some public parameters, such as $PK_{DM}$ and $PARA_{DM}$, in order to verify a signature. If these parameters are modified by the adversary, the verification will fail. To prevent this attack, we store the public parameters in DM's PKC (PKC_DM). The verifier should first get a valid PKC_DM from the repository, and then pick up the right parameters from PKC_DM to properly verify the signature.

### 6.3. Mobility registration security

Our mutual authentication protocol can provide protection for registration messages. As HMIPv6 has a local registration (LBU/LBA) and a remote registration (RBU/RBA), MN and AR sign LBU and LBA with PCS respectively during the mutual authentication procedure, which guarantees the security of the local registration. In order to protect the remote registration, MN signs the RBU with $K_{MN\text{-}HA}$ using HMAC. After receiving the RBU, HA verifies the signature with the same shared key. In addition, a timestamp is used to prevent replay attacks aiming at the RBU. The same operations are carried out by HA on RBA messages. Hence the whole remote registration is secure.

## 7. Related work

**PKI-based security schemes:** PKI can be used to prevent different kinds of attacks and is suitable for large scale, hierarchical networks. To deploy PKI in HMIPv6 networks, Mizuno et al. [6] proposed a novel PKI-based security architecture. Mutual authentication is supported through IKE and cross-certificates [24] between mobile nodes and the mobile anchor point (MAP). The approach suffers from the problems that IKE has in dynamic mobile networks. In addition the MAP becomes a bottleneck of the system since it should handle authentications for all the accessing mobile nodes. The certificate-based binding update protocol [7] is another PKI-based solution for HMIPv6 networks which provides the functions of secure mobility registration, user authentication, and session key management. However, the goal of this scheme is to protect the communications between the mobile nodes and correspondent nodes[1]. Such scheme does not address the security issues that arise when mobile nodes move to different networks. Although PKI has certain advantages for large scale and explicit authentication, the complicated public key management as well as verification cost of PKC limits the applicability of these PKI-based schemes.

**CGA-based and IBC-based security schemes:** Cryptographically generated addresses (CGA [38]) is a security technique whereby the interface of IP address is generated by hashing a public key and some other parameters associated with node while not allocated by PKI. As such, [39] is a security extension to HMIPv6 based on CGA, which allows the MN to establish a security association with the selected MAP for authentication and other security operations. However CGAs themselves are not certified by any trusted authority, then the association between public key and MN cannot be verified. Therefore, a malicious node is able to generate its own public－private key pair and enter the visiting network as a free rider. In addition, the special construction of CGA renders it cannot be used in other address assignment mechanisms. Besides, several schemes [8-11] introduced IBC into HMIPv6 networks. Zhu et al. [8] developed an IBC-based security architecture to achieve authentication and non-interactive key establishment between access routers and mobile nodes. However such scheme concentrates on the security of wireless mesh networks. Kandikattu and Jacob [9] designed a secure framework with F-HMIPv6 [12] and a novel mobility management scheme. Access authentication and secure route optimization are implemented under the proposed framework by means of

[1] Correspondent nodes, defined in MIPv6 protocol, are the nodes with which a mobile node is communicating. The correspondent nodes may be either mobile or stationary.

IBC. Tian et al. [10] proposed a hierarchical identity-based signature scheme for mutual authentication in HMIPv6 networks. In such scheme, the authentication and mobility management procedures are integrated in order to improve efficiency. Wu et al. [11] further took reputation issues into consideration. However, the special format of IP address suggested in [8] and the low authentication efficiency of [10] and [11] constrain the appeal of these IBC-based solutions. Moreover, IBC is only suitable for small area networks where trust relationships can be easily established.

**PKI and IBC hybrid architectures:** A hybrid scheme combining PKI and identity-based encryption (IBE) was proposed by Chen et al. [14]. They suggested that the combination of the two mechanisms, PKI-based keys for trust authorities and IBC-based keys for users, has many advantages including scalability. Later, Price and Mitchell [15] dwelt into interoperation issues between conventional PKI and IBE infrastructures. Recently, Lee [16] proposed a unified public key infrastructure combining PKI and IBC. A new authority KGCA dedicated to the role of both PKG and CA was proposed for issuing certificates and partial private keys to the users. However, KGCA is critical for performance as it has to perform all the tasks of the PKG and CA. In general, none of these hybrid schemes have been applied to HMIPv6 networks.

## 8. Conclusions

In this paper, we have proposed an approach that incorporates PKI and CBC in a hierarchical security architecture and a novel mutual authentication and key establishment scheme for HMIPv6 networks. The motivation for our work is that none of the hybrid schemes previously proposed satisfy the security requirements of such networks. The proposed concatenated architecture harnesses the merits of both PKI and CBC, while addressing their limitations. Our mutual authentication protocol is based on a designated signature scheme (PCS), which ensures inter-domain trust by cross-certificate and intra-domain trust by CBS. In addition, a key establishment scheme has been defined to set up secure channels after authentication. The authentication scheme is integrated into the mobility management procedure in order to improve performance.

For the future research work, we plan to do the further simulations and implementations on our mutual authentication protocol. Moreover, the proposed hierarchical architecture and hybrid approach are expected to be explored for PMIPv6 security.

**Acknowledgements.** This work was supported in part by the Natural Science Foundation of Liaoning Province under Grant No. 201202069 and the Fundamental Research Funds for the Central Universities under Grant No. N120417003 and Grant No. N120404010.

## References


1. H. Soliman, C. Castelluccia, K. ElMalki, L. Bellier. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. RFC5380. (2008)
2. Johnson D, Perkins C. Mobility Support in IPv6. RFC3775. (2004)
3. Hyun-Sun Kang ,Chang-Seop Park. Authenticated Fast Handover Scheme in the Hierarchical Mobile IPv6. Information Security Applications, LNCS, 211-224. ( 2007)
4. Miyoung Kim, Youngsong Mun, Jaehoon Nah, Seungwon Sohn. An Authentication Scheme using AAA in Hierarchical MIPv6. draft-mun-mip6-authhmip-mobileipv6-00.txt. (2005)
5. C. Adams, S. Farrell, T. Kause, T. Mononen. Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). RFC4210. (2005)
6. S.Mizuno, J.koga, H.Ohwada, K.Suzuki, Y.Takagi. PKI Support in Hierarchical Mobile IPv6. draft-mizuno-mobileip-hmipv6-pki-00.txt. (2003)
7. Feng Bao, Robert Deng, Ying Qiu, Jianying Zhou. Certificate-based Binding Update Protocol (CBU). draft-qiu-mip6-certificated-binding-update-03.txt. (2005)
8. Ramanarayana Kandikattu, Lillykutty Jacob. A Secure IPv6-based Urban Wireless Mesh Network (SUMNv6). Computer Communications, 31(15): 3707-3718. (2008)
9. Xiaoyan Zhu, Yuguang Fang and Yumin Wang. How to Secure Multi-domain Wireless Mesh Networks. Wireless Networks, 16(5): 1215-1222. (2010)
10. Ye Tian, Yujun Zhang, Hanwen Zhang, Zhongcheng Li. Identity-based hierarchical access authentication in mobile IPv6 network. Proceedings of ICC '06, 1953 – 1958. (2006)
11. Zhi Zhang, Guohua Cui. A Secure Hierarchical Identify Authentication Scheme Combining Trust Mechanism in Mobile IPv6 Networks. Journal of Networks, 4(5):343-350. (2009)
12. HeeYoung Jung, Hesham Soliman, Seok Joo Koh, Jae Yong Lee. Fast Handover for Hierarchical MIPv6 (F-HMIPv6). draft-jung-mobopts-fhmipv6-00.txt. (2005)

A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology - Crypto '84, Springer-Verlag LNCS 196, 1984:47-53. (1984)

13. L. Chen, Keith Harrison, Andrew Moss, David Soldera, Nigel P. Smart. Certification of Public Keys within an Identity Based System. Proceedings of Information Security Conference/Information Security Workshop - ISC(ISW), 322-333. (2002)
14. Geraint Price, Chris J. Mitchell. Interoperation Between a Conventional PKI and an ID-Based Infrastructure. Proceedings of European Public Key Infrastructure Workshop - EUROPKI, 73-85. (2005)
15. Byoungcheon Lee. Unified Public Key Infrastructure Supporting Both Certificate-Based and ID-Based Cryptography. Proceedings of Availability, Reliability and Security - IEEEARES, 54-61. (2010)
16. Boneh D, Franklin M. Identity-based encryption from the weil pairing . SIAM Journal of Computing, 32(3): 586-615. (2003)
17. Antoine Joux. The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems Survey. Proceedings of the 5th International Symposium on Algorithmic Number Theory (ANTS-V), LNCS 2369, 11-18. (2002)
18. Joseph H. Silverman. The Arithmetic of Elliptic Curves. Springer, ISBN 0387094938. (2009)
19. Dan Boneh, Ben Lynn, Hovav Shacham. Short Signatures from the Weil Pairing. Proceedings of ASIACRYPT - ASIACRYPT, 514-532. (2001)

20. Craig Gentry. Certificate-Based Encryption and the Certificate Revocation Problem. Proceedings of Theory and Application of Cryptographic Techniques - EUROCRYPT, 272-293. (2003)
21. Bo Gyeong Kang, Je Hong Park, Sang Geun Hahn. A Certificate-Based Signature Scheme. Proceedings of The Cryptographer's Track at RSA Conference - CT-RSA, 99-111. (2004)
22. Wei Wu, Yi Mu, Willy Susilo, Xinyi Huang. Certificate-based Signatures Revisited. Journal of Universal Computer Science, 15(8):1659-1684, (2009).
23. Jim Turnbull. Cross-certification and PKI policy networking. http://hca.nat.gov.tw/download/012.pdf. (2000)

A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury. Authentication Protocol for Mobile IPv6. RFC4285. (2006)

24. D. Mills, U. Delaware, J. Martin, Ed, J. Burbank, W. Kasch. Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC5905. (2010)
25. Jean-françois Misarsky. How (not) to Design RSA Signature Schemes. Proceedings of Public Key Cryptography - PKC, 14-28. (1998)
26. Sandip Vijay, Subhash C. Sharma. Threshold Signature Cryptography Scheme in Wireless Ad-Hoc Computing. Contemporary Computing, 40(7):327-335. (2009)
27. Mohamed Abid, Songbo Song, Hassnaa Moustafa, Hossam Afifi. Integrating identity-based cryptography in IMS service authentication. International Journal of Network Security Its Applications, 1-13. (2010)
28. Paulo S. L. M. Barreto, Ben Lynn, Michael Scott. Efficient Implementation of Pairing-Based Cryptosystems. Journal of Cryptology, 17(4):321-334. (2004)
29. Paulo S. L. M. Barreto, Ben Ly International Cryptology Conference on Advances in Cryptology, LNCS 2442, 354-368. (2002)
30. Elisavet Konstantinou. Efficient cluster-based group key agreement protocols for wireless ad hoc networks. Journal of Network and Computer Applications, 34(1):384-393. (2011)
31. Xiong, X., Wong, D.S., Deng, X. TinyPairing: A Fast and Lightweight Pairing-Based Cryptographic Library for Wireless Sensor Networks. Proceedings of WCNC'2010, 1-6. (2010)
32. H. Krawczyk, M. Bellare, R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC2104. (1997)
33. R. Dutta, R. Barua, P. Sarkar. Pairing-based cryptographic protocols: A survey. Cryptology, ePrint Archive, Report 2004/064. ( 2004)
34. S. Gundavelli, Ed. K. Leung, V. Devarapalli, Wichorus, K. Chowdhury, B. Patil. Proxy Mobile IPv6, RFC5213. (2008)
35. Joong-Hee Lee, Jong-Hyouk Lee, Tai-Myoung Chung. Ticket-based Authentication Mechanism for Proxy Mobile IPv6 Environment, Proceedings of the Third International Conference on Systems and Networks Communications, 304-309. (2008)
36. Aura T. Cryptographically Generated Addresses (CGA), RFC 3972. (2005).
37. Haddad W, Krishnan S, Soliman H. Using cryptographically generated addresses (CGA) to secure HMIPv6 protocol (HMIPv6sec), draft-haddad-mipshop-hmipv6-security-06.( 2006)

**Tianhan Gao** 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 lecturer 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.

**Nan Guo** Nan Guo received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2005, respectively. She joined Northeastern University in September 2005. She has been an associate professor since 2008. She has been a visiting scholar at department of Computer Science, Purdue, from August 2010 to August 2011. She is the author or co-author of more than 20 research publications. Her primary research interests are security and privacy in service computing and digital identity management.

**Kangbin Yim** Kangbin Yim received his B.S., M.S., and Ph.D. from Ajou University, Suwon, Korea in 1992, 1994 and 2001, respectively. He is currently an associate professor in the Department of Information Security Engineering, Soonchunhyang University. He has served as an executive board member of Korea Institute of Information Security and Cryptology, Korean Society for Internet Information and The Institute of Electronics Engineers of Korea. He also has served as a committee chair of the international conferences and workshops and the guest editor of the journals such as JIT, MIS, JISIS and JoWUA. His research interests include vulnerability assessment, code obfuscation, malware analysis, leakage protection, secure hardware, and systems security. Related to these topics, he has worked on more than fifty research projects and published more than a hundred research papers.

*Received: November 14, 2012; Accepted: April 03, 2013*