Efficient ID-Based Registration Protocol Featured with User Anonymity in Mobile IP Networks

Lanjun Dang, Weidong Kou, *Senior Member, IEEE,* Hui Li, Junwei Zhang, Xuefei Cao, Bin Zhao, and Kai Fan

***Abstract*—A secure and efficient ID-based registration protocol with user anonymity is proposed in this paper for IP-based mobile networks. The protocol minimizes the registration delay through a minimal usage of the identity (ID)-based signature scheme that eliminates expensive pairing operations. User anonymity is achieved via a temporary identity (TID) transmitted by a mobile user, instead of its true identity. Additional replay protection from a Foreign Agent (FA) is included in the registration messages to prevent a possible replay attack. A formal correctness proof of the protocol using Protocol Composition Logic (PCL) is presented. Numerical analysis and computer simulation results demonstrate that the proposed protocol outperforms the existing ones in terms of the registration delay, the registration signaling traffic, and the computational load on a Mobile Node (MN) while improving security. For example, the proposed protocol reduces the registration delay up to 49.3 percent approximately, comparing to Yang's protocol.**

***Index Terms*—Mobile IP, registration, ID-based, user anonymity, authentication.**

I. INTRODUCTION

TODAY, there are two major technological forces that drive the communication era: wireless evolutionary systems and the Internet. With the convergence of wireless and IP, both data and voice communications rely increasingly on IP-based technologies. Next-generation mobile networks will be envisioned as all IP-based networks [1], [2]. Mobile IP [3], [4] which was designed to support mobility within the Internet, gives a standard global mobility solution for the IP-based mobile networks [5], [6]. As a form of remote redirection that involves all the mobility entities, the registration part of mobile IP is very crucial and must be guarded against any malicious attacks [7] that might try to take illegitimate advantages from any participating principals. In addition, the user's anonymity in mobile IP environments is also very important. Efficiency issue is of the same significance as the security in mobile IP applications. A mobile IP registration protocol should take into consideration of performance while providing the security for a wide deployment of mobile IP, especially for real-time services. This paper addresses the security issue of registration protocols in mobile IP networks, taking the efficiency into account.

Currently the basic mobile IP protocol [3], [4] makes use of the secret keys with manual key distribution for the authentications of its control messages. This approach is not scalable enough to support the increasing user populations. To improve the scalability, the certificate-based public key infrastructure (CA-PKI) is used for the authentications among mobile node (MN), foreign agent (FA), and home agent (HA) [8]–[10]; however, the proposal in [8]–[10] has a requirement on MN to perform heavy certificate-based public key cryptography operations. Afterwards, other registration protocols [11]–[15] are proposed, which employ only the minimal use of the public key cryptography to avoid this drawback; nevertheless, their registration delay is still somewhat long due to the certificate-based operations that are involved in. Besides these works, there are other schemes [8], [16]–[18] in which various techniques, such as IPSec, GSM, and one-way function, were introduced into mobile IP. To achieve a better performance, recently, research works in [19], [20] employ the identity (ID)-based public key cryptography (ID-PKC) [21], [22] attempting to exclude the time-consuming certificate operations (e.g., CRL retrieval and certificate validation); however, these works are only at a conceptual level and lacking of a detailed algorithm description, and they cannot be used in a real system. Hence, there is a need to introduce a specific ID-based signature scheme into mobile IP registration, which can lead to a secure and efficient implementation.

In this paper, we present a novel ID-based mobile IP registration protocol featured with user anonymity. There are four major contributions in this paper: 1) the paper introduces the ID-based signature (IBS) scheme without pairings [23] for the authentications between FA and HA to minimize the registration delay because it eliminates expensive pairing operations; 2) the proposed protocol achieves user's anonymity by letting MN transmit a temporary identity (TID) [24], [25] instead of its true identity; 3) the proposed protocol employs the nonces from MN, HA, and FA to prevent all possible replay attacks; 4) in order to optimize the proposed protocol, the secret keys $K'_{MN\text{-}HA}$ and $K_{MN\text{-}FA}$ are generated by MN,

Manuscript received July 5, 2006; revised May 27, 2007, December 12, 2007, November 26, 2008, and August 12, 2009; accepted August 29, 2009. The associate editor coordinating the review of this paper and approving it for publication was D. Zeghlache.

L. Dang, J. Zhang, and K. Fan are with the Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University, Xi'an, Shaanxi, 710071 P. R. China (e-mail: ljdang@mail.xidian.edu.cn; jwzhang.xd@gmail.com; kfan@mail.xidian.edu.cn).

W. Kou is with the IBM, Beijing, 100027 China (e-mail: kou_weidong@yahoo.com.cn).

H. Li is with the school of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi, 710071 China (e-mail: xd.lihui@gmail.com).

X. Cao is with the SIM LAB of China Mobile Research Institute, Beijing, China (e-mail: caoxuefei@chinamobile.com).

B. Zhao is with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907-2035 USA (e-mail: binzhao@purdue.edu).

This work is supported by the Programme of Introducing Talents of Discipline to Universities (111 Project) B08038, the National Natural Science Foundation of China (NSFC) Grant 90304008 and 60772136, and the National High Technology Research and Development Program of China (863 Program) 2007AA01Z435.

Digital Object Identifier 10.1109/TWC.2010.02.060445

rather than transmitted to MN over links. We use Protocol Composition Logic (PCL) [26] to prove correctness of the proposed protocol. Numerical analysis and computer simulation results demonstrate that the proposed protocol outperforms the existing ones while providing stronger security.

The rest of this paper is organized as follows: Section II reviews the IBS scheme without pairings. Section III proposes new mobile IP registration protocol based on the IBS scheme without pairings and describes the adversary models in mobile IP, and then presents the protocol goals. A formal proof of correctness using PCL and the security analysis under the adversary models for the proposed protocol are provided in Section IV. Numerical analysis and OPNET implementation are given in Section V. Finally, the paper concludes in Section VI.

II. ID-Based Signature (IBS) Scheme without Pairings Based on ECDLP

The IBS scheme in [23] is more efficient than other existing IBS schemes because it does not need any pairing operations and map-to-point hash operations. The IBS scheme is proved to be secure in terms of existential unforgeability against the chosen message and ID attacks [23]. In the IBS system, G is an order p cyclic subgroup of an elliptic curve E over a finite field $\mathbf{F}$, such that the elliptic curve discrete log problem (ECDLP) is intractable.

Setup: Given security parameter $k \in \mathbb{N}$, the Key Generation Server (KGS) generates system parameters and a master public/secret key pair as follows: (1) choose a generator P of G, pick a random $x \in {}_R\mathbb{Z}_p$ and compute $P_{pub} = xP$; (2) set the master public key $mpk = P_{pub}$ and the master secret key $msk = (x, P_{pub})$; (3) choose two hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p$; (4) publish system parameters $\langle E/\mathbf{F}, P, p, P_{pub}, H_1, H_2\rangle$ and keep x secret.

Extract: Given a user's identity $ID \in \{0,1\}^*$, the KGS generates the user's private key usk as follows: (1) pick a random $r \in {}_R\mathbb{Z}_p$ and compute $R = rP$; (2) compute $s = r - cx \pmod p$, where $c = H_1(P_{pub}, ID, R)$; (3) set usk to (c, s, ID, P_{pub}) and transport it to the user securely.

Sign: To sign a message $m \in \{0,1\}^*$ under the private key $usk = (c, s, ID, P_{pub})$, the user takes the following steps: (1) pick a random $t \in {}_R\mathbb{Z}_p$ and compute $T = tP$; (2) compute $e = H_2(P_{pub}, ID, m, T, c)$ and $\pi = t - es \pmod p$; (3) return the user's signature $\sigma = (c, T, \pi)$ on message m.

Verify: A verifier checks the user's signature $\sigma = (c, T, \pi)$ on message m as follows: (1) compute $e = H_2(P_{pub}, ID, m, T, c)$; (2) output: **accept** if $c = H_1(P_{pub}, ID, cP_{pub} + e^{-1}(T - \pi P))$, **reject** otherwise.

III. Proposed ID-Based Mobile IP Registration Protocol with User Anonymity

In this section, we propose new ID-based mobile IP registration protocol with user anonymity, and specify the adversary models in mobile IP, which are security threats and attacks that mobile entities have faced in mobile IP registration, and then present the protocol goals.

TABLE I
NOTATION

Symbol	Description
M, N	Concatenation of two messages M and N, in the order specified
$\|$	Concatenation of two data
$Request$	A bit pattern indicating a request
$Reply$	A bit pattern indicating a reply
$Result$	A value indicating result of the request
$Advertisement$	A bit pattern indicating an advertisement
MN_{HM}	MN's home address
MN_{CoA}	MN's care-of-address
HA_{id}	HA's IP address as its ID
FA_{id}	FA's IP address as its ID
N_{MN}, N_{HA}, N_{FA}	Nonces issued by MN, HA, and FA, respectively
$K_{MN\text{-}HA}$	Shared keys between MN and HA,
$K_{FA\text{-}HA}$	Shared keys between FA and HA
$K_{MN\text{-}FA}$	Shared keys between MN and FA
mpk	The master public key
msk	The master secret key
usk_{FA}, usk_{HA}	The private key of FA and HA, respectively
σ_F	FA's signature on M_3
σ_H	HA's signature on M_4
$\langle M\rangle K$	MAC value of message M under key K
A $\rightarrow$ B : M	A sends the message M to B
$\{M\}K$	Encryption of message M under key K
$Key\text{-}Request$	A bit pattern indicating session key request
$Key\text{-}Reply$	A bit pattern indicating session key reply

A. Notations

We will use the notations in Table I to describe the proposed protocol.

B. Protocol Description

Both FA and HA in the mobile IP system employ the ID-based public key infrastructure, in which the private key usk_{FA} of a FA is $(c_{FA}, s_{FA}, ID_{FA}, P_{pub})$ and the private key usk_{HA} of a HA is $(c_{HA}, s_{HA}, ID_{HA}, P_{pub})$.

1) Mobile node initial registration in its home network:

When a mobile node first enter its home network, HA will verify the MN's identity. If the identity is authentic, HA will share a secret $K_{MN\text{-}HA}$ with the MN, generate a nonce N_{HA} and compute its TID as $H(ID_{MN} \| N_{HA})$, where $H : \{0,1\}^* \rightarrow \{0,1\}^*$. HA will also pick $t_\alpha \in {}_R\mathbb{Z}_p$, and compute $\alpha = t_\alpha P$ to be used by the MN in its next registration. Finally, HA will allocate the data $(H(ID_{MN} \| N_{HA}), K_{MN\text{-}HA}, N_{HA}, \alpha)$ to the MN securely.

2) Mobile node location registration with its HA in a foreign network:

Fig. 1 shows the proposed mobile IP registration protocol that proceeds as follows:

- ***Agent Advertisement:***

(AA1) FA $\rightarrow$ MN : M_1
where $M_1 = Advertisement, FA_{id}, MN_{CoA}, N_{FA}$

- ***Registration:***

(R1) MN $\rightarrow$ FA : $M_2, \langle M_2\rangle K_{MN\text{-}HA}$

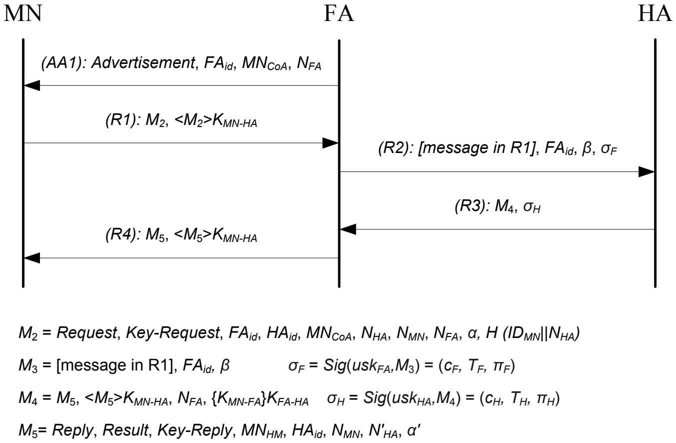

Fig. 1. Proposed mobile IP registration protocol.

where $M_2 = Request, Key\text{-}Request, HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, H(ID_{MN}\| N_{HA})$

On receiving the agent advertisement, MN generates a registration request consisting of the fixed portion, the non-authentication Extensions $(N_{FA}, FA_{id}, \alpha, H(ID_{MN}\| N_{HA}))$, and Mobile-Home Authentication Extension $\langle M_2\rangle K_{MN\text{-}HA}$ [3], [4]. Then MN sends the request to FA.

(R2) FA $\rightarrow$ HA : M_3, σ_F

where $M_3 =$ [message in R1]$, FA_{id}, \beta$

$$\sigma_F = Sig(usk_{FA}, M_3) = (c_F, T_F, \pi_F)$$

Upon receipt of R1, FA validates N_{FA}. If the nonce is valid, FA picks $t_\beta \in {}_R\mathbb{Z}_p$, computes $\beta = t_\beta P$, and generates the signature σ_F on the message M_3 using its private key usk_{FA} (see Section II). Then FA appends the non-authentication Extensions (FA_{id}, β) and the Foreign-Home Authentication Extension σ_F to the request message from MN and sends it to HA. If the nonce is not valid, FA ignores the registration request and sends MN a reply with suitable denial code.

(R3) HA $\rightarrow$ FA : M_4, σ_H

where

$$M_4 = M_5, \langle M_5\rangle K_{MN\text{-}HA}, N_{FA}, \{K_{MN\text{-}FA}\}K_{FA\text{-}HA}$$

$$M_5 = Reply, Result, Key\text{-}Reply, MN_{HM}, HA_{id}, N'_{HA}, N_{MN}, \alpha'$$

$$\sigma_H = Sig(usk_{HA}, M_4) = (c_H, T_H, \pi_H)$$

When HA receives the request, it will check if FA_{id} in M_3 equals FA_{id} in R1. If these two values are equal, HA validates N_{HA}; otherwise it rejects the request with a denial code. If the received N_{HA} is correct, HA checks if the signature σ_F is valid; otherwise it rejects the request with suitable denial code. If the signature verification algorithm returns **accept** (see Section II), HA has authenticated FA successfully; otherwise HA returns a reply with suitable denial code. Then HA uses $H(ID_{MN}\| N_{HA})$ in M_2 to find the shared secret $K_{MN\text{-}HA}$ in HA's database and validates $\langle M_2\rangle K_{MN\text{-}HA}$ with $K_{MN\text{-}HA}$. If the calculated $\langle M_2\rangle K_{MN\text{-}HA}$ equals the received $\langle M_2\rangle K_{MN\text{-}HA}$, HA has authenticated MN successfully; otherwise HA sends a reply with suitable denial code.

If the above verification succeeds, HA will accept MN's request, dynamically assign a home address to MN, and store the new mobility binding of MN_{HM} and MN_{CoA}. Then HA computes $K_{FA\text{-}HA} = t_\alpha \beta$ and erase t_α. Afterwards, HA updates the registration parameters as follows: a) HA picks $t'_\alpha \in {}_R\mathbb{Z}_p$ and computes $\alpha' = t'_\alpha P$ for MN's next registration; b) it produces a new nonce N'_{HA} and computes MN's new temporary identity $H(ID_{MN}\| N_{HA})$; c) it generates the new key $K'_{MN\text{-}HA}$ and secret key $K_{MN\text{-}FA}$ via the HMAC-SHA-1 one-way function [27]–[30]:

$$K'_{MN\text{-}HA} = HMAC-SHA-1(K_{MN\text{-}HA}, N'_{HA}\| N_{MN}\| HA_{id}) \quad (1)$$

$$K_{MN\text{-}FA} = HMAC-SHA-1(K_{MN\text{-}HA}, N_{HA}\| N_{MN}\| FA_{id}) \quad (2)$$

d) HA overlays $(ID_{MN}, H(ID_{MN}\| N_{HA}), K_{MN\text{-}HA}, N_{HA}, \alpha, t_\alpha)$ with $(ID_{MN}, H(ID_{MN}\| N'_{HA}), K'_{MN\text{-}HA}, N'_{HA}, \alpha', t'_\alpha)$ for MN's next registration.

Finally, HA constructs a registration reply message as follows: a) HA computes the Mobile-Home Authentication Extension $\langle M_5\rangle K_{MN\text{-}HA}$; b) it generates the signature σ_H on the message M_4 using its private key $usk_{HA}(c_{HA}, s_{HA}, ID_{HA}, P_{pub})$. Note that α is the corresponding T in the signature algorithm of the IBS scheme described in Section II; c) HA appends the non-authentication Extension α', the Mobile-Home Authentication Extension $\langle M_5\rangle K_{MN\text{-}HA}$, the non-authentication Extension $(N_{FA}, \{K_{MN\text{-}FA}\}K_{FA\text{-}HA})$, and the Foreign-Home Authentication Extension σ_H to the fixed portion of the registration reply and transmits the reply to FA.

(R4) FA $\rightarrow$ MN : $M_5, \langle M_5\rangle K_{MN\text{-}HA}$

On receiving the reply from HA, FA validates N_{FA}. If the nonce is valid, FA checks if the signature σ_H is valid; otherwise it sends a reply with a suitable denial code to MN. If the signature verification algorithm outputs **accept**, FA has authenticated HA successfully; otherwise FA returns a rejection reply to MN. If the above verification succeeds, FA will compute $K_{FA\text{-}HA} = t_\beta \alpha$ and erase t_β. Then FA decrypts $\{K_{MN\text{-}FA}\}K_{FA\text{-}HA})$ with $K_{FA\text{-}HA}$ to get $K_{MN\text{-}FA}$. Finally, FA relays the reply $(M_5, \langle M_5\rangle K_{MN\text{-}HA})$ to MN.

Upon receipt of R4, MN validates N_{MN}. If the nonce is correct, MN compares the calculated $\langle M_5\rangle K_{MN\text{-}HA}$ with the received $\langle M_5\rangle K_{MN\text{-}HA}$; otherwise MN's registration attempt fails. If these two MAC values are equal, MN computes $K'_{MN\text{-}HA}$ and $K_{MN\text{-}FA}$ according to (1) and (2). Then MN generates the new TID $H(ID_{MN}\| N'_{HA})$ and overlay $(ID_{MN}, H(ID_{MN}\| N_{HA}), K_{MN\text{-}HA}, N_{HA}, \alpha)$ with $(ID_{MN}, H(ID_{MN}\| N'_{HA}), K'_{MN\text{-}HA}, N'_{HA}, \alpha')$ for the next registration.

3) Tunneling:

When HA intercepts a datagram destined for MN, HA encapsulates the datagram and then routes it to the Care-of Address through a tunnel. After arriving at the end of the tunnel, the datagram is decapsulated and then correctly delivered by FA to MN.

C. Adversary Models in Mobile IP

1) Denial-of-Service (DoS) attacks: a) A malicious node can impersonate a legal MN to generate a bogus registration request specifying his own IP address as Care-of Address and thus redirect the latter's traffic toward itself and causing the legal MN to lose its network connectivity; b) an attacker may intercept the registration reply message from HA to a legal MN, causing the MN to receive maliciously altered traffic [10] or to lose the parameters synchronization with its HA and resulting in unsuccessful registration afterwards [31].

2) Replay attacks: a) By eavesdropping, an attacker can store a valid registration request that has been accepted by HA and replay it later for directing packets to MN's previous location; b) an attacker first records a valid request and its corresponding reply from some pervious run of successful registration. Then the attacker replays the request and corresponding reply to FA in turn. FA believes that the registration is one generated by a legitimate MN and HA. Therefore the attacker spoofs FA and can use resources on FA's local network for free [11], [18], [32].

3) Passive eavesdropping: In mobile IP registration, passive eavesdroppers are mainly interested in two pieces of information: a) the secret keys exchanged among mobile entities; b) a mobile user's identity information.

D. Protocol Goals

The following goals [11], [14], [33] should be achieved in the proposed protocol:

- Preventing the attacks described in the adversary models.
- Offering the scalability by using the ID-based public key cryptography.
- Minimizing the registration delay in order to achieve high efficiency.
- Computing selected values offline to reduce the processing time.
- Minimizing the computational load imposed on a MN, because it is a mobile device that has limited computational power and memory.
- Minimizing the message sizes and the numbers of the message exchange in order to save the bandwidth in networks.

IV. Formal Correctness Proof and Security Analysis

A. Formal Correctness Proof of the Proposed Protocol using PCL

We use PCL to prove the correctness of the proposed protocol. The detailed information on the PCL proof system can be found in [26], [34], [35]. The MN, FA, and HA roles of the proposed protocol are described formally using the programming language, which appears in Appendix A.

The desired security properties of the proposed protocol ($MIPreg$ is its one run instance) are:

1) Both MN and HA confirm the existence of the security association key $K_{MN\text{-}HA}$; FA and HA confirm the existence of their own secret keys usk_{FA} and usk_{HA}, respectively.
2) The fresh secret keys ($K'_{MN\text{-}HA}$, $K_{FA\text{-}HA}$, and $K_{MN\text{-}FA}$) should not be known to any other principal other than two participants, respectively. (For $K_{MN\text{-}FA}$, HA also know it.)
3) ID_{MN} should not be known to any other principal other than MN and HA.

ϕ_{auth}, ϕ_{sec}, and ϕ_{anony} formalize three security properties called authentication, key secrecy, and anonymity. Item 1), 2), and 3) is captured by authentication, key secrecy, and anonymity, respectively.

PRECONDITION: $MIPreg$ starts from a state in which the precondition θ holds, where

$$\begin{aligned}\theta := &\text{Has}(\hat{M}, (ID_{MN}, TID, K_{MN\text{-}HA}, N_{HA}, \alpha)) \wedge\\ &\text{Has}(\hat{H}, (ID_{MN}, TID, K_{MN\text{-}HA}, N_{HA}, t_\alpha)) \wedge\\ &(\forall Z.\text{Has}(\hat{Z}, K_{MN\text{-}HA}) \supset \hat{Z} = \hat{M} \vee \hat{Z} = \hat{H})\end{aligned}$$

AUTHENTICATION: $MIPreg$ is said to provide authentication if ϕ_{auth} holds, where

$$\begin{aligned}\phi_{auth} ::= &\text{Honest}(\hat{M}) \wedge \text{Honest}(\hat{F}) \wedge \text{Honest}(\hat{H}) \supset\\ &\forall M.\forall H.ActionsInOrder(\\ &\text{Send}(F, (\hat{F}, \hat{M}, AA1)), \text{Receive}(M, (\hat{F}, \hat{M}, AA1)),\\ &\text{Send}(M, (\hat{M}, \hat{F}, R1)), \text{Receive}(F, (\hat{M}, \hat{F}, R1)),\\ &\text{Send}(F, (\hat{F}, \hat{H}, R2)), \text{Receive}(H, (\hat{F}, \hat{H}, R2)),\\ &\text{Send}(H, (\hat{H}, \hat{F}, R3)), \text{Receive}(F, (\hat{H}, \hat{F}, R3)),\\ &\text{Send}(F, (\hat{F}, \hat{M}, R4)), \text{Receive}(M, (\hat{F}, \hat{M}, R4))\end{aligned}$$

The formula above formalizes a standard notion of authentication called matching conversations. It guarantees that the three principals have consistent views of protocol runs.

KEY SECRECY: $MIPreg$ is said to provide key secrecy if ϕ_{sec} holds, where

$$\begin{aligned}\phi_{sec} ::= &\text{Honest}(\hat{M}) \wedge \text{Honest}(\hat{F}) \wedge \text{Honest}(\hat{H}) \supset\\ &(\forall Z.\text{Has}(\hat{Z}, K'_{MN\text{-}HA}) \supset \hat{Z} = \hat{M} \vee \hat{Z} = \hat{H}) \wedge\\ &(\forall Z.\text{Has}(\hat{Z}, K_{MN\text{-}FA}) \supset \hat{Z} = \hat{M} \vee \hat{Z} = \hat{F} \vee \hat{Z} = \hat{H}) \wedge\\ &(\forall Z.\text{Has}(\hat{Z}, K_{FA\text{-}HA}) \supset \hat{Z} = \hat{F} \vee \hat{Z} = \hat{H})\end{aligned}$$

ANONYMITY: $MIPreg$ is said to provide anonymity if ϕ_{anony} holds, where

$$\begin{aligned}\phi_{anony} ::= &\text{Honest}(\hat{M}) \wedge \text{Honest}(\hat{F}) \wedge \text{Honest}(\hat{H}) \supset\\ &(\forall Z.\text{Has}(\hat{Z}, ID_{MN}) \supset \hat{Z} = \hat{M} \vee \hat{Z} = \hat{H}) \wedge\\ &\text{Has}(\hat{M}, ID_{MN}) \wedge \text{Has}(\hat{H}, ID_{MN})\end{aligned}$$

The formula above formalizes the security property of anonymity. It guarantees that only MN and HA know MN's real identity ID_{MN}.

From the analyses above, we conclude that the proposed protocol can be proved to be secure by the following two steps: 1) the protocol is proved to be secure under a given precondition; 2) the given precondition can be met through the self-sequential composition of the protocol, and the sequential composition of the protocol will not destruct the security of each sub-protocol. In other words, the proposed protocol is secure under the sequential composition.

Theorem 1: $MIPreg$ is a secure protocol, which guarantees authentication, key secrecy, and anonymity. Formally, $MIPreg \mapsto \phi$, where $\phi ::= \phi_{auth} \wedge \phi_{sec} \wedge \phi_{anony}$.

Proof:

1) $\Gamma := \Gamma1 \wedge \Gamma2 \wedge \Gamma3 \wedge \Gamma4$ are invariants of $MIPreg$. Formally,

$$MIPreg \mapsto \Gamma \tag{3}$$

In the case of $MIPreg$, the expected behaviors of three honest principals are captured by Γ listed in Table II. Invariants $\Gamma1$, $\Gamma2$, $\Gamma3$, and $\Gamma4$ are generally proved by induction over programs using $the\ Honesty\ Rule$. $\Gamma4$ states that no principal

TABLE II
INVARIANTS OF THE PROPOSED PROTOCOL (MIPREG)

$$\begin{aligned}
\Gamma_1 := &\ \text{Honest}(\hat{M}) \supset \\
&(\diamondminus \text{Send}(M, (\hat{M}, \hat{F}, R1)) \supset \\
&(\text{Receive}(M, (\hat{F}, \hat{M}, AA1)) < \text{Send}(M, (\hat{M}, \hat{F}, R1))))\wedge \\
&ActionInOrder(\text{Receive}(M, (\hat{F}, \hat{M}, AA1)), \\
&\text{Send}(M, (\hat{M}, \hat{F}, R1)), \text{Receive}(M, (\hat{F}, \hat{M}, R4))) \\
\Gamma_2 := &\ \text{Honest}(\hat{F}) \supset \\
&(\diamondminus \text{Send}(F, (\hat{F}, \hat{H}, R2)) \supset \\
&(\text{Receive}(F, (\hat{M}, \hat{F}, R1)) < \text{Send}(F, (\hat{F}, \hat{H}, R2))))\wedge \\
&(\diamondminus \text{Send}(F, (\hat{F}, \hat{M}, R4)) \supset \\
&(\text{Receive}(F, (\hat{H}, \hat{F}, R3)) < \text{Send}(F, (\hat{F}, \hat{M}, R4))))\wedge \\
&ActionInOrder(\text{Send}(F, (\hat{F}, \hat{M}, AA1)), \\
&\text{Receive}(F, (\hat{M}, \hat{F}, R1)), \text{Send}(F, (\hat{F}, \hat{H}, R2)), \\
&\text{Receive}(F, (\hat{H}, \hat{F}, R3)), \text{Send}(F, (\hat{F}, \hat{M}, R4))) \\
\Gamma_3 := &\ \text{Honest}(\hat{H}) \supset \\
&(\diamondminus \text{Send}(H, (\hat{H}, \hat{F}, R3)) \supset \\
&(\text{Receive}(H, (\hat{F}, \hat{H}, R2)) < \text{Send}(H, (\hat{H}, \hat{F}, R3))))\wedge \\
&ActionInOrder(\text{Receive}(H, (\hat{F}, \hat{H}, R2)), \\
&\text{Send}(H, (\hat{H}, \hat{F}, R3))) \\
\Gamma_4 := &\ (\text{Has}(\hat{X}, K_{MN\text{-}HA}) \supset \neg(\text{Send}(\hat{X}, m) \wedge \text{Contains}(m, K_{MN\text{-}HA})))\wedge \\
&(\text{Has}(\hat{X}, ID_{MN}) \supset \neg(\text{Send}(\hat{X}, m) \wedge \text{Contains}(m, ID_{MN})))\wedge \\
&(\text{Has}(\hat{X}, K'_{MN\text{-}HA}) \supset \neg(\text{Send}(\hat{X}, m) \wedge \text{Contains}(m, K'_{MN\text{-}HA})))\wedge \\
&(\text{Has}(\hat{X}, K_{MN\text{-}FA}) \supset \neg(\text{Send}(\hat{X}, m) \wedge \text{Contains}(m, K_{MN\text{-}FA})))\wedge \\
&(\text{Has}(\hat{X}, K_{FA\text{-}HA}) \supset \neg(\text{Send}(\hat{X}, m) \wedge \text{Contains}(m, K_{FA\text{-}HA}))) \\
\Gamma := &\ \Gamma_1 \wedge \Gamma_2 \wedge \Gamma_3 \wedge \Gamma_4
\end{aligned}$$

leaks the secret information. Due to space limitations, the detailed proofs are omitted here.

2) On execution of the FA role by a principal, authentication is guaranteed if Γ hold. Similar result holds for principals executing the MN and HA roles. Formally, $\Gamma \mapsto \theta[\text{FA}]_F\phi_{auth}, \theta[\text{MN}]_M\phi_{auth}, \theta[\text{HA}]_H\phi_{auth}, i.e.,$

$$\Gamma \mapsto \phi_{auth} \tag{4}$$

Similarly, we can prove the following (5) and (6).
$\Gamma \mapsto \theta[\text{FA}]_F\phi_{sec}, \theta[\text{MN}]_M\phi_{sec}, \theta[\text{HA}]_H\phi_{sec}, i.e.,$

$$\Gamma \mapsto \phi_{sec} \tag{5}$$

$\Gamma \mapsto \theta[\text{FA}]_F\phi_{anony}, \theta[\text{MN}]_M\phi_{anony}, \theta[\text{HA}]_H\phi_{anony}, i.e.,$

$$\Gamma \mapsto \phi_{anony} \tag{6}$$

Because one important property of the proposed protocol is user's anonymity, a detailed proof of the guarantee of anonymity for FA appears in Appendix B. A similar approach is applicable to the proof of the anonymity guarantee for MN and HA, and the proof of the guarantees of authentication and key secrecy. These proofs are omitted here due to space constraints.

3) From (3)(4)(5)(6), we can deduce that authentication, key secrecy, and anonymity are guaranteed if hold. Formally,

$$\Gamma \mapsto \phi_{auth}, \phi_{sec}, \phi_{anony}, \quad i.e., \quad \Gamma \mapsto \phi \tag{7}$$

4) From (3)(7), it is concluded that $MIPreg$ provides authentication, key secrecy, and anonymity. Formally, $MIPreg \mapsto \phi$. ■

Therefore, the proposed protocol is secure under the given precondition.

Theorem 2 (Composition properties of $MIPreg$): The proposed protocol is a secure protocol under the sequential composition, which means that MIP, a sequential composition of current and next successful run ($MIPreg$ and $MIPreg'$) of the protocol, guarantees the security properties of $MIPreg$ and $MIPreg'$. Formally, $MIP \mapsto \phi \wedge \phi'$.

Proof:

Considering the execution of the FA role by a principal, we have:

1) From the proof of theorem 1, we can know that both $MIPreg$ and $MIPreg'$ have the desired security properties. Formally, $MIPreg \mapsto \Gamma$, $\Gamma \mapsto \psi$, $\psi = \theta[FA]_F\phi$; $MIPreg' \mapsto \Gamma'$, $\Gamma' \mapsto \psi'$, $\psi' = \theta'[FA']_F\phi'$.
2) Weaken the hypotheses to $\Gamma \cup \Gamma'$. The proof of the protocol properties is clearly preserved under a larger set of assumptions. Formally, $\Gamma \cup \Gamma' \mapsto \psi$, $\Gamma \cup \Gamma' \mapsto \psi'$.
3) Because the post-condition of the modal formula ψ matches the pre-condition of ψ', i.e. ϕ matches θ', then the two parts can be sequentially composed by applying the sequencing rule S1. Assuming that ψ and ψ' are $[FA]_F\varphi$ and $\varphi[\text{FA}']_F\phi'$, respectively, we have: $\psi \mapsto [\text{FA}]_F\theta'$, $\varphi = \theta' \cup \phi$, $\Gamma'_\varphi = \Gamma'$, $\Gamma \cup \Gamma' \mapsto [\text{FA}, \text{FA}']_F\phi'$.
4) The invariants used in proving the properties of the two runs of the protocol, $\Gamma \cup \Gamma'_\varphi$, hold for both the runs. From this point and the formulas in steps 2) and 3), the security of composition properties of $MIPreg$ is preserved under their sequential composition, and furthermore the following formula is provable. Formally, $MIP \mapsto \theta[\text{FA}, \text{FA}']_F\phi \wedge \phi'$.

Similarly, we have $MIP \mapsto \theta[\text{MN}, \text{MN}']_M\phi \wedge \phi'$ and $MIP \mapsto \theta[\text{HA}, \text{HA}']_H\phi \wedge \phi'$. Furthermore, we have

$$MIP \mapsto \phi \wedge \phi'.$$

Hence, the given precondition is satisfied by proving composition properties of $MIPreg$, and the composition protocol is also secure. Also, we only give the proof of composition properties of $MIPreg$ from the FA role. The similar proofs from the MN and HA roles are omitted here due to space constraints. ■

Therefore, the protocol is secure under the sequential composition.

From the proof of theorem 1 and 2, we conclude that the protocol is proved to be secure.

B. Security Analysis of the Proposed Protocol under the Adversary Models

1) Denial-of-Service (DoS) attacks:

a) The proposed protocol can defeat the first kind of DoS attack by adding strong authentication on the registration messages exchanged between MN and HA. When the attacker generates a bogus registration request specifying his own IP address as Care-of Address of a legal MN to register with its HA, the attacker cannot generate the valid Mobile-Home Authentication Extension of the registration request because it does not know the shared key $K_{MN\text{-}HA}$ between MN and HA. HA will reject the bogus registration request due to the invalid authenticator $\langle M_2 \rangle K_{MN\text{-}HA}$ in R2. Therefore, the malicious node attacks unsuccessfully. b) The second kind of DoS attack happens when an attacker intercepts the registration reply from FA to MN in R4. Once MN does not receive the registration reply within a set time, the synchronization between MN and HA will be lost with respect to the registration parameters. In the proposed protocol, the synchronization problem can be solved using the following scheme: MN first makes the registration with the dynamic parameters. After a few registration attempts (e.g., three attempts), if the registration still fails, then MN uses the initial parameters to register with its HA. Upon receipt of MN's registration request, HA first searches for ID_{MN} in its dynamic parameter database according to MN's TID. If there is no such an entry, HA continues to search in its initial parameter database. Therefore, MN's registration request can be finally accepted by its HA and parameters can be resynchronized when HA transmits the reply to MN.

2) Replay attacks:

a) When an attacker replays a registration request that is previously accepted by HA for directing packets to MN's previous location, HA will validate N_{HA} in the registration request. Because HA's obsolete nonce in the request does not equal HA's new nonce stored on HA, HA will reject the request. Therefore, the replay attack fails. b) When an attacker replays a valid request and its corresponding reply from a previous run of successful registration, FA will check if the nonce N_{FA} in the registration messages is equal to FA's nonce sent in the last agent advertisement. Therefore, the nonce is not valid and FA will not allow MN to use its resources. This kind of replay attack is prevented, simply by including additional nonce replay protection originated from FA in the proposed protocol.

3) Passive eavesdropping:

a) To defeat this kind of eavesdropping, it is required either to encrypt the transmitted secret keys or not to put the secret keys on links. In the proposed protocol, the new secret key $K'_{MN\text{-}HA}$ between MN and HA can be generated locally by HA and MN for the next registration according to (1), respectively. The secret key between FA and HA can be generated according to the ID-based authenticated key exchange scheme [23]: $K_{FA\text{-}HA} = t_\alpha\beta = t_\alpha t_\beta P = t_\beta t_\alpha P = t_\beta\alpha$. Eavesdroppers cannot read the secret key $K_{MN\text{-}FA}$ because HA sends $\{K_{MN\text{-}FA}\}K_{FA\text{-}HA}$ to FA over links and MN locally generates the secret key $K_{MN\text{-}FA}$ according to (2). b) To prevent the attack, it is necessary to provide the anonymity of MN's identity. The proposed solution is to use a temporary identity of MN $H(ID_{MN}\|N_{HA})$ instead of his real identity. Identity information has never been exposed in the mobile IP environments. An adversary cannot identify the user who is trying to register, track his moving history and current location, and associate him with the session in which he participates, since the TID varies with each registration because of a different $N_{HA}(N_{HA} \neq N'_{HA})$.

Then we compare the proposed protocol with the existing ones: the basic protocol [3], [4], CA-PKI based protocol [9], and Yang's protocol [15] because they stand for three main types of registration protocols before ID-PKC is introduced in mobile IP. In addition, to achieve a good performance, two mobile IP registration protocols using self-certified public keys are proposed in [36], i.e., the protocol 2 and 3. Therefore, it is also required to compare the proposed protocol with the ones

TABLE III
AUTHENTICATION ANALYSIS

	MN-FA	FA-HA	MN-HA
Basic [3], [4]	None	None	MAC (static key)
CA-PKI [9]	Digital signature	Digital signature	Digital signature
Yang [15]	None	Digital signature	Symmetric encryption
The protocol 2 in [36]	None	MAC (static key)	MAC (dynamic key)
The protocol 3 in [36]	None	MAC (dynamic key)	MAC (dynamic key)
The proposed protocol	None	IBS without pairings	MAC (dynamic key)

TABLE IV
REPLAY PROTECTION METHOD AND ATTACK PREVENT ANALYSIS

	DoS Attack	Anti-replay Attack	Replay Attack	Man-in-middle Attack	Active Attack	Passive eaves-dropping
Basic [3], [4]	(I)	None	No	No	No	No
CA-PKI [9]	(I)	None	No	Yes	Yes	(I)
Yang [15]	(I)	Nonces	(I,II)	Yes	Yes	(I)
Protocol 2 in [36]	(I,II)	Nonces	(I,II)	Yes	Yes	(I,II)
Protocol 3 in [36]	(I,II)	Nonces	(I,II)	Yes	Yes	(I,II)
Proposed protocol	(I,II)	Nonces	(I,II)	Yes	Yes	(I,II)

Note: (I) and (II) denote the attack a) and b) in the paper, respectively.

based on self-certified public keys. The difference is that the former applies ID-based signature scheme without pairings to the authentications between FA and HA but the latter makes use of self-certified key exchange schemes and MAC. It can be concluded that the protocol 2 in [36] achieves weaker security than the proposed protocol in this paper because of the use of MAC with static key for the authentications between FA and HA. However, the two protocols in [36] provide more security confidence due to the key escrow problem in ID-PKC.

Table III shows the authentication analysis of three existing protocols, the two protocols in [36], and the proposed protocol. The proposed protocol employs the ID-based signature scheme without pairings for the authentications between FA and HA; the authentications between MN and HA are achieved in R2 and R4 by validating $\langle M_2\rangle K_{MN\text{-}HA}$ and $\langle M_5\rangle K_{MN\text{-}HA}$, respectively; the trust relation between MN and FA is established through HA. The protocols in [36] applies the MAC with dynamic key to the authentications between MN and HA. Yang's protocol employs digital signature for the authentications between FA and HA; however, symmetric encryptions between MN and HA cannot provide the convincing mutual authentications. Digital signature is used for the authentications among three entities in the CA-PKI based protocol.

TABLE V
PROCESSING PARAMETERS (ONE OPERATION)

Operation time(on MN)	
SHA	0.019111 ms
DES	0.007354 ms
Operation time(on FA, HA)	
SHA-1	0.000898 ms
DES	0.000358 ms
RSA 1024 Encryption	0.18 ms
RSA 1024 Decryption	4.77 ms
RSA 1024 Signature	4.75 ms
RSA 1024 Verification	0.18 ms
Point Scalar Multiplication	1.1 ms

The replay protection method and the attack prevent analysis are listed in Table IV. In the proposed protocol and the two protocols in [36], replay attacks can be defeated by including both FA's nonce and the nonces from MN and HA, i.e., N_{FA}, N_{MN} and N_{HA}, in registration messages; the second kind of DoS attack can be resisted and the registration parameters can be resynchronized by initializing MN and HA; MN's identity ID_{MN} and HA's nonce N_{HA} are hashed together to generate TID, whose value varies with each registration because of a different $N_{HA}(N_{HA} \neq N'_{HA})$. However, three existing protocols have not employed any scheme to solve the synchronization problem. User anonymity cannot be actually provided because the identity related data is transmitted together with the corresponding cipher-text, although Yang [15] claims that their protocol achieves the anonymity.

From the analysis and comparisons above, it is concluded that the proposed protocol achieves stronger security than three existing ones and the protocol 2 in [36] but provides less security confidence than the two protocols using self-certified public keys in [36].

V. PERFORMANCE EVALUATION

A. Simulation Setup

Simulations are carried out to evaluate the performance of the proposed protocol, based on OPNET Modeler 10.5. Table V lists the processing parameters of the cryptographic operations used in the simulations. The processing time of SHA and DES on MN are referred to [37]. For FA and HA, the processing time of RSA, SHA-1, DES, and modular exponentiation are from [38], [39]; the processing time of scalar multiplication is estimated based on the results in [40].

For Yang's protocol [15], RSA with a 1024-bit modulus and the public exponent of $e = 2^{16} + 1$ is used for sufficient security and fast computation. Therefore, an RSA public key consists of a pair (n, e), resulting in a total size of 131 bytes [41]. In addition, an RSA signature consists of a single 1024-bit value. FA and HA's IP address of 32 bits are used as their ID and certificate expiration time can be encoded in 2 bytes. An RSA certificate $\langle ID_A, (n, e), exp,$ CA's signature$\rangle$ will be a total of 265 bytes in length. For the protocols in [36], we choose the modulus 1024 bits, which can provide the required security [39]. For the proposed protocol, p is a 160-bit Solinas prime in the IBS scheme. Such choices of p deliver a comparable level of security to 1024-bit RSA [41], [42]. Therefore, a point on $E/\mathbf{F}$ transmitted over links is of 160 bits.

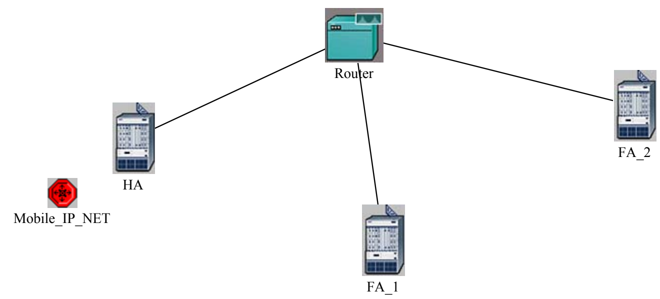

Fig. 2. The network topology in the simulated scenario 1.

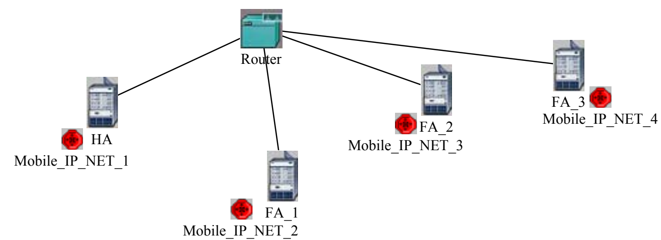

Fig. 3. The network topology in the simulated scenario 2.

Two scenarios are considered to assess the behavior of the proposed protocol. In order to simulate realistic scenarios, we have imported traffic flows as the background load between HA and FA_1. The scenarios utilize 802.11b WLAN interface with roaming capability (i.e., WLAN access points) to simulate hand-offs between mobile IP agents. To specify the Mobile_IP_NETs' movement, the network model uses the trajectory files that contain one uniform traversal time (5 minutes) for all (3) path segments to determine the mobile subnets' location at a given time. First, we study the performance of the proposed protocol by simulating the compared protocols in the scenario 1 as depicted in Fig. 2. One mobile subnet, one home network, two foreign networks, and one router were set in the scenario 1. The mobile subnet contains a mobile router (MR) and a client node. The MR is manually configured with common BSS ID and IP network address as that of the HA WLAN router. All the foreign agents are also WLAN routers with different BSS Identifiers. As the mobile subnet moves along the trajectory, it changes the access point and changes the mobile agent as well. Second, we investigate the scalability property of the proposed protocol by using more realistic and more complex simulated networks in the scenario 2. Fig. 3 shows the network topology with 4 mobile subnets that are located in the home network and 3 foreign networks respectively at the beginning of the simulation. During the simulation, the four mobile subnets move along their respective trajectories, and then they continually change the access point and change the mobile agent as well. Also, in order to see how much the registration delay is affected by adding more mobile subnets roaming among different foreign networks, we compare the registration delay of the proposed protocol for the two scenarios.

The OPNET simulation project used in this paper are based on OPNET's standard Mobile IP project. In order to extend the functionality of standard models used for the simulation, we add a statistic "Registration Delay" to mobile IP process model, and define 18 mobile IP process models, 30 node models, and 24 packet formats. The links between FA, router, and HA are set to T1. Mobile IP service is activated at 50 seconds and the lifetime of the mobile binding kept at HA is 10 seconds in the simulation duration of 1000 seconds.

B. Scenario 1 and Simulation Results

If two secret keys $K'_{MN\text{-}HA}$ and $K_{MN\text{-}FA}$ in the proposed protocol are transmitted to MN over links rather than generated by MN, then a variant of the proposed protocol can be derived.

1) Registration delay:

It is clear that the performance of CA-PKI based protocol [9] is restricted by the heavy certificate-based public key cryptography operations on MN. Therefore, the basic protocol, Yang's protocol, the two protocols in [36], the variant, and the proposed protocol are implemented in the scenario 1, respectively. Because the registration delay varies over the course of a simulation, it is helpful to look at the time average for this statistics. Fig. 4 illustrates the time average of the registration delay for six compared protocols. Note that the registration delay as a whole appears to be leveling off, indicating a stable network. The large change early in the simulation reflects the sensitivity of averages to the relatively small number of samples collected. From the figure, we have the following five observations: (1) compared to Yang's protocol, the average registration delay of the proposed protocol is drastically reduced for two main reasons: a) the proposed protocol eliminates certificate-based operations and does not employ expensive pairings; b) $K'_{MN\text{-}HA}$ and $K_{MN\text{-}FA}$ are not transmitted by HA to MN but generated locally by MN, leading to the save of the time spent in transmitting these two keys over links and the associated encryption and decryption at HA and MN; (2) the protocol 3 in [36] is inferior to the proposed protocol in terms of the registration delay due to much modular exponentiation and large message sizes; (3) the proposed protocol has a longer registration delay than the protocol 2 in [36] because it provide higher level of security; (4) the proposed protocol takes a little more time than the basic protocol, because the proposed protocol provides much stronger security and there exists a trade-off between the security and efficiency; (5) the registration delay of the proposed protocol is smaller than that of the variant. It is clear that the secret key distribution in the proposed protocol is better than that in the variant. These observations confirm that the proposed protocol minimizes the registration delay while improving the security. The simulation results agree with the analytical results. For example, the registration delay of the proposed protocol is reduced up to 49.3 percent approximately, compared to Yang's protocol.

2) Registration signaling traffic:

Table VI lists the message sizes of six protocols. Compared with Yang's protocol, the proposed protocol saves the communication bandwidth between FA and HA because of no RSA signature and certificate of large size in the exchanged messages; the messages between MN and FA of the proposed protocol are slightly longer than those of Yang's protocol due to the effort on the security improvement. The protocols in [36] have more traffic than the proposed protocol because of the transmission of the witness. The proposed protocol has a smaller message size than the variant because $K'_{MN\text{-}HA}$ and $K_{MN\text{-}FA}$ are not transmitted over links. Certainly, the least message is exchanged in the basic protocol since its security is the weakest. Thus, the proposed protocol has less registration signaling traffic while providing stronger security.

3) Computational load on MN:

The basic protocol only needs two SHA operations since it maintains the lowest level of security; Yang's protocol needs nine DES operations on MN; the protocol 2 in [36] does five SHA and one DES operations on MN; the protocol 3 in [36] does six SHA and three DES; the variant needs four SHA and five DES operations on MN, of which DES operations can be saved by using offline computation. However, the proposed protocol only performs three SHA operations on MN considering offline computation. Although the variant protocol seems to save SHA on generating the keys, it needs more SHA operations while validating MAC due to the longer message M_5. Moreover, the proposed protocol can generate the keys offline, but the variant cannot validate MAC offline. Therefore, the proposed protocol can save the computation time and battery consumption on MN while improving the security.

In conclusion, the proposed protocol outperforms the existing protocols in terms of the registration delay, the registration

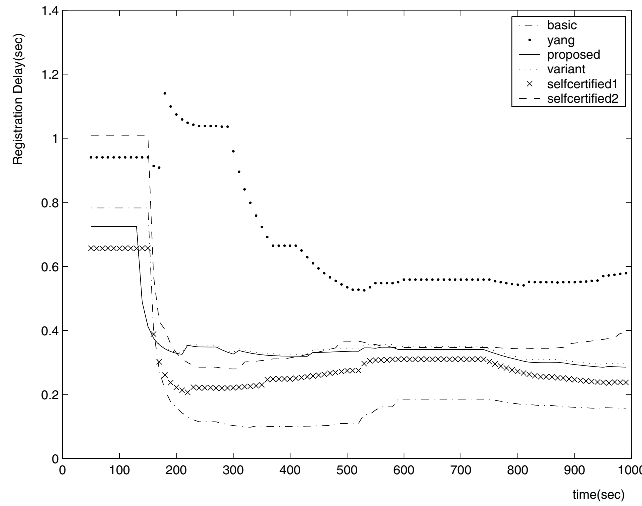

Fig. 4. The comparison result of six protocols in terms of the registration delay.

TABLE VI
THE MESSAGE SIZE (BYTES) OF THE COMPARED PROTOCOLS

	MN-FA	FA-HA	HA-FA	FA-MN
Basic [3], [4]	50	50	46	46
CA-PKI [9]	66	578	582	66
Yang [15]	50	50	46	46
The protocol 2 in [36]	206	364	108	54
The protocol 3 in [36]	226	404	124	70
The variant	82	176	228	130
The proposed protocol	82	176	146	48

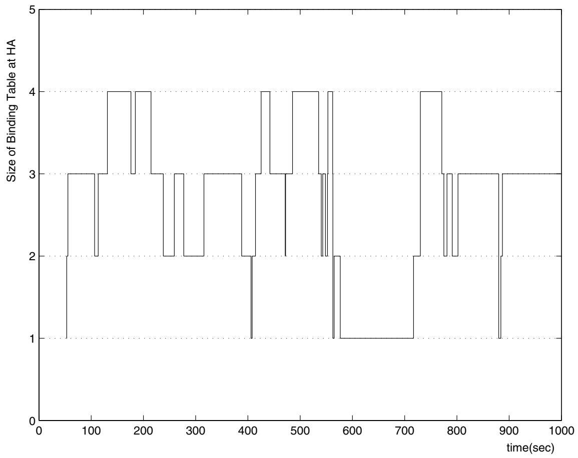

Fig. 5. The size of the binding table at HA in the scenario 2.

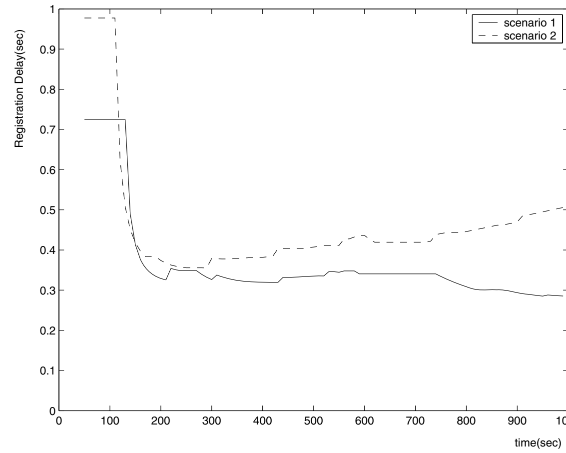

Fig. 6. The comparison result of registration delays of the proposed protocol in the scenario 1 and 2.

signaling traffic, and the computational load on a MN while providing the improved security.

C. Scenario 2 and Simulation Results

In order to apply the proposed protocol to real networks, we should investigate the scalability property of the proposed protocol in a more realistic and more complex scenario. For the purpose, the proposed protocol is implemented in the scenario 2. Fig. 5 shows the size of the binding table recorded at HA. As illustrated in this figure, the results of the simulation indicate that the number of mobile subnets served by HA continually change over the simulation duration as the four mobile subnets move along their respective trajectories and change the mobile agent at frequent intervals. As expected, the size of the binding table at HA has a maximum of 4 and the size after around 888 seconds is 3. This is because among the four mobile subnets only the Mobile_IP_NET_4 moves around HA and does not need the mobile binding at HA at the end of the simulation. The simulation results match to the theoretical analysis. It is useful to observe that how much the registration delay is affected by comparing the registration delay of the proposed protocol for the two scenarios. Fig. 6 shows the time average of the registration delay of the proposed protocol in the scenario 1 and 2. Notice that both simulations converge to steady state after initial spikes. Further, the registration delay is lower for the scenario 1, which is experiencing less traffic. These results seem reasonable. It can be concluded that the proposed protocol performs well in more realistic and more complex networks.

VI. Conclusions And Future Works

This paper explores the idea of a secure and efficient IBS scheme without pairings in mobile IP registration to minimize the registration delay. A significant feature is user's anonymity in the proposed protocol. All possible replay attacks can be prevented using the nonces from MN, HA, and FA. A formal correctness proof of the proposed protocol using PCL is provided in this paper. Simulation results demonstrate that the proposed protocol outperforms the existing protocols while providing stronger security, and performs very well under more complex scenario. It can be concluded that the proposed protocol achieves the foregoing protocol goals.

For the future works, one of our near term tasks is to conduct a research on how to apply the proposed mobile IP registration protocol to a variety of wireless networks, such as WLAN, Bluetooth, and beyond 3G mobile networks. In addition, we will pursue how to integrate the proposed protocol with AAA for its flexible mobility among different administrative domains.

Appendix A
Actions of the Cord of the Proposed Protocol ($MIPreg$ Program)

MIPreg:MN $= (M, ID_{MN}, TID, K_{MN-HA}, N_{HA}, \alpha)[$
receive $\hat{F}, \hat{M}, M_1$; match $M_1 / FA_{id}, MN_{CoA}, N_{FA}$;
new N_{MN}; match $HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID / M_2$;
match $HASH_{K_{MN-HA}}(M_2) / MAC_1$; send $\hat{M}, \hat{F}, M_2, MAC_1$;
receive $\hat{F}, \hat{M}, M_5, MAC_2$; match $MAC_2 / HASH_{K_{MN-HA}}(M_5)$;
match $M_5 / MN_{HM}, HA_{id}, N'_{HA}, N_{MN}, \alpha'$;
match $HASH_{K_{MN-HA}}(N'_{HA} \| N_{MN} \| HA_{id}) / K'_{MN-HA}$;
match $HASH_{K_{MN-HA}}(N_{HA} \| N_{MN} \| FA_{id}) / K_{MN-FA}$;
match $HASH(ID_{MN} \| N'_{HA}) / TID';]_M$
MIPreg:FA $= (F, \hat{M}, \hat{H})[$
new N_{FA}; send $\hat{F}, \hat{M}, FA_{id}, MN_{CoA}, N_{FA}$;
receive $\hat{M}, \hat{F}, M_2, MAC_1$;
match $M_2 / HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID$;
new t_β; match $t_\beta P / \beta$; match $M_2, MAC_1, FA_{id}, \beta / M_3$;
match sign $M_3, usk_{FA} / \sigma_F$; send $\hat{F}, \hat{H}, M_3, \sigma_F$;
receive $\hat{H}, \hat{F}, M_4, \sigma_H$; verify σ_H, M_4, HA_{id};
match $M_4 / M_5, MAC_2, N_{FA}, Ek$;
match $t_\beta \alpha / K_{FA-HA}$; match dec $Ek, K_{FA-HA} / K_{MN-FA}$;
send $\hat{F}, \hat{M}, M_5, MAC_2;]_F$
MIPreg:HA $= (H, ID_{MN}, TID, K_{MN-HA}, N_{HA}, t_\alpha)[$
receive $\hat{F}, \hat{H}, M_3, \sigma_F$; verify σ_F, M_3, FA_{id};
match $M_3 / M_2, MAC_1, FA_{id}, \beta$;
match $M_2 / HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID$;
match $TID / HASH(ID_{MN} \| N_{HA})$;
match $MAC_1 / HASH_{K_{MN-HA}}(M_2)$;
match $t_\alpha \beta / K_{FA-HA}$; new N'_{HA}, t'_α;
match $HASH(ID_{MN} \| N'_{HA}) / TID'$;
match $HASH_{K_{MN-HA}}(N'_{HA} \| N_{MN} \| HA_{id}) / K'_{MN-HA}$;
match $HASH_{K_{MN-HA}}(N_{HA} \| N_{MN} \| FA_{id}) / K_{MN-FA}$;
match $MN_{HM}, HA_{id}, N'_{HA}, N_{MN}, \alpha' / M_5$;
match $HASH_{K_{MN-HA}}(M_5) / MAC_2$;
match enc $K_{MN-FA}, K_{FA-HA} / Ek$; match $M_5, MAC_2, N_{FA}, Ek / M_4$;
match sign $M_4, usk_{HA} / \sigma_H$; send $\hat{H}, \hat{F}, M_4, \sigma_H;]_H$

APPENDIX B
PROOF OF THE GUARANTEE OF ANONYMITY FOR FA OF $MIPreg$

AA1, ARP, AA4	$\theta[FA]_F$	
	$\mathrm{Send}(F,(\hat{F},\hat{M},AA1)) < \mathrm{Receive}(F,(\hat{M},\hat{F},R1)) < \mathrm{Send}(F,(\hat{F},\hat{H},R2)) <$	
	$\mathrm{Receive}(F,(\hat{H},\hat{F},R3)) < \mathrm{Send}(F,(\hat{F},\hat{M},R4))$	(1)
	$TID \equiv HASH(ID_{MN} \parallel N_{HA})$	(2)
ARP, HASH3	$\theta[\mathrm{receive}\ \hat{M},\hat{F},M_2,MAC_1;$	
	$\mathrm{match}\ M_2 / HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID]_F$	
	$\mathrm{Receive}(F,(\hat{M},\hat{F},M_2,MAC_1)) \supset$	
	$\exists X.\mathrm{Computes}(X,TID) \wedge \mathrm{Send}(X,TID) \wedge$	
	$(\mathrm{Send}(X,TID) < \mathrm{Receive}(F,(\hat{M},\hat{F},M_2,MAC_1)))$	(3)
HASH1	$\mathrm{Computes}(X,TID) \equiv \mathrm{Has}(\hat{X},ID_{MN}) \wedge \mathrm{Has}(\hat{X},N_{HA})$	(4)
HASH4	$\mathrm{Has}(\hat{X},TID) \equiv \mathrm{Has}(\hat{X},HASH(ID_{MN} \parallel N_{HA}) \supset$	
	$\mathrm{Computes}(X,HASH(ID_{MN} \parallel N_{HA})) \vee$	
	$(\exists Y,m.\mathrm{Computes}(Y,HASH(ID_{MN} \parallel N_{HA})) \wedge$	
	$\mathrm{Send}(Y,m) \wedge \mathrm{Contains}(m,HASH(ID_{MN} \parallel N_{HA})))$	(5)
(5), Γ	$\theta[\mathrm{receive}\ \hat{M},\hat{F},M_2,MAC_1;$	
	$\mathrm{match}\ M_2 / HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID]_F$	
	$\mathrm{Honest}(\hat{M}) \wedge \mathrm{Honest}(\hat{F}) \wedge \mathrm{Honest}(\hat{H}) \supset$	
	$\mathrm{Has}(\hat{X},TID) \equiv \mathrm{Has}(\hat{X},HASH(ID_{MN} \parallel N_{HA}) \supset$	
	$\mathrm{Computes}(X,HASH(ID_{MN} \parallel N_{HA}))$	(6)
(6), HASH1	$\theta[\mathrm{receive}\ \hat{M},\hat{F},M_2,MAC_1;$	
	$\mathrm{match}\ M_2 / HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID]_F$	
	$\mathrm{Honest}(\hat{M}) \wedge \mathrm{Honest}(\hat{F}) \wedge \mathrm{Honest}(\hat{H}) \supset$	
	$\mathrm{Computes}(X,HASH(ID_{MN} \parallel N_{HA})) \supset \mathrm{Has}(\hat{X},ID_{MN}) \supset \hat{X} = \hat{M} \vee \hat{X} = \hat{H}$	(7)
(7), ϕ_{auth}	$\theta[\mathrm{receive}\ \hat{M},\hat{F},M_2,MAC_1;$	
	$\mathrm{match}\ M_2 / HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID]_F$	
	$\mathrm{Honest}(\hat{M}) \wedge \mathrm{Honest}(\hat{F}) \wedge \mathrm{Honest}(\hat{H}) \supset \hat{X} \neq \hat{H} \wedge \hat{X} = \hat{M}$	(8)
(7), (8)	$\theta[\mathrm{receive}\ \hat{M},\hat{F},M_2,MAC_1;$	
	$\mathrm{match}\ M_2 / HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, FA_{id}, \alpha, TID]_F$	
	$\mathrm{Honest}(\hat{M}) \wedge \mathrm{Honest}(\hat{F}) \wedge \mathrm{Honest}(\hat{H}) \supset \mathrm{Has}(\hat{M},ID_{MN}) \wedge \mathrm{Has}(\hat{M},TID)$	(9)
ARP	$\theta[\mathrm{receive}\ \hat{H},\hat{F},M_4,\sigma_H]_F$	
	$\mathrm{Receive}(F,(\hat{H},\hat{F},M_4,\sigma_H)) \supset$	
	$\exists Y,m.\mathrm{Send}(Y,m) \wedge \mathrm{Contains}(m,(M_4,\sigma_H))$	(10)
(10), ϕ_{auth}	$\theta[\mathrm{receive}\ \hat{H},\hat{F},M_4,\sigma_H]_F$	
	$\mathrm{Honest}(\hat{M}) \wedge \mathrm{Honest}(\hat{F}) \wedge \mathrm{Honest}(\hat{H}) \supset$	
	$\exists Y,m.\mathrm{Send}(Y,m) \wedge \mathrm{Contains}(m,(M_4,\sigma_H)) \wedge \hat{Y} = \hat{H}$	(11)
(11), Γ	$\theta[\mathrm{receive}\ \hat{H},\hat{F},M_4,\sigma_H]_F$	
	$\mathrm{Honest}(\hat{M}) \wedge \mathrm{Honest}(\hat{F}) \wedge \mathrm{Honest}(\hat{H}) \supset$	
	$\mathrm{Receive}(H,(\hat{F},\hat{H},M_3,\sigma_F)) \wedge \mathrm{Computes}(H,HASH(ID_{MN} \parallel N_{HA}))$	(12)
	$\mathrm{Computes}(H,HASH(ID_{MN} \parallel N_{HA})) \equiv \mathrm{Has}(\hat{H},ID_{MN}) \wedge \mathrm{Has}(\hat{H},N_{HA})$	(13)
(9), (13)	$\theta[FA]_F$	
	$\mathrm{Honest}(\hat{M}) \wedge \mathrm{Honest}(\hat{F}) \wedge \mathrm{Honest}(\hat{H}) \supset \phi_{anony}$	(14)

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the editor for their constructive comments that have helped us to improve the presentation of this paper.

REFERENCES

[1] C. Politis, K. A. Chew, N. Akhtar, M. Georgiades, R. Tafazolli, and T. Dagiuklas, “Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks," *IEEE Wireless Commun.*, vol. 11, no. 4, pp. 76-88, Aug. 2004.

[2] S. J. Kwon, S. Y. Nam, H. Y. Hwang, and D. K. Sung, “Analysis of a mobility management scheme considering battery power conservation in IP-based mobile networks," *IEEE Trans. Veh. Technol.*, vol. 53, no. 6, pp. 1882-1890, Nov. 2004.

[3] C. Perkins, “IP mobility support," IETF RFC 2002, Oct. 1996.

[4] C. Perkins, “IP mobility support for IPv4," IETF RFC 3344, Aug. 2002.

[5] H. C. Chao and C. Y. Huang, “Micro-mobility mechanism for smooth handoffs in an integrated ad-hoc and cellular IPv6 network under high-speed movement," *IEEE Trans. Veh. Technol.*, vol. 52, no. 6, pp. 1576-1593, Nov. 2003.

[6] J. Xie and L. F. Akyildiz, “A novel distributed dynamic location management scheme for minimizing signal costs in mobile IP," *IEEE Trans. Mobile Comput.*, vol. 1, no. 3, pp. 163-175, July-Sept. 2002.

[7] W. Haitao and Z. Shaoren, “The security issues and countermeasures in mobile IP," in *Proc. IEEE ICII'01*, vol. 5, pp. 122-127, 29 Oct. 2001.

[8] J. Zao, S. Kent, J. Gahm, G. Troxel, M. Condell, P. Helinek, N. Yuan, and I. Castineyra, “A public-key based secure mobile IP," *Wireless Netw.*, pp. 373-390, May 1999.

[9] S. Jacobs, “Mobile IP public key based authentication," Internet Draft, <draft-jacobs-mobileip-pki-auth-03.txt>, Aug. 2001. Expired.

[10] J. P. Yoo, K. Kim, H. Choo, J. I. Lee, and J. S. Song, “Secure and scalable mobile IP registration scheme using PKI," in V. Kumar *et al.* (eds.): *ICCSA 2003*, *LNCS 2668*, pp. 220-229. Springer-Verlag, 2003.

[11] Sufatrio and K. Y. Lam, “Mobile IP registration protocol: a security attack and new secure minimal pubic-key based authentication," in *Proc. IEEE Int. Symp. Parallel Architectures 1999*, Sept. 1999.

[12] S. Chung and K. Chae, “An efficient public-key based authentication with mobile-IP in e-commerce," in *Proc. IEEE Int. Conf. Parallel Processing 2000*, 2000.

[13] C. C. Yang, M. S. Hwang, J. W. Li, and T. Y. Chang, “A solution to mobile IP registration for AAA," in J. Lee and C. H. Kang (eds.): *CIC 2002*, *LNCS 2524*, pp. 329-337. Springer-Verlag, 2003.

[14] M. Mufti and A. Khanum, “Design and implementation of a secure mobile IP protocol," in *Proc. IEEE Int. Conf. Netw. Commun. 2004*, pp. 53-57, June 2004.

[15] C. Y. Yang and C. Y. Shiu, “A secure mobile IP registration protocol," *International J. Netw. Security*, vol. 1, no. 1, pp. 38-45, July 2005.

[16] D. Johnson, C. Perkins, and J. Arkko, “Mobility support in mobile IPv6," IETF RFC 3775, June 2004.

[17] H. Haverinen, N. Asokan, and T. Maattanen, “Authentication and key generation for mobile IP using GSM authentication and roaming," in *Proc. IEEE ICC'01*, vol. 8, pp. 2453-2457, June 2001.

[18] D. H. Choi, H. Kim, and K. Jung, “A secure mobile IP authentication based on identification protocol," in *Proc. IEEE ISPACS 2004*, pp. 709-712, Nov. 2004.

[19] B. G. Lee, D. H. Choi, H. G. Kim, S. W. Sohn, and K. H. Park, “Mobile IP and WLAN with AAA authentication protocol using Identity-based cryptography," in *Proc. IEEE ICT'03*, vol. 1, pp.597-603, 23 Feb. 2003.

[20] K. C. Jeong, H. Choo, and S. Y. Ha, “ID-based secure session key exchange scheme to reduce registration delay with AAA in mobile IP networks," in V. S. Sunderam *et al.* (eds.): *ICCS 2005*, *LNCS 3515*, pp. 510-518. Springer-Verlag, 2005.

[21] A. Shamir, “Identity-based cryptosystems and signature schemes," in G. R. Blakley and D. Chaum (eds.): *Advances in Cryptology-CRYPTO'84*, *LNCS 196*, pp. 47-53. Springer-Verlag, 1985.

[22] D. Boneh and M. K. Franklin, “Identity-based encryption from the Weil pairing," in J. Kilian (ed.): *Advances in Cryptology-CRYPTO'01*, *LNCS 2139*, pp. 213-229. Springer-Verlag, 2001.

[23] R. W. Zhu, G. Yang, and D. S. Wong, “An efficient Identity-based key exchange protocol with KGS forward security for low-power devices," in X. Deng and Y. Ye (eds.): *WINE 2005*, *LNCS 3828*, pp. 500-509. Springer-Verlag, 2005. (The last edition is published in *Theoretical Computer Science*, vol. 378, no. 2, pp. 198-207, Elsevier, June 2007.)

[24] J. Zhu and J. Ma., “A new authentication scheme with anonymity for wireless environments," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 231-235, 2004.

[25] K. Mangipudi and R. Katti, “A hash-based strong password authentication protocol with user anonymity," *International J. Netw. Security*, vol. 2, no. 3, pp. 205-209, May 2006.

[26] A. Datta, “Security analysis of network protocols compositional reasoning and complexity-theoretic foundations," Ph.D. dissertation, Dept. of Computer Science, Standford Univ., Stanford, Calif., 2005.

[27] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, “Efficient authentication and key distribution in wireless IP networks," *IEEE Wireless Commun.*, vol. 10, no. 6, pp. 52-61, Dec. 2003.

[28] P. Calhoun, T. Johansson, C. Perkins, and P. McCann, “Diameter MIPv4 application," IETF RFC 4004, Aug. 2005.

[29] C. Perkins and P. Calhoun, “Authentication, authorization, and accounting (AAA) registration keys for mobile IP," IETF RFC 3957, Mar. 2005.

[30] H. Krawczyk, M. Bellare, and R. Canetti, “HMAC: keyed-hashing for message authentication," IETF RFC 2104, Feb. 1997.

[31] W. Mao, *Modern Cryptography: Theory and Practice*. Upper Saddle River, NJ: Prentice Hall, pp. 364-367, 2004.

[32] C. Perkins and P. Calhoun, “Mobile IPv4 challenge/response extensions," IETF RFC 3012, Nov. 2000.

[33] S. G. Choi and K. Kim, “Authentication and payment protocol preserving location privacy in mobile IP," in *Proc. IEEE GLOBECOM 2003*, vol. 3, pp. 1410-1414, Dec. 2003.

[34] C. He, M. Sundararajan, A. Datta, A. Derek, and J. C. Mitchell, “A modular correctness proof of TLS and IEEE 802.11i," in *Proc. 12th ACM Conf. Computer Commun. Security*, pp. 2-15, Nov. 2005. (Invited to ACM Trans. Inf. Syst. Security, Special Issue Sel. Papers from CCS'05.)

[35] A. Datta, A. Derek, J. C. Mitchell, and A. Roy, “Protocol composition logic (PCL)," *Electronic Notes Theoretical Computer Science*, vol. 172, pp. 311-358, Apr. 2007.

[36] L. Dang, W. Kou, J. Zhang, X. Cao, and J. Liu, "Improvement of mobile IP registration protocols in mobile wireless networks," submitted to *IEEE Trans. Mobile Comput.*, unpublished.

[37] P. G. Argyroudis, R. Verma, H. Tewari, and D. O'Mahony, "Performance analysis of cryptographic protocols on handheld devices," in *Proc. 3rd IEEE Int. Symp. Netw. Computing Applications*, Cambridge, MA, pp. 169-174, Aug. 2004.

[38] W. Dai, "Speed comparison of popular crypto algorithms," Crypto++ 5.2.1 Benchmarks, July 2004. [Online]. Available: http://www.weidai.com/index.html.

[39] H. Orman and P. Hoffman, "Determining strengths for public keys used for exchanging symmetric keys," IETF RFC 3766, Apr. 2004.

[40] S. L. M. B Paulo, Y. K. Hae, L. Ben, and S. Michael, "Efficient algorithms for pairing-based cryptosystems," in M. Yung (ed.): *CRYPTO 2002*, *LNCS 2442*, pp. 354-369. Springer-Verlag, 2001.

[41] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable Secure Comput.*, vol. 3, no. 4, pp. 386-399, Oct.-Dec. 2006.

[42] E. R. Verheul, "Self-blindable credential certificates from the weil pairing," in C. Boyd (ed.): *ASIACRYPT 2001*, *LNCS 2248*, pp. 533-551. Springer-Verlag, 2001.

Lanjun Dang received her M.E. degree and PH.D. degree in Communication and Information Systems from Xidian University, Xi'an, China, in 2005 and 2008, respectively. During her pursuit of Ph.D. degree, she was with the State Key Laboratory of Integrated Services and Networks and her research interests included the security of mobile IP networks and information security. Presently, she is with the Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University and focuses on the security aspect of mobile IP and next generation mobile communication.

Weidong Kou received his M.S. degree in Applied Mathematics in 1982 from Beijing University of Posts and Telecommunications and Ph.D. degree in Electrical Engineering in 1985 from Xidian University, respectively. Prof. Kou is a Senior Member of IEEE. Prof. Kou has authored/edited seven books published by Springer, IBM Press, and Kluwer, in the areas of e-commerce, security, and multimedia technologies, and published over 100 papers on journals and conferences, including papers in prestigious journals such as IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON SIGNAL PROCESSING, and IEEE TRANSACTIONS ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING. He has over 20 issued patents from US, Canada, Europe and Asia countries. He has received various invention achievement and technical excellence awards from IBM, AT&T, and Siemens. He served as a member of American national standard committees, ANSI X9B9 (Financial Image Interchange) and ANSI X3L3 (JPEG and MPEG), for more than four years. He has also served as a Guest Editor of special issues on e-commerce for the International Journal on Digital Libraries. Prof. Kou was the General Chair and Program Chair for a number of international conferences, including 2004 IEEE International conference on e-Commerce Technology for Dynamic e-Business. Prof. Kou was Director of the State Key Laboratory of Integrated Service Networks, and Dean of the School of Computer Sciences in Xidian University. Presently, he is a Technical Executive and Chief Architect of IBM Software Group in Greater China Group. He also serves as Adjunct Professor at the University of Maryland Baltimore County, USA.

Hui Li received B.Sc. degree from Fudan University in 1990, M.A.Sc. and Ph.D. degrees from xidian University in 1993 and 1998. Since June 2005, he has been the professor in the school of Telecommunications Engineering, Xidian University, Xi'an Shaanxi, China. His research interests are in the areas of cryptography, wireless network security, information theory and network coding. He is a co-author of two books. He served as technique committee co-chairs of ISPEC 2009 and IAS 2009.

Junwei Zhang received the B.E. degree in Computer Science and Technology from Xidian University in 2004. Currently, he is pursuing his Ph.D. degree program in Computer Architecture at Xidian University. He is with the Key Laboratory of Computer Networks and Information Security (Ministry of Education) and his research interests include network security and cryptography.

Xuefei Cao received her M.E. degree and Ph.D. degree in Communication and Information Systems from Xidian University, Xiąŕan, China, in 2006 and 2008, respectively. During her pursuit of Ph.D. degree, she was with the State Key Laboratory of Integrated Services and Networks and her research interests included cryptology and communication security. Presently, she is with the SIM LAB of China Mobile Research Institute and focuses on the security aspect of SIM card and mobile communication services.

Bin Zhao received B.S. degree in Electrical and Communication Engineering and M.S. degree in Communication and Information Systems both with the highest honors from Xidian University, China, in 2005 and 2008 respectively. He was a research assistant in the State Key Laboratory of Integrated Service Networks, Xi'an, China, from 2005 to 2008. He is currently pursuing his Ph.D. degree in School of Electrical and Computer Engineering at Purdue University, USA. His research interests include image and signal processing, multimedia and information security, and digital communications and networks.

Kai Fan received his B.S., M.S. and Ph.D. degrees from Xidian University, P. R. China, in 2002, 2005, and 2007, respectively, in Telecommunication Engineering, Cryptography, and Telecommunication and Information System. He is working as an associate professor in the School of Telecommunication Engineering at Xidian University. He has published over 20 papers in journals and conferences. He has taken part in making seven national standard specifications. He has managed two national research projects. His research interests include e-commerce security and information security.