Computer Communications 32 (2009) 611–618

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Enhanced authentication scheme with anonymity for roaming service in global mobility networks

Chin-Chen Chang [a,b,*], Chia-Yin Lee [b], Yen-Chang Chiu [b]

[a] Department of Information Engineering and Computer Science Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan
[b] Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 62145, Taiwan

ARTICLE INFO

Article history:
Received 19 March 2008
Received in revised form 17 November 2008
Accepted 17 November 2008
Available online 6 December 2008

Keywords:
Authentication
Roaming
Key agreement
The forgery attack
Energy consumption

ABSTRACT

User authentication is an important security mechanism for recognizing legal roaming users. In 2006, Lee, Hwang, and Liao proposed an enhanced authentication scheme with user anonymity for roaming environments. This article shows that Lee–Hwang–Liao's scheme cannot provide anonymity under the forgery attack. Moreover, the heavy computation cost may consume battery power expeditiously for mobile devices. Therefore, we propose a novel authentication scheme to overcome these weaknesses that is efficient, secure, and suitable for battery-powered mobile devices in global mobility networks.

1. Introduction

Rapid development of wireless networks brings about many security problems in mobile communication. A special network environment provides personal communication users with a global roaming service called the global mobility network (GLOMONET) [1]. Through universal roaming technology, mobile users can access the services provided by the home agent in a foreign network.

How to authenticate mobile users in GLOMONET is an important security issue. Many user authentication schemes [1–8] have been proposed in recent years for the roaming environment. In 2004, Zhu and Ma [5] proposed a new authentication scheme using smart cards; Lin and Lee [6] later produced a possible attack to Zhu–Ma's scheme. In 2005, Lee, Chang, and Lin [7] proposed an improvement to overcome the weakness in Zhu–Ma's scheme. Recently, Lee, Hwang, and Liao [8] also pointed out some security weaknesses in Zhu–Ma's scheme and put forth an improved edition.

In this article, we show that Lee–Hwang–Liao's scheme suffers from the forgery attack, which is defined by Lin et al. [6,7]. Under this kind of attack, the real identity of roaming users will be exposed. Besides, mobile devices are powered by a battery and the constrained energy results in limited computation capability. In other words, asymmetric and symmetric cryptosystems are required to achieve the security requirement, which increases the computation cost and energy consumption of Lee et al.'s scheme. To improve these disadvantages, we propose an efficient authentication scheme with anonymity that uses low-cost functions such as one-way hash functions and exclusive-OR operations to achieve security goals. Having these features, it is more suitable for battery-powered mobile devices.

The remainder of this paper is organized as follows. In Section 2, we review Lee–Hwang–Liao's scheme and discuss its weakness. An efficient user authentication scheme is proposed in Section 3. Security discussions are described in Section 4. In Section 5, we compare the proposed scheme with previous. Finally, we make some conclusions in Section 6.

2. A review of previous works

In this section, we first briefly describe Lee–Hwang–Liao's scheme and then point out its weakness. This scheme cannot protect user privacy against all possible threats. Moreover, the communication between the mobile user and the foreign agent is vulnerable.

2.1. Lee–Hwang–Liao's scheme

In 2006, Lee, Hwang and Liao showed that Zhu–Ma's scheme has some security weaknesses and proposed an improved scheme. Table 1 lists all of the notations used in Lee et al.'s scheme.

There are three phases in their scheme: the initialization phase, the first phase, and the second phase. Three entities are involved:

* Corresponding author. Address: Department of Information Engineering and Computer Science Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.
E-mail addresses: ccc@cs.ccu.edu.tw (C.-C. Chang), licy@cs.ccu.edu.tw (C.-Y. Lee), cyc94@cs.ccu.edu.tw (Y.-C. Chiu).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.11.032

Table 1
Some notations of Lee–Hwang–Liao's scheme.

Notations	Descriptions
MN	A mobile user
PW_{MN}	A password of MN
T_X	The timestamp generated by an entity X
HA	The home agent of a mobile user
FA	The foreign agent of a foreign network
ID_X	The identity of an entity X
$Cert_X$	The certificate of an entity X defined in X.509
$(M)_K$	Encryption of a message M using a symmetric key K
$E_K(M)$	Encryption of a message M using an asymmetric key K
$h(.)$	A one-way hash function
$\|\|$	A concatenation operator
$\oplus$	A XOR operator

MN is a mobile user; FA is the agent of the foreign network; and HA is the home agent of the mobile user MN. When MN roams in a new foreign network, FA must authenticate the identity of MN through MN's home agent HA. We will now describe Lee–Hwang–Liao's scheme in detail.

We will now describe Lee–Hwang–Liao's scheme in detail. In the initialization phase, a mobile user MN registers with the home agent HA and obtains a smart card through a secure channel for future service. In the first phase, the foreign agent FA authenticates the mobile user MN and issues a temporary certificate. Additionally, a session key is established between the foreign agent FA and the mobile user MN. In the second phase, the foreign agent FA serves for the mobile user MN when MN roams in the foreign network, and they can modify their session key simultaneously. Detailed processes are given in the following sections.

2.1.1. Initialization phase

First, a new mobile user MN submits his identity ID_{MN} to the home agent HA. Then, HA generates a password for MN by calculating $PW_{MN} = h(N||ID_{MN})$, where N is a long-term secret key of HA. Finally, HA delivers PW_{MN} and a smart card, which contains ID_{HA}, r and a one-way hash function $h(.)$, to MN through a secure channel. Note that $r = h(N||ID_{HA}) \oplus h(N||ID_{MN}) \oplus ID_{HA} \oplus ID_{MN}$, where ID_{HA} is the identity of HA. Fig. 1 illustrates the initialization phase.

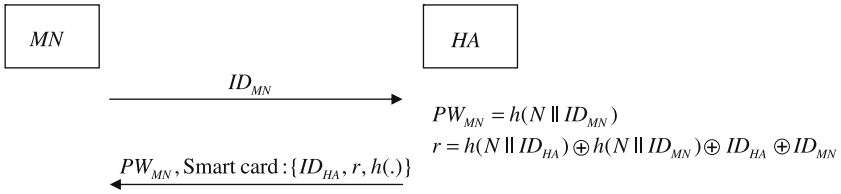

Fig. 1. Initialization phase of Lee–Hwang–Liao's scheme.

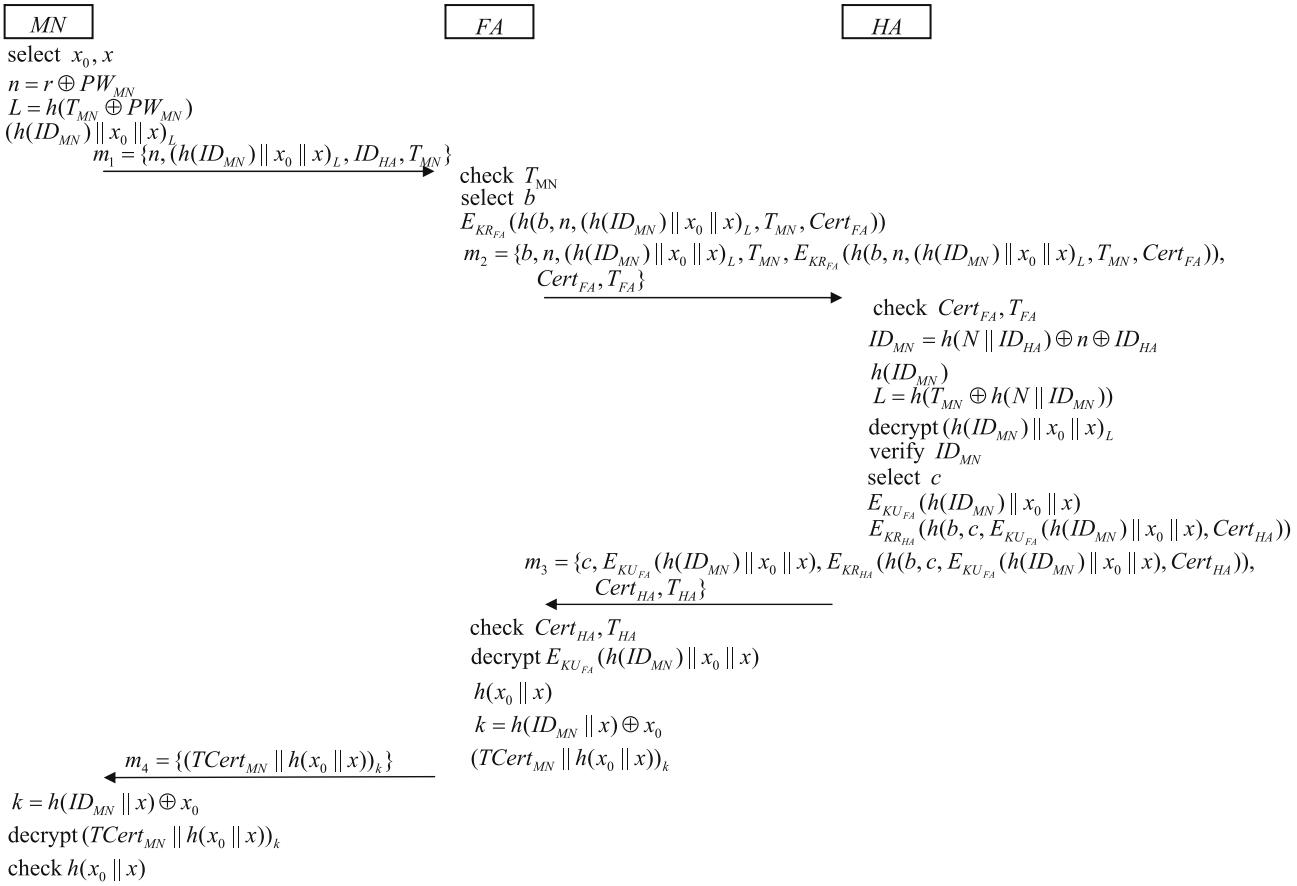

Fig. 2. First phase of Lee–Hwang–Liao's scheme.

2.1.2. First phase

When roaming in the foreign network, the mobile user *MN* sends some messages to the foreign agent *FA* for mutual authentication. Then, *FA* generates a temporary certificate to *MN* for future authentication. If *MN* remains unchanged in the same area, it authenticates *FA* with this temporary certificate. We illustrate the first phase in Fig. 2, and the detailed steps are described as follows:

(1) *MN* enters password PW_{MN} to the device, which generates two random secret parameters x_0 and x. *MN* computes $n = r \oplus PW_{MN}$ and generates temporary key $L = h(T_{MN} \oplus PW_{MN})$, where T_{MN} is *MN*'s timestamp.
(2) *MN* encrypts $(h(ID_{MN})||x_0||x)$ with L using a symmetric cryptosystem and transmits the message $\{n, (h(ID_{MN}) \,||\, x_0 \,||\, x)_L, ID_{HA}, T_{MN}\}$ to *FA*.
(3) Upon receiving messages from *MN*, *FA* checks the timestamp T_{MN} with the current date and time. If it is not valid, then *FA* terminates the login request. Otherwise, *FA* performs the following steps.
(4) *FA* generates a secret random number b and computes a signature $E_{KR_{FA}}(h(b, n, (h(ID_{MN})||x_0||x)_L, T_{MN}, Cert_{FA}))$ using the private key KR_{FA}. After that, *FA* transmits $\{b, n, (h(ID_{MN})||x_0||x)_L, T_{MN}\}$, the signature with his certificate $Cert_{FA}$, and the current timestamp T_{FA} to *MN*'s home agent *HA* according to ID_{HA}.
(5) After receiving the transmitted messages from *FA*, *HA* verifies timestamp T_{FA} and certificate $Cert_{FA}$. If both are valid, then *HA* verifies $\{b, n, (h(ID_{MN})||x_0||x)_L, T_{MN}\}$ according to the signature $E_{KR_{FA}}(h(b, n, (h(ID_{MN})||x_0||x)_L, T_{MN}, Cert_{FA}))$ signed by *FA*. If the result is valid, *HA* obtains identity ID_{MN} by calculating $ID_{MN} = h(N||ID_{HA}) \oplus n \oplus ID_{HA}$.
(6) The temporary key L can be derived by computing $L = h(T_{MN} \oplus h(N||ID_{MN}))$. With this temporary key L, $(h(ID_{MN})||x_0||x)$ is obtainable.
(7) By checking the hashing value $h(ID_{MN})$, *HA* can verify *MN*'s identity. If ID_{MN} is legitimate, *HA* encrypts $(h(ID_{MN})||x_0||x)$ using *FA*'s public key $E_{KU_{FA}}$.
(8) *HA* generates a secret random number c and computes a signature $E_{KR_{HA}}(h(b, c, E_{KU_{FA}}(h(ID_{MN})||x_0||x), Cert_{HA}))$ using his private key $E_{KR_{HA}}$.
(9) *HA*sends the following message to *FA*:

$$\{c, E_{KU_{FA}}(h(ID_{MN})||x_0||x), E_{KR_{HA}}(h(b, c, E_{KU_{FA}}(h(ID_{MN})||x_0||x), Cert_{HA})), Cert_{HA}, T_{HA}\}.$$

(10) Upon receiving this message, *FA* checks the validity of timestamp T_{HA} and certificate $Cert_{HA}$. If both are valid, then *FA* decrypts $E_{KU_{FA}}(h(ID_{MN})||x_0||x)$ using private key $E_{KR_{FA}}$ to obtain $(h(ID_{MN})||x_0||x)$.
(11) *FA* generates a temporary certificate $TCert_{MN}$, which includes the period of validity and other information to *MN*. Finally, *FA* transmits the ciphertext $(TCert_{MN}||h(x_0||x))_k$ to *MN*, where the encryption key is $k = h(ID_{MN}||x) \oplus x_0$. After *MN* has been authenticated, *FA* establishes a session key k.
(12) Finally, *MN* computes $k = h(ID_{MN}||x) \oplus x_0$ and then decrypts $(TCert_{MN}||h(x_0||x))_k$. By checking the hash value $h(x_0||x)$, *MN* can ensure that *FA* is authenticated by *HA*. Thus, the mutual authentication process is complete.

2.1.3. Second phase

In this phase, we assume that *MN* stays in the same area. This means that the foreign agent *FA* will not change. When *MN* visits *FA* at the ith session, the following process is conducted to authenticate *FA*:

(1) *MN* generates a new secret random number x_i and modifies the session key $k_i = h(ID_{MN}) \oplus x_{i-1}$, for $i = 1, 2, \ldots, n$.
(2) *MN* encrypts $(x_i||TCert_{MN}||OtherInformation)$ with the ith session key k_i.
(3) *MN* sends the message $\{TCert_{MN}, (x_i||TCert_{MN}||Other\ Information)_{k_i}\}$ to *FA*.
(4) Upon receiving the message transmitted from *MN*, *FA* checks the validity of certificate $TCert_{MN}$. If it is valid, *FA* computes the ith session key $k_i = h(ID_{MN}) \oplus x_{i-1}$ and then decrypts $(x_i||TCert_{MN}||OtherInformation)_{k_i}$. By verifying the $TCert_{MN}$, *FA* authenticates *MN*. Furthermore, *FA* stores x_i for later authentication.

2.2. Weaknesses of Lee–Hwang–Liao's scheme

Although Lee, Hwang, and Liao proposed an improved version of Zhu–Ma's scheme, some security weaknesses remain. Under anonymity attacks, a legal mobile user can obtain another legal user's identity. Moreover, a legal user can forge another legal user to access the foreign network by stealing his or her smart card. We depict these two attacks as follows:

(1) A legal user*MN* can compute $h(N||ID_{HA}) = n \oplus ID_{HA} \oplus ID_{MN}$ to obtain $h(N||ID_{HA})$.
(2) When another legal user MN' communicates with *FA*, *MN* collects the parameter n' transmitted from MN'. With the knowledge of $h(N||ID_{HA})$, *MN* can obtain the real identity of MN' by computing $ID_{MN'} = n' \oplus h(N||ID_{HA}) \oplus ID_{HA}$. Thus, the anonymity feature cannot be realized.

If MN''s smart card is stolen by *MN*, the attacker *MN* can successfully forge MN' to communicate with *FA* through the following steps.

(1) *MN* inserts MN''s smart card into the terminal device and then enters the fake password $PW^* = 0$. The attacker can obtain r' by calculating $r' \oplus PW^* = r' \oplus 0 = r' = h(N||ID_{HA}) \oplus h(N||ID_{MN}) \oplus ID_{HA} \oplus ID_{MN'}$.
(2) Having parameters r', $h(N||ID_{HA})$, ID_{HA}, and $ID_{MN'}$, *MN* can derive MN''s real password $PW_{MN'}$ by calculating $PW_{MN'} = r' \oplus h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MN'}$. The attacker can then

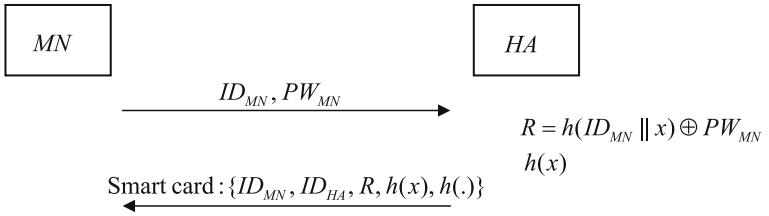

Fig. 3. Registration phase of the proposed scheme.

use *MN*'s smart card and password $PW_{MN'}$ to forge the identity of *MN'* successfully and to access service in the foreign network.

Lee–Hwang–Liao's scheme uses timestamps to avoid replay attacks [9]. However, it is difficult to synchronize the clock when each entity is located in different time zones. Hence, additional synchronized time mechanisms are needed to adjust the clock between the two parties.

To solve the above-mentioned problems, we propose a novel authentication scheme with anonymity for the wireless environment. Our scheme uses nonces to avoid possible attacks and uses one-way hash functions to reduce the computation cost. Because only exclusive-OR operations and one-way hash functions are used, it is especially suitable for limited energy mobile devices.

3. Proposed scheme

Our scheme consists of three phases: registration, authentication, and session key establishment. Three entities are involved: the mobile user *MN*, the foreign agent *FA*, and the home agent *HA*. We assume that each *FA* and *HA* share a long-term common secret key K_{FH}. Here, K_{FH} can be established using any key agreement method, such as the Diffie–Hellman key agreement protocol [10]. Note that all secret keys $K_{FH_i}, (i = 1, 2, \ldots n)$ shared between FA_i, $(i = 1,2,\ldots n)$ and *HA* differ. *HA* needs a secure database to store these keys.

In the registration phase, a new mobile user *MN* submits his/her identity ID_{MN} and the selected password PW_{MN} to *HA* for registration. *HA* then performs the following steps:

(1) *HA* uses its private key x to generate the secret value R by computing $R = h(ID_{MN}||x) \oplus PW_{MN}$, where $h(.)$ is a collision free one-way hash function such as SHA [11].
(2) Compute the hashing value $h(x)$. *HA* issues a smart card containing $\{ID_{MN}, ID_{HA}, R, h(x), h(.)\}$ and delivers it to *MN* through a secure channel.

The handshake between *MN* and *HA* is depicted in Fig. 3.

We assume that a mobile user *MN* roams in a foreign network and tries to access service. Before providing services, the foreign agent *FA* needs to authenticate *MN* through *MN*'s home agent *HA*. For authentication, *MN* inserts his/her smart card into the device and enters password PW^*_{MN}. The card processes the following operations:

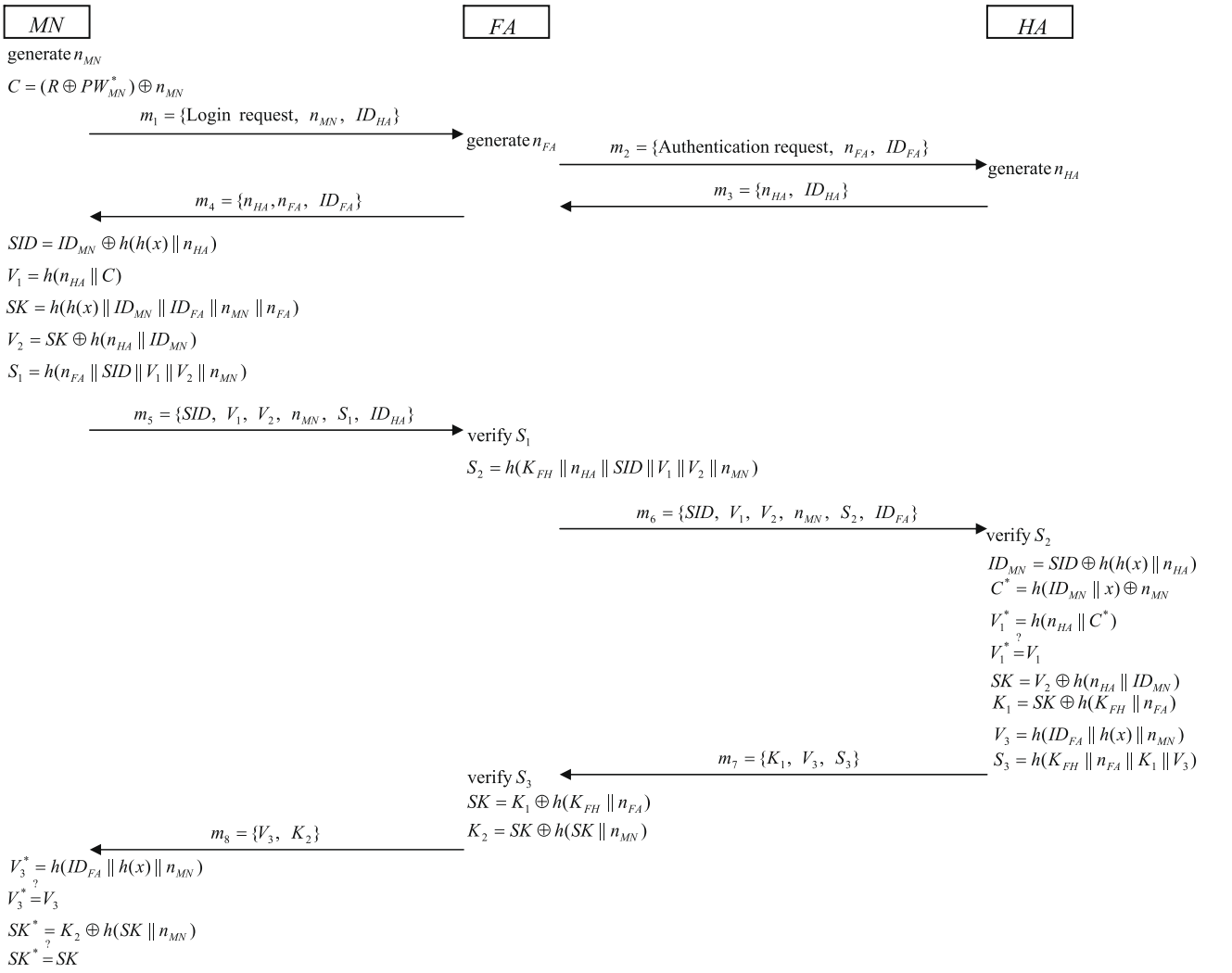

Fig. 4. Authentication and key establishment phases of the proposed scheme.

(1) Generate a nonce n_{MN} randomly.
(2) Calculate the parameter C by computing $C = (R \oplus PW^*_{MN}) \oplus n_{MN}$.

MN sends a login message $m_1 = \{Login\ request, n_{MN}, ID_{HA}\}$ to *FA* for authentication. "*Login request*" is the header of the message; this alerts a new session between *MN* and *FA*. Upon receiving m_1, *FA* records the nonce n_{MN} and obtains the information of the home agent *HA* by recognizing ID_{HA}. Then, *FA* generates a random nonce n_{FA} and sends an authentication message $m_2 = \{Authentication\ request, n_{FA}, ID_{FA}\}$ to *HA*, where "*Authentication request*" is the header of the message. This notifies *HA* to authenticate the roaming user *MN*.

After receiving the authentication request, *HA* checks ID_{FA} to determine whether it is an ally. If the result is valid, then *HA* generates a nonce n_{HA} and sends a message $m_3 = \{n_{HA}, ID_{HA}\}$ to *FA*. After receiving m_3, *FA* sends message $m_4 = \{n_{HA}, n_{FA}, ID_{FA}\}$ to *MN*.

MN will perform the following steps after receiving message m_4:

(1) Record the nonces n_{HA} and n_{FA}.
(2) Generate the shadow identity *SID* of *MN* by computing $SID = ID_{MN} \oplus h(h(x)||n_{HA})$.
(3) Compute the parameter $V_1 = h(n_{HA}||C)$.
(4) Generate the session key *SK* by computing $SK = h\ (h(x)||ID_{MN}||ID_{FA}||n_{MN}||n_{FA})$.
(5) Compute the parameter $V_2 = SK \oplus h(n_{HA}\ ||\ ID_{MN})$.
(6) Compute the hashing value $S_1 = h(n_{FA}||SID||V_1||V_2||n_{MN})$.
(7) Send message $m_5 = \{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$ to *FA*.

Upon receiving the message m_5, *FA* executes the following steps:

(1) Use the nonce n_{FA} with the received *SID*, V_1, V_2 and n_{MN} to compute the hashing value $S^*_1 = h(n_{FA}||SID||V_1||V_2||n_{MN})$, and check whether $S^*_1 \stackrel{?}{=} S_1$.
(2) Compute $S_2 = h(K_{FH}||n_{HA}||SID||V_1||V_2||n_{MN})$.
(3) Send *HA* message $m_6 = \{SID, V_1, V_2, n_{MN}, S_2, ID_{FA}\}$ to verify whether *MN* is legal.

After receiving message m_6, *HA* checks ID_{FA} to determine whether it is an ally. Then, *HA* uses the corresponding secret key K_{FH} and the nonce n_{HA} to compute $S^*_2 = h(K_{FH}||n_{HA}||SID||V_1||V_2||n_{MN})$ and to determine whether $S^*_2 \stackrel{?}{=} S_2$. If the result is valid, the identity of *FA* is authenticated, and *HA* will perform the following steps:

(1) Compute the hashing value $h(h(x)||n_{HA})$.
(2) Obtain the user's identity ID_{MN} by computing $ID_{MN} = SID \oplus h(h(x)||n_{HA})$.
(3) Verify the format of ID_{MN}. If the format is not valid, *HA* terminates the connection.
(4) Compute $C^* = n_{MN} \oplus h(ID_{MN}\ ||\ x)$.
(5) Use the nonce n_{HA} to compute $V^*_1 = h(n_{HA}||C^*)$ and then check whether $V^*_1 \stackrel{?}{=} V_1$. If they are equal, then password PW^*_{MN} equals PW_{MN}, and *HA* continues the procedure. Otherwise, it sends *FA* a message warning that *MN* is an illegal user.
(6) Obtain *SK* from V_2 by computing $SK = V_2 \oplus h(n_{HA}||ID_{MN})$.
(7) Compute $K_1 = SK \oplus h(K_{FH}||n_{FA})$, $V_3 = h(ID_{FA}||h(x)||n_{MN})$, and $S_3 = h(K_{FH}||n_{FA}||K_1||V_3)$.
(8) Send message $m_7 = \{K_1, V_3, S_3\}$ to *FA* to inform that *MN* is a legal user.

Having finished the above authentication processes, *FA* and *MN* will generate a common session key in the key establishment phase. With message m_7, *FA* uses the secret key K_{FH} and the nonce n_{FA} to compute $S^*_3 = h(K_{FH}||n_{FA}||K_1||V_3)$ and then checks whether $S^*_3 \stackrel{?}{=} S_3$. If it is valid, then *FA* performs the following steps:

(1) Obtain the session key *SK* by computing $SK = K_1 \oplus h(K_{FH}||n_{FA})$.
(2) Compute $K_2 = SK \oplus h(SK||n_{MN})$ and send message $m_8 = \{V_3, K_2\}$ to *MN*.

After receiving message m_8, *MN* computes $V^*_3 = h(ID_{FA}||h(x)||n_{MN})$ and checks whether $V^*_3 \stackrel{?}{=} V_3$. If the result is valid, then *FA* is a legal foreign agent, and*MN* computes $SK^* = K_2 \oplus h(SK||n_{MN})$. If $SK^* = SK$, *MN* is sure that *FA* also has a authenticated session key. Next, *MN* records the authenticated session key *SK* for future communications with *FA*. We describe the authentication phase and key establishment phase in Fig. 4.

4. Security discussions

The logical analysis proposed by Burrows et al. [12] is a useful model to prove the validity of authentication and key distribution protocols. In Section 4.1, we use Burrows et al.'s rules (BAN logic) to demonstrate the execution of the proposed scheme. In Section 4.2, we show that our scheme can withstand some possible attacks.

4.1. Authentication proof based on BAN logic

We use BAN logic to prove our authentication protocol. The symbols $h(x)$, $K_{FH,}$ and *SK* denote the secret keys; n_{MN}, n_{FA}, and n_{HA} are nonces. The main goal of our protocol is to establish a session key *SK* between mobile user *MN* and foreign agent *FA*. We use the following logical postulates to show that *MN* and *FA* can mutually authenticate and share session key *SK*.

MN **believes** $MN \overset{SK}{\leftrightarrow} FA$,
MN **believes** *FA* **believes** $MN \overset{SK}{\leftrightarrow} FA$,
FA **believes** $MN \overset{SK}{\leftrightarrow} FA$, and
FA **believes** *MN* **believes** $MN \overset{SK}{\leftrightarrow} FA$.

According to the analytic procedures of BAN logic, the protocol rounds need to be transformed into an idealized form. We first define the following constructs:

(X, Y): formula X or formula Y is one part of formula (X, Y),
$\langle X \rangle_Y$: formula X combined with a secret parameter Y,
$\{X\}_K$: formula X encrypted by key K,
$P \overset{K}{\leftrightarrow} Q$: P and Q may use the shared key K to communicate. Here K will never be discovered by anyone except P and Q,
$P \overset{S}{\Longleftrightarrow} Q$: the formula S is secret known only to P and Q. Only P and Q may use S to prove their identities to each other.

We use BAN logic to transform our protocol, illustrated in Fig. 4, into the idealized form. The messages m_1,m_2, m_3, and m_4 are omitted, since they do not contribute logical properties of BAN logic. Other idealized messages are illustrated as follows:

$m_5.MN \rightarrow FA : \langle(\langle\langle ID_{MN}\rangle_{(h(x),n_{HA})}, \langle n_{HA}, h(ID_{MN}||x)\rangle_{h(ID_{MN}||x)}, \langle MN \overset{SK}{\leftrightarrow} FA\rangle_{(n_{HA},ID_{MN})}\rangle, n_{FA}\rangle,$
$m_6.FA \rightarrow HA : \langle(\langle\langle ID_{MN}\rangle_{(h(x),n_{HA})}, \langle n_{HA}, h(ID_{MN}||x)\rangle_{h(ID_{MN}||x)}, \langle MN \overset{SK}{\leftrightarrow} FA\rangle_{(n_{HA},ID_{MN})}\rangle, n_{HA}\rangle\rangle_{K_{FH}},$
$m_7.HA \rightarrow FA : \langle\langle MN \overset{SK}{\leftrightarrow} FA\rangle_{(K_{FH},n_{FA})}, \langle ID_{FA}, n_{MN}\rangle_{h(x)}, n_{FA}\rangle_{K_{FH}},$
$m_8.FA \rightarrow MN : \langle ID_{FA}, n_{MN}\rangle_{h(x)}, \langle MN \overset{SK}{\leftrightarrow} FA\rangle_{(SK,n_{MN})}.$

To analyze the proposed protocol, we make the following assumptions:

A1. MN **believes fresh**(n_{MN}),
A2. FA **believes fresh**(n_{FA}),
A3. HA **believes fresh**(n_{HA}),
A4. MN **believes** $MN \overset{h(x)}{\Longleftrightarrow} HA$,
A5. HA **believes** $MN \overset{h(x)}{\Longleftrightarrow} HA$,
A6. FA **believes** $FA \overset{K_{FH}}{\Longleftrightarrow} HA$,
A7. HA **believes** $FA \overset{K_{FH}}{\Longleftrightarrow} HA$,
A8. MN **believes** $MN \overset{SK}{\leftrightarrow} FA$,
A9. FA **believes** (MN **controls** $MN \overset{SK}{\leftrightarrow} FA$),
A10. HA **believes** (MN **controls** $MN \overset{SK}{\leftrightarrow} FA$),
A11. HA **believes** (MN **controls** ID_{MN}),
A12. ID_{MN} is unknown for anyone except the mobile user MN.

Assumptions A1, A2, and A3 are basic assumptions of BAN logic. We analyze the idealized form of the proposed protocols using those assumptions and rules of BAN logic. We show the main steps of the proof as follows:

By m_5 and A2, we apply the *freshness conjunctions* rule to derive

$$FA \textbf{ believes fresh } (\langle ID_{MN} \rangle_{(h(x),\, n_{HA})},\ (n_{HA},\ (h(ID_{MN} \,||\, x),\ n_{MN})),\ \langle MN \overset{SK}{\leftrightarrow} FA \rangle_{(n_{HA}, ID_{MN})}) \quad \text{(Statement1)}$$

By m_6 and A7, we apply the *message-meaning* rule to derive

$$HA \textbf{ believes } FA \textbf{ said } ((\langle ID_{MN} \rangle_{(h(x), n_{HA})}, \langle n_{HA}, h(ID_{MN} \| x) \rangle_{h(ID_{MN} \| x)},\ \langle MN \overset{SK}{\leftrightarrow} FA \rangle_{(n_{HA}, ID_{MN})}), n_{HA}). \quad \text{(Statement 2)}$$

By (Statement 2) and A3, we apply the *nonce-verification* rule to derive

$$HA \textbf{ believes } FA \textbf{ believes } (\langle ID_{MN} \rangle_{(h(x), n_{HA})}, \langle n_{HA}, h(ID_{MN} \| x) \rangle_{h(ID_{MN} \| x)},\ \langle MN \overset{SK}{\leftrightarrow} FA \rangle_{(n_{HA}, ID_{MN})}). \quad \text{(Statement3)}$$

By (Statement 3), we apply the rule of BAN logic to break conjunctions then produce

$$HA \textbf{ believes } FA \textbf{ believes } \langle ID_{MN} \rangle_{(h(x),\, n_{HA})}, \quad \text{(Statement 4)}$$

$$HA \textbf{ believes } FA \textbf{ believes } \langle n_{HA}, (h(ID_{MN} \| x) \rangle_{h(ID_{MN} \| x)}, \text{ and} \quad \text{(Statement 5)}$$

$$HA \textbf{ believes } FA \textbf{ believes } \langle MN \overset{SK}{\leftrightarrow} FA \rangle_{(n_{HA},\, ID_{MN})}. \quad \text{(Statement 6)}$$

By A3, A5, and (Statement 4), we apply the *message-meaning* rule and the *nonce-verification* rule to deduce

$$HA \textbf{ believes } MN \textbf{ believes } ID_{MN}. \quad \text{(Statement 7)}$$

By A11 and (Statement 7), we apply the *jurisdiction* rule to derive

$$HA \textbf{ believes } ID_{MN}. \quad \text{(Statement 8)}$$

From A12 and (Statement 8), we can deduce the following rule

$$HA \textbf{ believes } MN \overset{ID_{MN}}{\Longleftrightarrow} HA. \quad \text{(Statement 9)}$$

By A3, (Statement 6), and (Statement 9), we apply the *message-meaning* rule and the *nonce-verification* rule to deduce

$$HA \textbf{ believes } MN \textbf{ believes } MN \overset{SK}{\leftrightarrow} FA. \quad \text{(Statement 10)}$$

By A10 and (Statement 10), we apply the *jurisdiction* rule to derive

$$HA \textbf{ believes } MN \overset{SK}{\leftrightarrow} FA. \quad \text{(Statement 11)}$$

By m_7 and A6, we apply the *message-meaning* rule to derive

$$FA \textbf{ believes } HA \textbf{ said } (\langle MN \overset{SK}{\leftrightarrow} FA \rangle_{(K_{FH},\, n_{FA})}, \langle ID_{FA}, n_{MN} \rangle_{h(x)}, n_{FA}). \quad \text{(Statement 12)}$$

By A2 and (Statement12), we apply the *nonce-verification* rule to derive

$$FA \textbf{ believes } HA \textbf{ believes } (\langle MN \overset{SK}{\leftrightarrow} FA \rangle_{(K_{FH},\, n_{FA})}, \langle ID_{FA}, n_{MN} \rangle_{h(x)}). \quad \text{(Statement 13)}$$

By (Statement 13), we break the conjunctions to produce

$$FA \textbf{ believes } HA \textbf{ believes } (\langle MN \overset{SK}{\leftrightarrow} FA \rangle_{(K_{FH}, n_{FA})}) \quad \text{and (Statement 14)}$$

$$FA \textbf{ believes } HA \textbf{ believes } \langle ID_{FA}, n_{MN} \rangle_{h(x)}. \quad \text{(Statement 15)}$$

By A2, A6, and (Statement 14), we apply the *message-meaning* rule and the *nonce-verification* rule to deduce

$$FA \textbf{ believes } HA \textbf{ believes } \langle MN \overset{SK}{\leftrightarrow} FA \rangle. \quad \text{(Statement 16)}$$

By (Statement 10) and (Statement 16), we can imply the following statement

$$FA \textbf{ believes } MN \textbf{ believes } \langle MN \overset{SK}{\leftrightarrow} FA \rangle. \quad \text{(Statement 17)}$$

By A9 and (Statement 17), we apply *jurisdiction* rule to derive

$$FA \textbf{ believes } \langle MN \overset{SK}{\leftrightarrow} FA \rangle. \quad \text{(Statement 18)}$$

By A1, A8, and m_8, we apply the *message-meaning* rule and the *nonce-verification* rule to derive

$$MN \textbf{ believes } FA \textbf{ believes } MN \overset{SK}{\leftrightarrow} FA. \quad \text{(Statement 19)}$$

By A8, (Statement 17), (Statement 18), and (Statement 19), we prove that the proposed protocol establishes a secure session key between MN and FA. Moreover, we also prove that MN and FA authenticate each other using our protocol.

4.2. Withstanding possible attacks

We show that the proposed scheme can resist certain possible attacks. Assume that wireless communications are insecure and that there exists an adversary *Eve*. She can intercept all messages communicated among MN, FA, and HA. In addition, we assume that *Eve* can obtain or steal legal user MN's smart card. Based on these assumptions, *Eve* might execute certain attacks to destroy the proposed scheme.

4.2.1. Replay attacks

Eve can collect messages $m_1, m_2, \ldots, m_8$, which are transmitted among MN, FA, and HA. *Eve* might replay the old message $m_1 = \{Login\ request, n_{MN}, ID_{HA}\}$ to FA and receive the message

Table 2
Performance comparisons.

Scheme	Ours	Lee–Hwang–Liao's (2006)	Zhu–Ma's (2004)
MN	7*Hash* + 5*XOR*	4*Hash* + 3*XOR* + 2*Sym*	2*Hash* + 3*XOR* + 2*Sym*
FA	3*Hash* + 2*XOR*	4*Hash* + 1*XOR* + 2*Sym* + 2*Asym*	2*Hash* + 1*XOR* + 1*Sym* + 2*Asym*
HA	8*Hash* + 3*XOR*	5*Hash* + 3*XOR* + 1*Sym* + 2*Asym*	5*Hash* + 3*XOR* + 1*Sym* + 3*Asym*
Total	18*Hash* + 10*XOR*	13*Hash* + 7*XOR* + 5*Sym* + 4*Asym*	9*Hash* + 7*XOR* + 4*Sym* + 5*Asym*
Time complexity	$O(1)$	$O(n^3)$	$O(n^3)$
Rounds	8	4	4

$m_4 = \{n_{HA}, n_{FA}, ID_{FA}\}$ from *FA*. Upon receiving $m_4 = \{n_{HA}, n_{FA}, ID_{FA}\}$, *Eve* replays the message $m_5 = \{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$ to *FA*. After receiving $m_5 = \{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$, *FA* transmits the message $m_6 = \{SID, V_1, V_2, n_{MN}, S_2, ID_{FA}\}$ to *HA*. However, *HA* cannot derive the correct identity ID_{MN}, because the nonce n_{HA} contained in *SID* is not the same as the received one. Without the correct identity of *MN*, the equation $V_1^* = V_1$ will not hold. Thus, *HA* will know that the mobile user is not valid. As a result, *HA* transmits a warning message to *FA* and terminates the connection. Thus, our scheme can resist replay attacks by using random nonces.

4.2.2. Forgery attacks

Eve might intercept the messages $m_1 = \{Login\ request, n_{MN}, ID_{HA}\}$ and $m_5 = \{SID, V_1, V_2, n_{MN}, S_1, ID_{HA}\}$ transmitted from a legal mobile user *MN* in the previous sessions. *Eve* replays the login request m_1 to *FA*, forges a message $m_5^* = \{SID^*, V_1^*, V_2^*, n_{MN}^*, S_1^*, ID_{HA}\}$, and sends m_5^* to *FA*. *FA* will transmit the message $m_6 = \{SID^*, V_1^*, V_2^*, n_{MN}^*, S_2, ID_{FA}\}$ to *HA*. Upon receiving the message m_6 sent by *FA*, *HA* determines if the message is valid. Verification will fail, because $V_1^* \neq V_1$. *HA* will terminate this connection. Hence, resistance to the forgery attack is ensured.

4.2.3. Lost smart card

Although *Eve* can obtain or steal a legal mobile user *MN*'s smart card, she still cannot impersonate *MN* to login to the server. Since *Eve* does not have *MN*'s correct password, she can only guess the password at random. Without the correct password, the smart card computes incorrect parameters $\{SID, V_1, V_2\}$, so the identity will not be successfully authenticated by *HA*.

4.2.4. Known-key attacks

Our scheme uses the ephemeral nonces n_{MN}, n_{FA} and n_{HA} in each session. Nonces are random and independent in each session. Moreover, the session key $SK = h(h(x) \| ID_{MN} \| ID_{FA} \| n_{MN} \| n_{FA})$ is established by the legal user's smart card and *HA* in each session; thus, the session keys are also independent. Therefore, the knowledge of previous session keys does not help to derive a new session key, and vice versa. As a result, the known-key attack does not work in the proposed scheme.

5. Comparison with related works

This section compares the performance, energy consumption, and functionality of the proposed scheme with that of related works and our scheme. Table 2 shows the performance comparison results. The following notations are used in Table 2: *Hash* is the operation of the one-way hash function; *XOR* is the operations of exclusive-OR; *Sym* is the operation of symmetric encryption/decryption; and *Asym* is the encryption/decryption operation or the signature operation by using the asymmetric cryptosystem.

Table 3
Functionality comparisons.

Scheme	Ours	Lee–Hwang–Liao's (2006)	Zhu–Ma's (2004)
Energy consumption	Low	High	High
User anonymity	Yes	No	No
No password table	Yes	Yes	Yes
Mutual authentication	Yes	Yes	No
Session key establishment	Yes	Yes	Yes
Forgery attacks resistance	Yes	No	No
No synchronized time mechanisms required	Yes	No	No
The password is chosen by the user freely	Yes	No	No

The well-known SHA-1, AES (Rijndael) [13], and 1024-bit RSA [14] stand for one-way hash function, the symmetric cryptosystem, and the asymmetric cryptosystem, respectively. From the experimental results of related researches [15–18], we know that one-way hash functions are more efficient than symmetric cryptosystems and asymmetric cryptosystems.

Because the procedures of SHA are *XOR* operations and rotation operations, calculating a hashing value using SHA can be bounded in a constant time; that is, the time complexity of calculating a hashing value is $O(1)$. By analyzing the algorithm of a symmetric cryptosystem such as AES, we find that more than 80% [19] computation overhead results from the *MixColumns* procedure. Since the *MixColumns* executes the operation of matrix multiplication, the time complexity of matrix multiplication is $O(n^{2.81})$ using Strassen's algorithm [20]. Therefore, encryption/decryption operations of AES can be illustrated within $O(n^{2.81})$. In addition, different skills used to implement the AES algorithm will result in different performances. If we adopt the look-up table to implement *MixColumns*, the time complexity of AES can be reduced to a constant time. On the other hand, the security of an asymmetric cryptosystem, such as RSA, is based on big integer factorization, and its operations are the modular exponentiations. Thus, if the key length and data size are both n bits, the time complexity of encryption/decryption operation is approximately $O(n^3)$, because the complexity of multiplication is $O(n^2)$ and the complexity of exponentiation is $O(n)$.

Both Zhu–Ma's scheme and Lee–Hwang–Liao's scheme use a hybrid cryptosystem to conduct authentication. The total time complexity of these two schemes is $O(n^3)$. Because we use one-way hash functions to perform mutual authentication, the time complexity of our scheme is only $O(1)$. Moreover, how to synchronize the clock is a problem in global roaming environments. In this article, we use nonces instead of timestamps to avoid the clock synchronization problem. Although the rounds of communication may increase, an additional clock synchronization mechanism is not needed.

Another issue for mobile devices is limited battery life. Obtained from Potlapally et al.'s experiment [21], we present energy consumption comparisons among various cryptosystems on mobile devices. Note that the computation of the exclusive-OR operation can be ignored due to its little consumption. Using SHA-1 to calculate the hashing value, one byte of data consumes about 0.76 μ*J* of energy. To encrypt one byte of data, the energy consumption of AES is 7.87 + 1.21 = 9.08 μ*J*. To generate a signature using 1024-bit RSA, the energy consumption is 270.13 + 546.5 = 816.63 mJ. Summarizing these results, we obtain an energy consumption ratio of SHA-1:AES:RSA ≈ 1:11.95:1074513.16. This means that the proposed scheme consumes low energy by using a one-way hash function SHA-1. Therefore, battery life will increase.

Table 3 lists the functionality comparisons between the proposed scheme and others. Compared to previous schemes, the energy consumption of our scheme is much lower. Besides, our scheme achieves all security requirements and allows mobile users to change their password freely.

6. Conclusions

In this article, we discuss some security weaknesses in Lee–Hwang–Liao's scheme, propose a novel authentication scheme with anonymity, and compare our scheme with related works. Due to its lower computation cost and energy consumption, the proposed scheme is more suitable for battery-powered mobile devices in global mobility networks. Since message transmission is also an essential factor that affects system performance. If a novel timestamp technology without any clock synchronization mecha-

nism can be proposed, therefore, reducing the rounds of our protocol will be practicable in the future.

References

[1] S. Suzukiz, K. Nakada, An authentication technique based on distributed security management for the global mobility network, IEEE Journal Selected Areas in Communications 15 (8) (1997) 1608–1617.

[2] L. Buttyan, C. Gbaguidi, S. Staamann, U. Wilhelm, Extensions to an authentication technique proposed for the global mobility network, IEEE Transactions on Communications 48 (3) (2000) 373–376.

[3] Z.J. Tzeng, W.G. Tzeng, Authentication of mobile users in third generation mobile system, Wireless Personal Communications 16 (1) (2001) 35–50.

[4] K.F. Hwang, C.C. Chang, A self-encryption mechanism for authentication of roaming and teleconference services, IEEE Transactions on Wireless Communications 2 (2) (2003) 400–407.

[5] J. Zhu, J. Ma, A new authentication scheme with anonymity for wireless environments, IEEE Transactions on Consumer Electronics 50 (1) (2004) 230–234.

[6] C.H. Lin, C.Y. Lee, Cryptanalysis of a new authentication scheme with anonymity for wireless environments, in: Proceedings of the Second International Conference on Advances in Mobile Multimedia, Bali, Indonesia, 2004, pp. 399–402.

[7] C.Y. Lee, C.C. Chang, C.H. Lin, User authentication with anonymity for global mobility networks, in: Proceedings of IEE Mobility Conference 2005: The Second Asia Pacific Conference on Mobile Technology, Applications and Systems, Guangzhou, China, 2005, pp. 3-1B-6:1–5.

[8] C.C. Lee, M.S. Hwang, I.E. Liao, Security enhancement on a new authentication scheme with anonymity for wireless environments, IEEE Transactions on Industrial Electronics 53 (5) (2006) 1683–1687.

[9] P. Syverson, A taxonomy of replay attacks, in: Proceedings of the 7th IEEE Computer Security Foundations Workshop, Franconia, USA, 1994, pp. 131–136.

[10] W. Diffie, M. Hellman, New directions in cyptography, IEEE Transactions on Information Theory 22 (6) (1976) 644–654.

[11] National Institute of Standards and Technology, U.S. Department of Commerce, "Secure Hash Standard," U.S. Federal Information Processing Standard Publication 180-2, 2002.

[12] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Transactions on Computer Systems 8 (1) (1990) 18–36.

[13] National Institute of Standards and Technology, U.S. Department of Commerce, "Advanced Encryption Standard," U.S. Federal Information Processing Standard Publication 197, 2001.

[14] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of ACM 21 (2) (1978) 120–126.

[15] D.S. Wong, H.H. Fuentes, A.H. Chan, The performance measurement of cryptographic primitives on palm devices, in: Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC 2001), New Orleans, USA, 2001, pp. 92–101.

[16] P.G. Argyroudis, R. Verma, H. Tewari, D. O'Mahony, Performance analysis of cryptographic protocols on handheld devices, in: Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004), Cambridge, USA, Sep. 2004, pp. 169–174.

[17] M. Passing, F. Dressler, Experimental performance evaluation of cryptographic algorithms, in: Proceedings of the 3rd IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Vancouver, Canada, 2006, pp. 882–887.

[18] M. Passing, F. Dressler, Practical evaluation of the performance impact of security mechanisms in sensor networks, in: Proceedings of the 31st IEEE Conference on Local Computer Networks, Tampa, USA, 2006, pp. 623–629.

[19] M.R. Doomun, K.S. Soyjaudah, D. Bundhoo, Energy consumption and computational analysis of Rijndael-AES, in: Proceedings of the Third IEEE International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Uzbekistan, 2007, pp. 1–6.

[20] T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, Introduction to Algorithms, second ed., The MIT Press, Cambridge, MA, USA, 2001.

[21] N.R. Potlapally, S. Ravi, A. Raghunathan, N.K. Jha, A study of the energy consumption characteristics of cryptographic algorithms and security protocols, IEEE Transactions on Mobile Computing 5 (2) (2006) 128–143.