ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2012, Vol.41, No.3

An Improved Delegation-Based Authentication Protocol for PCSs

Cheng-Chi Lee[1], Rui-Xiang Chang[2], Te-Yu Chen[3], Lung Albert Chen[4,*]

[1] Department of Library and Information Science,Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang City, Taipei County 24205, Taiwan, R.O.C.
e-mail: cclee@mail.fju.edu.tw

[2] Department of Photonics & Communication Engineering, Asia University
No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, R.O.C.

[3] Department of Information Networking Technology,
Hsiuping University of Science and Technology,
No.11 Gongye Rd, Dali Dist., Taichung City 412-80, Taiwan, R.O.C

[4] Department of Multimedia Information Science and Applications, Asia University
No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, R.O.C.
e-mail: achen@asia.edu.tw

crossref http://dx.doi.org/10.5755/j01.itc.41.3.857

Abstract. Portable Communication Systems (PCS) can provide mobile users with an opportunity to enjoy global roaming services. A lot of researchers have previously proposed their secure protocols for protecting the mobile privacy of the users in PCS. Most protocols pointed out that Lee-Yeh's protocol and Lee et al.'s protocol are vulnerable to some attacks. Then they proposed their improved protocols to remedy these shortcomings. Unfortunately, we found out that the Lee et al.'s protocol still cannot achieve user anonymity and does not provide perfect forward secrecy. In this paper, we also propose an improved protocol to solve these security problems. Compared with other protocols, our proposed protocol not only achieves all security requirements and functionality requirements but also is more efficient.

Keywords: authentication; delegation-based authentication; portable communication systems; user anonymity; perfect forward secrecy; roaming; public-key.

1. Introduction

Wireless communication systems have become one of the most important applications in our daily life. Generally speaking, mobile users can access the services provided by the home location register (*HLR*) in a visited location register (*VLR*). When mobile station (*MS*) roams into a foreign network, *VLR* authenticates the roaming users with the help of s user's *HLR*. In recently years, many protocols discussed the user anonymity for wireless environment [4-9, 12, 13, 19, 20]; and theses protocols used the public-key systems to protect the privacy of the *MS*.

In 2005, Lee and Yeh [10] proposed a new delegation-based authentication protocol for portable communication systems (PCSs). Their protocol also used the public-key cryptosystems to provide user anonymity, non-repudiation, mutual authentication and communication load. Besides, their protocol used off-line authentication processes to provide communicational efficiency, such as GSM [17]. By this, *HLR* helps *VLR* to authenticate with *MS* in the first authentication processes. Then *VLR* can authenticate *MS* without contacting *HLR* in the later authentication processes. This movement reduces the time of authentication.

However, Lee et al. [11] pointed out that Lee-Yeh's off-line authentication processes are vulnerable to masquerade user attacks. Any malicious *VLR* can forge a valid message to login *HLR*. That is, if a malicious *VRL* successfully logins into the *HLR*, the *MS* cannot repudiate these correct messages that are not produced by him/her. Therefore, Lee et al. proposed a slightly modified improvement of Lee-Yeh's protocol based on hash chain [14, 15] to remedy this security weakness. They claimed that their enhanced protocol achieves non-repudiation in both

[*] Correcponding author

the on-line and the off-line authentication processes. Unfortunately, we found that both Lee-Yeh's and Lee et al.'s protocols cannot achieve user anonymity and does not provide perfect forward secrecy [21]. Perfect forward secrecy emphasizes that an adversary obtains a subset of session keys in some ways based on which he/she cannot discover the further session keys. Recently, some related papers about this area have been proposed by some researchers [1, 16, 18, 22]. Tang and Wu pointed out that Lee-Yeh's protocol is vulnerable to a possible attack [18]. As a result, they proposed an improved scheme for protecting mobile privacy in wireless networks. However, Lu et al. [16] showed that the Tang-Wu's protocol also cannot provide mobile privacy. In 2010, Youn and Lim [22] showed that Lee et al.'s protocol [11] cannot achieve private roaming service. Youn and Lim then proposed an improved scheme to remedy the weakness. However, Chen et al. [1] pointed out that the Youn-Lim's protocol is also vulnerable to two drawbacks and presented an improved scheme.

The following security requirements and functionality requirements of the delegation-based authentication protocol for PCSs should be taken into consideration.

Security requirements:

1. **Prevent impersonation attacks:**

   An adversary trying to impersonate as the legitimate user to fool the trust server, or vise versa, to impersonate as the trust server to communicate with the legitimate user, should be prevented.

2. **Prevent replay attacks:**

   An adversary attempting to intercept the messages between two communicating parties and replay these messages in the further processes, should be prevented.

3. **Prevent guessing attacks:**

   An adversary trying to mount a guessing attack by guessing the user's password [3], should be prevented.

4. **Prevent stolen-verifier attacks:**

   An adversary wanting to steal the password-verifier from the trust server and use it directly to masquerade as a legitimate user in an authentication run, should be prevented.

5. **Prevent denial of server attacks**

   An adversary attempting to disrupt the authentication between a legal mobile user and authentication server, should be prevented. Attacks like this would prevent legal users from gaining access to the authentication server [24].

Functionality requirements:

1. **Mutual authentication:**

   Not only a user can verify the identity of a server, but also a server can authenticate a user.

2. **Session key agreement:**

   Severs and users can establish a session key for protecting their subsequent communications.

3. **Non-repudiation:**

   No user can deny that he/she is the producer of these messages before these messages are verified.

4. **User anonymity:**

   It conceals the identity of the communicating parties. User anonymity prevents an adversary from obtaining sensitive personal information. The identity of the user should not be sent in the public network [4-9, 23].

5. **Perfect forward secrecy:**

   When an adversary obtains a subset of session keys, in any way, he/she cannot discover the further session keys.

In this paper, we propose another improved scheme to overcome these weaknesses. The proposed scheme achieves not only the security requirements, but also the functionality requirements.

This paper is organized as follows: in Section 2, we review Lee et al.'s delegation-based authentication protocol [11]. The security flaws of Lee et al.'s protocol are shown in Section 3. Section 4 describes our improved protocol. In Section 5, we discuss the security and the efficiency of our improved protocol. Finally, we conclude in Section 6.

2. Review of Lee et al.'s protocol

In this section, we will review Lee et al.'s delegation-based authentication protocol [11]. Their scheme is divided into three processes: the setup process, the on-line authentication process, and the off-line authentication process. In the setup process, *MS* registers with the *HLR* and obtains a smart card through a secure channel for some service. In the on-line authentication process, when the *MS* roams in a new *VLR*, the *VLR* authenticates the identity of the *MS* through the *HLR*. In the off-line authentication process, the *VLR* can authenticate the *MS* without contacting the *HLR* and requesting further processes. Table 1 lists the notations used in this paper. The detailed phases are shown in the following sections.

2.1. Setup process

The *HLR* generates a secret random number x to compute his/her public key $v = g^x \bmod p$, where x is a *HLR's* private key. The *MS* sends a request to the *HLR* for registration through a secure channel. Then *HLR* generates a random number k to compute the *MS's* public key $K = g^k \bmod p$ and private key $\sigma = x + kK \pmod{p}$. Finally, the key pair (σ, K) is stored in the *MS*'s SIM card. Additionally, the *MS* generates a random number n_1 and pre-computes a hash chain $h^{(1)}(n_1)$, $h^{(2)}(n_1)$,…, $h^{(n+1)}(n_1)$, where $h^{(1)}(n_1) = h(n_1)$ and $h^{(i+1)}(n_1) = h(h^{(i)}(n_1))$ for $i = 1, 2, \ldots, n$.

Table 1. The notations used in this paper

Notations	Descriptions
MS	A mobile user
VLR	Visited Location Register
HLR	Home Location Register
K_{VH}	The long-term secret key shared between *VLR* and *HLR*
ID_H, ID_V	The identity of *HLR* and *VLR*
p	A large prime
q	A prime factor of p-1
g	A generator in group Z_p^*
$[M]_K$	Encryption of a message M using a symmetric key K
$h()$	A one-way hash function
||	String concatenation operation
⇒	A secure channel
→	A common channel

2.2. On-line authentication process

Step 1. $MS \rightarrow VLR$: K

The *MS* obtains the public key K from his /her SIM card and sends K to *VLR*.

Step 2. $VLR \rightarrow MS$: n_2, ID_V

After receiving this message from *MS*, *VLR* generates a random number n_2 and responses n_2 and ID_V to *MS*.

Step 3. $MS \rightarrow VLR$: r, s, K, N_1, ID_H, ID_V

After receiving these messages from *VLR*, the *MS* computes $r = g^t \bmod p$ and picks N_1 from his/her database to compute $s = \sigma \cdot h(N_1 \| n_2 \| ID_V) + t \cdot r \pmod{p}$, where t is a random number and $N_1 = h^{(n+1)}(n_1)$. Finally, *MS* sends $\{r, s, K, N_1, ID_H, ID_V\}$ to *VLR*.

Step 4. $VLR \rightarrow HLR$: $[N_1 \| n_2 \| K]K_{VH}$, ID_H, ID_V

After receiving these messages from *MS*, *VLR* computes g^s and $(vK^K)^{h(N_1 \| n_2 \| ID_V)} r^r \pmod{p}$ and then checks to see if g^s is the same as $(vK^K)^{h(N_1 \| n_2 \| ID_V)} r^r \pmod{p}$. If they are the same, the *VLR* has successfully authenticated the *MS* and sends $\{[N_1 \| n_2 \| K]K_{VH}, ID_H, ID_V\}$ to *HLR*'; otherwise, *VLR* rejects *MS*'s request.

Step 5. $HLR \rightarrow VLR$: $[[N_1, n_3, ID_V]_\sigma \| n_2 \| l \| C_1]K_{VH}$, ID_H, ID_V

After receiving these messages from *VLR*, the *HLR* obtains K by decrypting $[N_1 \| n_2 \| K]K_{VH}$ and further finds the corresponding σ in his/her database according to K. If not found, the *HLR* rejects this authentication process. Otherwise, the *HLR* computes $C_1 = h(N_1 \| n_2 \| n_3 \| \sigma)$ and $l = N_1$, where n_3 is a random number. Then, the *HLR* further computes $[[N_1, n_3, ID_V]_\sigma \| n_2 \| l \| C_1]K_{VH}$ by using the long-term shared key K_{VH} and the *MS*'s private key σ. Finally, the *HLR* sends $\{[[N_1, n_3, ID_V]_\sigma \| n_2 \| l \| C_1]K_{VH}, ID_H, ID_V\}$ to *VLR*.

Step 6. $VLR \rightarrow MS$: $[N_1, n_3, ID_V]_\sigma$, ID_V

After receiving these messages from the *HLR*, the *VLR* obtains $[N_1, n_3, ID_V]_\sigma$, n_2, l, C_1 by decrypting $[[N_1, n_3, ID_V]_\sigma \| n_2 \| l \| C_1]K_{VH}$. Then the *VLR* verifies n_2 and l and then sets C_1 as the current session key *SK*. Finally, the *VLR* sends $\{[N_1, n_3, ID_V]_\sigma, ID_V\}$ to *MS*. After receiving these messages from the *VLR*, the *MS* obtains N_1 by using his/her private key and checks to see if N_1 is the same as the previous sent N_1 in Step 3. If they are the same, *MS* has successfully authenticated *VLR* and computes C_1 as the current session key *SK*. The detailed steps are shown in Fig. 1.

2.3. Off-line authentication process

$MS \rightarrow VLR$: $[h^{(n-i+1)}(n_1)]_{Ci}$

MS selects $h^{(n-i+1)}(n_1)$ from his/her database and computes $[h^{(n-i+1)}(n_1)]_{Ci}$, where n is the limited time of off-line authentication and $i = 1, 2, \ldots, n$. Finally, the *MS* sends $[h^{(n-i+1)}(n_1)]_{Ci}$ to the *VLR*. After receiving these messages from the *MS*, the *VLR* obtains $h^{(n-i+1)}(n_1)$ by using the session key C_i and checks if $h(h^{(n-i+1)}(n_1))$ is the same as l. If they are the same, the *VLR* updates $l = h^{(n-i+1)}(n_1)$ and $i = i+1$, where the count $i \leqq n$. Afterwards, the *VLR* computes the session key $C_{i+1} = h(l, C_i)$.

3. Weaknesses of Lee et al.'s protocol

In this section, we will demonstrate that Lee et al.'s protocol fails to provide perfect forward secrecy and perfect backward secrecy. Besides, their protocol cannot achieve a dynamic ID. That is, if the clients use their protocol to process the secret information, such as the personal privacy or the tracking of the user, the adversary can intercept the user's ID to know who is communicating with the remote server *S*. More details are described as follows:

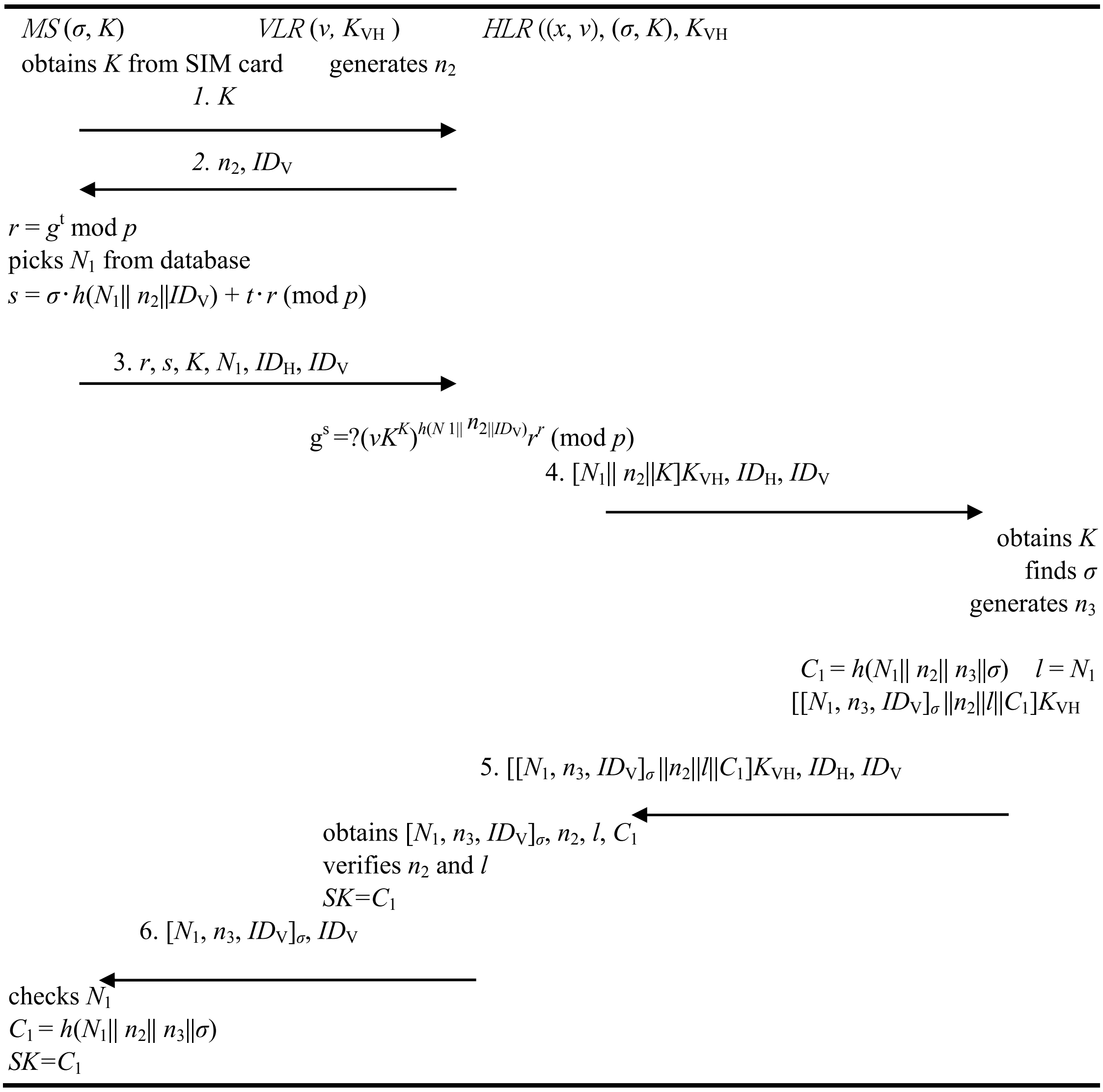

$MS\,(\sigma, K)$
$VLR\,(v, K_{\mathrm{VH}})$
$HLR\,((x, v), (\sigma, K), K_{\mathrm{VH}}$
obtains K from SIM card
generates n_2
1. K
2. n_2, ID_{V}
$r = g^{t} \bmod p$
picks N_1 from database
$s = \sigma \cdot h(N_1 \| n_2 \| ID_{\mathrm{V}}) + t \cdot r \pmod p$
3. $r, s, K, N_1, ID_{\mathrm{H}}, ID_{\mathrm{V}}$
$g^{s} =? (vK^{K})^{h(N_1 \| n_2 \| ID_{\mathrm{V}})} r^{r} \pmod p$
4. $[N_1 \| n_2 \| K]K_{\mathrm{VH}}, ID_{\mathrm{H}}, ID_{\mathrm{V}}$
obtains K
finds σ
generates n_3
$C_1 = h(N_1 \| n_2 \| n_3 \| \sigma)$ $l = N_1$
$[[N_1, n_3, ID_{\mathrm{V}}]_{\sigma} \| n_2 \| l \| C_1]K_{\mathrm{VH}}$
5. $[[N_1, n_3, ID_{\mathrm{V}}]_{\sigma} \| n_2 \| l \| C_1]K_{\mathrm{VH}}, ID_{\mathrm{H}}, ID_{\mathrm{V}}$
obtains $[N_1, n_3, ID_{\mathrm{V}}]_{\sigma}, n_2, l, C_1$
verifies n_2 and l
$SK=C_1$
6. $[N_1, n_3, ID_{\mathrm{V}}]_{\sigma}, ID_{\mathrm{V}}$
checks N_1
$C_1 = h(N_1 \| n_2 \| n_3 \| \sigma)$
$SK=C_1$

Figure 1. The on-line authentication process of Lee et al.'s protocol

3.1. Lack of dynamic ID

The most important issue is not only the security problem but also the personal privacy. In the recent years, there are many researches that point out some advantages in the user anonymity for wireless environments [2, 4-9, 11, 12, 14]. In a normal public network, the adversary could intercept the user's identity and find out who was communicating with VLR and obtain sensitive personal information. Therefore, a user's identity must be anonymous. Namely, a user's identity should be encrypted or replaced with a temporal identity. But we found out that Lee et al.'s protocol cannot achieve any dynamic ID. The detail is described in the following paragraph.

In the on-line authentication process, the *MS* sends *K* to the *VLR* in Step 1. However, the public key *K* is similar to the identity of the mobile user. Although the public key *K* is only used in the on-line authentication process, *K* is both immobile and sent through a public network. Any user can intercept the user's public key *K* from the public wireless network, including illegal ones. That is, Lee et al.'s protocol fails to achieve anonymity service. When *MS* communicates with *VLR* in an on-line authentication process, any one could figure out who is communicating with *VLR* and *HLR*. It triggers the personal privacy problems. Therefore, we think the user's anonymity should be taken into consideration in PCSs. It's obvious that Lee et al.'s protocol does not provide user anonymity to protect a user's privacy.

3.2. Perfect forward secrecy

Perfect forward secrecy is a very important security attribute. However, we found that Lee et al.'s delegation-based authentication protocol for PCSs fails to provide perfect forward secrecy. Perfect forward secrecy means that if an adversary obtains a subset of session key in some ways, he/she cannot extract the past session keys. More details are described in the following paragraphs.

In Lee et al.'s off-line authentication protocol, the *MS* sends an authentication request $[h^{(n-i+1)}(n_1)]_{C_i}$ to the *VLR*, where *n* is the limited time of off-line authentication and $i = 1, 2,...,n$. Then the VLR obtains $h^{(n-i+1)}(n_1)$ by using C_i and checks if $h(h^{(n-i+1)}(n_1))$ is the same as *l*. If they are the same, *VLR* updates $l=h^{(n-i+1)}\cdot(n1)$ and $i = i+1$, where the count $i \leqq n$. Then, the *VLR* computes the session key $C_{i+1} = h(l, Ci)$ for securing communications with the MS. Finally, the *MS* and the *VLR* store the session key C_{i+1} and *l* for the next communication. Once the session key C_i is disclosed in an off-line authentication, the adversary can obtain $h^{(n-i+1)}(n_1)$ and compute the session key $C_{i+1}=h(l, C_i)$. Besides, he/she also can obtain the next session key by using C_{i+1}.

As an example, let's assume that $n = 10$. Then after the on-line authentication, *MS* stores $h^{(9)}(n_1)$, $h^{(8)}(n_1)$, $h^{(7)}(n_1)$….. $h^{(1)}(n_1)$ in his/her database and the *VLR* obtains $l = h^{(10)}(n_1)$ and C_1. In the first off-line authentication, the *MS* sends an authentication request $[h^{(9)}(n_1)]_{C1}$ to the *VLR*, where C_1 is the session key established in the on-line authentication. Then the *VLR* obtains $h^{(9)}(n_1)$ by using C_1 and checks if $h(h^{(9)}(n_1))$ is the same as *l*. If they are the same, the *VLR* updates $l = h^{(9)}(n_1)$ and computes the current session key $C_2 = h(l, C_1)$ for the next communication with the *MS*. If the adversary obtains the session key C_1, somehow, he/she can decrypt $[h^{(9)}(n_1)]_{C1}$ and compute $l = h^{(10)}(n_1)$. Then the adversary can also compute the current session key $C_2 = h(l, C_1)$ and store C_2 for the second off-line authentication. This means that if a given session key C_i is disclosed, all the other session keys C_{i+1} will be opened. That is, when the *MS* communicates with the *VLR*, the adversary can decrypt all the massages between the *MS* and the *VLR*. Therefore, Lee et al.'s protocol cannot provide perfect forward secrecy.

4. Our improved protocol

In this section, we propose an improvement on Lee et al.'s protocol, which keeps the merits of the original protocol, and at the same time, can provide user anonymity and achieve perfect forward secrecy. To provide user anonymity in Lee et al.'s protocol, we assume that the identity of the user is encrypted or has been replaced with a temporal identity. Our improved protocol consists of three processes: the setup process, the on-line authentication process, and the off-line authentication process. The detailed phases are shown in the following sections.

4.1. Setup process

The *HLR* computes his/her public key $v= g^x \bmod p$, where *x* is the *HLR's* private key. When the *MS* sends a request to the *HLR* for registration through a secure channel, the *HLR* computes the *MS's* public key $K = g^k \bmod p$ and private key $\sigma = x + kK \pmod p$ and decides an initialized temporary identity T_{ID}, where *k* is a random number generated by *HLR*. Afterwards, *MS*'s SIM card contains the key pair (σ, K) and T_{ID}. Additionally, *MS* pre-computes a hash chain $h^{(1)}(n_1)$, $h^{(2)}(n_1)$,…, $h^{(n+1)}(n_1)$, where n_1 is a random number generated by *MS*.

4.2. On-line authentication process

Step 1. $MS \rightarrow VLR$: T_{ID}

The *MS* obtains the initialized temporary identity T_{ID} from his/her SIM card and sends T_{ID} to *VLR*.

Step 2. $VLR \rightarrow MS$: n_2, ID_{V}

After receiving this message from *MS*, *VLR* generates a random number n_2 and responses n_2 and ID_{V} to *MS*.

Step 3. $MS \rightarrow VLR$: r, s, T_{ID}, N_1, ID_{H}, ID_{V}

After receiving these messages from *VLR*, *MS* computes $r = g^{\mathrm{t}} \bmod p$ and picks N_1 and T_{ID} from his/her database to compute $s = \sigma \cdot h(N_1\|\, n_2\|ID_{\mathrm{V}}) + t{\cdot}r \pmod p$, where *t* is a random number and $N_1 = h^{(n+1)}(n_1)$. Finally, *MS* sends $\{r, s, T_{\mathrm{ID}}, N_1, ID_{\mathrm{H}}, ID_{\mathrm{V}}\}$ to *VLR*.

Step 4. $VLR \rightarrow HLR$: $[N_1\|\, n_2\|\, T_{\mathrm{ID}}]K_{\mathrm{VH}}$, ID_{H}, ID_{V}

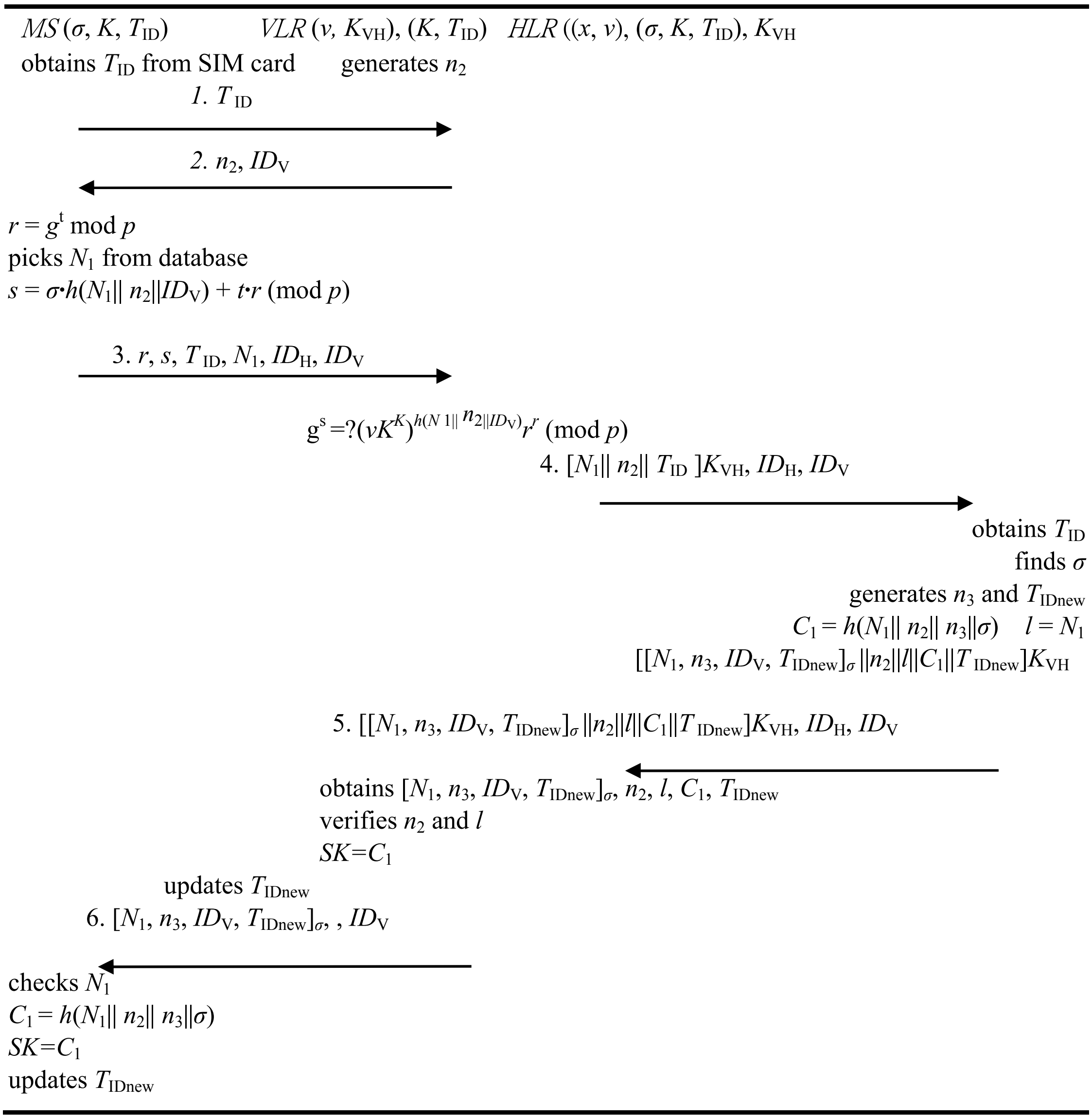
After receiving this message from the *MS*, the *VLR* obtains *K* by checking T_{ID} from his/her database. We assume that the *VLR* maintains a table of the mapping between the public key *K* and the corresponding initial temporary identity T_{ID}. Then the *VLR* computes g^{s} and $(vK^K)^{h(N\,1\|\, n_{2\|ID\mathrm{V}})}r^{\mathrm{r}} \pmod p$ and then checks if g^s is the same as $(vK^K)^{h(N\,1\|\, n_{2\|ID\mathrm{V}})}r^{\mathrm{r}} \pmod p$. If they are the same, the *VLR* has successfully authenticated the *MS* and sends $\{[N_1\|\, n_2\|\, T_{\mathrm{ID}}]K_{\mathrm{VH}}, ID_{\mathrm{H}}, ID_{\mathrm{V}}\}$ to *HLR*; otherwise, the *VLR* rejects the *MS*'s request.

Step 5. $HLR \rightarrow VLR$: $[[N_1, n_3, ID_{\mathrm{V}}, T_{\mathrm{IDnew}}]_\sigma \|n_2\|l\|C_1\|T_{\mathrm{IDnew}}]K_{\mathrm{VH}}$, ID_{H}, ID_{V}

After receiving these messages from the *VLR*, the *HLR* obtains T_{ID} by decrypting $[N_1\|n_2\|T_{\mathrm{ID}}]K_{\mathrm{VH}}$ and further finds the corresponding σ in his/her database according to T_{ID}. If it is not found, *HLR* rejects this authentication process. Otherwise, the *HLR* computes $C_1 = h(N_1\|\, n_2\|\, n_3\|\sigma)$ and $l = N_1$, where n_3 is a random number generated by the *HLR*. Then, the *HLR* further generates a new temporary identity T_{IDnew} and computes $[[N_1, n_3, ID_{\mathrm{V}}, T_{\mathrm{IDnew}}]_\sigma \|n_2\|l\|C_1\|T_{\mathrm{IDnew}}]K_{\mathrm{VH}}$ by using the long-term shared key K_{VH} and *MS*'s private key σ. Finally, *HLR* sends $\{[[N_1, n_3, ID_{\mathrm{V}}, T_{\mathrm{IDnew}}]_\sigma \|n_2\|l\|C_1\|T_{\mathrm{IDnew}}]K_{\mathrm{VH}}, ID_{\mathrm{H}}, ID_{\mathrm{V}}\}$ to *VLR*.

Step 6. *VLR* → *MS*: $[N_1, n_3, ID_V, T_{IDnew}]_\sigma, ID_V$

After receiving these messages from the *HLR*, the *VLR* obtains $[N_1, n_3, ID_V, T_{IDnew}]_\sigma$, n_2, l, C_1, T_{IDnew} by decrypting $[[N_1, n_3, ID_V, T_{IDnew}]_\sigma \| n_2 \| l \| C_1 \| T_{IDnew}]K_{VH}$. Then *VLR* verifies n_2 and l and then sets C_1 as the current session key *SK*. Finally, the *VLR* replaces T_{ID} with T_{IDnew} in his/her database. Then the *VLR* sends $\{[N_1, n_3, ID_V, T_{IDnew}]_\sigma, ID_V\}$ to *MS*. After receiving these messages from *VLR*, *MS* obtains N_1 by using his/her private key and checks if N_1 is the same as the previous sent N_1 in Step3. If they are the same, *MS* has successfully authenticated the *VLR,* and computes C_1 as the current session key *SK*. Finally, *MS* obtains T_{IDnew} and updates the SIM card for the next authentication. The detailed steps are shown in Fig. 2.



MS (σ, K, T_{ID}) *VLR* $(v, K_{VH}), (K, T_{ID})$ *HLR* $((x, v), (\sigma, K, T_{ID}), K_{VH}$

obtains T_{ID} from SIM card

generates n_2

1. T_{ID}

2. n_2, ID_V

$r = g^t \bmod p$

picks N_1 from database

$s = \sigma \cdot h(N_1 \| n_2 \| ID_V) + t \cdot r \ (\bmod p)$

3. $r, s, T_{ID}, N_1, ID_H, ID_V$

$g^s = ?(vK^K)^{h(N\,1\| n_2 \| ID_V)} r^r \ (\bmod p)$

4. $[N_1 \| n_2 \| T_{ID}]K_{VH}, ID_H, ID_V$

obtains T_{ID}

finds σ

generates n_3 and T_{IDnew}

$C_1 = h(N_1 \| n_2 \| n_3 \| \sigma)$ $l = N_1$

$[[N_1, n_3, ID_V, T_{IDnew}]_\sigma \| n_2 \| l \| C_1 \| T_{IDnew}]K_{VH}$

5. $[[N_1, n_3, ID_V, T_{IDnew}]_\sigma \| n_2 \| l \| C_1 \| T_{IDnew}]K_{VH}, ID_H, ID_V$

obtains $[N_1, n_3, ID_V, T_{IDnew}]_\sigma, n_2, l, C_1, T_{IDnew}$

verifies n_2 and l

$SK = C_1$

updates T_{IDnew}

6. $[N_1, n_3, ID_V, T_{IDnew}]_\sigma, , ID_V$

checks N_1

$C_1 = h(N_1 \| n_2 \| n_3 \| \sigma)$

$SK = C_1$

updates T_{IDnew}

Figure 2. The improved on-line authentication process

4.3. Off-line authentication process

MS → *VLR*: $[h^{(n-i+1)}(n_1) \oplus T_{IDnew}]_{Ci}$

The *MS* obtains $h^{(n-i+1)}(n_1)$ and T_{IDnew} from his/her database and computes $[h^{(n-i+1)}(n_1) \oplus T_{IDnew}]_{Ci}$, where n is the limited time of off-line authentication and $i = 1, 2, ..., n$. Finally, the *MS* sends $[h^{(n-i+1)}(n_1) \oplus T_{IDnew}]_{Ci}$ to the *VLR*. After receiving these messages from the *MS*, the *VLR* obtains $h^{(n-i+1)}(n_1)$ by using the session key C_i and T_{IDnew}. Then *VLR* checks if $h(h^{(n-i+1)}(n_1))$ is the same as l. If they are the same, *VLR* updates $l = h^{(n-i+1)}(n_1)$ and $i = i+1$, where the count $i \leqq n$. The *VLR* computes the session key $C_{i+1} = h(l, C_i)$ and decides a new temporary identity T_{IDnewi} and updates the verification table. Afterwards, the *VLR* sends $[T_{IDnewi} \oplus T_{IDnew}]_{Ci+1}$ to the *MS* and sends $[T_{IDnewi}]K_{VH}$

to the *HLR*. After receiving these messages, the *MS* obtains T_{IDnewi} and updates the SIM card for the next authentication process. Besides, the *HLR* obtains T_{IDnewi} and updates his/her database.

5. Security analysis

In this paper, we propose a modification to the improved Lee et al.'s protocol, to achieve the requirement of user anonymity and perfect forward secrecy. The focus of this section is on security requirements and functional requirements. Therefore, in this section, we will only discuss the essential security requirements and functional requirements that a portable communication system should have.

5.1. Resistance to impersonation attacks

Impersonation attacks are very treacherous when the adversary has the ability to send a valid message to fool another user or the server herself. This attack should be taken into consideration and should be avoided. Assume that the adversary is trying to impersonate a legitimate user to login to the server. Then he/she needs to send a valid message to the *VLR* in the off-line authentication processes. However, the adversary cannot impersonate any legitimate users to deceive the *VLR*, because he/she cannot compute $[h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}}]_{\mathrm{C}i}$ without knowing $h^{(\mathrm{n}-i+1)}(n_1)$ and T_{IDnew} which are secretly stored in the SIM card and the session key C_{i}. It can be assured that the adversary cannot perform impersonation attacks in our improved protocol.

Besides, the adversary might want to impersonate a legitimate *VLR* to cheat the *MS* to obtain some benefits. However, the adversary has no way to perform this attack, because he/she cannot decrypt $[h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}}]_{\mathrm{C}i}$ without the session key C_{i}. Therefore, the adversary cannot impersonate a *VLR* to cheat the legitimate user in our improved protocol.

5.2. Resistance to denial of service attacks

Denial-of-Service attacks can disturb the availability of the authentication between the legitimate user and server. This kind of attack can prevent legitimate users to access the server. We can assume that the adversary wants to perform a denial of service attacks to paralyze the *VLR*. This DoS will not work in our improved protocol. In off-line authentication processes, the MS can obtain $h^{(\mathrm{n}-i+1)}(n_1)$ and T_{IDnew} from the SIM card and send $[h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}}]_{\mathrm{C}i}$ to access the *VLR*. After the *VLR* receives this message, he/she obtains C_{i} and T_{ID} from his/her database and verifies the *MS* by checking if $h(h^{(\mathrm{n}-i+1)}(n_1))$ is the same as l. If it holds, the *VLR* updates $l = h^{(\mathrm{n}-i+1)}(n_1)$ and T_{IDnewi} and computes the session key $C_{\mathrm{i+1}} = h(l, C_{\mathrm{i}})$. Since the *VLR* can control the amount of incoming login messages in the off-line authentication processes, no one can perform the denial of service attack on our improved protocol.

5.3. Resistance to replay attacks

Assuming that the adversary wants to replay the message $[h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}}]_{\mathrm{C}i}$ to cheat the *VLR*, he/she will fail, because the *VLR* has the ability to detect this attack. When the adversary intercepts the login message in the off-line authentication processes and retransmits it, the *VLR* obtains $h^{(\mathrm{n}-i+1)}(n_1)$ by using the session key C_{i+1} and T_{IDnewi}. Then the *VLR* checks to see if $h(h^{(\mathrm{n}-i+1)}(n_1))$ is the same as l. In this case, the replay message is encrypted by the previous session key C_i. The *VLR* uses the further session key C_{i+1} to decrypt this intercept message. The replayed message cannot pass the equation test $h(h^{(\mathrm{n}-i+1)}(n_1)) =? l$. Therefore, the *VLR* will detect and reject this failed message. Our improved protocol can withstand the replay attack.

5.4. User privacy

User anonymity has become an essential functional requirement in mobile communications, because an adversary might intercept the user's identity from the public network and use it to trace the mobile user. However, in the improved protocol, we substitute a temporary identity T_{ID} for the public key K to protect the privacy of the *MS* in the on-line authentication processes. Since the user's public key K is not transmitted over the public network in the on-line authentication processes, the adversary cannot trace the mobile user. Besides, after the on-line authentication processes, as the temporary identity T_{ID} is replaced with a new temporary identity $\mathrm{T}_{\mathrm{IDnew}}$, the adversary cannot use the old one to figure out the trace of the *MS*. Therefore, user intractability is achieved by the anonymity of a temporary identity and user anonymity is provided in our improved protocol.

5.5. Perfect forward secrecy

Perfect forward secrecy is a form of security requirements in network systems. In general, perfect forward secrecy means that an adversary cannot extract the past session keys, even if, by using some methods, he/she manage to obtain a subset of session keys. If somehow the adversary obtains a subset of session keys C_{i} , he/she can intercept the login message $[h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}}]_{\mathrm{C}i}$ of the *MS* and decrypt it. However, the adversary cannot compute the further session key $C_{\mathrm{i+1}}= h(l, C_{\mathrm{i}})$ without the existence of l. He/she can only obtain $h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}}$ by decrypting $[h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}}]_{\mathrm{C}i}$. The adversary therefore can't compute $h^{(\mathrm{n}-i+1)}(n_1) \oplus T_{\mathrm{IDnew}} \oplus T_{\mathrm{IDnew}}=l$, since he/she doesn't have the temporary identity T_{IDnew} of *MS*. That is, only both *MS* and *VLR* have the necessary temporary identity T_{IDnew} to obtain l. Therefore, we conclude that our improved protocol can provide perfect forward secrecy.

5.6. Mutual authentication

Mutual authentication can be achieved in our improved protocol. In the on-line authentication processes, the *MS* authenticates the *VLR* and the *HLR* by checking N_1 in Step 6. Only a legal *HLR* can compute $[N_1, n_3, ID_V, T_{IDnew}]_\sigma$ by using a user's private key. The *VLR* authenticates the *MS* and the *HLR* by checking the proxy signature $g^s =?(vK^K)^{h(N\ 1||\ n_2||ID_V)}r^r$ (mod p) in Step 4 and n_2 in Step 6, respectively. Only a legal *MS* can compute $s=\sigma\cdot h(N_1||n_2||ID_V)+t\cdot r$ (mod p) by using his/her private key, and the *HLR* then can compute $[[N_1, n_3, ID_V, T_{IDnew}]_\sigma||n_2||l||C_1||\ T_{IDnew}]K_{VH}$ by using a long-term shared key between the *VLR* and the *HLR*. The *HLR* authenticates the *VLR* by checking T_{ID} in Step 5. Besides, the *HLR* authenticates the *MS* through the VLR in Step 4 that checks the equation $g^s =?(vK^K)^{h(N\ 1||\ n_2||ID_V)}r^r$ (mod p). In the off-line authentication, the *MS* sends a login message $[h^{(n-i+1)}(n_1) \oplus T_{IDnew}]_{Ci}$ to the *VLR*, and the *VLR* verifies the *MS* by checking if $h(h^{(n-i+1)}(n_1))$ is the same as l. If they are the same, the *VLR* has successfully authenticated the *MS*. The *VLR* updates $l = h^{(n-i+1)}(n_1)$ and T_{IDnewi} and computes the further session key $C_{i+1} = h(l, C_i)$. Then the *VLR* sends $[T_{IDnewi} \oplus T_{IDnew}]_{Ci}$ as a response to the *MS*, and the *MS* decrypts it and verifies the *VLR* by checking T_{IDnew}. If they are the same, the *MS* has successfully authenticated the *VLR* and updates T_{IDnewi}. That is, both the *MS* and the *VLR* are able to obtain the same T_{ID} both to compute the session key C_i, and to update the further session key $C_{i+1}= h(l, C_i)$. Therefore, our improved protocol can provide mutual authentication.

5.7. The security of session key *SK*

If the adversary tries to obtain the one-time session key C_1 in the on-line authentication processes, he/she can intercept all the messages from the public wireless environment. However, the adversary cannot compute $C_1 = h(N_1||\ n_2||\ n_3||\sigma)$ without the user's private key σ. Only the *MS* and the *HLR* can compute the session key $C_1 = h(N_1||\ n_2||\ n_3||\sigma)$, because both have the user's private key σ. Even if the adversary intercepts any messages in the on-line authentication processes, he/she has no way to decrypt $[[N_1, n_3, ID_V, T_{IDnew}]_\sigma ||n_2||l||C_1||T_{IDnew}]K_{VH}$ to obtain C_1 without relying on the long-term shared key K_{VH}. Besides, the adversary also cannot obtain the session key in the off-line authentication processes, because he/she cannot compute $C_{i+1} = h(l, C_i)$ without $h(h^{(n-i+1)}(n_1))$ and C_i. Therefore, our improved protocol can provide the session key security.

5.8. Non-repudiation

In the off-line authentication processes, the *MS* obtains $h^{(n-i+1)}(n_1)$ and T_{IDnew} from his/her database and computes $[h^{(n-i+1)}(n_1) \oplus T_{IDnew}]_{Ci}$, where n is the limited time of off-line authentication and i = 1, 2,...,n. Then, the *MS* sends $[h^{(n-i+1)}(n_1)\oplus T_{IDnew}]_{Ci}$ to the *VLR*. When the *VLR* receives these messages from the *MS*, he/she obtains $h^{(n-i+1)}(n_1)$ by using the session key C_i and T_{IDnew}. Then the *VLR* checks if $h(h^{(n-i+1)}(n_1))$ is the same as l. If they are the same, the *VLR* has successfully authenticated the *MS*. Only a legal *MS* can compute $[h^{(n-i+1)}(n_1)\oplus T_{IDnew}]_{Ci}$ and $C_{i+1} = h(l, C_i)$ to login the *VLR*. No one can masquerade a legal *MS* to compute $[h^{(n-i+1)}(n_1)\oplus T_{IDnew}]_{Ci}$ to deceive the *VLR*. If a mobile user wants to deny the fact that he/she has transmitted a particular message, the *VLR* can detect this attempt by using the session key C_i. Therefore, our improved protocol can achieve this essential requirement.

Table 2. Properties of the improved protocol and previously proposed protocols

	Ours	Lee et al. [11]	Lee and Yeh [10]
Prevention of an impersonation attack	O	O	X
Prevention of a denial of service attack	O	O	O
Prevention of a replay attack	O	O	O
User anonymity	O	X	X
Perfect forward secrecy	O	X	X
Mutual authentication	O	O	O
Session key establishment	O	O	O
Non-repudiation	O	O	X

Table 2 lists the properties of the improved protocol and that of the previously proposed protocols. Compared with the previous protocols, our improved protocol can achieve all the security requirements and provide anonymity service for mobile users to roam in portable communication systems.

Since the Chen et al.'s protocol [1] is the newest protocol in this research area, we compare the efficiency of our improvement with this protocol. Table 3 shows the computation costs of both protocols in an on-line authentication process. Since the setup process and the off-line authentication process of both protocols are similar, we only compare the on-line authentication process between both protocols. We can see that our proposed protocol is more efficient than the Chen et al.'s protocol.

Table 3. Comparison of computation costs in an on-line authentication process

	Ours			Chen et al. [1]		
	MS	VLR	HLR	MS	VLR	HLR
Modular exponentiation	1	4	0	1	4	1
Modular multiplication	2	0	0	2	0	1
Symmetric encryption/ decryption	1	2	3	1	2	3
Hash function	2	1	1	2	1	1

6. Conclusions

In this paper, we have demonstrated that Lee et al.'s protocol fails to provide perfect forward/backward secrecy and is not able to preserve user anonymity. In addition, Lee-Yeh's protocol suffers from the same problems, since Lee et al.'s protocol inherits from Lee and Yeh's protocol. Their protocols fail to provide the anonymity service, which is the key to delegation-based authentication. Neither Lee-Yeh's nor Lee et al.'s protocols can provide perfect forward secrecy, since, if once a subset of session key is revealed, all session keys will be opened. The improved protocol presented in this paper not only retains the advantages from the original research, but also enhances the essential requirements. We therefore believe that our improved protocol will provide a practicable solution in the real world.

Acknowledgment

The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: 100-2221-E-030-015, and 100-2218-E-164-002.

References

[1] **H. B. Chen, Y. H. Lai, K. W. Chen, W. B. Lee**, Enhanced delegation based authentication protocol for secure roaming service with synchronization, *Journal of Electronic Science and Technology*, vol. 9, no. 4, pp. 345-351, Dec. 2011.

[2] **M. L. Das**, Two-factor user authentication in wireless sensor networks, *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086-1090, 2009. http://dx.doi.org/10.1109/TWC.2008.080128.

[3] **Y. Ding, P. Horster**, Undetectable on-line password guessing attacks, *ACM SIGOPS Operating Systems Review*, vol. 29, no. 4, pp. 77-86, 1995. http://dx.doi.org/10.1145/219282.219298.

[4] **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*, vol. 53, no. 5, pp. 1683-1687, 2006. http://dx.doi.org/10.1109/TIE.2006.881998.

[5] **C. C. Lee, R. X. Chang, T. Williams**, On the anonymity of an enhanced authentication scheme for a roaming service in global mobility networks, *accepted to appear in International Journal of Secure digital Information age.*

[6] **C. C. Lee, C. T. Li, R. X. Chang**, A simple and efficient authentication scheme for mobile satellite communication systems, *International Journal of Satellite Communications and Networking*, vol. 30, no. 1, pp. 29-38, Jan. 2012. http://dx.doi.org/10.1002/sat.993.

[7] **C. T. Li, C. C. Lee**, A novel user authentication and privacy preserving scheme with smart cards for wireless communications, *Mathematical and Computer Modeling*, vol. 55, no. 1-2, pp. 35-44, Jan. 2012. http://dx.doi.org/10.1016/j.mcm.2011.01.010.

[8] **C. C. Lee, I. E. Liao, M. S. Hwang**, An efficient authentication protocol for mobile communications, *Telecommunication Systems*, vol. 46, no. 1, pp. 31-41, Jan. 2011. http://dx.doi.org/10.1007/s11235-009-92764.

[9] **C. C. Lee, T. H. Lin, C. S. Tsai**, A new authenticated group key agreement in a mobile environment, *Annals Of Telecommunications - Annales Des Telecommunications*, vol. 64, no. 11, pp. 735-744, Dec. 2009.

[10] **W. B. Lee, C. K. Yeh**, A new delegation-based authentication protocol for use in portable communication systems, *IEEE Transactions on Wireless Communications,* vol. 4, no. 1, pp. 57-64, 2005. http://dx.doi.org/10.1109/TWC.2004.840220.

[11] **T. F. Lee, S. H. Chang, T. Hwang, S. K. Chong**, Enhanced delegation-based authentication protocol for PCSs, *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, pp. 2166-2171, 2009. http://dx.doi.org/10.1109/TWC.2009.070032.

[12] **M. Long, C. H. Wu, J. D. Irwin**, Localized authentication for internetwork roaming across wireless LANs, *Communications IEE Proceedings,* vol. 151, no. 5, pp. 496-500, 2004.

[13] **T. F. Lee, C. C. Chang, T. Hwang**, Private authentication techniques for the global mobility network, *Wireless Personal Communications*, vol. 35, no. 4, pp. 329-336, 2005. http://dx.doi.org/10.1007/s11277-005-6177-z.

[14] **H. Y. Lin, L. Harn**, Authentication protocols with non-repudiation services in personnel communication systems, *IEEE Communications Letters*, vol. 3, no. 8, pp. 236-238, 1999. http://dx.doi.org/10.1109/4234.781006.

[15] **L. Lamport**, Password authentication with insecure communication, *Communication of ACM*, vol. 24, pp. 770-772, 1981. http://dx.doi.org/10.1145/358790.358797.

[16] **J. Z. Lu, H. Q. Ren, J. Zhou**, Efficient delegation-based authentication protocol with strong mobile privacy, *Proceedings of the International Conference on Wireless Information Networks and Systems* (*WINSYS 2011)*, Seville, Spain, 18-21 July, pp. 123-127, 2011.

[17] **M. Rahnema**, Overview of the GSM system and protocol architecture, *IEEE Communications Magazine,* vol. 31, no. 4, pp. 92-100, 1993. http://dx.doi.org/10.1109/35.210402.

[18] **C. Tang, D. O. Wu**, An efficient mobile authentication scheme for wireless networks, *IEEE Transactions on Wireless Communications*, vol.7, no. 4, pp. 1408-1416, 2008. http://dx.doi.org/10.1109/TWC.2008.061080.

[19] **C. C. Wu, W.B. Lee, W. J. Tsaur**, A secure authentication scheme with anonymity for wireless communications, *IEEE Communications Letters*, vol. 12, no. 10, pp. 722-723, 2008. http://dx.doi.org/10.1109/LCOMM.2008.080283.

[20] **S. J. Wang**, Anonymous wireless authentication on a portable cellular mobile system, IEEE Transactions on Computers, vol. 53, no. 10, pp. 1317–1329, 2004. http://dx.doi.org/10.1109/TC.2004.70.

[21] **E. J. Yoon, K. Y. Yoo**, Cryptanalysis of robust E-mail protocols with perfect forward secrecy, *IEEE*

Communications Letters, vol. 11, no. 5, pp. 372-374, 2007. http://dx.doi.org/10.1109/LCOMM.2007.061770

[22] **T. Y. Youn, J. Lim**, Improved delegation-based authentication protocol for secure roaming service with unlinkability, *IEEE Communications Letters*, vol. 14, no. 9, pp. 791−793, Sep. 2010. http://dx.doi.org/10.1109/LCOMM.2010.080210.100353.

[23] **J. Zhu, J. Ma**, A new authentication scheme with anonymity for wireless environments, *IEEE Transactions Consumer Electronics*, vol. 50, no. 1, pp. 231-235, 2004. http://dx.doi.org/10.1109/TCE.2004.1277867.

[24] **R. Zhang, K. Chen**, Improvements on the WTLS protocol to avoid denial of service attacks, *Computers & Security*, vol. 24, no. 5, pp. 76-82, 2005. http://dx.doi.org/10.1016/j.cose.2004.10.002.

Received November 2010.