An Efficient User Authentication Scheme with Smart Cards for Wireless Communications

Woongryul Jeon[1], Yunho Lee[2], and Dongho Won[1,*]

[1]*College of Information and Communication Engineering, Sungkyunkwan University,*
300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do 440-746, Korea
wrjeon@security.re.kr, dhwon@security.re.kr

[2]*Department of Cyber Security and Police, Gwangju University*
277 Hyodeok-ro, Nam-gu, Gwangju-si, Korea
leeyh@gwangju.ac.kr

[*]*The corresponding author*

Abstract

Since 2004, several user authentication schemes purpose to provide user anonymity in wireless communication have been announced, however, many of them failed to provide user anonymity, actually. In 2011, Li and Lee proposed a secure user authentication scheme for wireless communications. Differently from the previous researches, Li and Lee claimed two more session keys to enhance entire security of the scheme. However, to fulfil their claim, Li and Lee adopted Diffie-Hellman key agreement method in their scheme, and it required plenty of resources. Thus, in this paper, we point out inefficiency of Li and Lee's scheme and propose a more efficient user authentication scheme for wireless communications.

Keywords: *Mobile computing, Remote user authentication, Security, Wireless communications, User anonymity.*

1. Introduction

In modern days, wireless communications with mobile device have become one of the most important application in our daily life. The mobile device provides several customized services which require private information, including location information. Thus authentication with anonymity becomes a hot issue in mobile communications, because location information reveals pattern of the mobile users, [1]-[14].

In 2004, Zhu and Ma proposed an authentication scheme in wireless communications [15], and this scheme considers the anonymity to protect the user's location information. However, several studies proved that Zhu and Ma's scheme failed to provide user anonymity. In 2006, Lee et al. proved several security vulnerabilities of Zhu et al.'s scheme and proposed improved one [16]. However, in 2008, Wu et al. revealed that both schemes did not provide user anonymity [17]. They proposed an improved scheme which preserves user anonymity, but Lee et al. pointed out security flaws of Wu et al.s' [18]. Recently, in 2010, He et al.

Table 1. Notations used in this paper

Notations	Description
MU	Mobile user
FA	Foreign agent
HA	Home agent
ID_A	Identity of an entity A
PW_A	Password of A
T_A	Timestamp of A
N	Strong secret key of HA
$Cert_A$	Certificate of an entity A
SK	The common session key
$E_K[\cdot]/D_K[\cdot]$	The symmetric encryption/decryption function with key K
$E_K\{\cdot\}/D_K\{\cdot\}$	The asymmetric encryption/decryption function with key K
P_A	Public key of an entity A
S_A	Secret key of an entity A
$h(\cdot)$	A one-way hash function
$\|\|$	Concatenation operation
$\oplus$	Bitwise exclusive-or operation
$A \rightarrow B : M$	A sends message M to B.

proposed an efficient user authentication scheme [19]. However, Li and Lee pointed out that He et al.'s scheme does not provide user anonymity and unfairness in key agreement [20]. Thus, Li and Lee proposed a new authentication scheme with user anonymity for wireless communications.

Differently from the previous researches, Li and Lee claimed two more session keys to enhance the entire security of the scheme. Li and Lee's scheme establishes two more session keys, one is between MU and HA(home agent), and another is between FA and HA, besides previous researches established one session key between MU(mobile user) and FA(foreign agent). To establish two more session keys, Li and Lee used Diffie-Hellman key agreement method in their scheme. However it requires plenty of resources, and it causes inefficiency of the scheme. In addition, Li and Lee's scheme requires 12 additional modular exponentiation than He et al.'s scheme.

Thus, in this paper, we propose an efficient user authentication scheme which keeps Li and Lee's properties. The remainder of this paper is organized as follows. In section 2, we briefly review Li and Lee's scheme and, in section 3, we reveal the drawback of Li and Lee's scheme. In section 4, we propose an efficient scheme and security analysis is given in section 5. Finally, we make some conclusions in section 6.

2. Review of Li and Lee's scheme

Li and Lee's scheme consists of four phases; the registration phase, the login phase, the authentication phase and the password change phase. Following table 1 shows all notations throughout this paper.

In Li and Lee's scheme, HA initializes the scheme by choosing the public parameter (p, q, g), where g is in a multiplicative group of order q, and both p and q are public large prime numbers, where $2 \leq g \leq p-1$, $g^q \ mod \ p = 1$, and $p = 2q + 1$. The HA selects a

private key $S_{HA} = c$, and computes corresponding public key $P_{HA} = g^c$. Likewise, FA also selects a private key $S_{FA} = e$, and computes public key $P_{FA} = g^e$. Now, we briefly review of Li and Lee's authentication scheme.

2..1 Registration phase

This phase is started when MU wants to register itself to HA. This phase is performed via a secure channel, thus a malicious adversary does not capture or modify information in the communication channel. The following steps describe the registration phase.

1. $MU \rightarrow HA : ID_{MU}$, $h(ID_{MU} \oplus PW_{MU} \oplus d)$
   The MU freely chooses his/her identity ID_{MU} and password PW_{MU}, and generates a random number d. Then MU computes $h(ID_{MU} \oplus PW_{MU} \oplus d)$ and sends it with ID_{MU} to HA via secure channel.
2. $HA \rightarrow MU : TK_{MU}$, $h(\cdot)$, r
   Upon receiving the request message from MU, HA computes $TK_{MU} = h(N||ID_{MU}) \oplus h(ID_{MU} \oplus PW_{MU} \oplus d)$ and computes $r = ID_{HA} \oplus E_N[(ID_{MU}||m)]$, where m is the secret value for each mobile user and HA does not store it. Finally, HA issues a smartcard which contains TK_{MU}, $h(\cdot)$, r to MU.
   Upon receiving the smartcard from HA, MU enters d into smartcard. As a result, the smartcard contains TK_{MU}, $h(\cdot)$, r, d.

2..2 Login phase

In the login phase, Li and Lee assume that the static Diffie-Hellman key shared between entity A and entity B are well-protected and the entity never shares its private key with anyone else. Following steps shows the login phase.

1. MU inserts his/her smartcard into the card reader and inputs ID_{MU} and PW_{MU}.
2. The smartcard computes $TK^*_{MU} = TK_{MU} \oplus h(ID_{MU} \oplus PW_{MU} \oplus d)$ to retrieve $h(N||ID_{MU})$. Then the smartcard computes $A = g^a \ mod \ p$, $F = E_L[T_{MU}||ID_{FA}||A]$, and $M = E_{DH}[r]$, where $L = h(T_{MU} \oplus TK^*_{MU})$ is the temporary symmetric key, a is a 256 bit random number, and $DH = P^a_{HA} \ mod \ p = g^{ac} \ mod \ p$ is the Diffie-Hellman key with HA. Both parameters A and DH can be pre-computed off-line.
3. $MU \rightarrow FA : m_1 = \{A, T_{MU}, U\}$
   MU computes $DH' = P^a_{FA} \ mod \ p = g^{ea} \ mod \ p$ and then sends the request message $m_1 = \{A, T_{MU}, U\}$ to FA, where $U = E_{DH'}[M, F, ID_{HA}, T_{MU}]$. DH' is also can be pre-computed off-line.

2..3 Authentication phase

When MU visits a new foreign network, the authentication phase is invoked. Following steps show the authentication phase.

1. FA verifies timestamp T_{MU}. If it is valid, then FA computes DH' and decrypts U to retrieve M, F, ID_{HA}, and T_{MU}. To confirm ID_{HA}, FA can recognize MU's home agent.

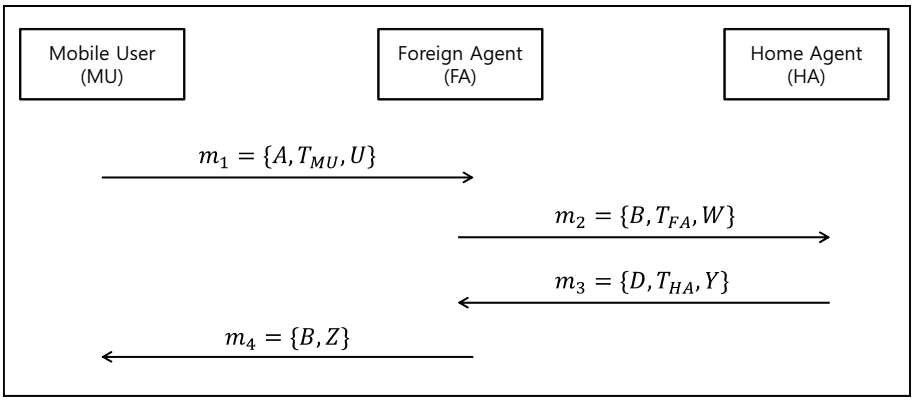

Figure 1. Login and authentication phase of Li and Lee's scheme

2. $FA \rightarrow HA : m_2 = \{B, T_{FA}, W\}$
   FA computes both $B = g^b \ mod \ p$ and $V = E_{S_{FA}}\{h(A, B, M, F, T_{MU}, T_{FA}, Cert_{FA})\}$ and sends the $m_2 = \{B, T_{FA}, W\}$ to HA, where $W = E_{DH''}[A, B, M, F, T_{MU}, V, Cert_{FA}]$. $DH'' = P_{HA}^b \ mod \ p = g^{cb} \ mod \ p$ is the Diffie-Hellman key with HA, where b is a random number generated by FA. DH'' and B is also can be pre-computed off-line.
3. $HA \rightarrow FA : m_3 = \{D, T_{HA}, Y\}$
   Upon receiving the m_2 from FA, HA verifies T_{FA}. If it is valid, HA decrypts W to retrieve A, B, M, F, T_{MU}, T_{FA}, V, and $Cert_{FA}$. Then HA verifies $Cert_{FA}$ and FA's public key P_{FA}. If they are valid, HA computes $ID_{HA} \oplus D_{DH}[M] = E_N[ID_{MU}||m]$ and decrypts $E_N[ID_{MU}||m]$ using HA's master key N to reveal MU's identity ID_{MU}. If MU is a registered user, then HA computes $L = h(T_{MU} \oplus h(N||ID_{MU}))$ and decrypts $D_L[F]$ to retrieve T_{MU}, ID_{FA}, and A.
   Then, HA checks if decrypted T_{MU} and ID_{FA} are the same as the received T_{MU} and $Cert_{FA}$. If they are valid, HA computes D, X and Y as follows;

   - $D = g^d \ mod \ p$
   - $X = E_{S_{HA}}\{h(A, B, D, T_{HA}, Cert_{HA})\}$
   - $Y = E_{SK'}[h(h(N||ID_{MU})||D)||A||B||D||X||Cert_{HA}]$

   where d is a random number generated by HA and $SK' = B^d \ mod \ p = g^{bd} \ mod \ p$ is a session key with FA. Parameter D also can be pre-computed off-line. Finally, HA sends $m_3 = \{D, T_{HA}, Y\}$ to FA.
4. $FA \rightarrow MU : m_4 = \{B, Z\}$
   Upon receiving the message from HA, FA verifies T_{HA}. If it is valid, FA computes SK' and decrypts Y to obtain $h(h(N||ID_{MU})||D)$, A, B, D, X and $Cert_{HA}$. Then FA verifies signature of HA using HA's public key P_{HA}.
   FA computes $SK = A^b \ mod \ p = g^{ab} \ mod \ p$ and sends $m_4 = \{B, Z\}$, where $Z = E_{SK}[TCert_{MU}||h(h(N||ID_{MU})||D)||A||B||D]$ to MU. The $TCert_{MU}$ is a temporary certificate which includes lifetime and other information.
5. Upon receiving the message m_4 from FA, MU computes SK and decrypts Z to obtain $TCert_{MU}$, $h(h(N||ID_{MU})||D)$, A, B, and D. Then MU computes own

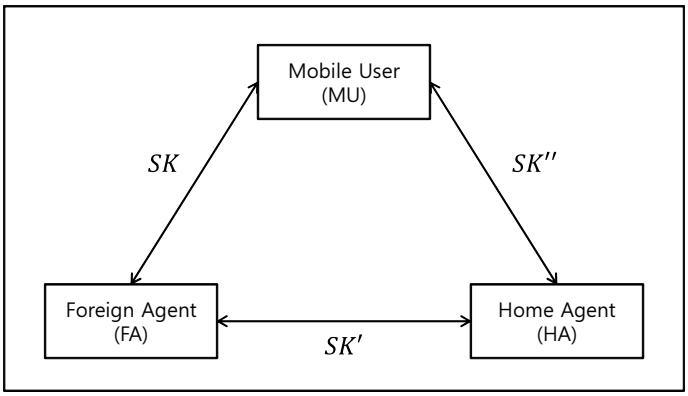

Figure 2. Three established session keys of Li and Lee's scheme

$h(h(N||ID_{MU})||D)$ and compares it with decrypted value. if they are equal, then MU confirms that FA is verified by HA and computes $SK'' = D^a \ mod \ p = g^{da} \ mod \ p$. Finally, MU establishes common session keys SK and SK'' to communicate with FA and HA.

As a result, three session keys are established and Fig.2 shows them.

2..4 Password change phase

The password update phase is invoked when a mobile user requests password update. This phase does not require any communication with other external entities, since no entity maintains the password verification table. Following steps show the password update phase.

1. Computes $TK^*_{MU} = TK_{MU} \oplus h(ID_{MU} \oplus PW_{MU} \oplus d)$ and $h(ID_{MU} \oplus PW^{new}_{MU} \oplus d')$.
2. Computes $TK^{new}_{MU} = TK^*_{MU} \oplus h(ID_{MU} \oplus PW^{new}_{MU} \oplus d')$ to replace TK_{MU} and d with TK^{new}_{MU} and d'.

3. Efficiency analysis of Li and Lee's scheme

This section describes efficiency analysis of Li and Lee's scheme. Li and Lee pointed out that He et al.'s scheme has some security vulnerabilities in their paper as follows;

1. Lack of user friendliness
2. Unfairness in key agreement
3. Attacks against the user anonymity

The goal of their scheme is naturally to deter these vulnerabilities and following table 2 shows comparison between Li and Lee's scheme and He et al.'s scheme [20].

Li and Lee aimed for their scheme to provide user anonymity and user-friendly password. Also they provide fairness in key agreement to adopt Diffie-Hellman key agreement method. As a result, differently from other previous researches, Li and Lee's scheme establishes two additional session keys, SK' and SK'', where SK' is shared between FA and HA, and SK'' is shared between MU and HA.

Table 2. Functionality comparison between Li and Lee's scheme and He et al.'s scheme

Functionality	Li and Lee	He et al.
Without password table	Yes	Yes
Freely change password	Yes	Yes
User anonymity	Yes	No
Prevention of replay attack	Yes	Yes
Prevention of impersonation attack	Yes	Yes
Non-repudiation	Yes	Yes
User friendliness	Yes	No
Fairness in key agreement	Yes	No
Session key between MU and FA	Yes	Yes
Session key between MU and HA	Yes	No
Session key between HA and FA	Yes	No

Owing to these extra session keys, Li and Lee's scheme require 12 additional modular exponentiations than He et al.'s scheme. Generally, the modular exponentiation is not appropriate for mobile device, since it consumes plenty of resources. To mitigate overhead of mobile device, Li and Lee claimed that 6 modular exponentiations can be pre-computed off-line, however, 6 operations are still required on communication process. Following table 3 shows performance comparison with Li and Lee's scheme and He et al.'s scheme [20].

Table 3. Performance comparison

Primitives	Li and Lee	He et al.
Random number generation	3	4
Modular exponentiation	12	0
Hash operation	10	18
Symmetric encryption	6	2
Symmetric decryption	7	3
Asymmetric encryption	0	1
Asymmetric decryption	0	1
Signature generation	2	2
Signature verification	2	2

Consequently, there are three drawbacks in Li and Lee's scheme.

Firstly, SK' which is shared between FA and HA, is unnecessary, since FA and HA already use PKI(public key infrastructure). In the authentication phase, upon receiving the message from FA, HA verifies FA's certificate and public key. Likewise, FA also verifies HA's certificate and public key, too. Thus, FA and HA can communicate securely using asymmetric encryption. Therefore, SK' is unnecessary.

Secondly, the modular exponentiation is unnecessary. Although, modular exponentiation may be tolerable for mobile device, it is possible to establish a session key without these expensive computations. Furthermore, Li and Lee's scheme establishes SK'' which is shared between MU and HA, in the authentication phase, but this is inappropriate, since the purpose of the authentication phase is to establish a session key between MU and FA. To enhance efficiency, SK'' has to be computed in the registration phase, instead of the

authentication phase.

Thirdly, Li and Lee's scheme does not provide session-key update phase, thus when MU wants to update current session key, MU has to process entire authentication phase. The absence of the session key update phase exacerbates the total efficiency of the scheme.

Therefore, we propose an efficient user authentication scheme with anonymity for wireless communication.

4. Improved scheme

This section describes an improved scheme. The improved scheme aims to achieve followings;

1. The improved scheme enhances efficiency than Li and Lee's scheme.
2. The improved scheme provides user anonymity and user-friendly ID and PW.
3. The improved scheme provides key fairness in key agreement.

The improved scheme consists of four phases, initial phase, login phase, authentication phase and management phase. The management phase includes password update phase and session key update phase.

Now, we demonstrate the improved scheme, by phases.

4..1 Initial phase

Fig.3 shows initial phase of the improved scheme. In this phase, MU registers itself to HA and shares a session key with HA. The following steps are performed in the initial phase.

1. $MU \rightarrow HA : ID_{MU}$, $h(ID_{MU} \oplus PW_{MU} \oplus rn)$, x_0
   MU chooses his/her identity ID_{MU} and PW_{MU} freely and computes $h(ID_{MU} \oplus PW_{MU} \oplus rn)$, where rn is a random number generated by MU. Then MU choose a random number x_0 and finally sends ID_{MU}, $h(ID_{MU} \oplus PW_{MU} \oplus rn)$, and x_0 to HA via a secure channel.
2. $HA \rightarrow MU : smartcard$, $TCert_{MU}$
   Upon receiving the message from MU, HA generates a random number e, and computes both $t = h(ID_{HA}||N||e)$ and $r = t \oplus h(ID_{MU} \oplus PW_{MU} \oplus rn)$. Then HA issues $TCert_{MU_{HA}}$, and stores ID_{HA}, $h(t)$, e, r and $h(\cdot)$ to smartcard. Finally, HA sends the smartcard and $TCert_{MU_{HA}}$ to MU via s secure channel, and computes a session key $sk_{HA} = h(t||x_0)$. As a result, HA keeps an entry (ID_{MU}, $TCert_{MU_{HA}}$).
3. MU enters rn into smartcard and computes session key $sk_{HA} = h(t||x_0)$. As a result, the smartcard contains ID_{HA}, $h(t)$, e, r, $h(\cdot)$ and rn.

As a result, MU shares a session key sk_{HA} with HA.

4..2 Login phase

When MU visits FA, login phase is started. The following steps are performed in the login phase.

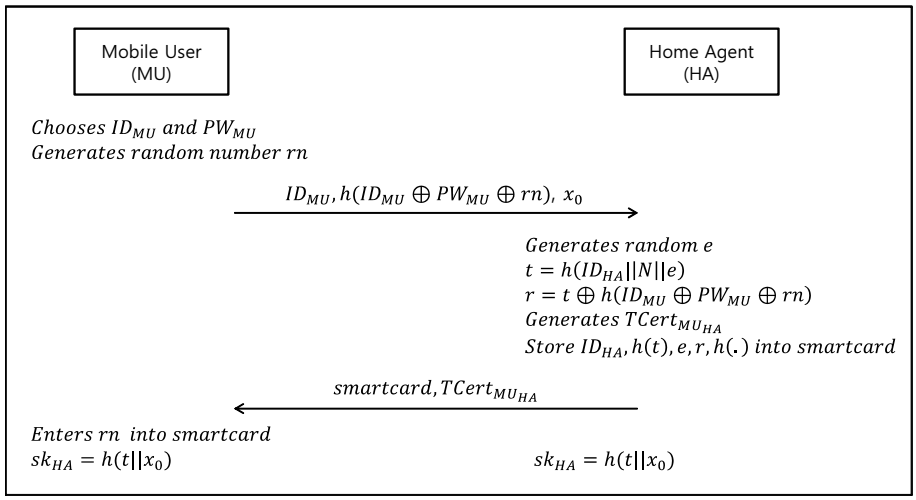

Figure 3. Initial phase of the improved scheme

1. MU inserts his/her smartcard to the card reader and inputs ID_{MU} and PW_{MU}.
2. The card reader computes $t^* = r \oplus h(ID_{MU} \oplus PW_{MU} \oplus rn)$, and then computes $h(t^*)$. After this operation, the card reader retrieves $h(t)$ from the smartcard and compares $h(t^*)$ and $h(t)$. If they are equal, the authentication phase is invoked. Otherwise, the card reader terminates the protocol.

4..3 Authentication phase

Fig.4 shows the authentication phase of our improved scheme. After the login phase, the authentication phase is invoked. The following steps are performed in the authentication phase.

1. $MU \rightarrow FA : c_1, e, ID_{HA}, T_{MU}$
   MU generates a timestamp T_{MU}, and both random numbers y_0 and y. Then, MU computes a temporary symmetric key $L = h(t||T_{MU})$, where t is retrieved in the login phase. Now MU computes a message authentication code $MAC = h(TCert_{MU_{HA}}||y||y_0||L)$, and $c_1 = E_L[TCert_{MU_{HA}}||y||y_0||MAC]$. Finally, MU sends c_1, e, ID_{HA}, T_{MU}.
2. $FA \rightarrow HA : c_1, e, w, Cert_{FA}, Sign_{FA}, T_{MU}, T_{FA}$
   Upon receiving the message from MU, FA verifies T_{MU}. If it is invalid, then FA terminates the protocol. Otherwise, FA generates a random number w, and timestamp T_{FA}. Then, FA computes the digital signature $Sign_{FA} = E_{S_{FA}}\{c_1||e||w||T_{MU}||T_{FA}\}$, and finally sends c_1, e, w, $Cert_{FA}$, $Sign_{FA}$, T_{MU} and T_{FA} to HA.
3. $HA \rightarrow FA : c_2, c_3, Cert_{HA}, Sign_{HA}, T_{HA}$
   Upon receiving the message from FA, HA verifies both T_{FA} and $Cert_{FA}$. If they are invalid, then HA terminates the protocol. Otherwise, HA verifies $Sign_{FA}$ with $Cert_{FA}$. Then, HA computes $t = h(ID_{HA}||N||e)$ using received e and $L = h(t||T_{MU})$ subsequently. Then HA decrypts c_1 with computed L to obtain $TCert_{MU_{HA}}$, y, y_0 and MAC. With both MAC and $TCert_{MU_{HA}}$, HA can verifies c_1 and MU.
   After verification, HA generates T_{HA}. Then HA computes both $c_2 = E_{sk_{HA}}$ $[h(y||$

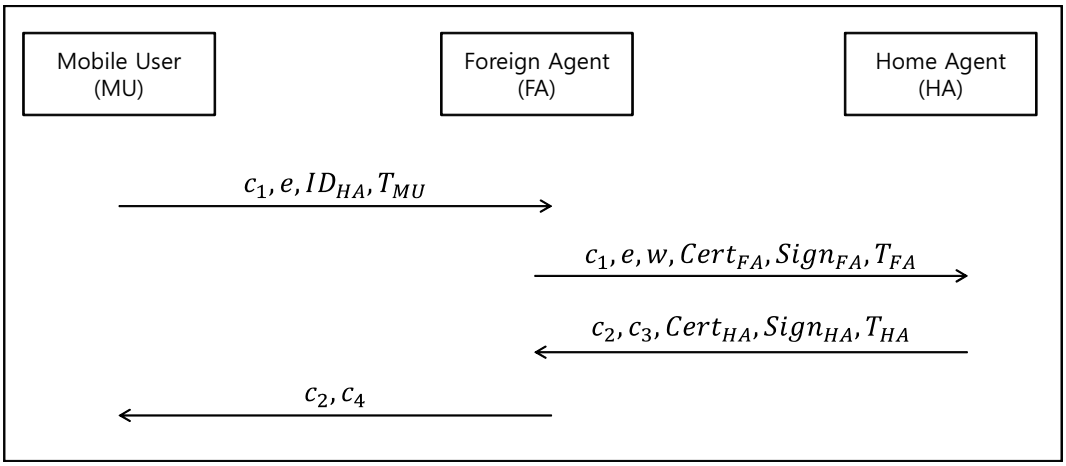

Figure 4. Login and authentication phase of the improved scheme

$w)||y_0]$, and $c_3 = E_{P_{HA}}\{h(y||w)||y_0\}$. Finally, HA sends c_2, c_3, $Cert_{HA}$, $Sign_{HA}$, and T_{HA} to FA, where $Sign_{HA} = E_{S_{HA}}\{h(c_2||c_3||T_{HA})\}$.

4. $FA \rightarrow MU$: c_2, c_4
   Upon receiving the message from HA, FA checks $Cert_{HA}$ and T_{HA}. If they are valid, FA verifies $Sign_{HA}$ and decrypts c_3 to obtain $h(y||w)||y_0$. Then FA computes a session key $sk_{FA} = h(h(y||w)||y_0))$ and issues a temporary certificate $TCert_{MU_{FA}}$. Finally, FA computes $MAC = h(c_2||sk_{FA})$ and $c_4 = E_{sk_{FA}}[TCert_{MU_{FA}}||MAC]$. and sends them to MU.
5. MU decrypts c_2 with sk_{HA} shared with HA and obtains $h(y||w)||y_0$. Then MU computes a session key $sk_{FA} = h(h(y||w)||y_0)$ and decrypts c_4 using computed key. Finally, MU checks MAC from c_4.

As a result, MU shares a session key sk_{FA} with FA. Fig.5 shows the established two session keys in the initial phase and the authentication phase.

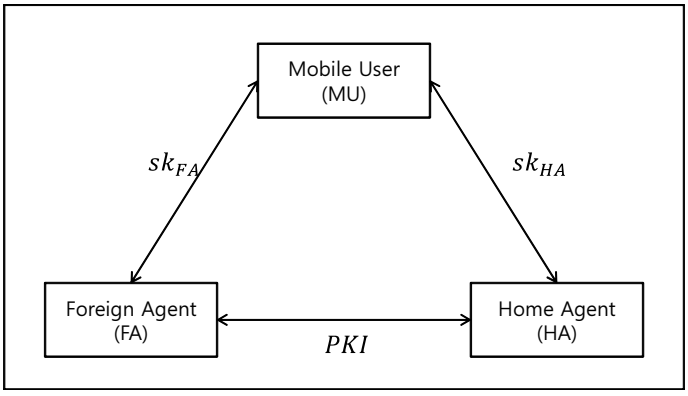

Figure 5. Two established session keys of the improved scheme

4..4 Management phase

The management phase is invoked when MU already shares a session key with FA or HA and wants to update password or current session key. The management phase includes password update phase, and session key update phase.

4..4.1 Password update phase

The password update phase is invoked when MU requests password update. This phase does not require any communication with other external entities, because no entity maintains the password verification table. Following steps show the password update phase.

1. MU inserts his/her smartcard to the card reader and inputs ID_{MU} and PW_{MU}.
2. The card reader computes $t^* = r \oplus h(ID_{MU} \oplus PW_{MU} \oplus rn)$, and then computes $h(t^*)$. After this operation, the card reader retrieves $h(t)$ from the smartcard and compares $h(t^*)$ and $h(t)$. If they are equal, the authentication succeed.
3. MU After authentication, MU enters a new password PW_{MU}^{new} and computes $r^{new} = t \oplus h(ID_{MU} \oplus PW_{MU}^{new} \oplus rn)$. Then, the card reader replace r with r^{new}.

4..4.2 Session key update phase

As a result of the initial phase and the authentication phase, MU establishes two session keys sk_{HA} and sk_{FA}, and the session key update phase is started when MU wants to update current session key. This session key updates phase is invoked by MU's request, and MU requests the update during the communication.

Session key update with HA

1. $MU \rightarrow HA : c, mac$
   The current session key sk_{HA} is $h(t||x_i)$. To update the current session key, MU generates a random number x_{i+1}. Then MU computes both $c = E_{sk_{HA}}$ $[x_{i+1}||$ $TCert_{MU_{HA}}||$ $Other\ Information]$ and mac. Finally, MU sends c and mac to HA and computes the next session key as $h(t||x_{i+1})$.
2. Upon the receiving the message from MU, HA decrypts c and verifies both $TCert_{MU_{HA}}$ and mac. If they are valid, then HA computes the next session key as $h(t||x_{i+1})$.

Session key update with FA

1. $MU \rightarrow FA : c, mac$
   The current session key sk_{FA} is $h(h(y||w)||y_i)$. To update the current session key, MU generates a random number y_{i+1}. Then MU computes $c = E_{sk_{FA}}$ $[y_{i+1}||$ $TCert_{MU_{FA}}||$ $Other\ Information]$ and mac. Finally, MU sends c and mac to FA and computes the next session key as $h(h(y||w)||y_{i+1})$.
2. Upon the receiving the message from MU, FA decrypts c and verifies both $TCert_{MU_{FA}}$ and mac. If they are valid, then FA computes the next session key as $h(h(y||w)||y_{i+1})$.

5. Security analysis of the improved scheme

This section shows that the improved scheme can withstand several possible attacks under two assumptions as follows.

1. An adversary can intercept all messages communicated among MU, FA and HA.
2. An adversary can obtain or steal legal user MUs smartcard.

Based on two assumptions, an adversary may execute certain attacks to break the improved scheme.

5..1 User anonymity

In our improved scheme, ID_{MU} is never transmitted in wireless communications except the initial phase. Owing to the fact that we assume the initial phase is executed via a secure channel, ID_{MU} is not reveal to FA or any adversary. Therefore, the improved scheme provides user anonymity.

5..2 Replay attack

In the improved scheme, each entity generates own timestamps, T_{MU}, T_{FA}, and T_{HA} in authentication phase, to prevent replay attack. Therefore, even if an attacker retransmits the intercepted message, MU, FA and HA can easily detect it by checking those timestamps.

5..3 Stolen-verifier attack

Since, HA does not keep any verifiable information, our improved scheme is secure against stolen-verifier attacks. When MU registers itself to HA, HA computes both $t = h(ID_{HA}||N||e)$ and $r = t \oplus h(ID_{MU} \oplus PW_{MU} \oplus rn)$. However, HA does not keep both e and r. That is, whatever the number of users is, HA only keeps its secret key N and its identity ID_{HA}. Therefore, our scheme is secure against stolen-verifier attack.

5..4 Known-key attack

Both session keys $sk_{HA} = h(t||x_i)$ and $sk_{FA} = h(h(y||w)||y_i)$ are established in each session. The security of the session keys depends on the security of $t = h(ID_{HA}||N||e)$ and random values. Since random values x_i and y_i are independent in each session, all session keys are independent. Thus, the knowledge of previous session keys does not make some advantage to derive a new session key, and vice versa. Therefore, the improved scheme is secure against known-key attack.

5..5 Password guessing attack

An malicious adversary can guess MU's password. Based on our two assumptions, to verify guessed password, an adversary can compute $t' = r \oplus h(ID_{MU} \oplus PW_{MU}^{guessed} \oplus rn)$ and then compare $h(t')$ and $h(t)$, or compare $h(ID_{MU} \oplus PW_{MU}^{guessed} \oplus rn)$ and $h(ID_{MU} \oplus PW_{MU} \oplus rn)$. However, owing to the fact that ID_{MU} is kept only by MU and HA, it is impossible. In our improved scheme, ID_{MU} is only transmitted in the initial phase via a secure channel, thus an adversary cannot find ID_{MU}. Therefore, the improved scheme is secure against password guessing attack.

Table 4. Functionality comparison between ours and previous researches

Functionality	Ours	Li and Lee	He et al.
Without password table	Yes	Yes	Yes
Freely change password	Yes	Yes	Yes
User anonymity	Yes	Yes	No
Prevention of replay attack	Yes	Yes	Yes
Prevention of impersonation attack	Yes	Yes	Yes
Non-repudiation	Yes	Yes	Yes
User friendliness	Yes	Yes	No
Fairness in key agreement	Yes	Yes	No
Session key between MU and FA	Yes	Yes	Yes
Session key between MU and HA	Yes	Yes	No
Session key between HA and FA	N/A	Yes	No

5..6 Forgery attack

Every transmitted data includes message authentication code or digital signature, thus every entity can notice forgery attack to verify message integrity. In the authentication phase, MU and FA sends message to each other with message authentication code MAC, thus they can detect message forgery attack. Likewise, FA and HA sends message to each other with digital signature and corresponding certificates, thus they can detect message forgery attack. Therefore, the improved scheme is secure against forgery attack.

5..7 Comparison with the improved scheme and previous researches

This section gives comparison of the improved scheme with previous researches. Following table 4 shows functionalities comparison between the improved scheme and previous researches.

As we mentioned above, the session key between FA and HA is unnecessary, since they can communicate securely, based on the PKI. Table 4 shows that the improved scheme provides same functionalities than Li and Lee's scheme, and following table 5 shows performance comparison between ours and previous researches.

Since Li and Lee's scheme does not provide session key update phase, to update the session key, entire protocol has to be executed again. On the contrary, the improved

Table 5. Performance comparison between ours and previous researches

Primitives	ours	Li and Lee	He et al.
Random number generation	3	3	4
Modular exponentiation	0	12	0
Hash operation	10	10	18
Symmetric encryption	3	6	2
Symmetric decryption	3	7	3
Asymmetric encryption	2	0	1
Asymmetric decryption	2	0	1
Signature generation	2	2	2
Signature verification	2	2	2

scheme provides session key update phase with only 1 random number generation, 1 hash operation and 1 symmetric encryption/decryption. Thus, the improved scheme is more efficient under the entire scheme.

As a result, we can conclude that the improved scheme is more efficient than previous researches.

6. Conclusion

After Zhu and Ma, several user authentication schemes with anonymity for wireless communication have been proposed, however, many of them did not provide user anonymity, perfectly.

In 2011, Li and Lee proposed a novel user authentication scheme with anonymity for wireless communications. Differently from the previous researches, Li and Lee claimed that two more session keys are required. To fulfil their claim, Li and Lee adopted Diffie-Hellman key agreement method in their scheme, although it requires plenty of resources.

To enhance the efficiency of previous schemes, in this paper, we proposed an efficient authentication scheme with anonymity.

Acknowledgements

This research was supported by the KCC(Korea Communications Commission), Korea, under the R & D program supervised by the KCA(Korea Communications Agency)(KCA-2012-12-912-06-003).

References

[1] J.Nam, S.Kim, S.Park and D.Won, *Security Analysis of a Nonce-Based User Authentication Scheme Using Smart Cards*, IEICE Trans. Fundamentals, vol.E90-A, no.1, pp.299–302, **(2007)**.

[2] J.Nam, J.Paik, U.Kim and D.Won, *Security Enhancement to a Password-Authenticated Group key Exchange Protocol for Mobile Ad-hoc Networks*, IEEE Commun., vol.12, no.2, pp.127–179, **(2008)**.

[3] J.Nam, J.Paik and D.Won, *Security Improvement on Wu and Zhu's Protocol for Password Authenticated Group Key Exchange*, IEICE Trans. Fundamentals, vol.E90-A, no.2, pp.865–868, **(2011)**.

[4] C.Chang, C.Lee, and Y.Chiu, *Enhanced authentication scheme with anonymity for roaming service in global mobility networks*, Computer Communications, vol.32, no.4, pp.611–618, **(2009)**.

[5] T.Chen, W.Lee, *A new method for using hash functions to solve remote user authentication*, Comput. Elect. Eng., vol.34, no.1, pp.53–62, **(2008)**.

[6] S.Zhong, *Efficient, anonymous, and authenticated conference key setup in cellular wireless networks*, Comput. Elect. Eng., vol.34, no.5, pp.357–367, **(2008)**.

[7] T.Chen, W.Lee, and H.Chen, *A self-verification authentication mechanism for mobile satellite communication systems*, Comput. Elect. Eng., vol.35, no.1, pp.41–48, **(2009)**.

[8] W.Juang, and J.Wu, *Two efficient two-factor authenticated key exchange protocols in public wireless LANs*, Comput. Elect. Eng., vol.35, no.1, pp.33–40, **(2009)**.

[9] J.Chen, M.Chen, and Y.Chang, *Enhancing WLAN/UMTS dual-mode services using a novel distributed multi-agent scheduling scheme*, Comput. Elect. Eng., vol.35, no.5, pp.609–621, **(2009)**.

[10] S.Zhong, *Identity-based mix: anonymous communications without public key certificates*, Comput. Elect. Eng., vol.35, no.5, pp.705–711, **(2009)**.

[11] C.Chang, S.Chang, and J.Lee, *An on-line electronic check system with mutual authentication*, Comput. Elect. Eng., vol.35, no.5, pp.757–763, **(2009)**.

[12] Y.Lee, S.Kim, and D.Won, *Enhancement of two-factor authenticated key exchange protocols in public wireless LANs*, Comput. Elect. Eng., vol.36, no.1, pp.213–223, **(2010)**.

[13] P.Dong, H.Zhang, H.Luo, T.Chi, and S.Kuo, *A network-based mobility management scheme for future Internet*, Comput. Elect. Eng., vol.36, no.2, pp.291–302, **(2010)**.

[14] R.Su, and Z.Cao, *An efficient anonymous authentication mechanism for delay tolerant networks*, Comput. Elect. Eng., vol.36, no.3, pp.435–441, **(2010)**.

[15] J.Zhu and J.Ma, *A new authentication scheme with anonymity for wireless environments*, IEEE Trans. Consumer. Elect., vol.50, no.1, pp.231–235, **(2004)**.

[16] C.Lee, M.Hwang, and I.Liao, *Security enhancement on a new authentication scheme with anonymity for wireless environments*, IEEE Trans. Indust. Elect., vol.53, no.6, pp.1683–1687, **(2006)**.

[17] C.Wu, W.Lee, and W.Tsaur, *A secure authentication scheme with anonymity for wireless communications*, IEEE Commun. Lett., vol.12, no.10, pp.722–723, **(2008)**.

[18] J.Lee, J.Chang, and D.Lee, *Security flaw of authentication scheme with anonymity for wireless communications*, IEEE Commun. Lett., vol.13, no.5, pp.292-293, **(2009)**.

[19] D.He, M.Ma, Y.Zhang, C.Chen and J.Bu, *A strong user authentication scheme with smart cards for wireless communications*, Computer communications. vol.34, no.3, pp.367–374, **(2011)**.

[20] C.Li, and C.Lee, *A novel user authentication and privacy preserving scheme with smartcards for wireless communications*, Mathematical and Computer Modelling, vol.55, no.1-2, pp.35–44, **(2012)**.

Authors

Woongryul Jeon
received the B.E. and M.E. degrees in Computer Engineering from Sungkyunkwan University, Korea, in 2006 and 2008. He is now in the Ph.D. Course in Sungkyunkwan University. His research interests include electronic voting, network security, and security assurance.

Yunho Lee
received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University, Korea, in 1991, 1993, and 2008, respectively. After working at Korea Telecom as a member of the technical staff from 1993 to 2000, he worked for KBS Internet as the director of the technical support team for 5 years. He is currently a professor at the Department of Cyber Security & Police, Gwangju University, Korea. His interests include cryptology and information security. He is particularly interested in electronic voting, digital watermarking and fingerprinting, and key exchange protocol.

Dongho Won
received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at ETRI (Electronics & Telecommunications Research Institute) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently Professor of School of Information and Communication Engineering. In the year 2002, he served as the President of KIISC (Korea Institute of Information Security & Cryptology). He was the Program Committee Chairman of the 8th International Conference on Information Security and Cryptology (ICISC 2005). His research interests are on cryptology and information security.