ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2014, T. 43, Nr. 2

Enhanced Secure Authentication Scheme with Anonymity for Roaming in Mobility Networks

Wen-Chung Kuo

National Yunlin University of Science & Technology,
Department of Computer Science and Information Engineering
No.123 University Road, Section 3, Douliou, Yunlin 64002, Taiwan, R.O.C
e-mail: simonkuo@yuntech.edu.tw

Hong-Ji Wei

University of Kang Ning, Libary and Information Center
No.188, Sec. 5, Anzhong Rd., Annan Dist., Tainan City 709, Taiwan, R.O.C.

Jiin-Chiou Cheng

Southern Taiwan University of Science and Technology,
Department of Computer Science and Information Engineering
No.1, Nantai St., Yongkang Dist., Tainan City 710, Taiwan, R.O.C.

crossref http://dx.doi.org/10.5755/j01.itc.43.2.4029

Abstract. In 2012, Kim and Kwak proposed an anonymous authentication scheme for mobility networks which claimed to improve upon the weakness of replay attack and man-in-the-middle attack in Mun *et al.*'s scheme. However, their proposed scheme is still vulnerable to replay and DoS attacks. A serious problem in their scheme is that FA cannot get the session key K_{MF}. In order to improve these shortcomings, we propose an enhanced secure authentication scheme with anonymity for roaming in mobility networks. The security analysis of our scheme demonstrates maintaining all of the security in Mun *et al.*'s scheme, but also efficiently improves upon the weaknesses in Kim-Kwak scheme.

Keywords: Authentication scheme; Anonymous authentication; Roaming authentication; Mobility networks.

1. Introduction

With popularization of smart phones and diverse applications, mobility networks are increasingly needed for mobile users. Because mobility networks transfer messages using electromagnetic waves, the message is vulnerable to be intercepted and may expose the user to privacy concerns. Many anonymous authentication schemes with roaming have been proposed for mobile networks to protect user's privacy [1, 3, 4, 6-10, 12-17]. In 2004, Zhu and Ma [17] first proposed a roaming authentication scheme with anonymity for wireless networks. However, in 2006, Lee et al. [4] pointed out that Zhu-Ma's scheme failed to anonymize the user and did not provide backward secrecy of the session key. Furthermore, Lee et al. also proposed an authentication scheme (LHL) with anonymity for wireless networks to provide anonymity and backward secrecy. Unfortunately, Wu et al. [10] proved that LHL-scheme still did not efficiently remove the security weaknesses and proposed an improved authentication scheme (WLT) with anonymity. In 2009, Lee et al. [5] and Xu and Feng [11] showed that the WLT-scheme had improved the weakness of backward secrecy, but did not efficiently protect anonymity of users.

Recently, Mun et al. [9] proposed a new framework of anonymous authentication scheme (MHLYC) to improve the weakness of anonymity in previous schemes. Kim and Kwak [3] found that the MH-LYC scheme is still weak against replay and man-in-the-middle (MITM) attacks while also proposing an improved anonymous authentication scheme (Kim-Kwak). Unfortunately, the Kim-Kwak scheme did not improve resilience against replay and denial-of-

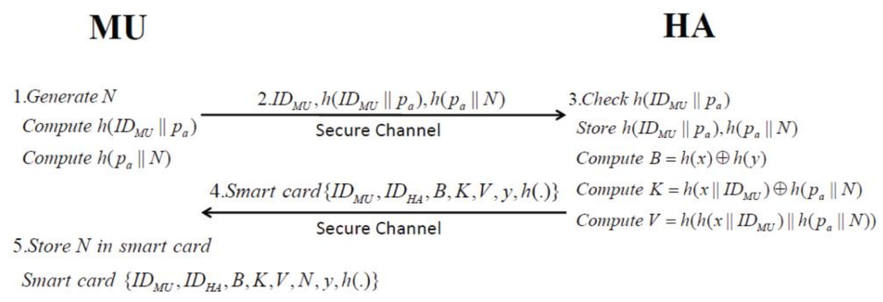

Figure 1. Registration phase of Kim-Kwak scheme

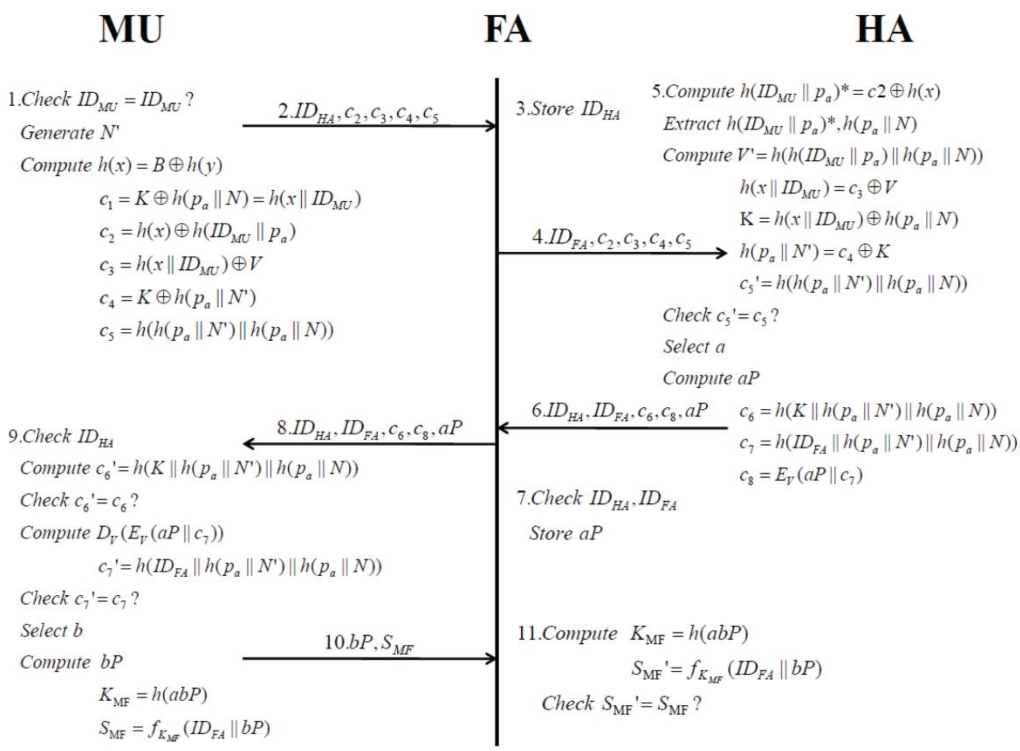

Figure 2. Authentication and key establishment phase of Kim-Kwak scheme

service(DoS) attacks even though FA cannot get the section key K_{MF}, i.e., MU cannot roaming in the FA's service area, according to our security analysis. In order to provide anonymity and protection against various attacks, we propose an enhanced secure authentication scheme for roaming in mobility networks in this paper. According to our analysis, we prove that the proposed scheme not only maintains all of the security in MHLYC-scheme but also improves the weakness against replay in the Kim-Kwak scheme.

The rest of paper is organized as follows: In Sections 2 and 3, we will review the Kim-Kwak scheme and prove the weakness in Kim-Kwak scheme. Then, we will propose an enhanced secure anonymous authentication scheme to overcome the weakness in the Kim-Kwak scheme in Section 4 and provide security analysis in Section 5. Concluding remarks are provided in Section 6.

2. Review of Kim and Kwak Scheme

In this section, we will briefly review the anonymous authentication scheme proposed by Kim and Kwak[3]. There are three phases in this scheme: registration, authentication and key establishment and update session key. The notations of the Kim-Kwak scheme are shown in Table 1 and the procedure of the Kim-Kwak scheme follows.

2.1. Registration phase

In this phase, the new MU computes $h(ID_{MU} \parallel p_a)$ and $h(p_a \parallel N)$ and then sends ID_{MU}, $h(ID_{MU} \parallel p_a)$ and $h(p_a \parallel N)$ to HA for registration. After registering with HA, MU will get a smart card with ID_{MU}, ID_{HA}, B, K, V, y and $h(\cdot)$ from HA and then MU stores N into it. Fig. 1 shows the procedure of the registration phase in detail.

Table 1. Notations

Items	Explain
MU	Mobile User
FA	Foreign Agent
HA	Home Agent
ID_x	Identity of an entity X
$h(\cdot)$	One-way hash function
N/N'	Random nonce of current session/ Random nonce of next session
$\oplus$	Exclusive OR operation
$\parallel$	Concatenation operation
$f_K(\cdot)$	MAC generation function by using key K
K_{XY}	Session key between entity X and Y
$PRNG(\cdot)$	Pseudo random number generator
E_k/D_k	Symmetric encryption/decryption with key K
p_a	Password of mobile user
x	Secret key of home agent
y	Random nonce generates for each mobile user
P	A point on the elliptic curve $E_p(a,b)$

2.2. Authentication and key establishment phase

MU can be authenticated by HA via FA after registering with HA. In this phase, MU computes $c_1 = K \oplus h(p_a \parallel N)$, $c_2 = h(x) \oplus h(ID_{MU} \parallel p_a)$, $c_3 = h(x \parallel ID_{MU}) \oplus V$, $c_4 = K \oplus h(p_a \parallel N')$ and $c_5 = h(h(p_a \parallel N') \parallel h(p_a \parallel N))$ and then sends ID_{HA}, c_2, c_3, c_4 and c_5 to FA. Next, FA transfers ID_{HA}, c_2, c_3, c_4 and c_5 to HA for authenticating MU. HA will check these messages to authenticate MU after receiving them from FA. After HA authenticates MU, he will send ID_{HA}, ID_{FA}, c_6; c_8 and aP to FA. Finally, FA can establish the session key between itself and MU by aP when receiving the above messages from HA. Fig. 2 shows the procedure of the authentication and key establishment phase in detail.

2.3. Update session key phase

If MU continually stays at the same FA, it can update the session key with FA. The update session key phase in Kim-Kwak scheme [3] is the same with MHLYC-scheme [9].

3. Weakness of Kim-Kwak Scheme

In 2012, Kim and Kwak [3] proposed an improved anonymous authentication scheme to overcome that MHLYC was susceptible to the replay attack and MITM attacks. According to our security analysis, however,the Kim-Kwak scheme did not improve resilience against replay or DoS attacks. Another issue of this scheme is that FA cannot get the session key K_{MF}. Following is a brief analysis of the security of the Kim-Kwak scheme.

3.1. Replay attack: in the authentication and key establishment phase

In this phase, the attacker is able to intercept messages ID_{HA}, c_2, c_3, c_4 and c_5 between MU and FA and tries to replay it to HA to impersonate MU. Because HA does not store $h(p_a \parallel N')$ into its database after authenticating MU, the attacker still can authenticate with HA by using intercepted messages and impersonate MU to communicate with others successfully.

3.2. DoS attack: in update session key phase

In this phase, the attacker can calculate $b_i'P$, for $i = 1, \ldots, n$, and constantly send it to FA for update session key. Because FA does not check the validity of $b_i'P$, it will make a response with a_iP and S_{MF_i} for each request. Therefore, the attacker can mount DoS attack with a flood of packets for request to block services of FA.

3.3. FA cannot get the session key K_{MF}

FA obtains aP and bP from HA and MU, respectively. FA still can not compute $K_{MF} = h(abP)$ because aP is calculated by HA and it is difficult to derive a from aP. Therefore, FA cannot calculate K_{MF} and establish the session key with MU in the authentication and key establishment phase.

4. Proposed Enhanced Secure Anonymous Authentication Scheme

MU wants to register with HA before using FA's roaming service. The registration phase procedure is as follows:

(R.1) $MU \rightarrow HA: ID_{MU}, h(ID_{MU} \parallel p_a), h(p_a \parallel N_0)$
MU generates a random number N_0 by $PRNG(\cdot)$, computes $h(ID_{MU} \parallel p_a)$ and $h(p_a \parallel N_0)$ with his own password p_a.

(R.2) $HA \rightarrow MU: ID_{MU}, ID_{HA}, B, K, V, y, h(\cdot)$ HA stores $h(ID_{MU} \parallel p_a)$ and $h(p_a \parallel N_0)$ from MU into its database and computes $B = h(x) \oplus h(y)$, $K = h(p_a \parallel N_0) \oplus h(x \parallel ID_{MU})$ and $V = h(h(ID_{MU} \parallel p_a) \parallel h(p_a \parallel N_0))$. Then, HA stores ID_{MU}, ID_{HA}, B, K, V, y and $h(\cdot)$ in the smart card and delivers it to MU through a secure channel.

4.2. Authentication and establishment of session key

MU can conduct anonymous authentication while roaming via FA after registering with HA. The procedure of authentication and establishment of session key phase is shown as follows:

(A.1) $MU \rightarrow FA: ID_{HA}, c_2, c_3, c_4, c_5$
MU inserts its smart card and inputs ID'_{MU} and p_a. The smart card checks whether ID'_{MU} equals the original ID_{MU}. If they are equal, then MU generates a random number N_{i+1} using $PRNG(\cdot)$ and computes $h(x) = B \oplus h(y)$, $c_1 = K \oplus h(p_a \parallel N_0)$, $c_2 = h(x) \oplus h(ID_{MU} \parallel P_a)$, $c_3 = h(x \parallel ID_{MU}) \oplus V$, $c_4 = K \oplus h(p_a \parallel N_{i+1})$ and $c_5 = h(h(p_a \parallel N_{i+1}) \parallel h(p_a \parallel N_i))$. Finally, MU sends ID_{HA}, c_2, c_3, c_4 and c_5 to FA.

(A.2) $FA \rightarrow HA: ID_{FA}, c_2, c_3, c_4, c_5, aP$
FA selects a new random number a and computes aP. Then, FA stores ID_{HA} and aP and sends $ID_{FA}, c_2, c_3, c_4, c_5$ and aP to HA.

(A.3) $HA \rightarrow FA: ID_{HA}, ID_{FA}, c_6, c_8$
HA performs the following steps to authenticate MU while receiving messages from MU.

Step 1. Compute $h(ID_{MU} \parallel p_a) = c_2 \oplus h(x)$.

Step 2. Compute $V = h(h(ID_{MU} \parallel p_a) \parallel h(p_a \parallel N_0))$.

Step 3. Compute $h(x \parallel ID_{MU}) = V \oplus c_3$.

Step 4. Compute $K = h(p_a \parallel N_0) \oplus h(x \parallel ID_{MU})$.

Step 5. Compute $h(p_a \parallel N_{i+1}) = K \oplus c4$.

Step 6. Compute $c'_5 = h(h(p_a \parallel N_{i+1}) \parallel h(p_a \parallel N_i))$.

Step 7. Check whether c'_5 equals to c_5.

If it exists HA, stores $h(p_a \parallel N_{i+1})$ in its database for next session.

Then, HA computes $c_6 = h(K \parallel h(p_a \parallel N_{i+1}) \parallel h(p_a \parallel N_i))$, $c_7 = h(ID_{FA} \parallel h(p_a \parallel N_{i+1}) \parallel h(p_a \parallel N_i))$ and $c_8 = E_V(aP \parallel c_7)$. Thus, HA sends ID_{HA}, ID_{FA}, c_6 and c_8 to FA. Otherwise, if c'_5 does not equal c_5. HA rejects this communication request between MU and HA.

(A.4) $FA \rightarrow MU: ID_{HA}, ID_{FA}, c_6, c_8, aP$
FA checks ID_{HA} and aP. If they exist in the database, FA authenticates HA and sends ID_{HA}, ID_{FA}, c_6 and c_8 to MU.

(A.5) $MU \rightarrow FA: bP, S_{MF}, UID$
MU checks that the information ID_{HA} from FA is equal to the original ID_{HA} which has been sent to FA previously. If it exists, then MU computes $c'_6 = h(K \parallel h(p_a \parallel N_{i+1}) \parallel h(p_a \parallel N_i))$, $c'_7 = h(ID_{FA} \parallel h(p_a \parallel N_i) \parallel h(p_a \parallel N_{i+1}))$, $D_V(c_8)$ and compares c'_6 and c'_7 with received c_6 and c_7 for authenticating HA and FA, respectively. If they are equal, MU selects a random number b and computes bP, $UID = h(ID_{MU} \parallel h(y))$, $K_{MF} = h(abP)$ and $S_{MF} = f_{K_{MF}}(ID_{FA} \parallel bP \parallel UID)$. Then MU sends bP, S_{MF} and UID to FA.

(A.6) After receiving the message from MU, FA computes KMF = h(abP) and $S'_{MF} = f_{K_{MF}}(ID_{FA} \parallel bP \parallel UID)$ and compares S'_{MF} with received SMF for authenticating MU. If they are equal, FA authenticates MU and stores bP, UID and K_{MF} into its database.

4.3. Update session key phase

If MU stays in FA's region for some time, MU must update the session key with FA. The procedure to update the session key is shown as follows:

(U.1) $MU \rightarrow FA: E_{K_{MF_{i-1}}}(b_iP),\ UID$
MU selects a new random number b_i and computes b_iP. Then, MU encrypts b_iP with $K_{MF_{i-1}} = h(a_{i-1}b_{i-1}P)$ and sends $E_{K_{MF_{i-1}}}(b_iP)$ and UID to FA.

(U.2) $FA \rightarrow MU: E_{K_{MF_{i-1}}}(a_iP),\ S_{MF_i}$
FA extracts $K_{MF_{i-1}}$ from the database by received UID and computes $D_{K_{MF_{i-1}}}(E_{K_{MF_{i-1}}}(b_iP))$ to obtain b_iP. Then, FA selects a new random number a_i and computes a_iP, $K_{MF_i} = h(a_ib_iP)$ and $S_{MF_i} = f_{K_{MF_i}}(a_ib_iP \parallel a_{i-1}b_{i-1}P)$. FA encrypts $E_{K_{MF_{i-1}}}(a_iP)$ and sends it to MU. Then, FA stores K_{MF_i} into its database.

(U.3) After receiving $E_{K_{MF_{i-1}}}(a_iP),\ S_{MF_i}$ from FA, MU computes $K_{MF_{i-1}} = h(a_{i-1}b_{i-1}P)$ and $D_{K_{MF_{i-1}}}(E_{K_{MF_{i-1}}}(a_iP))$ with $K_{MF_{i-1}}$ to obtain a_iP. Then, MU computes biP, $K_{MF_i} = h(a_ib_iP)$, $S'_{MF_i} = f_{K_{MF_i}}(a_ib_iP \parallel a_{i-1}b_{i-1}P)$ and checks whether S'_{MF_i} equals received S_{MF_i}.

If it exists, MU not only authenticates FA but also uses the new session key K_{MF_i} to communicate.

5. Security and Performance Analysis

In this section, we analyze our proposed scheme in terms of security and performance and demonstrate the comparisons of security and performance with previous proposed schemes [3, 4, 9, 10, 17] in Table 2 and Table 3, respectively.

5.1. Anonymity

Assume the attacker intercepts messages ID_{HA}, c_2, c_3, c_4 and c_5 from MU to FA. The attacker cannot ascertain the real identity of the mobile user because the attacker does not know $N_i, N_{i+1},\ x$ and p_a.

5.2. Secrecy of session key

In the authentication and key establishment and update session key phases, MU and FA utilize different a_iP and b_iP to establish the session key $K_{MF_i} = h(aibiP)$. Since ai and bi are different for each session and they are not determined by context, the attacker cannot calculate K_{MF_i} by $K_{MF_{i-1}}$ or $K_{MF_{i+1}}$.

5.3. Man-in-the-middle attack

In the authentication and establishment of session key phase, the attacker cannot establish a fake Man-in-the-middle session key between MU and FA because of mutual authentication between MU and FA by c_8 and S_{MF}, respectively.

5.4. Replay attack for authentication and establishment of session key phase

In the authentication and establishment of session key phase, MU selects a new random number N_{i+1} and computes $c_4 = K \oplus h(p_a \parallel N_{i+1})$ and $c_5 = h(h(p_a \parallel N_{i+1}) \parallel h(p_a \parallel N_i))$. When receiving messages from MU, HA computes c_5' and compares it with received c_5 for authenticating MU. If it exists, HA stores $h(p_a \parallel N_{i+1})$ into its database for the next authentication phase. Otherwise, HA denies this connection.

Attackers can attempt to perform replay attacks by the following two steps:

Step 1. Attackers intercept ID_{HA}, c_2, c_3, c_4 and $c_5 = h(h(p_a \parallel N_{i+1}) \parallel h(p_a \parallel N_i))$ from MU to FA.

Step 2. Attackers replay the intercepted message to FA.

However, the attacker still can not authenticate with HA by replaying the previous ID_{HA}, c_2, c_3, c_4 and c_5 from MU to FA because $c_5' = h(h(p_a \parallel N_{i+2}) \parallel h(p_a \parallel N_{i+1}))$ is not equal to c_5.

5.5. Replay attack for update session key phase

In the update session key phase, MU encrypts messages with the last session key $K_{MF_{i-1}}$ while updating the session key with FA. Because the session keys between the present phase and the last phase are different and have no correlation, the attacker can not update the session key by replaying messages transmitted from MU to FA in the update session key phase.

Table 2. Comparisons of security functionality

Scheme	Kim-Kwak[3] scheme	LHL[4] scheme	MHLYC[9] scheme	WLT[10] scheme	Zhu-Ma[17] scheme	Our scheme
Anonymity	Yes	No	Yes	No	No	Yes
Secrecy of session key	Yes	No	Yes	Yes	No	Yes
Prevent impersonation attack	Yes	No	Yes	No	No	Yes
Prevent replay attack	No	Yes	No	Yes	Yes	Yes
Prevent MITM attack	Yes	No	No	No	No	Yes
Prevent DoS attack	No	Yes	No	Yes	Yes	Yes
Mutual authentication (MU-FA)	Yes	Yes	Yes	Yes	No	Yes
Mutual authentication (MU-HA)	Yes	No	Yes	No	No	Yes
FA can establish session key K_{MF}	No	Yes	Yes	Yes	Yes	Yes

Table 3. Comparisons of computational overhead in authentication phase

Scheme	Kim-Kwak[3] scheme	LHL[4] scheme	MHLYC[9] scheme	WLT[10] scheme	Zhu-Ma[17] scheme	Our scheme
MU	8H+5XOR +2S+2P	3H+3XOR + 2S	5H+2XOR + 1S + 2P	3H + 2XOR + 2S	2H+3XOR + 2S	10H + 5XOR 2S + 2P
FA	2H+ 1S + 1P	4H+1XOR +1S + 2A	4H+2XOR + 1S + 2P	2H+ 1S + 2A	2H +1XOR + 1S + 2A	1H+ 1S 2P
HA	4H + 4XOR +1S + 1P	5H + 3XOR + 1S + 3A	3H + 3XOR	5H + 3XOR + 1S + 3A	5H + 3XOR + 1S + 3A	3H + 4XOR 1S
Total	14H + 9XOR +4S + 4P	12H + 7XOR + 4S + 5A	12H + 7XOR +2S + 4P	10H + 5XOR +4S + 5A	9H + 7XOR +4S + 5A	14H + 9XOR 4S + 4P
Computation time(sec)	2.0027	2.5026	2.0016	2.5025	2.50245	2.0027

5.6. Denial of service attack

In the update session key phase, MU encrypts biP with $K_{MF_{i-1}}$ and sends it with UID to FA. Because FA will extract a and $K_{MF_{i-1}}$ from its database by UID for verifying b_iP and $K_{MF_{i-1}}$ is different for each session, the attacker cannot mount DoS attack to block services of FA.

5.7. Performance comparison versus other schemes

In order to compare performance between schemes, we calculate the total operations in authentication phase for each scheme. From [2], authors provide an equivalence rate for comparison where $\text{RSA} = 2$, $\text{DES} = 2{,}000$, and $\text{SHA1} = 20{,}000$ operations per second. So for computing execution time, we equivalate Asymmetric, Symmetric and Hash operations with 0.5, 0.0005, and 0.00005 seconds, respectively. Note that XOR operations are discounted and considered free in these comparisons.

Table 3 shows that the computation of our proposed scheme with previous schemes [3, 4, 9, 10, 17] and proves that the computational cost of our proposed scheme is similar to Kim-Kwak scheme. Our security and performance analysis demonstrates that our proposed scheme not only retains the same computational overhead as Kim-Kwak scheme but also overcomes all weaknesses mentioned in Section 3. Furthermore, Our proposed scheme also provides several security functionalities such as anonymity, secrecy of session key and mutual authentication, and preventing impersonation, replay, MITM and DoS attacks.

6. Conclusions

In this paper, security analysis of the Kim-Kwak scheme determined susceptibility to replay and DoS attacks. In addition, MU cannot roam in the FA's service area because FA cannot create a session key K_{MF} with MU. In response, we propose an enhanced anonymous authentication scheme with roaming for mobility networks to overcome these weaknesses. We prove that our proposed scheme not only to prevents replay and DoS attacks but also allows FA to establish a session key K_{MF} with MU.

References

[1] **C. C. Chang, C. Y. Lee, Y. C. Chiu.** Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Computer Communications*, 2009, Vol. 32, No. 4, 611-618.

[2] **M. S. Huang.** Electronic file storage safety certification study report. [*Chinese*], ISBN:1009006844, 2009, http://www.airitibooks.com/detail.aspx? PublicationID=P20091103012.

[3] **J. S. Kim, J. Kwak.** Improved secure anonymous authentication scheme for roaming service in global mobility networks. *International Journal of Security and Its Applications*, 2012, Vol. 6, No. 3, 45-54.

[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*, 2006, Vol. 53, No. 5, 1683-1687.

[5] **J. S. Lee, J. H. Chang, D. H. Lee.** Security flaw of authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, 2009, Vol. 13, No. 5, 292-293.

[6] **K. Li, A. Xiu, F. He, D. H. Lee.** Anonymous authentication with unlinkability for wireless environments. *IEICE Electronics Express*, 2011, Vol. 8, No. 8, 536-541.

[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*, 2012, Vol. 55, No. 1-2,35-44.

[8] **C. T. Li.** A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. *Information Technology and Control*, 2012, Vol. 41, No. 1, 69-76.

[9] **H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, H. H. Choi.** Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modelling*, 2012, Vol. 55, 214-222.

[10] **C. C. Wu, W. B. Lee, W. J. Tsaur.** A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, 2008, Vol. 12, No. 10, 722-723.

[11] **J. Xu, D. G. Feng.** Security Flaws in Authentication Protocols with Anonymity for Wireless Environments. *ETRI Journal*, 2009, Vol. 31, No. 4, 460-462.

[12] **G. M. Yang, D. S. Wong, X. T. Deng.** Anonymous and authenticated key exchange for roaming networks. *IEEE Transactions on Wireless Communications*, 2007, Vol. 6, No. 9, 3461-3472.

[13] **G. M. Yang, D. S. Wong, X. T. Deng.** Formal security definition and efficient construction for roaming with a privacy-preserving extension. *Journal of Universal Computer Science*, 2008, Vol. 14, No. 3, 441-462.

[14] **G. M. Yang, Q. Huang, D. S. Wong, X. T. Deng.** Universal authentication protocols for anonymous wireless communications. *IEEE Transactions on Wireless Communications*, 2010, Vol. 9, No. 1, 168-174.

[15] **P. Zeng, Z. F. Cao, K. K. R. Choo, S. B. Wang.** On the Anonymity of Some Authentication Schemes for Wireless Communications. *IEEE Communications Letters*, 2009, Vol. 13, No. 3, 170-171.

[16] **T. Zhou, J. Xu.** Provable secure authentication protocol with anonymity for roaming service in global mobility networks. *Computer Networks*, 2011, Vol. 55, No. 1, 205-213.

[17] **J. Zhu, J. Ma.** A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics*, 2004, Vol. 50, No. 1, 231-235.

Received April 2013.