Kuwait J. Sci. **41** (1) pp. 155-169, 2014

Improvement of user authentication protocol with anonymity for wireless communications

BIN HU, QI XIE*, MENGJIE BAO AND NA DONG

School of Information Science and Engineering, Hangzhou Normal University, Hangzhou 310036, Zhejiang, China
**E-mail: qixie68@126.com*

ABSTRACT

To design a mobile user authentication protocol with anonymity for the global mobile network is a challenge, since wireless network is more vulnerable to attacks and mobile terminals' computational power is limited. In 2012, Li & Lee proposed a user authentication and privacy preserving scheme with smart card for wireless communications. In this paper, we improve the adversary model of this type of authentication scheme, and then demonstrate that Li & Lee's scheme is vulnerable to off-line password guessing attack. To remedy this security weakness, an improved scheme is proposed, which is more efficient than Li & Lee's scheme.

Keywords: Authentication; Key agreement; mobile networks; security; smart card.

INTRODUCTION

Nowadays many mobile users need to access the global mobility networks when they are roaming, and anonymous authentication among the mobile user (MU), the home agent (HA) and the foreign agent (FA) is an important mechanism. A secure and efficient anonymous authentication scheme should satisfy the following properties (Chang *et al.,* 2009; Chen *et al.,* 2011; He *et al.*, 2011; Jiang *et al.,* 2012; Lee *et al.,* 2006; Mun *et al.,* 2012; Wu *et al.*, 2008; Xu *et al.,* 2011; Youn *et al.,* 2009; Zhu & Ma. 2004).

(1) Mutual authentication: MU, HA and FA should authenticate each other to prevent illegal use of resources; (2) Anonymity: an adversary cannot obtain the user's identity from each session run and can also not identify the user twice from the authentication processes; (3) Efficiency: low communication cost and computation complexity due to the limited mobile terminals' computational power; (4) User friendly: the user needs not to remember long identity and can update password securely and freely; and (5) Security: the scheme can resist various known attacks.

Zhu & Ma (2004) addressed the anonymous authentication problem for wireless communications and proposed a first scheme. Later, Lee *et al.* (2006) showed that Zhu & Ma's scheme is vulnerable to forgery attacks, and does not provide perfect backward secrecy and mutual authentication, then they proposed an improved scheme. Wu *et al.* (2008) pointed out that Zhu & Ma's scheme and Lee *et al.*'s scheme cannot achieve anonymity and perfect backward secrecy, and proposed the improved scheme. Unfortunately, the improved scheme as well as Chang *et al.*(2009), He *et al.* (2011), and Mun *et al.* (2012) schemes also cannot provide anonymity and suffer from some attacks, such as forgery attacks and password guessing attacks (Jiang *et al.,* 2012; Xu *et al.,* 2011; Youn *et al.,* 2009). He *et al.* (2011) proposed a new anonymous authentication scheme for roaming service in global mobility networks, but Li & Lee (2012) pointed out that He *et al.*'s scheme lacks user friendliness and user anonymity. Moreover, the participants' contribution to key agreement is unfair. Further, they proposed an improved scheme using smart card to remedy these weaknesses.

Recently, Wang (2012) and Wang & Ma (2012) addressed the adversary model of authentication scheme using smart card as: (1) The adversary has full control of the communication channel and can eavesdrop, intercept, insert, delete, and modify the transmitted messages over the public channel; (2) The adversary may either know the user's password or extract the secret information stored in the smart card, but not both.

An additional condition should be added for addressing the anonymity of authentication schemes in the adversarial model, that is: (3) The adversary cannot identify the user's identity from the authentication process and can also not identify the user twice from all the session runs, even if he knows user's identity.

Following above model, in this paper, we will show that Li & Lee's improved scheme cannot resist the malicious FA's off-line password guessing attack. That is, if FA has ever participated the authentication process between MU and HA, and can get the information stored in the MU's smart card, then FA can launch off-line password guessing attack. To overcome this weakness, we then propose an improved scheme.

REVIEW OF LI AND LEE'S SCHEME

In this section, we briefly review Li &Lee's scheme. The trusted agent HA chooses the public parameters (p, q, g), where p and q are two large primes, $g$is a generator of a multiplicative subgroup with order q, $2 \leq g \leq p-1$, $g^q \, mod \, p = 1$, $p = 2q + 1$ is the modulus for the group; $h()$ is a one-way collision

resistant cryptographic hash function, $E_k[]/D_k[]$ and $E_k\{\}/D_k\{\}$ are symmetric and asymmetric encryption/decryption functions with key k, T_x is a time stamp generated by an entity x, $N$is HA's master private key, ($S_{HA} = c \in Z_q^*$,$P_{HA} = g^c \, mod \, p$) and ($S_{FA} = e \in Z_q^*$, $P_{FA} = g^e \, mod \, p$) be private-public key pairs of HA and FA , respectively.

Registration

The mobile user MU and HA perform the following interactive steps in this phase.

Step 1: The MU chooses his identity ID_{MU}, password PW_{MU} and a nonce d, then sends

$$\{ID_{MU}, H(ID_{MU} \oplus PW_{MU} \oplus d)\}$$

to HA over a secure channel.

Step 2: After receiving the registration information from MU, HA chooses a random number m and computes

$$TK_{MU} = H(N||ID_{MU}) \oplus H(ID_{MU} \oplus PW_{MU} \oplus d),$$

$$r = ID_{HA} \oplus E_N[(ID_{MU}||m)],$$

where the secret number m is different for every mobile user and is not stored in HA.Then, HA stores $\{TK_{MU}, H(.), r\}$ into a smart card and securely delivers it to MU.

Step 3: The MU stores d in the smart card and finally the smart card contains $\{TK_{MU}, H(.), r, d\}$.

Login

The mobile user MU inserts his smart card into the wireless mobile terminal and inputs his ID_{MU} and PW_{MU}. Then the smart card does the following steps:

Step 1: Chooses a random number a, then computes

$$TK_{MU}^* = TK_{MU} \oplus H(ID_{MU} \oplus PW_{MU} \oplus d) = H(N||ID_{MU}),$$

$$A = g^a \, mod \, p,$$

$$L = H\left(T_{MU} \oplus TK_{MU}^*\right),$$

$$F = E_L[T_{MU}||ID_{FA}||A],$$

$$M = E_{DH}[r],$$

where $DH = P_{HA}^{a} \, mod \, p = g^{ac} \, mod \, p$.

Step 2: Computes

$$DH^{'} = P_{FA}^{a} \, mod \, p = g^{ea} \, mod \, p,$$

$$U = E_{DH'}[M, F, ID_{HA}, T_{MU}].$$

Step 3: Sends $m_1 = \{A, T_{MU}, U\}$ to the foreign agent FA.

Authentication

This phase can achieve the mutual authentication between the mobile user MU and FA with the help of HA. Details are described as follows:

Step 1: The FA first verifies the validity of the timestamp T_{MU} after receiving the login request. Then the FA computes

$$DH^{'} = A^{e} \, mod \, p = g^{ae} \, mod \, p$$

and decrypts $D_{DH'}[U]$ to get $\{M, F, ID_{HA}, T_{MU}\}$.

Step 2: The FA chooses a random number b, and computes

$$B = g^{b} \, mod \, p,$$

$$V = E_{S_{FA}}\{H(A, B, M, F, T_{MU}, T_{FA}, Cert_{FA})\},$$

$$DH^{''} = P_{FA}^{b} \, mod \, p = g^{bc} \, mod \, p$$

$$m_2 = \left\{B, T_{FA}, W = E_{DH''}[A, B, M, F, T_{MU}, T_{FA}, V, Cert_{FA}]\right\}$$

where $Cert_{FA}$ is FA's certificate. After that, he sends m_2 to the HA.

Step 3: The HA verifies the validity of the timestamp T_{FA}, then computes

$$DH^{''} = B^{c} mod \, p = g^{bc} \, mod \, p$$

and decrypts $D_{DH''}[W]$ to get $\{A, B, M, F, T_{MU}, T_{FA}, V, Cert_{FA}\}$.

The HA verifies the validity of certificate $Cert_{FA}$ and public key $_{P_{FA}}$. If they are valid, the HA computes

$$DH = A^c modp = g^{ac} modp,$$

$$ID_{HA} \oplus D_{DH}[M] = E_N[ID_{MU}||m]$$

decrypts $D_N[E_N[ID_{MU}||m]]$ to get the MU's identity ID_{MU}.

If ID_{MU} is valid, the HA computes

$$L = H(T_{MU} \oplus H(N||ID_{MU}))$$

and decrypts $D_L[F]$ to get $\{T_{MU}, ID\_{FA}, A\}$.

Step 4: The HA checks whether the decrypted T_{MU} and ID_{FA} are equal to the received $T_{MU}$and ID_{FA}. If so, the HA chooses a random number f, and computes

$$D = g^f modp,$$

$$X = E_{S_{HA}}\{H(A, B, D, T_{HA}, Cert_{HA})\},$$

$$SK' = B^f modp = g^{bf} modp$$

$$Y = E_{SK'}[H(H(N||ID_{MU})||D)||A||B||D||X||Cert_{HA}],$$

where $SK^{'}$ is the session key with FA, $Cert_{HA}$ is HA's certificate. Otherwise, the FA will be notified by HA that the MU is not a legal user.

Step 5: The HA sends the message $m_3 = \{D, T_{HA}, Y\}$ to the FA.

Step 6: Upon checking T_{HA}, the FA computes

$$SK' = D^b modp = g^{fb} modp$$

and decrypts $D_{sk'}[Y]$ by using key SK' to get

$$\{H(H(N||ID_{MU})||D), A, B, D, X, Cert_{HA}\}$$

Then, the FA checks the validity of HA.

Step 7: FA computes

$$SK = A^b modp = g^{ab} modp,$$

$$Z = E_{SK}[TCert_{MU}||H(H(N||ID_{MU})||D)||A||B||D]$$

and sends a response message

$$m_4 = \{B, Z\}$$

to MU, where $TCert_{MU}$ is a temporary certificate which records lifetime and other information.

Step 8: The MU computes $SK = B^b modp = g^{ba} modp$, decrypts $D_{SK}[Z]$ and gets

$$\left\{TCert_{MU}, H^{'}(H(N||ID_{MU})||D), A, B, D\right\}.$$

The MU computes $H(H(N||ID_{MU})||D)$ and checks whether it equals to the decrypted $H^{'}(H(N||ID_{MU})||D)$. If they are equal, the authentication process is finished and the common session key SK and $SK^{''}$ are agreed.

Password change

MU can change his password by the following steps:

Step 1: The MU inserts his smart card into a terminal and enters his identity ID_{MU}, original password PW_{MU}, new password PW_{MU}^{new}, and a new random number $d^{'}$.

Step 2: The smart card computes

$$TK_{MU}^{*} = TK_{MU} \oplus H(ID_{MU} \oplus PW_{MU} \oplus d) = H(N||ID_{MU}),$$

$$TK_{MU}^{new} = TK_{MU}^{*} \oplus H\left(ID_{MU} \oplus PW_{MU}^{new} \oplus d^{'}\right).$$

Step 3: The smart card replaces TK_{MU}^{new} and $d^{'}$ with TK_{MU} and d, respectively.

ATTACK ON LI AND LEE'S SCHEME

Li & Lee's scheme achieves many merits, for example, their scheme can achieve outside attacks resistance, perfect forward secrecy and anonymity; HA and FA need not to share the secret key; and MU and HA can also generate the session key. Unfortunately, their scheme may suffer from the malicious FA's off-line password guessing attack according to the adversary model. The details are as follows:

According to the adversary model, the malicious FA_i can get the information $\{TK_{MU}, H(.), r, d\}$ stored in MU_j's smart card, in particular, FA_i may know the

cardholder's identity ID_j or know the small scope of the cardholder. If FA_i has ever helped MU_j to pass through the authentication process of home agent HA, then FA_i can launch off-line password guessing attack as follows.

In the Login phase, MU_j generates the login message $m_1 = \{A, T_{MU}, U\}$ and sends it to FA_i, where $U = E_{DH'}[M, F, ID_{HA}, T_{MU}]$, $DH' = g^{ea}p$, $F = E_L[T_{MU}||ID_{FA}||A]$, $L = H\left(T_{MU} \oplus TK^*_{MU}\right)$, $TK^*_{MU} = TK_{MU} \oplus H(ID_{MU} \oplus PW_{MU} \oplus d)$.

After receiving $m_1 = \{A, T_{MU}, U\}$, FA_i can compute DH' and $D_{DH'}[U]$ to get $\{M, F, ID_{HA}, T_{MU}\}$.

Because $L = H\left(T_{MU} \oplus TK^*_{MU}\right) = H(T_{MU} \oplus TK_{MU} \oplus H(ID_{MU} \oplus PW_{MU} \oplus d))$, then FA_i guesses ID_{MU} and PW_{MU}, where ID_{MU} maybe ID_j or ID_{MU} may belong to a small scope user. Therefore, FA_i can compute

$$L' = H\left(T_{MU} \oplus TK_{MU} \oplus H\left(ID'_{MU} \oplus PW'_{MU} \oplus d\right)\right),$$

and $E_{L'}[T_{MU}||ID_{FA}||A]$. After that, FA_i checks if $E_{L'}[T_{MU}||ID_{FA}||A]$ equals to F, if so, the guessed ID'_{MU} and $PW'_{MU}$are correct; otherwise, he guesses again. Since ID_{MU} and PW_{MU} are easy to remember, and ID_{MU} maybe known byFA_i or is searched in a small scope, and the password space is small. Hence, this attack is success.

If the malicious FA_i knows MU_j's password, then he can impersonate MU_j to access other foreign agents' resources since it can pass through the authentication process of HA. Or FA_i can sell it to other users cheaply, then the buyers can impersonate MU_j and access the resources from FA_i.

IMPROVED SCHEME

To overcome the weakness of Li & Lee's scheme, we propose the improved scheme, which consists of four stages: registration, login, authentication and password change. Note that password change is the same as that of Li & Lee's scheme.

Let E be an elliptic curve defined over a finite field with large order p, G be a generator on E with large order p, ($S_{HA} = c \in Z^*_q$,$P_{HA} = cG$) and ($S_{FA} = e \in Z^*_q$, $P_{FA} = eG$) be secret-public key pairs of HA and FA , respectively. Other notations are the same as that of Li & Lee's scheme.

Registration

The mobile user MU and HA perform the following interactive steps in this phase.

Step 1: The mobile user MU freely chooses his identity ID_{MU}, password PW_{MU} and generates a random number d. Then MU submits

$$\{ID_{MU}, H(ID_{MU} \oplus PW_{MU} \oplus d)\}$$

to HA over a secure channel.

Step 2: On receiving the message from MU, the HA chooses m and computes

$$TK_{MU} = H(N||ID_{MU}) \oplus H(ID_{MU} \oplus PW_{MU} \oplus d),$$

$$r = ID_{HA} \oplus E_N[(ID_{MU}||m)].$$

Step 3: The HA stores $\{TK_{MU}, H(.), r\}$ into the smart card and returns it to the MU.

Step 4: Finally the smart card contains $\{TK_{MU}, H(.), r, d, ID_{MU}\}$ after the MU storing d and ID_{MU} into the smart card.

Login

The MU inserts his smart card into the wireless mobile terminal and inputs his password PW_{MU}, then the smart card performs the following operations:

Step 1: Chooses a random number a, computes

$$TK^*_{MU} = TK_{MU} \oplus H(ID_{MU} \oplus PW_{MU} \oplus d) = H(N||ID_{MU}),$$

$$A = aG,$$

$$DH_{MH} = aP_{HA} = acG,$$

$$M = E_{DH_{MH}}\left[r||T_{MU}||ID_{FA}||A||TK^*_{MU}\right].$$

Step 2: Submits the login request $m_1 = \{M, ID_{HA}, A, T_{MU}\}$ to the foreign agent FA.

Authentication

This phase can achieve the mutual authentication between the mobile user MU and FA with the help of HA. Details are described as follows:

Step 1: The FA checks the validity of the timestamp T_{MU}. If it is invalid, the FA rejects this login request. Otherwise the FA chooses a random number b, computes

$$B = bG,$$

$$V = H(DH_{FH}, A, B, M, T_{MU}, T_{FA}, Cert_{FA}),$$

$$W = E_{DH_{FH}}[A, B, M, T_{MU}, T_{FA}, V, Cert_{FA}],$$

where $DH_{FH} = bP_{HA} = bcG$ and submits the message $m_2 = \{B, T_{FA}, W\}$ to the HA.

Step 2: The HA checks the validity of the timestamp T_{FA}. If it is valid, the HA computes

$$DH_{FH} = cB = cbG$$

and decrypts $D_{DH_{FH}}[W]$ to get

$$\{A, B, M, T_{MU}, T_{FA}, V, Cert_{FA}\}.$$

The HA computes $V' = H(DH_{FH}, A, B, M, T_{MU}, T_{FA}, Cert_{FA})$ and checks whether $V = V'$. If it is not match, the HA will terminate this connection. Or else, it goes to the next step.

Step 3: The HA verifies $Cert_{FA}$. If it is valid, the HA computes

$$DH_{MH} = cA,$$

decrypts $D_{DH_{MH}}[M]$ to get

$$\left\{r, T_{MU}, ID_{FA}, A, TK^*_{MU}\right\},$$

decrypts $D_N[ID_{HA} \oplus r]$ to get $\{ID_{MU}, m\}$ and computes $H(N||ID_{MU})$. Then HA checks the validity of ID_{MU} by checking $H(N||ID_{MU}) = TK^*_{MU}$. If MU is a legal user, the HA chooses a random number f, and computes

$$F = fG,$$

$$K = fB = bfG,$$

$$X = H(K, A, B, F, T_{HA}, Cert_{HA}),$$

$$Y = E_K[H(H(N||ID_{MU})||F)||A||B||F||X||Cert_{HA}].$$

and submits the message $m_3 = \{F, T_{HA}, Y\}$ to the FA.

Step 4: The FA checks the validity of the timestamp T_{HA}. If it is valid, the FA decrypts $D_K(Y)$ to get

$$\{H(H(N||ID_{MU})||F), A, B, F, X, Cert_{HA}\},$$

by $K = bF = bfG$.

Step 5: the FA verifies X and certificate $Cert_{HA}$. If they are valid, the FA computes

$$sk = bA = abG,$$

$$Z = E_{sk}\left[T_{Cert_{MU}}||H(H(N||ID_{MU})||F)||A||B||F\right]$$

where $T_{cert_{MU}}$ is a temporary certificates and records lifetime and other information. Then the FA submits the message

$$m_4 = \{B, Z\}$$

to MU.

Step 7: Once receiving the message m_4 from the FA, the MU computes

$$sk = aB = abG$$

and decrypts $D_{sk}[Z]$ to get

$$\left\{H^{'}(H(N||ID_{MU})||F), A, B, F\right\}.$$

In addition, the MU computes $H(H(N||ID_{MU})||F)$ to compare with the decrypted $H^{'}(H(N||ID_{MU})||F)$. If they are equal, the MU confirms that the FA is legal and computes the session key $sk = abG$ shared with FA. Also, the MU can compute the session key $sk^{'} = aF = afG$ with the HA.

SECURITY ANALYSIS AND PERFORMANCE COMPARISON

Security analysis

In this section, we will analyze the possible attacks on our scheme.

1. The proposed protocol provides session key security

In our scheme, the session key $sk = abG$ shared between MU and FA, MU and HA share the session key $sk^{'} = aF = afG$, which is related with random nonces a, b and f, and changed in each session run.Therefore, an adversary cannot compute other session keys if he knows one session key.

2. The proposed protocol provides user anonymity.

In the proposed scheme, ID_{MU} was well protected by symmetric cryptographic and hash operation primitives, since it is contained in r, and only HA can get the MU's real identity ID_{MU} by decrypting $D_N[ID_{HA} \oplus r]$ with its master secret key N. Obviously, the adversary is not able to get HA's master secret key N. Thus, our protocol can provide user anonymity.

On the other hand, since the login messages M contains MU's identity ID_{MU} and timestamp, it is changed in each session run, and an adversary cannot trace the login processes from the same mobile user.

3. The proposed protocol provides perfect forward secrecy.

In the proposed scheme, MU and HA share the session key $sk' = afG$.

If an attacker can know all the security keys of MU, FA and HA, and can obtain aG and fG, he still cannot compute sk' due to the Computational Diffie-Hellman (CDH) assumption.

4. The proposed protocol can be resistant to the password guessing attacks.

The proposed scheme can resist off-line dictionary attack, on-line dictionary attack, respectively.

Let's consider the off-line dictionary attack. If an adversary (may be a dishonest FA) gets the information stored in the smart card, and guesses MU's password PW'_{MU} to compute

$$TK^*_{MU}{}' = TK_{MU} \oplus H\left(ID_{MU} \oplus PW'_{MU} \oplus d\right).$$

However, the adversary cannot check if his guessed password PW'_{MU} is right or not, since TK^*_{MU} is contained in M, and only HA can decrypt it.

Next, let's consider the on-line dictionary attack. If an adversary (may be a dishonest FA) gets the information stored in the smart card, and guesses MU's password PW'_{MU} to compute

$$TK^*_{MU}{}' = TK_{MU} \oplus H\left(ID_{MU} \oplus PW'_{MU} \oplus d\right).$$

Then he generates the login message $U = E_{DH_{MF}}\left[M', ID_{HA}, T_{MU}\right]$, where

$$M' = E_{DH_{MH}}\left[r||T_{MU}||ID_{FA}||A||TK^*_{MU}{}'\right].$$

At last, HA will detect the incorrectID_{MU}, since he cannot verify $H(N||ID_{MU}) = TK^*_{MU}{}'$ if the adversary guessed password is not correct.

Therefore, the proposed scheme can resist dictionary attacks.

5. The proposed protocol can resist the replay attack.

In the proposed scheme, we insert the timestamp of all transmitted messages to resist the replay attacks.

6. The proposed protocol can resist the impersonation attacks.

Case 1: An adversary cannot impersonate MU, because he/she does not know the MU's password. According to above analyze of password guessing attack, the adversary's impersonation attack will be detected by HA.

Case 2: An adversary cannot impersonate FA, the reason is that he is unable to compute DH_{MH}, and cannot decrypt DH_{MH}. Therefore, he cannot respond the valid message to HA.

Case 3: An adversary cannot impersonate HA, since he cannot generate the valid signature to FA without knowing the HA's secret key, so the HA can detect his impersonation attack.

7. Mutual authentication

Our scheme provides mutual authentications between MU and FA, MU and HA, HA and FA by Diffie-Hellman exchange values, respectively.

Performance comparison

The following is performance comparison among our scheme and six recently proposed related schemes: Chen *et al.* (2011), He *et al.* (2011), Jiang *et al.* (2012), Li & Lee (2012), Mun *et al.* (2012) and Xu *et al.* (2011).

According to Li *et al.* (2008)'s experiment, it needs 0.0005 seconds for a one-way hash function, 0.0087 seconds for a symmetric encryption/decryption; Lee & Chang (2007) showed that an exponential operation is approximately equal to 60 symmetric encryptions/decryptions, and Li *et al.* (2012) showed that a scalar multiplication on elliptic curve is approximately equal to 29 modular multiplications, and an exponential operation is approximately equal to 240 modular multiplications. Therefore, it needs 0.063075 seconds and 0.522 seconds for a scalar multiplication on elliptic curve, and a modular exponentiation, respectively.

Consider login and verification phases of our scheme; it needs eleven scalar multiplication operations on elliptic curve, eight symmetric encryption/decryption and six hash operations. Therefore, our scheme only needs 0.77 seconds.

But for Li & Lee's scheme (2012), it needs fifteen modular exponentiation operations (where six modular exponentiation operations can be pre-computed off-line), fourteen symmetric encryption/decryption operations and ten hash operations. Therefore, their scheme needs 4.8 seconds for above-mentioned operations except pre-computations. On the other hand, their scheme needs additional computations for generation and verification of two signatures.

Additionally, Chen *et al.* (2011) and Mun *et al.* (2012) schemes need 0.06 and 0.26 seconds in login and verification phases, respectively, which are more

efficient than others. He *et al.* (2011) and Jiang *et al.* (2012) schemes need computations for four signature generation/verification operations and two public key encryption/ decryption operations in addition to 0.068 and 0.007 seconds, respectively. But these schemes have some weaknesses, such as cannot achieve anonymity, untraceability or perfect forward secrecy, etc. Therefore, the proposed scheme is considered efficient and secure.

CONCLUSIONS

In this paper, we showed that Li & Lee's improved scheme cannot resist the FA's off-line password guessing attack. In order to remedy their weakness, we propose an improved scheme, which keeps the main merits of Li & Lee's scheme. The proposed scheme is considered to be more secure and efficient than Li & Lee's scheme.

ACKNOWLEDGEMENT

This research was supported by the National Natural Science Foundation of China (No. 61070153), and Natural Science Foundation of Zhejiang Province (No. LZ12F02005).

REFERENCES

Chang, C. C., Lee, C. Y. & Chiu, Y. C. 2009. Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Computer Communications **32**(4): 611-618.

Chen,C., He, D., Chan, S., Bu, J., Gao Y. & Fan, R. 2011. Lightweight and provably secure user authentication with anonymity for the global mobility network. International Journal of Communication Systems **24**(3):347-362.

He, D., Ma, M., Zhang, Y., Chen, C. & Bu, J. 2011. A strong user authentication scheme with smart cards for wireless communications. Computer Communications **34**(3):367-374.

Jiang, Q., Ma, J., Li, G. & Yang, L. 2012. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. Wireless Personal Communications. DOI 10.1007/s11277-012-0535-4.

Lee, C. C., Hwang, M. S. & Liao, I. E. 2006. Security enhancementon a new authentication scheme with anonymityfor wireless environments. IEEE Trans. Ind. Electron **53**(5): 1683-1687.

Lee, J. S. & Chang, C. C. 2007. Secure communications for cluster-based adhoc networks using node identities.Journal of Network and Computer Applications. **30** (4): 1377-1396.

Li, C. T., Hwang, M. S. & Chu Y. P. 2008. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. Computer Communications **31**(12): 2803-2814.

Li, C. T. & Lee, C. C. 2012. A novel user authentication and privacy preserving scheme with smart cards for wireless communications. Mathematical and Computer Modelling **55**(1-2):35-44.

Li, W., Wen, Q., Su, Q. & Jin, Z. 2012. An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. Computer Communications **35**(0):188-195.

Mun, H., Han, K., Lee, Y. S., Yeun, C. Y. & Choi, H. H. 2012. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. Mathematical and Computer Modelling **55**(1-2): 214-222.

Wang, D. & Ma, C. 2012. Robust smart card based password authentication scheme against smart card loss problem. IACR Cryptology ePrint Archive 439-439.

Wang, Y. G. 2012. Password protected smart card and memory stick authentication against off-line dictionary attacks.In: Gritzalis, D., Furnell, S., M., T. (eds.). Springer Boston. SEC 2012, IFIP AICT, **376:** 489-500.

Wu, C. C., Lee, W. B. & Tsaur, W. J. 2008. A secure authentication scheme with anonymity for wireless communications. IEEE Communications Letters **12**(10):722-723.

Xu, J., Zhou, W. T. & Feng, D. G. 2011. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Computer Communications **34**(3): 319-325.

Youn, T. Y., Park, Y. H. & Li, M. J. 2009. Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks. IEEE Communications Letters **13**(7): 1118-1123.

Zhu, J. & Ma, J. 2004. A new authentication scheme with anonymity for wireless environments. IEEE Transactions on Consumer Electronics **50**(1): 230-234.

Submitted : *05/11/2012*
Revised : *10/03/2013*
Accepted : *17/03/2013*

تطوير بروتوكول التحقق من الهوية المجهولة للاتصالات اللاسلكية

بن هو و كي زي و مينجي باو و نادونج

كلية العلوم المعلوماتية والهندسة – جامعة هانغتشو – هانغتشو – تشجيانغ – الصين
الرمز البريدي: 310036

خلاصة

إن تصميم بروتوكول التحقق من الهوية المجهولة لمستخدم الهاتف النقال على شبكة الاتصال العالمية يشكل تحدياً ملحوظاً، لأن الشبكة اللاسلكية عادة ما تكون عرضة للهجمات وكذلك القدرة الحسوبية المحدودة للهواتف النقالة. وقد ابتكر الثنائي لي ولي في عام 2012 طريقة للتحقق من هوية المستخدم مع الحفاظ على الخصوصية باستخدام البطاقة الذكية للاتصالات اللاسلكية.

وفي هذا البحث نطور نموذجاً منافساً للتحقق من الهوية ومن ثم نبين بأن طريقة لي ولي معرضة للهجوم التخميني للكشف عن كلمة السر خارج نطاق الشبكية. ولعلاج هذا العجز للحماية نقترح طريقة مطورة وذات كفاءة أعلى من طريقة لي ولي .

مجلة الشريعة والدراسات الإسلامية

فصلية علمية محكمة تصدر عن مجلس النشر العلمي بجامعة الكويت
تعنى بالبحوث والدراسات الإسلامية

صدر العدد الأول في رجب ١٤٠٤هـ - أبريل ١٩٨٤م

* تهدف إلى معالجة المشكلات المعاصرة والقضايا المستجدة من وجهة نظر الشريعة الإسلامية.
* تشمل موضوعاتها معظم علوم الشريعة الإسلامية: من تفسير، وحديث، وفقه، واقتصاد وتربية إسلامية، إلى غير ذلك من تقارير عن المؤتمرات، ومراجعة كتب شرعية معاصرة، وفتاوي شرعية، وتعليقات على قضايا علمية.
* تنوع الباحثون فيها، فكانوا من أعضاء هيئة التدريس في مختلف الجامعات والكليات الإسلامية على رقعة العالمين: العربي والإسلامي.
* تخضع البحوث المقدمة للمجلة إلى عملية فحص وتحكيم حسب الضوابط التي التزمت بها المجلة، ويقوم بها كبار العلماء والمختصين في الشريعة الإسلامية، بهدف الارتقاء بالبحث العلمي الإسلامي الذي يخدم الأمة، ويعمل على رفعة شأنها، نسأل المولى عز وجل مزيداً من التقدم والازدهار.

جميع المراسلات توجه باسم رئيس التحرير

ص.ب ١٧٤٣٣ - الرمز البريدي: 72455 الخالدية - الكويت هاتف: ٢٤٨١٢٥٠٤ - ٢٤٩٨٤٧٢٣ - ٢٤٩٨٨٠٩٥
فاكس: ٢٤٨١٠٤٣٤

العنوان الإلكتروني: E-mail - jsis@ku.edu.kw

issn: 1029 - 8908

عنوان المجلة على شبكة الإنترنت: http://pubcouncil.kuniv.edu.kw/JSIS

اعتماد المجلة في قاعدة بيانات اليونسكو Social and Human Sciences Documentation Center

في شبكة الإنترنت تحت الموقع www.unesco.org/general/eng/infoserv/db/dare.html