New Efficient Password Authenticated Key Exchange Protocol for Imbalanced Wireless Networks

Chien-Lung Hsu*, Wen-Te Lin, and Yen-Chun Chou

Department of Information Management

Chang Gung University,

Tao-Yuan 333, Taiwan, ROC

Taiwan Information Security Center (TWISC),

Taipei 106, Taiwan, ROC

*clhsu@mail.cgu.edu.tw {b9244203, b9244118}@stmail.cgu.edu.tw

Received 29 March 2007; Revised 20 April 2007 ; Accepted 22 May 2007

Abstract. Yeh *et al*. recently proposed a password-based authenticated key exchange protocol based on RSA for imbalanced wireless networks. However, several scholars pointed out that Yeh *et al*.'s protocol is insecure against off-line password guessing attacks and inefficient enough for mobile devices in terms of the computational load. This paper will propose a new efficient and secure password authenticated key exchange protocol. Both security and performance of the proposed protocol are better than previously proposed protocols.

Keywords: Authentication, Key Exchange, Password, Wireless, Imbalanced, Password Guessing

1 Introduction

In a wireless network environment, information is transmitted in electromagnetic media through the air, rather than traditional wired or other physical conduits. All wireless signals traveling through the air without any protection are susceptible to analysis. This means proprietary information, healthcare records, user's identity, financial messages, or any other types of sensitive information might be compromised by malicious persons. Hence, secure communication in such an environment is a very important issue.

Password authenticated key exchange protocols allow two entities to authenticate each other with a human memorable password and agree on a secret common key shared between them. The session key is used to secure their communication channel for confidentiality. Such protocols have been widely used in wired network for their simplicity and convenience, since users can choose easy-to-remember passwords without any assistant device. Major challenges in designing password authenticated key exchange protocols in wireless networks are performance and security considerations. A wireless network is generally an imbalanced one in which computational capabilities and storage capacities of the servers are powerful and those of the mobile devices (e.g., handset, PDA, and so forth) are limited. It is difficult to implement security techniques used in wired network on mobile devices for their limited CPUs, memory, bandwidth, and storage abilities from a performance perspective. From security considerations, a password authenticated key exchange protocol must be secure against password guessing or dictionary attacks since passwords are generally drawn from a small and enumerable space. Password guessing attacks can be generally divided into three types [11]:

(i) *Detectable on-line password guessing attacks*: An adversary attempts to use his guessed password to perform an on-line transaction. If the transaction is accepted by the correspondent, the adversary is convinced of this password. Otherwise, the failed guess will be detected (and logged). Such an attack is generally unavoidable, but it can be handled appropriately. For instance, invalid trials must be controlled under appropriate intervals.

(ii) *Undetectable on-line password guessing attacks*: An adversary attempts to use his guessed password to perform an on-line transaction. Correctness of the guessed password must be verified by the responses sent from the correspondent. New transaction with the same correspondent will be initiated, provided that his guess fails. Failed guess is undetectable by the correspondent.

(iii) *Off-line password guessing attacks*: An adversary can guess user's password with eavesdropped or collected authentication messages in off-line manner. The adversary can freely guess user's password and check its correctness without being detected.

* Correspondence author

In 1992, Bellovin and Merritt [1] combined a symmetric and a asymmetric cryptographic techniques to propose a well-known encrypted key exchange (EKE) protocol against off-line password guessing attack. Since then, much research on EKE using different types of public key cryptosystems (e.g. RSA, ElGamal, and Diffie-Hellman key exchange) has been investigated [3, 4, 5]. It can be seen that these schemes are unsuitable for imbalanced wireless network from above performance perspective. In 2002, Zhu *et al*. [14] proposed a password based authenticated key exchange protocol based on RSA [9]. They claimed that their protocol can be implemented efficiently on most of the lightweight devices in wireless networks. However, Yeh *et al*. [11] latter demonstrated an undetectable on-line password guessing attacks on Zhu *et al*.'s protocol and proposed an improvement to eliminate this security flaw. Yeh *et al*. claimed that their protocol not only withstands undetectable on-line password guessing attack, but also provides explicit key authentication. Recently, Yoon and Yoo [12], Yang and Wang [10], and Zhang [13] demonstrated an off-line password guessing attack on Yeh *et al*.'s protocol to show the claimed requirement is violated. This paper will propose a new efficient password authenticated key exchange protocol for imbalanced wireless networks to eliminate the security flaw and gain better performance in terms of computational complexities, communication overheads, transmission number, and required storage.

The remainder of this paper is organized as follows. In Section 2, we give a brief review of Yeh *et al*.'s protocol [11] and discuss its security. In Section 3, we will propose our password authenticated key exchange protocol. In Section 4, we give security analyses and performance evaluations. Finally, we give the conclusions.

2 Brief Review of Yeh *et al.*'s Protocol

In this section, we will give a brief review of Yeh *et al.*'s protocol [11] and an off-line password guessing attack on Yeh *et al.*'s protocol.

2.1 Yeh *et al.*'s Protocol

There are two participants involved in Yeh *et al.*'s protocol [11]: a client B and a server A. The client B is a low-power device (e.g. PDA, handset, etc.) and the server is powerful in the imbalanced wireless networks. A and B share a password pw in advance. Let h_1, h_2, h_3, and h_4 be distinct cryptographic one-way hash functions and $E_k(M)/D_k(C)$ be a symmetric encryption/decryption of the plaintext M/the ciphertext C under the secret key k. A and B cooperatively perform the following steps for entity mutual authentication with key exchange:

Step 1. The client B sends a service request to server A.

Step 2. The server A generates a RSA public key (n, e) and private key d by using a public key generator, where n is the product of two large secret primes and $ed = 1 \pmod{\phi(n)}$.

Step 3. A randomly chooses an integer $r_A \in_R \{0, 1\}^l$ and sends (r_A, n, e) to the client B, where l is a set of all length l bits binary string.

Step 4. Upon receiving (r_A, n, e) from A, B performs an interactive protocol to verify the validity of A's public key (n, e). If the public key is invalid, B terminates this protocol. Otherwise, B chooses a random integer $r_B \in_R Z_n$, computes

$$\pi = E_{pw}(ID_A, ID_B, r_A, r_B) \quad (1)$$

$$z = \pi^e \bmod n \quad (2)$$

and sends z back to the server A.

Step 5. A computes

$$\pi = z^d \bmod n \quad (3)$$

$$(ID_A, ID_B, r_A, r_B) = D_{pw}(\pi) \quad (4)$$

Step 6. A computes

$$c_B = h_2(r_B) \quad (5)$$

$$K = h_3(r_A, c_B, ID_A, ID_B) \quad (6)$$

$$\sigma = E_K(ID_B) \tag{7}$$

and sends σ to the client B. Note that K is regarded as the secret session key shared between A and B.

Step 7. B uses his chosen random integer r_B to compute c_B' and K' by Eqs. (5) and (6), respectively. B decrypts the received σ to obtain ID_B' with the session key K'. If $ID_B' \neq ID_B$, B terminates this protocol. Otherwise, B computes $\delta = h_4(K)$ and sends it back to the server A.

Step 8. A computes $\delta' = h_4(K)$ and checks if δ' is equal to the received δ. If it does not hold, A terminates this protocol. Otherwise, A accepts the connection.

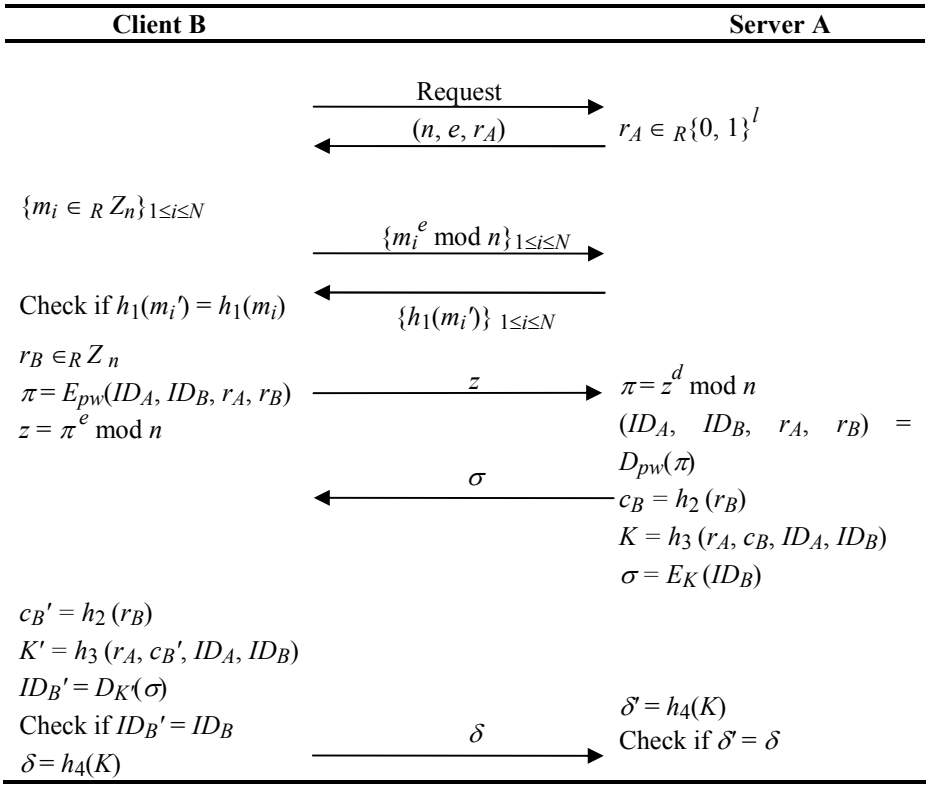

Fig. 1. Yeh *et al.*'s Protocol [11]

2.2 Discussions on Yeh *et al.*'s Protocol

In 2005, several scholars proposed an off-line password guessing attack on Yeh et al.'s protocol [11]. That is, an adversary can masquerade as a server A to obtain some authentication messages from the client, and then freely guess the client's password. Details of this attack are described below.

Step 1. The client B sends a service request to server A.

Step 2. The adversary F generates RSA private and public keys as d and (n, e) such that $ed = 1 \pmod{\phi(n)}$, respectively.

Step 3. The adversary F randomly chooses an integer $r_F \in_R \{0, 1\}^l$ and sends (r_F, n, e) to the client B.

Step 4. The client B performs an interactive protocol to verify the validity of A's public key (n, e). If the public key is invalid, B terminates this protocol. Otherwise, B computes π and z by Eqs. (1) and (2), respectively, and then transmits z back to the adversary F.

Step 5. On receiving z, the adversary F computes π by Eq. (3) and terminates this protocol.

Step 6. With the knowledge of π, the adversary guesses the client's password pw', decrypts π with pw', and checks if (ID_A, ID_B, r_A) can be correctly recovered. The adversary can repeat Step 6 to guess the client's password until correct identities are recovered. That implies the guessed password is genuine.

To eliminate above attack, Yang and Wang [10] modify the interactive protocol of Yeh *et al.*'s protocol [11]. Figure 2 illustrates Yang and Wang's improvement. Since Steps 5 to 8 of Yang and Wang's improvement are the same as those of Yeh *et al.*'s protocol, we only describe the remaining steps below.

Step 1. The client B sends a service request to A.
Step 2. The server A generates a RSA public key (n, e) and private key d.
Step 3. A randomly chooses an integer $r_A \in_R \{0, 1\}^l$, computes $\omega = ((e\|n\|r_A) \oplus h_1(pw))$ to the client B, where the symbol "‖" denotes the concatenation of binary string.
Step 4. The client B uses his password pw to recover (e, n, r_A) by $\omega \oplus h_1(pw)$, picks N integers m_i in Z_n for $1 \le i \le N$, and then cooperates with A to perform the following sub-steps:
Step 4.1 B computes $c_i = (m_i\|r_A)^e \bmod n$ (for $1 \le i \le N$) and sends it to A.
Step 4.2 A derives $m_i\|r_A$ by computing c_i^d, and sends $h_1(m_i)$ back to B.
Step 4.3 B computes $h_1(m_i)$ and checks if it is equal to the received $h_1(m_i)$.

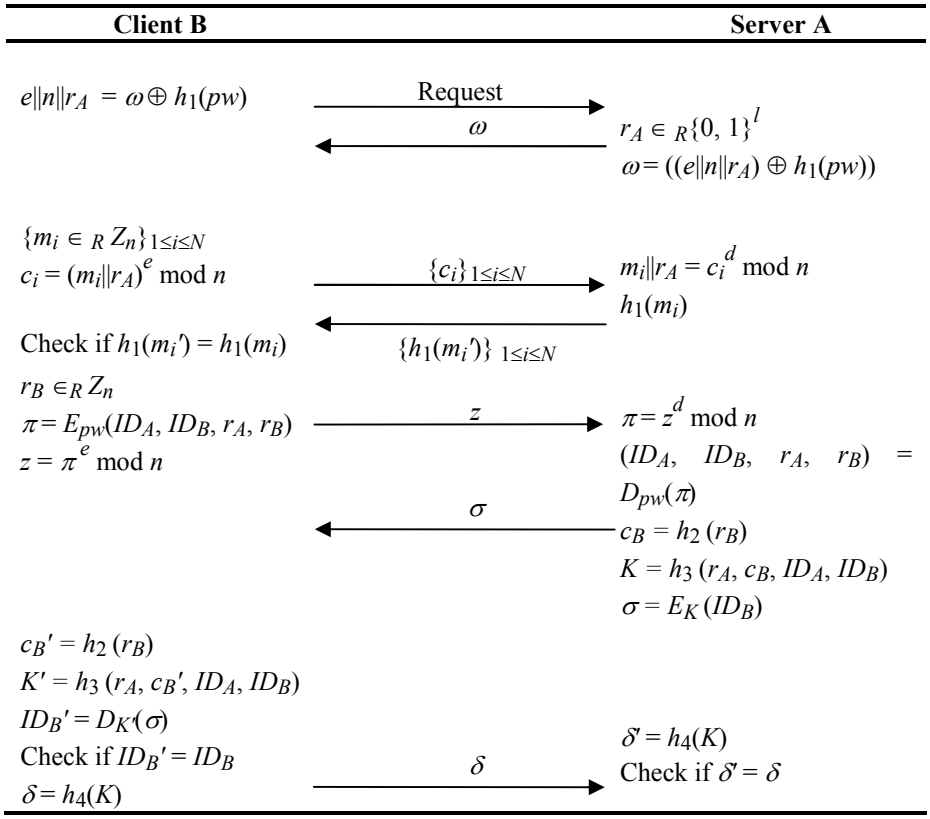

Fig. 2. Yang and Wang's Improved Protocol [11]

3 The Proposed Protocol

In the proposed protocol, we only use one one-way hash function h instead of four ones in Yeh *et al.*'s protocol. The symbols $E_k(M)$ and $D_k(C)$ are defined as a symmetric encryption and a decryption algorithms as those mentioned above. The server A and the client B also share the same password pw in advance. A and B cooperatively perform the following steps for entity authentication with key exchange as shown in Figure 3:

Step 1. The client B sends a service request to server A.
Step 2. The server A generates a RSA public key (n, e) and private key d by using a public key generator, where n is the product of two large secret primes and $ed = 1 \pmod{\phi(n)}$.
Step 3. A randomly chooses an integer $r_A \in_R Z_n$, computes

$$\pi = E_{pw}(r_A\|n\|e) \qquad (8)$$

and then sends π to the client B.

Step 4. Upon receiving π from A, B decrypts π as

$$r_A||n||e = D_{pw}(\pi) \quad (9)$$

Step 5. A and B cooperatively perform an interactive protocol to verify the validity of A's public key (n, e). If the public key is invalid, B terminates this protocol.

Step 6. B randomly chooses an integer $r_B \in_R Z_n$, computes

$$z = (r_B \oplus pw \oplus r_A)^e \bmod n \quad (10)$$

$$K = r_A \oplus r_B \oplus (ID_A||ID_B) \quad (11)$$

$$\sigma = h(r_A||r_B||ID_A||ID_B||K) \quad (12)$$

and sends (σ, z) back to the server A. Note that K is the session key shared between A and B.

Step 7. A decrypts the received z with his private key d, the password pw, and his chosen number r_A by

$$r_B' = (z^d \bmod n) \oplus pw \oplus r_A \quad (13)$$

Step 8. A further derives the shared session key K' as

$$K' = r_A \oplus r_B' \oplus (ID_A||ID_B) \quad (14)$$

and checks the following equality

$$\sigma = h(r_A||r_B'||ID_A||ID_B||K') \quad (15)$$

If it holds, legitimacy of the client B and the authenticity of the established session key K' are verified.

Step 9. A computes the following message for key confirmation as

$$\delta = h(K') \quad (16)$$

and sends it to the client B.

Step 10. On receiving the message δ, B checks its validity by Eq. (16). If above equality holds, B is convinced of the session key K and the legitimacy of the server A.

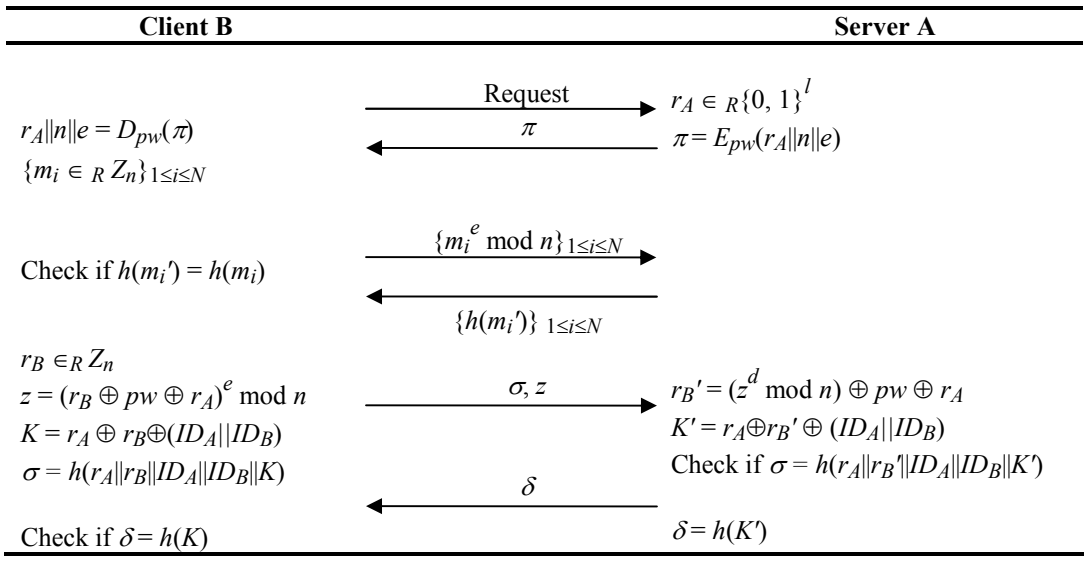

Fig. 3. The Proposed Protocol

4 Security Analyses and Performance Evaluations

In the following, we first analyze the security of our protocol and then give the performance evaluations in Sub-section 4.1 and 4.2, respectively.

4.1 Security Analyses

We analyze the security of the proposed protocol from the following security considerations and show that it is secure against some attacks below.

Considerations to on-line password guessing attack – Consider the scenario that the adversary F attempts to compromise the password *pw* by interacting with the server A or the client B. First, if the adversary masquerade as the server A, he can guess the password *pw'*, compute π' by Eq. (8), and then send π' to the client B. B can derive (r_A', n', e') by Eq. (9) using the genuine password *pw*. F then cooperates with B to perform an interactive protocol as that in Yeh *et al.*'s protocol. The adversary F, however, cannot response a valid $h(m_i)$ to B without knowing d' such that $e'd' = 1 \pmod{\phi(n')}$ if $pw' \neq pw$. Hence, this attack will be detected by the client. Second, if the adversary F masquerades as the client B, then he can guess a password *pw'* to decrypt π sent from B to obtain (r_A', n', e') by Eq. (9). However, the server is able to detect the on-line password guessing attack by checking message $m_i^{e'} \bmod n'$ sent from the adversary if $pw' \neq pw$. Therefore, the proposed protocol is secure against the on-line password guessing attack.

Considerations to off-line password guessing attack – There are two possible attacks plotted by the adversary F. In the first case, F can first intercept all communication between A and B, and then use it to guess the password *pw* by himself. It can be seen that π and *z* are computed from the password *pw*. With the knowledge of the intercepted π, the adversary cannot guess the password and check its correctness by Eq. (8) since he cannot derive the secret random integer r_A from other intercepted messages. If the adversary F attempts to guess the password *pw* by using *z*, he must derive the random numbers r_A and r_B in advance. We can see that r_B is protected by RSA encryption and r_A by the symmetric encryption under the password. The second case is similar to the off-line password guessing attack as mentioned in Subsection 2.2. It can be seen that *pw* is only known to the server A and client B. This attack will be detected by A or B as shown in the analysis of on-line password guessing attack before the adversary attempts to replace (n', e') with (n, e).

Considerations to session key compromising – If the adversary F attempts to compromise *K* by using the intercepted σ or δ, he will face the intractability of reversing the one-way hash function *h*. On the other hand, it can seen that the session key is derived as $K = r_A \oplus r_B \oplus (ID_A||ID_B)$ from Eq. (11). If the adversary F attempts to compromise *K* directly by Eq. (11), he must obtain two secret random number r_A and r_B in advance. However, r_A and r_B will not be revealed to F, and the session key *K* will not be compromised.

Considerations to replay attacks – Suppose all random numbers cannot be used twice in our protocol. Consider the scenario that the adversary F attempts to plot the impersonation attack by replaying his intercepted messages. If the adversary F replays the intercepted π to B, he will receive $m_i^e \bmod n$ from B where m_i is randomly chosen by B. The adversary cannot response a valid $h(m_i')$ to B without knowing the private key *d*. Moreover, the adversary F cannot plot a replay attack by masquerading as the client B due to the random number r_A chosen by the server A.

Considerations to mutual authentication – In the proposed protocol, the authentication is performed twice. The first one is considered in the steps 1 to 5 of our protocol, the server A and the client B will be authenticated to each other by the shared password. The second one is considered in the steps 6 to 10. The client B randomly chooses a number r_B and generates a valid (σ, *z*) by using (r_B, r_A, *pw*, *e*, *n*) to the server A. If A can derive correct r_B and *K* to pass Eq. (15), he will be convinced of B's legitimacy. If A can response a valid δ to B to pass Eq. (16), B is convinced of A's legitimacy. Hence, the proposed protocol achieves mutual authentication.

Considerations to key establishment and confirmation – We can see that the random number r_A and r_B are only known to A and B. If mutual authentication is achieved as mentioned above, r_A and r_B are verified. Hence, both A and B establish a secret session key shared between them by Eqs. (11) and (14). Moreover, if the message (σ, *z*) passes the verification Eq. (15), A is convinced of that B knows the key *K*. B is also convinced of that A knows the session *K* if Eq. (16) holds. Hence, the proposed protocol achieves key establishment and confirmation.

4.2 Performance Evaluations

Let T_h, T_E, and T_{exp} be the time for executing a one-way hash function, a symmetric encryption/decryption, and a modular exponentiation, respectively. Since the time for executing an exclusive OR operation is negligible for the comparison, we ignore it here. Let $|\varepsilon|$, $|n|$, and $|h|$ be the bit-length of a ciphertext, a modular *n*, and an output of a one-way hash function, respectively.

For simplicity, the parameter *l* is assumed to be $|n|$. We compare the performance of the proposed protocol with that of Zhu *et al.*'s [14], Yeh *et al.*'s [11], and Yang and Wang's protocols [10, 11, 14] in terms of the computational complexities, the communication costs, the number of transmission as shown in Table 1, 2, and 3.

From Tables 1, 2, and 3, it is easy to see the performance of the proposed protocol is better than that of the other protocols [10, 11, 14]. In addition, the proposed protocol uses only one one-way hash function, instead of four ones. Required storage of the proposed protocol is less than that of others and hence suitable for resource-limited mobile devices.

Table 1. Comparisons of Computational Complexities

Protocol	Client	Server	Total
Zhu *et al.*'s Protocol [14]	$(N+5)T_h + T_E + (N+1)T_{exp}$	$(N+5)T_h + T_E + (N+1)T_{exp}$	$(2N+10)T_h + 2T_E + (2N+2)T_{exp}$
Yeh *et al.*'s Protocol [11]	$(N+3)T_h + 2T_E + (N+1)T_{exp}$	$(N+3)T_h + 2T_E + (N+1)T_{exp}$	$(2N+6)T_h + 4T_E + (2N+2)T_{exp}$
Yang-Wang Protocol [10]	$(N+4)T_h + 2T_E + (N+1)T_{exp}$	$(N+4)T_h + 2T_E + (N+1)T_{exp}$	$(2N+8)T_h + 4T_E + (2N+2)T_{exp}$
The Proposed Protocol	$(N+2)T_h + T_E + (N+1)T_{exp}$	$(N+2)T_h + T_E + (N+1)T_{exp}$	$(2N+4)T_h + 2T_E + (2N+2)T_{exp}$

Table 2. Comparisons of Communication Costs

Protocol	Communication Costs
Zhu *et al.*'s Protocol [14]	$\|\varepsilon\| + (N+5)\|n\| + (N+1)\|h\|$
Yeh *et al.*'s Protocol [11]	$\|\varepsilon\| + (N+5)\|n\| + (N+1)\|h\|$
Yang-Wang Protocol [10]	$\|\varepsilon\| + (N+5)\|n\| + (N+1)\|h\|$
The Proposed Protocol	$\|\varepsilon\| + (N+1)\|n\| + (N+2)\|h\|$

Table 3. Comparisons of the Number of Transmissions

Protocol	Client	Server	Total
Zhu *et al.*'s Protocol [14]	3	3	6
Yeh *et al.*'s Protocol [11]	3	3	6
Yang-Wang Protocol [10]	3	3	6
The Proposed Protocol	2	3	5

Notice: The request transmission is excluded in the comparisons.

5 Conclusion

We have proposed a new efficient password authenticated key exchange protocol for imbalanced wireless networks. From security perspective, the proposed protocol is secure against on-line/off-line password guessing, replay, impersonation attacks. It is more secure than Zhu *et al.*'s and Yeh *et al.*'s protocols [11, 14]. Performance of the proposed protocol is also better than that of Zhu *et al.*'s, Yeh *et al.*'s, and Yang and Wang's protocols [10, 11, 14] in terms of computational complexities, communication costs, transmission number, and required storage.

Acknowledgement

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grants NSC 95-2218-E-001-001, NSC95-2218-E-011-015, and NSC94-2213-E-182-019.

References

[1] S.M. Bellovin, M. Merrit, "Encrypted key exchange: password-based protocols secure against dictionary attacks," *Proceedings of 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 72-84, 1992.

[2] Y. Ding, P. Horster, "Undetectable on-line password guessing attacks," *ACM Operating Systems Review*, Vol. 29, No. 4, pp. 77-86, 1995.

[3] W. Diffie, M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, 1976.

[4] D. Jablon, "Strong password-only authenticated key exchange," *ACM Computer Communications Review*, Vol. 20, No. 5, pp. 5-26, 1996.

[5] T. Kwon, J. song, "Efficient key exchange and authentication protocol protecting weak secrets," *IEICE Transactions on Fundamental*, Vol. E81-A, No. 1, pp. 97-111, 1998.

[6] C.L. Lin, H.M. Sun, T.Hwang, "Three-party encrypted key exchange：attacks and a solution," *ACM Operating Systems Review*, Vol. 34, No. 4, pp. 12-20, 2000.

[7] C.L. Lin, H.M. Sun, M. Steiner, T. Hwang, "Three-party encrypted key exchange without public-keys," *IEEE Communications Letters*, Vol. 5, No. 12, pp. 497-499, 2001.

[8] B.C. Neuman, T. Ts'o', "Kerberos：an authentication service for computer networks," *IEEE Communications Magazine*, Vol. 32, No. 9, pp. 33-38, 1994.

[9] R.L. Rivest, A. Shamir, L. Adelman, "A method for obtaining digital signature and public key cryptosystem," *Communications of ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[10] C.C. Yang, R.C. Wang, "Cryptanalysis of improvement of password authenticated key exchange based on RSA for imbalanced wireless networks," *IEICE Transactions on Communications*, Vol. E88-B, No. 11, pp. 4370-4372, 2005.

[11] H.T. Yeh, H.M. Sun, C.T. Yang, B.C. Chen, S.M. Tseng, "Improvement of password authenticated key exchange based on RSA for imbalanced wireless networks," *IEICE Transactions on Communications*, Vol. E86-B, No. 11, pp. 3278-3282, 2003.

[12] E.J. Yoon, K.Y. Yoo, "Cryptanalysis of password authenticated key exchange based on RSA for imbalanced wireless networks," *IEICE Transactions on Communications*, Vol. E88-B, No. 6, pp. 2627-2628, 2005.

[13] M. Zhang, "Breaking an improved password authenticated key exchange based on RSA for imbalanced wireless networks," *IEEE Communications Letters*, Vol. 9, No. 3, pp. 276-278, 2005.

[14] F. Zhu, D.S. Wong, A.H. Chan, R. Ye, "Password authenticated key exchange based on RSA for imbalanced wireless networks," *Proceedings of ISC 2002*, *LNCS 2433*, pp. 150-161, 2002.