An Improved User Authentication Scheme for Hierarchical Wireless Sensor Networks without Tamper-Proof Smart Card

Min-Shiang Hwang
Depart. of Computer Science & Information Engineering
Asia University
Taichung, Taiwan
Email: mshwang@asia.edu.tw

Eko Fajar Cahyadi
Depart. of Computer Science & Information Engineering
Asia University
Taichung, Taiwan

Yuen-Cheng Chou
Depart. of Computer Science & Information Engineering
Asia University
Taichung, Taiwan

Cheng-Ying Yang
Department of Computer Science
University of Taipei
Taipei, Taiwan

***Abstract*—Recently, Maitra et al. proposed an efficient and robust user authentication scheme for hierarchical wireless sensor networks. They claimed that their scheme does not need tamper-proof smart card and resisted different possible attacks include smart card stolen attack, impersonation attack, privileged insider attack, replay attack, off-line password guessing attack, theft attack, session key recovery attack, denial of service attack, and cluster head capture attack. However, we find some weaknesses of his scheme in this article. We show that their scheme is vulnerable to off-line password guessing with smart card stolen attack.**

***Keywords*-password; smart card; tamper-proof; user authentication; wireless sensor networks;**

I. INTRODUCTION

Remote user authentication is the mechanism that widely uses to identify the legitimate user in Internet [8], [12], [21], [27], [28]. Conventional remote user authentication schemes are suited to identify the remote users for single server environment of client/server architecture [2], [7], [17], [20], [24], [26]. However, the use of Internet has grown spectacularly. More and more users need services in different servers. In other word, the users in the network architecture are become in multi-server environment [4], [6], [10], [15]. In conventional user authentication schemes, users not only need to login to various servers with repetitive registration, but also need to remember the various user ID (identities) and passwords [3], [5], [9], [11].

In 2012, Ramasamy et al. proposed a user authentication scheme for smart cards [19]. However, Thandra et al. showed that their scheme is insecure [22]. In 2016, Thandra et al. also proposed a secure and efficient user authentication scheme [22]. However, Pan et al. shown that their scheme is vulnerable to denial of service, online and offline password guessing, and user impersonation attacks [18]. In 2016, Wei et al. proposed a user authentication scheme [25]. However, Tsai et al. shown that their scheme is vulnerable to denial of service, password guessing, and privileged insider attacks [23]. Recently, Liu et al. proposed an efficient user authentication scheme with a smart card [14]. However, Liu et al. shown that their scheme was vulnerable to the replaying attack [13].

Recently, Maitra et al. proposed an efficient and robust user authentication scheme for hierarchical wireless sensor networks [16]. They claimed that their scheme does not need tamper-proof smart card and resisted different possible attacks include smart card stolen attack, impersonation attack, privileged insider attack, replay attack, off-line password guessing attack, theft attack, session key recovery attack, denial of service attack, and cluster head capture attack. However, we find some weaknesses of his scheme in this article. We show that their scheme is vulnerable to off-line password guessing with smart card stolen attack and off-line password guessing with smart card stolen attack.

The rest of this paper is organized as follows. In Section 2, we briefly review Maitra et al.'s remote user authentication scheme. In Section 3, we analyze and show that some security flaws exist in Maitra et al.'s user authentication scheme. Finally, we present our conclusions in Section 4.

II. REVIEW OF MAITRA ET AL.'S SCHEME

In this section, we briefly review Maitra et al.'s user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card [16]. There are four participants in Maitra et al.'s remote user authentication scheme: users ($U_i, i = 1, 2, \cdots, m$ for short); Card reader (CR for short); Base stations (BS for short) and cluster head ($CH_j, j = 1, 2, \cdots, n$ for short). The scheme consists of four phases, namely the registration phase, the login phase, the authentication phase, and the password change phase. The notations used in this article are listed in Table **??**.

Table I
LIST OF NOTATION USED

Symbol	Description
U_i	i-th User
BS	Base station
SN_j	Sensor node j
CH_j	Cluster head j in the j-th cluster
pw_i	Password of user U_i
ID_i	Identity of user U_i
ID_{CH_j}	Identity of cluster head CH_j
ID_{SN_j}	Identity of sensor node SN_j
S_{CH_j}	Shared secret key between CH_j and BS
S_{SN_j}	Shared secret key between SN_j and BS
MK_{CH_j}	Unique shared master key randomly generated by the BS for CH_j
SK	Shared session key between U_i and CH_j
$h(\cdot)$	Cryptographic One-way hash function
E	Symmetric key encryption algorithm
D	Symmetric key decryption algorithm
s	Secret information of the base station
X_A	Shared secret between U_i and BS
T	Current time stamp
$\|$	Concatenation operation
$\oplus$	Bit wise XOR operation

A. The Registration Phase

In the registration phase, the base station BS makes a smart card for a new user (U_i). The registration phase is executed as follows:

1) The new user U_i firstly chooses a random number y_i, his/her identity ID_i and password pw_i.
2) U_i computes $pwr_i = h(pw_i \| y_i)$ and sends $\{ID_i, pwr_i\}$ to the base station BS through a secure channel.
3) After getting message $\{ID_i, pwr_i\}$ from the user U_i, base station computes $X_i = h(ID_i \| s) \oplus pwr_i$ and $B_i = h(h(ID_i \| s) \| pwr_i)$.
4) The base station issues a smart card for user U_i by storing $\{X_i, B_i, h(\cdot)\}$ into the memory of smart card.
5) After getting his/her smart card, user U_i stores y_i into the memory of smart card.

B. The Login Phase

In this phase, the user (U_i) wants to login to the base station BS_j for obtaining some services, the user (U_i) firstly attaches his/her smart card to a device reader and inputs his/her identity ID_i' and password PW_i'. The login phase is executed in the following:

1) Then card reader computes

$$\begin{aligned} pwr_i' &= h(pw_i \| y_i), \\ Y_i' &= X_i \oplus pwr_i', \\ B_i' &= h(Y_i' \| pwr_i'), \end{aligned}$$

and checks whether computed B_i' equals stored B_i. If true, proceed to next otherwise 'rejects' user U_i. Then, user U_i chooses ID_{CH_j} and submits it to the card reader.

2) The card reader further chooses a random number N_1 and computes

$$\begin{aligned} P_i &= h(Y_i' \| ID_{CH_j} \| N_1 \| pwr_i') \\ R_i &= N_1 \oplus pwr_i', \end{aligned}$$

and sends $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ to the base station.

C. The Authentication Phase

Upon receiving the authentication request message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ from user U_i, the base station BS executes this authentication phase in the following:

1) The base station computes

$$\begin{aligned} Y_i^* &= h(ID_i \| s), \\ pwr_i^* &= Y_i^* \oplus X_i, \\ N_1^* &= pwr_i^* \oplus R_i \\ P_i^* &= h(Y_i^* \| ID_{CH_j} \| N_1^* \| pwr_i^*). \end{aligned}$$

2) BS checks whether computed P_i^* equals sending P_i or not. If it holds good, base station further chooses a random number N_2 and computes

$$\begin{aligned} Z_i &= pwr_i^* \oplus N_2, \\ D_i &= h(Y_i^* \| N_2 \| ID_{CH_j} \| ID_i \| N_1^*). \end{aligned}$$

3) BS sends $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ to the user U_i. Again base station computes

$$\begin{aligned} N_3 &= N_2 \oplus N_1^*, \\ V_i &= h(ID_{CH_j} \| S_{CH_j}), \\ E_i &= V_i \oplus N_3, \\ A_i &= h(Y_i^* \| N_3 \| pwr_i^*), \\ L_i &= A_i \oplus V_i \\ G_i &= h(S_{CH_j} \| N_3 \| A_i \| ID_i \| ID_{CH_j}) \end{aligned}$$

4) BS sends $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ to the cluster head CH_j. After that the following computations are performed:
   a) After getting reply message $\{ID_i, ID_{CH_j}, Z_i, D_i\}$ from base station, card reader computes $N_2' = Z_i \oplus pwr_i'$, $D_i' = h(Y_i' \| N_2' \| ID_{CH_j} \| ID_i \| N_1)$ and checks whether computed D_i' equals sending D_i or not. If it holds good then computes $N_3' = N_1 \oplus N_2'$, $A_i' = h(Y_i' \| N_3' \| pwr_i')$ and session key $SK = h(ID_i \| ID_{CH_j} \| N_3' \| A_i')$.
   b) After receiving message $\{E_i, L_i, G_i, ID_i, ID_{CH_j}\}$ from base station, cluster head CH_j computes $V_i^\star = h(ID_{CH_j} \| S_{CH_j})$, $N_3^\star = V_i^\star \oplus E_i$, $A_i^\star = L_i \oplus V_i^\star$ and $G_i^\star = h(S_{CH_j} \| N_3^\star \| A_i^\star \| ID_i \| ID_{CH_j})$

and checks weather computed $G_i^\star$ equals sending G_i or not. If true, then it computes session key $SK = h(ID_i \parallel ID_{CH_j} \parallel N_3^\star \parallel A_i^\star)$.

Now, both parties (user U_i and cluster head CH_j) are agreed with common shared session key SK and can communicate securely to each other by shared secret session key SK in future.

III. Cryptanalysis of Maitra et al.'s Scheme

In this section, we will analyze Maitra et al.'s user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card [16]. Maitra et al. claimed that their scheme is resisted different possible attacks include smart card stolen attack, impersonation attack, privileged insider attack, replay attack, off-line password guessing attack, theft attack, session key recovery attack, denial of service attack, and cluster head capture attack. In this section, we show that Maitra et al.'s user authentication scheme is vulnerable to off-line password guessing with smart card stolen attack.

A. Off-line Password Guessing with Smart Card Stolen Attack

Maitra et al. claimed that an attacker is hard to derive user's password PW_i if the attacker gets the user's smart card and a login message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ between the user U_i and base station BS. In this section, we will show that Maitra et al.'s scheme is vulnerable to off-line password guessing with smart card stolen attack.

The attacker is able to intercept from the public channel. Thus the attacker obtains a login message $\{ID_i, ID_{CH_j}, P_i, R_i, X_i\}$ between the user U_i and base station BS. The attacker may guess the user's password PW_i as follows.

1) The attacker guesses the user's password PW'.
2) The smart card computes pwr_i' as follows:

$$pwr_i' = h(PW'||y_i),$$

here y_i is obtained from the smart card.

3) The smart card computes Y_i' and N_1' as follows:

$$\begin{aligned} Y_i' &= X_i \oplus pwr_i', \\ N_1' &= R_i \oplus pwr_i'. \end{aligned}$$

Here, X_i and R_i are intercepted from the last login message between the smart card and base station.

4) The attacker computes P_i' as follows:

$$P_i' = h(Y_i'||ID_{CH_j}||N_1'||pwr_i').$$

Next the attacker checks if P_i' is or not equal to P_i, here P_i is intercepted from the last login message between the smart card and base station. If it's hold, the guessed password is correct, otherwise, the attacker guess other password and checks it again as the above steps.

The attacker could repeat the above step to re-guess the other password. If it is true, this implies which the guessing password PW_i' is correct. Therefore, Maitra et al.'s user authentication scheme is vulnerable to the off-line password guessing with smart card stolen attack.

B. The improvement of Maitra et al.'s's Scheme

The main weakness of Maitra et al.'s's user authentication scheme is that the attacker could repeat to guess the password with smart card. To improve the weakness of Maitra et al.'s's scheme, the smart card in this scheme should set up the timer. If the user input the incorrect password 3 times, the smart card must initial the registration of the user.

IV. Conclusion

In this article, we have reviewed Maitra et al.'s user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card [16] and cryptanalyzed its security. Because the user password is chosen by easy to remember, we showed that Maitra et al.'s user authentication scheme cannot withstand the off-line password guessing with smart card stolen attack. We also propose an improvement of Maitra et al.'s's Scheme in this article.

Acknowledgment

This study was supported by the National Science Council of Taiwan under grant MOST 104-2221-E-468-004.

References

[1] R. Amin, "Cryptanalysis and Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment Using Smart Card", *International Journal of Network Security*, Vol. 18, No. 1, pp. 172-181, 2016.

[2] N. Anwar, I. Riadi, A. Luthfi, " Forensic SIM Card Cloning Using Authentication Algorithm", *International Journal of Electronics and Information Engineering*, Vol. 4, No. 2, pp. 71-81, 2016.

[3] C. C. Chang, W. Y. Hsueh, T. F. Cheng, "An Advanced Anonymous and Biometrics-based Multi-server Authentication Scheme Using Smart Cards", *International Journal of Network Security*, Vol. 18, No. 6, pp. 1010-1021, 2016.

[4] T. Y. Chen, C. C. Lee, M. S. Hwang, J. K. Jan, "Towards Secure and Efficient User Authentication Scheme Using Smart Card for Multi-Server Environments", *The Journal of Supercomputing*, Vol. 66, No. 2, pp. 1008-1032, 2013.

[5] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's Improvement on a Password Authentication Scheme for Multi-server Environments", *International Journal of Network Security*, Vol. 16, No. 4, pp. 318-321, 2014.

[6] D. He, W. Zhao, and S. Wu, "Security Analysis of a Dynamic ID-based Authentication Scheme for Multi-server Environment Using Smart Cards", *International Journal of Network Security*, Vol. 15, No. 5, pp. 350-356, 2013.

[7] M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[8] C. C. Lee, M. S. Hwang, I. E. Liao, "Security Enhancement on a New Authentication Scheme with Anonymity For Wireless Environments", *IEEE Transactions on Industrial Electronics*, Vol. 53, No. 5, pp. 1683-1687, 2006.

[9] L. H. Li, I. C. Lin, M. S. Hwang, "A Remote Password Authentication Scheme for Multi-server Architecture Using Neural Networks", *IEEE Transactions on Neural Networks*, Vol. 12, pp. 1498-1504, 2001.

[10] I. C. Lin, M. S. Hwang, L. H. Li, "A New Remote User Authentication Scheme for Multi-Server Architecture", *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13-22, 2003.

[11] C. H. Ling, W. Y. Chao, S. M. Chen, and M. S. Hwang, "Cryptanalysis of Dynamic Identity Based on a Remote User Authentication Scheme for a Multi-server Environment", in *2015 International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2015)*, Zhengzhou, April 11-12, 2015, Advances in Engineering Research, vol. 15, pp. 981-986, Atlantis Press, 2015.

[12] J. Ling, G. Zhao, "An Improved Anonymous Password Authentication Scheme Using Nonce and Bilinear Pairings", *International Journal of Network Security*, Vol. 17, No. 6, pp. 787-794, 2015.

[13] C. W. Liu, C. Y. Tsai, and M. S. Hwang, "Cryptanalysis of an Efficient and Secure Smart Card Based Password Authentication Scheme", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[14] Y. Liu, C. C. Chang, S. C. Chang, "An Efficient and Secure Smart Card Based Password Authentication Scheme", *International Journal of Network Security*, Vol. 19, No. 1, pp. 1-10, 2017.

[15] Y. Liu, C. C. Chang, C. Y. Sun, "Notes on An Anonymous Multi-server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Card and Biometrics", *International Journal of Network Security*, Vol. 18, No. 5, pp. 997-1000, 2016.

[16] T. Maitra, R. Amin, D. Giri, and P. D. Srivastava, "An Efficient and Robust User Authentication Scheme for Hierarchical Wireless Sensor Networks without Tamper-Proof Smart Card", *International Journal of Network Security*, Vol. 18, No. 3, pp. 553-564, 2016.

[17] E. O. Osei, J. B. Hayfron-Acquah, "Cloud Computing Login Authentication Redesign", *International Journal of Electronics and Information Engineering*, Vol. 1, No. 1, pp. 1-8, 2014.

[18] Chiu-Shu Pan, Cheng-Yi Tsai, Shyh-Chang Tsaur, Min-Shiang Hwang, "Cryptanalysis of an Efficient Password Authentication Scheme", *2016 3rd International Conference on Systems and Informatics (ICSAI 2016)*, 2016.

[19] R. Ramasamy and A. P. Muniyandi, "An Efficient Password Authentication Scheme for Smart Card", *International Journal of Network Security*, Vol. 14, No. 3, pp. 180-186, 2012.

[20] J. J. Shen, C. W. Lin, M. S. Hwang, "A Modified Remote User Authentication Scheme Using Smart Cards", *IEEE Transactions on Consumer Electronics*, Vol. 49, No. 2, pp. 414-416, 2003.

[21] M. Stanek, "Weaknesses of Password Authentication Scheme Based on Geometric Hashing", *International Journal of Network Security*, Vol. 18, No. 4, pp. 798-801, 2016.

[22] P. K. Thandra, J. Rajan, and S. A. V. S. Murty, "Cryptanalysis of an Efficient Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 2, pp. 362-368, 2016.

[23] C. Y. Tsai, C. S. Pan, and M. S. Hwang, "An Improved Password Authentication Scheme for Smart Card", *Recent Developments in Intelligent Systems and Interactive Applications*, Lecture Notes in Computer Science, Springer, 2017.

[24] Y. Wang and X. Peng, "Cryptanalysis of Two Efficient Password-based Authentication Schemes Using Smart Cards", *International Journal of Network Security*, Vol. 17, No. 6, pp. 728-735, 2015.

[25] J. Wei, W. Liu, X. Hu, "Secure and Efficient Smart Card Based Remote User Password Authentication Scheme", *International Journal of Network Security*, Vol. 18, No. 4, pp. 782-792, 2016.

[26] H. Wijayanto, M. S. Hwang, "Improvement on Timestamp-based User Authentication Scheme with Smart Card Lost Attack Resistance", *International Journal of Network Security*, Vol. 17, No. 2, 2015, pp. 160-164, 2015.

[27] H. Zhu, Y. Zhang, and Y. Zhang, "A Provably Password Authenticated Key Exchange Scheme Based on Chaotic Maps in Different Realm", *International Journal of Network Security*, Vol. 18, No. 4, pp. 688-698, 2016.

[28] X. Zhuang, C. C. Chang, Z. H. Wang, Y. Zhu, "A Simple Password Authentication Scheme Based on Geometric Hashing Function", *International Journal of Network Security*, Vol. 16, pp. 271-277, 2014.