

An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks

Huei-Ru Tseng, Rong-Hong Jan, and Wu Yang

Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan
{hueiru, rhjan, wuuyang}@cs.nctu.edu.tw

Abstract—Over the last few years, many researchers have paid a lot of attention to the user authentication problem. However, to date, there has been relatively little research suited for wireless sensor networks. Recently, Wong et al. proposed a dynamic user authentication scheme for WSNs that allows legitimate users to query sensor data at every sensor node of the network. We show that Wong et al.'s scheme is vulnerable to the replay and forgery attacks and propose a lightweight dynamic user authentication scheme for WSNs. The proposed scheme not only retains all the advantages in Wong et al.'s scheme but also enhances its security by withstanding the security weaknesses and allows legitimate users to change their passwords freely. In comparison with the previous scheme, our proposed scheme possesses many advantages, including resistance of the replay and forgery attacks, reduction of user's password leakage risk, capability of changeable password, and better efficiency.

Keywords—user authentication, wireless sensor networks, replay and forgery attacks, password.

I. INTRODUCTION

Wireless sensor network (WSN) consists of spatially distributed sensors to cooperatively monitor environmental conditions, such as temperature, humidity, pressure, motion, or vibration, at different locations. The collected data will be presented to users either upon inquiries or upon event detection. In general, most queries in WSN applications are issued at the base stations or at the backend of the application system. However, real-time data may no longer be accessed at the based station or the gateway node only. They could be accessed anywhere from a sensor node in an ad hoc manner.

For some applications, such as military surveillance, the collected data is critical. Hence, security measures should be taken to protect the collected secrets by preventing unauthorized users from gaining the information. Over the last few years, there has been a dramatic increase in the number of publications on user authentication [1-7]. However, to date, there has been relatively little research [8-10] suited for WSNs due to the resource-constrained nature, such as limited computation, battery power, and storage.

Recently, Wong et al. [10] proposed a dynamic user authentication scheme for wireless sensor networks. The proposed scheme comes with several advantages. First, it allows legitimate users to query sensor data at any of the

sensor nodes in an ad hoc manner. Second, it imposes very little computational load and requires only simple operations. Third, Wong et al. claimed that their scheme is secure against the replay and forgery attacks. However, their scheme has three security weaknesses, as follows:

- 1) It cannot protect against the replay and forgery attacks.
- 2) Passwords could be revealed by any of the sensor nodes.
- 3) A user cannot change his/her password freely.

We will discuss these weaknesses in detail later.

To overcome these weaknesses, we propose a modified scheme. The modified scheme not only fixes the weaknesses but also enhances the security of Wong et al.'s scheme. Moreover, our proposed scheme allows legitimate users to choose and change their passwords freely. In addition, the proposed scheme does not incur extra computation.

The rest of this paper is organized as follows: In Section 2, we will briefly review Wong et al.'s scheme. We analyze the scheme to show its weaknesses in Section 3. Next, a modified scheme to enhance the security of Wong et al.'s scheme is proposed in Section 4. Then, we shall analyze our proposed scheme, show that our scheme can resist several attacks, and provide a comparative study with Wong et al.'s scheme in Section 5. Finally, we will conclude our paper with possible future research directions in Section 6.

II. REVIEW OF WONG ET AL.'S SCHEME

Wong, Zheng, Cao, and Wang proposed a dynamic user authentication scheme for wireless sensor networks. Authorized users can access any of the sensor nodes in WSNs using mobile devices, such as PDAs, PCs, etc. Before issuing a query to a sensor node, a user has to register at the sensor gateway (GW) via a secure channel. Upon successful registration, the user can login to a nearest sensor login-node to retrieve sensor data. The scheme is divided into three phases: registration, login, and authentication. Before we discuss the overall operations in the scheme, it will be helpful to understand the notations used in this scheme first. We list the notations and their corresponding definitions in Table I. Three phases will be shown later again.

This paper was supported in part by Intel, in part by the National Science Council, Taiwan, Republic of China, under grant NSC 94-2752-E-009-PAE, NSC 94-2219-E-009-005, and NSC-94-2213-E-009-029 respectively, and in part by Taiwan Information Security Center at National Chiao Tung University.

TABLE I
NOTATIONS

Symbol	Definition
$userID$	A user's identity
PW	A user's password
Key	A sensor gateway-node's private key
H	A one-way hash function
TS	A timestamp
$//$	Concatenation

A. The Registration Phase

Assume a registration interface is launched on a user's mobile device. A user submits his/her ID ($userID$) and a password (PW) to a sensor gateway (GW) for registration. The GW then computes the pair (A, B) for the registering user. The (A, B) pair is computed as follows:

$$A = H(userID \parallel Key) \quad (1)$$

$$B = H(A \parallel H(PW)) \quad (2)$$

where Key is the GW's private key. Next, the GW stores the dataset $(userID, A, PW, B, TS)$ in its database. Then, the GW informs the user successful registration. Finally, the triple $(userID, A, TS)$ is distributed to all the sensor nodes.

B. The Login Phase

When a user wishes to query sensor data, he/she has to login to a sensor login-node. The user first submits his/her $userID^*$ and password PW^* to the login-node. After receiving the login information, the login-node first checks whether $userID^*$ exists in the list of datasets $(userID, A, TS)$. If not, the login-node sends $Msg(REJ_LOGIN)$ to the user. Otherwise it computes the triple (B^*, C_1, C_2) for the user. The triple (B^*, C_1, C_2) is computed as follows:

$$B^* = H(A \parallel H(PW^*)) \quad (3)$$

$$C_1 = H(T \text{ XOR } B^*) \quad (4)$$

$$C_2 = (B^* \text{ XOR } A) \quad (5)$$

where T is the current time. Then, the login-node sends $Msg(userID^*, C_1, C_2, T)$ to the GW for authentication.

C. The Authentication Phase

After receiving $Msg(userID^*, C_1, C_2, T)$ from the login-node, the GW first checks whether $userID^*$ exists in the database. If not, the GW sends $Msg(REJ_LOGIN)$ to the login-node. Otherwise it checks whether the transmission delay is within the allowed time interval ΔT . Assume the current time is T^* . If $(T^* - T) \geq \Delta T$, the GW also sends $Msg(REJ_LOGIN)$ to the login-node. Otherwise it computes (C_1^*, C_2^*) for the user.

The (C_1^*, C_2^*) pair is computed as follows:

$$C_1^* = H(T \text{ XOR } B) \quad (6)$$

$$C_2^* = (B \text{ XOR } A) \quad (7)$$

Then, the GW verifies if $(C_1^* = C_1)$ and $(C_2^* = C_2)$. If so, the GW sends $Msg(ACC_LOGIN)$ to the login-node and the login-node also sends $Msg(ACC_LOGIN)$ to the user. Otherwise the GW sends $Msg(REJ_LOGIN)$ to the login-node.

The overall handshake of Wong et al.'s scheme is illustrated in Fig. 1.

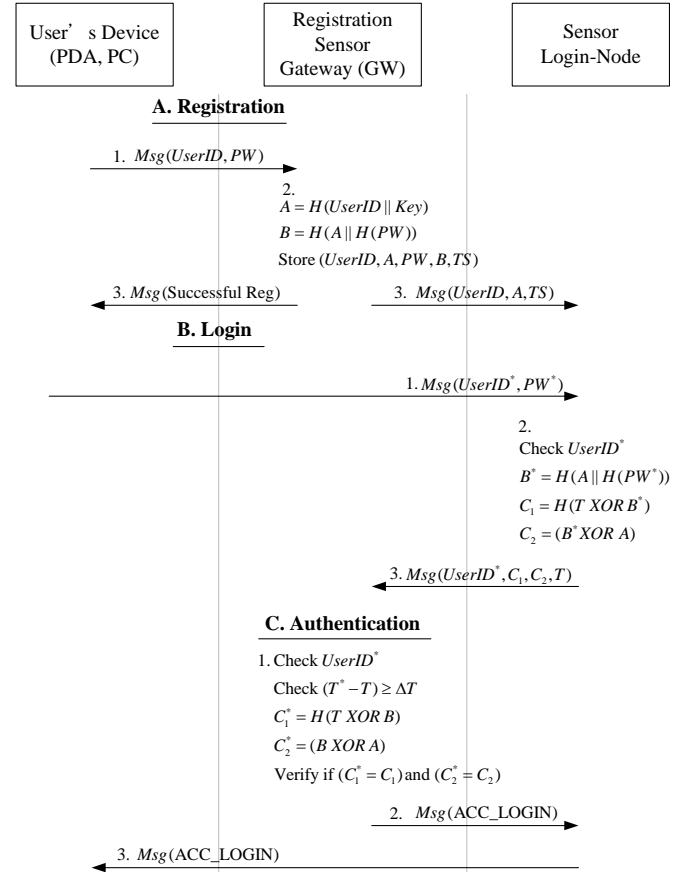


Fig. 1. Communication handshakes of Wong et al.'s scheme

III. CRYPTANALYSIS OF WONG ET AL.'S SCHEME

Although Wong et al. proposed a dynamic user authentication scheme that allows legitimate users to query at any of the sensor nodes and imposes very light computational load, there still remains several security weaknesses in their scheme. We will now examine these weaknesses in details.

- 1) It cannot stand against replay attacks. A replay attack is that an attacker tries to replay the same messages obtained in previous sessions. If the attacker can successfully login to the remote system through replay, then the scheme cannot withstand a replay attack. Assume that U is an

attacker who eavesdrops a user's login message $(userID^*, C_1, C_2, T)$. He/she can use the same message to login to the system successfully as long as the value T is still within the allowed time interval. That is, as long as the difference between the current time and the value T is less than ΔT , the attacker can use the same message to perform the replay attack.

- 2) It cannot stand against forgery attacks. In a forgery attack, if an attacker eavesdrops or intercepts the login messages, he/she can modify the login messages to masquerade as a legitimate user in order to access the resources of a remote system. Assume that U is the attacker who can steal from a sensor login-node another user's information $(userID, A, TS)$. He/she also intercepts the user's information $(userID, C_1, C_2, T)$ sent by the sensor login-node. The attacker can use the information to derive B^* as follows:

$$B^* = C_2 \text{ XOR } A \quad (8)$$

due to (5). Hence, U can use a new timestamp T' to compute a new C_1' as follows:

$$C_1' = H(T' \text{ XOR } B^*) \quad (9)$$

U then sends $Msg(userID, C_1', C_2, T')$ to the GW. Hence, C_1' will be successfully verified by the GW. Therefore, U can use another user's ID to launch a forgery attack.

- 3) Passwords can be revealed by any of the sensor nodes. Even though passwords are transmitted via a secure channel in the registration and login phases, all the passwords are still known to the GW and all the login nodes in plain text. There is no protection mechanism for the passwords in these phases. In case any of the GW or login nodes is compromised, all passwords leaked out.
- 4) A user cannot change his/her password with Wong et al.'s scheme. Passwords are fixed once they are set. A fixed password is more easily suffered from attacks than a regularly changed password.

IV. THE IMPROVED SCHEME

In this section, we present a modification of Wong et al.'s scheme that not only fixes the weaknesses but also enhances the security of Wong et al.'s scheme. The overall handshake of the proposed scheme is illustrated in Fig. 2. The proposed scheme is divided into four phases: registration, login, authentication, and password-changing phases. Note that the registration and the password-changing phases are performed via a secure channel. The four phases are discussed below.

A. The Registration Phase

A user submits his/her ID ($userID$) and password in hashed form $H(PW)$ to a GW for registration. Next, the GW stores the dataset $(userID, H(PW), TS)$ in its database. Then, the GW

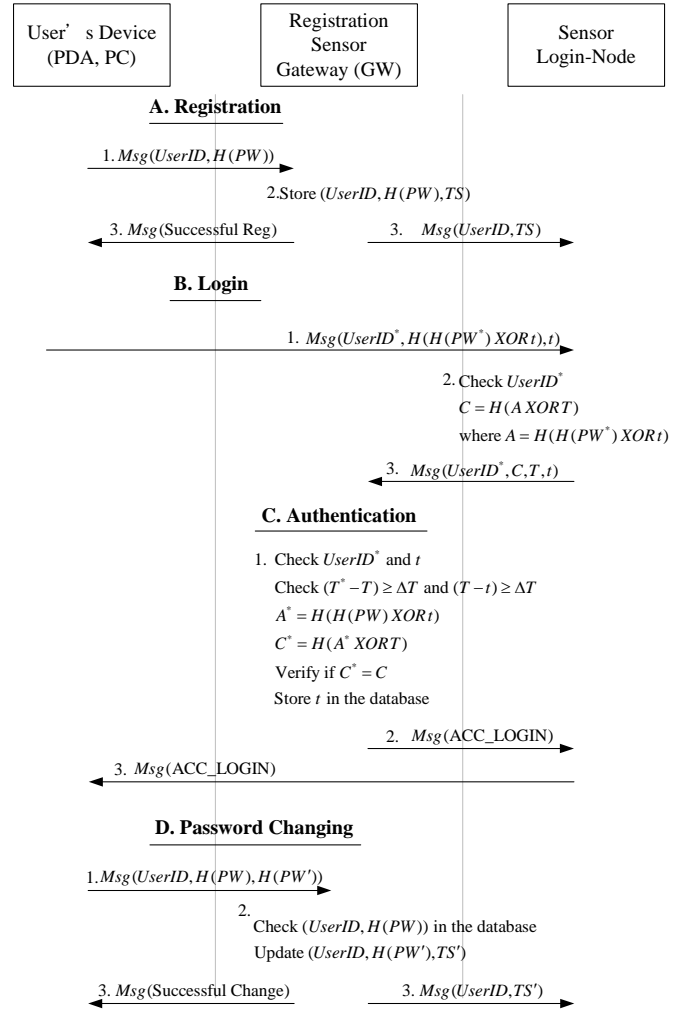


Fig. 2. Communication handshakes of the proposed scheme

replies to the user successful registration. Finally, the pair $(userID, TS)$ is then distributed to all the sensor nodes.

B. The Login Phase

The user first uses his/her password PW to compute a value A as follows:

$$A = H(H(PW^*) \text{ XOR } t) \quad (10)$$

where t is the current time. Then, he/she submits the triple $(userID^*, A, t)$ to a login-node. After receiving the login information, the login-node first checks whether $userID^*$ is in the list of datasets $(userID, TS)$. If not, the login-node then sends $Msg(REJ_LOGIN)$ to the user. Otherwise it computes the value C for the user, as follows:

$$C = H(A \text{ XOR } T) \quad (11)$$

where T is the current time. Then, the login-node sends $Msg(userID^*, C, T, t)$ to the GW for authentication.

C. The Authentication Phase

After receiving $Msg(userID^*, C, T, t)$ from the login-node, the GW first checks whether $(userID^*, t)$ is in the database. If $userID^*$ is not in the database or $(userID^*, t)$ is already contained in the database, the GW sends $Msg(REJ_LOGIN)$ to the login-node. Otherwise it checks whether the transmission delay is within the allowed time interval. If $(T^* - T) \geq \Delta T$ or $(T - t) \geq \Delta T$, the GW sends $Msg(REJ_LOGIN)$ to the login-node. Otherwise it computes (A^*, C^*) for verification. The (A^*, C^*) pair is computed as follows:

$$A^* = H(H(PW) \text{ XOR } t) \quad (12)$$

$$C^* = H(A^* \text{ XOR } T) \quad (13)$$

The GW verifies if $(C^* = C)$. If so, the GW stores t in the database and sends $Msg(ACC_LOGIN)$ to the login-node and the login-node also sends $Msg(ACC_LOGIN)$ to the user. Otherwise the GW sends $Msg(REJ_LOGIN)$ to the login-node.

D. The Password-Changing Phase

If the user wants to change his/her password, he/she needs to submit $userID^*$, original hashed password $H(PW)$, and new hashed password $H(PW')$ to the GW. After receiving the password-change request, the GW first checks whether $(userID^*, H(PW))$ is correct. If $userID^*$ is not in its database or $H(PW)$ is incorrect, the GW sends $Msg(REJ_CHANGE)$ to the user. Otherwise, it updates the corresponding dataset with $(userID, H(PW'), TS')$, where TS' is the current timestamp. Then, the GW replies to the user successful password change. Finally, the new pair $(userID, TS')$ is then distributed to all the sensor nodes.

V. ANALYSIS OF OUR SCHEME

Our enhanced scheme is a modification of Wong et al.'s scheme. In this section, we shall analyze our scheme and show that our scheme can resist several additional attacks. In addition, we shall provide a comparative study with Wong et al.'s scheme. Note that our proposed scheme does not add additional computational cost when compared with Wong et al.'s scheme.

A. Security Analysis

The proposed scheme can amend several security flaws in Wong et al.'s scheme. The advantages of our proposed scheme are described below.

- 1) The modified scheme can protect against the replay attack, that is to say, an attacker cannot replay the same login messages successfully. In the login phase, the user needs to use his/her password to compute a value containing the current time t (10). In the authentication

phase, the GW first checks whether $(userID^*, t)$ exists in the database. If $(userID^*, t)$ is already in the database, it means that this user has already login to this system at time t . The GW then rejects the user's login request. Hence, the attacker cannot launch a replay attack.

- 2) The modified scheme can protect against the forgery attack, that is to say, an attacker cannot impersonate legitimate user even if he/she intercepts $(userID^*, A, C, T, t)$ and steals from a sensor login-node another user's information $(userID, TS)$. In the proposed scheme, even if the attacker gains the list stored in the sensor login-node, the scheme is still secure since there is no secret information stored in the sensor login-node. The hash values are useless to an attacker. In order to forge a login message, the attacker has to know the user's password, due to (10). However, it is difficult to derive the user's password from the hashed value A . It is considered practically impossible for an attacker to derive the user's password from the hashed value [11].
- 3) Passwords are not revealed to any of the sensor nodes. In order to keep a user's password secret, in the registration and login phases, the user transmits his/her password in hashed form, rather than as plain text, as is done in Wong et al.'s scheme.
- 4) In the proposed scheme, a user can use the dataset $(userID^*, H(PW), H(PW'))$ to change his/her password PW with the new password PW' via a secure channel. The new password is also protected in this phase.

B. Efficiency Analysis

In this subsection, we examine the performance of our proposed scheme. The notations are defined in Table II [10]. The performance comparison between Wong et al.'s scheme and our proposed scheme is presented in Table III.

TABLE II
EVALUATION PARAMETERS

Symbol	Definition
T_H	The time for performing a one-way hash function
T_{XOR}	The time for performing an XOR operation
C_{MH}	The delay time for the communication between the login-node and the GW in multi-hops

TABLE III
PERFORMANCE COMPARISON BETWEEN WONG ET AL.'S SCHEME AND THE PROPOSED SCHEME

Phase	Wong et al.'s Scheme	Our Proposed Scheme
Registration	$3T_H + 1C_{MH}$	$1T_H + 1C_{MH}$
Login	$3T_H + 2T_{XOR} + 1C_{MH}$	$2T_H + 2T_{XOR} + 1C_{MH}$
Authentication	$1T_H + 2T_{XOR} + 1C_{MH}$	$2T_H + 2T_{XOR} + 1C_{MH}$
Total	$7T_H + 4T_{XOR} + 3C_{MH}$	$5T_H + 4T_{XOR} + 3C_{MH}$

We can see from Table III that the computations between Wong et al.'s scheme and our proposed scheme in the three phases (registration, login, and authentication) are very similar. Clearly, in these phases, our proposed scheme does not add additional computational cost. Compared with their scheme, our proposed scheme is also efficient.

VI. CONCLUSION

In this paper, we proposed a lightweight dynamic user authentication scheme that is built upon Wong et al.'s scheme. We point out that Wong et al.'s scheme is subject to several security attacks, as discussed above. Hence, we propose a modified scheme that not only retains all the advantages in Wong et al.'s scheme but also enhances its security by withstanding the security weaknesses. In comparison with the previous scheme, our proposed scheme possesses many advantages, including resistance to the replay and forgery attacks, reduction of user's password leakage risk, capability of changeable password, and better efficiency. An area of future research that should be considered is how to achieve mutual authentication between the users and the sensor nodes. In addition, since there is a centralized GW-node in the proposed scheme, the performance in authentication might be improved by designing a decentralized GW-node.

REFERENCES

- [1] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, May 2004, pp. 629-631.
- [2] A. Awasthi, "Comment on a dynamic id-based remote user authentication scheme," *Transactions on Cryptology*, vol. 1, no. 2, Aug. 2004, pp. 15-17.
- [3] I. E. Liao, C. C. Lee, and M. S. Hwang, "Security enhancement for a dynamic id-based remote user authentication scheme," *In Proceedings of the IEEE International Conference on Next Generation Web Services Practices (NWeSP 2005)*, Aug. 2005, pp. 22-26.
- [4] C. Y. Lee, C. H. Lin, and C. C. Chang, "An improved low computation cost user authentication scheme for mobile communication," *In Proceedings of the IEEE International Conference on Advanced Information Networking and Applications (AINA 2005)*, vol. 2, Mar. 2005, pp. 249-252.
- [5] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," *ACM SIGOPS Operating Systems Review*, vol. 36, no. 4, Oct. 2002, pp. 23-29.
- [6] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, May 2003, pp. 414-416.
- [7] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, Nov. 2003, pp. 1243-1245.
- [8] Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks," *Workshop on Real-World Wireless Sensor Networks (REALWSN 2005)*, Jun. 2005.
- [9] Z. Benenson, F. Gärtner, and D. Kesdogan, "User authentication in sensor networks (extended abstract)," *In Proceedings of Informatik 2004, Workshop on Sensor Networks*, Sept. 2004.
- [10] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," *In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06)*, vol. 1, Jun. 2006, pp. 244-251.
- [11] B. Schneier, *Applied Cryptography*, John Wiley & Sons Inc., New York, 2nd edition, 1996.

Huei-Ru Tseng received the B.S. and M.S. degrees in Information Management from National Taiwan University of Science and Technology, Taipei, Taiwan, in 2002 and 2004, respectively. She is currently pursuing the Ph.D. degree in the Department of Computer Science at National Chiao Tung University, Hsinchu, Taiwan. Her research interests include wireless networks, network security, and cryptography.

Rong-Hong Jan received the B.S. and M.S. degrees in Industrial Engineering, and the Ph.D. degree in Computer Science from National Tsing Hua University, Hsinchu, Taiwan, in 1979, 1983, and 1987, respectively. He joined the Department of Computer Science, National Chiao Tung University, in 1987, where he is currently a Professor. During 1991-1992, he was a Visiting Associate Professor in the Department of Computer Science, University of Maryland, College Park, MD. His research interests include wireless networks, mobile computing, distributed systems, network reliability, and operations research.

Wuu Yang received the B.S. in Computer Science from National Taiwan University in 1982 and the M.S. and Ph.D. in Computer Science from University of Wisconsin at Madison in 1987 and 1990, respectively. Currently, he is a Professor in the National Chiao Tung University, Taiwan. His current research interests include Java and network security, programming languages and compilers and attribute grammars. He is also very interested in the study of human languages and human intelligence.