# Cryptanalysis and Improvement of the Robust User Authentication Scheme for Wireless Sensor Networks

Yung-Cheng Lee[1,*], Hsin-Yu Lai[2] and Pei-Ju Lee[3]

[1]Department of Security Technology and Management, WuFeng University, Chiayi, Taiwan

[2]Graduate School of OptoMechatronics and Materials, WuFeng University, Chiayi, Taiwan

[3]School of Information Science, University of Pittsburgh, 135 N Bellefield, Pittsburgh, PA 15260

Received 25 July 2012; received in revised form 10 September 2012; accepted 08 October 2012

## Abstract

Wireless sensor networks are widely used in industrial process control, human health care, environmental control, vehicular tracking and battlefield surveillance, etc. A wireless sensor network consists of lots of sensor nodes and a gateway node. The sensor node usually communicates with the gateway node and users over an ad hoc wireless network. However, due to the open environments, the wireless sensor networks are vulnerable to variety of security threats. Thus, it is a critical issue to adopt a suitable authentication mechanism for wireless sensor networks to enhance security. In 2009, Vaidya et al. proposed a robust user authentication schemes for wireless sensor networks. In this article, we will show that their scheme is vulnerable to the guessing attack and the impersonation attack. Since it needs a secure channel for communications in password changing phase, their scheme is also inconvenient and expensive for users to update passwords. We also propose an improved scheme to remedy the flaws. The improved scheme withstands the replay attack and off-line guessing attack, and the users can freely update their passwords via public channels.

**Keywords**: wireless sensor networks, authentication, guessing attack, impersonation attack

## 1. Introduction

Wireless sensor networks (WSNs) [1-4, 6] are used in many industrial and consumer applications such as industrial process, human health care, environmental control, vehicular tracking, habitat monitoring and battlefield surveillance, etc. A WSN system consists of lots of sensor nodes and a gateway node [7]. The sensor nodes, with low processing power and limited storage space, usually communicate over an ad hoc wireless network [10]. The sensor nodes transmit data through network to the gateway cooperatively or independently. Generally, the communications of the WSNs are bidirectional so that the sensor nodes send data to the gateway and the gateway is capable to control the sensor's activity.

Due to the open environments, the security problem is one of the most important issues for the wireless sensor networks. Especially in some applications, e.g., battlefield surveillance, the collected data is critical. It is required to adopt security mechanisms to protect the collected secrets. It is essential to provide authentication between the gateway node (*GWN*) and sensor nodes (*SDs*), between the *GWN* and users and between the sensor nodes and users while transmitting data [3]. User authentication protocol provides a method for every entity to validate each other; it is an important mechanism for network

* Corresponding author. E-mail address: yclee@wfu.edu.tw
Tel.: +886-5-2267125

security. Authentication mechanism can prevent adversaries attack WSNs by retrieving, modifying or replacing the information collected by sensor nodes. Until now, a lot of methods proposed to enhance the security of the application systems. But due to the highly constrained nature on computation capability and memory space of sensor nodes, it is difficult to implement complex security algorithms in WSNs [8].

In 1981, Lamport [5] proposed the first user authentication scheme for communication in insecure channel. Hereafter, many user authentication schemes have been proposed to prevent unauthorized users gaining access to the system. Wong et al. [12] proposed a dynamic user authentication scheme for wireless sensor networks. But their scheme has security weaknesses such as it cannot withstand the replay and forgery attacks, passwords could be revealed by any of the sensor nodes, and password cannot be updated freely. Das [4] proposed a two-factor user authentication scheme in WSNs to overcome the security flaws. Tseng [9] also propose a modified scheme to remedy the weakness. However, Tseng et al.'s scheme is vulnerable to guessing attack and impersonation attack

In 2009, Vaidya et al. [10] proposed an improved robust user authentication schemes for WSNs, which is a variation of strong-password based solution proposed by Wong *et al.* [12] and modified version of the scheme [11]. Though Vaidya et al.'s scheme provides mutual authentication and capable to protect against the replay attack, the forgery attack and the man-in-the-middle attack. However, in this article, we will show that their scheme is vulnerable to the guessing attack and the impersonation attack. Moreover, since it needs a secure channel for communications in password changing phase, Vaidya et al.'s scheme is inconvenient and expensive for users to update their passwords. We propose an improved scheme to remedy the flaws. The improved scheme can withstand the replay attack and the off-line guessing attack, and the users can freely update their passwords through insecure open channels.

The rest of this paper is organized as follows: All notations used throughout this article are listed in Section 2. In Section 3, we briefly describe Vaidya et al.'s scheme. Next, the weaknesses of Vaidya et al.'s scheme are shown in Section 4. The improved scheme and its security analysis are presented in Section 5 and 6, respectively. Finally, we make conclusions in Section 7.

## 2. Preliminaries and notations

Normally, a wireless sensor network is composed of four phases: registration phase, login phase, authentication phase, and password changing phase. All notations used throughout this article are listed as follows.

(1) $U$ : A legitimate user.

(2) $ID$ : A user's identity.

(3) $GWN$ : A gateway node.

(4) $SD$ : A sensor node.

(5) $PW$ : A user's password.

(6) $x$ : The secret information of the gateway node.

(7) $h(\ )$ : A one-way hash function.

(8) $\oplus$ : The exclusive-OR (XOR) operation.

(9) $A \Rightarrow B:\{M\}$: The entity *A* sends message *M* to the receiver *B* via a secure channel.

(10) $A \rightarrow B:\{M\}$: The entity *A* sends message *M* to the receiver *B* through a public channel.

## 3. Vaidya et al.'s robust user authentication scheme

Vaidya et al.'s scheme is described briefly as follows.

### *3.1. Registration phase*

When a user wants to join the system, he/she sends identity $ID$ and hashed password *vpw* to the gateway node. The steps of the registration phase are as follows.

Step R-1: $U \Rightarrow GWN:\{ID, vpw\}$

The user *U* first chooses a password *PW* and computes $vpw = h(PW)$. Then, the user submits $\{ID, vpw\}$ to the *GWN* via a secure channel.

Step R-2: $GWN \Rightarrow SD:\{ID, X, T_S\}$

After receiving $\{ID, vpw\}$, the *GWN* computes $X = h(ID, x)$ with the secret key *x*, and stores $\{ID, vpw, X, T_S\}$ in the database, where $T_S$ is the current timestamp. Then, the *GWN* distributes $\{ID, X, T_S\}$ to all sensor nodes. Next, the *GWN* responses to the user with successful registration information $\{Succ\_Reg(X)\}$.

Step R-3: The user stores *X*

Upon receiving $\{Succ\_Reg(X)\}$, the user stores *X* for future use.

### *3.2. Login phase*

If a user wants to retrieve or transmit data from/to the sensor nodes, firstly, he/she should login the system. The login steps are as follows.

Step L-1: $U \rightarrow SD:\{ID, A, t\}$

The user first computes $A = h(vpw, t)$, where *t* is the current timestamp. Then he/she sends $\{ID, A, t\}$ to a sensor node *SD* through a public channel.

Step L-2: $SD \rightarrow GWN:\{ID, C, T_0, t\}$

After receiving the login request $\{ID, A, t\}$, the sensor node checks whether *ID* is in its lookup table and checks whether *t* is in a valid time interval. The login request will be rejected if it is not. Otherwise, the sensor node computes $C = h(X \oplus A \oplus T_0)$ and sends $\{ID, C, T_0, t\}$ to the *GWN*. Where $T_0$ is the current time stamp.

### 3.3. Authentication phase

The steps of the authentication phase are as follows.

Step A-1: $GWN \rightarrow SD: \{Acc\_Login, V, T_1\}$

On receiving $\{ID, C, T_0, t\}$ from the sensor node, the *GWN* checks whether $\{ID, T_0, t\}$ are valid. The login request will be stopped if it is not. If $\{ID, T_0, t\}$ are valid, the *GWN* computes $A' = h(vpw, t)$ and $C' = h(X \oplus A' \oplus T_0)$. Then a reject message is sent to the sensor node if $C' \neq C$. Otherwise, the *GWN* computes $\{ID, X, T_S\}$ and sends the accept message $\{Acc\_Login, V, T_1\}$) to the sensor node, where $T_1$ is the current timestamp.

Step A-2: $SD \rightarrow U: \{Acc\_Login, Y, T_1, T_2\}$

After receiving $\{Acc\_Login, V, T_1\}$, the sensor node checks whether $T_1$ is in a valid time interval. If $T_1$ is valid, the *SD* checks whether $V' = V$ after computing $V' = h(X, A, T_1)$. If $V' = V$, *SD* computes $Y = h(V, T_2)$ and sends $\{Acc\_Login, Y, T_1, T_2\}$ to the user, where $T_2$ is the current timestamp.

Step A-3: The user authenticates the sensor node.

Upon receiving the message $\{Acc\_Login, Y, T_1, T_2\}$, the user checks the freshness of timestamps $T_1$ and $T_2$. If $T_1$ and $T_2$ are both in the allowed time interval, the user computes $V' = h(X, A, T_1)$ and $Y' = h(V', T_2)$. The user will start obtaining or transmitting data if $Y' = Y$ holds.

### 3.4. Password-changing phase

The Vaidya et al.'s scheme provides users to freely update their passwords. The steps of the password changing phase are as follows. Note that the password changing phase should be performed via secure channels.

Step C-1: $U \Rightarrow GWN: \{ID, vpw, vpw_{new}\}$

If the user wants to update the password, firstly, he/she chooses a new password $PW_{new}$ and computes $vpw_{new} = h(PW_{new})$. Then, the user sends the triple $\{ID, vpw, vpw_{new}\}$ to the *GWN* via a secure channel.

Step C-2: $GWN \Rightarrow SD: \{ID, TS_1\}$

Upon receiving $\{ID, vpw, vpw_{new}\}$, the *GWN* checks *ID* and *vpw*. If both of them are true, the *GWN* updates its database and sends password changing successful information $\{Succ\_Change\}$ to the user. At the same time, the *GWN* distributes the updated information to all the sensor nodes.

Step C-3: All sensor nodes update their databases.

Upon receiving updated information, all server nodes update their databases after *ID* is verified.

## 4. Weakness of the Vaidya et al.'s scheme

Though Vaidya et al.'s scheme, besides providing mutual authentication, has several advantages such as protection against the replay attack, the forgery attack and the man-in-the-middle attack. However, in this section, we will show that their scheme is vulnerable to the guessing attack and the impersonation attack. Moreover, since it needs a secure channel for communications, Vaidya et al.'s scheme is inconvenient and expensive on updating password.

(1) It is vulnerable to the password guessing attack.

In Step L-1 of the login phase, the user sends $\{ID, A, t\}$ to a sensor node through public channel, where $A = h(vpw, t)$ and $vpw = h(PW)$. An adversary can be easily guesses the password by the following steps:

Step G-1: Adversary intercepts $\{ID, A, t\}$ in Step L-1.

Step G-2: By using the guessed password $PW'$ and the intercepted timestamp $t$, the adversary computes $A'$ with $A' = h(h(PW'), t)$.

Step G-3: The step G-2 is repeated if $A' \neq A$. The correct password will be obtained if $A' = A$.

In general, for the sake of easily memorization, the bit-length of the password is not quite long. Thus, the correct password can be easily obtained with a very high probability of $P = 1/2^{|PW|}$, where $|PW|$ is the bit-length of password. For illustration, the password guessing attack is shown in Fig. 1.

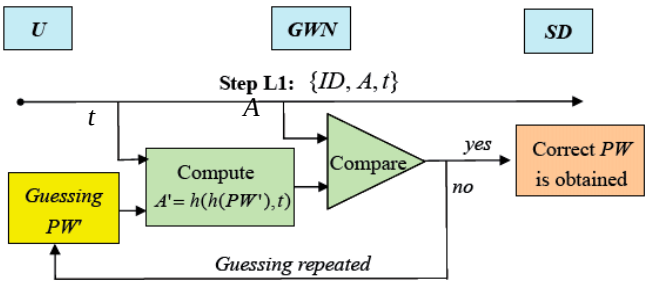


Fig. 1 The password guessing attack on Vaidya et al.'s scheme

(2) It is vulnerable to the impersonation attack.

Vaidya et al.'s scheme is also vulnerable to the impersonation attack. We describe the impersonation attack by the following three cases:

Case 1. An adversary impersonates as the legitimate user.

As described in (1) of this section, Vaidya et al.'s scheme cannot withstand guessing attack. If the password is correctly guessed, the adversary can impersonate as a legitimate user to retrieve information from any sensor node. The attack is successful due to the gateway and sensor nodes authenticate the users only by passwords.

Case 2. An adversary impersonates as the sensor node to fool the user.

The *GWN* sends $\{Acc\_Login, V, T_1\}$ to the *SD* in Step A-1for authentication, an adversary can compute $Y'$ by using the intercepted information *V* and the new timestamp $T_2'$ with $Y' = h(V, T_2')$. Then, the adversary sends $\{Acc\_Login, Y', T_1, T_2'\}$ to the user. Upon receiving $\{Acc\_Login, Y', T_1, T_2'\}$, the user will authenticate the adversary if $T_2'$ is in the allowed time interval. Thus, an adversary can impersonate as the sensor node to release fake sensor data. For illustration, the impersonation attack is shown in Fig. 2.

Case 3. A malicious sensor node impersonates as the gateway node.

Suppose that a malicious sensor node wants to impersonate as the gateway node to attack the system. Due to the malicious *SD* (*MSD* for short) knows *X* and can obtain *A* from Step L-1, he/she can compute *V* with $V = h(X, A, T_1)$ for legitimate *SD* to authenticate *GWN* in Step A-1. That is the *MSD* can compute and forward fake message for other sensor nodes to pass the verification, and the legitimate *SDs* suppose that they communicate with the real *GWN*.

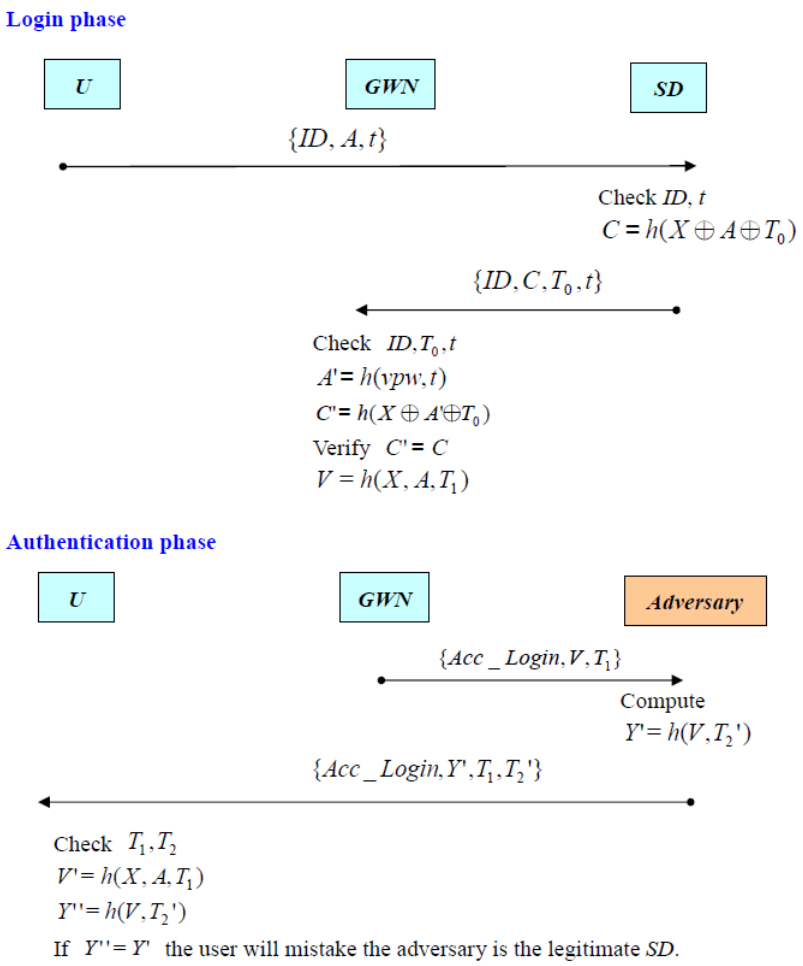


Fig. 2 The impersonation attack (An adversary impersonates as a sensor node)

(3) It needs secure channel in password-changing phase.

Since the user sends $\{ID, vpw, vpw_{new}\}$ to the gateway node for password updating, where $vpw = h(PW)$ and $vpw_{new} = h(PW_{new})$, an adversary will obtain the old password $PW$ and the new password $PW_{new}$ easily if the message is transmitted through public channels. Thus, in Vaidya et al.'s scheme, a secure channel should be required in password changing phase. However, the secure channel is more expensive than the public channel. In order to prevent secret message from leakage, the user should forwards the message in person or use a cryptographic mechanism to ensure the security. This makes it is inconvenient and expensive on updating password.

## 5. The improved user authentication scheme for wireless sensor networks

In this section, we will describe the improved scheme. The improved scheme is also composed of four phases. The registration phase of the improved scheme is the same as Vaidya et al.'s scheme. The login phase, authentication phase, and password changing phase are described as follows.

### *5.1. Login phase*

If a user wants to obtain or transmit data from sensor nodes, the login steps are as follows.

Step IL-1: $U \rightarrow SD: \{ID, A, T_{U1}\}$

The user $U$ computes $A = h(vpw, X, T_{U1})$ and sends $\{ID, A, T_{U1}\}$ to a sensor node $SD$ through a public channel, where $T_{U1}$ is the current timestamp.



Step IL-2: $SD \rightarrow GWN: \{ID, B, T_{U1}, T_{S1}\}$

Upon receiving the login request $\{ID, A, T_{U1}\}$, the sensor node checks whether $ID$ and $T_{U1}$ are valid. The login request will be rejected if it is not. Otherwise, the sensor node retrieves the corresponding $A$ and computes $B = h(X \oplus A \oplus T_{S1})$ and sends $\{ID, B, T_{U1}, T_{S1}\}$ to the $GWN$, where is $T_{S1}$ the current timestamp.

### *5.2. Authentication phase*

The steps of the authentication phase are as follows.

Step IA-1: $GWN \rightarrow SD: \{C, T_G\}$

On receiving $\{ID, B, T_{U1}, T_{S1}\}$ from the $SD$, the $GWN$ checks whether $\{ID, T_{U1}, T_{S1}\}$ are valid. The login request will be rejected if it is not. If $\{ID, T_{U1}, T_{S1}\}$ are valid, the $GWN$ computes $A' = h(vpw, X, T_{U1})$ and $B' = h(X \oplus A' \oplus T_{S1})$. Then $GWN$ checks whether $B' = B$ holds. The $GWN$ computes $C = h(X, B', T_G)$ and sends message $\{C, T_G\}$ to the sensor node if $B' = B$, where $T_G$ is the current timestamp.

Step IA-2: $SD \rightarrow U: \{D, T_{S2}\}$

After receiving $\{C, T_G\}$, the sensor node checks whether $T_G$ is in a valid interval. If $T_G$ is valid, *SD* computes $C' = h(X, B, T_G)$. The *GWN* is authenticated if $C' = C$. Next, *SD* computes $D = h(h(X \oplus A), T_{S2})$ and sends $\{D, T_{S2}\}$ to the user.

Step IA-3: The user authenticates the sensor node.

After receiving $\{D, T_{S2}\}$, the user checks the freshness of timestamps $T_{S2}$. If $T_{S2}$ is in a valid time interval, the user computes $D' = h(h(X \oplus A), T_{S2})$. The user will start to obtain or transmit data if $D' = D$ holds.

*5.3. Password changing phase*

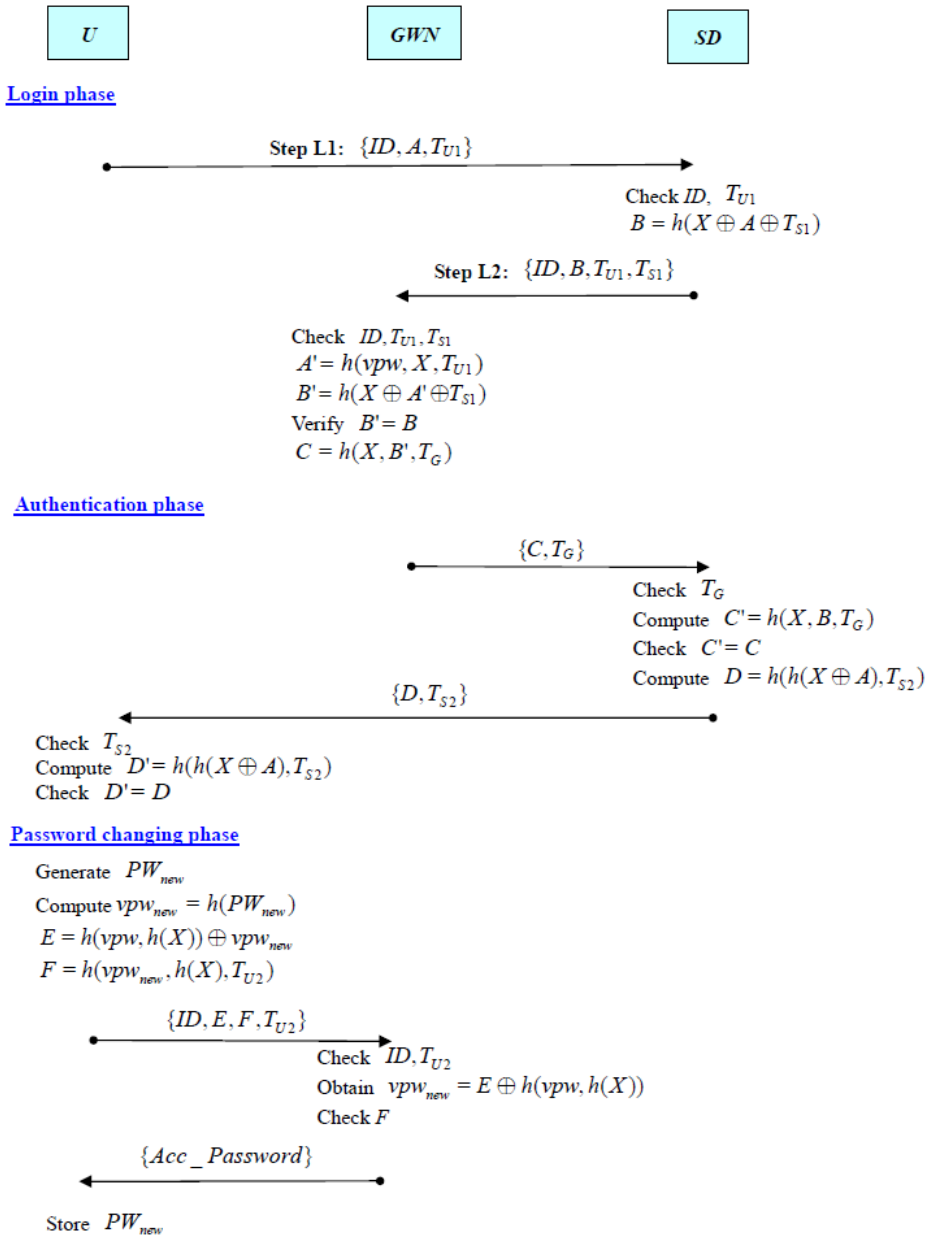


Fig. 3 The improved user authentication scheme for wireless sensor networks

The steps of the password changing phase are as follows. The communications of the password changing phase can be via insecure open channels.

Step IC-1: $U \rightarrow GWN$: $\{ID, E, F, T_{U2}\}$

The user first chooses a new password $PW_{new}$ and computes $vpw_{new} = h(PW_{new})$. Next, the user computes $E = h(vpw, h(X)) \oplus vpw_{new}$ and $F = h(vpw_{new}, h(X), T_{U2})$, where $T_{U2}$ is the current timestamp. Finally, the user sends $\{ID, E, F, T_{U2}\}$ to the *GWN*.

Step IC-2: $GWN \rightarrow U$: $\{Acc\_Password\}$

Upon receiving $\{ID, E, F, T_{U2}\}$, the *GWN* checks *ID* and $T_{U2}$. If both of them are valid, the *GWN* obtains $vpw_{new}$ by $vpw_{new} = E \oplus h(vpw, h(X))$. Then *GWN* computes $F' = h(vpw_{new}, h(X), T_{U2})$ and checks whether *F'* is equal to the received message *F*. The *GWN* sends a successful password changing information $\{Acc\_Password\}$ to the user if $F' = F$ holds. Finally, the user replaces *PW* with $PW_{new}$. The improved scheme is shown in Fig. 3 above.

## 6. Discussions and security analysis of the improved scheme

In the improved scheme, only hash function and bitwise exclusive-OR operations are adopted in computation, thus the computation overhead is quite low. The scheme also has the merits as follows.

(1) The proposed scheme withstands the replay attack.

Due to the transmission information is maliciously or fraudulently repeated, many authentication schemes suffer the replay attack. In the improved scheme, all the transmission information contains timestamp, the receiver can detect the resent information by checking the freshness of the timestamp. Thus the improved scheme can withstand the replay attack.

(2) The proposed scheme resists the off-line guessing attack.

If an adversary wants to guess the password, though he/she intercepts $\{ID, A, T_{U1}\}$ from Step IL-1, it is infeasible to correctly guess the password since $A = h(vpw, X, T_{U1})$ and *X* is unknown by the adversary. Similarly, if an adversary wants to obtain the password from the transmission information in Step IL2, the trials also will fail due to $B = h(X \oplus A \oplus T_{S1})$. Moreover, since $D = h(h(X \oplus A), T_{S2})$, an adversary also cannot guess the password by using the information *D*. Thus the improved scheme resists the off-line guessing attack.

(3) The proposed scheme provides mutual authentication.

In the Step IL-2, the *GWN* will authenticate the user and *SD* by checking whether $B' = B$ holds. The *SD* authenticates the user and the *GWN* by verifying *C* in Step IA-1. At last, in the Step IA-2, the user will authenticate the *SD* and *GWN* if $D' = D$ is hold. Thus the improved scheme provides mutual authentication among the user, the sensor node and the gateway nodes.

## 7. Conclusions

Vaidya et al. proposed a robust user authentication schemes for wireless sensor networks. Though Vaidya et al.'s scheme provides mutual authentication and capable to protect against the replay attack, the forgery attack and the man-in- the-middle attack. However, since it needs a secure channel in password changing phase, Vaidya et al.'s scheme is inconvenient and expensive for users to update their passwords. Moreover, their scheme is vulnerable to the guessing attack and the impersonation attack. We propose an improved scheme to remedy the flaws. The improved scheme can withstand the replay attack and off-line guessing attack, and the users can freely update their passwords via public channels.

## Acknowledgment

This work was partially supported by the National Science Council of the Republic of China under the contract number NSC 101-2632-E-274-001-MY3.

## References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol.38, pp.393-422, 2002.

[2] Z. Benenson, N. Gedicke and O. Raivio, "Realizing robust user authentication in sensor networks," Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), 2005.

[3] C.Y Chong, S. Kumar, "Sensor networks: evolution, opportunities, and challenges," Proceedings of the IEEE, vol.91, pp.1247-1256, 2003.

[4] M.L. Das, "Two-factor user authentication in wireless sensor network," IEEE Transaction on Wireless Communications, vol.8, pp.1086-1090, 2009.

[5] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol.24, pp.770-772, 1981.

[6] I. E. Liao, C. C. Lee and M. S. Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme," Proceedings of the IEEE International Conference on Next Generation Web Services Practices (NWeSP 2005), 2005, pp.22-26.

[7] K. Martinez, J.K. Hart, R. Ong, "Environmental sensor networks," IEEE Computer, vol.37, pp.50-56, 2004.

[8] Z. Tan, "Cryptanalysis of a two-factor user authentication scheme in wireless sensor networks," Advances in Information Sciences and Service Sciences, vol.3, pp.117-126, 2011.

[9] H.-R. Tseng, R.-H. Jan and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," Proceedings of the IEEE Global Telecommunications Conference, GLOBECOM '07, 2007, pp.986-990.

[10] B. Vaidya, M. Chen and J.J.P.C. Rodrigues, "Improved robust user authentication scheme for wireless sensor networks," 2009 Fifth IEEE Conference on Wireless Communication and Sensor Networks (WCSN), 2009, pp.1-6.

[11] B Vaidya, J.S. Silva, J.J. Rodrigues, "Robust dynamic user authentication scheme for wireless sensor networks," Proceedings of the 5th ACM Symposium on QoS and Security for wireless and mobile networks (Q2SWinet 2009), Tenerife, Spain, 2009, pp.88-91.

[12] K.H.M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), vol.1, 2006, pp.318-327.