Security Analysis of a Three-factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments

Wei-Liang Tai[1], Ya-Fen Chang[2], and Po-Lin Hou[2]

(Corresponding author: Ya-Fen Chang)

Department of Information Communications, Chinese Culture University[1]

Department of Computer Science and Information Engineering,

National Taichung University of Science and Technology[2]

No. 129, Section 3, Sanmin Road, Taichung, Taiwan

(Email: cyf@nutc.edu.tw)

(Received Sept. 26, 2018; Revised and Accepted May 17, 2019; First Online June 25, 2019)

Abstract

The Internet of Things (IoT) can be applied to applications in various fields such as industry, medical care, and public security because IoT enables remote sensing and control in heterogeneous environments. Wireless sensor networks (WSNs) are an important infrastructure in IoT, where a sensor node provides the collected data to authorized users. Because of the resource-constrained nature of sensor nodes such as transmission and computational capabilities and the limited energy, how to ensure both security and efficiency of WSNs in IoT environments becomes a challenge. Recently, Li *et al.* proposed a three-factor anonymous authentication scheme by adopting a fuzzy commitment scheme and an error correction code to handle the user′s biometric data for WSNs in IoT environments. They claimed their scheme could ensure computational efficiency and achieve more security and functional features. After analyzing their authentication scheme, we find that it cannot ensure security. First, a malicious user can retrieve a sensor node′s secret and impersonate the sensor node. Second, a malicious user can acquire the sensory data without the gateway node even with a forged identity. Third, the malicious user can retrieve another legal user′s essential information for authentication and impersonate this innocent user. In this paper, how these security flaws damage Li *et al.*′s authentication scheme and further discussions will be shown in detail.

Keywords: Authentication; Elliptic Curve Cryptography; Internet of Things; Wireless Sensor Network

1 Introduction

The rise of the Internet of Things (IoT) [3] brings significant changes to people′s daily life. Because IoT enables remote sensing and control in heterogeneous environments, IoT is widely applied to applications in various fields such as industry, transportation, agriculture, medical care, military and public security such that Industry 4.0, Smart Transportation, Smart Home, Smart Medical, and Smart City can be realized. This makes people′s life more and more convenient.

In IoT applications, wireless sensors play an important role because they sense the surroundings, generate sensory data, and transmit data through heterogeneous network environments. Thus, wireless sensor networks (WSNs) are an important infrastructure in IoT, and a sensor node in WSNs provides the collected data to authorized users.

However, wireless sensors regarded as one of the most important devices in IoT are usually unattended. Researches indicate that the energy consumption of sensor nodes is proportional to the transmission distance so WSNs should be extended [1,9]. To increase the life cycle of WSNs, a gateway node and heterogeneous WSNs are introduced. In heterogeneous WSNs, sensors may possess different capacities such as transmission and computational capacities. It denotes that some sensor nodes such as the gateway nodes can transmit data over long distances, and the desired sensory data can be delivered to a backed server for further and real-time analysis. This property makes users obtain specific information quickly and make decisions as soon as possible.

Due to the resource-constrained nature of wireless sensors, such as transmission and computational capabilities and the limited energy, and the characteristics of public transmission medium, how to ensure both security and efficiency of WSNs in IoT environments becomes a tough and urgent issue. In 2013, Xue *et al.* proposed a time-based voucher-based mutual authentication and key agreement scheme for wireless sensor networks [12].

In Xue *et al.*′s scheme, the gateway node generates time credentials for each user and sensor node. With time credentials, a user, the gateway node and a sensor node can authenticate each other. Xue *et al.*′s scheme uses only simple computational operations, such as hash function and XOR (exclusive-or) operation, to comply with the resource-constrained nature of wireless sensors. However, in 2015, He *et al.* [5] showed that Xue *et al.*′s scheme is vulnerable to several attacks, offline password guessing attack, impersonation attack and modification attack. He *et al.* also proposed an improved temporal-credential-based mutual authentication and key agreement scheme with pseudo identity. In 2016, Jiang *et al.* [7] showed that Xue *et al.*′s scheme suffers from stolen smart card attack, user impersonation attack, and tracking attack. By using ECC, Jiang *et al.* also proposed an improvement based on He *et al.*′s scheme. In Jiang *et al.*′s scheme, sensor nodes only need to execute simple computational operations while a user and the gateway node need to execute ECC operations. As a result, the difficulty of elliptic curve discrete logarithm (ECDL) can increase the security level of their scheme. Meanwhile, Amin *et al.* proposed an anonymity preserving three-factor authenticated key exchange protocol for wireless sensor networks [2]. Unfortunately, Chang *et al.* showed that Amin *et al.* protocol cannot ensure user anonymity and suffers from desynchronization attack [4]. Although there are also some two-factor authentication schemes for wireless sensor networks, it has been demonstrated that the security of these two-factor authentication schemes is doubted [6, 10, 11].

Recently, Li *et al.* [8] showed that Xue *et al.*′s, He *et al.*′s, and Jiang *et al.*′s scheme commonly have the following flaws.

1) These schemes cannot detect wrong password and lack mechanisms to update password.

2) Messages are directly exchanged between a user and a sensor such that these schemes are not suitable for IoT environments.

3) These schemes are all vulnerable to known session-specific temporary attack and clock synchronization attack.

To overcome the drawbacks and preserve the advantages, Li *et al.* proposed a three-factor anonymous authentication scheme by adopting a fuzzy commitment scheme and an error correction code to handle the user′s biometric data for WSNs in IoT environments with ECC and simple computational operations such as hash function and XOR operation. They claimed their scheme could ensure computational efficiency and achieve more security and functional features.

After analyzing the scheme proposed by Li *et al.*, we find that their scheme cannot ensure security as claimed. First, a malicious user can retrieve a sensor node′s secret and impersonate the sensor node to deliver forged sensory data. Second, a malicious user can acquire the sensory data without the gateway node even with a forged identity. Third, the malicious user can retrieve another legal user′s essential information for authentication and impersonate this innocent user. If different access rights are granted to different users, this flaw makes a privileged account compromised. The rest of this paper is organized as follows. Section 2 reviews Li *et al.*′s scheme. Security analysis and advanced discussions are given in Section 3. At last, some conclusions are drawn.

2 Review of Li *et al.*′s Scheme

This section reviews Li *et al.*′s three-factor anonymous authentication scheme for WSNs in IoT environments. The notations used in Li *et al.*′s scheme are listed in Table 1. In Li *et al.*′s scheme, ECC is employed. First, the gateway node, GWN, selects an addition group G over a finite field F_p on the elliptic curve E of prime order n, where the point P is the generator. Then GWN randomly selects a number $x \in Z_n^*$ as its private key, chooses a master key K_{GWN}, and computes the public key $X = xP$. GWN keeps x and K_{GWN} secretly and makes $\{E(F_p), G, P, X\}$ public. Li *et al.*′s scheme is composed of four phases: sensor registration phase, user registration phase, login and authentication phase, and password change phase. Because password change phase is not related to our security analysis of Li *et al.*′s scheme, password change phase is omitted. The details are as follows.

Table 1: Notations used in Li *et al.*′s three-factor anonymous authentication scheme

Notation	**Definition**
U_i, GWN, S_j	i^{th} user, gateway node, j^{th} sensor node
ID_i/SID_j	Identity of U_i/S_j
PW_i	Password of U_i
b_i	Biometric of U_i
SC	U_i's smart card
K_{GWN}	GWN's master key
K_{GWN-S_j}	Secret key shared between GWN and S_j
$SK_i/SK_j/SK_{GWN}$	Session key computed by $U_i/S_j/GWN$
$h(.)$	A secure hash function
$C \subseteq \{0,1\}^n$	A set of codewords
$F(.)$	A fuzzy commitment scheme
$f(.)$	A decoding function
r_i, r_g, r_j	Random numbers generated by U_i,GWN and S_j, respectively
$\|$	Concatenation operation
$\oplus$	XOR operation

2.1 Sensor Registration Phase

Before S_j is deployed, GWN selects an identity SID_j and computes the secret key $K_{GWN-S_j} = h(SID_j \parallel K_{GWN})$ for S_j. Then GWN stores $\{SID_j, K_{GWN-S_j}\}$ in S_j's memory. At last, GWN deploys these sensors in a particular area to form a wireless sensor network.

2.2 User Registration Phase

When a user wants to acquire sensory data from sensor nodes, he/she has to register at GWN in the first place. The details are as follows:

Step 1. An identity ID_i and a password PW_i are selected by U_i.

Step 2. U_i generates a nonce a_i and computes $RPW_i = h(PW_i \parallel a_i)$.

Step 3. U_i imprints the biometric on a special device and gets the biometric information b_i.

Step 4. U_i submits the registration request $\{ID_i, RPW_i, b_i\}$ to GWN via a secure manner.

Step 5. Upon receiving the registration request, GWN chooses a random codeword $c_i \in C$ for U_i.

Step 6. GWN computes $F(c_i, b_i) = (\alpha, \delta) = (h(c_i), c_i \oplus b_i)$, $A_i = h(ID_i \parallel RPW_i \parallel c_i)$ and $B_i = h(ID_i \parallel K_{GWN}) \oplus h(RPW_i \parallel c_i)$.

Step 7. GWN stores $\{\alpha, \delta, A_i, B_i, X, f(.)\}$ into a smart card, SC, and issues it to U_i via a secure channel.

Step 8. GWN stores ID_i in its database and deletes other information.

Step 9. After getting SC, U_i stores a_i into it. Then, SC contains $\{\alpha, \delta, A_i, B_i, X, f(.), a_i\}$.

2.3 Login and Authentication Phase

When U_i wants to access the data collected by the sensor S_j, U_i should be first authenticated by GWN. The details are as follows:

Step 1. U_i inserts SC into a card reader and imprints the biometric b_i' on a special device.

Step 2. SC computes $c_i' = f(\delta \oplus b_i') = f(c_i \oplus (b_i \oplus b_i'))$ and checks if $h(c_i') = \alpha$. If it does not hold, this session is terminated by SC; otherwise, the imprinted biometric b_i' is verified successfully, and U_i inputs ID_i and PW_i.

Step 3. SC computes $A_i' = h(ID_i \parallel h(PW_i \parallel a_i) \parallel c_i')$ and checks if $A_i' = A_i$. If it does not hold, this session is rejected by SC; otherwise, U_i's identity ID_i and password PW_i are verified successfully by SC.

Step 4. SC chooses random numbers r_i and $s \in Z_n^*$.

Step 5. SC computes $M_1 = B_i \oplus h(h(PW_i \parallel a_i) \parallel c_i')$, $M2 = sP$, $M3 = sX = sxP$, $M4 = ID_i \oplus M_3$, $M5 = M_1 \oplus r_i$, $M6 = h(ID_i \parallel r_i) \oplus SID_j$ and $M7 = h(M_1 \parallel SID_j \parallel M_3 \parallel r_i)$.

Step 6. U_i sends the login request $\{M_2, M_4, M_5, M_6, M_7\}$ to GWN.

Step 7. After receiving the login request, GWN computes $M_3' = xM_2 = xsP$ and $ID_i' = M_4 \oplus M_3'$ and checks if ID_i' exists in the database. If it does not exist, this login request is rejected by GWN; otherwise, this phase proceeds.

Step 8. GWN computes $M_1' = h(ID_i' \parallel K_{GWN})$, $r_i' = M_5 \oplus M_1'$, $SID_j' = M_6 \oplus h(ID_i' \parallel r_i')$ and $M_7' = h(M_1' \parallel SID_j' \parallel M_3' \parallel r_i')$ and checks if $M_7' = M_7$. If it does not hold, this session is terminated by GWN; otherwise, GWN generates a random number r_g.

Step 9. GWN computes $K'_{GWN-S_j} = h(SID_j' \parallel K_{GWN})$, $M_8 = ID_i' \oplus K'_{GWN-S_j}$, $M_9 = r_g \oplus h(ID_i' \parallel K'_{GWN-S_j})$, $M_{10} = r_g \oplus r_i'$ and $M_{11} = h(ID_i' \parallel SID_j' \parallel K'_{GWN-S_j} \parallel r_i' \parallel r_g)$ and sends $\{M_8, M_9, M_{10}, M_{11}\}$ to S_j.

Step 10. Upon receiving $\{M_8, M_9, M_{10}, M_{11}\}$, S_j computes $ID_i' = M_8 \oplus K_{GWN-S_j}$, $r_g' = h(ID_i'' \parallel K_{GWN-S_j}) \oplus M_9$, $r_i'' = r_g' \oplus M_{10}$, and $M_{11}' = h(ID_i'' \parallel SID_j \parallel K_{GWN-S_j} \parallel r_i'' \parallel r_g')$ and checks if $M_{11}' = M_{11}$. If it does not hold, this session is terminated by S_j; otherwise, S_j generates a random number r_j.

Step 11. S_j computes $M_{12} = r_j \oplus K_{GWN-S_j}$, $SK_j = h(ID_i'' \parallel SID_j \parallel r_i'' \parallel r_g' \parallel r_j)$ and $M_{13} = h(K_{GWN-S_j} \parallel SK_j \parallel r_j)$ and sends the response $\{M_{12}, M_{13}\}$ to GWN.

Step 12. After getting the response $\{M_{12}, M_{13}\}$, GWN computes $r_j' = M_{12} \oplus K'_{GWN-S_j}$ $SK_{GWN} = h(ID_i' \parallel SID_j' \parallel r_i' \parallel r_g \parallel r_j')$ and $M_{13}' = h(K'_{GWN-S_j} \parallel SK_{GWN} \parallel r_j')$ and checks if $M_{13}' = M_{13}$. If it does not hold, this session is terminated; otherwise, this phase proceeds.

Step 13. GWN computes $M_{14} = M_1' \oplus r_g$, $M_{15} = r_i' \oplus r_j'$ and $M_{16} = h(ID_i' \parallel SK_{GWN} \parallel r_g \parallel r_j')$ and sends $\{M_{14}, M_{15}, M_{16}\}$ to U_i.

Step 14. U_i computes $r_g'' = M_{14} \oplus M_1$, $r_j'' = M_{15} \oplus r_i$, $SK_i = h(ID_i \parallel SID_j \parallel r_i \parallel r_g'' \parallel r_j'')$ and $M_{16}' = h(ID_i \parallel SK_i \parallel r_g'' \parallel r_j'')$ and checks if $M_{16}' = M_{16}$. If it does not hold, this session is terminated; otherwise, the authentication process is completed.

After the above, U_i can acquire sensory data from S_j via GWN while a session key SK_i is shared among U_i, S_j and GWN, where $SK_i = SK_j = SK_{GWN}$.

3 Security Analysis of Li *et al.*'s Scheme and Advanced Discussions

In this section, how our found security flaws damage Li *et al.*'s authentication scheme will be shown. First, a legal and malicious user can obtain the secret key K_{GWN-S_j} shared between GWN and S_j after he has acquired sensory data from S_j. After obtaining K_{GWN-S_j}, the legal and malicious user can impersonate S_j to negotiate a session key shared with GWN and the legal user and to deliver forged sensory data. Meanwhile, this malicious user can access S_j without GWN even with a forged identity. Moreover, this user who has successfully obtained K_{GWN-S_j} can reveal the identity of another legal user U_i who also acquires sensory data from S_j, and the innocent user U_i's essential information $h(ID_i \parallel K_{GWN})$ will be retrieved at the same time. Thereupon, the malicious user can impersonate the innocent user U_i to access the desired sensor nodes at will. For clarity and simplicity, we demonstrate how the above security flaws work with U_1 as the malicious user, U_2 as the innocent user and S_1 as the common accessed sensor node. In additional to the found security flaws, further discussions are also made in this section. The details are as follows:

3.1 Leakage of the Secret Key Shared Between GWN and S_j and Impersonating S_j

U_1 is a legal user so he can acquire the sensory data from authorized sensor nodes. In login and authentication phase, U_1 can acquire the sensory data from the specific sensor node S_1 via GWN. It denotes that U_1 is aware of S_1's identity SID_1. U_1 begins to eavesdrop after he sends the login request $\{M_2, M_4, M_5, M_6, M_7\}$ to GWN for acquiring the sensory data from S_1. Within a reasonable period of time, GWN will send $\{M_8, M_9, M_{10}, M_{11}\}$ to S_1, where $M_8 = ID_i' \oplus K'_{GWN-S_j} = ID_1 \oplus K_{GWN-S_1}$, $M_9 = r_g \oplus h(ID_1 \parallel K_{GWN-S_1})$, $M_{10} = r_g \oplus r_i'$ and $M_{11} = h(ID_1 \parallel SID_1 \parallel K_{GWN-S_1} \parallel r_i' \parallel r_g)$. Because U_1 knows his identity ID_1, he can retrieve $K_{GWN-S_1} = M_8 \oplus ID_1$.

However, GWN is responsible for forwarding messages to multiple sensor nodes. It denotes that U_1 may intercept multiple $\{M_8, M_9, M_{10}, M_{11}\}'$s. In this case, U_1 still can reveal K_{GWN-S_1} successfully. To ensure which revealed value is K_{GWN-S_1}, U_1 only needs to do the following.

Step 1. For the intercepted and untested $\{M_8, M_9, M_{10}, M_{11}\}$, U_1 computes $w_1 = M_8 \oplus ID_1$, $w_2 = M_9 \oplus h(ID_1 \parallel w_1)$, $w_3 = M_{10} \oplus w_2$, and $w_4 = h(ID_1 \parallel SID_1 \parallel w_1 \parallel w_3 \parallel w_2)$.

Step 2. U_1 checks if $w_4 = M_{11}$. If it holds, U_1 successfully obtains $K_{GWN-S_1} = w_1$; otherwise, the process will go back to Step 1.

By the above procedure, U_1 can successfully retrieve K_{GWN-S_1} even multiple $\{M_8, M_9, M_{10}, M_{11}\}'$s are intercepted. It is because $w_1 = M_8 \oplus ID_1 = K_{GWN-S_1}$, $w_2 = M_9 \oplus h(ID_1 \parallel w_1) = r_g$, $w_3 = M_{10} \oplus w_2 = r_i$, and $w_4 = h(ID_1 \parallel SID_1 \parallel w_1 \parallel w_3 \parallel w_2) = h(ID_1 \parallel SID_1 \parallel K_{GWN-S_1} \parallel r_i \parallel r_g) = M_{11}$.

On the other hand, U_1 can impersonate S_1 to cheat another legal user U_2 who also wants to access S_1. As shown in the review of Li et al's scheme, U_2 and GWN will execute login and authentication phase when U_2 wants to acquire S_1's sensory data. As a result, GWN will send $\{M_8, M_9, M_{10}, M_{11}\}$ to S_1. Because GWN is responsible for forwarding messages to multiple sensor nodes and S_1's identity is also not revealed in the transmitted $\{M_8, M_9, M_{10}, M_{11}\}$, U_1 eavesdrops and does the following to impersonate S_1.

Step 1. Upon intercepting $\{M_8, M_9, M_{10}, M_{11}\}$, U_1 computes $ID_2'' = M_8 \oplus K_{GWN-S_1}$, $r_g' = h(ID_2'' \parallel K_{GWN-S_1}) \oplus M_9$, $r_i'' = r_g' \oplus M_{10}$, and $M_{11}' = h(ID_2'' \parallel SID_1 \parallel K_{GWN-S_1} \parallel r_i'' \parallel r_g')$.

Step 2. U_1 checks if $M_{11}' = M_{11}$. If it does not hold, this process goes back to Step 1; otherwise, U_1 successfully intercepts the request sent to S_1 and generates a random number r_j.

Step 3. U_1 computes $M_{12} = r_j \oplus K_{GWN-S_1}$, $SK_j = h(ID_2'' \parallel SID_1 \parallel r_i'' \parallel r_g' \parallel r_j)$ and $M_{13} = h(K_{GWN-S_1} \parallel SK_j \parallel r_j)$.

Step 4. U_1 sends the response $\{M_{12}, M_{13}\}$ to GWN.

After getting the response $\{M_{12}, M_{13}\}$, GWN computes $r_j' = M_{12} \oplus K'_{GWN-S_1}$, $SK_{GWN} = h(ID_2' \parallel SID_1' \parallel r_i' \parallel r_g \parallel r_j')$ and $M_{13}' = h(K'_{GWN-S_1} \parallel SK_{GWN} \parallel r_j')$. GWN checks if $M_{13}' = M_{13}$. This must hold, and login and authentication phase proceeds. At last, U_2, GWN, and U_1 will negotiate a shared session key. That is, U_1 can successfully impersonate S_1 and deliver forged sensory data.

3.2 Bypassing GWN

If K_{GWN-S_1} has been revealed by U_1, U_1 can bypass GWN and acquire sensory data from S_1 directly. Moreover, U_1 can acquire S_1's data successfully even with a forged identity. In login and authentication phase, GWN will send $\{M_8, M_9, M_{10}, M_{11}\}$ to S_1, where $M_8 = ID_i' \oplus K'_{GWN-S_1}$, $M_9 = r_g \oplus h(ID_1 \parallel K_{GWN-S_1})$, $M_{10} = r_g \oplus r_i'$ and $M_{11} = h(ID_1 \parallel SID_1 \parallel K_{GWN-S_1} \parallel r_i' \parallel r_g)$. Because U_1 knows K_{GWN-S_1} and SID_1, he can access S_1 without GWN by the following.

Step 1. U_1 generates two random numbers R_1 and R_2.

Step 2. U_1 computes $M_8 = ID_1 \oplus K_{GWN-S_1}$, $M_9 = R_1 \oplus h(ID_1 \parallel K_{GWN-S_1})$, $M_{10} = R_1 \oplus R_2$ and $M_{11} = h(ID_1 \parallel SID_1 \parallel K_{GWN-S_1} \parallel R_2 \parallel R_1)$. Then U_1 sends $\{M_8, M_9, M_{10}, M_{11}\}$ to S_1.

Step 3. After receiving $\{M_8, M_9, M_{10}, M_{11}\}$, S_1 computes $ID_1'' = M_8 \oplus K_{GWN-S_1}$, $r_g' = h(ID_1'' \parallel K_{GWN-S_1}) \oplus M_9 = R_1$, $r_i'' = r_g' \oplus M_{10} = R_2$, and $M_{11}' = h(ID_i'' \parallel SID_j \parallel K_{GWN-S_1} \parallel r_i'' \parallel r_g') = h(ID_1 \parallel SID_1 \parallel K_{GWN-S_1} \parallel R_2 \parallel R_1)$.

Step 4. S_1 checks if $M_{11}' = M_{11}$. It must hold so S_1 generates a random number r_j.

Step 5. S_1 computes $M_{12} = r_j \oplus K_{GWN-S_1}$, $SK_j = h(ID_i'' \parallel SID_j \parallel r_j'' \parallel r_g' \parallel r_j) = h(ID_1 \parallel SID_1 \parallel R_2 \parallel R_1 \parallel r_j)$ and $M_{13} = h(K_{GWN-S_1} \parallel SK_j \parallel r_j)$. Then S_j sends the response $\{M_{12}, M_{13}\}$ to the other communication party. However, the other communication party is U_1 instead of GWN.

Step 6. After getting the response $\{M_{12}, M_{13}\}$, U_1 computes $r_j' = M_{12} \oplus K_{GWN-S_1}$ and $SK_{GWN} = h(ID_i' \parallel SID_j' \parallel r_i' \parallel r_g \parallel r_j') = h(ID_1 \parallel SID_1 \parallel R_2 \parallel R_1 \parallel r_j') = SK_j$.

According to the above, it is ensured that U_1 who has revealed K_{GWN-S_1} can bypass GWN and acquire sensory data from S_1 directly. Furthermore, because S_1 has no information to determine whether the identity of the communication user exists in GWN's database or not, U_1 can use a forged identity to obtain $S1'$s sensory data. In this case, U_1 only needs to execute the above by replacing ID_1 with the forged identity. Meanwhile, S_1 will retrieve the forged identity. Thereupon, even if an audit mechanism is applied, only the forged identity will be traced.

3.3 Revealing Another Legal User′s Identity and Essential Information for Authentication and Impersonating the Innocent User

After U_1 has obtained K_{GWN-S_1}, U_1 can eavesdrop to reveal another legal user U_2's identity and essential information $h(ID_2 \parallel K_{GWN})$ for authentication when U_2 wants to acquire sensory data from S_1. In login and authentication phase, U_2 will send the login request $\{M_2, M_4, M_5, M_6, M_7\}$ to GWN, where $M_2 = sP$, $M_4 = ID_2 \oplus M_3 = ID_2 \oplus sX = ID_2 \oplus sxP$, $M_5 = M_1 \oplus r_i = h(ID_2 \parallel K_{GWN}) \oplus r_i$, $M_6 = h(ID_2 \parallel r_i) \oplus SID_1$ and $M_7 = h(M_1 \parallel SID_1 \parallel M_3 \parallel r_i)$. Upon receiving the login request, GWN checks whether ID_2 exists in the database or not. If ID_2 exists, the phase proceeds and GWN sends $\{M_8, M_9, M_{10}, M_{11}\}$ to S_1, where $M_8 = ID_2 \oplus K_{GWN-S_1}$, $M_9 = r_g \oplus h(ID_2 \parallel K_{GWN-S_1})$, $M_{10} = r_g \oplus r_i$ and $M_{11} = h(ID_2 \parallel SID_1 \parallel K_{GWN-S_1} \parallel r_i \parallel r_g)$.

However, ID_2 and SID_1 are concealed in the transmitted messages, and GWN is responsible for forwarding messages to multiple sensor nodes. It denotes that U_1 may intercept multiple $\{M_2, M_4, M_5, M_6, M_7\}'$s and $\{M_8, M_9, M_{10}, M_{11}\}'$s. U_1 still can reveal ID_2 and $h(ID_2 \parallel K_{GWN})$ successfully. To ensure whether the revealed ID_2 and $h(ID_2 \parallel K_{GWN})$ are correct or not, U_1 only needs to do the following.

Step 1. For the intercepted and untested $\{M_8, M_9, M_{10}, M_{11}\}$, U_1 computes $q_1 = M_8 \oplus K_{GWN-S_1}$, $q_2 = M_9 \oplus h(q_1 \parallel K_{GWN-S_1})$, $q_3 = M_{10} \oplus q_2$, and $q_4 = h(q_1 \parallel SID_1 \parallel K_{GWN-S_1} \parallel q_3 \parallel q_2)$.

Step 2. U_1 checks if $q_4 = M_{11}$. If it holds, it denotes that U_1 has successfully obtained $ID_2 = q_1$, and the procedure proceeds; otherwise, the process will go back to Step 1.

Step 3. Because GWN will send $\{M_8, M_9, M_{10}, M_{11}\}$ to S_1 after receiving $\{M_2, M_4, M_5, M_6, M_7\}$ within a reasonable period of time, U_1 only needs to use $\{M_2, M_4, M_5, M_6, M_7\}'$s received prior to the matched $\{M_8, M_9, M_{10}, M_{11}\}$. For the intercepted and untested $\{M_8, M_9, M_{10}, M_{11}\}$ received prior to the matched $\{M_8, M_9, M_{10}, M_{11}\}$, U_1 computes $q_4 = M_6 \oplus h(q_1 \parallel q_3)$.

Step 4. U_1 checks if $q_4 = SID_1$. If it holds, it denotes U_1 has successfully retrieve U_2's identity ID_2, and U_1 can obtain $h(ID_2 \parallel K_{GWN})$ by computing $h(ID_2 \parallel K_{GWN}) = M_5 \oplus q_3$; otherwise, the process will go back to Step 3.

According to the above, U_1 can retrieve U_2's identity ID_2 and essential parameter $h(ID_2 \parallel K_{GWN})$ for authentication. Thereupon, U_1 can impersonate U_2 because he can compute M_2, M_3, M_4, M_5, M_6, and M_7, send $\{M_2, M_4, M_5, M_6, M_7\}$ to GWN, and compute the shared session key $SK_i = h(ID_2 \parallel SID_1 \parallel r_i \parallel r_g'' \parallel r_j'')$ after receiving $\{M_{14}, M_{15}, M_{16}\}$ from GWN, where $r_g'' = M_{14} \oplus M_1 = M_{14} \oplus h(ID_2 \parallel K_{GWN})$. If different access rights are granted to different users, this security flaw makes a malicious user able to obtain a privileged account.

3.4 Advanced Discussions

As shown in the previous sections, a legal and malicious user can obtain the secret key K_{GWN-S_j} shared between GWN and S_j after he has acquired sensory data from S_j. After obtaining K_{GWN-S_j}, this malicious user can access S_j without GWN even with a forged identity. Moreover, this user who has successfully obtained K_{GWN-S_j} can reveal the identity of another legal user U_i who also acquires sensory data from S_j, and the innocent user U_i's essential information $h(ID_i \parallel K_{GWN})$ will be retrieved at the same time. Thereupon, the malicious user can impersonate the innocent user U_i to access the desired sensor nodes at will.

Why the above security flaws can be successfully mounted in Li *et al.*′s scheme is because of the following reasons. First, a user′s identity is concealed for anonymity. So the secret K_{GWN-S_j} is used to help S_j to retrieve U_i's identity ID_i. However, because U_i is aware of ID_i and K_{GWN-S_j} is constant, U_i can easily retrieve K_{GWN-S_j} from the transmitted parameter $M_8 = ID_i \oplus K_{GWN-S_j}$. Second, only GWN is aware of whether the user communicating with it exists in the system or not, and S_j only can determine whether

$\{M_8, M_9, M_{10}, M_{11}\}$ is sent by GWN because it is supposed that only GWN and S_j know K_{GWN-S_j}. As a result, if K_{GWN-S_j} is compromised, the user who has obtained K_{GWN-S_j} can cheat GWN and S_j. Third, although the concept of key exchange is adopted by U_i and GWN to make only GWN able to retrieve U_i's identity ID_i from $M_4 = ID_i \oplus M_3 = ID_i \oplus sX = ID_i \oplus sxP = ID_i \oplus xsP = ID_i \oplus xM2$, the secret $h(ID_i \parallel K_{GWN})$ can still be retrieved easily. It is because the transmitted parameter $M_5 = M_1 \oplus r_i = h(ID_i \parallel K_{GWN}) \oplus r_i$ and $h(ID_i \parallel K_{GWN})$ is constant. Although r_i's in different sessions should differ from each other, a malicious user who has successfully obtained K_{GWN-S_j} can retrieve r_i and check whether the retrieved $h(ID_i \parallel K_{GWN})$ is correct or not by $M_6 = h(ID_i \parallel r_i) \oplus SID_j$. The possible and feasible strategy to overcome the found security flaws is to combine nonces with K_{GWN-S_j} and $h(ID_i \parallel K_{GWN})$ to make them vary in different sessions.

4 Conclusions

In this paper, we first review a three-factor anonymous authentication scheme for wireless sensor networks in IoT environments. After analyzing their scheme, we find that it suffers from some security flaws. First, a legal and malicious user can obtain the secret key K_{GWN-S_j} shared between GWN and S_j after he has acquired sensory data from S_j. After obtaining K_{GWN-S_j}, the legal and malicious user can impersonate S_j to negotiate a session key shared with GWN and the legal user and to deliver forged sensory data. Meanwhile, this malicious user can access S_j without GWN even with a forged identity. Moreover, this user who has successfully obtained K_{GWN-S_j} can reveal the identity of another legal user U_i who also acquires sensory data from S_j, and the innocent user U_i's essential information $h(ID_i \parallel K_{GWN})$ will be retrieved at the same time. Thereupon, the malicious user can impersonate the innocent user U_i to access the desired sensor nodes at will. If different access rights are granted to different users, this security flaw makes a malicious user able to obtain a privileged account. Why these found security flaws can damage Li *et al.*'s scheme is because nonces are not combined with shared secrets $h(ID_i \parallel K_{GWN})$ and K_{GWN-S_j}. As a result, a malicious user can easily retrieve them. To amend these flaws, different mechanisms to conceal identities and secrets should be adopted.

Acknowledgments

This work was supported in part by Ministry of Science and Technology under the Grant MOST 107-2622-H-025-001-CC3 and in part by National Taichung University of Science and Technology under the Grant NTCUST108-25.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of anonymity preserving three-factor authenticated key exchange protocol for wireless sensor network," *Computer Networks*, vol. 101, no. 4, pp. 41–61, 2016.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, pp. 2787–2805, 2010.

[4] Y. F. Chang, R. K. Huang, and W. L. Tai, "A critique of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," in *Proceedings of International Conference on Innovation and Management*, pp. 537–544, Feb. 2017.

[5] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Information Sciences*, vol. 321, pp. 263–277, 2015.

[6] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1767–1775, 2014.

[7] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.

[8] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K. K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[9] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Computer Networks*, vol. 53, no. 12, pp. 2022–2037, 2009.

[10] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4081–4092, 2018.

[11] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[12] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316–323, 2013.

Biography

Wei-Liang Tai received the Ph.D. degree in computer science and information engineering from National Chung Cheng University, Taiwan, in 2008. He is currently Associate Professor, Department of Information Communications, Chinese Culture University. His main interests are in information security and forensics and multimedia signal processing.

Ya-Fen Chang is a Professor of Department of Computer Science and Information Engineering at National Taichung University of Science and Technology in Taiwan. She received her B.S. degree in computer science and information engineering from National Chiao Tung University and Ph.D. degree in computer science and information engineering from National Chung Cheng University, Taiwan. Her current research interests include electronic commerce, information security, cryptography, mobile communications, image processing, and data hiding.

Po-Lin Hou is a M.S. student of Department of Computer Science and Information Engineering at National Taichung University of Science and Technology in Taiwan. He received the B.I.M. degree in information management from Ling Tung University in Taiwan in 2016. His main interests are in DevOps, information security, and network security.