Sensors **2013**, *13*, 9589-9603; doi:10.3390/s130809589

OPEN ACCESS

sensors

ISSN 1424-8220

www.mdpi.com/journal/sensors

Article

An Advanced Temporal Credential-Based Security Scheme with Mutual Authentication and Key Agreement for Wireless Sensor Networks

Chun-Ta Li [1], Chi-Yao Weng [2] and Cheng-Chi Lee [3,4,*]

[1] Department of Information Management, Tainan University of Technology, 529 Zhongzheng Road, Tainan City 71002, Taiwan; E-Mail: th0040@mail.tut.edu.tw

[2] Department of Computer Science, National Tsing Hua University, 101 Kuang-Fu Road, Hsinchu City 30013, Taiwan; E-Mail: cyweng@is.cs.nthu.edu.tw

[3] Department of Library and Information Science, Fu Jen Catholic University, 510 Jhongjheng Road, Sinjhuang Dist., New Taipei City 24205, Taiwan

[4] Department of Photonics and Communication Engineering, Asia University, 500 Lioufeng Road, Taichung City 41354, Taiwan

* Author to whom correspondence should be addressed; E-Mail: cclee@mail.fju.edu.tw.

Received: 29 May 2013; in revised form: 18 July 2013 / Accepted: 19 July 2013 / Published: 24 July 2013

Abstract: Wireless sensor networks (WSNs) can be quickly and randomly deployed in any harsh and unattended environment and only authorized users are allowed to access reliable sensor nodes in WSNs with the aid of gateways (GWNs). Secure authentication models among the users, the sensor nodes and GWN are important research issues for ensuring communication security and data privacy in WSNs. In 2013, Xue *et al.* proposed a temporal-credential-based mutual authentication and key agreement scheme for WSNs. However, in this paper, we point out that Xue *et al.*'s scheme cannot resist stolen-verifier, insider, off-line password guessing, smart card lost problem and many logged-in users' attacks and these security weaknesses make the scheme inapplicable to practical WSN applications. To tackle these problems, we suggest a simple countermeasure to prevent proposed attacks while the other merits of Xue *et al.*'s authentication scheme are left unchanged.

Keywords: cryptanalysis; key agreement; mutual authentication; temporal credential; wireless sensor network

---

1. Introduction

Wireless sensor networks are innovative *ad hoc* networks that include a large number of sensor nodes with resource-constrained characteristics such as limited power, communication and computational capabilities [1–4]. As soon as sensor nodes are massively and randomly deployed in a target field, the basic functions of the gateway node are to collect sensitive data for authorized users [5,6]. In many cases, a WSN may be deployed in hostile environments and malicious intruders may launch possible attacks for disrupting the normal operations (such as impersonating a legal user to abuse the network resources, inject false messages or invalid sensors into the WSN, launch security attacks and so on) of a WSN. Therefore, entity authentication [7–16] plays an important role in WSNs and logging-in users and deployed sensors should be authenticated to be the admissible participants by the GWN.

In the recent literature, there are a few works that detail a complete secure user authentication schemes for wireless sensor networks with all their different features. In [17] Das proposed an efficient two-factor scheme of user authentication, which is based on easy-to-remember passwords and smart cards. In Das' scheme, it only needs XOR and hashing computations and this reduces the computational complexity, which is suitable for resource-constrained WSNs. Although Das' scheme enhances system performance, it did not make up for the security weaknesses [18–20]. Das' scheme has later attracted a lot of attention and several two-factor user authentication schemes with mutual authentication and key agreement have been proposed in Li *et al.* [20], Yeh *et al.* [21], Das *et al.* [22], Li *et al.* [23], and Xue *et al.* [24]. In [20], Li *et al.* proposed a secure billing service based on the framework of Das' scheme. In [21], Yeh *et al.* introduced an ECC-based user authentication scheme for preventing all the security flaws of the previous scheme [25]. However, in [23], Li *et al.* showed that Yeh *et al.*'s scheme is insecure against several security attacks and further proposed an improved version of Yeh *et al.*'s scheme, which covers all the identified weaknesses and is more efficient for practical WSN environments. In [24], Xue *et al.* suggest a lightweight temporal-credential-based mutual authentication and key agreement scheme that not only provides more functionality features with higher security, but also ensures low costs of computation, communication and storage.

1.1. Our Contributions

Contributions made in this work can be summarized as follows:

i. We analyze the security weaknesses of one of the most recent temporal-credential-based authentication schemes for WSNs proposed by Xue *et al.* [24]. Xue *et al.* claimed that their authentication scheme is secure against various known attacks with mutual authentication and key agreement and is suitable for resource-constrained WSNs. However, we find that Xue *et al.*'s authentication scheme still has other security weaknesses such as disclosure of the password and failing to prevent the lost smart card problem and many logged-in users' attacks.

ii. We propose an advanced scheme to prevent the security threats of Xue *et al.*'s authentication scheme and the phases in our scheme are shown to be efficient in terms of computational complexity and communication overhead.

iii. Our advanced scheme provides both mutual authentication and key agreement among the user, GWN and the sensor node in wireless sensor networks.

iv. Our three-party authentication scheme can be used to verify users and sensor nodes without revealing their passwords whenever it is deemed to be necessary.
v. A service period feature can be used to revoke users or sensor nodes in a controlled manner and prevent abuse by an authority node GWN.
vi. Status-bit and login recording features are efficiently implemented and assist in catching misbehaving attackers trying to abuse network resources. The above-mentioned features are especially useful when non-registered attackers attempt illegal activities such as many logged-in user attacks.

1.2. Organization of the Paper

The remainder of the paper is organized as follows: Section 2 reviews Xue *et al.*'s authentication scheme [24], whose security weaknesses are shown in Section 3. We propose an advanced authentication scheme with higher security in Section 4, whose security and comparisons of related schemes are analyzed in Section 5 and Section 6, respectively. Section 7 concludes the paper.

2. A Review of Xue *et al.*'s Temporal-Credential-Based Authentication Scheme

In this section, we review Xue *et al.*'s temporal-credential-based mutual authentication scheme [24]. This scheme is mainly composed of three phases: registration, login, authentication and key agreement. Moreover, their scheme is composed of three roles: gateway node (GWN), sensor node (S_j) and user (U_i). For convenience of description, we summarize the notations used throughout this paper in Table 1.

Table 1. Notations used throughout this paper.

Symbol	Description
U_i	User
S_j	Sensor node
GWN	Gateway node
ID_i/PW_i	Identity/Password of the user U_i
SID_j/PW_j	Pre-configured identity/password of the sensor node S_j
K_{GWN_U}/K_{GWN_S}	Two private system parameters only know to GWN
TC_i/TC_j	A temporal credential issued by GWN to U_i/S_j
TS	The timestamp value
KEY_{ij}	The shared session key between U_i and S_j
TE_i	The expiration time of U_i's temporal credential
$\oplus$	The bitwise exclusive-OR operation
$H(\bullet)$	The one-way hashing function
$\|\|$	The bitwise concatenation operation

2.1. Registration Phase

Before registration of the user U_i and the sensor node S_j, each U_i has a secure password pre-shared with GWN and U_i's identity ID_i and hash value of U_i's password $H(PW_i)$ are stored in GWN's side. Moreover, each S_j has a pre-configured password PW_i and hash value of S_j's password $H(PW_i)$ is stored in GWN's side. This phase has two parts for U_i and S_j and we review them as follows:

(U-1) U_i selects ID_i and computes $VI_i = H(TS_1 || H(PW_i))$ and sends $\{ID_i, TS_1, VI_i\}$ to GWN via an open and public channel, where TS_1 is current timestamp value of U_i.

(U-2) After receiving the registration request from U_i, GWN checks if $|TS_1 - T^*_{GWN}| < \Delta T$, where T^*_{GWN} is the current system timestamp of GWN and ΔT is the expected time interval for the transmission delay. If it does not hold, GWN sends REJ message back to U_i. Otherwise, GWN retrieves its own copy of $H(PW_i)$ by using the key "ID_i", computes $VI_i^* = H(TS_1 || H(PW_i))$ and checks if $VI_i^* = VI_i$. If not, GWN terminates it; otherwise, GWN computes $P_i = H(ID_i || TE_i)$, $TC_i = H(K_{GWN\_U} || P_i || TE_i)$ and $PTC_i = TC_i \oplus H(PW_i)$ and personalizes the smart card for U_i with the parameters:$\{H(\bullet), ID_i, H(H(PW_i)), TE_i, PTC_i\}$.

Before deployment of sensor nodes in a target field, each S_j performs the following steps for registration:

(S-1) S_j computes $VI_j = H(TS_2 || H(PW_j))$ and sends $\{SID_j, TS_2\}$ to GWN via an open and public channel, where TS_2 is current timestamp value of S_j.

(S-2) After receiving the message from S_j, GWN checks if $|TS_2 - T^*_{GWN}| < \Delta T$, where T^*_{GWN} is the current system timestamp of GWN and ΔT is the expected time interval for the transmission delay. If it does not hold, GWN sends REJ message back to S_j. Otherwise, GWN retrieves its own copy of $H(PW_j)$ by using the key "SID_j", computes $VI_j^* = H(TS_2 || H(PW_j))$ and check if $VI_j^* = VI_j$. If not, GWN terminates it; otherwise, GWN computes $TC_j = H(K_{GWN\_S} || SID_j)$ and $REG_j = H(H(PW_j) || TS_3) \oplus TC_j$ and sends $\{TS_3, REG_j\}$ to S_j.

(S-3) After receiving the message from GWN, S_j checks if $|TS_3 - T_j^*| < \Delta T$, where T_j^* is the current timestamp value of S_j. If not, S_j terminates it; otherwise, S_j computes its temporal credential $TC_j = REG_j \oplus H(H(PW_j) || TS_3)$ and stores it.

2.2. Login Phase

If the user U_i wants to access sensor data from the wireless sensor network, U_i inserts a smart card into a terminal and enters ID_i and PW_i. The terminal computes $H(H(PW_i))$ and checks the validity of ID_i and PW_i with the stored ID_i and $H(H(PW_i))$. If not, the smart card terminates this login request. Otherwise, U_i passes the verification and he/she can read the information stored in the smart card. U_i computes $TC_i = PTC_i \oplus H(PW_i)$.

2.3. Authentication and Key Agreement Phase

(A-1) U_i computes $DID_i = ID_i \oplus H(TC_i || TS_4)$, $C_i = H(H(ID_i || TS_4) \oplus TC_i)$ and $PKS_i = K_i \oplus H(TC_i || TS_4 || \text{"000"})$ and sends the mutual authentication message $\{DID_i, C_i, PKS_i, TS_4, TE_i, P_i\}$ to GWN, where TS_4 is current timestamp value of U_i, K_i is a random key only

known to U_i and the binary number ”000” is used for distinguishing $H(TC_i||TS_4||\text{”000”})$ and $H(TC_i||TS_4)$.

(A-2) After receiving the message from U_i, GWN checks the validity of TS_4. If TS_4 is valid for the transmission delay, GWN computes $ID_i = DID_i \oplus H(H(K_{GWN\_U}||P_i||TE_i)||TS_4)$, $P_i^* = H(ID_i||TE_i)$, $TC_i = H(K_{GWN\_U}||P_i||TE_i)$ and $C_i^* = H(H(ID_i^*||TS_4) \oplus TC_i)$ and verifies whether $C_i^* \neq C_i$ or $P_i^* \neq P_i$. If it holds, GWN rejects U_i's login request; otherwise, GWN computes $K_i = PKS_i \oplus H(TC_i||TS_4||\text{”000”})$ and chooses a nearby suitable sensor node S_j as the accessed sensor node. GWN further computes S_j's temporal credential $TC_j = H(K_{GWN\_S}||SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i||TC_j||TS_5)$, $C_{GWN} = H(ID_i||TC_j||TS_5)$ and $PKS_{GWN} = K_i \oplus H(TC_j||TS_5)$ and sends $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ to S_j, where TS_5 is current timestamp value of GWN.

(A-3) After receiving the message from GWN, S_j checks the validity of TS_5. If TS_5 is valid for the transmission delay, S_j computes $ID_i = DID_{GWN} \oplus H(DID_i||TC_j||TS_5)$ and $C_{GWN}^* = H(ID_i||TC_j||TS_5)$ and checks if $C_{GWN}^* = C_{GWN}$. If not, S_j terminates this session. Else, S_j convinces that the received message is from a legitimate GWN. Moreover, S_j computes $K_i = PKS_{GWN} \oplus H(TC_j||TS_5)$, $C_j = H(K_j||ID_j||SID_j||TS_6)$ and $PKS_j = K_j \oplus H(K_i||TS_6)$ and sends $\{SID_j, TS_6, C_j, PKS_j\}$ to U_i and GWN, where K_j is a random key chosen by S_j.

(A-4) After receiving the message from S_j, U_i and GWN separately computes $K_j = PKS_j \oplus H(K_i||TS_6)$ and $C_j^* = H(K_j||ID_i||SID_j||TS_6)$. For GWN, if $C_j^* = C_j$, S_j is authenticated by GWN. For the user U_i, if $C_j^* = C_j$, S_j and GWN are authenticated by U_i. Finally, U_i and S_j can separately compute a common session key $KEY_{ij} = H(K_i \oplus K_j)$ and U_i and S_j will use KEY_{ij} for securing communications in future.

3. Security Analysis on Xue *et al.*'s Scheme

Xue *et al.* claimed that their authentication scheme is robust and secure against insider, password guessing and stolen smart card attacks. In fact, based on our security analysis, we observe that Xue *et al.*'s temporal-credential based scheme is insecure against these security requirements. The details of our attacks are as follows.

3.1. Stolen Verifier and Insider Attack

In Xue *et al.*'s scheme, GWN needs to maintain the verifier table and it stores each U_i's identity ID_i and hash value to U_i's password $H(PW_i)$ in GWN's side. In a practical environment, the PW_i chosen by U_i could be short and easily human memorizable, which might be convenient for U_i to remember easily and in practice many users use same identities and passwords to access various online applications or remote servers for their convenience. Thus, we assume that an attacker U_A may steal the password-verifier from GWN's database and launches off-line guessing attacks on it to obtain U_i's real password PW_i. The details of stolen verifier attack are as follows.

Step 1: U_A steals verifier table from GWN's database and retrieves the hash value of U_i's password $H(PW_i)$.

Step 2: U_A guesses a password PW_i^* and computes $H(PW_i^*)$.

Step 3: U_A compares the result of $H(PW_i^*)$ with stolen $H(PW_i)$.

A match in Step 3 above indicates the correct guessing of U_i's easy-to-remember password and Xue *et al.*'s authentication scheme then cannot resist the stolen verifier attack. Moreover, if a privileged insider of GWN knows U_i's password PW_i, he/she may try to use the knowledge of U_i's PW_i and ID_i to access other applications or servers.

3.2. Off-Line Password Guessing Attack

In step (U-1) of registration phase of Xue *et al.*'s scheme, U_i sends$\{ID_i, TS_1, VI_i\}$ to GWN via an open and public environment, where TS_1 is current timestamp value of U_i and $VI_i = H(TS_1||H(PW_i))$. If an attacker U_A eavesdrops U_i's registration message $\{ID_i, TS_1, VI_i\}$, U_A can launch the off-line password guessing attack by performing the following step:

Step 1: U_A guesses a password PW_i^* and computes $VI_i^* = H(TS_1||H(PW_i^*))$.
Step 2: U_A compares the result of VI_i^* with eavesdropped VI_i.

A match in Step 2 above indicates the correct guessing of U_i's easy-to-remember password and Xue *et al.*'s authentication scheme suffers from off-line password guessing attack in user side. On the other hand, in step (S-1) of registration phase, S_j sends $\{SID_j, TS_2, VI_i\}$ to GWN via an open and public environment, where TS_2 is the current timestamp value of S_j and $VI_j = H(TS_2||H(PW_j))$. If an attacker U_A eavesdrops S_j's registration message $\{SID_j, TS_2, VI_j\}$, U_A can launch an off-line password guessing attack by performing the following steps:

Step 1: U_A guesses a password PW_j^* and computes $VI_j^* = H(TS_2||H(PW_j^*))$.
Step2: U_A compares the result of VI_j^* with eavesdropped VI_j.

A match in Step 2 above indicates the correct guessing of S_j's password and Xue *et al.*'s authentication scheme is then open to an off-line password guessing attack on the sensor side. Moreover, once U_A has successfully guessed S_j's random password, U_A can use PW_j^* and the eavesdropped message in step (S-2) of the registration phase to derive S_j's temporal credential TC_j by computing $TC_j=REG_j \oplus H(H(PW_j^*)||TS_3) = H(K_{GWN\_S}||SID_j)$. Finally, Xue *et al.*'s scheme may suffer from masquerading attacks and an attacker U_A who knows TC_j can easily impersonate the sensor node S_j.

3.3. Lost Smart Card Problem

Let us consider the scenario of a lost smart card problem. In the case where U_i's smart card is lost and it is picked up by an attacker U_A, the stored parameters can be extracted by launching a power analysis attack [22]. As we know, the content of U_i's smart card is $\{H(\bullet), ID_i, H(H(PW_i)), TE_i, PTC_i\}$. With this information, U_A can launch another off-line password guessing attack by performing the following steps:

Step 1: U_A guesses a password PW_i^* and computes $H(H(PW_i^*))$.
Step 2: U_A compares the result of $H(H(PW_i^*))$ with extracted $H(H(PW_i^*))$.

If Step 2 holds, the guessed password PW_i^* is the same as U_i's real password PW_i. Otherwise, U_A tries another password. Once U_A successfully guesses U_i's real password, U_A can use PW_i^* and the content of U_i's smart card to derive U_i's temporal credential TC_i by computing $TC_i = PTC_i \oplus H(PW_i^*) = H(K_{GWN\_U}||P_i||TE_i)$. Thus, Xue *et al.*'s scheme may suffer from masquerading attacks and an attacker

U_A who knows TC_i can easily impersonate a legal user U_i to log in to the gateway node and GWN is not aware of having caused any problem.

3.4. Many Logged-in Users' Problem

The many logged-in users attack [26,27] means that if a registered user U_i's smart card is massively duplicated and his/her identity ID_i and password PW_i are exposed to m non-registered users U_a, where $a = 1, 2, \ldots, m$. Each one who has a smart card and knows ID_i and PW_i can log in to GWN at the same time and GWN is not aware of having caused any problem. In Xue *et al.*'s scheme, each non-registered user U_a generates his/her timestamp TS_a and random key K_a and sends a legal login message $\{DID_a, C_a, PKS_a, TS_a, TE_i, P_i\}$ to GWN, where $DID_a = ID_i \oplus H(TC_i||TS_a)$, $C_a = H(H(ID_i||TS_a) \oplus TC_i)$ and $PKS_a = K_a \oplus H(TC_i||TS_a||\text{"000"})$. After receiving all the login requests from U_a, GWN gets the same identity ID_i with different timestamps TS_a and random keys K_a and GWN allows them to log in and access U_i's account simultaneously.

4. Advanced Authentication Scheme

In this section, we propose an advanced scheme with strong security. Our advanced scheme consists of four phases, namely pre-registration phase, registration phase, login phase, authentication and key agreement phase. The details of each of these phases are as follows.

4.1. Pre-Registration Phase

Before registration of the user U_i and the sensor node S_j, each U_i has a pre-configured pair of identity ID_i^{pre} and password PW_i^{pre} with GWN and the unique parameter $H(ID_i^{pre}||PW_i^{pre})$ and ID_i^{pre} are kept by GWN to check the validity of registration user. Moreover, each S_j has a pre-configured identity SID_j and a 160-bits random number r_j and the hash value of S_j's pre-configured identity and random number $H(SID_j||r_j)$ and SID_j are stored on the GWN's side.

4.2. Registration Phase

This phase has two parts for U_i and S_j and the details will be described as follows:

(U-1) U_i selects his/her own ID_i and password PW_i. Then U_i computes $VI_i = H(TS_1||H(ID_i^{pre}||PW_i^{pre}))$, $CI_i=H(ID_i^{pre}||PW_i^{pre}) \oplus H(ID_i||PW_i||r_i)$, $DI_i = ID_i \oplus H(ID_i^{pre}||PW_i^{pre})$ and sends $\{ID_i^{pre}, TS_1, VI_i, CI_i, DI_i\}$ to GWN via an open and public channel, where TS_1 is current timestamp value of U_i and r_i is a random number generated by U_i.

(U-2) After receiving the registration request from U_i, GWN checks if $|TS_1 - T^*_{GWN}| < \Delta T$, where T^*_{GWN} is the current system timestamp of GWN and ΔT is the expected time interval for the transmission delay. If it does not hold, GWN sends REJ message back to U_i. Otherwise, GWN retrieves its own copy of $H(ID_i^{pre}||PW_i^{pre})$ by using the parameter "ID_i^{pre}", computes $VI_i^* = H(TS_1||\ H(ID_i^{pre}||PW_i^{pre}))$ and checks if $VI_i^* = VI_i$. If not, GWN terminates it; otherwise, GWN computes $Q_i=CI_i \oplus H(ID_i^{pre}||PW_i^{pre}) = H(ID_i||PW_i||r_i)$, $ID_i = DI_i \oplus H(ID_i^{pre}||PW_i^{pre})$, $P_i = H(ID_i||TE_i)$, $TC_i = H(K_{GWN\_U}||P_i||TE_i)$ and $PTC_i = TC_i \oplus Q_i$ and personalizes the smart card for U_i with the parameters:$\{H(\bullet), H(Q_i), TE_i, PTC_i\}$. Note that GWN maintains a write protected

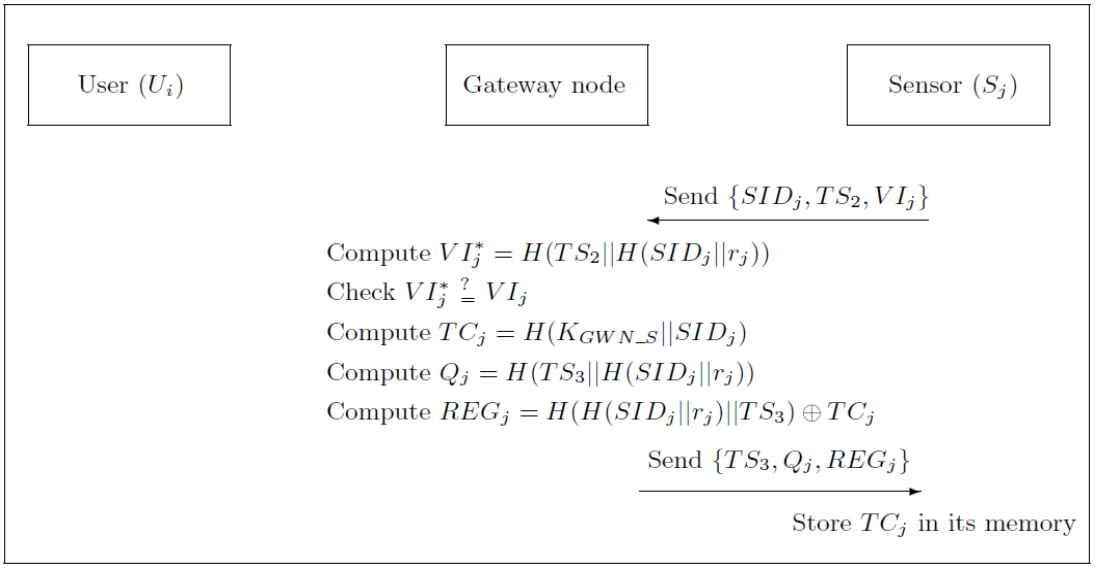
file as depicted in Table 2, where the *Status-bit* indicates the status of the user, *i.e.*, when U_i is logged-in to GWN, the status-bit is set to one, otherwise it is set to zero. Finally, GWN sends $H(Q_i)$ and smart card to U_i via an public and open environment.

(U-3) After receiving $H(Q_i)$ and smart card from GWN, U_i checks whether the computed $H(H(ID_i||PW_i||r_i))$ is equal to $H(Q_i)$. If they are not equal, U_i aborts this session and the smart card. Otherwise, GWN is authenticated by U_i. U_i enters r_i into his/her smart card and U_i's smart card contains $\{H(\bullet), H(Q_i), TE_i, PTC_i, r_i\}$. Note that U_i does not need to remember r_i after finishing this phase. The communication handshakes of the registration phase of the user U_i are depicted in Figure 1.

Table 2. The identity table of GWN after finishing the registration phase.

User Identity	Password-Verifier	Status-Bit	Last Login	Service Period
…	…	…	…	…
ID_i	Q_i	0/1	N/A	TE_i
…	…	…	…	…

Figure 1. Communication handshakes of the registration phase of the user U_i.



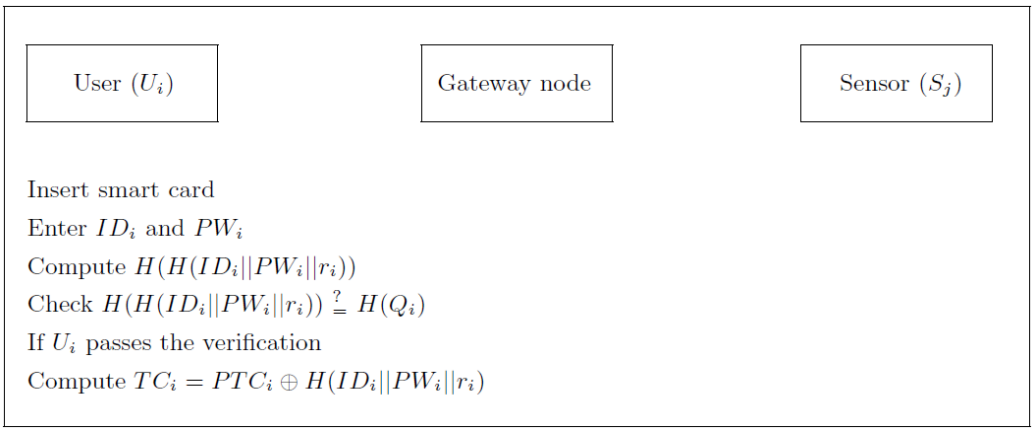
Before deployment of sensor nodes in a target field, each S_j performs the following steps for registration.

(S-1) S_j computes $VI_j = H(TS_2||H(SID_j||r_j))$ and sends $\{SID_j, TS_2, VI_j\}$ to GWN via an open and public channel, where TS_2 is current timestamp value of S_j.

(S-2) After receiving the message from S_j, GWN checks if $|TS_2 - T^*_{GWN}| < \Delta T$, where T^*_{GWN} is the current system timestamp of GWN and ΔT is the expected time interval for the transmission delay. If it does not hold, GWN sends REJ message back to S_j. Otherwise, GWN retrieves its own copy of $H(SID_j||r_j)$ by using the key "SID_j", computes $VI_j^* = H(TS_2||H(SID_j||r_j))$ and checks if $VI_j^* = VI_j$. If not, GWN terminates it; otherwise, GWN computes $TC_j = H(K_{GWN\_S}||SID_j)$, $Q_j = H(TS_3||H(SID_j||r_j))$ and $REG_j = H(H(SID_j||r_j)||TS_3) \oplus TC_j$ and sends $\{TS_3, Q_j, REG_j\}$ to S_j.

(S-3) After receiving the message from GWN, S_j checks if $|TS_3 - T_j^*| < \Delta T$, where T_j^* is the current timestamp value of S_j. If not, S_j terminates it. Otherwise, S_j checks whether the computed $H(TS_3||H(SID_j||r_j)$ is equal to Q_j. If they are equal, S_j computes its temporal credential $TC_j = REG_j \oplus H(H(SID_j)||r_j||TS_3)$ and stores it. Note that S_j does not need to store r_j after finishing the phase. The communication handshakes of the registration phase of sensor node S_j are depicted in Figure 2.

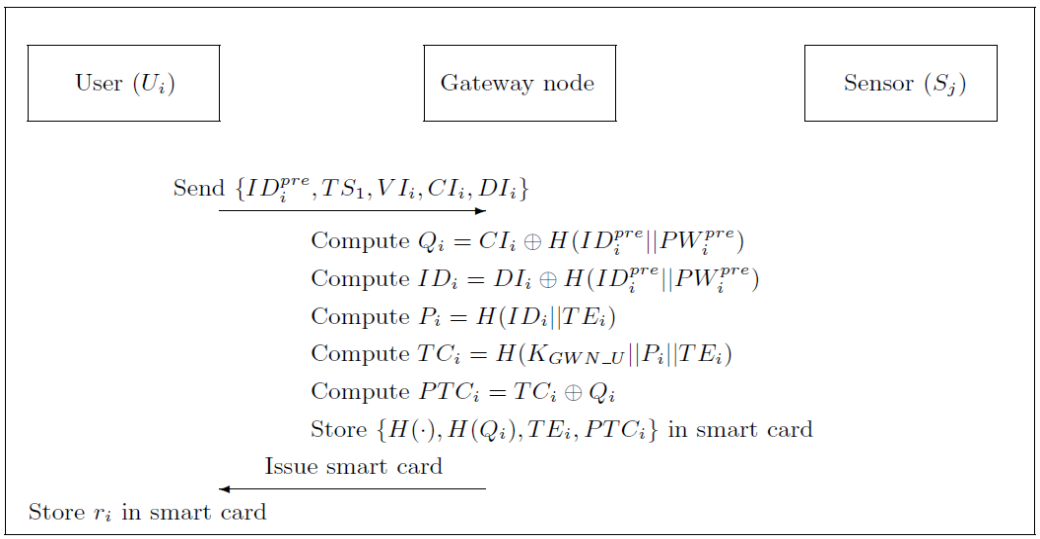
Figure 2. Communication handshakes of the registration phase of sensor node S_j.



4.3. Login Phase

If the user U_i wants to access sensor data from the wireless sensor network, U_i inserts a smart card into a card reader and enters ID_i and PW_i. The smart card retrieves r_i, computes $H(H(ID_i||PW_i||r_i)) \neq H(Q_i)$, and the smart card terminates this login request. Otherwise, U_i passes the verification and he/she can read the information stored in the smart card. U_i computes $TC_i = PTC_i \oplus H(ID_i||PW_i||r_i)$. The details of the login phase are shown in Figure 3.

Figure 3. Illustration of the login phase of our advanced scheme.



4.4. Authentication and Key Agreement Phase

(A-1) U_i computes $DID_i = ID_i \oplus H(TC_i||TS_4)$, $C_i = H(H(ID_i||PW_i||r_i)||TS_4) \oplus TC_i)$ and $PKS_i = K_i \oplus H(TC_i||TS_4||\text{"000"})$ and $H(TC_i||TS_4)$.

(A-2) After receiving the message from U_i, GWN checks the validity of TS_4. If TS_4 is valid for the transmission delay, GWN computes $TC_i^* = H(K_{GWN\_U}||P_i||TE_i)$ and $ID_i = DID_i \oplus H(TC_i^*||TS_4)$ and retrieves U_i's password-verifier of $Q_i = H(ID_i||PW_i||r_i)$ by using the parameter "ID_i". Then, GWN further computes $C_i^* = H(H(Q_i||TS_4) \oplus TC_i)$ and verifies whether $C_i^* = C_i$. If it does not hold, GWN rejects U_i's login request; otherwise, the status-bit is set to one and TS_4 is recorded in the 4th field of the identity table to demonstrate U_i's last login. GWN computes $K_i = PKS_i \oplus H(TC_i||TS_4||\text{"000"})$ and chooses a nearby suitable sensor node S_j as the accessed sensor node. GWN further computes S_j's temporal credential $TC_j = H(K_{GWN\_S}||SID_j)$, $DID_{GWN} = ID_i \oplus H(DID_i||TC_j||TS_5)$, $C_{GWN} = H(ID_i||TC_i||TS_5)$ and $PKS_{GWN} = K_i \oplus H(TC_j||TS_5)$ and sends $\{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}\}$ to S_j, where TS_5 is current timestamp value of GWN.

(A-3) After receiving the message from GWN, S_j checks the validity of TS_5. If TS_5 is valid for the transmission delay, S_j computes $ID_i = DID_{GWN} \oplus H(DID_i||TC_j||TS_5)$ and $C^*_{GWN} = H(ID_i||TC_j||TS_5)$ and check if $C^*_{GWN} = C_{GWN}$. If not, S_j terminates this session. Else, S_j convinces that the received message is from a legitimate GWN. Moreover, S_j computes $K_i = PKS_{GWN} \oplus H(TC_j||TS_5)$, $C_j = H(K_j||ID_i||SID_i||TS_6)$ and $PKS_j = K_j \oplus H(K_i||TS_6)$ and sends$\{SID_j, TS_6, C_j, PKS_j\}$ to U_i and GWN.

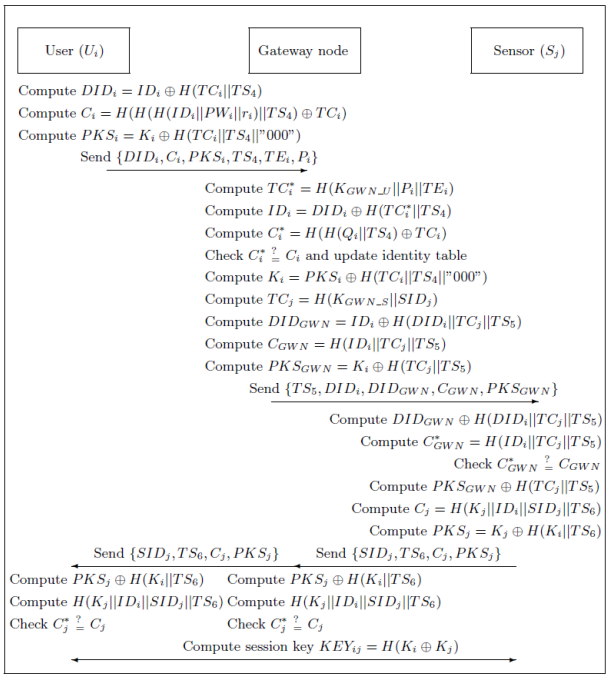
(A-4) After receiving the message from S_j, U_i and GWN separately computes $K_j = PKS_j \oplus H(K_i||TS_6)$ and $C_j^* = H(K_j||ID_i||SID_j||TS_6)$. For GWN, if $C_j^* = C_j$, S_j is authenticated by GWN. For the user U_i, if $C_j^* = C_j$, S_j and GWN are authenticated by U_i. Finally, U_i and S_j can separately compute a common session key $KEY_{ij} = H(K_i \oplus K_j)$ and U_i and S_j will use KEY_{ij} for securing communications in future.

After finishing the authentication and key agreement phase, the identity table is updated and the content of the identity table is shown in Table 3. The detailed steps of the authentication and key agreement phase are shown in Figure 4.

Table 3. The identity table of GWN after finishing the authentication and key agreement phase.

User Identity	Password-Verifier	Status-Bit	Last Login	Service Period
…	…	…	…	…
ID_i	Q_i	0/1	TS_4	TE_i
…	…	…	…	…

Figure 4. Illustration of the authentication and key agreement phase of our advanced scheme.



5. Security Analysis on Our Advanced Authentication Scheme

In this section, for security analysis on our advanced authentication scheme, we use the threat model described in Section 3 and show that our proposed scheme can withstand the following security attacks. Let us consider the following threat scenarios.

– *Scenario 1*. We assume that a privileged-insider of GWN can steal U_i's identity and password verifier from the GWN's identity table.
– *Scenario 2*. We assume that an attacker can eavesdrop U_i's registration message.
– *Scenario 3*. We assume that a legal user's smart card has been stolen or lost and the attacker can extract the secret parameters stored in the smart card.
– *Scenario 4*. We assume that U_i's identity ID_i, password PW_i and login parameters $\{H(\bullet), H(Q_i), TE_i, PTC_i, r_i\}$ are leaked to more than one non-registered users.

5.1. Resistance to Stolen Verifier and Insider Attacks

In registration phase of our advanced authentication scheme, U_i registers to GWN by presenting $Q_i = H(ID_i||PW_i||r_i)$ instead of PW_i and $H(PW_i)$. For the threat model in Scenario 1, we assume that a privileged-insider of GWN can steal U_i's identity and password-verifier from GWN's identity table. Note that the value of r_i is not revealed to GWN and the bit length of $|r_i|$ is large enough. If SHA-256 is used in our advanced scheme, the attacker may attempt to derive PW_i and r_i from password-verifier $Q_i = H(ID_i||PW_i||r_i)$. Due to the intractability under the assumption of a secure one-way hashing function and the bit-length of r_i is 160 bits. Thus, the probability to guess correct r_i is $1/2^{160}$. Moreover, the attacker must guess a correct password PW_i and the probability to guess a correct p character PW_i approximated to $1/2^{6p}$. Therefore, it is computationally infeasible for the attacker to derive U_i's password PW_i and random number r_i at the same time because the probability approximated to

$1/2^{(6p+160)}$. As a result, a privileged-insider still cannot derive U_i's real password PW_i by performing off-line password guessing attacks on $H(ID_i||PW_i||r_i)$ and our advanced authentication scheme is secure against stolen verifier and insider attacks.

5.2. Resistance to Off-Line Password Guessing Attacks

In step (U-1) of registration phase of our scheme, U_i sends $\{ID_i^{pre}, TS_1, VI_i, CI_i, DI_i\}$ to GWN via an open and public environment. For the threat model in Scenario 2, if an attacker U_A eavesdrops U_i's registration message $\{ID_i^{pre}, TS_1, VI_i, CI_i, DI_i\}$. First, U_A cannot derive U_i's password-verifier $H(ID_i||PW_i||r_i)$ from $CI_i = H(ID_i^{pre}||PW_i^{pre}) \oplus H(ID_i||PW_i||r_i)$ because U_A does not know U_i's unique parameter $H(ID_i^{pre}||PW_i^{pre})$. Second, U_i's password-verifier $H(ID_i||PW_i||r_i)$ is under protection of a one-way hashing function and it is computationally infeasible without knowing U_i's identity ID_i, password PW_i and the random number r_i. We assume the bit-length of ID_i is q characters and the probability to guess a correct m character ID_i approximated to $1/2^{6q}$. Therefore, it is computationally infeasible for the attacker to derive U_i's identity ID_i, password PW_i and random number r_i at the same time because the probability approximated to $1/2^{(6p+6q+160)}$. On the other hand, in step (S-1) of registration phase of our scheme, S_j registers to GWN by presenting $\{SID_j, TS_2, VI_j = H(TS_2||H(SID_j||r_j))\}$ instead of PW_j and $H(PW_j)$. Therefore the attacker cannot launch an off-line guessing attack unless he/she knows the random number r_j. In this case, a possible off-line password guessing attack on user or sensor side is not working in our advanced scheme.

5.3. Resistance to Smart Card Lost Problem

The smart card lost problem is an inherent limitation of remote user authentication schemes. For the threat model in Scenario 3, we assume that U_i's smart card has been stolen or lost and the attacker U_A can extract the secret parameters $\{H(\bullet), H(Q_i), TE_i, PTC_i, r_i\}$ stored in the smart card. However, in order to log in to GWN by using U_i's lost or stolen smart card, U_A needs to guess real identity ID_i and password PW_i correctly at the same time. In fact, it is computationally infeasible to guess these two parameters correctly at the same time in polynomial time since ID_i and PW_i are well-protected by a one-way hashing function. Therefore, our proposed scheme can withstand this type of attack too.

5.4. Resistance to the Many Logged-in Users Problem

For the threat model in Scenario 4, we assume that U_i's identity ID_i, password PW_i and parameters $\{H(\bullet), H(Q_i), TE_i, PTC_i, r_i\}$ are leaked to more than one non-registered users. However, the gateway node GWN maintained a status-bit field and a last login field in its identity table. Therefore, no one is allowed to login GWN at the same time out of all who know ID_i, PW_i and valid parameters $\{H(\bullet), H(Q_i), TE_i, PTC_i, r_i\}$. Based on the protection of GWN's identity table, the advanced scheme is secure against many logged-in users attacks.

6. Comparisons of Related Schemes

In this section, we will analyse the functionality and performance of our advanced scheme and compare it with Xue *et al.*'s scheme [24] and other related schemes [17,21]. Functionality and

performance comparisons of our scheme and other related schemes [17,21,24] are shown in Table 4 and Table 5, respectively. In Table 4, we can see that our advanced scheme not only provides proper password protection and secure service billing, but also prevents many logged-in users attack and other attacks. According to the analysis results reported in [10,24], the time complexity of various operations in terms of T_H and T_{ECC} are listed in Table 5. We have compared the computational complexity using both formulated results and rough quantitative analysis in Table 5 for different phases: the registration, login and authentication phases of [17,21,24], and our scheme. For example in the test environment (CPU: 2.4 GHz, RAM: 4.0 G), we have run it 100 times to get the average result. T_H is about 3,000 times faster than T_{ECC} (T_H is nearly 0.0002 second on average when using SHA-256 and T_{ECC} is nearly 0.6 second on average when using ECC-160). Our advanced scheme, Yeh *et al.* [21] and Xue *et al.* [24] all provide the functions of session key agreement and mutual authentication between each two of the user, GWN and the sensor node.

Table 4. Functionality comparisons of our advanced scheme and related schemes.

Items/Schemes	Das [17] (2009)	Yeh *et al.* [21] (2011)	Xue *et al.* [24] (2013)	Our Advanced Scheme
Mutual authentication	No	Yes	Yes	Yes
Key agreement	No	Yes	Yes	Yes
Password protection	No	No	No	Yes
Provision of service billing	No	No	Yes	Yes
Resistant to stolen verifier attack	Yes	Yes	No	Yes
Resistant to insider attack	No	Yes	No	Yes
Resistant to lost smart card attack	No	No	No	Yes
Resistant to many logged-in users' attack	No	No	No	Yes

Table 5. Performance comparisons of our advanced scheme and related schemes.

Participant/Computations	Das [17] (2009)	Yeh *et al.* [21] (2011)	Xue *et al.* [24] (2013)	Our Advanced Scheme
User (U_i)	4 T_H	1 T_H + 2 T_{ECC}	7 T_H	9 T_H
Sensor (S_j)	1 T_H	3 T_H + 2 T_{ECC}	5 T_H	6 T_H
Gateway node (GWN)	7 T_H	4 T_H + 4 T_{ECC}	10 T_H	11 T_H
Computation costs	12 T_H	8 T_H + 8 T_{ECC}	22 T_H	26 T_H
Computation time	0.0024 s	4.8016 s	0.0044 s	0.0052 s

T_H: Time for SHA-256 one-way hashing computation; T_{ECC}: Time for ECC-160 encryption/decryption computation; s: Second.

Moreover, our scheme and Xue *et al.* [24] both provide the service billing function. Our advanced scheme requires $9T_H$ for the user, $6T_H$ for the sensor node and $11T_H$ for GWN. Assume T_H = 0.0002 second and T_{ECC} = 0.6 second according to our simulation.

Compared with other three schemes which cannot ensure password protection, all participants in three phases of our advanced scheme require about 0.0052 seconds, which can be almost ignored, so our advanced scheme does not increase too much computational complexity while providing more function requirements and preventing more security attacks.

7. Conclusions

In this paper, we have analyzed the vulnerability and security attacks existing in Xue *et al.*'s temporal-credential-based mutual authentication scheme and proposed an advanced secure authentication scheme which can satisfy mutual authentication and key agreement between the user, the gateway node and the sensor node. Compared to the existing schemes, our advanced scheme supports extra functionalities such as user password protection and login recording strategy for enhancing the system security. In addition, through the use of lightweight one-way hashing computation, our authentication scheme significantly reduces the implementation cost. Through informal security analysis, we have shown that our proposed scheme has the ability to resist various known attacks, including stolen verifier attacks, insider attacks, lost smart card problems and many logged-in users attack, *etc.* As a result, extra functionalities are added and its higher security along with low computational cost make our advanced scheme very appropriate for securing wireless sensor networks in practice.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract No.: NSC 101-2221-E-165-002 and NSC 102-2221-E-030-003.

Conflict of Interest

The authors declare no conflict of interest.

References

1. Asadi, M.; Zimmerman, C.; Agah, A. A game-theoretic approach to security and power conservation in wireless sensor networks. *Int. J. Netw. Secur.* **2013**, *15*, 50–58.
2. Das, A.K. Improving Identity-based Random Key Establishment Scheme for Large-scale hierarchical wireless sensor networks. *Int. J. Netw. Secur.* **2012**, *14*, 1–21.
3. Li, C.T. Secure smart card based password authentication scheme with user anonymity. *Inform. Technol. Contr.* **2011**, *40*, 157–162.
4. Mi, Q.; Stankovic, J.A.; Stoleru, R. Practical and secure localization and key distribution for wireless sensor networks. *Ad Hoc Netw.* **2012**, *10*, 946–961.
5. Jie, H.; Guohua, O. A public key polynomial-based key pre-distribution scheme for large-scale wireless sensor networks. *Ad Hoc Sens. Wirel. Netw.* **2012**, *16*, 45–64.
6. Poornima, A.S.; Amberker, B.B. Secure end-to-end data aggregation (seeda) protocols for wireless sensor networks. *Ad Hoc Sens. Wirel. Netw.* **2013**, *17*, 193–219.
7. Delgado-Mohatar, O.; Fuster-Sabater, A.; Sierra, J.M. A light-weight authentication scheme for wireless sensor networks. *Ad Hoc Netw.* **2011**, *9*, 727–735.
8. Han, K.; Kim, K.; Choi, W.; Choi, H.H.; Seo, J.; Shon, T. Efficient authenticated key agreement protocols for dynamic wireless sensor networks. *Ad Hoc Sens. Wirel. Netw.* **2012**, *14*, 251–269.
9. Li, C.T.; Hwang, M.S. An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.* **2010**, *33*, 1–5.

10. Li, C.T.; Hwang, M.S. A lightweight anonymous routing protocol without public key en/decryptions for wireless *ad hoc* networks. *Inform. Sci.* **2011**, *181*, 5333–5347.
11. Li, Z.; Gong, G. Computationally efficient mutual entity authentication in wireless sensor networks. *Ad Hoc Netw.* **2011**, *9*, 204–215.
12. Li, C.T.; Lee, C.C. A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Math. Comput. Model.* **2012**, *55*, 35–44.
13. Li, C.T. A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. *Inform. Technol. Contr.* **2012**, *41*, 69–76.
14. Ramasamy, R.; Muniyandi, A.P. An efficient password authentication scheme for smart card. *Int. J. Netw. Secur.* **2012**, *14*, 180–186.
15. Barsocchi, P.; Chessa, S.; Martinovic, I.; Oligeri, G. A cyber-physical approach to secret key generation in smart environments. *J. Amb. Intell. Human. Comput.* **2013**, *4*, 1–16.
16. Barsocchi, P.; Chessa, S.; Martinovic, I.; Oligeri, G. AmbiSec: Securing smart spaces using entropy harvesting. *Lect. Notes Comput. Sci.* **2010**, *6439*, 73–85.
17. Das, M.L. Two-factor user authentication scheme in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1086–1090.
18. Han, K.; Kim, K.; Choi, W. An enhanced two-factor user authentication scheme in wireless sensor networks. *Ad Hoc Sens. Wirel. Netw.* **2010**, *10*, 361–371.
19. Khan, M.K.; Alghathbar, K. Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. *Sensors* **2010**, *10*, 2450–2459.
20. Li, C.T.; Lee, C.C.; Wang, L.J.; Liu, C.J. A secure billing service with two-factor user authentication in wireless sensor networks. *Int. J. Innov. Comput. Inform. Contr.* **2011**, *7*, 4821–4831.
21. Yeh, H.L.; Chen, T.H.; Liu, P.C.; Kim, T.H.; Wei, H.W. A secure authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sens. J.* **2011**, *11*, 4767–4779.
22. Das, A.K.; Sharma, P.; Chatterjee, S.; Sing, J.K. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *J. Netw. Comput. Appl.* **2012**, *35*, 1646–1656.
23. Li, C.T.; Lee, C.C.; Lee, C.W. An improved two-factor user authentication protocol for wireless sensor networks using elliptic curve cryptography. *Sens. Lett.* **2013**, in press.
24. Xue, K.; Ma, C.; Hong, P.; Ding, R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *J. Netw. Comput. Appl.* **2013**, *36*, 316–323.
25. Chen, T.H.; Shih, W.K. A robust mutual authentication protocol for wireless sensor networks. *ETRI J.* **2010**, *32*, 704–712.
26. Li, C.T.; Lee, C.C.; Weng, C.Y.; Fan, C.I. An extended multi-server-based user authentication and key agreement scheme with user anonymity. *KSII Trans. Int. Inform. Syst.* **2013**, *7*, 119–131.
27. Li, C.T. A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card. *IET Inform. Secur.* **2013**, *7*, 3–10.