ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2016, T. 45, Nr. 1

Cryptanalysis and Improvement of an Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks

Fushan Wei[1;2], Jianfeng Ma[1], Qi Jiang[1], Jian Shen[3], Chuangui Ma[2]

[1] *School of Computer Science and Technology, Xidian University*
Xi'an 710071, China

[2] *State Key Laboratory of Mathematical Engineering and Advanced Computing,*
Zhengzhou 450002, China
e-mail: weifs831020@163.com

[3] *School of Computer and Software, Nanjing University of Information Science and Technology,*
Nanjing 210000, China

crossref http://dx.doi.org/10.5755/j01.itc.45.1.11949

Abstract. In order to address the scenario in which the user wants to access the real-time data directly from the sensor node in wireless sensor networks (WSNs), Das proposed a two-factor authentication scheme. In 2010, Khan et al. pointed out that Das's scheme has some security flaws and proposed an improved scheme. Recently, Yuan demonstrated that Khan et al.'s improvement is still insure against several attacks. Yuan also proposed an enhanced two-factor user authentication scheme using user's biometrics to fix the security flaws in Khan et al.'s scheme. In this paper, we show that Yuan's scheme still suffers from the stolen smart card attack and the GW-node impersonation attack. Moreover, biometric keys are misused in Yuan's scheme such that even the valid user cannot pass the biometric verification. To remedy these problems, we propose an improved two-factor authenticated key distribution scheme based on fuzzy extractors. Security and performance analysis demonstrates that our scheme is more secure and efficient than previous schemes.

Keywords: wireless sensor networks; two-factor authentication; bio-metrics; smart card.

1. Introduction

Wireless sensor network (WSN) is a high and new technology that consists of spatially distributed autonomous sensors to cooperatively monitor physical or environ-mental conditions and pass their data through the network to a main location. WSNs are widely used in many applications, such as battlefield surveillance, health care monitoring, forest fire detection, water quality monitoring, and traffic control [1]. WSNs are often deployed in an unattended or a rather hostile environment, and the data collected are confidential and valuable. Therefore, user authentication is a primary concern in WSNs before accessing data from the sensor nodes [2–4].

Usually, most of the queries in WSN applications are managed by base sta-tions or Gateway nodes (GW-nodes) of the network. However, there are also great needs to access the real-time data inside the WSN. In such cases, the user can directly access the real-time data from the sensor nodes(S-nodes) when needed, not only from the GW-node. In order to address security concerns in such a scenario, Das [5] presented a two-factor user authentication scheme using smart card and password. Two-factor authentication is an approach to authenticate someone which requires the presentation of two different kinds of authentication factors [6, 7]. In two-factor authentication, compromise of one authentication factor could not break the two-factor authentication. Hence, two-factor authentication schemes are more difficult to compromise. Das claimed his scheme can resist replay attack, stolen-verifier attack, guessing attack, and impersonation attack. However, Das's scheme is found to be insecure against various attacks. Nyang and Lee [8] demonstrated that Das's scheme is insecure against off-line dictionary attack, sensor node compromising attack, and does not protect query response messages. They also proposed an improved scheme to overcome the drawbacks of Das's schemes. Chen and Shih [9] showed that Das's scheme does not provide mutual authentication and proposed their improvement. He et al. [10] found that Das's scheme is vulnerable to the insider attack and the derived impersonation attack. Khan and Alghathbar [11] pointed out that Das's scheme is vulnerable to the GW-node bypassing attack and privileged insider attack, it does not provide methods to change users' passwords, and it does not achieve mutual authentication between the GW-node and the sensor node. Khan et al. also presented an improved scheme to overcome the security weaknesses of Das's scheme. Unfortunately, Sun et al. [12] showed that Khan and Alghathbar scheme still suffers from the GW-node impersonation attack, the GW-node bypassing attack, and the privileged insider attack. They proposed a new user authentication scheme which is proved to be secure under the security model of Bellare and Rogaway [13]. Very recently, Yuan [14] also found that in Khan and Alghathbar scheme, there is no provision of non-repudiation, it is susceptible to attack due to a lost smart card, and mutual authentication between the user and the GW-node does not attained. To fix these weaknesses, Yuan proposed an improved scheme using user's biometrics and proved the security of the new scheme by the GNY logic [15]. Yuan claimed his improvement contains several security features and is more secure.

In this paper, we demonstrate that the scheme proposed by Yuan has the following vulnerabilities; (1) The biometric keys are misused such that even a valid user cannot pass the biometric verification; (2) When a user's smart card is stolen, the adversary can personalize many registered users attack and impersonate the GW-node; (3) A malicious user can perform the GW-node impersonation attack using the information stored in his smart card; (4) No session key is established between the user and the sensor node, so the adversary can eavesdropping the real-time data transmitted in the insecure network. To fix the aforementioned weaknesses, we propose an improved two-factor authenticated key distribution scheme using fuzzy extractors [16]. Based on the security analysis and the performance evaluation, we believe that the proposed scheme is more secure and efficient than other related schemes.

The remainder of this paper is organized as follows. In Section 2, we briefly review Yuan's scheme. We demonstrate the vulnerabilities of this scheme in Section 3. In Section 4, our proposed scheme is described. The security of our scheme is analyzed in Section 5. We compare the efficiency and security features of our protocol with related schemes in Section 6. In Section 7, we conclude the paper with a brief summary and outline our future work.

2. Review of Yuan's scheme

In this section, we will briefly review Yuan's enhanced two-factor authentication scheme. For more details, refer to [14]. Some notations used throughout this paper are summarized in Table 1. Yuan's scheme is composed of three phases: the registration phase, the authentication phase and the password updating phase.

Table 1. Notations

Notation	Meaning	Notation	Meaning
GW	identity of the gateway node	ID_i	identity of the user U_i
$P W_i$	password of the user U_i	DID_i	dynamic login identity of the user U_i
S_n	identiy of a sensor node	K	secret key of the gateway node
$x_a; x_s$	secret parameters	$\oplus$	exclusive OR
$\|$	concatenation	$h(m)$	cryptographic hash of m
$BP ub$	the public key of the GW-node	$BP ri$	the secret key of the GW-node
$E_x\{M\}$	M is encrypted by x	$D_x\{M\}$	M is decrypted by x

2.1. Registration phase

In the registration phase, the user U_i inputs his personal biometrics M_i on the specific device, provides his identity ID_i and password $P W_i$ to the GW-node in a secure manner. On receiving the registration request, the GW-node computes $N_i = h(ID_i \| h(PW_i) \| E_i) \oplus h(K)$, where $E_i = h(M_i)$. The GW-node generates a smart card with parameters $ID_i; N_i; h(h(P W_i)); h(\cdot); E_i; x_a$, and sends the user's smart card to U_i through a secure channel.

2.2. Authentication phase

When the user U_i wants to access the real-time data from the WSN, the authentication phase is invoked. The steps involved are as follows:

Step A.1 The user U_i inserts his smart card into the card reader and in-puts M_i. The smart card computes $E_i^* = h(M_i)$ and checks whether $E_i^* = E_i$ or not. If the verification fails, the user's authentication request is terminated. Otherwise U_i also inputs ID_i and $P W_i$, the smart card verifies these two values with the stored ones in it. If the entered ID_i and $P W_i$ are correct, the smart card computes $DID_i = h(ID_i \| h(PW_i) \| E_i) \oplus h(x_a \| T)$, where T is the current timestamp of U_is‘ system. The smart card also computes $C_i = h(N_i \| x_a \| T)$ and sends *login-req* = $E_{BPub}\{DID_i; C_i; T\}$ to the GW-node.

Step A.2 Upon receiving *login-req* at time T^*, the GW-node decrypts the ciphertext by its private key $BPri$ and gets $(DID_i; C_i; T) = D_{BPri}\{login\text{-}req\}$. The GW-node first checks if $(T^* - T) \leq \Delta T$, where ΔT is the expected time interval for the transmission delay. If the verification is successful, the GW-node computes $N_i^* = (DID_i \oplus h(x_a \| T)) \oplus h(K)$ and $C_i^* = h(N_i^* \| x_a \| T)$. If $C_i \neq C_i^*$, the GW-node rejects the login request; otherwise the GW-node also computes $A_i = h(DID_i \| S_n \| x_s \| T_1)$, where S_n is some nearest sensor node that will respond to the query of U_i and T_1 is the current timestamp of the GW-node's system. Here x_s is a secret parameter shared between the GW-node and the sensor node S_n. Finally, the GW-node sends the message $(DID_i \| A_i \| T_1)$ to the sensor node S_n.

Step A.3 Upon receiving $(DID_i \| A_i \| T_1)$ at time T_2, the sensor node S_n checks if $(T_2 - T_1) \leq \Delta T$. If it holds, S_n computes $A^*_i = h(DID_i \| S_n \| x_s \| T_1)$ and checks whether $A^*_i = A_i$ or not. If the check if successful, S_n computes $B_i = h(S_n \| x_s \| T_3)$ and sends back the mutual authentication message $(B_i; T_3)$ to the GW-node, where T_3 is the current timestamp of the sensor node's system.

Step A.4 Upon receiving $(B_i; T_3)$ at time T_4, the GW-node checks if $(T_4 - T_3) \leq \Delta T$. If it holds, the GW-node computes $B_i^* = h(S_n \| x_s \| T_3)$ and checks whether $B_i^* = B_i$ or not. If it is true, the GW-node computes $F_i = h(h(K) \| x_a \| T_5)$ and sends the message $(F_i; T_5)$ to the user U_i.

Step A.5 Upon receiving $(F_i; T_5)$ at time T_6, the user U_i checks if $(T_6 - T_5) \leq \Delta T$. If it is true, the user U_i computes $h(K)^* = N_i \oplus h(ID_i \| h(P\ W_i) \| E_i)$, $F_i^* = h(h(K)^* \| x_a \| T_5)$, and checks whether $F_i^* = F_i$ or not. If it holds, the user trusts in the GW-node and enjoys the data from the WSN.

2.3. Password updating phase

The user U_i inserts his smart card into the card reader and inputs his biometric template M_i to verify his biometric. If U_i passes the biometric verification, he can input ID_i, the old password PW_i and the new password PW_i^*. The smart card validates ID_i and $P\ W_i$ with the stored values. If these two values are correct, the smart card computes $N_i^* = N_i \oplus h(ID_i \| h(PW_i) \| E_i) \oplus h(ID_i \| h(PW_i^*) \| E_i)$. The smart card then replaces $N_i, h(h(PW_i))$ with N_i^*, $h(h(PW_i^*))$.

3. Cryptanalysis of Yuan's Scheme

3.1. Misuse of biometrics

In Yuan's scheme, biometric keys are introduced to provide non-repudiation and resist the stolen smart card attack. More specifically, the user U_i inputs his biometric M_i to the GW-node in the registration phase. The GW-node computes $E_i = h(M_i)$ and stores E_i in U_i's smart card. In the authentication phase, the user U_i needs to input his biometric M_i again. The smart card computes $E_i^* = h(M_i)$ and checks whether $E_i^* = E_i$. If the verification is successful, further operations will be performed.

However, biometric keys are actually misused in Yuan's scheme. As is noted by [17], biometric matching is probabilistic in nature, which means that two samples of the same individual are never exactly the same. Unlike some pass-word systems that perform a one-way hash function on the user input, biometric systems cannot rely on the same process. The reason is that the hash values will never be the same for the reference template value and current presented sample. Instead, biometric authentication must tolerate failures within a reasonable bound. As a result, biometrics in the registration phase and the authentication phase of Yuan's scheme are not exactly the same. Yuan's scheme is incorrectly designed such that even the honest user cannot pass the biometric verification.

3.2. Stolen smart card attack

Yuan claimed his scheme can resist the stolen smart card attack. However, we find that Yuan's scheme is still insecure against the same attack if user's smart card is stolen.

If an adversary steals a smart card, he can perform the following two at-tacks. For one thing, the adversary can perform the many registered user attack without the GW-node's secrets. Firstly, the adversary extracts ID_i, N_i, $h(h(PW_i))$, E_i, and x_a from the smart card by side channel attacks [18, 19]. The adversary guesses the correct password PW_i via off-line dictionary attacks with the information $h(h(PW_i))$. Yuan stated that the adversary cannot obtain $h(P\ W_i)$ from $h(h(PW_i))$ because of the one-way characteristic of the hash function. However, this is actually incorrect. Because the adversary can iteratively guess a password $PW_i^{'}$ and verify whether $h(h(PW_i^{'})) = h(h(PW_i))$ or not until he finds out the correct password. The adversary then gets $h(K)$ by computing $N_i \oplus h(ID_i \| h(PW_i) \| E_i)$. Secondly, the adversary can generate a new smart card with parameters ID_i^*, $N_i^* = h(K) \oplus h(ID_i^* \| h(PW_i^*) \| E_i^*)$, $h(h(PW_i^*))$, $h(\cdot)$, E_i^*, and x_a, where ID_i^*, $P\ W_i^*$, and E_i^* are the identity, the password, and the bio-metric of the new user, respectively. It is obvious that the new smart card can pass user authentication of the WSN. The adversary can generate many valid smart cards in this way and employs them to access data from the network.

For another attack, the adversary can impersonate the victim user whose smart card is stolen, because the adversary can obtain the victim user's ID_i, $P\ W_i$, and E_i from the smart card. This attack demonstrates that Yuan's scheme does not achieve the two-factor security. Anyone could impersonate the user as long as he gets the user's smart card.

3.3. GW-node impersonation attack

In Yuan's scheme, It was claimed that mutual authentication between the user and the GW-node is achieved. Mutual authentication between the user and the GW-node means that nobody except the GW-node can authenticate himself to the user, and vise versa. However, we will show that a malicious user U_j can impersonate the GW-node to fool an honest user U_i. The malicious use U_j extracts the parameters N_j, x_a, and E_j from his smart card. U_j can compute $h(K) = N_j \oplus h(ID_j \| h(PW_j) \| E_j)$ using his identity ID_j and password PW_j. In order to impersonate the GW-node, after receiving the login request of the honest user U_i, the malicious user U_j simply waits for a while and send the message $(F_i; T_5)$ back to U_i, where $F_i = h(h(K)\|x_a\|T_5)$ and T_5 is the current timestamp of U_j. Moreover, the malicious user U_i can also perform the many registered user attack as described in section 3.2. Therefore, the GW-node impersonation attack is a serious security flaw in Yuan's scheme.

3.4. No session key is distributed between the user and the sensor node

In Yuan's scheme, the user can access the real-time data from the sensor node after login in. Unfortunately, no session key is shared between the user and the sensor node, which means the real-time data will be transmitted in plaintext. Therefore, the adversary can simply eavesdropping the real-time data from the insecure network. To ensure the confidentiality and integrity of the real-time data, a session key should be established between the user and the sensor node. Moreover, public key mechanism is used in Yuan's scheme to ensure that the first message comes from the user U_i. Considering power consumption and computation capacity, we should avoid using the public key mechanism in WSNs. As a result, Yuan's scheme is inefficiently designed to prove that the first message comes from U_i.

4. Our Proposed Scheme

In this section, we propose an improved user authentication scheme based on [14], which keeps the merits of the original scheme and can overcome the security weaknesses described in previous section. Our main technical tool is the fuzzy extractor [16]. Roughly speaking, a fuzzy extractor consists of two efficient algorithms *Gen* and *Rep*. The generation algorithm *Gen* takes the user's bio-metric M_i as input and outputs an extracted random string R_i and an auxiliary string P_i. The reproduction algorithm *Rep* takes as inputs the auxiliary string P_i and the user's biometric M_i*, and returns the random string R_i as long as the two biometric templates M_i and M_i* are close enough. We should note that R_i remains uniformly random even given the auxiliary string P_i. For more details, refer to [16, 20]. To avoid the GW-node impersonation attack and the GW-node bypassing attack, we require that the GW-node generates $x_n = h(S_n/\!/x_a)$ and writes it in the sensor node S_n before deploying the WSN, where x_n can be seen as S_n's secret. There are three phases in our improved scheme: the registration phase, the authentication phase and the password updating phase.

4.1. Registration phase

When registering with the GW-node, the user Ui inputs his biometric template Mi on the specific device. We assume this device extracts the biometric template and carries out the calculations in the fuzzy extractor. A pair $(Ri; Pi)$ is generated using Ui's biometric template Mi by the generation algorithm *Gen* in the fuzzy extractor. Ui computes $h(IDi\|Ri\|PWi)$ and sends the message $(IDi;\ h(IDi\|Ri\|P\ Wi))$ to the GW-node in a secure manner. On receiving the registration request, the GW-node computes $Vi = h(IDi\|K\|xa)$, $Ni = Vi \oplus h(IDi/\!/Ri/\!/P\ Wi)$ and $Hi = h(Vi)$. The GW-node generates a smart card with parameters IDi, Ni, Hi, $h(\cdot)$, and sends the user's smart card to Ui through a secure channel. Ui updates the data in the smart card by adding the auxiliary string Pi and the reproduction algorithm *Gen*.

4.2. Authentication phase

The authentication phase is invoked when U_i wants to access the real-time data from the WSN. The detailed steps of the authentication phase, as shown in Fig.1, are described as follows:

1. U_i inserts his smart card into the card reader, inputs his biometric M_i*, identity ID_i and password PW_i. The smart card computes R_i* using the re-production algorithm *Gen* with inputs M_i* and P_i. The smart card computes $V_i* = N_i \oplus h(ID_i\|R_i*\|PW_i)$ and checks whether $H_i = h(V_i*)$. If the verification is successful, the smart card computes $A_i = h(V_i*\|T_1)$ and sends the message $(ID_i; A_i; T_1)$ to the GW-node, where T_1 is the current timestamp of U_i's system.
2. Upon receiving the message $(ID_i; A_i; T_1)$ at time T_1*, the GW-node checks if $T_1*-T_1 \leq \varDelta T$, where $\varDelta T$ denotes the expected time interval for the transmis-sion delay. If it is true, the GW-node computes $A*_i = h(h(ID_i\|K\|x_a)\|T_1)$. If $A*_i = A_i$, the GW-node accepts the login request. The GW-node then chooses a random session key SK_i for the user and the sensor node S_n. The GW-node computes $K_{GW;n} = h(ID_i\|GW\ \|S_n\|x_n\|T_2)$ and $B_i = E_{KGW;n}\ \{ID_i\|GW\ \|S_n\|\ SK_i\|T_2\}$ using a symmetric encryption scheme, where T_2 is the current timestamp of the GW-node's system. Finally, the GW-node broadcasts the message $(ID_i; GW; S_n; B_i; T_2)$ to all the sensor nodes.
3. Upon receiving the message $(ID_i; GW; S_n; B_i; T_2)$ at time T_2*, the sensor node S_n checks if $T_2* - T_2 \leq \varDelta T$. If it is true, S_n computes $K_{GW;n} = h(ID_i/\!/GW\ /\!/S_n/\!/x_n/\!/T_2)$ and decrypts B_i. If ID_i, GW , S_n and T_2 from the de-crypted message are the same as received ones, S_n computes $C_i = h(ID_i/\!/GW\ /\!/S_n/\!/x_n/\!/SK_i/\!/T_3)$ and sends back the message $(S_n; C_i; T_3)$ to the GW-node, where T_3 is the current timestamp

of S_n's system. S_n also stores the session key SK_i for future communication.

4. Upon receiving the message (S_n; C_i; T_3) at time T_3*, the GW-node checks if $T_3^* - T_3 \le \Delta T$. If it is true, the GW-node computes $C_i^* = h(ID_i\|GW \|S_n\|x_n\| SK_i\|T_3)$ and checks if $C_i^* = C_i$. If the verification fails, the GW-node terminates the session. Otherwise, it computes $K_{GW;i} = h(ID_i\|GW //S_n//T_4//V_i)$ and $D_i = E_{K_{GW;i}}\{ID_i \|GW \|S_n\|SK_i\|T4\}$ using a symmetric encryption scheme, where $T4$ is the current timestamp of the GW-node's system. The GW-node sends the message (S_n; D_i; $T4$) to the user U_i.

5. Upon receiving the message (S_n; D_i; $T4$) at time $T4$*, U_i checks if $T4^* - T4 \le \Delta T$. If it is true, U_i also computes $K_{GW;i} = h(ID_i\|GW \|S_n\|T4\|V_i)$ and decrypts D_i. If ID_i, GW, S_n and $T4$ from the decrypted message are correct, U_i accepts the session and stores the session key SK_i for future communication.

Finally, U_i and S_n could use the common session key SK_i in upcoming private communication.

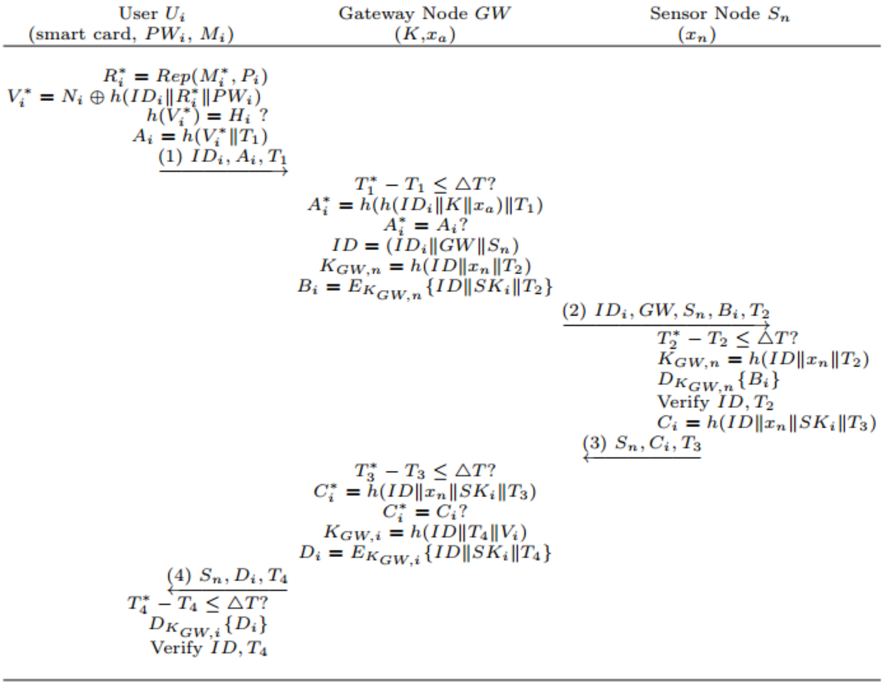
User U_i
(smart card, PW_i, M_i)
Gateway Node GW
(K, x_a)
Sensor Node S_n
(x_n)
$R_i^* = Rep(M_i^*, P_i)$
$V_i^* = N_i \oplus h(ID_i\|R_i^*\|PW_i)$
$h(V_i^*) = H_i$?
$A_i = h(V_i^*\|T_1)$
(1) ID_i, A_i, T_1
$T_1^* - T_1 \le \Delta T$?
$A_i^* = h(h(ID_i\|K\|x_a)\|T_1)$
$A_i^* = A_i$?
$ID = (ID_i\|GW\|S_n)$
$K_{GW,n} = h(ID\|x_n\|T_2)$
$B_i = E_{K_{GW,n}}\{ID\|SK_i\|T_2\}$
(2) ID_i, GW, S_n, B_i, T_2
$T_2^* - T_2 \le \Delta T$?
$K_{GW,n} = h(ID\|x_n\|T_2)$
$D_{K_{GW,n}}\{B_i\}$
Verify ID, T_2
$C_i = h(ID\|x_n\|SK_i\|T_3)$
(3) S_n, C_i, T_3
$T_3^* - T_3 \le \Delta T$?
$C_i^* = h(ID\|x_n\|SK_i\|T_3)$
$C_i^* = C_i$?
$K_{GW,i} = h(ID\|T_4\|V_i)$
$D_i = E_{K_{GW,i}}\{ID\|SK_i\|T_4\}$
(4) S_n, D_i, T_4
$T_4^* - T_4 \le \Delta T$?
$D_{K_{GW,i}}\{D_i\}$
Verify ID, T_4

Figure 1. Authentication phase of the proposed scheme

4.3. Password updating phase

This phase is invoked whenever U_i wants to change his password $P\ W_i$ with a new one, say $P\ W_i^*$. U_i inserts his smart card into the terminal and inputs his identity ID_i, the biometric M_i', the old password PW_i and the new password PW_i^*. The smart card computes R_i^* using the reproduction algorithm Rep with inputs M_i' and P_i. The smart card then computes $V_i^* = N_i \oplus h(ID_i//R_i^*//PW_i)$, $H_i^* = h(V_i^*)$ and checks whether $H_i = H_i^*$. If the verification is successful, the smart card computes $N_i^* = N_i \oplus h(ID_i\|R_i^*\|PW_i) \oplus h(ID_i\|R_i^*\|PW_i^*)$ and replaces N_i with N_i^*.

5. Security Analysis

In this section, we analyze the security of the proposed scheme. The advantages of the proposed scheme are explained as follows.

Resistance to the replay attack. A replay attack (replaying an intercepted message) cannot work in our scheme due to the timestamp in each message. Suppose the intruder intercepts a valid login request (ID_i; A_i; T_1) and tries to login to the GW-node by replaying the same. The verification of this login request fails because of the interval $T_1^* - T_1 > \Delta T$, where T_1^* is the GW-node's system time while receiving the replayed message.

Resistance to the privileged insider attack. Consider the privileged insider attack [11]. If a malicious privileged insider of the GW-node knows the pass-words of the registered users, the GW-node can impersonate the users to access other servers because many users use same passwords to access different applications for their convenience. In the proposed scheme, the GW-node only knows $h(ID_i\|R_i\|PW_i)$ and cannot get the user's password without the knowledge of R_i. R_i can only be computed using the user's biometric template and P_i. The GW-node can neither get a valid biometric template of the user nor know P_i, so the proposed scheme can resist the privileged insider attack.

Resistance to the GW-node impersonation attack. If a malicious user U_j wants to impersonate the GW-node to another honest user U_i, U_j needs to compute $V_i = h(ID_i \| K \| x_a)$. However, U_j can only extract $V_j = h(ID_j \| K \| x_a)$ from his smart card. To compute V_i, U_j needs to get K and x_a from V_j, but this is unlikely because K and x_a are high-entropy secret keys. So a malicious user cannot impersonate the GW-node in the proposed scheme.

Resistance to the stolen verifier attack. An adversary can attack any system which has verifier tables for authentication, but in our proposed scheme, the GW-node does not store any verification table at all. As a result, the proposed scheme can resist the stolen-verifier attack.

Resistance to the stolen smart card attack. If the user U_i's smart card is stolen, the adversary can extract the parameters ID_i, N_i, H_i and P_i from the smart card. However, the adversary still cannot impersonate the user. In order to impersonate the user, the adversary needs to compute V_i from N_i, which in turn needs to compute $h(ID_i /\!/ R_i /\!/ PW_i)$. However, the adversary does not know $P\ W_i$ and R_i from the parameters extracted from the smart card. What is more, it is obvious that the adversary cannot impersonate the GW-node or the sensor node in this situation.

Resistance to the off-line dictionary attack. In the proposed scheme, the user's password PW_i is combined with the secret value R_i. R_i is a random high-entropy random value which can only be computed using P_i and the user's valid biometric templates. So our protocol can resist the off-line dictionary attack performed by the GW-node or other insider users. The only exception is when the adversary gets the user's smart card and a valid biometric template, the adversary can guess the correct password by an off-line dictionary attack in this case. We will comment on such a situation later.

Resistance to the compromised sensor node attack. If the sensor node S_n is compromised in our scheme, the adversary knows S_n's secret key $x_n = h(S_n \| x_a)$. It is obvious that the adversary can impersonate S_n since S_n is compromised. However, the adversary cannot impersonate any other sensor node in the WSN because the secret keys of the sensor nodes are different. And due to the high entropy of x_a, the adversary cannot extract x_a from $h(S_n \| x_a)$.

Mutual authentication. In the proposed scheme, after receiving the first message, the GW-node can verify the authenticity of the user by checking whether $A^*_i = A_i$. The user can verify the authenticity of the GW-node by checking whether ID_i, GW, S_n and T_4 from the decrypted message are correct. So our scheme achieves mutual authentication between the user and the GW-node. With a similar analysis, we can see that our scheme also provides mutual authentication between the GW-node and the sensor node.

Session key distribution. A user authentication scheme in WSN will be followed by the delivery of the real-time data. The user and the sensor node should have a common session key to protect the confidentiality and integration of the data. In the proposed scheme, a session key SK_i is distributed between the user and the sensor node with the help of the GW-node. The GW-node serves as a key distribution center and distributes a unique secure session key to the user and the sensor node. The user and the sensor node can communicate in a secure and authentic way with the session key SK_i.

Comment In the proposed scheme, the user uses the password, the smart card and the biometric template to authenticate himself to the GW-node. So our scheme is basically a multi-factor authentication scheme. A multi-factor authentication scheme is designed to remain secure even if all but one of the factors has been compromised. We can see that if the password and the biometric template are compromised, the adversary cannot impersonate the user because he does not know the parameters stored in user's smart card. If the password and the smart card are compromised, the adversary still cannot impersonate the user because he cannot compute R_i in the fuzzy extractor without the user's valid biometric template. However, when the biometric template and the smart card are compromised, the adversary can guess the correct password via an off-line dictionary attack. More specifically, the adversary can compute the correct $R_i = Rep(M_i; P_i)$ with the valid biometric template. Then he can guess a password $P\ W_i{}^*$ and computes $V_i{}^* = N_i \oplus h(ID_i \| R_i \| PW_i{}^*)$. If $h(V_i{}^*)$ is equal to H_i, then the correct password is obtained. Otherwise, the adversary can guess another password and repeat the above steps until the correct password is found. As is noted in [12], it is still an open problem whether there exists a secure smart-card based user authentication scheme merely by using symmetric key techniques when all security factors are compromised except the password. Moreover, the above attack is not considered as a serious security flaw from a practical point of view. The reason is as follows. First, even if the adversary compromises the smartcard and the user's biometric, he still needs to perform an off-line dictionary attack to guess the correct password, which requires a lot of time and computing resources. Second, the adversary can only impersonate the user to the GW-node after guessing the correct password. The adversary cannot perform the many registered user attack as described in [14]. Last but not least, it needs more effort for the adversary to steal the smart card and get a valid biometric template simultaneously. So our scheme can provide an enhanced level of assurance in higher-security scenarios.

6. Performance Analysis

In this section, we compare security features and efficiency of the proposed protocol with related schemes [5, 8, 10–12, 14]. Table 2 presents the comparison of computation cost and communication cost of the proposed scheme and other schemes. With respect to computation, we only consider some expensive types of computation. Let "H" denote the computation cost of one hash operation, "T_{pub}" denote the computation cost of one public key operation, "T_{sym}" denote the computation cost of one symmetric key encryption/decryption. The computation cost of an efficient fuzzy extractor [20] is no more than the cost of one hash operation. For simplicity, we use the cost of one hash operation to represent the computation cost of the algorithms of *Gen* and *Rep* in the fuzzy extractor. With respect to bandwidth, we assume that the identifications can be represented with 32 bits, the output size of secure hash functions. Nonces is 160 bits, the timestamp can be represented with 64 bits. The ciphertext is the same size with the plaintext in symmetric encryptions, and the size of the ciphtext is usually doubled in public key encryptions.

We can see from Table 2 that the computation costs of the registration phase and the password updating phase are more or less the same. The registration/password updating phase is a one-time job for some period of time, so we focus on the computation cost of the authentication phase. Our scheme needs 11 hash operations and 4 symmetric encryption/decryption operations in the authentication phase. The symmetric encryption/decryption operations arise from the distribution of the session key. Among the related schemes [5, 8, 10–12, 14], only Nyang and Lee's scheme [8] establishes the session key for the user and the sensor node. Our scheme is more efficient than Nyang and Lee's scheme. In terms of hash operations, our protocol is slightly less efficient than Das's scheme [5] and Sun et al.'s scheme [12]. However, Das's scheme is insecure against several attacks. Although Sun et al.'s scheme is quite efficient in computation and provides strong

Table 2. Comparisons of efficiency

	The proposed scheme	Das's scheme [5]	N-L-scheme [8]	H-G-C-scheme [10]	K-A-scheme [11]	S-L-F-scheme [12]	Yuan's scheme [14]
E1	2H	0	0	H	H	0	0
E2	2H	3H	3H	5H	2H	2H	5H
E3	4H+Tsym	4H	7H+Tsym	5H	4H	2H	8H+Tpub
E4	5H+2Tsym	4H	8H+Tsym	5H	5H	5H	8H+Tpub
E5	2H+Tsym	H	4H+2Tsym	H	2H	2H	2H
E6	4H	N/A	N/A	6H	4H	2H	6H
E7	1344bits	832bits	1344bits	928bits	992bits	1056bits	1600bits
E8	4	3	3	3	3	8	4

E1: Computation cost of the registration phase for a user
E2: Computation cost of the registration phase for a GW-node
E3: Computation cost of the authentication phase for a user
E4: Computation cost of the authentication phase for a GW-node
E5: Computation cost of the authentication phase for a sensor node
E6: Computation cost of the password updating phase for a user
E7: Bandwidth of the authentication phase
E8: Message flows of the authentication phase
N/A:Not Available

Table 3. Comparisons of security features

	The proposed scheme	Das's scheme [5]	N-L-scheme [8]	H-G-C-scheme [10]	K-A-scheme [11]	S-L-F-scheme [12]	Yuan's scheme [14]
C1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C2	Yes	No	No	Yes	No	Yes	No
C3	Yes	No	No	Yes	No	Yes	No
C4	Yes	Yes	Yes	Yes	Yes	Yes	Yes
C5	Yes	No	No	No	No	No	No
C6	Yes	No	Yes	Yes	Yes	Yes	Yes
C7	Yes	No	No	No	No	Yes	Yes
C8	Yes	No	No	No	No	Yes	Yes
C9	Yes	No	Yes	No	No	No	No

C1: Resist the replay attack
C4: Resist the stolen verifier attack
C7: Resist the compromised sensor node attack
C2: Resist the privileged insider attack
C5: Resist the stolen smart card attack
C8: Mutual authentication
C3: Resist the GW-node impersonation attack
C6: Resist the off-line dictionary attack
C9: Session key distribution

security, it needs 8 message flows. In wireless sensor networks, transmitting radio signals on resource-constrained wireless devices usually consumes much more power than computation does, so it is more important to reduce the number of message flows than the computation cost. Sun et al.'s scheme has high communication complexity and is not suitable for WSNs. With respect to communication complexity, our scheme needs more bandwidth than schemes [5, 10–12]. The rea-son is still because a session key is distributed in our scheme. The bandwidth is increased due to the transmission of the common session key. Our scheme needs 4 message flows, this is the least number of message flows to achieve mutual authentication among the user, the GW-node and the sensor node.

Table 3 summarizes security features of the proposed protocol with related schemes [5, 8, 10–12, 14]. We can see from Table 3 that our scheme provides more security features than other related schemes. Our scheme is an improvement of Yuan's scheme. It is not only more secure but also more efficient than Yuan's scheme. It is worth noting that our scheme is the only one scheme which can resist the stolen smart card attack.

Considering the computation cost, communication cost and security features as a whole, only Sun et al.'s scheme [12] is comparable to our scheme. However, Sun et al.'s scheme is insecure against the stolen smart card attack and does not distribute session key for the user and the sensor node. What is more, Sun et al.'s scheme has high communication complexity to achieve provable security. Therefore, our scheme is more secure than related scheme while preserving high efficiency. As a result, the proposed scheme is more suitable for real-life applications in WSNs.

7. Conclusions and future work

In this paper, we have analyzed the security weaknesses of a recently proposed two-factor user authentication protocol by Yuan for WSNs. We show that Yuan's scheme is susceptible to the stolen smart card attack and the GW-node impersonation attack. Moreover, the biometrics are misused and no session key is established in Yuan's scheme. We also propose an improved scheme to defeat the attacks. The proposed scheme not only preservers the merits of Yuan's scheme but also fixes its security flaws. The security and performance comparison shows that our protocol achieves both higher efficiency and stronger security. Therefore, we believe the proposed scheme is more suitable for applications in WSNs.

Until now, there is no formal security model to prove the security of the two-factor user authentication schemes in WSNs. This is the reason why several two-factor user authentication schemes are insecure against various attacks. Our future work will focus on summarizing the security requirements of the two-factor user authentication schemes in WSNs and presenting a formal security model to evaluate the security of these schemes.

Acknowledgment

The authors would like to thank the anonymous referees for their helpful comments. This study was funded by the National High Technology Research and Development Program (863 Program) (No. 2015AA011704), the National Natural Science Foundation of China (Nos. 61309016, 61379150, 61501515), Postdoctoral Science Foundation of China (No. 2014M562493), Postdoctoral Science Foundation of Shanxi Province, Fundamental Research Funds for the Central Universities (Program No. JB140302), and Key Scientic Technological Project of Henan Province (No. 122102210126,092101210502).

References

[1] **S. Xie, Y. Wang.** Construction of tree network with limited delivery latency in homogeneous wireless sensor networks. *Wireless Personal Communications*, 2014, Vol. 78, No. 1, 231-246.

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

[3] **D. He, S. Zeadally**. Authentication protocol for ambient assisted living system. *IEEE Communications Magazine*, 2015, Vol. 53, No. 1, 71-77.

[4] **P. Guo, J. Wang, B. Li, S. Lee.** A variable threshold-value authentication architecture for wireless mesh networks. *Journal of Internet Technology*, 2014, Vol. 15, No. 6, 929-936.

[5] **M. L. Das.** Two-factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 2009, Vol. 8, No. 3, 1086-1090.

[6] **D. He, D. Wang**. Robust biometrics-based authentication scheme for multi-server environment. *IEEE Systems Journal*, 2015, Vol. 9, No. 3, 816-823.

[7] **D. He, N. Kumar, J.-H. Lee, R. S. Sherratt**. Enhanced three-factor security protocol for mass consumer storage devices. *IEEE Transactions on Consumer Electronics*, 2014, Vol. 60, No. 1, 30-37.

[8] **D. H. Nyang, M. K. Lee**. Improvement of Das's two-factor authentication protocol in wireless sensor networks. Cryptology, ePrint archive, 2009. http://eprint.iacr.org/2009/631.pdf. Accessed 28 February 2010.

[9] **T. H. Chen, W. K. Shih**. A robust mutual authentication protocol for wireless sensor networks. *ETRI Journal*, 2010, Vol. 32, No. 5, 704-712.

[10] **D. J. He, Y. Gao, S. Chan**, **C. Chen, J. Bu**. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc & Sensor Wireless Networks, 2010, Vol. 10, No. 4, 361-371.

[11] **M. K. Khan, K. Alghathbar**. Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. *Sensors*, 2010, Vol. 10, No. 3, 2450-2459.

[12] **D. Z. Sun, J. X. Li, Z. Y. Feng, Z. F. Cao, G. Q. Xu.** On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. *Personal and Ubiquitous Computing*, 2013, Vol. 17, No. 5, 895-905.

[13] **M. Bellare, P. Rogaway**. Entity authentication and key distribution. In: *Proceedings of 13th Annual International Cryptology Conference: Advances in Cryptology-Crypto'93*, 2013, Springer-Verlag, Berlin, Germany, LNCS 773, pp. 232-249.

[14] **J. J. Yuan**. An enhanced two-factor user authentication in wireless sensor networks. *Telecommunication Systems*, 2014, Vol. 55, No. 1, 105-113.

[15] **L. Gong, R. Needham, R. Yahalom**. Reasoning about belief in cryptographic protocols. In: *Proceedings of 1990 IEEE Computer Society Symposium Research in Security and Privacy*, 1990, pp. 234-246.

[16] **Y. Dodis, L. Reyzin, A. Smith.** Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: *Proceedings of International Europe Cryptology Conference: Advances in Cryptology-Eurocrypto'04*, 2004, Springer-Verlag, Berlin, Germany, LNCS 3027, pp. 523-540.

[17] **A. Bhargav-Spantrel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino, S. J. Elliott**. Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, 2007, Vol. 15, No.5, 529-560.

[18] **T. S. Messerges, E. A. Dabbish, R. H. Sloan**. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 2002, Vol. 51, No. 5, 541-552.

[19] **P. Kocher, J. Jaffe, B. Jun**. Differential power analysis. In: *Proceedings of 19th Annual International Cryptology Conference: Advances in Cryptology-CRYPTO'99*, 1999, Springer-Verlag, Berlin, Germany, LNCS 1666, pp. 388-397.

[20] **Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, A. Smith**. Robust fuzzy extractors and authenticated key agreement from close secrets. *IEEE Transactions on Information Theory*, 2012, Vol. 58, No. 9, 6207-6222.

Received April 2015.