A new three-factor authentication scheme overcome repeat registered attack for wireless sensor networks

Ye Li, and *Min* Zhang*

School of Foreign languages, Southwest Minzu University, China, 610066

Keywords: Wireless sensor networks (WSNs), Authentication, repeat registered attack, Proverif.

Abstract. In the wireless sensor networks (WSNs), users sometimes need to access real-time information from a certain sensor node. In order to prevent unauthorized users from acquiring information from the sensor node, a lot of authentication schemes suited for the WSNs condition have been proposed. Recently, Das has proposed a secure and light-weight authentication scheme for the WSNs based on three factors, claiming that it can withstand various attacks. But after a careful analysis, there are still several security problems as follows: a) The scheme has some design flaws; b)The scheme may suffer sensor node impersonation attack; c) The scheme may suffer repeat registered attack; d) When the user access the sensor node, the scheme cannot protect the identity information of the sensor node. To solve these problems, a new scheme using the secure sketch algorithm is presented in this paper. The security of improved scheme has been analyzed by ProVerif. Thorough analysis shows that the presented scheme can provide stronger security and slight lower computation at client than Das's protocol. What's more, it can overcome repeat registered attack and achieve sensor node's identity anonymity protection.

1 Introduction

The wireless sensor networks (WSNs) are usually deployed in harsh enviroment, such as in enemy positions or other unsafe environments. At the same time, WSNs have a lot of nature attributes, such as limited data processing ability, limited storage capacity, limited bandwidth, limited energy, and other limited factors. As the two important fields in WSNs, the sensor nodes are deployed randomly in a target field while the BS(Base Station) collects the information of all sensor nodes and manages WSNs or performs costly operation. The sensor node is insecure whereas BS is secure. Usually, If a user wants to acquire information from the sensor node without real-time requirements, he/she must communicate with the BS in order to acquire data from the sensor node. In the military or healthcare applications, the authorized user needs to access the real-time information directly from sensor nodes without the BS participation. The details are shown as figure 1.

* Corresponding author: cdcszhangmin@126.com

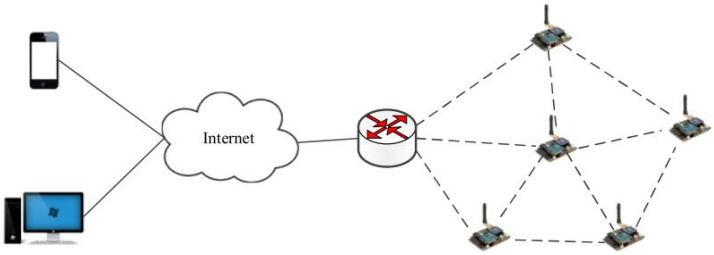

Fig. 1. The Real-time Access Method.

In order to ensure that unauthorized users cannot join the network or acquire any valuable information, a friendly and reliable authentication machanism becomes necessary. In 2009, Das [1] proposed a novel two-factor authentication scheme based on the smart card and the password for WSNs. This scheme has a lot of advantages, for example the base station (BS) need not to maintain a database for storing users' identities or passwords. Besides, a lot of new authentication schemes later proposed have been based on his scheme. Under some stringent assumptions just like the information stored in sensor nodes cannot be acquired or modified. Das's scheme can resist common attacks such as guessing attack, replaying attack, stealing verifier attack and so on. However, Nyang-Lee[2] pointed out Das's scheme[1] could not resist offline password guessing attack and node capture attack. In order to solve these problems, they proposed a new scheme [2] which can not only achieve secure communication between user and SN but also resist password guessing attack. Unfortunately, Nyang-Lee's scheme cannot resist denial of service (Dos). In 2010, He et al. [3] pointed out Das's scheme had both advantages such as light-weighted computation, resistance to various attacks . At the same time, the scheme has some disadvantages also which involve possible insider attack and impersonation attack. In order to exploit its strong points and avoid its weakness, He et al.[3] proposed an improved scheme. In 2011, Kumar-Lee [4] pointed out He et al.'s scheme could not achieve mutual authentication and session key establishment between the user and the sensor node. From the analysis in Kumar-Lee's scheme, we can see that He et al.'s scheme cannot achieve user anonymity. In 2012, Yoo et al. [5] proposed an efficient two-factor authentication scheme. However, this scheme could not protect user's privacy [6]. In 2013, Sun et al.[7] proposed a robust two-factor user authentication scheme. However, the analysis in [6] shows that Sun et al.'s scheme cannot achieve user privacy protection, mutual authentication and session key agreement. In 2013, Xue et al. proposed a light-weight scheme based on temporal credential. However, from Jiang et al.'s scheme [6] we can see that Xue et al.'s scheme is vulnerable to identity guessing attack, tracking attack, smart card lost attack and privileged-insider attack. For solving these problems, Jiang et al. proposed a two-factor user authentication scheme for WSNs. Owing to the attractive advantages in biometric, a lot of biometric-based or three-factor user authentication schemes for WSNs have been proposed [8-12]. In 2014, Das proposed three-factor authentication scheme [8] and pointed out that there are several drawbacks. For example, Jiang et al.'s scheme may suffer insider attack and be hard to use. In 2013, Althobaiti et al. [10] proposed an authentication scheme for WSNs based on biometrics. Althobaiti et al.'s scheme is efficient in computation. However, Das[11] pointed out that Althobaiti et al.'s scheme could not resist node capture attack, impersonation attack and man-in-the-middle attack. Recently, Das proposed a secure and efficient three-factor authentication protocol for the WSNs[12] in January of 2015.This scheme has a lot of advantages such as light-weight. However, with a careful research, we also find quite a few problems in his scheme. In order to solve these problems in Das's scheme[12], a new three-factor authentication scheme for the WSNs is proposed in this paper.

2 The weaknesses of the das's scheme

There are some advantages in the Das's scheme just like light-weight and dealing with biometric reasonably. However, the scheme needs to be improved after our careful analysis. In this section, we present four flaws in the Das's protocol. The details of these attacks are shown as follows. The scheme has some design flaws: 1） In the authentication and key agreement phase of Das's scheme, the BS cannot get the value of M_4 by computing $h(ID_i \| X_s)$ because the BS cannot obtain the information of ID_i . Firstly, ID_i cann't be sent to the BS and the BS doesn't store ID_i also during the authentication and key agreement phase. From the analysis, we can see that the scheme proposed by Das is not effective. 2） The scheme is vulnerable to sensor node impersonation attack: It is generally known that all the sensor nodes are not equipped with tamper resistant hardware. The attacker can acquire all the information stored in sensor node by side channel attack. In the Das's scheme, the sensor node SN_j stores its master key MK_{SN_j} in the memory. What's worse, the data transferred between the BS and the sensor nodes are encrypted by the key MK_{SN_j}. If an attacker acquires the master key MK_{SN_j} of the sensor node by side channel attack, he can acquire or modify the information transferring between the BS and SN_j. What's worse, the attacker can communicate with the BS by disguising himself as an authorized sensor node. 3）The Scheme may Suffer Repeat Registered Attack: If one attacker acquires the identity ID_i of one user, he can register for the BS though the same ID_i and then get the information $h(ID_i \| X_s)$. In the login phase of the Das's scheme, the attacker can acquire the data of RN_{U_i} also and then he can compute M_3. At the same time, the attacker can get RN_{SN_j} from M_9 . At last, the attacker can compute session key $SK_{ij} = h(ID_i \| ID_{Sn_j} \| h(M_4) \| M_5 \| RN_{SN_j} \| T_1 \| T_5)$. From the analysis, we can see that the session key may be revealed by attacker. 4）The Scheme cannot Achieve the Identity of Sensor Node Anonymously: Sometimes, the identity that which sensor node is being visited may leak important information especially in military and healthcare applications. So the proposed scheme must protect the identity of sensor nodes which the user needs to access. In the Das's scheme, the user sends $< ID_{SN_j}, M_2, M_3, T_1 >$ without protecting the ID_{SN_j} via public channel.

3 The proposed scheme

In this section, a new scheme based on secure sketch is proposed to overcome the problems of the Das's scheme. There are five phases in this scheme: a) initialization, b) registration, c) login and authentication, d) password change and biometric update phase, e) dynamic node addition phase. In order to describe and analyze our scheme better, we use as possible same as notations used in the Das's scheme. We introduce the notations in Table 1.

3.1 Initialization Phase

In this phase, there are some necessary preparatory works as following steps:1)The BS generates Kpub_key and Kpri_key by the public key algorithm such as ECC (Elliptic Curve Cryptography). 2)The BS generates a 1024-bit random master key Xs. The BS must assure the value of Kpri_key and Xs absolute safety. 3)The BS assigns a unique identity IDSNj for

each deployed sensor; 4) The BS writes IDSNj and Kpub_key into the memory of each deployed sensor node. 5)Then, SNj can be deployed in the target field according to the steps in the reference [13].

Table 1 Notations used in the proposed paper

Symbol	Description
N	A random nonce generated by U_i in the registration phase
pw_i	Password of user U_i
PW_i	The security and cancelable template of password
S	The help data generated by the secure sketch theory;
B_i^{reg}, B_i^{aut}, B_i^{pwd}	The biometric of the user at the registration/ authentication / password change phase
K_{pub_key}, K_{pri_key}	The public key/ private key of the BS
$E_{pub\_k}(M)$	Asymmetric encryption of M using the public key pub_k
$D_{pri\_k}(M)$	Asymmetric decryption of M using the private key pri_k
$S=SS(B_i^{reg})$	Generates help data S from B_i^{reg} by secure sketch algorithm[15]
$B_i^{reg}=Rec(S, B_i^{aut})$	Recover B_i^{reg} from S and B_i^{aut} if only the value of B_i^{aut} is close to B_i^{reg}.

3.2 Registration phase

If U_i wants to become a legal user in WSNs, he must register with the BS according to the following steps: 1) U_i provides his/her identity IDi, password pwi, and biometric B_i^{reg} . At the same time, U_i generates a random number N;2) U_i gets help data S by computing $S=SS(B_i^{reg})$ and gets the current time t_{reg} ;3) U_i acquires the cancelable password template PW_i by computing $PW_i = h(\mathrm{pw}_i \| \mathrm{N} \| \mathrm{B}_i^{reg})$, and sends the registration information $< PW_i, ID_i, T_{reg} >$ to the BS via a secure channel;4)After receiving the requesting information from Ui, the BS checks the validity of T_{reg} by computing $T_{current} - T_{reg} > \Delta t$. During the time interval Δt, different users cannot be allowed to register using the same identity. Then, the BS computes $r_i = h(\mathrm{ID}_i \| \mathrm{X}_s \| t_{reg})$ and $M_1 = \mathrm{ID}_i \oplus h(\mathrm{X}_s \| t_{reg})$, $M_2 = PW_i \oplus r_i$. At the same time, the BS writes $M_1, M_2 h(.)$ into smart card and sends it to Ui . Emphatically the user can select his identity freely whereas the BS cannot permit the same identity selected by different persons during the time interval Δt. 5) After receiving the smart card from the BS, Ui writes $h(PW_i), \mathrm{S}, \mathrm{SS}(.), N, t_{reg}$ into smart card. Then, he can finish the registration phase. From above analyses, smart card contains the following information $h(PW_i), h(.), M_1, M_2, \mathrm{S}, \mathrm{SS}(.), N, t_{reg}$. The summary of the registration phase is given in Figure 2.

3.3 Login and authentication phase

In this phase, if one registered user wants to acquire real-time data from any sensor nodes inside WSNs, he must execute the following steps: 1),User provides $ID_i, PW_i^{aut}, B_i^{aut}$; 2)Smart card computes: $B_i^{reg} = \mathrm{Re}c(B_i^{aut}, S)$, $PW_i^{aut} = h(\mathrm{pw}_i^{aut} \| \mathrm{N} \| \mathrm{B}_i^{reg})$, then executes $h(pw_i^{aut}) ? = h(PW_i)$. If the result doesn't hold, this phase is terminated. 3) Smart card computes $r_i = PW_i^{aut} \oplus M_2$ and generates a random number RN_{U_i} . Then smart card

computes $M_3 = RN_{U_i} \oplus r_i$, $M_4 = h(\mathrm{ID}_i \| \mathrm{ID}_{SN_J} \| \mathrm{r}_i \| \mathrm{RN}_{U_i})$, $M_5 = h(\mathrm{ID}_i \| \mathrm{RN}_{U_i}) \oplus \mathrm{ID}_{SN_j}$. The Ui sends $< M_1, M_3, M_4, M_5, t_{reg} >$ to the BS. 4)After receiving $< M_1, M_3, M_4, M_5, t_{reg} >$, the BS executes the following steps: $ID_i = M_1 \oplus h(x_s \| t_{reg})$, $r_i = h(ID_i \| x_s \| t_{reg})$, $RN_{U_i} = M_3 \oplus r_i$, $ID_{Sn_j} = M_5 \oplus h(ID_i \| RN_{U_i})$. Then the BS computes $M_4 = h(\mathrm{ID}_i \| \mathrm{ID}_{SN_J} \| \mathrm{r}_i \| \mathrm{RN}_{U_i})$ again and verifies $M_4 ? = M_4$; 5)If the iv step holds, the BS generates RNBS, and computes $M_6 = h(RN_{U_i} \| ID_i), M_7 = r_i \oplus RN_{BS}$ .The session key between the BS and Ui is $K_{U\_B} = h(RN_{U_i} \| RN_{BS})$. At the same time, the BS sends h(.) and access request to SNj. 6)After receiving instruction from the BS, SNj generates RNSNj and computes $K_{U\_B} = h(ID_{SN_j} \| RN_{BSj})$ as session key between Ui . Then, SNj encrypts K_{U_B} by computing $\mathrm{info} = \mathrm{E}_{key\_pub}(K_{U\_S})$ and sends info to the BS. 7) After receiving info from SNj, the BS gets K_{U_S} by decrypting $\mathrm{info} = \mathrm{E}_{key\_pub}(K_{U\_S})$ using its private key *key_pri* . Then, the BS encrypts K_{U_S} by $E_{K_{U\_S}}(K_{U\_S})$. At last, the BS sends $E_{K_{U\_S}}(K_{U\_S}), M_6, M_7$ to the user Ui. 8)After receiving $< E_{K_{U\_B}}(K_{U\_S}), M_6, M_7 >$ from the BS. Ui computes $M_6^* = h(\mathrm{RN}_{u_i} \| \mathrm{ID}_i)$ and verifies $M_6 ? = M_6^*$. If the result holds, Ui computes , $r_i = M_2 \oplus PW_i$ $RN_{BS} = M_7 \oplus r_i$, $K_{U\_B} = h(RN_{BS} \| RN_{U_i})$, $K_{U\_S} = D_{KU\_B}(\mathrm{E}_{K_{U\_B}}(K_{U\_S}))$. Then, Ui can communicate with SNj by encrypting information with the key K_{U_S} . The details are shown in Figure 3.

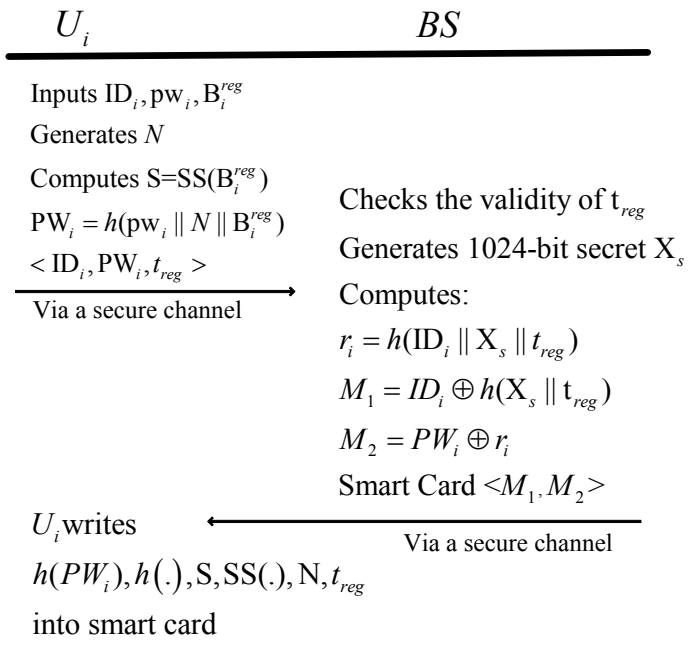

Fig. 2. The registration phase.

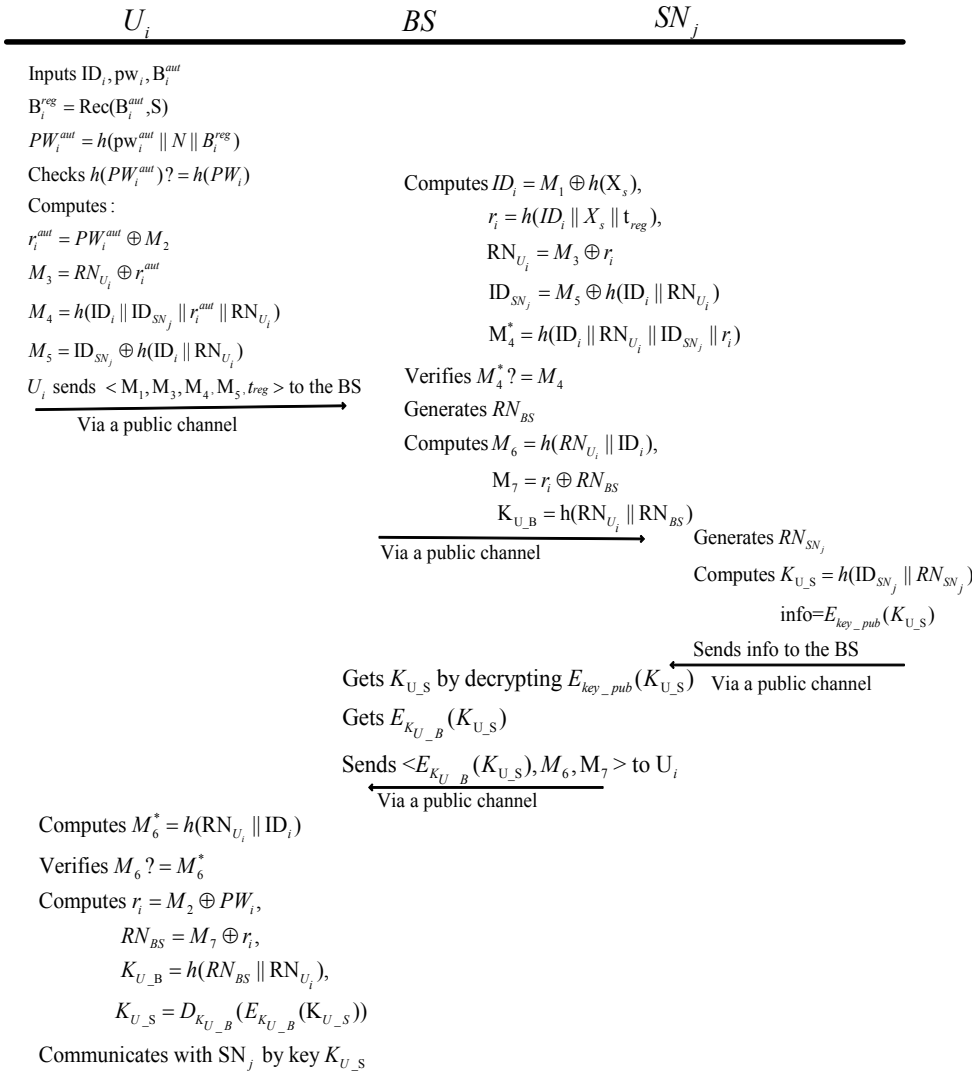

Fig.3. The login and authentication phase.

3.4 Password and biometric update phase

Sometimes, user needs to change his password or biometric in WSNs. In our scheme, user can alter his password or biometric arbitrarily without contacting the BS. This phase involves the following steps:1) Ui provides his/her old password pw_i^{old}, new biometric B_i^{new} and identity ID_i; 2)Then smart card computes: $B_i^{new} = \mathrm{Re}c(B_i^{new}, S)$, $pw_i^{old} = h(pw_i^{old} \| N \| B_i^{reg})$ and verifies $h(pw_i^{old})? = h(pw_i)$. 3)If the result holds, Ui inputs new password pw_i^{new} and computes $pw_i^{old} = h(pw_i^{old} \| N \| B_i^{reg})$, $S^{new} = SS(B_i^{new})$, $h(pw_i^{new})$. 4)Then smart card computes $M_2^{new} = M_2 \oplus pw_i^{old} \oplus pw_i^{new}$, and replaces M_2, $h(pw_i), S$ with $M_2^{new}, h(pw_i^{new}), S^{new}$ respectively.

4 Security analysis of the proposed scheme

4.1 Formal security validation using ProVerif

In this section, we prove the security of our proposed scheme using ProVerif which is automated formal tool. ProVerif is based on applied calculus and can be used to verify authentication and secrecy properties. There are three parts in the ProVerif : (1) declaration part; (2) process part; (3) main part. The ProVerif code for the definition of functions, reduction, equation, free names and constants is as follows. We perform the above process in the online demo for ProVerif (http://proverif.rocq.inria.fr/index.php). The performance results as shown in the Fig 4. From the experimental results, we can see that our proposed scheme is security.

```
The HTML output is kept for at least 30 minutes. It is kept much longer if there is enough free space. You can
obviously save the web pages if you want to keep them.
ProVerif text output:

Completing equations...
Completing equations...
-- Query inj-event(EndUser(id)) ==> inj-event(BeginUser(id))
Completing...
Starting query inj-event(EndUser(id)) ==> inj-event(BeginUser(id))
RESULT inj-event(EndUser(id)) ==> inj-event(BeginUser(id)) is true.
-- Query not attacker(KUB[])
Completing...
Starting query not attacker(KUB[])
RESULT not attacker(KUB[]) is true.
-- Query not attacker(KUS[])
Completing...
Starting query not attacker(KUS[])
RESULT not attacker(KUS[]) is true.
```

Fig. 4. The performance resul.

4.2 Security analysis

In this section, our scheme presents how various known attacks can be resisted.

4.2.1 Repeat registered Attack

In the proposed scheme, the user can select his/her identity randomly. So there is a case that different people may select the same identity. However, our scheme can overcome this problem. At first, the attacker cannot select other people's identity in the required time interval. After the time interval, the registration time is not the same, so the attacker can get different value of $r_i = h(ID_i \,||\, X_s \,||\, t_{reg})$. Then, the adversary cannot sponsor identity masquerade attack.

4.2.2 The proposed scheme can be carried out effectively

In the login and authentication phase of the Das's scheme, the BS can get user's identity ^{ID_i} by computing $ID_i = M_1 \oplus h(X_s \,||\, t_{reg})$. The value of M_1 and t_{reg} will be sent to the BS while X_s belongs to the BS. What's more, the information of the sensor node is unlikely to be revealed. In the sensor node's memory, only ID_{SN_j} and the BS's public key Kpub_key are

stored. ID_{SN_j} and Kpub_key can not be kept secretly. So our proposed scheme can ensure information stored in the sensor nodes securely.

4.2.3 Protection of user and sensor node anonymity

In our proposed scheme, the user's identity and the sensor node's identity are not transfered in the original form. The user's identity ID_i is protected by the BS's master key X_s and the sensor node's identity is protected by $h(\mathrm{ID}_i \| \mathrm{RN}_{U_i})$. At the same time, the identity of sensor node is protected by $ID_{SN_j} \oplus h(\mathrm{ID}_i \| RN_{U_i})$. From the analysis, we can see that our proposed scheme can achieve user and sensor node's identity anonymous protection.

4.2.4 Mutual authentication

During the login and authentication phase of our proposed scheme, both the BS and the user can authenticate each other. After receiving $M_6^* = h(\mathrm{RN}_{U_i} \| \mathrm{ID}_i)$ from the BS, the user must execute $M_6 ? = M_6^*$ because only the BS can acquire the value of RN_{U_i} and ID_i.

4.2.5 Three-factor security

In our scheme, a user must provide {password, smart card, biometric} in order to obtain legal identity. Even the attacker acquires the password of any one of them, he cannot acquire biometric from it or other information stored in smart card. The user cannot acquire pw_i, B_i^{reg} from $h(\mathrm{pw}_i)$ because of the collision-resistant property of h(.). From the analysis, we can see that a user can finish authentication successfully only when he provides all the following information {password, smart card, biometric}. So our proposed scheme can achieve three factors. All the security properties between the proposed scheme and Das's scheme have been compared in Table 2.

Table 2. The comparison of security properties.

	Das's scheme	**Our scheme**
Whether achieving the user and sensor node identity anonymity	No	Yes
Whether overcoming the sensor node impersonation attack	No	Yes
Whether overcoming the repeat registered attack	No	Yes
Whether can be carried out effectively	No	Yes
Whether the scheme resists smart card lost attack	Yes	Yes
whether considering the fuzzy of biometric	Yes	Yes
Whether the scheme resists privilege inside attack	Yes	Yes
Whether achieving three-Factor authentication	Yes	Yes
Whether considering the light-weight authentication	Yes	Yes

4.3 Performance Analysis

The capability of our proposed scheme will be compared with that of the Das's in this section. For convenience, some notations are defined as described below.

T_x :the time for executing an XOR operation; T_h : the time for executing MD5 operation; T_s : the time for executing a symmetric decryption/encryption operation;TPE: the time for

performing a asymmetric encryption operation;TPD: the time for performing a asymmetric decryption operation; T_{ss} : the time for generating S from client's biometric information W during the registration phase by fuzzy extractors algorithm; T_{rec} :the time for recovering W from the sketch S and the user login biometric information W by fuzzy extractors algorithm;TGen: the time for obtaining help data P and secret key R W by secure sketch algorithm; TRep:the time for recovering from W and help string P by secure sketch.

Step 1: The value of T_x is very insignificant, so we can neglect it.

Step 2: From the analysis in section 1.2, we can see that the error correction algorithm consumes most of the time in the secure sketch scheme. So we can have $T_{\mathrm{Re}c} \approx T_{Decoding}$ which means the time of decoding.

Step 3: In section 1.2.1, Error correction of coding and decoding consume the main time of secure sketch. At the same time, fuzzy extractor is constructed by secure sketch and universal hash function. So we can get $T_{ss} + T_{\mathrm{Re}c} + T_{Gen} + T_{\mathrm{Re}p} = 2T_{Coding} + 2T_{Decoding} + 2T_H$. T_{Coding} denotes the time of coding. $T_{Decoding}$ denotes the time of decoding.

Step 4: On an Intel Core i5-3470 platform, we measured the consumption time BCH(172,71) and MD5, $T_{Coding} = 0.78\mathrm{sec}$, $T_{Decoding} = 0.18\mathrm{sec}$, $T_H = 0.00097\mathrm{sec}$, $T_{Gen} = T_{Coding} + T_H = 0.78097\mathrm{sec}$, $T_{\mathrm{Re}p} = T_{Decoding} + T_H = 0.18097\mathrm{sec}$, $T_s = 0.001\mathrm{sec}$, $T_{PE} = 0.004\mathrm{sec}$, $T_{PD} = 0.0156\mathrm{sec}$ (sec denotes second).

Table 3. Comparison of performance (Registration phase).

	User	**The BS**	**The sensor Node**
Das(2015) [12]	$2T_X + 4T_H + T_{Gen} = 0.78485$	$T_H = 0.00097$	0
Our scheme	$T_{ss} + 2T_H = 0.78194$	$2T_X + 2T_H = 0.00194$	0

Table 4. Comparison of performance (login and authentication phase).

	User	**The BS**	**The sensor Node**
Das(2015) [12]	$4T_X + 7T_H + T_{\mathrm{Rep}} = 0.18776$	$3T_H + T_X + T_s = 0.00391$	$T_X + 2T_H + T_S = 0.00294$
Our scheme	$4T_X + 6T_H + T_{\mathrm{Rec}} + T_S = 0.18682$	$4T_X + 3T_H + T_{PD} + T_S = 0.01951$	$T_{PE} + T_H = 0.00497$

Table 5. Comparison of performance (Password change phase).

	Client	**Server**	**The sensor Node**
Das(2015) [12]	$2T_X + 6T_H + T_{\mathrm{Rep}} + T_{Gen} = 0.96776$	0	0
Our scheme	$2T_X + 4T_H + T_{\mathrm{Rec}} + T_{SS} = 0.96388$	0	0

From Table 3-5, we can come to the conclusion that our proposed scheme consumes less time at client compared with that of Das during all the three important phases. Despite more time consumed at the BS during the registration and authentication phase, it will have little effect owing to the strong computation power of the BS. As a result, our scheme not only can resolve the problem of fuzzy of biometric but also can overcome the security problems of the Das's scheme. So our proposed scheme is more reasonable and more practical.

5 Conclusion

In this article, we analyze the security problems of the Das's scheme carefully. Then, a new authentication for WSNs based on Secure Sketch is proposed to solve all the security problems in the Das's protocol. At the last sector, we compare the security and performance of our proposed scheme with the Das's. From the above analyses, we can draw the conclusion

that our scheme has higher security and a lower computation cost than the Das's at client in spite of a slight higher computation cost in the BS and the sensor node.

This work has been supported by the Fundamental Research Funds for the Central Universities of Southwest Minzu University (No. 2018SQN53), and Supported by Sichuan Science and Technology Program(NO.2017JY0230)

References

1. Das M L. Two-factor user authentication in wireless sensor networks[J]. Wireless Communications, IEEE Transactions on, 2009, 8(3): 1086-1090.
2. Nyang D H, Lee M K. Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks[J]. IACR Cryptology ePrint Archive, 2009, 2009: 631.
3. He D, Gao Y, Chan S, et al. An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks[J]. Ad Hoc & Sensor Wireless Networks, 2010, 10(4): 361-371.
4. Kumar P, Lee H J. Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks[C]//Wireless Advanced (WiAd), 2011. IEEE, 2011: 241-245.
5. Yoo S G, Park K Y, Kim J. A security-performance-balanced user authentication scheme for wireless sensor networks[J]. International journal of distributed sensor networks, 2012, 2012.
6. Jiang Q, Ma J, Lu X, et al. An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks[J]. Peer-to-Peer Networking and Applications, 2014: 1-12.
7. Sun D Z, Li J X, Feng Z Y, et al. On the security and improvement of a two-factor user authentication scheme in wireless sensor networks[J]. Personal and ubiquitous computing, 2013, 17(5): 895-905.
8. Das A K. A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks[J]. Peer-to-Peer Networking and Applications, 2014: 1-22.
9. Das A K. An efficient and novel three-factor user authentication scheme for large-scale heterogeneous wireless sensor networks[J]. International Journal of Communication Networks and Distributed Systems, 2015, 15(1): 22-60.
10. Althobaiti, O., Al-Rodhaan, M., Al-Dhelaan, A.: An efficient biometric authentication protocol for wireless sensor networks. International Journal of Distributed Sensor Networks 2013, Article ID 407971, 1–13 (2013)
11. Das A K. A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor[J]. International Journal of Communication Systems, 2015.
12. Ashok Kumar Das. A Secure and Efficient User Anonymity-Preserving Three-Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks. Wireless Personal Communication,2015,82(1):1377-1404.
13. Das, A. K. (2012). A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks. International Journal of Information Security, 11(3), 189–211.