A Biometric-based User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks

Ying Chen[1,2], Yangming Ge[1], Wenyuan Wang[1], and Fengyu Yang[1,2]
[1]School of Software, Nanchang Hangkong University
Nanchang 330063, Jiangxi-P.R.China
[e-mail: {c_y2008, gym_2018, nchu_wwy, frueyang}@163.com]
[2]Internet of Things Technology Institute, Nanchang Hangkong University
Nanchang, 330063, Jiangxi-P.R.China
[{c_y2008, frueyang} @163.com]
*Corresponding author: Yangming Ge

Received August 28, 2017; revised November 6, 2017; accepted November 28, 2017; published April 30, 2018

Abstract

Heterogeneous wireless sensor networks (HEWSN) is a kind of wireless sensor networks (WSN), each sensor may has different attributes, HEWSN has been widely used in many aspects. Due to sensors are deployed in unattended environments and its resource constrained feature, the design of security and efficiency balanced authentication scheme for HEWSN becomes a vital challenge. In this paper, we propose a secure and lightweight user authentication and key agreement scheme based on biometric for HEWSN. Firstly, fuzzy extractor is adopted to handle the user's biometric information. Secondly, we achieve mutual authentication and key agreement among three entities, which are user, gateway and cluster head in the four phases. Finally, formal security analysis shows that the proposed scheme defends against various security pitfalls. Additionally, comparison results with other surviving relevant schemes show that our scheme is more efficient in term of computational cost, communication cost and estimated time. Therefore, the proposed scheme is well suitable for practical application in HEWSN.

Keywords: Heterogeneous wireless sensor networks, biometric feature, mutual authentication, key agreement

The authors thank the anonymous referees for their thorough reviews and constructive comments. The research is supported by National Natural Science Foundation of China (Grant no. 61762067, 61501217 and 61662049), Natural Science Foundation of Jiangxi Province (Grant no. 20161BAB212034), and Jiangxi Province Education Department (Grant No. GJJ160692).

http://doi.org/10.3837/tiis.2018.04.021 **ISSN : 1976-7277**

1. Introduction

In wireless sensor networks (WSN), a large number of sensor nodes are used to monitor data, and then the collected data are transmitted to the user via self-organizing multi-hop routing communication. WSN has a widely application in military, medical, industrial safety and other monitoring fields. Generally, WSN can be divided usaully into two categories: one is homogeneous wireless sensor networks (HOWSN) and the other is heterogeneous wireless sensor networks (HEWSN). The HOWSN is composed of a large number of homogeneous sensor nodes, which are deployed in specific target areas for collecting information, these sensor nodes sense perceptual information, and then the information is sent to user from the base station through the internet. However, the way of sensor node communication is multi-hop routing, which results to increase the transmission time and consume more energy. And more importantly, the sensor node which is close to the base station will be required to assist other long-distance sensor nodes to transmit information to base station, which will decreases lifetime of the entire network[1][2]. The architecture of HOWSN is shown in **Fig. 1**.

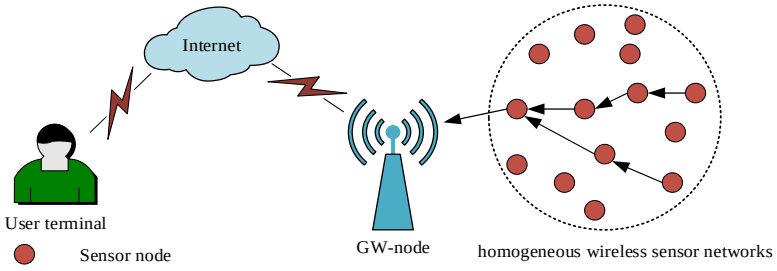

Fig. 1. The architecture of HOWSN

Compared to HOWSN, some cluster header nodes are added in HEWSN, **Fig. 2** shows the architecture of HEWSN. HEWSN will become more and more popular in many fields than the HOWSN, there are some different aspects between them. Firstly, all sensor nodes of HEWSN are divided into some clusters, each cluster head node has more powerful computational ability, larger storage space and longer transmission distances. Secondly, the information sensed by ordinary sensor nodes is transmitted to the cluster head which is responsible for collecting, integrating and transmitting message. Finally, the integrate information is sent to base station. In a sum, HEWSN adopts hierarchical method, compared to HOWSN, HEWSN can reduces energy costs and extends the lifetime of the WSN[3].

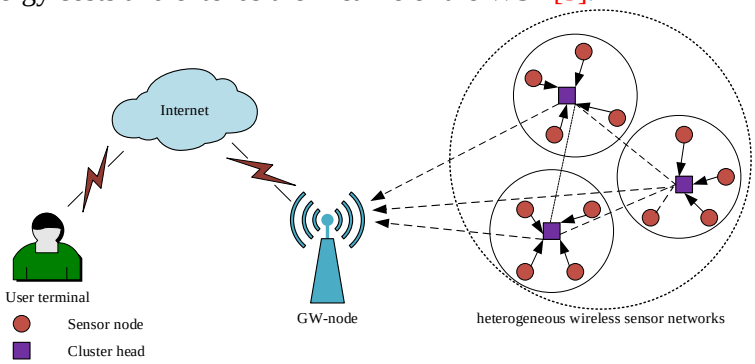

Fig. 2. The architecture of HEWSN

Due to sensor node deployed in unattended fields, HEWSN is vulnerable to vaoius attacks. In addition, ordinary sensor node has a fatal flaw that which has constrained resources such as lack storage and energy, low computational and short radio transmission range. Therefore, it is vital importance to design a security and efficiency balanced authentication scheme for HEWSN.

The remaining parts of this paper are organized as follows: Section 2 reviews the relevanted literatures. Perliminaries used in this paper are described in Section 3. In Section 4, we propose a biometric-based user authentication scheme. The security analysis is described in Section 5. Security and performance comparison with other surviving relevant schemes is described in Section 6. Finally, Section 7 concludes the full paper.

2. Literatures Review

In order to guarantee to access HEWSN safely, some user authentication schemes for HEWSN have been proposed by many researchers.

In 2006, Wong et al. [4] proposed a lightweight user authentication scheme based on password. However, Das [5] pointed out that Wong et al.'s authentication scheme is vulnerable to stolen-verifier attacks in 2009. In order to overcome the extremely serious security flaw that Wong et al.'s verification tables are stored in the database of authentication nodes, Das proposed a two-factor authentication scheme based on password and smart card. In 2010, Chen et al. [6] pointed out that Das's scheme cannot support mutual authentication between gateway node (*GWN*) and sensor node (*SN*), and then they proposed a robust mutual authentication protocol for WSN. In the same year, Li and Hwang [7] proposed a biometric-based efficient remote user authentication scheme with smart card, it is more efficient compared to other schemes. Yuan and Jiang [8] proposed a user authentication scheme based on biometric, the protocol utilized only Hash operation and provided password changed freely. In 2011, Yeh et al. [9] pointed out that Das's scheme has other security problems, for example, it is unable to resists forgery attack. Thence, a security authentication scheme based on Elliptic Curve Cryptography (ECC) was proposed by them to solves the above-mentioned problems. Meantime, Yoon et al. [10] showed that Yuan's scheme cannot resist user forgery attack, *GWN* forgery attack and sensor node forgery attack. Then, an improved biometric authentication scheme was proposed by them. Li et al.[11] pointed out that authentication scheme of reference [7] does not resist middle attcks, and they proposed a biometric-based improved user authentication scheme with smart card. In 2012, He [12] indicated that Yoon's scheme cannot resist denial-of-service attack and fake attack from sensor nodes, then, they put forward an improved scheme. In 2013, Yoon and Kim [13] proposed an improved biometric-based user authentication scheme for WSN, the characteristic of their scheme used only secure one-way hash function and didn't require the user password, therefore, Yoon's scheme has more efficiency and convenience compared with other related traditional authentication schemes. Shi and Gong [14] proposed an improved ECC-based efficient authentication scheme based on Yeh et al.'s [9] authentication scheme. Xue et al. [15] pointed out that most of the previous authentication methods have security flaws, so they proposed a mutual authentication and key agreement scheme based on temporal credential. In 2014, Choi et al. [16] pointed out that scheme of reference [14] is vulnerable to stolen samrt card attack, and they proposed an enhanced protocal for WSN. Wang and Wang [17] put forward a general principle that public-key techniques are intrinsically indispensable to construct a two-factor authentication scheme. In 2015, Sheetal and Sandeep [18] found that Xue's scheme is vulnerable to impersonation attack, stolen smart card attack, server spoofing

attack. Hence, they proposed a password based authentication scheme. At the same year, Chang et al.'s [19] and Choi et al. [20] pointed out that Yoon's scheme has various security problems, including biological recognition errors, user verification problems, user anonymity deficiency, denial-of-service attacks and session key exposure, in order to solve those security problems, an improved biometric authentication scheme based on fuzzy extraction was proposed by them. In 2016, Park et al. [21] founded that Choi et al.'scheme could not resist user impersonation attack, to overcome that security fault, they proposed an enhanced biometric-based authentication scheme for WSN. Laterly, a dynamic user authentication and key agreement scheme was proposed by Chang et al. [22], in their scheme, heterogeneous architecture was adopted to reduce the energy consumption of the whole WSN. In 2017, Moon et al. [23] demonstrated that Park et al.'s scheme could not resist user impersonation attack, and then they proposed an improved biometric-based authentication scheme for WSN. Li et al. [24] designed a user authentication scheme for wireless body area networks to protect user privacy message and provided the anonymous mutual authentication. Afterwards, Li et al.[25] put forward a three-factor anonymous user authentication scheme for Internet of Things (IoT) , the merits of the proposed scheme to utilize fuzzy commitment scheme to handle the user's biometric information. Srinivas et al. [26] proposed a novel authentication and key agreement scheme for WSN using biohashing, and their scheme also supports dynamic node addition and user friendly password change mechanism.

As aforementioned schemes, Chang et al.'s scheme provided for heterogeneous architecture, and in which the sensor nodes require none computation cost [19]. Therefore, we propose a more efficient user authentication scheme to extend the lifetime of WSN by take advantage of the merits of HEWSN. Furthermore, there are many advantages of biometric key, and some of the main advantages are described as follows:

(1) It has no possibility of forgetting and losing biometric key.
(2) It is difficult to copy and share biometric key.
(3) It is extremely difficult to forge and distribute biometric key.
(4) It is difficult to guess biometric key.
(5) It is more difficult to crack biometric key than traditional password.

Therefore, a biometric-based user authentication scheme will be more suitable than traditional password-based user authentication schemes for HEWSN [9][13][15].

3. Preliminaries

3.1 Fuzzy Extractor

The biometric-based fuzzy extractor [21][27-29] converts biometric data into a randomly value, which consists of two procedures (*Gen, Rep*), and they are described as follows:

(1) $Gen\ (B_i) = (R_i, P_i)$;
(2) $Rep\ (B_i^*, P_i) = R_i$ *if* B_i^* *is reasonably close to* B_i.

The function *Gen* is a propabilistic generation procedure, its' input is B_i, and its' outputs include an "extracted" string $R_i \in \{0,1\}^l$ and an auxiliary string $P_i \in \{0,1\}^*$. The function *Rep* is a deterministic reproduction procedure, which recovery R_i from the corresponding auxiliary string P_i. Even if the biometrics inputted by user is disturbed by the scanning device, the retrieved R_i maintains a reasonable similarity status with the original biometric information for a long time, it satisfies the request of authentication.

3.2 Related Assumptions

It is necessary to make the following assumption in order to make a better description and compare with other authentication schemes.

Assumption 1. With regard to the one-way hash function $y = h(x)$, it is extremely easy to compute y for a given x, but it is extremely difficult to compute x for a given y.

Assumption 2. The attacker U_A can monitor the public communication channel among the user U_i, the gateway node GWN and the cluster header node $CHID_j$. Furthermore, U_A has the ability to eavesdrop, intercept and modify the information transmitted through the public communication channel.

3.3 Secure Channel Description

Generally, the information transmission channel are mainly divided into two categories for WSN, one is public communication channel and the other is secure communication channel. For the public channel lack of security, any people can monitor, intercept and modify the transmitted data. However, secure channel has higher security properity, the message transmitted in secure channel will be keep confidentiality through adoptting some special measures (e.g. message encryption, face to face password exchange) to achieve secure transmition. In the paper, we think that all messages are transmitted in secure channel in order to better focus on the key problem.

4. The Proposed Scheme

In this section, we propose a secure and efficient remote user authentication scheme which is based on biometric information for HEWSN. The notations and its description in the proposed paper are shown in **Table 1**.

Table 1. Notations and its description

Notation	Description
U_i	A user i
GWN	A trusted gateway node
CH_j	A cluster header node j
S_q	A sensor node q
$CHID_j$	The identity of CH_j
ID_i	The identity of U_i
x_g	A secret key of GW
B_i	Biometric template
y_i	The secret number of U_i
k_j	A pre-shared key of GWN and CH_j,where $k_j=h(CHID_j\|\|x_g)$
$h(\cdot)$	A secure one-way Hash function

The entire authentication structure system of HEWSN is shown in **Fig. 3**, and which mainly includes three different roles, namely user, gateway node and cluster node. The whole process of the proposed authentication scheme is divided into four phases: (1) registration phase, (2) login phase, (3) mutual authentication and key agreement phase, and (4) revocation and reissue phase.

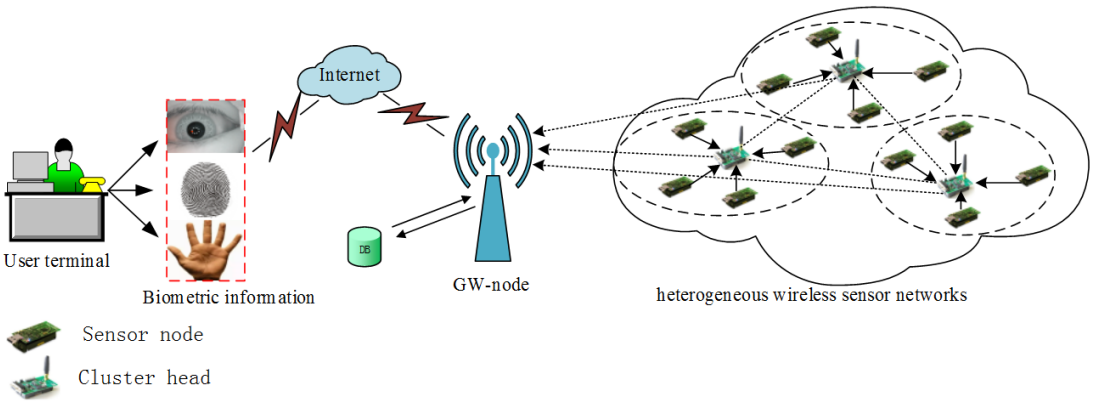

Fig. 3. Structure of the proposed authentication system

4.1 Registration Phase

When the remote user authentication scheme starts, the user and *GWN* need to follow the following steps:

Step 1. The gateway node generates a secret key x_g and calculates the key $k_j = h(CHID_j \| x_g)$ shared with each cluster header node j. Then, the cluster header node CH_j load the shared key k_j. Finally, they are deployed to the designated fields.

Step 2. User U_i chooses ID_i freely, and imprints her/his own biometric template B_i via the corresponding scanning device. Then, U_i utilizes the biometric template B_i to calculate and acquire the biometric key $BPW_i = h(R_i)$ by means of the fuzzy extraction method $< R_i, P_i >= Gen(B_i)$. Finally, U_i sends $< ID_i, BPW_i >$ to the *GWN* through the secure communication channel.

Step 3. After receiving the message from the U_i, *GWN* selects a randomly value y_i for U_i and calculates the relevant parameter according to the equations (1-6).

$$f_i = h(ID_i \| x_g) \tag{1}$$

$$A = h(y_i) \oplus h(ID_i \| BPW_i \| y_i) \tag{2}$$

$$B = h(ID_i \| BPW_i) \oplus y_i \tag{3}$$

$$C = h(ID_i \| BPW_i \| y_i) \oplus f_i \tag{4}$$

$$D = h(h(x_g) \| y_i) \tag{5}$$

$$q = h(f_i) \oplus D \oplus BPW_i \oplus h(x_g) \tag{6}$$

Then, *GWN* stores $y_i \oplus h(x_g)$ and D in its database.

Step 4. The *GWN* stores the parameters A, B, C, q and $h(\cdot)$ in a smart card and sends it to the user U_i through a secure channel. The registration phase is shown in **Fig. 4**.

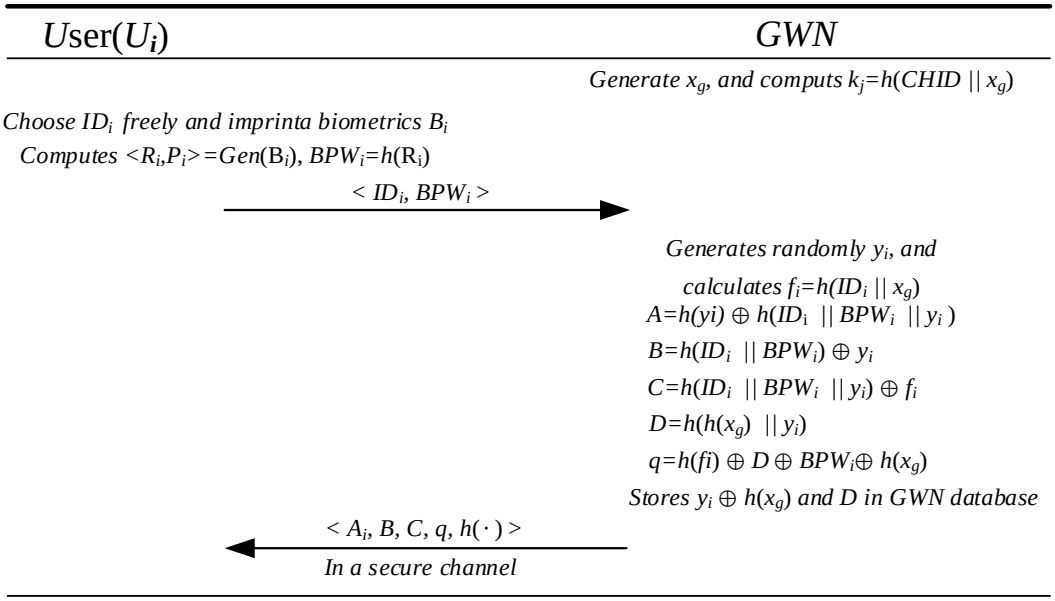

Fig. 4. The proposed registration phase

4.2 Login Phase

When user wants to login to *GWN*, she/he must performs the following steps:

Step 1. U_i inserts her/his smart card into the card reader and inputs ID_i, and she/he uses the scanning device to obtain B_i^*. Then, the smart card calculates $R_i^* = REP(B_i^*, P_i)$ and $BPW_i^* = h(R_i^*)$ by fuzzy extraction method.

Step 2. The smart card calculates $y_i = B \oplus h(ID_i \| BPW_i^*)$ and $A^* = h(y_i) \oplus h(ID_i \| BPW_i^* \| y_i)$, and then verifies $A^* ? = A$, where A is stored in the smart card. If their values are not equal, the smart card rejects this login request. Otherwise, it proceeds to the next step.

Step 3. The smart card picks up the current timestamps T_i, and then calculates the relevant parameters according to the equations (7-10).

$$M_1 = T_i \oplus h(y_i) \tag{7}$$

$$f_i = h(ID_i \| BPW_i \| y_i) \oplus C \tag{8}$$

$$N_i = q \oplus h(f_i) \oplus BPW_i \tag{9}$$

$$DID_i = h(T_i \| N_i \| y_i) \tag{10}$$

Step 4. The smart card sends the login request message $< M_i, N_i, DID_i >$ to *GWN*. The login phase is shown in **Fig. 5**.

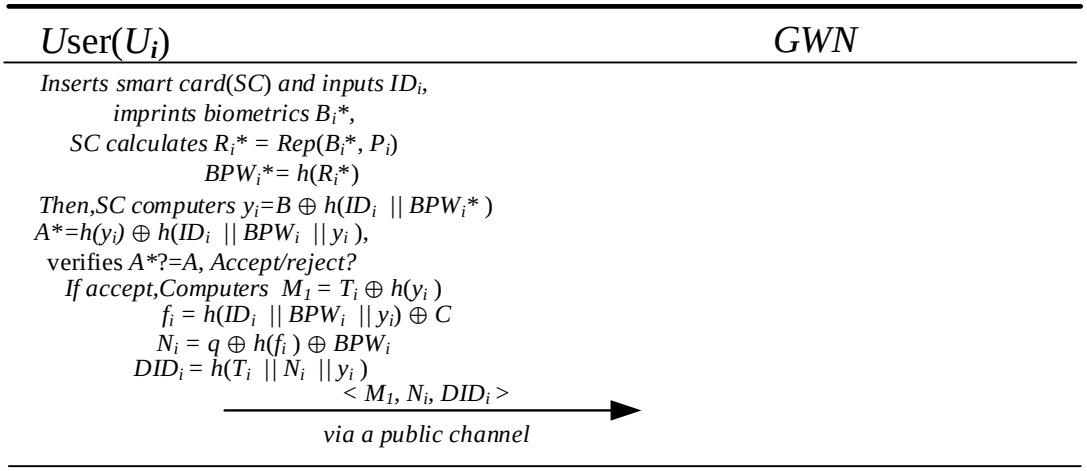

Fig. 5. The proposed login phase

4.3 Mutual Authentication and Key Agreement Phase

Upon receiving the login request, the *GWN* authenticates U_i according to the following steps:

Step 1. After *GWN* received the login request message from U_i, *GWN* calculates $D = N_i \oplus h(x_g)$ with its private key x_g and then checks whether *D* is in its database or not. If it isn't, *GWN* refuses the login request of U_i and stops the session. If it is, *GWN* can finds that corresponding parameter $y_i \oplus h(x_g)$, and y_i can be easily retrieved via x_g.

Step 2. *GWN* recovers $T_i = M_1 \oplus h(y_i)$ using the received message M_1 from U_i and y_i retrieved in Step 1, then, *GWN* picks up the current timestamp T^*. If $(T^* - T_i) < \Delta T$, where ΔT is the specified transmission delay time, *GWN* then calculates and verifies $h(T_i \| N_i \| y_i) ? = DID_i$. If the above condition does hold, *GWN* confirms that U_i is a legitimate user. Otherwise, *GWN* rejects the login request of U_i and stops the session. Then, *GWN* selects a nearby cluster header CH_j as the access node of data for U_i.

Step 3. *GWN* picks up the current timestamp T_g and utilizes the pre-shared key $k_j = h(CHID_j \| x_g)$ between *GWN* and CH_j to calculates the relevant parameters according to the equations (11-13).

$$M_2 = h(CHID_j \| x_g) \oplus T_g \tag{11}$$

$$R = h(CHID_j \| x_g) \oplus h(y_i) \tag{12}$$

$$Auth = h(T_g \| CHID_j \| x_g) \| h(y_i) \tag{13}$$

Then, *GWN* sends message $< M_2, R, Auth >$ to the nearby cluster header CH_j.

Step 4. After receiving the message $< M_2, R, Auth >$ from *GWN*, CH_j obtains $T_g = k_j \oplus M_2$ utilizing k_j and M_2, CH_j picks up the current timestamp T^{**}. If $(T^{**} - T_g) < \Delta T$, CH_j calculates $h(y_i) = k_j \oplus R$ utilizing R and k_j, and verifies

$h(T_g \| k_j \| h(y_i))? = Auth$. If the above condition does not hold, CH_j rejects the request and stops the session, otherwise CH_j believes that *GWN* is valid.

Step 5. The cluster header node CH_j picks up the current timestamp T_j and calculates the relevant parameters according to the equations (14-15).

$$M_3 = T_j \oplus h(k_j \| T_g) \tag{14}$$

$$Ack_1 = h(h(y_i) \| T_g \| T_j \| k_j) \tag{15}$$

Then, CH_j sends the message $< M_3, Ack_1 >$ back to the *GWN*.

Step 6. After receiving the message $< M_3, Ack_1 >$ from CH_j, *GWN* utilizes the M_3 from the acquired message to retrieves $T_j = h(h(CHID_j \| x_g) \| T_g) \oplus M_3)$. Then *GWN* selects the current timestamp T^{***}. If $(T^{***} - T_j) < \Delta T$, *GWN* computes and validates $h(h(y_i) \| T_g \| T_j \| k_j)? = Ack_1$. If the above condition does hold, *GWN* ensures that CH_j is valid. Meanwhile, *GWN* receives the correct time value T_g. Conversely, the session will be stopped by *GWN*.

Step 7. *GWN* calculates the following parameters according to the equations (16-18):

$$M_4 = T_g \oplus h(h(y_i) \| T_i) \tag{16}$$

$$M_5 = T_j \oplus h(y_i \| T_i \| T_g) \tag{17}$$

$$Ack_2 = h(y_i \| T_i \| T_g \| T_j) \tag{18}$$

Then, *GWN* sends the message $< M_4, M_5, Ack_2 >$ back to U_i.

Step 8. U_i retrieves T_g and T_j from the equations (19-20) after receiving the message $< M_4, M_5, Ack_2 >$ from *GWN*, the processes are expressed as follows**:**

$$T_g = h(h(y_i) \| T_i) \oplus M_4 \tag{19}$$

$$T_j = h(y_i \| T_i \| T_g) \oplus M_5 \tag{20}$$

Then, U_i calculates and verifies $h(y_i \| T_i \| T_g \| T_j)? = Ack_2$. If the above condition does hold, U_i firmly believes *GWN* and CH_j are valid, otherwise the session will be stopped.

Step 9. After U_i, *GWN* and CH_j have completed mutual authentication, they compute $sk = h(h(y_i) \| T_g \| T_j)$, where *sk* will be used as the secure communication session key. The mutual authentication and key agreement phase is shown in **Fig. 6**.

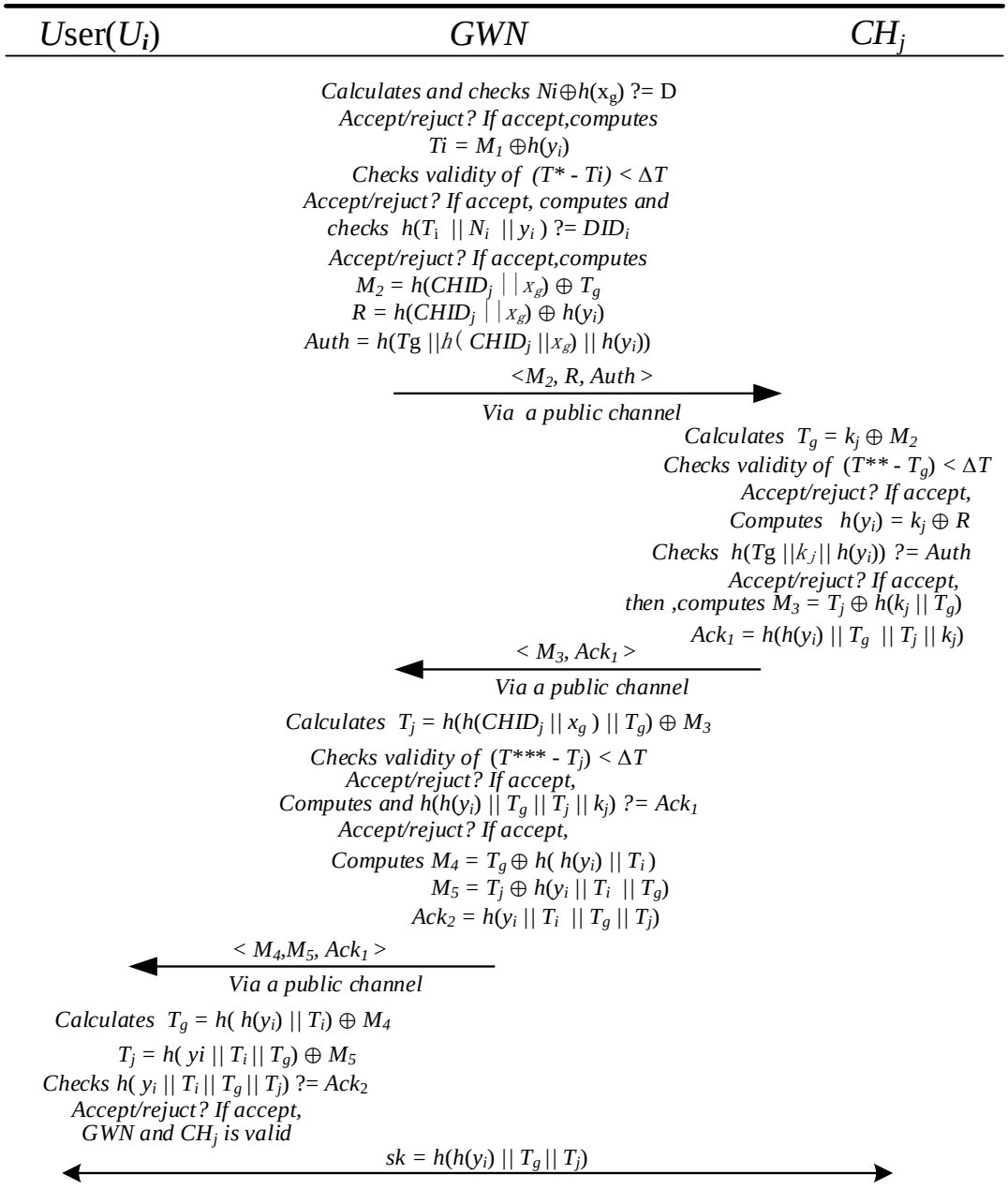

Fig. 6. The proposed mutual authentication and key agreement phase

4.4 Revocation and Reissue Phase

Since biometric information cannot be changed, in order to have similar function that user can freely change password, the proposed scheme achieve this goal by changing the user *ID*. After changing the *ID*, the user only needs to input new *ID* when she/he logins in HEWSN, the biometric key is inputted in the same way that described in the login phase. The specific implementation processes are as follows:

Step 1. U_i inputs her/his original ID_i and imprimts biometric template B_i^{**} from the biometric information scanning device, and then her/his calculates $R_i^{**} = REP(B_i^{**}, P_i)$ to obtain the biometric key $BPW_i^{**} = h(R_i^{**})$ by means of the fuzzy extraction method.

Step 2. The smart card computes $y_i = B \oplus h(ID_i \| BPW_i^{**})$, and verifies $A^{**} = h(ID_i \| BPW_i^{**} \| y_i) ? = A$, If the condition does hold, the smart card believes that the U_i is valid. Contrarily, the smart card rejects the request of U_i 's login, and stops the session right away.

Step 3. After the verification success, U_i chooses a new identity ID_i^{new} freely, and then related calculations are made according to the equations (21-25):

$$f_i^{new} = h(ID_i^{new} \| x_g) \tag{21}$$

$$A^{new} = h(y_i) \oplus h(ID_i^{new} \| BPW_i \| y_i) \tag{22}$$

$$B^{new} = h(ID_i^{new} \| BPW_i \| y_i) \oplus y_i \tag{23}$$

$$C^{new} = h(ID_i^{new} \| BPW_i \| y_i) \oplus f_i^{new} \tag{24}$$

$$q^{new} = h(f_i^{new}) \oplus D \oplus BPW_i \oplus h(x_g) \tag{25}$$

Step 4. The smart card replaces A, B, C, and q with A^{new}, B^{new}, C^{new}, and q^{new} respectively. The revocation and reissue phase is shown in **Fig. 7**.

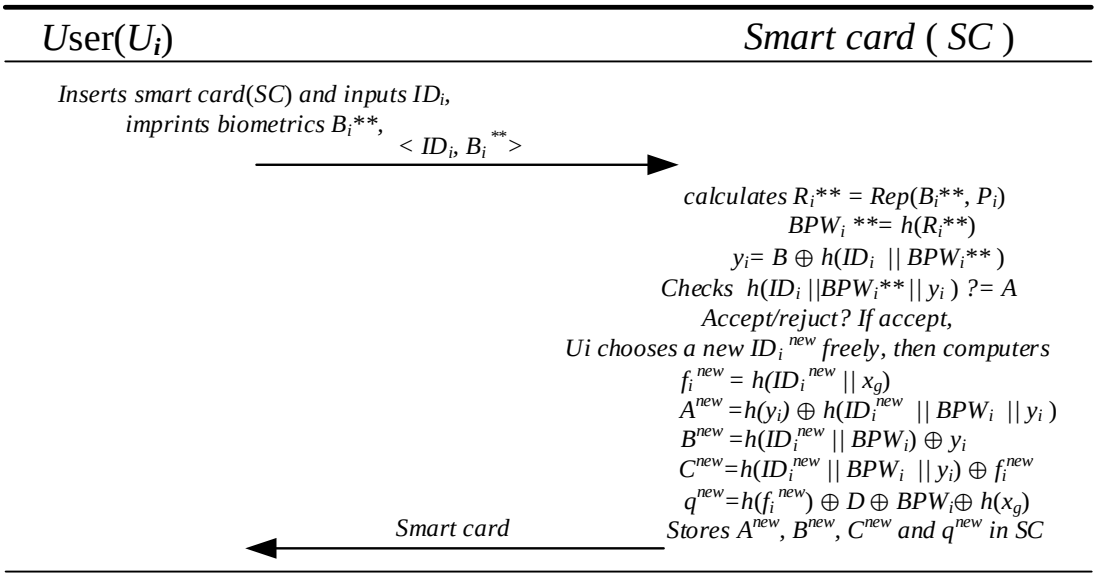

Fig. 7. The proposed revocation and reissue phase

5. Security Analysis

In this section, we discuss the security and functional features of the proposed scheme, and our scheme resist most of known attacks and achieve some ideal functional features.

5.1 Biometric Recognition Error

In the proposed scheme, biometric recognition error can be avoided by using the fuzzy extractor. The scheme proposed by Yoon and Kim [30] used a hash function to check the conformity in the biometrics. As we all known, one-way hash function has a property that the output value of the hash function will be changed dramatically even though the input data makes slight differences. In a practical application, biometric recognition error occurs inevitably, which leads to the consequences that legitimate user cannot complete the verification of login phase. For this problem, the proposed scheme uses fuzzy extraction method to solve it easily, so our scheme can resist biometric recognition error.

5.2 Resistance to Replay Attack

Assuming that an attacker U_A has eavesdropped the transmitted message on the public channel, for the sake of impersonating anyone of the three parties such as U_i, *GWN* and $CHID_j$, U_A replays the previous authentication message intercepted from the public channel to pass the related verification, but it is invalid for the proposed scheme because the timestamps T_i, T_g and T_j are included in each authentication phase. For example, when the *GWN* verifies a user during the authentication phase, *GWN* retrieves T_i through the obtained message $< M_i, N_i, DID_i >$ after receiving the access request of U_A, and then determines whether U_i is legal via $(T^* - T_i) < \Delta T$, *GWN* can confirms that U_i is legitimate if this is true, otherwise U_i is illegal. So our scheme can resistant to replay attacks.

5.3 Resistance to User Impersonation Attack

Assuming that the attacker U_A wants to impersonate a user U_i and a *GWN*, U_A has to intercepts the login message $< M_1, Ni, DID_i >$ from the public communication channel, and then forges a login request message as follows:

Step 1. The attacker U_A picks up the current timestamp T_A, and then guesses a value y_i' randomly.

Step 2. U_A computes $M_{1A} = T_A \oplus h(y_i')$ and $DID_{iA} = h(T_A \| N_i \| y_i')$.

However, because attacker U_A cannot fake M_{1A} and DID_{iA} without knowing private value y_i of U_i. Likewise, the change of parameters M_{1A} and DID_{iA} will be detected by the Step 2 of mutual authentication and key agreement phase. Thus, the proposed scheme can resist user impersonation attack.

5.4 Resistance to Gateway Faked Attacks

Assuming that the attacker U_A wants to get the data collected by the cluster header $CHID_j$. Without passing verification of *GWN*, the attacker U_A will fakes a *GWN* to deceive the cluster header $CHID_j$. The specific practices of U_A will be described as following steps:

Step 1. The attacker U_A picks up the current timestamp T_A, and guesses a value y_i' randomly.

Step 2. U_A substitutes T_A and y_i' into equations (11-13) and obtains equations (26-28) correspondingly:

$$M_{2A} = h(CHID_j \| x_g) \oplus T_A \tag{26}$$

$$R_A = h(CHID_j \| x_g) \oplus h(y_i) \tag{27}$$

$$Auth_A = h(T_A \| h(CHID_j \| x_g) \| h(y_i^{'})) \quad (28)$$

Then, the message $< M_{2A}, R_A, Auth_A >$ will be sent to the $CHID_j$ directly. Obviously, the owned value $k_j = h(CHID_j \| x_g)$ by *GWN* is not known to U_A. Therefore, the *GWN* fake attack launched by the attacker is invalid for the proposed scheme.

5.5 Resistance to Cluster Header Node Impersonation Attack

Just like Section5.4, since the attacker U_A does not know k_j, U_A cannot be impersonated as a cluster header node to fool *GWN*. Therefore, the proposed scheme can resist the cluster header node impersonation attacks.

5.6 Resistance to Stolen-Verifier Attack

Although the related parameters, such as $y_i \oplus h(x_g)$, are stored in the database of *GWN*, it will not happen any threats to validate user's login request on security. Assuming that the attacker U_A has obtained a verification table from *GWN* which contains $y_i \oplus h(x_g)$ and *D*, if U_A wants to be disguised as the user U_i, she/he has to utilizes $y_i \oplus h(x_g)$ to retrieve the private value y_i of U_i via the operations described in Section5.3, but it is not computationally feasible to retrieve y_i without knowing the private value x_g of *GWN*. Therefore, the attack is invalid for the proposed scheme.

5.7 Resistance to Stolen Smart Card Attacks

Assuming that the information stored in the smart card can be extracted by the attacker U_A in some way (such as energy analysis attack [31]). If U_A has stolen a user U_i's smart card, and U_A can obtain the parameter *A,B,C,q* and $h(\cdot)$ stored in the smart card. Then a login request message is forged by U_A, the specific practices will be illustrated by the following steps:

Step 1. The attacker U_A picks up the current timestamp T_A.

Step 2. The attacker U_A uses the parameters *A, B, C, q and* $h(\cdot)$, T_A to computes $y_i = h(ID_i \| BPW_i^*) \oplus B$, then, she/he substitutes related parameters into equations (7-10), The processes of calculation are as follows:

$$M_{1A} = T_A \oplus h(y_i) \quad (29)$$

$$f_i = h(ID_i \| BPW_i \| y_i) \oplus C \quad (30)$$

$$N_i = h(f_i) \oplus BPW_i \oplus q \quad (31)$$

$$DID_{iA} = h(T_A \| N_i \| y_i) \quad (32)$$

The bogus message faked by the attacker is $< M_{1A}, N_i, DID_{1A} >$, but the bogus login request message cannot pass the authentication of *GWN*. U_A cannot retrieves correctly y_i via $y_i = h(ID_i \| BPW_i) \oplus B$, because U_A cannot obtains U_i's ID_i and B_i, so the proposed scheme can resist to stolen smart card attacks.

5.8 Resistance to Guessing Attacks

Because the proposed scheme do not use the password, hence, it don't exist password -guessing attack. Moreover, the user's biometric information B_i is always protected by the hash function $h(\cdot)$. Considering that B_i has a high level of information entropy, unlike the traditional password, the attacker U_A cannot calculate the user's biometric key value by means of the hash value. Therefore, our scheme has ability to against guessing attacks.

5.9 Forward Secrecy

The proposed scheme obtains the session key *sk* between U_i and $CHID_j$ according to the equal $sk = h(h(y_i) \| T_g \| T_j)$, an attacker has to obtains y_i, T_g and T_j to calculates the session key of U_i or $CHID_j$. Although the attacker has ability to intercepts and modifies the transmitted message in public channel, yet it is impossible for the attacker to computes the session key *sk*, because T_g and T_j are independent of each other, analysis result demonstrates that the proposed scheme provide perfect forward secrecy.

5.10 Resistance to Insertion Attacks

If attacker U_A wants to login in *GWN* and obtains the service without registation, she/he must invades *GWN* and inserts the information $< D_A, y_A \oplus h(x_g) >$ into the database of *GWN*. However, it is definitely infeasible computational case that U_A inserts the information $< D_A, y_A \oplus h(x_g) >$ into the gateway node database without knowing the secret value x_g of *GWN*. So that we can get the conclusion that the proposed scheme can against the insertion attack.

5.11 Resistance to Capture Attacks of Cluster Header Node

Assuming that the attacker U_A has captured a cluster header node *j* and obtained the key $k_j = h(CHID_j \| x_g)$ stored in the cluster header node *j*. If U_A launches an attack toward the proposed scheme, it will only impact the secure communication between the user and the compromised cluster header node *j* for WSN, however, the communication among the other cluster header nodes will not be affected in any way because a different key $k_t = h(CHID_t \| x_g)$ is shared between cluster header node *t* and *GWN*. Furthermore, U_A does not know the key of the other non-compromised cluster header, which results in a consequence that the attacker U_A cannot access the data of non-compromised cluster header *t*. So the proposed scheme can resist capture attack.

5.12 User Anonymity and Non-traceability

If U_A wants to get the message of a specific user U_i, the attacker's first step is to acquires user's identity ID_i according to the message $< M_1, N_i, DID_i >$ in login phase. However, it's impossible for U_A to retrieve ID_i from the intercepted message because the ID_i was not included in the message $< M_1, N_i, DID_i >$ by $M_1 = h(y_i) \oplus T_i$, $N_1 = h(x_g \| y_i) \oplus h(x_g)$ and $DID_i = h(T_i \| h(h(x_g) \| y_i) \oplus h(x_g) \| y_i)$. In addition, we can also make a more serious assumption that the attacker possesses the smart card for a appropriate time, and the data stored in smart card has been acquired in some ways by U_A. After obtaining the message $< A, B, C, q, h(\cdot) >$, where $A = h(y_i) \oplus h(ID_i \| BPW_i \| y_i)$, $B = h(ID_i \| BPW_i) \oplus y_i$ and

$C = h(ID_i \| BPW_i \| y_i) \oplus f_i$. Although the ID_i are included in the three equals above mentioned, ye it is impossible for U_A to computes and obtains user's real ID_i because which is protected according to one-way hash function. Similarly, the attacker also can't acquire user's real ID_i via ID and $y_i \oplus h(x_g)$ stored in the database of *GWN*. In addition, we can know that every user's identity is temporal and which can be changed dynamically via $DID_i = h(T_i \| N_i \| y_i)$ because every session includes different timestamp T_i. In conclusion, the proposed scheme provides user anonymity.

5.13 Mutual Authentication

The proposed scheme realize the mutual authentication among user, cluster header node and gateway node.

(1) U_i authenticated by *GWN*

When U_i sends the login request message $< M_1, N_i, DID_i >$ to the *GWN*, *GWN* retrieves D_i and y_i from its database with private key x_g, then *GWN* makes judgment via $h(T_i \| N_i \| y_i) ? = DID_i$. U_i is legitimate and valid if above condition does hold, and then *GWN* accepts the login request of U_i.

(2) *GWN* authenticated by CH_j

After U_i was authenticated by *GWN* in process (1) aboved mentioned, *GWN* generates and sends an verified message $< M_2, R, Auth >$ to the nearby cluster header CH_j, CH_j uses private key k_j to verify $h(T_g \| k_j \| h(y_i)) ? = Auth$. CH_j believes firmly that *GWN* is valid if above condition does hold, and sends a feedback message $< M_3, Ack_1 >$ to the *GWN*. Conversely, CH_j rejects the login request and stops the session.

(3) CH_j authenticated by *GWN*

After receiving the feedback message $< M_3, Ack_1 >$ from CH_j, *GWN* retrieves the timestamps $T_j = h(k_j \| T_g) \oplus M_3$, and then checks $h(T_g \| k_j \| T_j \| h(y_i)) ? = Ack_1$, if above condition does hold, *GWN* ensure that CH_j is legal. Finally, *GWN* computes the feedback messages $< M_4, M_5, Ack_2 >$ and sends it to U_i.

(4) *GWN* authenticated by U_i

After receiving the feedback message $< M_4, M_5, Ack_2 >$, U_i retrieves the timestamps $T_g = h(h(y_i) \| T_i) \oplus M_4$ and $T_j = h(y_i \| T_i \| T_g) \oplus M_5$, and then verifies $h(y_i \| T_i \| T_g \| T_j) ? = Ack_{21}$. If above condition does hold, U_i believes that *GWN* and CH_j are valid.

6. Security and Performance Comparisons

In this section, we present the performance of the developed scheme with other surviving relevant schemes [9][13][15][19][21] in terms of security aspects, computation cost and communication cost.

6.1 Comparison of Security and Functional Features

Table 2 represents the security and functional features comparison of our scheme with other

surviving relevent schemes [9][13][15][19][21]. It can be observed that the schemes [15][19][21] are vulnerable to impersonation attack and the schemes [9][13][15][21] do not provide user anonymity property. Further, the schemes [15][19] neither protect from stolen smart card attack nor protect guessing attack. The scheme in [9] does not provide protection against the node capture attack. The schemes in [13][21] can not solve revocation and reissue problem. Yeh et al. [9] scheme does not facilitate session key aggreement as well as provide mutual authentication and the schemes in references [9][15] do not accurate password change phase. From **Table 2**, we observe that none of the authentication schemes are completely secured against various security threats and also do not provide all security features. However, the proposed scheme is secure against all the security threats as well as facilitates various security features such as user anonymity, mutual authentication, session key verification, etc.

Table 2. Comparison of security and functional features

Property	**Park et al.**[21]	**Chang et al.**[19]	**Yoon et al.**[13]	**Xue et al.**[15]	**Yeh et al.**[9]	**Ours**
A1	Yes	—	No	—	—	Yes
A2	Yes	Yes	Yes	Yes	Yes	Yes
A3	No	No	Yes	No	Yes	Yes
A4	Yes	Yes	Yes	Yes	Yes	Yes
A5	Yes	No	Yes	No	Yes	Yes
A6	Yes	No	Yes	No	Yes	Yes
A7	Yes	Yes	Yes	Yes	Yes	Yes
A8	Yes	Yes	Yes	Yes	No	Yes
A9	No	—	No	—	—	Yes
A10	Yes	Yes	No	Yes	No	—
A11	Yes	Yes	Yes	Yes	No	Yes
A12	No	Yes	No	No	No	Yes
A13	Yes	Yes	Yes	Yes	No	Yes

Note: A1: Resists to biometric recognition error, A2: Resists to replay attack, A3: Resists to impersonation attack, A4: Resists to stolen verifier attack, A5: Resists to stolen smart card attack, A6: Resists to guessing attack, A7: Resists to insertion attack, A8: Resists to node capture attack, A9: Solves revocation and reissue problem, A10: Provides password change phase, A11: Provides session key verification, A12: Provides user anonymity, A13: Provides mutual authentication.

6.2 Comparison of Computational Costs

In **Table 3**, we have shown the computational costs of our scheme along with other related schemes [9][13][15][19][21]. For calcultating computation costs, we firstly define some userful notation as follows:

T_h: is the time cost for one-way hash operation

T_{ed}: is the time cost for encryption/decryption operation

T_{ecc}: is the time cost for an elliptic curve operation

Meanwhile, A conclusion according to the reference [32] has been indicated that $T_{ecc}>>T_{ed}>>T_h$. Moreover, T_h, T_{ed} and T_{ecc} are 0.0005s, 0.0087s and 0.0621s respectively according to reference [33]. Therefore, the estimated execution time of the relevant schemes [9][13][15][19][21] and the proposed scheme are 0.5023s, 0.0413s, 0.0145s, 0.0105s, 0.2830s, and 0.0130s, respectively.

Table 3. Computation costs comparison of our scheme with other related schemes

Participant ↓	**Park et al.** [21]	**Chang et al.** [19]	**Yoon et al.** [13]	**Xue et al.** [15]	**Yeh et al.** [9]	**Ours**
U_i's cost	$6T_h$ +$2T_{ecc}$	$11T_h$	5 T_h +1 T_{ed}	9 T_h	4 T_h +2 T_{ecc}	$11T_h$
GWN's cost	$7T_h$ +$2T_{ed}$	$6T_h$	5 T_h +2 T_{ed}	14 T_h	4 T_h +4 T_{ecc}	$11T_h$
CHD_j's cost	0	0	0	0	0	$4T_h$
SN's cost	$4T_h$+$1T_{ed}$+$2T_{ecc}$	$4T_h$	3 T_h +1 T_{ed}	6 T_h	3 T_h +2 T_{ecc}	0
Total cost	$17T_h$+$3T_{ed}$+$4T_{ecc}$ =0.2830s	$21T_h$ =0.0105s	$13T_h$+4 T_{ed} =0.0413s	29 T_h =0.0145s	$11T_h$ +8 T_{ecc} =0.5023s	$26T_h$ =0.0130s

From **Table 3**, we can see that the computation costs of the proposed protocol is better than that of the existing schemes [9][13][15][21]. Though the proposed scheme require more computation cost as compared to Chang et al.'s [19], yet Chang et al.'s [19] scheme suffers from impersonation attack, stolen verifier attack and guessing attack. Since the proposed scheme is secure against various security attacks and faciliates various security feature, it may be sonsidered better than the Chang et al.'s scheme [19]. Therefore, we think that it is worthy to increase a little computation cost for higher security. Furthermore, the proposed scheme adopts the architecture of HEWSN, the sensor nodes don't need to perform any operation, which can reduce greatly energy consumption, so the lifetime of the entire WSN is extended.

Overall, our scheme not only keep the efficiency of computation, but also achieve well known functional and security features.

6.3 Comparison of Communication Costs

In **Table 4**, we have presented the communication cost of the proposed scheme along with other related schemes [9][13][15][19][21] . For computing the communication cost, we set the length of output of symmertric-key encryption/decryption algorithm, ECC point multiplication, output of one-way hash function at 128, 320, and 160 bits according to reference [34], reference [35], and reference [36], respectivley. Further, we assume that the length of timestamp is 32 bits and the length of identity is 160 bits. The proposed scheme require commnuication cost 1760 bits, whereas the Yeh et al. [9], Yoon et al. [13], Xue et al. [15], Chang et al. [19] and Park et al. [21] need the communication cost of 1664, 992, 1888, 1408 and 1952 bits, respectively. It is observed from **Table 4** that the scheme in [9][13][19] require less communication over the proposed scheme. However, we have seen in security and functional feature section that those schemes [9][13][19] do not provide various security attributes and also are vulnerable to various security attacks. In a word, to pay some extra cost for higher security features and functionalities is reasonable and hence the proposed scheme is better and suitable for practical application.

Table 4. Communication costs comparison of our scheme with other related schemes

Schemes ↓	**Communication cost**	**Communication mode between different roles**
Yeh et al. [9]	1664 bits	$U_i \rightarrow GWN$, $GWN \rightarrow U_i$, $SN \rightarrow GWN$
Xue et al. [15]	1888 bits	$U_i \rightarrow GWN$, $GWN \rightarrow SN$, $SN \rightarrow U_i$
Yoon et al. [13]	992 bits	$U_i \rightarrow GWN$, $GWN \rightarrow SN$, $SN \rightarrow U_i$
Chang et al. [19]	1408 bits	$U_i \rightarrow GWN$, $GWN \rightarrow SN$, $SN \rightarrow GWN$, $GWN \rightarrow U_i$
Park et al. [21]	1952 bits	$U_i \rightarrow GWN$, $GWN \rightarrow SN$, $SN \rightarrow U_i$
Ours	1760 bits	$U_i \rightarrow GWN$, $GWN \rightarrow SN$,$SN \rightarrow GWN$, $GWN \rightarrow U_i$

7. Conclusions

In this paper, user authentication scheme based on biometrics for HEWSN is proposed. In the proposed scheme, (1) we take advantage of merit of biometric key replace traditional password, (2) only one-way hash function and XOR operation are used in the scheme, (3) the HEWSN with hierarchical transmission is used to reduce the energy consumption of the entire WSN, thereby which can prolongs the life cycle of the WSN. Analysis results show that the proposed scheme can provide mutual authentication and key agreement securely. Moreover, the proposed scheme can resist most attacks, such as stolen verifier attack, replay attack and guess attack and which has higher security compared with other related authentication schemes. Based on performance evaluation, the proposed scheme provides better performance than the existing schemes in terms of computation cost and communication cost. Further, the scheme proposed in this paper is more suitable for WSN applications in various fields.

References

[1] S. Kumari, M. K. Khan and M. Atiquzzaman,"User authentication schemes for wireless sensor networks: A review," *Ad Hoc Networks*, vol.27, pp.159-194, 2015. Article (CrossRef Link)

[2] Y. T. Tsou, C. S. Lu and S. Y. Kuo,"SER: Secure and efficient retrieval for anonymous range query in wireless sensor networks," *Computer Communications*, vol.108, pp.1-16, 2017. Article (CrossRef Link)

[3] M. S. Farash, M. Turkanović and S. Kumari, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*,vol.36,pp.152-176, 2016. Article (CrossRef Link)

[4] W. H. Wong, Y. Zheng and J. Cao, "A Dynamic User Authentication Scheme for Wireless Sensor Networks," in *Proc. of IEEE Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing*,vol.1,pp.244-151, 2006. Article (CrossRef Link)

[5] M. L. Das,"Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol.8, no.3, pp.1086-1090,2009. Article (CrossRef Link)

[6] T.H. Chen and W. K. Shih,"A Robust Mutual Authentication Protocol for Wireless Sensor Networks," *Etri Journal*, vol.32, no.5, pp.704-712, 2010. Article (CrossRef Link)

[7] C. T. Li, M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network & Computer Applications*, vol.33, no.1, pp.1-5,2010. Article (CrossRef Link)

[8] J.J Yuan and J. Jiang,"A Biometric-Based User Authentication for Wireless Sensor Networks," *Wuhan University Journal of Natural Sciences*, vol.15, no.3, pp.272-276, 2010. Article (CrossRef Link)

[9] H. L. Yeh, T. H. Chen and P.C. Liu, "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *Sensors*, vol.11, no.5, pp.4767-4779, 2011. Article (CrossRef Link)

[10] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of robust mutual authentication protocol for wireless sensor networks," in *Proc. of IEEE International Conf. on Cognitive Informatics and Cognitive Computing*, pp.392-369, 2011. Article (CrossRef Link)

[11] X. Li, J. W. Niu, J. Ma, et al. "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *Journal of Network & Computer Applications*, vol. 34, no. 1, pp.73-79, 2011. Article (CrossRef Link)

[12] D. He,"Robust biometric-based user authentication scheme for wireless sensor networks," *Ad hoc & Sensor Wireless Networks*, vol.25, no.3, pp.309-321, 2012. Article (CrossRef Link)

[13] E. J. Yoon and C. Kim, "Advanced Biometric-Based User Authentication Scheme for Wireless Sensor Networks," *Sensor Letters*, vol.11, no.9, pp.1836-1843, 2013. Article (CrossRef Link)

[14] W. Shi and P. Gong, "A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *International Journal of Distributed Sensor Networks*, no.730831, pp.51-59, 2013. Article (CrossRef Link)
[15] K. Xue, C. Ma and P. Hong, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network & Computer Applications*, vol.36, no.1, pp.316-323, 2013. Article (CrossRef Link)
[16] Y. Choi, D. Lee, J. Kim, et al. "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *Sensors*, vol.14, no.6, pp. 10081, 2014. Article (CrossRef Link)
[17] D. Wang and P. Wang,"On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," *Computer Networks*, vol.73, pp.41-57, 2014. Article (CrossRef Link)
[18] K. Sheetal and K. S. Sandeep,"Advanced password based authentication scheme for wireless sensor networks," *Journal of Information Security and Applications*, vol.20, pp.37-46, 2015. Article (CrossRef Link)
[19] I. P. Chang, T. F. Lee, T. H. Lin, et al. "Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks," *Sensors*, vol.15, no.12, pp.29841-29854, 2015. Article (CrossRef Link)
[20] Y. Choi, Y. Lee and D. Won, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction," *International Journal of Distributed Sensor Networks*, vol.2016, no.4, pp.1-16, 2016. Article (CrossRef Link)
[21] Y. H. Park, S. Y. Lee and C. K. Kim,"Secure biometric-based authentication scheme with smart card revocation/reissue for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol.12, no.7, 2016. Article (CrossRef Link)
[22] C. C. Chang, W. Y. Hsueh and T. F. Cheng, "A Dynamic User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks," *Wireless Personal Communications*, vol.89, no.2, pp.447-465, 2016. Article (CrossRef Link)
[23] J. Moon, D. Lee and Y. Lee, "Improving Biometric-Based Authentication Schemes with Smart Card Revocation/Reissue for Wireless Sensor Networks," *Sensors*, vol.17, no.5, pp.1-24, 2017. Article (CrossRef Link)
[24] X. Li, M. H. Ibrahim and S. Kumari, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, 2017. Article (CrossRef Link)
[25] X. Li, J. Niu and S. Kumari, "A Three-factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments," *Journal of Network & Computer Applications*, article in press. Article (CrossRef Link)
[26] J. Srinivas, S. M. D. Mukhopadhyay, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Networks*, vol.54, pp.147-169, 2017. Article (CrossRef Link)
[27] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *International Journal of Communication Systems*, pp.1-15, 2015.Article (CrossRef Link)
[28] C. Wang, X, Zhang and Z. Zheng, "Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme," *Plos One*, vol.11, no.2, 2016. Article (CrossRef Link)
[29] Y. Dodis, B. Kanukurthi and J. Katz, "Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets," *IEEE Transactions on Information Theory*, vol.58, no.9, pp.6207-6222, 2012. Article (CrossRef Link)
[30] J. H. Yoon and J. H. Kim,"A closed-form analytic correction to the Black–Scholes–Merton price for perpetual American options," *Applied Mathematics Letters*, vol.26, no.12, pp.1146-1150, 2013. Article (CrossRef Link)

[31] H. J. Mahanta, A. K. Azad and A. K. Khan, "Power analysis attack: A vulnerability to smart card security," in *Proc. of International Conf. on Signal Processing and Communication Engineering Systems*, pp.506-510, 2015. Article (CrossRef Link)
[32] T. Hasegawa, J. Nakajima and M. Matsui, "A practical implementation of elliptic curve cryptosystems over GF(p) on a 16-bit microcomputer," in *Proc. of International Workshop on Public Key Cryptography.Spring Berlin Heidelberg*, pp.182-194, 1998. Article (CrossRef Link)
[33] P. Mohit, R. Amin, A. Karati, et al. "A standard mutual authentication protocol for cloud computing based health care system," vol.41, no.4, pp.1-13, 2017. Article (CrossRef Link)
[34] Advanced Encryption Standard (AES). Retrieved on June 26, 2017 from Article (CrossRef Link)
[35] K. Neal, M Alfred, V. Scott., "The State of Elliptic Curve Cryptography," *Designs Codes & Cryptography*, vol.19, no.2, pp.173-193, 2000. Article (CrossRef Link)
[36] Secure hash standard. Retrieved on June 26, 2017 from Article (CrossRef Link)

Ying Chen is an associate professor at Nanchang Hangkong University, Nanchang, Jiangxi, P. R. China. He received his B.E. degree, Master degree and PhD degree from Jilin University, Changchun, Jilin, P. R. China. His current research interests include wireless sensor network, Internet of Things, biometric information recogniton, information security.

Yangming Ge received the Bachelor degree in Measuring and Optical Engineering from Nanchang Hangkong University, Nanchang, China, in 2014. He is currently a postgraduate, Internet of Things Technology Institute, Nanchang Hangkong University, Nanchang, China. His research is focused on user authentication and access control in wireless sensor networks.

Wenyuan Wang received his B.E. degree in Software Engineering from Nanchang Hangkong Univer-sity, Nanchang, Jiangxi, P.R.China, in june 2016. He is currently pursing a master's degree at the School of Software in Nachang Hangkong University. His current research interest is Deep Learning and network communication.

Fengyu Yang is an associate professor at Software School of Nanchang Hangkong University, Nanchang, Jiangxi, P.R. China. He received his master degree from Zhejiang University of Technology, Hangzhou, Zhejiang, P.R.China. Hiscurrent research interests include modular software design, automatic software testing, data mining on big data. Also, he has taken part in many pratical projects for companies.