Computers and Electrical Engineering 63 (2017) 182–195

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Efficient end-to-end authentication protocol for wearable health monitoring systems☆

Qi Jiang[a,*], Jianfeng Ma[a], Chao Yang[a], Xindi Ma[a], Jian Shen[b], Shehzad Ashraf Chaudhry[c]

[a] School of Cyber Engineering, Xidian University, Xi'an, China
[b] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China
[c] Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 9 March 2017
Revised 12 March 2017
Accepted 13 March 2017
Available online 7 April 2017

Keywords:
Wearable health monitoring systems
Authentication
Key agreement
Privacy
Quadratic residues
Smart card

ABSTRACT

Wearable health monitoring systems (WHMSs) will play an increasingly important role in future e-healthcare and enable smart and ubiquitous healthcare services. Given its sensitivity, the health data should be protected against unauthorized access. As a result, it is critical to design an end-to-end mutual authentication protocol that enables secure communication between the wearable sensor and medical professionals. Recently, Amin et al. proposed an anonymity preserving mutual authentication protocol for WHMSs. However, we identify that their protocol suffers from stolen mobile device attack, desynchronization attack, and sensor key exposure. Then we put forward an improved end-to-end authentication protocol based on quadratic residues. Comprehensive security analysis is conducted to show that the proposed protocol fixes these flaws of Amin et al.'s protocol and satisfies all desired requirements. The comparison with these existing protocols demonstrates that our protocol provides a practical end-to-end security solution for WHMSs.

1. Introduction

As one of the promising means to alleviate the issues associated with the increasing aging population and healthcare costs, as well as to improve healthcare quality, wearable health-monitoring systems (WHMSs) have attracted an increasing attention from both the industry and academia. WHMSs, which consist of various types of wearable or even implantable medical sensors, are enabling smart and ubiquitous monitoring of health condition of a mobile patient in a non-invasive way, from anywhere and at any time, and will potentially transform the future of healthcare [1].

Currently, advances in miniature sensors, wireless communications and cloud computing have made WHMSs a reality [1–3]. The architecture of a typical WHMS is shown in Fig. 1. The medical sensors and a personal mobile device, which can be a smart phone, a PDA, a pocket PC, etc., form a body area network (BAN) or body sensor network (BSN). These medical sensors sense significant physiological parameters, e.g., heart rate, blood pressure, body temperature, respiration rate, electrocardiogram, and transmit the data to the mobile device which acts as the intermediary to share this information over long distances. Then the intermediary sends the measured health data to a remote medical server or the medical professional's mobile device [1].

☆ Reviews processed and approved for publication by Editor-in-Chief.

* Corresponding author.
E-mail address: jiangqixdu@gmail.com (Q. Jiang).

http://dx.doi.org/10.1016/j.compeleceng.2017.03.016
0045-7906/

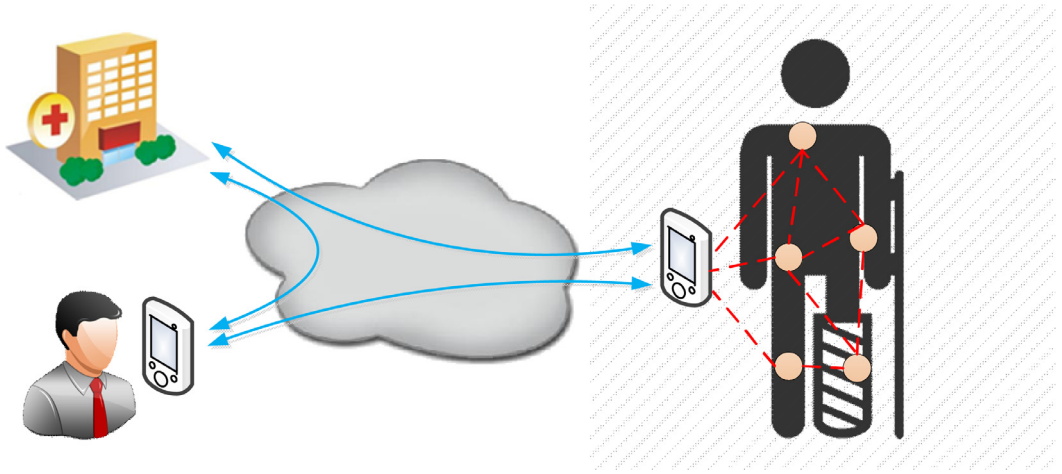

Fig. 1. Typical architecture of wearable health monitoring systems (WHMSs).

In WHMSs, the health data can be accessed by medical professionals anywhere and anytime through Internet and wireless networks. Specifically, a medical professional can access the health data in two ways. One is to access the data maintained by the medical server. The other is to access the real-time data measured by sensors directly. Given its sensitivity, there are laws stipulating privacy rules regarding electronic health data in healthcare systems, such as the Health Insurance Portability and Accountability Act (HIPAA) [4,5]. Thus there is strong awareness of the security and privacy of health data in WHMSs. Since the sensitive health information is transmitted through a path composed of various network devices and open channels, the information should be protected against various types of active and passive attacks [6]. In this paper, we mainly concern the design of an end-to-end mutual authentication and key agreement protocol between the wearable sensor and medical professionals to achieve end-to-end secure communication between them. Although several authentication protocols [7–16] has been proposed in the literature, all these protocols either fail to provide adequate security protection or suffer from various security vulnerabilities.

1.1. Architecture of WHMSs

In WHMSs, there are three types of participants, i.e., medical professional (doctor, patient, nurse, etc.), medical sensors and gateway. The medical sensor nodes sense the health condition of the patient and then send the health data to the gateway or medical professionals. The gateway is the brain of WHMSs, which provides registration to all the medical professionals and sensor nodes. The medical professionals can access the sensitive information of the patient from either the gateway or the sensor node to diagnose and monitor the patient's health conditions [7]. In traditional wireless medical sensor networks (WMSNs), the role of gateway is played by a smart device of the patients [7–9]. However, due to limited computing capability and power supply, mobile devices, such as smart phones and PDAs, are not suitable to perform expensive operations, such as providing registration services to medical professionals and sensors. In order to avoid this dilemma, we propose the slightly modified architecture, in which the role of registration center is played by a dedicated medical server in the medical center, as is illustrated in Fig. 1.

1.2. Related works

It is generally accepted that WHMSs must prevent unauthorized access to the sensitive health information and guarantee security and privacy of these participants. One more challenge that cannot be ignored is that power consumption of mobile devices and sensors should be minimized to lengthen the operational lifetime of WHMSs, since the power supply of sensors and mobile devices is relatively limited [1]. In this line, a number of two-factor authentication and key agreement protocols have been put forward. In such protocols, two different types of security credential, i.e., smart card and password, are needed for a user to corroborate his/her identity.

In 2012, Kumar et al. [8] suggested an authentication protocol for monitoring the health conditions of a patient and claimed that their protocol is capable of withstanding known security threats. Unfortunately, Khan and Kumari [9] found that Kumar et al.'s protocol has several security attacks. In addition, they proposed an enhanced protocol which is more efficient and secure against known attacks. He et al. [10] also showed that Kumar et al.'s protocol is vulnerable to some attacks and then put forward a user authentication protocol for healthcare applications using WMSNs.

In 2015, Wu et al. [11] showed that the protocol of He et al. [10] suffers from offline password guessing and impersonation attacks. Wu et al. [11] proposed an improved user authentication protocol using hash function to remove the loopholes of the protocol of He et al. Mir et al. [12] also showed that He et al.'s protocol is still susceptible to the offline password

guessing attack and user impersonation attack. They also proposed an enhanced protocol to fix them. Independently, Li et al. [13] demonstrated that He et al.'s protocol [10] suffers from some pitfalls and further gave a bio-hash based authentication protocol.

Das et al. [14] reviewed Li et al.'s protocol and showed that their protocol is insecure against privileged insider attack, sensor node capture attack and fails to provide user anonymity. To fix these drawbacks, they presented a secure biometrics-based user authentication protocol. Li and Lee [15] proposed a chaotic map based two-factor authentication and key agreement protocols for WBANs. Liu and Chung [16] put forward a two-factor authentication protocol using bilinear pairing, in which smart cards are used to store authentication data. Furthermore, a secure data transmission is given to safeguard the privacy and security of both medical professionals and patients. Recently, Amin et al. [7] proposed an anonymity preserving mutual authentication protocol for WHMSs. It is claimed that their protocol is secure and capable of withstanding various attacks. However, we identify that their protocol has several pitfalls.

Independently, Li et al. [17] proposed a security protocol based on certificateless signcryption for secure transmission of data between BAN and servers. Xiong [18] proposed a certificateless public key cryptography (CLPKC) based authentication protocol for BANs. Most recently, He et al. [19] provided an anonymous authentication protocol based on CLPKC for wireless BANs. Shen et al. [20] proposed a suite of authentication and key management protocols based on ECC and hash chains for BAN to achieve mutual authentication and secure communication among sensor nodes, the patient controller and medical professionals. Abdmeziem and Tandjaoui [21] proposed a lightweight key management protocol to establish an end-to-end secure channel between a resource limited node and a remote entity based on the concept of cooperation. The main idea is to offload resource consuming cryptographic primitives from the constrained node to powerful third parties. One common feature of the above protocols is that they only employ single type of security credential, i.e. the cryptographic key.

1.3. Contributions

Our contributions are presented as follows.

We analyze the most recent authentication protocol of Amin et al [7] and show its security drawbacks. Specifically, we identify that their protocol suffers from stolen mobile device attack, i.e., the user identity and password can be exhaustively guessed in an offline manner with the secrets stored in the stolen mobile device. In addition, their protocol is prone to desynchronization attack. A legal user can be prevented from accessing the sensor data by blocking the confirmation message in the previous authentication phase. Furthermore, the protocol suffers from the problem of sensor key exposure where sensor key will be compromised when the temporal parameters in an authentication session are disclosed.

We then present an efficient and secure user authentication protocol based on quadratic residues for WHMSs. Through comprehensive security analysis, we demonstrate that our protocol is secure against all the possible attacks including the security pitfalls revealed in Amin et al.'s protocol, and provides more security features. The comparison with these existing protocols demonstrates that our protocol achieves a balance between security and efficiency and is ready for practical use in WHMSs.

The remainder of this paper is organized as follows. We review and analyze Amin et al.'s protocol in Sections 2 and 3, respectively. In Section 4, we propose an end-to-end authentication and key agreement protocol for WHMSs. Section 5 presents security and efficiency analysis of the improved protocol. Section 6 concludes this paper.

2. Review of Amin et al.'s protocol

We briefly review Amin et al.'s authentication protocol [7], which consists of five phases, i.e., (1) Setup, (2) Medical professional registration, (3) Patient registration, (4) Login and authentication, and (5) Password change phase. The notations involved in this paper are listed as follows.

U_i	Medical professional;
GW	Gateway node;
SN_j	Sensor node;
PW_i	U_i's password;
ID_i	U_i's identity;
ID_{SN_j}	SN_j's identity;
K	GW's secret key;
TID_i	Unique temporary identity generated by GW for U_i;
R_1, R_2, R_3	Random number generated by U_i, GW, SN_j, respectively;
$h(\cdot)$	One-way hash algorithm;
$\|\|$	Concatenation;
$\oplus$	Bitwise XOR operation.

2.1. Setup phase

The registration center first chooses a long-term secret key K for the GW and then computes a secret key $SK_{GW-SN_j} = h(ID_{SN_j}||K)$ for SN_j, where $1 \le j \le s$ and s represents the number of sensor nodes. The hash algorithm used is defined as $h:\{0,1\}^* \rightarrow \{0,1\}^l$, where l is the output length of $h(\cdot)$.

2.2. Medical professional registration phase

This phase is executed by a medical professional U_i before providing medical services. The details are presented as follows.

Step 1: U_i picks an identity ID_i, a password PW_i, and then computes $HPW_i = h(ID_i \oplus PW_i)$. Then, he/she sends $\langle ID_i, HPW_i \rangle$ to GW securely by using the TLS protocol or offline means.

Step 2: On receiving $\langle ID_i, HPW_i \rangle$, GW computes $Reg_i = h(ID_i||R_i||HPW_i)$, $A_i = R_i \oplus HPW_i$, $B_i = h(ID_i||R_i||K)$, $C_i = B_i \oplus h(ID_i \oplus R_i \oplus HPW_i)$, $D_i = R_i \oplus h(TID_i||K)$, where R_i is a random number of U_i. To achieve untraceability, a different TID_i is selected by GW in each session.

Step 3: GW stores $\langle TID_i, D_i \rangle$ in a table for further use and forwards $\langle TID_i, Reg_i, A_i, C_i, h(\cdot) \rangle$ to U_i through a secure communication channel. After receiving $\langle TID_i, Reg_i, A_i, C_i, h(\cdot) \rangle$, U_i stores all these information into his/her mobile device.

2.3. Patient registration phase

In this phase, the patient firstly selects and forwards his/her name to the registration center. Then it selects an appropriate sensor kit and appoints medical professional. The registration center forwards patient's identity and relevant information of sensors to the appointed medical professional.

2.4. Login and authentication phase

Mutual authentication and session key exchange between the participants are achieved in this phase. The details are presented as follows.

Step 1: U_i inputs ID_i and PW_i into the mobile device. Then, the device calculates $HPW_i^* = h(ID_i \oplus PW_i)$, $R_i^* = A_i \oplus HPW_i$, $Reg^*{}_i = h(ID_i||R^*{}_i||HPW_i^*)$, and verifies whether $Reg^*{}_i ? = Reg_i$ holds. If it is negative, the device aborts; otherwise, it proceeds to the next step.

Step 2: The mobile device generates a random nonce R_1, calculates $B_i^* = C_i \oplus h(ID_i \oplus R_i^* \oplus HPW_i^*)$, $CID_i = ID_i \oplus h(TID_i||R_i^*||T_1)$, $M_1 = h(ID_i||B^*{}_i||R_1||T_1)$, $M_2 = h(R_i||T_1) \oplus R_1$, and then sends $< TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1 >$ to GW.

Step 3: GW retrieves D_i according to TID_i, and calculates $R_i^* = D_i \oplus h(TID_i||K)$, $ID_i^* = CID_i \oplus h(TID_i||R_i^*||T_1)$, $B_i^* = h(ID_i||R_i^*||K)$, $M_1^* = h(ID_i^*||B^*{}_i||R^*{}_1||T_1)$. GW checks whether $M_1^* ? = M_1$ holds. If this condition holds, GW accepts that U_i is authentic and proceeds to the next step; otherwise, it aborts this session.

Step 4: GW generates a random number R_2 and then calculates $SK_{GW-SN_j} = h(ID_{SN_j}||K)$, $M_3 = h(h(h(ID_i \parallel R_1{}^* \parallel R_2) \parallel \text{"1"}) \parallel SK_{GW-SN_j} \parallel R_2)$, $M_4 = h(ID_i||R_1||R_2) \oplus SK_{GW-SN_j}$, $M_5 = R_2 \oplus h(SK_{GW-SN_j})$. Finally, GW sends $\langle M_3, M_4, M_5 \rangle$ to SN_j.

Step 5: SN_j calculates $R'_2 = M_5 \oplus h(SK_{GW-SN_j})$, $M'_6 = M_4 \oplus SK_{GW-SN_j}$, $M'_3 = h(h(M'_6 \parallel \text{"1"}) \parallel SK_{GW-SN_j} \parallel R'_2)$, and then checks whether $M'{}_3 ? = M_3$ holds. If it is true, SN_j generates a random number R_3 and computes $SK = h(M'{}_6||R'{}_2||R_3)$, $M_7 = h(SK||R_3||SK_{GW-SN_j})$, $M_8 = h(R'_2) \oplus R_3$. Finally, SN_j sends $\langle M_7, M_8 \rangle$ to GW.

Step 6: After receiving $\langle M_7, M_8 \rangle$, GW computes $R'{}_3 = M_8 \oplus h(R_2)$, $SK' = h(h(ID_i||R_1||R_2)||R_2||R'{}_3)$, $M'_7 = h(SK'||R'_3||SK_{GW-SN_j})$ and then checks whether $M'{}_7 ? = M_7$ holds. If it is incorrect, GW aborts the session, otherwise, it generates a new unique identity $TID'_i (\neq TID_i)$ for U_i and then computes $M_9 = R_2 \oplus h(ID_i||R_1)$, $M_{10} = h(ID_i||SK'||R'{}_3)$, $M_{11} = TID'_i \oplus h(R_2 \oplus R_3)$. Finally, GW sends $\langle M_8, M_9, M_{10}, M_{11} \rangle$ to U_i.

Step 7: After receiving $\langle M_8, M_9, M_{10}, M_{11} \rangle$, U_i computes $R_2{}^* = M_9 \oplus h(ID_i||R_1)$, $R_3{}^* = M_8 \oplus h(R_2{}^*)$, $TID'_i = M_{11} \oplus h(R_2{}^* \oplus R_3{}^*)$, $M_{10}^* = h(ID_i||SK^*||R_3{}^*)$ and then checks whether $M_{10}^* ? = M_{10}$ holds. If it is correct, U_i believes that $\langle M_8, M_9, M_{10}, M_{11} \rangle$ is valid and then sends a confirmation message to GW. The mobile device now updates old TID_i with the newTID'_i.

Step 8: GWcomputes new value $D_i{}' = R_i \oplus h(TID_i{}'||K)$ and replaces$\langle TID_i, D_i \rangle$ with $\langle TID_i{}', D_i \rangle$.

2.5. Password change phase

This phase is executed to update the old password to a new one. The details are presented as follows.

Step 1: U_i inputsID_i and PW_i into the mobile device. Then, it performs $HPW_i^* = h(ID_i \oplus PW_i)$, $R_i^* = A_i \oplus HPW_i$, $\text{Reg}^*{}_i = h(ID_i||R^*{}_i||HPW_i^*)$ and checks whether $\text{Reg}^*{}_i ? = \text{Reg}_i$is correct. If it is false, the mobile device aborts the password change phase, otherwise, proceeds to the next step.

Step 2: After verifying the legitimacy of U_i, the mobile device requests U_i to enter new password.

Step 3: U_i inputs a new password PW_i^{new}, then the mobile device calculates $HPW_i^{new} = h(ID_i \oplus PW_i^{new})$, $Reg^{new}{}_i = h(ID_i||R^*{}_i||HPW_i^{new})$, $A_i^{new} = R^*{}_i \oplus HPW^{new}{}_i$, $B_i = h(ID_i||R_i||K)$, $C_i^{new} = B_i \oplus h(ID_i \oplus R_i{}^* \oplus HPW_i^{new})$. Finally, the mobile device stores $\langle Reg_i^{new}, A_i^{new}, C_i^{new} \rangle$ into the mobile device. Thus, U_i can easily change the password without involvement of *GW*.

3. Weaknesses of Amin et al.'s protocol

Before presenting the cryptanalysis of Amin et al.'s protocol, we first give the adversary model, i.e., the capability of the adversary [22]. 1) The adversary may capture all messages sent or received in the authentication session. 2) The adversary may obtain a stolen or lost mobile device of the user, and then extract the secret parameters in the device by side channel attacks.

In [7], Amin et al. claimed that their protocol can withstand various attacks even if the mobile device is stolen. However, we observe that Amin et al.'s protocol is prone to stolen mobile device attack, desynchronization attack, and secret sensor key exposure. So Amin et al.'s protocol is not ready for practical deployment.

3.1. Stolen mobile device attack

Passwords, which are chosen by users, are potentially prone to password guessing attack, including online password guessing and offline password guessing attack. Stolen mobile device attack is actually offline password guessing attack in the case that the mobile device is lost/stolen. Specifically, an adversary launches offline password guessing attack with the parameters stored in the mobile device, in addition to the captured messages of the authentication session.

In [7], it is assumed that the probability of guessing ID_i and PW_i using Reg_i is negligible. However, Wang et al. [24] pointed out that the identity of a user can be revealed by the attacker when the user's device is stolen. Thus it is more prudent to take this risk into consideration.

Suppose that the mobile device is stolen or lost, and then the attacker A reveals the parameters $\langle TID_i, \mathrm{Reg}_i, A_i, C_i, h(.) \rangle$ from the card. With the secret information $Reg_i = h(ID_i||R_i||HPW_i)$, $A_i = R_i \oplus HPW_i$, A may derive $R_i = A_i \oplus HPW_i$ and $Reg_i = h(ID_i||(A_i \oplus HPW_i)||HPW_i) = h(ID_i||(A_i \oplus (h(ID_i \oplus PW_i)))||(h(ID_i \oplus PW_i)))$, and mount offline password guessing attack described below.

(1) A chooses a possible ID_i^* and PW_i^*, and computes $Reg_i^* = h(ID_i^*||(A_i \oplus (ID_i^* \oplus PW_i^*))||(ID_i^* \oplus PW_i^*))$.
(2) A validates whether $Reg_i ? = Reg_i^*$ holds. If it is positive, A has sought out the correct pair of identity and password. Otherwise, A repeats the steps 1) and 2) until the correct password is found.

Therefore, their protocol is vulnerable to stolen mobile device attack.

3.2. Desynchronization attack

In Amin et al.'s protocol, U_i and *GW* update to a new temporary identity TID'_i in each successful authentication session. Specifically, *GWN* generates a new random number TID'_i, computes and sends $M_{11} = TID'_i \oplus h(R_2 \oplus R_3)$ to U_i via the message $< M_8, M_9, M_{10}, M_{11} >$. After receiving this message, U_i updates the temporary identity to TID'_i before it sends the confirmation message to *GW*. On receiving the confirmation message, *GW* updates the original entry $< TID_i, D_i >$ of U_i to $< TID'_i, D'_i >$.

However, Ami et al.'s protocol only takes into consideration the ideal situation in which each message is successfully received by the intended entities. The dependence on successful message delivery is a weakness that may cause desynchronization of some critical parameters. Specifically, if the confirmation message in the authentication phase is not successfully delivered to *GW*, U_i updates the temporary identity to TID'_i, while *GW* still keeps the old temporary identity. Consequently, U_i and *GW* are desynchronized on the value of the temporary identity and any subsequent login and authentication request of U_i is rejected. While U_i is using the new TID'_i, *GW* expects U_i to use the old value TID_i. U_i's following login requests will be taken by *GW* as illegitimate requests, since there are no entry with TID'_i in the table. Thus the login request with TID'_i will be denied. The detail of desynchronization attack is illustrated in Fig. 2.

3.3. Sensor key exposure

In the authentication phase, if U_i is legitimate, *GW* sends $\langle M_3, M_4, M_5 \rangle$ to SN_j, where R_2 is a random number, $M_3 = h(h(h(ID_i \parallel R_1{}^* \parallel R_2) \parallel \text{"1"}) \parallel SK_{GW-SN_j} \parallel R_2)$, $M_4 = h(ID_i||R_1{}^*||R_2) \oplus SK_{GW-SN_j}$, $M_5 = R_2 \oplus h(SK_{GW-SN_j})$. If $h(ID_i||R_1{}^*||R_2)$ or R_2 is compromised, the sensor secret can be derived by computing $SK_{GW-SN_j} = h(ID_i||R_1{}^*||R_2) \oplus M_4$, and the hash of SK_{GW-SN_j} can also be derived by computing $h(SK_{GW-SN_j}) = R_2 \oplus M_5$. Therefore, Amin et al.'s protocol suffers from the problem of sensor key exposure.

4. Our improved protocol

As is indicated by Wang et al. [24], it is a necessity to employ public key primitives to avoid stolen mobile device attack and desynchronization attack. We enhance Amin et al.'s protocol in the following aspects. (1) The public key primitive

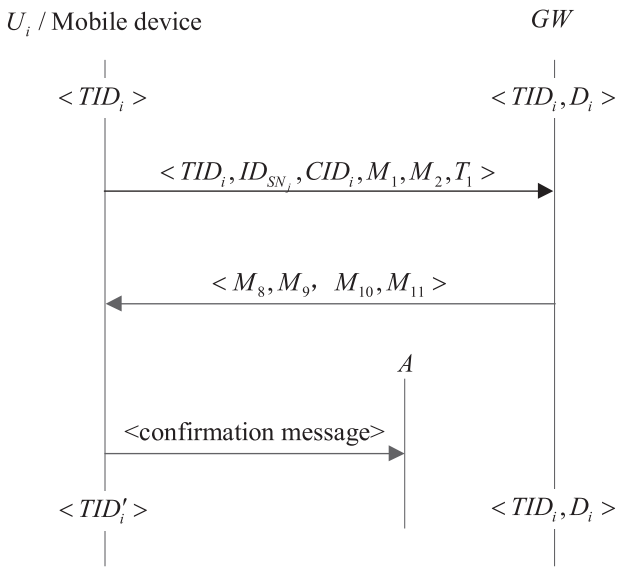

Fig. 2. Desynchroniazation attack on Amin et al's protocol.

quadratic residues is employed to avoid the first two attacks. (2) The concept of fuzzy verifier is adopted to achieve the feature of local password verification. (3) The hash function and timestamp mechanism are used to secure the interaction between gateway and sensor nodes. Our improved protocol also has 5 phases: setup, medical professional registration, patient registration, login and authentication, password change.

4.1. Setup phase

The registration center *GW* first generates two large primes p and q, and computes $n=pq$, and keeps p and q as the private key. Then it chooses a long-term secret key K.

4.2. Medical professional registration phase

This phase is executed by a medical professional U_i before providing medical services. The details are presented as follows, see Fig. 3.

Step 1: U_i picks an identityID_i, a password PW_i, generates a random number a, and then computes $HPW_i=h(a\oplus PW_i)$. Then, he/she sends $\langle ID_i, HPW_i\rangle$ to *GW* securely.

Step 2: On receiving $\langle ID_i, HPW_i\rangle$, *GW* chooses an integer $2^4 \le m \le 2^8$, a random number R_i for U_i, computes $Reg_i=h(h(ID_i||R_i||HPW_i)modm)$, $A_i=R_i\oplus HPW_i$, $B_i=h(ID_i||R_i||K)$, $C_i=B_i\oplus h(ID_i\oplus R_i\oplus HPW_i)$. Reg_i is a fuzzy verifier.

Step 3: *GW* stores $\langle ID_i, R_i\rangle$in a table for further use and forwards $\langle Reg_i, A_i, C_i, m, n, h(\cdot)\rangle$ to U_i securely. After receiving $\langle Reg_i, A_i, C_i, m, n, h(\cdot)\rangle$, U_i stores $\langle Reg_i, A_i, C_i, m, n, a, h(\cdot)\rangle$ into his/her mobile device.

4.3. Patient registration phase

At first, the patient selects and forwards his/her name to the registration center and then it selects an appropriate sensor kit and appoints a medical professional. The registration center computes a secret key $SK_{GW-SN_j} = h(ID_{SN_j}||K)$ for SN_j and forwards patient's identity and relevant data about medical sensors to the corresponding medical professional.

4.4. Login and authentication phase

In this phase, the participants are mutually authenticated, and a session key is established between U_i and SN_j. The details are presented as follows, see Fig. 4.

Step 1: U_i inputs ID_i and PW_i into the mobile device. Then, it calculates $HPW_i^*=h(a\oplus PW_i)$, $R_i^*=A_i\oplus HPW_i$, $Reg_i^* = h(h(ID_i||R_i^*||HPW_i^*)modm)$, and verifies whether $Reg^*{}_i ? = Reg_i$ holds. If it is not true, the mobile device rejects the login request; otherwise, it proceeds to the next step.

Step 2: The mobile device generates a random nonce R_1, calculates $B_i^*=C_i\oplus h(ID_i\oplus R_i^*\oplus HPW_i^*)$, $CID_i = (ID_i||R_1)^2 \bmod n$, $M_1 = h(ID_i||B_i^*||R_1||T_1)$, and then sends $< ID_{SN_j}, CID_i, M_1, T_1 >$ to *GW*.

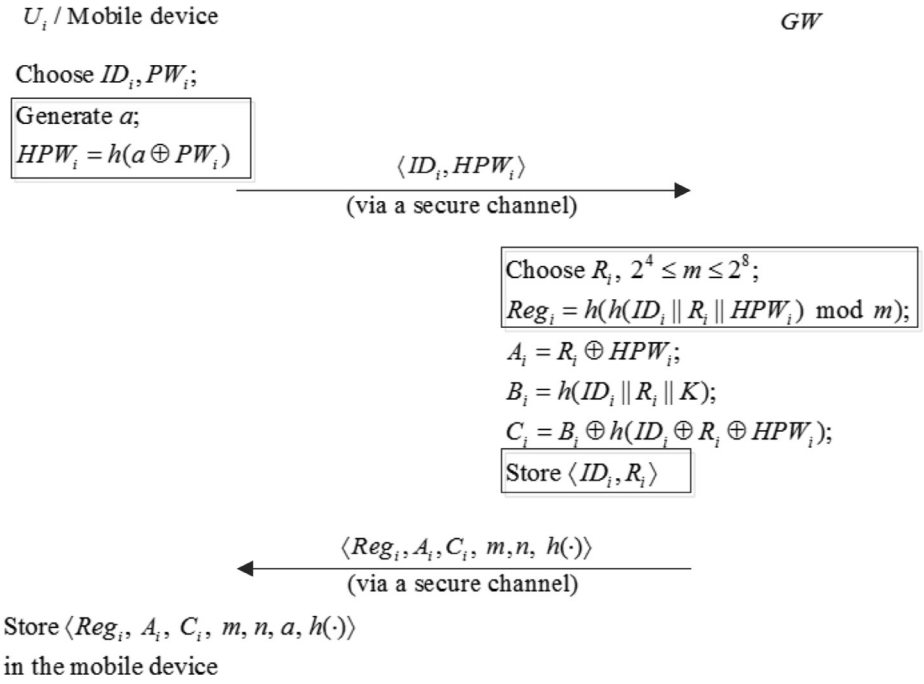

Fig. 3. User registration phase of the improved protocol.

Step 3: *GW* decrypts CID_i using p and q to get ID_i^* and R_1^*, and retrieves $R_i{}^*$ according to ID_i^*. If there exists a valid entry in the table, *GW* continues; otherwise, it rejects the login request. Next, *GW* computes $B_i{}^* = h(ID_i||R_i{}^*||K)$, $M_1{}^* = h(ID_i{}^*||B_i{}^*||R_1{}^*||T_1)$, and checks whether $M_1^* ? = M_1$ holds. If it holds, *GW* accepts that U_i is authentic and proceeds to the next step; otherwise, it aborts this session.

Step 4: *GW* generates a random number R_2 and calculates $SK_{GW-SN_j} = h(ID_{SN_j}||K)$, $M_2 = h(ID_i^*||R_1^*||R_2)$, $M_3 = h(h(M_2 \| \text{"1"}) \| SK_{GW-SN_j} \| R_2 \| T_2)$, $M_4 = M_2 \oplus h(SK_{GW-SN_j}||T_2)$, $M_5 = R_2 \oplus h(SK_{GW-SN_j}||T_2)$. Finally, *GW* sends $< M_3, M_4, M_5, T_2 >$ to SN_j.

Step 5: SN_j calculates $R_2' = M_5 \oplus h(SK_{GW-SN_j}||T_2)$, $M_2' = M_4 \oplus h(SK_{GW-SN_j}||T_2)$, $M_3' = h(h(M_2' \| \text{"1"}) \| SK_{GW-SN_j} \| R_2' \| T_2)$, and then checks whether $M'_3 ? = M_3$ holds. If it is true, SN_j randomly chooses a number R_3 and computes $SK = h(M'_2||R'_2||R_3)$, $M_6 = h(SK||R_3||SK_{GW-SN_j})$, $M_7 = h(R'_2) \oplus R_3$. Finally, SN_j sends $< M_6, M_7 >$ to *GW*.

Step 6: After receiving $< M_6, M_7 >$, *GW* computes $R'_3 = M_7 \oplus h(R_2)$ $SK' = h(h(ID_i^*||R_1||R_2)||R_2||R'_3)$, $M'_6 = h(SK'||R'_3||SK_{GW-SN_j})$ and then checks whether $M'_6 \neq M_6$ holds. If it is incorrect, *GW* aborts the connection, otherwise, compute $M_8 = R_2 \oplus h(ID_i^*||R_1)$, $M_9 = h(ID_i^*||SK'||R'_3)$. Finally, *GW* sends $< M_7, M_8, M_9 >$ to U_i.

Step 7: After receiving $< M_7, M_8, M_9 >$, U_i computes $R_2^* = M_8 \oplus h(ID_i||R_1)$, $R_3^* = M_7 \oplus h(R_2^*)$, $SK^* = h(h(ID_i||R_1||R_2^*)||R_2^*||R_3^*)$, $M_9 = h(ID_i||SK^*||R_3^*)$ and then checks whether $M_9^* \neq M_9$ holds. If it is correct, U_i believes that he/she is communicating with legal *GW* and SN_j.

4.5. Password change phase

This phase is performed when updating the old password to a new one. The details are presented as follows, see Fig. 5.

Step 1: U_i inputsID_i and PW_i into the mobile device. Then, it performs $HPW_i{}^* = h(a \oplus PW_i), R_i{}^* = A_i \oplus HPW_i, Reg_i^* = h(h(ID_i||R_i^*||HPW_i^*) mod m)$and checks whether $Reg_i^* ? = Reg_i$ holds. If it is positive, the mobile device proceeds to Step 2; otherwise, it terminates the process of password change.

Step 2: After verifying the legitimacy of U_i, the mobile device requests U_i to enter new password.

Step 3: U_i inputs a new password $PW_i{}^{new}$, then the mobile device calculates $HPW_i{}^{new} = h(Ia \oplus PW_i{}^{new})$, $Reg_i^{new} = h(h(ID_i||R_i^*||HPW_i^{new}) modn)$, $A_i{}^{new} = R^*{}_i \oplus HPW^{new}{}_i$, $B_i = h(ID_i||R_i||K)$, $C_i{}^{new} = B_i \oplus h(ID_i \oplus R_i{}^* \oplus HPW_i{}^{new})$. Finally, the mobile device stores $\langle Reg_i{}^{new}, A_i{}^{new}, C_i{}^{new} \rangle$into the mobile device. Thus, U_i can easily change the password without interacting with *GW*.

5. Security and efficiency analysis

We first present that the improved protocol is capable of defending various known attacks and provides the security features required for WHMSs through detailed security analysis. Then we present the security comparison and efficiency analysis.

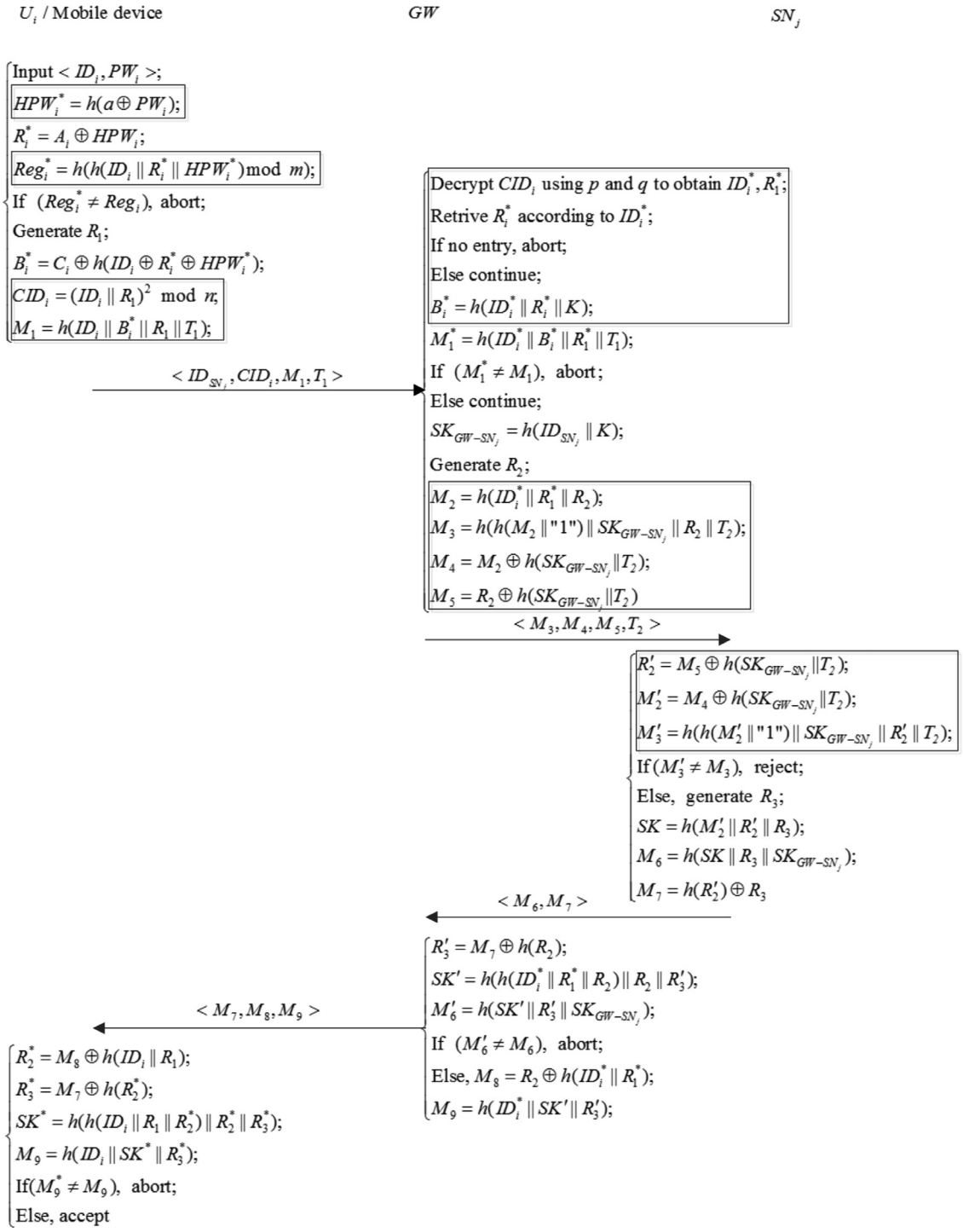

Fig. 4. Authentication and key agreement of the improved protocol.

5.1. Security analysis

This subsection not only shows that our improved protocol could overcome weaknesses in Amin et al.'s authentication protocol, but also shows that our improved protocol achieves all the desired security features.

Suppose that $n=pq$, where p and q are two large primes. If y has a square root x, i.e., there is a solution for $y=x^2 mod\ n$, then y is a quadratic residue mod n. The quadratic residue problem is defined as follows [23].

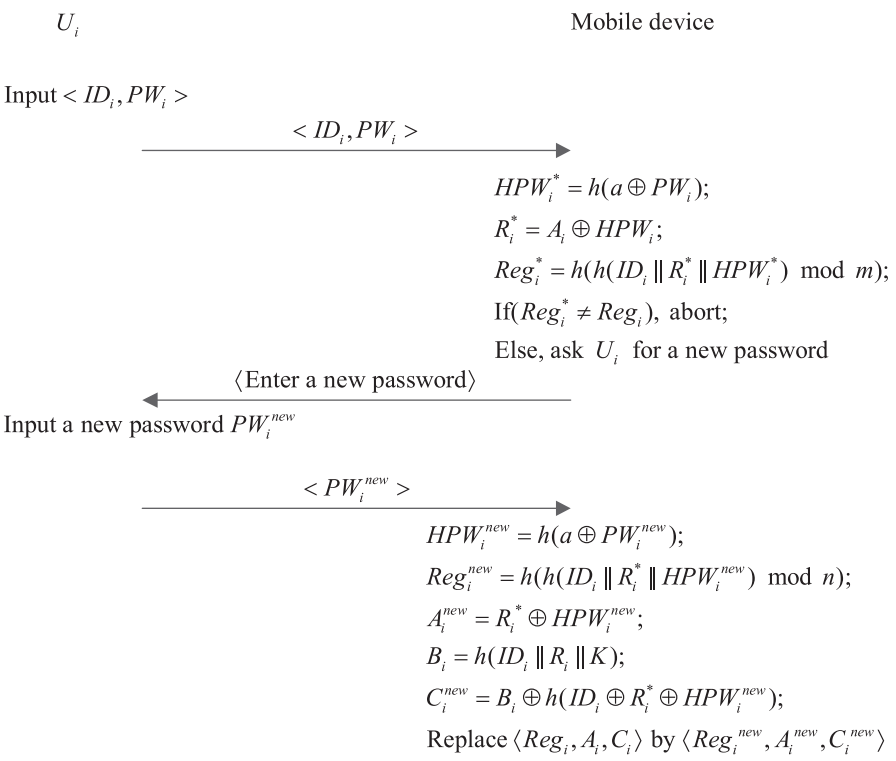

Fig. 5. Password change phase of our improved protocol.

For $y \in QR_n$, where QR_n is the set of all quadratic residues mod n, it is computationally infeasible to find x without the knowledge of p and q due to the hardness of factoring n .

5.1.1. Resisting stolen mobile device attack

We first show how our improved protocol resists the stolen mobile device attack. Suppose that the opponent A has obtained the lost mobile device of U_i and extracted the parameters $\langle Reg_i, A_i, C_i, m, n, a, h(\cdot)\rangle$ from the device. Then A guesses ID_i^* and PW_i^*, and computes $Reg_i^* = h(ID_i^* || (A_i \oplus (ID_i^* \oplus PW_i^*)) || (ID_i^* \oplus PW_i^*) mod m)$. However, A cannot definitely find out the correct pair ID_i^* and PW_i^* by checking the equation $Reg_i^* = Reg_i$, because Reg_i is a "fuzzy verifier" [24].

Moreover, our improved protocol also resists stolen mobile device attack even when A could intercept the message $< ID_{SN_j}, CID_i, M_1, T_1 >$ sent by U_i in the authentication phase. A can derive $B_i^* = C_i \oplus h(ID_i \oplus R_i^* \oplus HPW_i^*)$ where $HPW_i{}^* = h(a \oplus PW_i^*)$, $R_i{}^* = A_i \oplus HPW_i^*$. Due to the hardness of quadratic residue problem, it is impossible for the adversary to compute R_1. A is unable to calculate $M_1^* = h(ID_i || B_i^* || R_1 || T_1)$, which is a necessity to check the validity of PW_i^*. Therefore, A cannot verify the correctness of the conjectured ID_i^* and PW_i^* through checking the equation $M_1^* = M_1$.

Above all, our improved protocol is completely secure against stolen mobile device attack.

5.1.2. Resisting desynchronization attack

In Amin et al.'s protocol, U_i updates its temporary identity to a new one after every successful authentication session. Specifically, in each session, U_i update its temporary identity to a new one first, and GW update the temporary identity of U_i after receiving the confirmation message. That is, there is a synchronization between U_i and GW. In our improved protocol, there is no such synchronization. As a result, it is easy to see that desynchronization attack is impossible in our improved protocol.

5.1.3. Resisting sensor key exposure

In Amin et al.'s protocol, the sensor key SK_{GW-SN_j} which is shared between S_j and GW is used to protect the ephemeral random numbers. This usage will cause the dependence between the random numbers and the master sensor key. As is shown in Section 3.3, the compromise or leakage of random numbers will leads to the compromise or leakage of master sensor key. In our improved protocol, we avoid this risk by introducing the mechanisms of timestamp and hash. Specifically, we compute $M_4 = M_2 \oplus h(SK_{GW-SN_j} || T_2)$ and $M_5 = R_2 \oplus h(SK_{GW-SN_j} || T_2)$. In this case, even though $h(ID_i || R_1{}^* || R_2)$ or R_2 is compromised, the opponent can only obtain the hashed value $h(SK_{GW-SN_j} || T_2)$ of SK_{GW-SN_j}. Due to the unidirectionality of hash algorithm, the opponent cannot reveal the master sensor key. Thus our improved protocol is immune from sensor key exposure.

5.1.4. Resisting medical professional impersonation attack

Assume that an opponent A has the user U_i's mobile device and extracted the data $\langle Reg_i, A_i, C_i, m, n, a, h(\cdot)\rangle$ stored in it, where $Reg_i = h(h(ID_i||R_i||HPW_i) mod m)$, $C_i = B_i \oplus h(ID_i \oplus R_i \oplus HPW_i)$. A has to possess both PW_i and the mobile device to produce a legal message $< ID_{SN_j}, CID_i, M_1, T_1 >$. Specifically, the key to prove the legitimacy of U_i is the value $M_1 = h(ID_i||B_i^*||R_1||T_1)$. The most critical component of the computation of M_1 is the value $B_i^* = C_i \oplus h(ID_i \oplus R_i^*||HPW_i^*)$. However, without either PW_i or the mobile device, A cannot calculate B_i^*. Moreover, even if A has compromised the user password, A still cannot calculate B_i^* without the value $C_i = B_i \oplus h(ID_i \oplus R_i \oplus HPW_i)$ stored in the mobile device. Therefore, our improved protocol could resist medical professional impersonation attack even when either the password or the mobile device is compromised.

5.1.5. Resisting gateway impersonation attack

Since the message $< M_3, M_4, M_5, T_2 >$ sent from GW to SN_j is protected by the hash mechanism using the shared key SK_{GW-SN_j} between GW and SN_j. Without knowing SK_{GW-SN_j}, the opponent A cannot compute a valid $M_3 = h(h(M_2 \parallel \text{"1"}) \parallel SK_{GW-SN_j} \parallel R_2 \parallel T_2)$. That is, A cannot forge the message $< M_3, M_4, M_5, T_2 >$.

The message $< M_7, M_8, M_9 >$ sent from GW to U_i is protected by the $M_9 = h(ID_i||SK^*||R_3^*)$. To compute a valid value M_9, A has to have a knowledge of R_1 to compute the value $SK^* = h(h(ID_i||R_1||R_2^*)||R_2^*||R_3^*)$. To get R_1, A has to know the secret key p and q of GW. It is impossible since the secret key is carefully protected by the administrator. The other way left to A is to decrypt the value $CID_i = (ID_i||R_1)^2 \bmod n$, which is computationally infeasible due to hardness of quadratic residue problem.

Hence, the improved protocol can defend gateway impersonation attack.

5.1.6. Resisting sensor node impersonation attack

Since the message $< M_6, M_7 >$ sent from SN_j to GW is protected by the hash mechanism using the shared key SK_{GW-SN_j} between GW and SN_j. Without knowing SK_{GW-SN_j}, the opponent A cannot compute a valid $M_6 = h(SK||R_3||SK_{GW-SN_j})$. That is, A cannot forge the message $< M_6, M_7 >$.

Thus, the improved protocol can resist sensor node impersonation attack.

5.1.7. Resisting modification attack

Assume that an opponent A intercepts these messages, such as $< ID_{SN_j}, CID_i, M_1, T_1 >$, $< M_3, M_4, M_5, T_2 >$, $< M_6, M_7 >$, $< M_7, M_8, M_9 >$, and then transmits modified messages. However, all these messages are protected by a hash value computed with a secret value. For instance, in the first message $< ID_{SN_j}, CID_i, M_1, T_1 >$, A cannot calculate $M_1 = h(ID_i||B_i^*||R_1||T_1)$, since $B_i^* = C_i \oplus h(ID_i \oplus R_i^*||HPW_i^*)$ is a secret value which cannot be computed without knowing either C_i or PW_i. Any modification will be detected by the message receiver who will check the hash value in the message. Therefore, our improved protocol is capable of defending modification attack.

5.1.8. Resisting replay attack

Suppose that an opponent A could replay these captured messages, such as $< ID_{SN_j}, CID_i, M_1, T_1 >$, $< M_3, M_4, M_5, T_2 >$, $< M_6, M_7 >$, $< M_7, M_8, M_9 >$. In our improved protocol, timestamp is employed in the first two messages. Then GW and S_j could discover message replay through validating the freshness of timestamps.

On the other hand, the third message contains a random number R_2 which is sent by GW. If it is replayed, GW will observe the duplication immediately. Similarly, the fourth message also includes a random value R_1 which is selected by U_i. U_i can also detect the replayed messages in the same way.

Moreover, A has no way to bypass receiver's validation of timestamp or random number, as these messages are protected by a hash value computed with a secret value. Therefore, our improved protocol could defend replay attack.

5.1.9. Mutual authentication

Mutual authentication provides a first line of defense for all systems. In our proposed protocol, an adversary cannot generate legal $M_1 = h(ID_i||B_i^*||R_1||T_1)$ without knowing U_i's private key B_i^*. So GW can authenticate U_i by verifying the correctness of M_1. Similarly, U_i can authenticate GW by verifying the correctness of $M_9 = h(ID_i||SK^*||R_3^*)$. Hence, our improved protocol achieves mutual authentication between U_i and GW.

As for the interaction between GW and S_j, S_j can authenticate GW by verifying the correctness of $M_3 = h(h(M_2||\text{"1"})||SK_{GW-SN_j}||R_2||T_2)$. At the same time, GW could authenticate S_j by verifying the correctness of $M_6 = h(SK||R_3||SK_{GW-SN_j})$. Hence, our improved protocol also achieves mutual authentication between GW and S_j.

5.1.10. Session key agreement

Special attentions have been paid to the security and usability of health data at rest [24,25]. In this paper, we provide session key agreement to protect the data in transit. In the improved protocol for WHMSs, U_i and S_j share the session key $SK = h(h(ID_i||R_1||R_2)||R_2||R_3)$ to protect future communication. Note that, the security of the session key depends on the secrecy of these involved random numbers. As is presented in Section 4, all these values are carefully protected by the secret values shared between the participants. Therefore, our improved protocol could provide session key agreement. All of the following data transmission will be protected by the session key, which will be protected from eavesdropping, modification, or deletion. As a result, a shared key is established in our protocol.

Table 1
Comparison of security features.

	He et al.'s protocol [10]	Amin et al.'s protocol [7]	Our protocol
Resisting stolen mobile device attack	✗	✗	√
Resisting desynchronization attack	✗	✗	√
Resisting sensor key exposure	√	✗	√
Resisting user impersonation attack	√	√	√
Resisting gateway impersonation attack	√	√	√
Resisting sensor node impersonation attack	√	√	√
Resisting modification attack	√	√	√
Resisting replay attack	√	√	√
Mutual authentication	√	√	√
Secure key agreement	√	√	√
Known key security	√	√	√
User anonymity	√	√	√
User untraceability	√	√	√

5.1.11. Known key security

Suppose the session key $SK = h(h(ID_i||R_1||R_2)||R_2||R_3)$ of current session is disclosed to the opponent A. However, he/she can compute none of the past and future session keys using SK. Since the session key is protected by $h(\cdot)$ and the random numbers $< R_1,R_2,R_3 >$ are different in each session. As a result, our improved protocol achieves known key security.

5.1.12. Anonymity

Suppose the opponent A first has captures all the messages transmitted between the participants during the protocol execution and then tries to guess the identity of the user. From the description of the protocol, U_i's identity ID_i is involved in the field $CID_i = (ID_i||R_1)^2 \bmod n$ in the first message. To get ID_i, A has to know the secret key p and q of GW. It is impossible since the secret key is carefully protected by the administrator. The other way left for A to obtain ID_i is to decrypt the value $CID_i = (ID_i||R_1)^2 \bmod n$, which is computationally infeasible due to the hardness of quadratic residue problem. Hence, our improved protocol fulfills user anonymity.

5.1.13. Untraceability

In each authentication session of our protocol, each field of these messages $< ID_{SN_j}, CID_i, M_1, T_1 >$, $< M_3,M_4,M_5,T_2 >$, $< M_6,M_7 >$, $< M_7,M_8,M_9 >$ is dynamic. Specifically, R_1 is randomly selected, in turn, CID_i is different in each session. In addition, as R_2 and R_3 are also randomly chosen, all fields in these messages are different for each session. Thus, the proposed protocol fulfills user untraceability.

5.2. Security comparisons

We compare our improved protocol with the ones in [10] and [7], and the results of comparison are summarized in Table 1.

From Table 1, it is easy to know that both He et al.'s protocol and Amin et al.'s protocol are susceptible to several attacks, e.g., stolen mobile device attack and desynchronization attack. Moreover, Amin et al.'s protocol is prone to sensor key exposure. Our improved protocol could provide more adequate security protection because it can meet all security requirements. Our protocol is the only one that resists all known attacks and provides all the desired security features.

5.3. Efficiency analysis

We compare the efficiency of the improved protocol with that of state of the art protocols [7,8,10,11, 31]. We concern login and authentication phase and ignore the bit XOR operation which is very efficient. T_H, T_S, T_M, T_{QR} denote the cost for executing the hash, the symmetric encryption/decryption, the modular squaring, and the computation of a square root modulo n, respectively.

Table 2 shows comparison results of the improved protocol and the earlier ones [7,8,10,11,13]. Our protocol is more efficient than the previous ones at the side of medical professional. The sensor node in our protocol needs one more hash operation than Amin et al.'s porotocol. Since hash operation is very lightweight, it does not incur much energy cost for sensor nodes. Although the computation cost for the gateway of our proposed scheme is higher than that of Amin et al.'s protocol, generally, it is not a concern, because the gateway is powerful and has no resource constraints. Moreover, Amin et al.'s protocol [7] is prone to stolen mobile device attack, desynchronization attack, and sensor key exposure.

6. Conclusion

Wearable health monitoring systems which enable smart and ubiquitous healthcare will play a pivotal role in future e-healthcare. Due to its high sensitivity, the health data in transit should be protected from unauthorized access. In this

Table 2
Efficiency comparisons.

	U_i	GWN	S_j	Total
Kumar et al.'s protocol [8]	$4T_H+2T_S$	$1T_H+3T_S$	T_H+2T_S	$6T_H+7T_S$
He et al.'s protocol [10]	$4T_H+2T_S$	$2T_H+5T_S$	$1T_H+2T_S$	$7T_H+9T_S$
Wu et al.'s protocol [11]	$10T_H+2T_S$	$6T_H+5T_S$	$4T_H+1T_S$	$20T_H+8T_S$
Li et al.'s protocol [13]	$6T_H+2T_S$	$7T_H+6T_S$	$5T_H+2T_S$	$18T_H+10T_S$
Amin et al.'s protocol [7]	$12T_H$	$16T_H$	$6T_H$	$34T_H$
Our protocol	$9T_H+1T_M$	$14T_H+1T_{QR}$	$7T_H$	$30T_H+1T_M+1T_{QR}$

context, an end-to-end mutual authentication protocol is the key ingredient to enable secure communication between the wearable sensor and medical professionals. However, it is not an easy task to design a secure and efficient authentication protocol. In this paper, we have analyzed an anonymity preserving mutual authentication protocol by Amin et al. Although Amin et al.'s protocol has many salient features compared with these previous protocols, we have revealed that the login and authentication phase of Amin et al.'s protocol still fails to resist three subtle attacks. First, their protocol suffers from stolen mobile device attack, in which the user identity and password can be exhaustively guessed in an offline manner with the secrets stored in the stolen mobile device. Second, their protocol is prone to desynchronization attack. A legal user can be prevented from accessing the sensor data by blocking the confirmation message in the authentication phase. Third, the protocol suffers from sensor key exposure. The disclosure of temporal parameters in the authentication session will lead to the exposure of the sensor secret key. To overcome those weaknesses, we have proposed an improved end-to-end authentication protocol based on quadratic residues. Comprehensive security analysis is presented to demonstrate that the proposed protocol is capable of resisting various known attacks and those flaws of Amin et al.'s protocol. We also compared the proposed protocol with the previous ones in aspect of security features and computational cost, and the results show that our protocol meets all security requirements and provides more adequate security protection. As a result, our protocol is ready for practical use in wearable health monitoring systems.

Acknowledgments

This work is supported by Supported by National Natural Science Foundation of China (Program Nos. 61672413, U1405255, U1536202, 61372075, 61672415, 61671360), National High Technology Research and Development Program (863 Program) (Program No. 2015AA016007), Natural Science Basic Research Plan in Shaanxi Province of China (Program No.2016JM6005), Fundamental Research Funds for the Central Universities (Program Nos. JB161501, JBG161511), the China 111 Project (No. B16037), the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET).

References

[1] Pantelopoulos A, Bourbakis N G. A survey on wearable sensor-based systems for health monitoring and prognosis. IEEE Trans Syst Man Cybern Part C (Appl Rev) 2010;40(1):1–12.
[2] Xia Z, Wang X, Zhang L, Qin Z, Sun X, Ren K. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans Inf Forensics Secur 2016;11(11):2594–608. doi:10.1109/TIFS.2016.2590944.
[3] Xia Z, Wang X, Sun X, Wang Q. A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data. IEEE Trans Parallel Distrib Syst 2015;27(2):340–52 2016.
[4] Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. ACM Comput Surv (CSUR) 2012;45(1):3.
[5] Arshad H, Nikooghadam M. Design of a secure authentication and key agreement scheme preserving user privacy usable in telecare medicine information systems. J Med Syst 2016;40(11):237.
[6] Diez F P, Touceda D S, Camara J M S, Zeadally S. Toward self-authenticable wearable devices. IEEE Wirel Commun 2015;22(1):36–43.
[7] Amin R, Islam SK H, Biswas G P, Khan K M, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Fut Gener Comput Syst 2016. http://dx.doi.org/10.1016/j.future.2016.05.032.
[8] Kumar P, Lee S-G, Lee H-J. E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors 2012;12(2):1625–47.
[9] Khan M K, Kumari S. An improved user authentication protocol for healthcare services via wireless medical sensor networks. Int J Distrib Sens Netw 2014:10. http://dx.doi.org/10.1155/2014/347169.
[10] He D, Kumar N, Chen J, Lee C-C, Chilamkurti N, Yeo S S. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimed Syst 2013;21(1):49–60.
[11] Wu F, Xu L, Kumari S, Li X. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimed Syst 2015. http://dx.doi.org/10.1007/s00530-015-0476-3.
[12] Mir O, Munilla J, Kumari S. Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks. Peer Peer Netw Appl 2017;10(1):79–91.
[13] Li X, Niu J, Kumari S, Liao J, Liang W, Khan M K. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Secur Commun Netw 2016;9(15):2643–55.
[14] Das A K, Sutrala A K, Odelu V, Goswami A. A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks. Wireless Person Commun 2016. doi:10.1007/s11277-016-3718-6.
[15] Li C T, Lee C C, Weng C Y. A secure cloud-assisted wireless body area network in mobile emergency medical care system. J Med Syst 2016;40(5):1–15.
[16] Liu C H, Chung Y F. Secure user authentication scheme for wireless healthcare sensor networks. Comput Electr Eng 2016. http://dx.doi.org/10.1016/j.compeleceng.2016.01.002.
[17] Li F, Hong J. Efficient certificateless access control for wireless body area networks. IEEE Sens J 2016;16(13):5389–96.
[18] Xiong H. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Trans Inf Forensics Secur 2014;9(12):2327–39.

[19] He D, Zeadally S, Kumar N, Lee J-H. Anonymous authentication for wireless body area networks with provable security. IEEE Syst J 2016 2544805. doi:10.1109/JSYST.2016.
[20] Shen J, Tan H, Moh S, Chung I, Liu Q, Sun X. Enhanced secure sensor association and key management in wireless body area networks. J Commun Netw 2015;17(5):453–62.
[21] Abdmeziem M R, Tandjaoui D. An end-to-end secure key management protocol for e-health applications. Comput Electr Eng 2015;44:184–97.
[22] Wang D, He D, Wang P, Chu C-H. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans Depend Secure Comput 2015;12(4):428–42.
[23] Rosen K. Elementary number theory and its applications. MA: Addison-Wesley; 1988.
[24] Fu Z, Wu X, Guan C, Sun X, Ren K. Towards efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inf Forensics Secur 2016;11(12):2706–16. doi:10.1109/TIFS.2016.2596138.
[25] Fu Z, Ren K, Shu J, Sun X, Huang F. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Trans Parallel Distrib Syst 2016;27(9):2546–59. doi:10.1109/TPDS.2015.2506573.

Qi Jiang received the B.S. degree in Computer Science from Shaanxi Normal University in 2005 and Ph.D. degree in Computer Science from Xidian University in 2011. He is now an associate professor at School of Cyber Engineering, Xidian University. His research interests include security protocols and wireless network security, cloud security, etc.

Jianfeng Ma received M. S. degree from Xidian University in 1992, and the Ph. D. degree from Xidian University in 1995. Currently he is a Professor at School of Cyber Engineering, Xidian University. He has published over 150 journal and conference papers. His research interests include applied cryptography, wireless network security, data security, and mobile smart system security.

Chao Yang received the Ph. D. degree from Xidian University in 2008. He is now an associate professor at School of Cyber Engineering, Xidian University. His research interests include cloud and big data security, mobile and smart computing security, etc.

Xindi Ma is currently a Ph. D. candidate of Xidian University, China. His research interests include location privacy, game theory, etc.

Jian Shen received the M.E. and Ph.D. degrees in Computer Science from Chosun University, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a professor at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer networking, and information security systems.

Shehzad Ashraf Chaudhry received his MS Computer Science with distinction, from International Islamic University, Islamabad, Pakistan in 2009. Currently he is working as Lecturer at the Department of Computer Science & Software Engineering, International Islamic University, Islamabad. His research interests include lightweight cryptography, multimedia security, etc.