Research Article

An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems

Jiaqing Mo,1 Wei Shen,1 and Weisheng Pan2

1School of Computer Science and Software, Zhaoqing University, Zhaoqing, China
2Education Technology and Computer Center, Zhaoqing University, Zhaoqing, China

Correspondence should be addressed to Jiaqing Mo; mojiaqing@126.com

Received 1 November 2019; Revised 31 January 2020; Accepted 10 February 2020; Published 23 April 2020

Copyright © 2020 Jiaqing Mo et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wearable health monitoring system (WHMS), which helps medical professionals to collect patients’ healthcare data and provides diagnosis via mobile devices, has become increasingly popular thanks to the significant advances in the wireless sensor network. Because health data are privacy-related, they should be protected from illegal access when transmitted over a public wireless channel. Recently, Jiang et al. presented a two-factor authentication protocol on quadratic residues with fuzzy verifier for WHMS. However, we observe that their scheme is vulnerable to known session special temporary information (KSSTI) attack, privileged insider attack, and denial-of-service (DoS) attack. To defeat these weaknesses, we propose an improved two-factor authentication and key agreement scheme for WHMS. Through rigorous formal proofs under the random oracle model and comprehensive informal security analysis, we demonstrate that the improved scheme overcomes the disadvantages of Jiang et al.’s protocol and withstands possible known attacks. In addition, comparisons with several relevant protocols show that the proposed scheme achieves more security features and has suitable efficiency. Thus, our scheme is a reasonable authentication solution for WHMS.

1. Introduction

At present, electronic-health (e-health) services are greatly promoted with the significant advances in computer science, wireless communication technologies, low-power sensors, and various security solutions [1–8] have been developed to build secure e-health systems. Wireless sensor network (WSN) plays an important role in e-health via sensing, measuring, gathering patient’s information for doctor’s diagnosis, or recording in the medical server. Wearable health monitoring system (WHMS), one of the most popular application of e-health notation, has attracted extensive attention in academia and industry for its mobility, flexibility, and low cost [9–12]. WHMS is a WSN, with wearable sensors installed or implanted in the body of the patient, monitors the health conditions of patients by sensing, measuring, and gathering their physiological data and sends them to the medical professional or medical center via a wireless channel for proper diagnosis and further medical treatment. With data like heart rate, blood pressure, and body temperature, doctors in distance can assess the patient’s health status. Figure 1 illustrates a typical scenario of WHMS. Advantages of providing healthcare services using WHMS are as follows:

(1) Enhance medical care quality
(2) Continuous monitoring of patients
(3) Save money and time for patients
(4) Real-time physician diagnosis and intervention

1.1. Related Works. Although WHMS provides efficiency and simplicity for medical professionals, and patients can benefit greatly from WHMS, security and privacy cannot be overlooked since the sensed data are transmitted via insecure wireless channels. Thus, it is necessary to design a robust authenticated mechanism to protect the patient’s physiological data which are sensitive and should be a secret. If the patient’s data are illegally captured and tampered by the attacker, medical professionals will make wrong diagnosis.
based on these data. Furthermore, the leaked data may be used for commercial purpose or other horrible purposes. Specifically, medical professionals should be authenticated before accessing the physiological data from the wearable sensors on the patient, and their identity and password should not be revealed if the malicious attacker eavesdrops the messages through the gateway in WHMS, and vice versa. In the meantime, a shared session key should be generated between medical professionals and the sensor node deployed on the patient’s body to protect secure communication among the communicating parties.

To address this issue, some user authentication protocols have been proposed for patient’s health monitoring [13–23]. Several authentication schemes [16–18] based on elliptical curve cryptography (ECC) have been presented because ECC can reach the identical RSA security level with faster computation and smaller key size. Although the security of these ECC-based schemes are continuously enhanced, these schemes are still not lightweight enough for WHMS since point multiplication consumes a large computation resource, while the computation capability and energy of the mobile device and sensors are limited.

Kumar et al. [24] suggested a user authentication protocol named E-SAP to monitor patient’s physiological data in wireless medical sensor network in 2012, claiming that their protocol was secure against known attacks. However, both He et al. [25] and Khan and Kumari [26] scrutinized Kumar et al.’s scheme and found some security defects like password guessing attack and lack of user anonymity and put forward their improved versions, respectively. Unfortunately, Wu et al. [20], Mir et al. [21], and Li et al. [22] independently pointed out that He et al.’s scheme [25] was vulnerable to security weaknesses, including denial-of-service attack, impersonation attack, offline guessing attack, and sensor node capture attack. To fix these loopholes, they suggested an improved version and declared that their new proposal was more secure than the previous ones. In 2016, Das et al. [27] identified the security defects in Li et al.’s protocol [28], i.e., privileged insider attack, sensor capture attack, and lack of user anonymity, and suggested an enhanced scheme based on biometrics. Later, Amin et al. [19] introduced a mutual authenticated protocol with user anonymity in WHMS and declared that their scheme was robust against the known threats. However, it was revealed by Jiang et al. [29] that this protocol suffers from several weaknesses, such as stolen mobile device attack, desynchronization attack, and sensor key exposure. To secure Amin et al.’s scheme, Jiang et al. suggested an improved two-factor (password and smartcard) scheme using quadratic residues [29, 30], fuzzy verifier [31], and timestamp mechanism. Further, security analysis showed that their scheme achieved the desired security features; thus, they had confidence in the security of their solution.

Independently, Challa et al. [32] proposed an improved three-factor (password, smartcard, and biometrics) authenticated protocol for wireless healthcare sensor network to improve the security of Liu and Chung’s scheme [23]. However, in their scheme the user communicates with the remote sensor directly which means power consumption of the sensor increases greatly, and the sensor’s lifetime will reduce rapidly. Thus, their scheme is inapplicable to the wireless healthcare sensor network. Ali et al. [33] devised an anonymous three-factor-based protocol to thwart security threats like offline password guessing attack, user impersonation attack, and known session key temporary information attack in Amin et al.’s scheme [19]. Shen et al. [34] put forward a multilayer authenticated protocol using ECC for the wireless body area network to implement secure authentication and group key generation between the sensor and the mobile device. Li et al. [35] suggested a lightweight authentication protocol for centralized WBAN with two hops while preserving anonymity and unlinkability of data transmission. Shen et al. [36] presented an efficient ECC-based pairing-free certificateless public key signature authentication protocol for WBAN with two round messages. However, according to [37, 38], these kinds of authentication protocol with just two round messages are prone to failure of perfect forward secrecy.

1.2. Motivations and Contributions. When cryptanalyzing Jiang et al.’s scheme [29], regrettably, we find that their protocol is not as robust as they claimed. Although fuzzy verifier is used to thwart offline password guessing attack in Jiang et al.’s scheme, their scheme is still vulnerable to privileged insider attack, which leads to user impersonation attack. Ridiculously, Jiang et al.’s scheme [29] is subject to KSSTI attack, which means that their protocol is vulnerable to sensor key disclosure as the previous one.
Further, we reveal that their protocol suffers from denial-of-service (DoS) attack.

Motivated by the thought of addressing the security defects in Jiang et al.’s scheme [29], we propose an improved two-factor authenticated scheme making use of quadratic residues for WHMS environment.

Our contributions of this work are threefold as listed below:

(i) First, we cryptanalyze the recent authentication scheme of Jiang et al. [29] in WHMS and find its vulnerability of KSSTI attack, privileged insider attack, and DoS attack

(ii) Second, we propose an improved secure two-factor authentication and key agreement using quadratic residues to address the security weaknesses in Jiang et al.’s protocol

(iii) Third, we provide the formal security proof of our proposed scheme under the random oracle model and conduct an informal security analysis to demonstrate that the improved scheme is secure against known attacks. Moreover, we make a performance comparison between the improved protocol and the related schemes

1.3. Organization of the Paper. The remainder of this paper is sketched as follows: Section 2 explains the preliminaries of quadratic residues and security requirements. We cryptanalyze Jiang et al.’s protocol [29] in Section 3. In Section 4, we present our improved two-factor authentication and key agreement scheme for WHMS. Next, security analysis and performance comparison are given in Section 5. Finally, the paper is concluded in Section 6.

2. Preliminaries

2.1. Quadratic Residues. According to [29, 30], the definition of quadratic residue is described as follows.

Let \( p \) and \( q \) denote two large primes, respectively, and \( n = pq \). If there is a solution for \( y = x^2 \mod n \), i.e., \( y \) has a square root, then \( y \) is called a quadratic residue mod \( n \).

Let \( Q_n \) be a set of quadratic residue numbers in \([1, n-1]\), and \( y \in Q_n \). Because of the difficulty in factoring \( n \), it is hard to find \( x \) without the knowledge of \( p \) and \( q \).

2.2. Security Requirements. It is important to understand the security requirements in designing or cryptanalyzing an authentication protocol. Hence, according to the previous works [38, 39], the security requirements of authentication protocol for WHMS are summarized as follows.

(1) Resisting Stolen Mobile Device Attack. If an unauthorized person obtains the lost/stolen mobile device, it is impossible for him to impersonate a valid user with a counterfeit login request by using the information extracted from the mobile device

(2) Resisting Impersonation Attack. The communication parties in WHMS include the user, GWN, and sensor node. It is an important requirement that the attacker is incapable of logging in WHMS to imitate a legitimate user and access the privileged resources in such a way. In addition, if the malicious attacker can impersonate the GWN to identify the legitimacy of the user in the authentication process, it means that the data in sensors can be accessed in an unauthorized manner. The authenticated scheme should also prevent the attacker from sensor node impersonation attack, in which the attacker can impersonate sensor nodes and sends bogus data to the user

(3) Resisting Known Attacks. It requires that the authentication scheme for WHMS be secure from various known basic or sophisticated attacks, such as replay attack, privileged insider attack, KSSTI attack, man-in-the-middle attack, and desynchronization attack

(4) Forward and Backward Secrecy. It requires that the attacker not be able to obtain the previous session keys or the future ones by using the compromised session key

(5) User Anonymity. It is a crucial requirement to prevent the attacker from tracing the user’s behavior to preserve user privacy

(6) Sensor Anonymity. It is an additional requirement to enhance the security of authentication protocol for WHMS, because the information sent from the sensor to medical professional is sensitive, and sensor anonymity can help confuse the intelligent attacker’s traffic analysis that may render the communication ineffective

(7) Mutual Authentication and Key Agreement. It is an essential requirement in WHMS scenario, and it requires the communication parties be able to authenticate each other and generate a shared session key to provide confidentiality of messages in wireless channel

3. Cryptanalysis on Jiang et al.’s Protocol

In this section, we cryptanalyze Jiang et al.’s protocol [29]. Due to the space limitation, the review of protocol [29] is omitted. The symbols involved are listed in Table 1.

Jiang et al. [29] criticized Amin et al.’s scheme [19] for its vulnerability of stolen mobile device attack, desynchronization attack, and sensor key exposure. To eliminate these security risks, they put forward countermeasures like public key primitive quadratic residue, the concept of fuzzy verifier, hash function, and timestamp mechanism to enhance the security of Amin et al.’s scheme. Unfortunately, we point out several security vulnerabilities in Jiang et al.’s protocol. More specifically, it is susceptible to KSSTI attack, privileged insider attack, and DoS attack. Before elaborating a security analysis, we summarize the following adversary model used in this work.
3.2. KSSTI Attack. For an authenticated protocol with key agreement, if the attacker cannot compute the session key through the session-specific temporary information such as random number which has been compromised, we say that this protocol is able to resist KSSTI attack. In Jiang et al.’s scheme, if $U_i$ is legitimate, GWN forwards message $\{M_3, M_4, M_5, T_3\}$ to $S_j$, where $M_4 = h(M_2 \oplus h(SK_{GW-Sj}||T_2))$, $M_5 = R_3 \oplus h(SK_{GW-Sj}||T_2)$, and $R_3 = M_2 \oplus h(R_3)$. Thus, it is not hard to compute the session key if the random number $R_3$ is disclosed. Therefore, Jiang et al.’s scheme is subject to KSSTI attack.

3.3. Privileged Insider Attack. The similar analysis is mentioned in Das et al. and Das [27, 47]. In the medical professional registration phase, a medical professional $U_i$ sends his registration $\{ID_1, HPW_i\}$ to GWN securely, where $HPW_i = h(r_i \oplus PW_i)$. Suppose the message $\{ID_1, HPW_i\}$ is known by an insider who is being an attacker, and further suppose that the lost/stolen mobile device containing the secret data $(Reg_i, A_i, C_i, m, n, r_i, h())$ is obtained by the attacker, he can extract all the secret information from the card using side-channel analysis [43]. Note that $A_i = R_1 \oplus HPW_i$, $C_i = B_i \oplus h(ID_1 \oplus R_1 \oplus HPW_i)$. Using these information, the attacker can carry out an attack as follows:

1. The attacker computes $R_1 = A_i \oplus HPW_i, B_i = C_i \oplus h(ID_1 \oplus R_1 \oplus HPW_i)$
2. The attacker selects a random number $R_1'$, and computes $CID_1' = (ID_1|R_1') \mod n, M_1' = h(ID_1)|B_i|R_1'||T_1'$. $T_1'$ is the current timestamp
3. The attacker sends $\{SID_j, CID_1', M_1', T_1\}$ to GWN

Upon receipt of the message, GWN will pass the validation to the attacker and treat the attacker as a valid user and successfully perform the subsequent step of the authentication phase as depicted in Jiang et al.’s protocol. Lastly, GWN sends message $\{M_7, M_8, M_9\}$ to the user, but the attacker receives the message and computes $R_9' = M_8 \oplus h(ID_1|R_1'|, R_9' = M_2 \oplus h(R_2')$, and $SK'_i = h(h(ID_1)|R_1'|R_2') \oplus R_2' \oplus R_3')$. Obviously, the result is true. Therefore, the attacker has generated a shared session key with $S_j$.

Thus, the attacker can imitate $U_i$ to login to GWN successfully. In this regard, Jiang et al.’s scheme is not secure against privileged insider attack.

3.4. DoS Attack. To authenticate $U_i$, GWN maintains a table containing secret data $ID_1$ and $R_i$ with respect to user $U_i$. When GWN receives the login request from $U_i$, GWN will retrieve $R_i$ in light of $ID_1$ to perform the subsequent procedure. However, because $(ID_1, R_i)$ is stored in the table, if an insider (being attacker) deletes or modifies all or some entries in the table, GWN will fail to lookup entries related to the user who has successfully registered and sends a login request to GWN, which leads to the legitimate user rejected by the GWN. Therefore, Jiang et al.’s scheme is susceptible to DoS attack.

4. The Proposed Scheme

In this section, we propose a secure and efficient authenticated key agreement scheme for WHMS to thwart the security weaknesses found in Jiang et al.’s scheme. Our scheme not only retains the advantages of Jiang et al.’s scheme but...
also provides additional security properties and is secure against different attacks. Similarly, our scheme consists of 5 phases: setup, medical professional registration, patient registration, login and authentication phase, and password change.

4.1. Setup Phase. This phase is identical to that of Jiang et al.’s scheme. The registration center GWN chooses two large prime nonces \( p \) and \( q \) and calculates \( n = pq \), then keeps the private key \((p, q)\).

4.2. Medical Professional Registration Phase

Step 1. \( U_i \) keys his ID, and PW, a random nonce \( r_i \), and calculates HPW = \( h(r_i \oplus PW) \); then, he transmits \{(ID, HPW),} to GWN via a secure channel.

Step 2. Upon receiving the registration request, GWN selects \( m \in \{2^2, 2^3\} \), a random nonce \( R \), calculates a fuzzy verifier \( \text{Reg} = h(h(ID, w))[HPW, mod m) \), \( A_i = R \oplus HP \) \( W_i \), \( B_i = h(ID, w)[K] \), and \( C_i = B_i \oplus h(ID, w)[HPW, \) after that, GWN sends \{Reg, \( A_i, C_i, m, n, h() \} \) to \( U_i \) through a secure channel.

Step 3. After receiving the message, \( U_i \) calculates \( A_i = A_i \oplus h(ID, w) \) \( R_i \) \( \oplus h(h(ID, w) \oplus m) \) \( m \) \( and \) \( updates \) \( MD \) \( with \) \{Reg, \( A_i, C_i, m, n, h() \}. \)

4.3. Patient Registration Phase. This phase is almost the same as in Jiang et al.’s scheme [29].

Step 1: The patient forwards his ID to the registration center.

Step 2: The registration center selects an appropriate sensor kit and assigns a professional.

Step 3: The registration center computes \( SK_{GW-SJ} = h(SID, w) \) for \( S_j \) as a secret key and delivers the relevant information of the patient to the designated professional.

4.4. Login and Authentication Phase. In this phase, a mutual authentication is performed and a session key is generated between \( U_i \) and sensor \( S_j \) for subsequent communication.

Step 1. \( U_i \) selects his ID, and PW, and MD computes \( r_i = D_i \oplus h(h(ID, w)[PW, mod m) \), \( HPW = h(r_i \oplus PW) \), \( A_i = A_i \oplus h(ID, w) \), \( R_i = A_i \oplus HPW \), \( \text{Reg} = h(h(ID, w)[HPW, \) \( mod m) \), and tests \( \text{Reg} = \text{Reg} \) if it is false, MD chooses a random number \( R_i \) and computes \( B_i = C_i \oplus h(ID, w)[HPW, \), \( C_i = (ID, w)[SID, w] \) \( mod m) \), \( M_i = h(ID, w)[B_i \oplus R_i \) \( T_i), \) and forwards \{CID, \( M_i, T_i \} \) to GWN. \( T_i \) is the current timestamp.

Step 2. On receiving login request msg1, GWN decrypts \( CID_i \) with \( (p, q) \) to obtain \((ID_i, \) \( R_i, \) \( T_i) \) and checks the validity of the timestamp \( T_i \). If the verification fails, GWN aborts the session. Otherwise, GWN computes \( B_i = h(ID, w)[K] \) \( M_i = h(ID, w)[B_i \oplus R_i \) \( T_i) \) and then tests \( M_i = M_i \). If inequality holds, GWN aborts the procedure. Otherwise, GWN calculates \( SK_{GW-SJ} = h(SID, w) \), selects a random nonce \( R_2 \), and computes \( M_2 = h(ID, w)[R_i \) \( R_i \) \( T_i) \) \( M_3 = h(ID, w)[R_i \) \( R_i \) \( T_i]) \) \( M_4 = M_2 \oplus h(SK_{GW-SJ}, T_2) \) \( M_5 = R_2 \oplus h(SK_{GW-SJ}, T_2) \) \( T_2) \). Finally, GWN sends msg2 = \{M3, M4, M5, T2 \} to \( S_j \).

Step 3. On receiving msg2 from GWN, \( S_j \) first checks the freshness of \( T_2 \). If not, \( S_j \) terminates the procedure. Otherwise, \( S_j \) computes \( R_2' = M_5 \oplus h(SK_{GW-SJ}, T_2) \) \( M_2 = M_2 \oplus h(SK_{GW-SJ}, T_2) \) \( T_2) \). If it is false, \( S_j \) aborts the session. Otherwise, \( S_j \) chooses a random number \( R_3 \) and computes SK = \( h(M_2, \) \( R_2 \) \( R_2') \), \( M_4 = h(SK, R_3) \oplus SK_{GW-SJ}, \) and \( M_5 = h(R_3', T_3) \) \( R_3' \), \( T_3 \) \( is the current timestamp. \( S_j \) then forwards msg3 = \{M6, M7, T3 \} to GWN.

Step 4. On receiving msg3 from \( S_j \), GWN first checks the validity of \( T_3 \). If it is invalid, GWN terminates the procedure. Otherwise, GWN computes \( R_3' = M_5 \oplus h(SK, T_3) \), \( SK' = h(M_4, T_3), \) \( and \( M_4' = h(SK, T_3) \) \( SK_{GW-SJ}, \) and checks whether \( M_4' = M_6 \) holds. If yes, GWN computes \( M_8 = R_2 \) \( h(ID, w)[R_i \) \( R_2'), \) \( M_9 = R_i \oplus h(ID, w)[R_i \) \( R_3'), \) and \( M_10 = h(ID, w)[SK, T_4) \) \( T_4) \) \( and \) \( delivers \) \{M8, M9, M10, T4 \} to \( U_i \), where \( T_4 \) is the current timestamp.

Step 5. After receiving msg4 from GWN, \( U_i \) validates the timestamp \( T_4 \). If not, \( U_i \) aborts the procedure. Otherwise, \( U_i \) computes \( R_4' = M_6 \oplus h(ID, w)[R_i \) \( T_4), \) \( SK' = h(ID, w)[R_i \) \( T_4') \) \( T_4'), \) and \( M_4' = h(ID, w)[SK, T_4) \) \( T_4) \) \( checks \) \( whether \) \( M_4' = M_6 \) \( holds. \) If it is false, \( U_i \) terminates the connection. Otherwise, \( U_i \) believes that both GWN and \( S_j \) are credible.

The login and authentication phase is summarized in Figure 2.

4.5. Password Change Phase. This phase is also similar to that in Jiang et al.’s scheme [29], and it is applicable if \( U_i \) intends to update his password.

Step 1. \( U_i \) keys ID, and PW.

Step 2. MD computes HPW = \( h(r_i \oplus PW) \), \( A_i = A_i \oplus h(I \) \( D, w)[r_i \) \( w), \) \( R_i = A_i \oplus HPW \), and \( \text{Reg}^* = h(ID, w)[HPW, \) \( mod m) \) \( checks \) \( the \) \( condition \) \( \text{Reg}^* = \text{Reg}. \) If it holds, MD quits this procedure.

Step 3. \( U_k \) keys his new password PWnew, then, MD computes HPW = \( h(r_i \oplus PW) \), \( A_i = A_i \oplus h(I \) \( D, w)[r_i \) \( w), \) \( R_i = A_i \oplus HPW \), \( C_i = (ID, w)[SID, w] \) \( mod m) \), \( A_i^{\text{new}} = A_i \oplus h(ID, w)[R_i \) \( HPW, \) \( C_i^{\text{new}} = B_i \oplus h(ID, w)[R_i \) \( HPW, \) \( A_i^{\text{new}} = A_i \oplus h(ID, w)[R_i \) \( w), \) \( \text{Reg}^* = h(ID, w)[HPW, \) \( mod m) \) \( checks \) \( the \) \( condition \) \( \text{Reg}^* = \text{Reg}. \) If it holds, MD quits this procedure.

Step 4. Finally, (\( \text{Reg}^*, \) \( C_i \)) is replaced with (\( \text{Reg}^*, \) \( A_i^{\text{new}}, \) \( C_i^{\text{new}} \)) by MD.
Input $\langle \text{ID}_i, \text{PW}_i \rangle$;

$\text{HPW}_i = h(\text{ID}_i \oplus \text{PW}_i)$;

$A_i = A_i \oplus h(\text{ID}_i)$;

$R'_i = A_i \oplus \text{HPW}_i$;

$\text{Reg}_i = h(h(\text{ID}_i \| R'_i \| \text{HPW}_i) \mod m)$;

If $\text{Reg}_i \neq \text{Reg}_i^*$, abort;

Choose $R_1$;

$B_i = C_i \oplus h(\text{ID}_i \| R_i \| \text{HPW}_i)$;

$\text{CID}_i = (\text{ID}_i \| R_i \| \text{SID}_j)^2 \mod n$;

$M_1 = h(\text{ID}_i \| R_1 \| T_1)$;

$\text{msg}_1 = \{\text{CID}_i, M_1, T_1\}$

Decrypt $\text{CID}_i$ with $(p, q)$ to obtain $(\text{ID}_i', R_i', R_i, T_i)$;

If $T_1$ is not fresh, abort;

$B_i = h(\text{ID}_i \| R_i \| K)$;

$M'_1 = h(\text{ID}_i \| B_i \| R_i \| T_i)$;

If $M'_1 \neq M_1$, abort;

$\text{SK}_{\text{GW-Sj}} = h(\text{SID}_j \| K)$;

Generate $R_2$;

$M_2 = h(\text{ID}_i \| R'_i \| R_i)$;

$M_3 = h(\text{ID}_i \| B_i \| h(\text{SK}_{\text{GW-Sj}} \| R_i \| T_2))$;

$M_4 = M_2 \oplus h(\text{SK}_{\text{GW-Sj}} \| T_2)$;

$M_5 = R_i \oplus h(\text{SK}_{\text{GW-Sj}} \| \text{SID}_j \| T_2)$;

$\text{msg}_2 = \{M_3, M_4, M_5, T_2\}$

If $T_2$ is not fresh, abort;

$R'_2 = M_3 \oplus h(\text{SK}_{\text{GW-Sj}} \| T_2)$;

$M_6 = h(M_3 \| R'_2 \| T_2)$;

If $M_6 \neq M_6'$, abort;

Choose $R_3$;

$\text{SK} = h(M_3 \| R'_2 \| R_i)$;

$M_8 = h(\text{SK} \| R_i \| \text{SK}_{\text{GW-Sj}})$;

$M_9 = R_i \| h(T_3)$;

$\text{msg}_3 = \{M_6, M_7, T_3\}$

If $T_3$ is not fresh, abort;

$R'_3 = M_3 \oplus h(R_i \| T_3)$;

$\text{SK}' = h(M_3 \| R'_3 \| R_i)$;

$M'_6 = h(\text{SK}' \| R_i \| \text{SK}_{\text{GW-Sj}})$;

If $M'_6 \neq M_6'$, abort;

$M_8 = R_i \oplus h(\text{ID}_i \| R_i)$;

$M_9 = R_i \oplus h(\text{ID}_i \| R_i \| T_4)$;

$M_{10} = h(\text{ID}_i \| \text{SK}' \| R_i \| T_4)$;

$\text{msg}_4 = \{M_8, M_9, M_{10}, T_4\}$

If $T_4$ is not fresh, abort;

$R'_4 = M_8 \oplus h(\text{ID}_i \| R_i)$;

$R'_5 = M_8 \oplus h(\text{ID}_i \| R_i \| R_i)$;

$\text{SK}' = h(\text{ID}_i \| R_i \| R_i \| R_i)$;

If $M_{10} = h(\text{ID}_i \| \text{SK}' \| R_i \| T_4)$, accept $\text{SK}'$.

Figure 2: The login and authentication phase of the improved protocol.
At last, MD contains the information \( \{ \text{Reg}_{\text{new}}, A_i^{\text{new}}, C_i^{\text{new}}, m, n, h() \} \).

### 5. Security Analysis and Performance Comparison

In this section, we evaluate the security of our proposal under the random oracle model [48] and a comprehensive heuristic security analysis. In addition, the performance comparisons with relevant competitive schemes are made.

#### 5.1. Authentication Proof Based on Random Oracle Model

In this section, we use the random oracle model to provide an authentication proof of the proposal. For simplicity, we present our formal security proof based on the security model of the previous works [48, 49].

**Theorem 1.** Suppose \( A \) is a polynomial time-bounded attacker running in time \( t_A \) and let \( \text{Adv}^{\text{AKE}}_{P, \text{PW}}(A) \) be the advantage of \( A \) in breaking the semantic security of the improved authenticated key exchanged (AKE) scheme \( P \) and \( \text{Adv}^{\text{RAE}}(t) \) be the advantage of the attacker \( A \) in cracking robust authenticated encryption (RAE) [50] in polynomial time \( t \). To break the semantic security of the proposed scheme, \( A \) asks at most \( q_a \) times Send queries, \( q_e \) times Execute queries, and \( q_h \) times Hash queries. Thus, we have

\[
\text{Adv}^{\text{AKE}}_{P, \text{PW}}(A) \leq \frac{q_i^2 + q_e^2}{2i} + \frac{(q_i + q_e)^3}{2^{\lambda} + 1} + \frac{2q_i}{|D_{\text{PW}}|},
\]

(1)

where \( l_i \) denotes the security parameter, \( l_i \) denotes the length of the random number, \( D_{\text{PW}} \) denotes a password dictionary with a frequency distribution following Zipf's law [51], and \( |D_{\text{PW}}| \) denotes the size of \( D_{\text{PW}} \).

**Proof.** A set of hybrid games \( G_m \) \((i = 0, 1, 2, 3, 4, 5)\) are completed in the proof. \( S_i \) represents the event that the attacker successfully guesses a correct bit in the Test query in each game \( G_m \), and \( \text{Pr}[S_i] \) represents the probability of \( S_i \). The details of each game are described as follows.

- **Gm0**: this starting game is considered identical to a real attack scenario under random oracle model. Thus, we have

\[
\text{Adv}^{\text{AKE}}_{P, \text{PW}}(A) = 2 \text{Pr}[S_0] - 1.
\]

(2)

- **Gm1**: according to the improved scheme, this game simulates queries including Test, Execute, Send, Hash, and Corrupt. And three lists \( L_L, L_A, \) and \( L_T \) are created to store the answer of various oracles. We can see that the simulation of \( G_m \) is indistinguishable to execution of \( Gm_0 \). Thus, we have

\[
\text{Pr}[S_1] = \text{Pr}[S_0].
\]

(3)

- **Gm2**: in this game, we consider the collisions of random oracle query and random numbers in protocol \( P \). If the collision of hash oracle and transcripts \( \text{msg}_1, \text{msg}_2, \text{msg}_3, \) and \( \text{msg}_4 \) occurs, the simulator aborts and lets the attacker win the game. According to the birthday paradox, the collision probability of the hash oracle is \( q_i^2 q_e^2 / 2^{\lambda + 1} \) at most, and the collision probability of random numbers \( R_1, R_2, \) and \( R_3 \) is \( (q_i + q_e)^3 / 2^{\lambda + 2} \). Thus, we have

\[
|\text{Pr}[S_2] - \text{Pr}[S_1]| \leq q_i^2 q_e^2 / 2^{\lambda + 1} + (q_i + q_e)^3 / 2^{\lambda + 2}.
\]

(4)

- **Gm3**: in this game, all the oracles are simulated as the previous game. If the attacker guesses \( M_1, M_2, M_3, \) and \( M_4 \) without making corresponding \( h() \) queries, the simulation will terminate. Thus, \( Gm_3 \) and \( Gm_2 \) are indistinguishable, and we have

\[
|\text{Pr}[S_3] - \text{Pr}[S_2]| \leq q_i / 2^{\lambda}.
\]

(5)

- **Gm4**: in this game, we take into account both online and offline attacks performed by the attacker. This game can be demonstrated as two cases. The first denotes online guessing attack, and the second denotes offline guessing attack.

  **Case 1.** The attacker asks \( \text{Corrupt}(U, 1) \) to guess \( PW \) and \( r_i \). So, two subcases are considered as follows:

  **Case 1.1.** The attacker chooses a password from \( D_{PW} \) online and simulates \( \text{Send}(U, \mu, \text{GWN}^k, \text{msg}_1) \) query \( q_e \) times. Thus, the collision probability is \( q_i / |D_{PW}| \).

  **Case 1.2.** We consider the situation that the attacker guesses \( r_i \) online intentionally or accidentally, and the collision probability is at most \( q_i / 2^{\lambda} \).

- **Case 2.** To launch offline guessing attack, the attacker asks \( \text{Corrupt}(U, 1) \) along with \( \text{Corrupt}(U, 0) \) query, as well as Execute and Send queries. Then, Hash oracle will be queried at least \( q_h \) times, and the simulation will be terminated once an invalid value is returned. Thus, the collision probability is at most \( q_i q_e / 2^{\lambda} \).

According to the analysis of the above cases, we have

\[
|\text{Pr}[S_4] - \text{Pr}[S_3]| \leq q_i / |D_{PW}| + q_i q_e / 2^{\lambda} + q_i \text{Adv}^{\text{RAE}}_{A}(t_A).
\]

(6)

- **Gm5**: in this game, the attacker executes \( \text{Send}, \text{Execute}, \) and \( \text{Hash} \) oracle queries on transcripts to break strong forward security. After choosing two indices from \( \{1, 2, \ldots, q_i + q_e\} \), the attacker executes a Test oracle and asks \( \text{Corrupt}(U, 1) \) query. The simulation will abort if the Test oracle cannot return the session key for the \( i \)th instance of \( U \) and the \( j \)th instance of \( S_j \). Thus, we have

\[
|\text{Pr}[S_5] - \text{Pr}[S_4]| \leq q_h (q_i + q_e)^2 \text{Adv}^{\text{RAE}}_{A}(t_A).
\]

(7)

Considering all the games, the attacker has no advantage in surmising the correct bit \( b \). Thus, we have
Using equations (2)–(8), the theorem is proved.

5.2. Analysis of Security Features. This section provides an informal security analysis, which demonstrates that the proposed scheme not only overcomes the security weaknesses in Jiang et al.’s scheme but also withstands various attacks.

(1) **Resistance to Stolen Mobile Device Attack.** Assume that MD is acquired by the attacker, and he extracts the secret data \(\{\text{Reg}_i, A_i, C_i, D_i, m, n, h()\}\) by power analysis [42] or side-channel technique [43]. From the medical professional registration phase, we can see that \(\text{Reg}_i = h(h(\text{ID}_i)\|\text{R}_i\|\text{HPW}_i) \mod m\), where \(\text{HPW}_i = h(r_i \oplus \text{PW}_i)\). If the attacker tries to guess the ID, and PW, via \(\text{Reg}_i = h(h(\text{ID}_i)\|\text{R}_i\| h(r_i \oplus \text{PW}_i)) \mod m\), he will not succeed since \(r_i\) and \(r_i\) are sufficiently large and he cannot guess them in polynomial time according to item 4 of the adversary model in Section 3.1. Furthermore, the attacker can get \(C_i = B_i \oplus h(h(\text{ID}_i)\|\text{HPW}_i)\), where \(B_i = h(h(\text{ID}_i)\|K)\), but he will also fail when he launches an offline dictionary attack on ID, and PW, because \(r_i\) and \(K\) are sufficiently large. Therefore, the proposal can withstand stolen mobile device attack.

(2) **Resistance to Privileged Insider Attack.** Suppose that a privileged insider has obtained the user’s registration request \(\{\text{ID}_i, \text{HPW}_i\}\), and he also gets the user’s mobile device that contains secret information \(\{\text{Reg}_i, A_i, C_i, D_i, m, n, h()\}\), where \(\text{Reg}_i = h(h(\text{ID}_i)\|\text{R}_i\|\text{HPW}_i) \mod m\), \(A_i^* = A_i \oplus h(\text{ID}_i)\|r_i\| h(r_i \oplus \text{PW}_i)\), \(C_i = B_i \oplus h(h(\text{ID}_i)\|\text{HPW}_i)\), \(D_i = r_i \oplus h(h(\text{ID}_i)\|\text{PW}_i)) \mod m\), and \(B_i = h(h(\text{ID}_i)\|K)\). If the attacker chooses a pair \((\text{ID}, \text{PW})\) from \(D_{\text{ID}} \times D_{\text{PW}}\) to perform offline password guessing attack via \(r_i = D_i \oplus h(h(\text{ID}_i)\|\text{PW}_i) \mod m\) and \(\text{HPW}_i = h(r_i \oplus \text{PW}_i)\), and we set \(|D_{\text{PW}}| = |D_{\text{ID}}| = 2^k\) [51, 52], it can be assured that there are \(|D_{\text{ID}}| \times |D_{\text{PW}}|/m = 2^{2k}\) candidates \((\text{ID}, \text{PW})\) to prevent the attacker from guessing out the correct password. Moreover, if the insider attacker tries to compromise \(\text{PW}_i\) from \(A_i^*\) or \(C_i\), he will still fail since he does not know random numbers \(r_i\) and \(r_i\) and the long-term key \(K\). Therefore, the proposal can resist privileged insider attack.

(3) **Resistance to KSSTI Attack.** In our scheme, the session key \(SK = h(h(M_2)\|R_3) = h(h(\text{ID}_i)\|R_i)\|R_3)\) is generated with the parameters \(\text{ID}_i, R_i, R_1, R_2,\) and \(R_3\), which are provided by the mobile device, GWN, and sensor, respectively. If the attacker captures messages \(\text{msg}_2 = \{M_3, M_4, M_5, T_2\}\) and \(\text{msg}_3 = \{M_6, M_7, T_3\}\), we discuss that the proposed scheme can resist KSSTI attack in three cases.

**Case 1. Suppose \(R_2\) is compromised.** It is clear that the attacker can calculate \(R_3 = M_7 \oplus h(R_2\|T_3)\). To obtain \(M_2\), the attacker intends to compute \(M_2 = M_4 \oplus h(SK_{GW-SJ}\|T_2)\). However, the attacker knows nothing about \(SK_{GW-SJ}, \text{SID}_j\), and \(K\), resulting in failure of computing \(M_2\) by \(M_2 = M_4 \oplus h(SK_{GW-SJ}\|T_2)\). Thus, the attacker cannot compute the session key if \(R_2\) is compromised.

**Case 2. Suppose \(R_3\) is compromised.** To get \(R_2\), the attacker first computes \(h(R_2\|T_3) = M_7 \oplus R_3\), and \(h(\text{ID}_i)\|R_3) = M_9 \oplus R_3\) and then mounts an offline guessing attack. However, he will be unsuccessful according to item 4 of the adversary model in Section 3.1. Moreover, he cannot compute \(M_2\) by \(M_2 = M_4 \oplus h(SK_{GW-SJ}\|T_2)\) as we analyzed in Case 1. Thus, his dream will not come true in computing the session key \(SK = h(M_2)\|R_3\|R_3)\).

**Case 3. Suppose \(R_1\) is compromised.** In our protocol, if the attacker attempts to derive \(R_2\) by computing \(R_2 = M_4 \oplus h(\text{ID}_i)\|R_1)\), the attacker has to know the identity \(\text{ID}_i\) of the user. However, it is impossible for him to retrieve \(\text{ID}_i\) from other components in the public messages. Thus, the attacker cannot compute the session key if he only knows \(R_1\).

(4) **Resistance to GWN Impersonation Attack.** During the authentication protocol execution, if the attacker makes an effort to masquerade GWN, he has to generate messages \(\{M_3, M_4, M_5, T_2\}\) and \(\{M_6, M_7, M_8, M_9, T_4\}\) and transmit them to \(S_j\) and \(U_j\), respectively, where \(M_3 = h(h(M_2)^{-1})\|SK_{GW-SJ}\|R_1\|T_2)\), \(M_4 = M_2 \oplus h(SK_{GW-SJ}\|T_2)\), \(M_5 = R_2 \oplus (SK_{GW-SJ}\|\text{SID}\|T_2)\), \(M_6 = h(\text{ID}_i)^*\|R_1\|R_1\|R_1\), \(M_7 = R_2 \oplus h(\text{ID}_i)\|R_1\), \(M_8 = R_3 \oplus h(\text{ID}_i)\|R_3\), and \(M_9 = h(\text{ID}_i)\|SK\|\text{SID}\|R_1\|T_4)\). However, without the knowledge of \((\text{SID}_j, K, \text{ID}_i, \text{ID}_j, R_1, R_2, R_3, SK)\), the attacker is unable to generate these two messages to cheat the sensor and the user. Hence, the proposal can withstand GWN impersonation attack.

(5) **Resistance to Desynchronization Attack.** There are two conditions that may lead to desynchronization attack. First, both parties of communication stored authentication data that needs to be updated simultaneously, and if the message sent from one party to the other is intercepted by the attacker, the result is that the authentication data in one party has been updated whereas the other party’s is still unchanged. In our protocol, MD and the sensor are not required to update their authentication data simultaneously. Second, the authenticated protocol needs to maintain verification tables in GWN, or the server is subject to this attack. However, our improved scheme is not required to store a verification table in GWN. In short, our improved scheme is free from desynchronization attack.
(6) Resistance to Sensor Impersonation Attack. In this attack, the attacker generates a valid message \( \{M_6, M_7, T_3\} \) to cheat the GWN. However, because \( S_{KW-S} \) is carefully protected by the GWN and the attacker has no knowledge of \( R_1 \) and \( R_2 \), the attacker cannot succeed in forging the message \( \{M_6, M_7, T_3\} \). Therefore, the improved scheme is able to resist sensor impersonation attack.

(7) Resistance to Replay Attack and Man-in-the-Middle Attack. Generally, random nonce and timestamp are the two main techniques to prevent replay attack in authentication protocols. In our improved scheme, if the attacker captures the login message \( \{CID_S, M_1, T_1\} \) and replays it to GWN, he cannot be authenticated by GWN because GWN will check the freshness of \( T_1 \) and verify the hash value \( M_1 \) which is computed with secret random numbers \( R_1 \) and \( R_2 \) shared between mobile device and the sensor. In addition, if the attacker generates an imitated login message with a new timestamp \( T_1' \), the GWN will reject it because \( T_1' \) should be a parameter of \( M_1 \), and \( M_1 \) cannot pass the verification of GWN. Thus, the improved scheme is secured from replay attack. Moreover, without knowing \( (ID_i, R_1, R_1', R_2, R_3) \), the attacker is unable to compute the session key \( SK = h(M_2 ||R_1 ||R_3) \). Hence, the attacker will fail in passing the authentication of the sensor \( S_j \), which means he cannot produce a valid session with \( S_j \) via retransmitting the request message of \( U_i \). Thus, the proposal can thwart man-in-the-middle attack.

(8) Perfect Forward and Backward Secrecy. As can be seen from the login and authentication phase, the session key \( SK = h(M_2 ||R_1 ||R_3) = h(h(ID_i ||R_1 ||R_3) \oplus R_1 ||R_3) \) is computed by \( U_i \) and \( S_j \), and it relies on \( (ID_i, R_1, R_1', R_2, R_3) \), where the parameters \( (R_1, R_1', R_2, R_3) \) are randomly generated and unpredictable. Even if the attacker knows the leaked long-term key \( K \) of GWN, it is still impossible for him to calculate the session key because he has no knowledge of these random numbers provided by each communication party, i.e., \( U_i \), GWN, and \( S_j \). That is to say, the improved protocol can provide perfect forward and backward secrecy.

(9) Resistance to User Impersonation Attack. Assume that the attacker obtains the mobile device and extracts the secret information \( \{Reg, A_i^*, C_i, D_i, m, n, h()\} \), where \( Reg = h(h(ID_i ||R_1 ||HPW_i) \mod m) \), \( A_i^* = A_i \oplus h(ID_i ||C_i) \), \( C_i = B_i \oplus h(ID_i ||R_i ||HPW_i) \), \( D_i = r_i \oplus h(h(ID_i ||PW_i) \mod m) \), and \( B_i = h(ID_i ||R_i ||K) \). To generate a valid login request \( \{CID_S, M_1, T_1\} \), the attacker should first derive both password and mobile device of the medical professional. In particular, GWN validates the legitimacy of the medical professional by checking \( M_1^* = h(ID_i ||B_i ||R_i ||T_1') \), and the key to compute \( M_1 \) is to get the value of \( B_i \). However, without the knowledge of parameters \( (ID_i, PW_i, R_1 , R_2, R_3) \), the attacker cannot compute \( B_i \), which means the attacker’s legitimacy will not be corroborated by GWN. Hence, the improved scheme is secure from user impersonation attack.

(10) User Anonymity. User anonymity is extremely important in preserving the patient’s privacy. Suppose that the attacker intercepts all the messages of the parties involved during the protocol execution, and in these messages, the component CI \( D_i = (ID_i ||R_1 ||R_2 ||K)^2 \mod n \) is related to the identity of the medical professional directly. However, the attacker cannot decrypt CI\( D_i \) to get ID\( i \) because he has no knowledge of \( n \) or \( (p, q) \). Besides, if the attacker attempts to mount identity guessing attack on \( M_6, M_9, \) and \( M_{10} \), respectively, where

<table>
<thead>
<tr>
<th>Table 2: Comparison of security features.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notation</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>S1</td>
</tr>
<tr>
<td>S2</td>
</tr>
<tr>
<td>S3</td>
</tr>
<tr>
<td>S4</td>
</tr>
<tr>
<td>S5</td>
</tr>
<tr>
<td>S6</td>
</tr>
<tr>
<td>S7</td>
</tr>
<tr>
<td>S8</td>
</tr>
<tr>
<td>S9</td>
</tr>
<tr>
<td>S10</td>
</tr>
<tr>
<td>S11</td>
</tr>
<tr>
<td>S12</td>
</tr>
<tr>
<td>S13</td>
</tr>
</tbody>
</table>

Table 3: Execution time of cryptographic operation.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Meaning</th>
<th>Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T_h )</td>
<td>Time of a hash operation</td>
<td>0.0004 [53]</td>
</tr>
<tr>
<td>( T_m )</td>
<td>Time of a modular squaring</td>
<td>= ( T_h ) [41]</td>
</tr>
<tr>
<td>( T_p )</td>
<td>Time of ECC point multiplication</td>
<td>7.3529 [44]</td>
</tr>
<tr>
<td>( T_s )</td>
<td>Time of symmetric encryption/decryption</td>
<td>0.1303 [44]</td>
</tr>
<tr>
<td>( T_{QR} )</td>
<td>Time of square root modular n</td>
<td>1.8382 [41, 44]</td>
</tr>
<tr>
<td>( T_R )</td>
<td>Time of Rep operation</td>
<td>= ( T_p ) [53]</td>
</tr>
</tbody>
</table>
5.3. Security and Performance Comparison. In this section, we compare the security features and performances of the improved scheme with the relevant competitive schemes [27, 29, 33, 53, 54].

Table 2 shows the comparison results of security features between the improved scheme and the related ones [27, 29, 33, 53, 54]. From Table 2, it is evident that our scheme has overcome the security weaknesses existing in Jiang et al.’s scheme [29], while the other protocols have security vulnerabilities more or less, e.g., protocols [27, 29, 33] suffer from user impersonation attack and cannot preserve user anonymity, protocols [53, 54] are vulnerable to stolen mobile device attack, and protocol [54] cannot resist replay and privileged insider attack. Particularly, some protocols [33, 53] cannot resist user impersonation attack when the mobile device is obtained by the attacker.

To facilitate the comparison of performances during the login and authentication phase, we use the various time notations of cryptographic operation as shown in Table 3. To make a comparison of computation cost fairly, we also provide the time cost of various cryptographic calculations as the benchmark [41, 44, 53] in Table 3. Additionally, we assume that the length of an identity, a random number, a hash value, a timestamp, an elliptic curve point, the block size of AES symmetric encryption/decryption, and the modular exponentiation are 32 bits, 128 bits, 160 bits, 32 bits, 320 bits, 128 bits [55], and 1024 bits [14], respectively. The comprehensive study of the improved scheme and the related schemes [27, 29, 33, 53, 54] is given in Table 4. Furthermore, the performances of the sensor node are summarized in Table 5, because energy consumption is vital to evaluate the lifetime of the sensor node. For the convenience of understanding, the comparison graphs of computation cost, communication overhead, and traffic of sensor node are shown in Figures 3, 4, and 5, respectively.

<table>
<thead>
<tr>
<th>U_i</th>
<th>GWN</th>
<th>S_j</th>
<th>Total cost</th>
<th>Estimated time (ms)</th>
<th>Communication overhead (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8T_h + T_R + 2T_S</td>
<td>9T_h + T_M</td>
<td>11T_h + T_R + 2T_P</td>
<td>20T_h + T_R + 10T_S</td>
<td>8.66</td>
<td>2944</td>
</tr>
<tr>
<td>9T_h + T_M</td>
<td>10T_h</td>
<td>11T_h + T_R + 2T_S</td>
<td>30T_h + 6T_M + T_QR</td>
<td>1.84</td>
<td>2560</td>
</tr>
<tr>
<td>11T_h + T_R + 2T_P</td>
<td>13T_h + 2T_S</td>
<td>24T_h + T_R + 4T_P</td>
<td>30T_h + 6T_M + T_QR</td>
<td>36.77</td>
<td>3072</td>
</tr>
<tr>
<td>10T_h</td>
<td>5T_h + 2T_S</td>
<td>3T_h + 2T_P</td>
<td>24T_h + T_R + 4T_P</td>
<td>7.88</td>
<td>2496</td>
</tr>
<tr>
<td>9T_h + T_M</td>
<td>7T_h</td>
<td>5T_h</td>
<td>27T_h + T_M + 4T_S</td>
<td>51.61</td>
<td>2880</td>
</tr>
<tr>
<td>11T_h + T_R + 2T_S</td>
<td>13T_h + T_QR</td>
<td>4T_h + 2T_P</td>
<td>22T_h + 6T_P</td>
<td>1.97</td>
<td>2592</td>
</tr>
</tbody>
</table>

\[ M_8 = R_2 \oplus h(ID_2^* || R_2^*), \quad M_9 = R_3 \oplus h(ID_3^* || R_3^*), \quad M_{10} = h(ID_2^* || SK || R_3^* || T_3) \]

Table 4: Performance comparison.

Although our scheme is not the most efficient one in terms of computation cost and communication overhead, our improved scheme requires a little more computation cost and communication overhead than protocol [29]. However, the performance of our improved scheme is more efficient than protocols [27, 33, 53, 54] as justified from Table 4. In particular, protocols [33, 54] are the two most inefficient schemes among all the schemes since they employ ECC in which point multiplication needs more time than other operations, and elliptic curve point also needs more length than other symbols in communication.

From Table 5, it can be seen that the traffic length of sensor node in our protocol is 864 bits, which is just slightly higher than that in [29], but much lower than those in [27, 33, 53, 54]. Therefore, the potential energy consumption of our improved scheme is keeping at a manageable level for WMHS that helps to prolong the lifetime of the sensor.

Although our scheme is not the most efficient one, it is worth noting that the security analysis and the comparison results of security features in Table 2 have shown that our improved scheme overcomes the security risks in [27, 29, 33, 53, 54]. In a word, our improved scheme has higher security level while its computation cost and communication overhead are within reasonable level for WMHS environment.

6. Conclusion

To defeat the subtle security weaknesses like KSSTI attack, privileged insider attack, and DoS attack in Jiang et al.’s protocol for WMHS, we propose an improved two-factor authenticated key agreement protocol using quadratic residues. The completeness and validity of the improved scheme is proved under the random oracle model. Additionally, we provide a security analysis to demonstrate that the improved scheme is secure against various known attacks.
Furthermore, performance comparisons between the improved scheme and the related ones demonstrate that our scheme outperforms the previous ones with regard to security features, computation cost, and communication overhead. Owing to these metrics, we believe that our improved scheme provides a reasonable solution for practical use in WHMS environment.

### Data Availability

1. The [27] data used to support the findings of this study have been deposited in the [Springer] repository ([DOI: 10.1007/s11277-016-3718-6]).
2. The [29] data used to support the findings of this study have been deposited in the [Elsevier] repository ([DOI: 10.1016/j.compeleceng.2017.03.016]).
3. The [33] data used to support the findings of this study have been deposited in the [Springer] repository ([DOI: 10.1007/s12652-018-1015-9]).
4. The [53] data used to support the findings of this study have been deposited in the [Springer] repository ([DOI: 10.1007/s12083-016-0485-9]).
5. The [54] data used to support the findings of this study have been deposited in the [IEEE Xplore] repository ([DOI: 10.1109/JSYST.2019.2899580]).

### Conflicts of Interest

The authors declare no conflict of interest regarding the publication of this paper.

### Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (Project No. 61672007) and Science and Technology Innovation Guidance Project 2017 (Project No. 201704030605).

### References


