IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 6, 2020, accepted February 27, 2020, date of publication March 6, 2020, date of current version March 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2978891

Efficient and Provably Secure Anonymous User Authentication Scheme for Patient Monitoring Using Wireless Medical Sensor Networks

GUOAI XU[1,2], **FEIFEI WANG**[1], **MIAO ZHANG**[1,2], **AND JUNHAO PENG**[3]
[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]National Engineering Laboratory of Mobile Network Security, Beijing 100876, China
[3]School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

Corresponding author: Feifei Wang (wangfeifei99@bupt.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB0803600, and in part by the National Natural Science Foundation of China under Grant 61873069.

ABSTRACT Wireless medical sensor networks (WMSNs) are playing an increasingly important role in smart healthcare applications. Since the data transmitted in WMSNs is closely related to patient's life and health, and considering the resource-constrain feature of the sensor node, constructing an authentication scheme for WMSNs is a formidable task. Recently, Soni *et al.* presented an elliptic curve cryptosystem based three-factor authentication scheme for WMSNs. However, we discover that their scheme suffers from serious vulnerabilities, such as sensor node capture attack, no forward secrecy, and the violation of three-factor security. To enhance the security and efficiency, we present a novel scheme using Rabin cryptosystem and chaotic maps. We use several widely-accepted security analysis methods to verify the correctness and security of our scheme. The Burrows–Abadi–Needham logic proof confirms the completeness of our scheme. The heuristic analysis indicates that our scheme is resistant to potential attacks and provides various security attributes like forward secrecy and three-factor security. Furthermore, we demonstrate that our scheme is provably secure in the random oracle model. Finally, the performance comparisons indicate that our scheme is superior to the related schemes both in security and efficiency and is more applicable to WMSNs owing to low overhead of the sensor node.

INDEX TERMS Internet of Things, wireless medical sensor networks, authentication, user anonymity, random oracle model.

I. INTRODUCTION

With the fast development of the Internet of things (IoT) technologies, wireless medical sensor networks (WMSNs) are playing an increasingly important role in real-time patient monitoring, telemedicine, and smart healthcare system [1]–[3]. The architecture model of WMSN is depicted in Figure 1. WMSN consists of a large number of medical sensor nodes, and one or multiple gateway nodes [4], [5]. The medical sensor nodes gather patient's vital signs data like temperature, respiratory rate, heart rate, blood pressure, etc. With the help of the gateway, the medics are allowed to access patient's physiological data through multiple types of terminals devices after identity authentication. By the aid of WMSNs, the medics can make remote medical diagnosis for the patients at everywhere.

The entities of WMSNs communicate with each other via unprotected wireless channel. They are susceptible to various network attacks and privacy leaks [6], [7]. It is essential to verify the identity of communicating parties, and protect communication security as well as user privacy in WMSNs.

The aim of user authentication protocol is to provide such security protection [8]. However, WMSNs are applied in the security-critical applications that are in high demand for security. Besides, the medical sensor node has limited computing capability and energy power. Constructing an authentication scheme for WMSNs that can overcome the security threats from all sides as well as satisfy the demand of high efficiency needs to be explored in depth.

The associate editor coordinating the review of this manuscript and approving it for publication was Qingchun Chen.

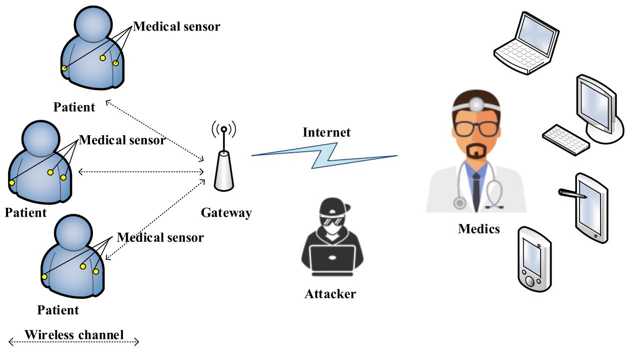


FIGURE 1. Architecture model of WMSN.

The authentication factors such as the password, the smart card, and the biometric are the cornerstone of user authentication [9]. In the past two decades, many smart card based password authentication schemes, i.e., two-factor authentication schemes, have been put forward [10]–[12]. However, most of two-factor authentication schemes suffer from smart card loss attack or do not support password validation and update locally [13]. In recent years, with the maturity of biometric technology, the biometric is added to user authentication as it is inherent and difficult to lose and forge [14]. Three-factor authentication schemes employing the biometric are able to provide better security than two-factor authentication schemes, and have become a research hotspot.

Over the years, there are some authentication schemes for WMSNs introduced [15]–[18]. In 2012, Kumar *et al.* [19] put forward a symmetric cryptosystem based two-factor authentication protocol. However, He *et al.* [20] discovered that their protocol suffers from smart card loss attack as well as privileged insider attack, and introduced an enhanced protocol. Afterwards, Li *et al.* [21] demonstrated that He *et al.*'s protocol is susceptible to off-line guessing attack and desynchronization attack. In 2016, Amin *et al.* [22] provided a hash function based two-factor authentication protocol. However, their protocol is not resistant to forgery attack. In 2018, Wu *et al.* [23] put forward a hash function based two-factor authentication protocol. However, their protocol was observed to have weaknesses like no forward secrecy. Mao *et al.* [24] provided a biometrics-based authentication protocol employing elliptic curve cryptosystem. Unfortunately, their protocol involves session key exposure when the nonce is compromised. Challa *et al.* [25] put forward an ECC-based three-factor authentication protocol. In 2019, Chen *et al.* [26] presented a three-factor authentication protocol using symmetric cryptosystem. However, their protocol cannot resist off-line guessing attack. Soni *et al.* [27] pointed out that Challa *et al.*'s protocol [25] is flawed with session key disclosure attack and forgery attack, and introduced an improved protocol.

A. MOTIVATIONS AND CONTRIBUTIONS

The data transmitted in WMSNs is closely related to patient's life and health. If the data is disclosed or even maliciously modified by the attacker, it will lead to very serious consequences. Therefore, the authentication scheme for WMSNs should be secure against potential attacks. On the other hand, the resource-constrain feature of the sensor node demands that the authentication scheme for WMSNs should have high efficiency. Since the existing authentication schemes for WMSNs have diverse weaknesses or their efficiency needs to be improved. It urges us to construct an efficient authentication scheme for WMSNs with high security.

We sum up the contributions of this paper as below.

1. We point out that Soni *et al.*'s scheme [27] has vulnerabilities such as sensor node capture attack, no forward secrecy, and the violation of three-factor security.
2. To enhance the security and efficiency, we present an efficient and provably secure biometric-based authentication scheme for WMSNs using Rabin cryptosystem and chaotic maps, in which we establish secure session key at a minimum cost. The security of our scheme is based on the hardness of large number prime factorization and Chebyshev chaotic Diffie–Hellman problem.
3. We use several security analysis methods to verify the correctness and security of our scheme, such as Burrows–Abadi–Needham logic analysis, the formal analysis under the random oracle (RO) model, and the heuristic analysis. In addition, the performance comparisons show that our scheme has high efficiency and provides more security attributes. Moreover, our scheme incurs low overhead for the sensor node.

B. ORGANIZATION OF THE PAPER

The structure of the paper is as follows. We give some preliminaries in Section II. We point out the weaknesses of Soni *et al.*'s scheme in Section III. We present an efficient and provably secure biometric-based authentication scheme for WMSNs in Section IV. We give the security analysis in Section V. We present the performance comparisons in Section VI. Finally, Section VII is a conclusion of the paper.

II. PRELIMINARIES

A. RABIN CRYPTOSYSTEM

The user A chooses two large primes μ, ν as its private key, where $\mu \equiv 3(mod\,4)$, $\nu \equiv 3(mod\,4)$. A computes $\omega = \mu \cdot \nu$ as its public key, and publishes ω. To encrypt the message m, the user B computes $c = m^2 \, mod\, \omega$. B sends the ciphertext c to A. To decrypt c, the user A who has μ, ν finds four roots (m_1, m_2, m_3, m_4) of the equation by using the Chinese surplus theorem. m involves some specific information such as timestamp, which is used to identify m. The security of Rabin cryptosystem is based on the hardness of large number prime factorization.

B. CHEBYSHEV CHAOTIC MAPS

The Chebyshev polynomial $T_n(x)$ is calculated based on $T_n(x) = \cos(n \cdot \arccos x)$, where $x \epsilon [-1, 1]$, n is the degree of polynomial.

Based on the definition of the enhanced Chebyshev polynomial introduced by Zhang [28], we have

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)\,(mod\,p) \quad n \geq 2$$

where $x \epsilon [-\infty, +\infty]$, p is a large prime.

- Chebyshev Chaotic Discrete Logarithm Problem (CHDLP): For given $T_u(x)$ and x, it is computationally infeasible to compute u.
- Chebyshev Chaotic Diffie–Hellman Problem (CHDHP): For given $T_a(x)$, $T_b(x)$ and x, it is computationally infeasible to calculate $T_{ab}(x) \equiv T_a(T_b(x)) \equiv T_b(T_a(x))\,(mod\,p)$.

C. ATTACKER MODEL

In the light of the attacker model presented in [29], the ability of the adversary $\mathcal{A}$ is as below.

1) $\mathcal{A}$ can eavesdrop the messages transmitted through the open channel. In addition, $\mathcal{A}$ can block, replay, and modify the messages transmitted through the open channel.
2) $\mathcal{A}$ can obtain the sensitive data of the smart card or the password of user. In addition, $\mathcal{A}$ can obtain user's biometric [29].
3) In case of testing forward secrecy, $\mathcal{A}$ can obtain gateway's secret key and sensor node's secret key.
4) The identity of user may not be properly kept [30]. Users's passwords are subject to the Zipf's law [31]. We assume $\mathcal{A}$ is capable of enumerating all the items in $D_{PW} * D_{ID}$, where D_{ID}, D_{PW} are identity space, password space, respectively [32].

D. SECURITY REQUIREMENTS OF WMSNs

As discussed in [12], [32], [33], [34], the authentication scheme for WMSNs should fulfil the following requirements.

1. The scheme should achieve the essential features of authentication protocol, i.e., mutual authentication and session key agreement [32].
2. The scheme should be resistant to known attacks like forgery attack, replay attack, de-synchronization attack, privileged insider attack, man-in-the-middle attack, and off-line guessing attack [32].
3. The scheme should not involve session key exposure. That is to say, the scheme should be secure against session key disclosure attack, session-specific temporary information attack, known key attack, and provide forward secrecy [33].
4. The scheme should preserve desired attributes, i.e., user anonymity, three-factor security [34].
5. The scheme should have high efficiency for the sensor node. The resource-constrained sensor node has limited computing capability and energy power. The scheme should fully consider the computing and communication cost of the sensor node. For example, the user (the medic) is usually far away from the medical sensor node, the sensor node should not deliver messages to user directly, but exchange messages with the user by the aid of the gateway that acts as a relay node [12].

III. CRYPTANALYSIS OF SONI *et al.*'s SCHEME

A. DESCRIPTION OF SONI et al.'s SCHEME

Soni *et al.* [27] pointed out that Challa *et al.*'s protocol [25] is flawed with session key disclosure attack and forgery attack, and introduced an improved protocol. In this phase, we give a brief description of Soni *et al.*'s scheme [27] and reveal its vulnerabilities. The notations of the paper are summarized in Table 1.

TABLE 1. Notations.

Symbols	Description
U_i	The user, namely, the medic
S_j	The medical sensor node
GW	The gateway
ID_i,PW_i, b_i	Identity, password, biometric of U_i
DID_i	Dynamic identity of U_i
SID_j	Identity of S_j
T_1, T_2, T_3, T_4	Timestamps
mk	Master key of the gateway
κ_j	Secret key of S_j
SK	Session key
$(P)_x/(P)_y$	x-co-ordinate/ y-co-ordinate of the elliptic curve point P
$Gen()$	Probabilistic generation function of fuzzy extractor
$Rep()$	Deterministic reproduction function of fuzzy extractor
$H_1()$	Hash function
$H_2()$	Biohashing function, it maps the biometric and a random data to a unique compact code

1) PRE-DEPLOYMENT PHASE

GW selects an elliptic curve group $E_p(a, b)$. And P is a generator of $E_p(a, b)$. GW picks the private key s, and calculates the public key $G_{pub} = sP$. GW also selects the master key mk. Afterwards, GW selects a unique identity SID_j for each medical sensor node S_j, and computes the secret key $\kappa_j = H_1(SID_j \| mk)$. GW distributes $\{SID_j, \kappa_j\}$ to S_j in a secure way, and publishes $\{G_{pub}, P\}$.

2) USER REGISTRATION PHASE

Step 1. U_i selects his identity ID_i, and computes $PID_i = H_1(r_1 \| ID_i)$, $MID_i = H_1(ID_i)$, where r_1 is a random number. U_i sends the registration request $\{PID_i, MID_i\}$ to GW via the confidential channel.

Step 2. Upon getting $\{PID_i, MID_i\}$, GW computes $\rho_i = PID_i \oplus H_1(MID_i \oplus H_1(s \| mk))$. If ρ_i is not found in the database, GW computes $A_i = H_1(PID_i \| s)$, $\lambda_i = H_1(MID_i \| s)$. GW saves $\{\rho_i, \lambda_i\}$ in the database. Then GW stores A_i in a smart card, and hands it over to U_i in a secure way.

Step 3. Upon getting the smart card, U_i picks his password PW_i, imprints his biometric b_i. The smart card computes $Gen(b_i) = (\sigma_i, \theta_i)$, $B_i = H_1(PW_i \| r_1)$, $C_i = H_1(B_i \| PID_i)$, $E_i = r_1 \oplus H_1(ID_i \| PW_i \| \sigma_i)$, $F_i = A_i \oplus H_1(ID_i \| \sigma_i)$. The smart card stores $\{C_i, E_i, F_i, \theta_i\}$, and removes A_i.

3) LOGIN AND AUTHENTICATION PHASE

Step 1. U_i enters ID_i^* and PW_i^*, imprints b_i^*. The smart card computes $Rep\left(b_i^*, \theta_i\right) = (\sigma_i^*)$, $r_1^* = E_i \oplus H_1(ID_i^* \parallel PW_i^* \parallel \sigma_i^*)$, $B_i^* = H_1(PW_i^* \parallel r_1^*)$, $PID_i^* = H_1(r_1^* \parallel ID_i^*)$, $C_i^* = H_1(B_i^* \parallel PID_i^*)$, checks if $C_i^* = C_i$. If they are equal, the smart card selects a nonce α. Then the smart card calculates $R_i = \alpha P$, $N_i = \alpha G_{pub} = ((N_i)_x, (N_i)_y)$, $N = H_1((N_i)_x \parallel (N_i)_y)$, $DID_i = PID_i^* \oplus N$, $A_i^* = F_i \oplus H_1(ID_i^* \oplus \sigma_i^*)$, $G_i = SID_j \oplus H_1(A_i^* \parallel N)$, $K_i = H(DID_i \parallel G_i \parallel R_i \parallel A_i^* \parallel T_1)$, where T_1 is the current timestamp. The smart card delivers $\{DID_i, G_i, R_i, K_i, T_1\}$ to GW.

Step 2. After getting $\{DID_i, G_i, R_i, K_i, T_1\}$, GW verifies if T_1 is valid. If so, GW computes $N_i = sR_i = \left((N_i)_x, (N_i)_y\right)$, $N = H_1((N_i)_x \parallel \left(N_i)_y\right)$, $PID_i = DID_i \oplus N$, $A_i = H_1\left(PID_i \parallel s\right)$, $SID_j = G_i \oplus H_1(A_i \parallel N)$, $K_i{}' = H\left(DID_i \parallel G_i \parallel R_i \parallel A_i \parallel T_1\right)$, checks if $K_i{}' = K_i$. If they are equal, GW chooses a random number β, computes $P_i = \beta \cdot N_i = \left((P_i)_x, (P_i)_y\right)$, $O_i = \beta \cdot G_{pub} = ((O_i)_x, (O_i)_y)$, $V_i = H_1(A_i \oplus H_1\left((P_i)_x \parallel (P_i)_y\right))$, $\kappa_j = H_1(SID_j \parallel mk)$, $W_i = V_i \oplus H_1(\kappa_j \parallel T_2 \parallel T_1)$, $L_i = H_1(V_i \parallel SID_j \parallel \kappa_j \parallel T_2 \parallel T_1)$, where T_2 is the current timestamp. GW delivers $\{W_i, L_i, T_2, T_1\}$ to S_j.

Step 3. After receiving $\{W_i, L_i, T_2, T_1\}$, S_j verifies the validity of T_2. Then S_j computes $V_i = W_i \oplus H_1(\kappa_j \parallel T_2 \parallel T_1)$, $L_i{}' = H_1(V_i \parallel SID_j \parallel \kappa_j \parallel T_2 \parallel T_1)$, checks if $L_i{}' = L_i$. If they are equal, S_j computes $SK = H_1(V_i \parallel SID_j \parallel H_1\left(\kappa_j\right) \parallel T_1 \parallel T_3)$, $M_i = H_1(SK \parallel SID_j \parallel T_3)$, $Q_i = H_1(SID_j \parallel V_i) \oplus H_1\left(\kappa_j\right)$, where T_3 is the current timestamp. S_j sends $\{Q_i, M_i, T_3\}$ to GW.

Step 4. After receiving $\{Q_i, M_i, T_3\}$, GW verifies the validity of T_3, computes $SK = H_1(V_i \parallel SID_j \parallel H_1\left(\kappa_j\right) \parallel T_1 \parallel T_3)$, $M_i = H_1(SK \parallel SID_j \parallel T_3)$, checks if $M_i{}' = M_i$. If they are equal, GW sends $\{Q_i, M_i, O_i, T_3, T_4\}$ to U_i, where T_4 is the current timestamp.

Step 5. After receiving $\{Q_i, M_i, O_i, T_3, T_4\}$, the smart card verifies the validity of T_4. Then the smart card computes $P_i = \alpha \cdot O_i = \left((P_i)_x, (P_i)_y\right)$, $V_i = H_1(A_i^* \oplus H_1\left((P_i)_x \parallel (P_i)_y\right))$, $H_1\left(\kappa_j\right) = Q_i \oplus H_1(SID_j \parallel V_i)$, $SK = H_1(V_i \parallel SID_j \parallel H_1\left(\kappa_j\right) \parallel T_1 \parallel T_3)$, $M_i{}' = H_1(SK \parallel SID_j \parallel T_3)$, checks if $M_i{}' = M_i$. If they are equal, U_i believes he negotiates a session key SK with S_j.

B. WEAKNESSES OF SONI *et al.*'s SCHEME

We reveal the vulnerabilities of Soni *et al.*'s scheme in this subsection.

1) FORWARD SECRECY

When the adversary compromises the private key s and the master key mk of GW, and intercepts $\{DID_i, G_i, R_i, K_i, T_1\}$, $\{W_i, L_i, T_2, T_1\}$ and $\{Q_i, M_i, T_3\}$ from public channel. The adversary can reveal the session key as follows.

Step 1. The adversary computes $N_i = sR_i = \left((N_i)_x, (N_i)_y\right)$, $N = H_1((N_i)_x \parallel \left(N_i)_y\right)$, $PID_i = DID_i \oplus N$, $A_i = H_1\left(PID_i \parallel s\right)$.

Step 2. The adversary computes $SID_j = G_i \oplus H_1(A_i \parallel N)$, $\kappa_j = H_1(SID_j \parallel mk)$, $V_i = W_i \oplus H_1(\kappa_j \parallel T_2 \parallel T_1)$.

Step 3. The adversary computes $SK = H_1(V_i \parallel SID_j \parallel H_1\left(\kappa_j\right) \parallel T_1 \parallel T_3)$.

2) THREE-FACTOR SECURITY

Suppose that the smart card's parameters $\{C_i, E_i, F_i, \theta_i\}$ and the biometric b_i are compromised, the adversary can reveal the password as follows.

Step 1. The adversary computes $Rep\left(b_i, \theta_i\right) = (\sigma_i)$.

Step 2. The adversary chooses a pair of (ID_i^*, PW_i^*) from dictionary space.

Step 3. The adversary computes $r_1^* = E_i \oplus H_1(ID_i^* \parallel PW_i^* \parallel \sigma_i)$, $PID_i^* = H_1(r_1^* \parallel ID_i^*)$, $B_i^* = H_1(PW_i^* \parallel r_1^*)$, $C_i^* = H_1(B_i^* \parallel PID_i^*)$.

Step 4. The adversary checks if $C_i^* = C_i$. If they are equal, it shows that (ID_i^*, PW_i^*) are the correct identity and password of U_i. Otherwise, go to step 2, until $\mathcal{A}$ finds the correct one.

To perform the above attack, the adversary needs to execute a deterministic reproduction function, and compute hash function 3 times for every pair of (ID_i^*, PW_i^*). The time complexity of this attack is $\mathcal{O}(3T_H * |D_{ID}| * |D_{PW}|)$, where T_H denotes the executing time of hash function.

With the smart card and the biometric, the adversary is able to obtain the password. In addition, with $\{C_i, E_i, F_i, \theta_i\}$ and b_i, the adversary computes $A_i = F_i \oplus H_1(ID_i \oplus \sigma_i)$. Then he is able to impersonate the user successfully. Hence, Soni *et al.*'s scheme fails to achieve three-factor security.

3) SENSOR NODE CAPTURE ATTACK

Suppose that the adversary compromises the sensor node S_j, and obtains $\{SID_j, \kappa_j\}$, he can reveal the established session key between S_j and U_i in the following steps.

Step 1. The adversary intercepts $\{W_i, L_i, T_2, T_1\}$ and $\{Q_i, M_i, T_3\}$ from public channel.

Step 2. The adversary computes $V_i = W_i \oplus H_1(\kappa_j \parallel T_2 \parallel T_1)$, $SK = H_1(V_i \parallel SID_j \parallel H_1\left(\kappa_j\right) \parallel T_1 \parallel T_3)$.

If the unsuspecting user U_i continues to access the compromised S_j, the adversary can compute the session key between S_j and U_i as above. The adversary can reveal the old and future session keys between S_j and U_i. Therefore, Soni *et al.*'s scheme is vulnerable to sensor node capture attack.

IV. THE PROPOSED SCHEME

The proposed scheme is comprised of five phases, that is, pre-deployment phase, user registration phase, medical sensor node registration phase, login and authentication phase, and password update phase. The participants consist of the user U_i, the medical sensor node S_j, and the gateway GW.

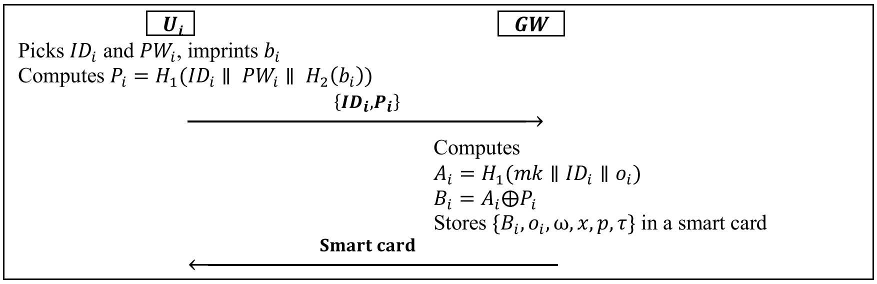


FIGURE 2. User registration phase of the proposed scheme.

GW is responsible for generating the system parameters, managing user and server registration, and assisting the user and the medical sensor node to perform mutual authentication and session key establishment.

A. PRE-DEPLOYMENT PHASE

GW chooses its master key mk. GW chooses two large primes μ, ν, where $\mu \equiv 3(mod\,4), \nu \equiv 3(mod\,4)$, and computes $\omega = \mu\nu$. Then GW selects the Chebyshev polynomial's parameters p, x, where p is a big prime, $x\epsilon[-\infty, +\infty]$. GW chooses a positive integer τ conforming to $2^8 \leq \tau \leq 2^{10}$. GW chooses a hash function $H_1(\cdot)$ and a biohashing function $H_2(\cdot)$. Biohashing function is used to transform the biometric into a unique compact code. GW keeps mk, μ, ν as secret, publishes p, x.

B. USER REGISTRATION PHASE

In this phase, the user sends an enrollment request to GW as described in Figure 2.

Step 1. U_i picks his identity ID_i and password PW_i, imprints his biometric b_i, and computes $P_i = H_1(ID_i \parallel PW_i \parallel H_2(b_i))$. Afterwards, U_i sends the registration request $\{ID_i, P_i\}$ to GW via the confidential channel.

Step 2. Upon getting $\{ID_i, P_i\}$, GW chooses a random number o_i, and computes $A_i = H_1(mk \parallel ID_i \parallel o_i)$, $B_i = A_i \oplus P_i$. GW saves $\{ID_i, o_i, cou = 0\}$ in the database. GW stores $\{B_i, o_i, \omega, x, p, \tau\}$ in a smart card, and delivers it to U_i in a secure way.

Step 3. U_i computes $V_i = H_1(P_i)\, mod \tau$, stores V_i in the smart card.

C. MEDICAL SENSOR NODE REGISTRATION PHASE

S_j enrolls in GW as follows.

Step 1. S_j chooses its identity SID_j, and delivers $\{SID_j\}$ to GW via the confidential channel.

Step 2. Upon getting $\{SID_j\}$, GW computes $\kappa_j = H_1(SID_j \parallel mk)$. GW delivers $\{\kappa_j\}$ to S_j via the confidential channel.

Step 3. S_j stores the secret key κ_j securely.

D. AUTHENTICATION AND KEY AGREEMENT PHASE

U_i accesses S_j with the help of GW as described in Figure 3.

Step 1. U_i enters ID_i^*, PW_i^*, imprints b_i^*. The smart card computes $P_i^* = H_1(ID_i^* \parallel PW_i^* \parallel H_2(b_i^*))$, $V_i^* = H_1\left(P_i^*\right) mod\, \tau$, and checks if $V_i^* = V_i$. If they are equal, the smart card selects a nonce α, and calculates $A_i^* = B_i \oplus P_i^*$, $G_i = H_1(A_i^* \parallel \alpha)$, $N_i = T_{G_i}(x)$, $F_i = (ID_i^* \parallel N_i \parallel SID_j \parallel o_i)^2 mod\, \omega$, $C_i = H_1(A_i^* \parallel F_i \parallel N_i \parallel T_1)$, where T_1 is the current timestamp. The smart card delivers $\{F_i, C_i, T_1\}$ to GW.

Step 2. After getting $\{F_i, C_i, T_1\}$, GW verifies whether T_1 is valid. If it is not valid, the protocol aborts. Otherwise, GW uses μ, ν to decrypt F_i, and gets $(ID_i \parallel N_i \parallel SID_j \parallel o_i{}')$. GW retrieves o_i from the database using ID_i, checks if $o_i{}' = o_i$. If they are not equal, the protocol aborts. Otherwise, GW computes $A_i = H_1(mk \parallel ID_i \parallel o_i)$, $C_i{}' = H(A_i \parallel F_i \parallel N_i \parallel T_1)$, verifies if $C_i{}' = C_i$. If they are equal, GW computes $\kappa_j = H_1(SID_j \parallel mk)$, $E_i = H_1(\kappa_j \parallel T_2) \oplus N_i$, $K_i = H_1(\kappa_j \parallel E_i \parallel T_2)$, where T_2 is the current timestamp. GW delivers $\{E_i, K_i, T_2\}$ to S_j. If $C_i{}' \neq C_i$, it indicates that in all probability U_i's smart card has been compromised. GW performs $cou = cou{+}1$. When $cou \geq 10$, GW suspends U_i's smart card. The protocol aborts.

Step 3. After receiving $\{E_i, K_i, T_2\}$, S_j verifies the validity of T_2. Then S_j computes $K_i{}' = H_1(\kappa_j \parallel E_i \parallel T_2)$, verifies if $K_i{}' = K_i$. If they are equal, S_j chooses a nonce β. S_j calculates $N_s = T_\beta(x)$, $N_i = E_i \oplus H_1(\kappa_j \parallel T_2)$, $SK = T_\beta(N_i)$, $L_i = H_1(SK \parallel N_S)$, $M_i = H_1(\kappa_j \parallel L_i \parallel N_i \parallel N_S)$. S_j delivers $\{N_s, L_i, M_i\}$ to GW.

Step 4. Upon getting $\{N_s, L_i, M_i\}$, GW computes $M_i{}' = H_1(\kappa_j \parallel L_i \parallel N_i \parallel N_S)$, verifies if $M_i{}' = M_i$. If they are equal, GW delivers $\{N_s, L_i\}$ to U_i.

Step 5. After receiving $\{N_s, L_i\}$, the smart card computes $SK = T_{G_i}(N_S)$, $L_i{}' = H_1(SK \parallel N_S)$, verifies if $L_i{}' = L_i$. If they are equal, U_i believes he negotiates a session key with S_j.

E. PASSWORD UPDATE PHASE

U_i updates the password as shown in Figure 4.

Step 1. U_i enters ID_i^* and PW_i^*, imprints b_i^*. The smart card computes $P_i^* = H_1(ID_i^* \parallel PW_i^* \parallel H_2(b_i^*))$,

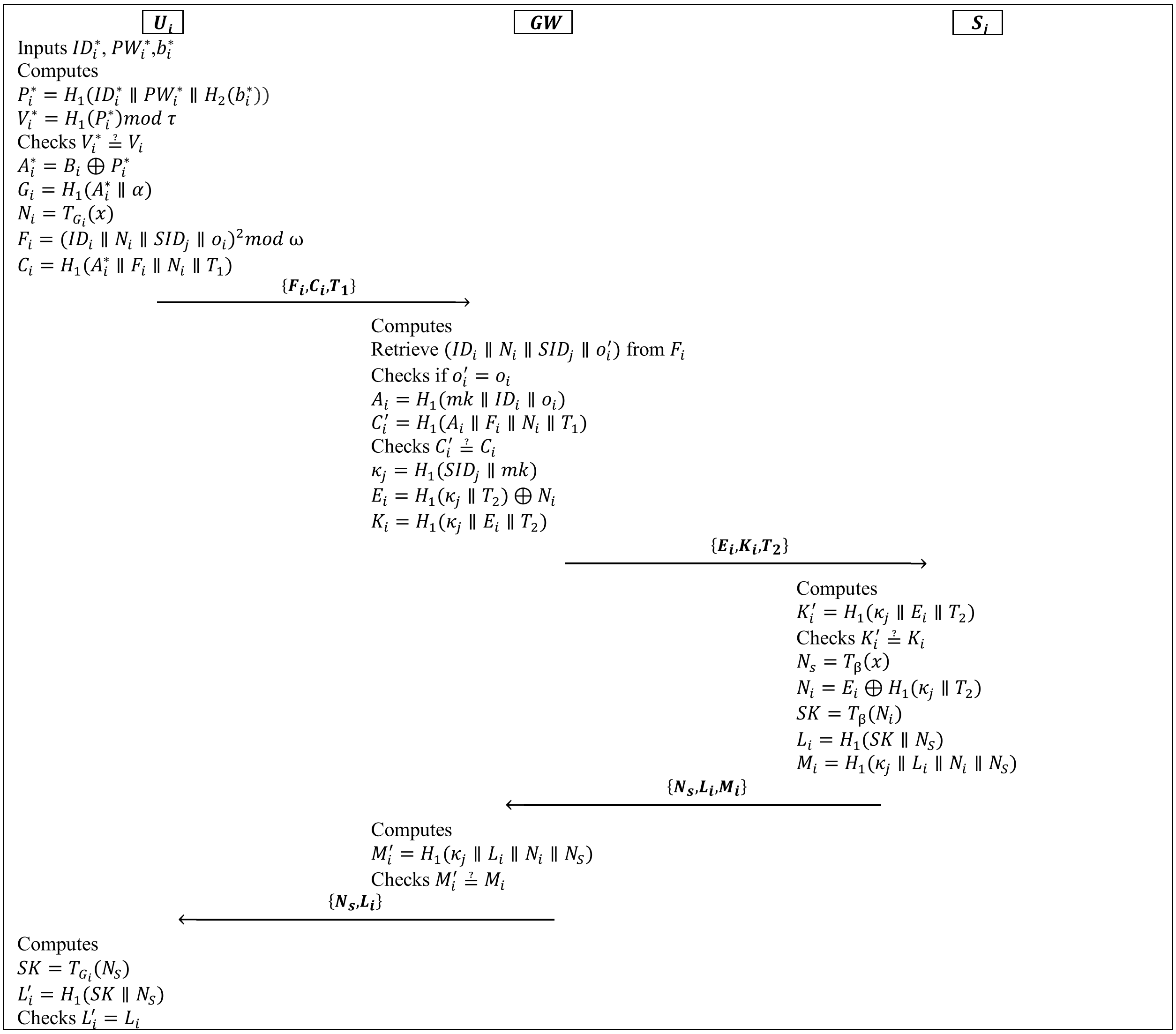


FIGURE 3. Login and authentication phase of the proposed scheme.

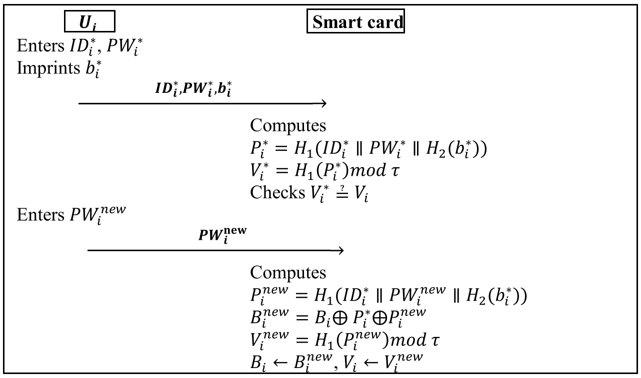


FIGURE 4. Password update phase of the proposed scheme.

$V_i^* = H_1\left(P_i^*\right) mod \tau$, and checks if $V_i^* = V_i$. If it does not hold, the protocol aborts.

Step 2. U_i enters a new password PW_i^{new}. The smart card calculates $P_i^{new} = H_1(ID_i^* \parallel PW_i^{new} \parallel H_2(b_i^*))$, $B_i^{new} = B_i \oplus P_i^* \oplus P_i^{new}$, $V_i^{new} = H_1\left(P_i^{new}\right) mod \tau$. The smart card removes V_i, B_i, and stores V_i^{new}, B_i^{new} in the memory.

V. SECURITY ANALYSIS

We give the rigorous security analysis of our scheme in this section. Firstly, Burrows–Abadi–Needham (BAN) logic [35] proof shows the completeness of our scheme. Then the formal analysis under RO model demonstrates that our scheme is provably secure. Besides, the informal analysis proves that our scheme is not susceptible to any weakness and provides desired attributes.

A. BAN LOGIC PROOF OF OUR SCHEME

We use the BAN logic analysis to confirm the mutual authentication and session key establishment features of our scheme. Table 2 summarizes the notations and rules of BAN logic.

TABLE 2. **The notations and rules of BAN logic.**

Symbols	Description
P, Q	A principal
X	A statement
$P \lhd X$	P sees X, P gets X
$P\| \sim X$	P said X, X was sent by P
$\overset{K}{\to} P$	K is the public key of P
$P \overset{K}{\leftrightarrow} Q$	The key K is only known to P and Q
$< X >_K$	X is combined with K
$\{X\}_K$	X is encrypted using K
$\#(X)$	X is fresh
$P\| \equiv X$	P has faith in the truth of X
$P \Rightarrow X$	P has jurisdiction over X
Rule 1: Message meaning rule	$\frac{P\|\equiv P\overset{K}{\leftrightarrow}Q\ ,P\lhd<X>_K}{P\|\equiv Q\|\sim X}$ or $\frac{P\|\equiv\overset{K}{\to}Q\ ,P\lhd\{X\}_K}{P\|\equiv Q\|\sim X}$
Rule 2: Nonce-verification rule	$\frac{P\|\equiv\#(X),P\|\equiv Q\|\sim X}{P\|\equiv Q\|\equiv X}$
Rule 3: Jurisdiction rule	$\frac{P\|\equiv Q\Rightarrow X,P\|\equiv Q\|\equiv X}{P\|\equiv X}$
Belief rule	$\frac{P\|\equiv Q\|\equiv(X,Y)}{P\|\equiv Q\|\equiv X}$

Our scheme is supposed to meet the goals as below.

- Goal 1: $S_j| \equiv U_i| \equiv (U_i \xleftrightarrow{SK} S_j)$
- Goal 2: $S_j| \equiv (U_i \xleftrightarrow{SK} S_j)$
- Goal 3: $U_i| \equiv S_j| \equiv (U_i \xleftrightarrow{SK} S_j)$
- Goal 4: $U_i| \equiv (U_i \xleftrightarrow{SK} S_j)$

We give the idealized form of our scheme as follows.

- M1: $U_i \to GW\ < \{ID_i, N_i\}_\omega, T_1 >_{A_i}$
- M2: $GW \to S_j\ < U_i| \equiv N_i, T_2 >_{\kappa_j}$
- M3: $S_j \to GW\ < N_s, L_i, N_i >_{\kappa_j}$
- M4: $GW \to U_i < N_S, S_j| \equiv U_i \xleftrightarrow{SK} S_j, N_i >_{A_i}$

The initial assumptions of our scheme are as follows.

- A1: $GW| \equiv GW \xleftrightarrow{A_i} U_i, GW| \equiv \xrightarrow{\omega} GW$
- A2: $GW| \equiv \#(T_1)$
- A3: $GW| \equiv U_i \Rightarrow < ID_i, N_i >$
- A4: $S_j| \equiv GW \xleftrightarrow{\kappa_j} S_j$
- A5: $S_j| \equiv \#(T_2)$
- A6: $S_j\ |\equiv GW \Rightarrow (U_i| \equiv N_i)$
- A7: $S_j| \equiv U_i \Rightarrow (U_i \xleftrightarrow{SK} S_j)$
- A8: $GW| \equiv GW \xleftrightarrow{\kappa_j} S_j$
- A9: $GW| \equiv \#(N_i)$
- A10: $GW| \equiv S_j \Rightarrow < N_s, L_i >$
- A11: $U_i| \equiv GW \xleftrightarrow{A_i} U_i$
- A12: $U_i| \equiv \#(N_i)$
- A13: $U_i| \equiv GW \Rightarrow (S_j| \equiv U_i \xleftrightarrow{SK} S_j)$
- A14: $U_i| \equiv S_j \Rightarrow (U_i \xleftrightarrow{SK} S_j)$

The proof is as below.

According to M1, we have

(1) $GW \lhd <\{ID_i, N_i\}_\omega, T_1 >_{A_i}$

In accordance with (1), A1, and Rule 1, we have

(2) $GW| \equiv U_i| \sim <ID_i, N_i, T_1 >$

In the light of (2), A2, and Rule 2, we have

(3) $GW\ | \equiv U_i| \equiv <ID_i, N_i >$

In accordance with (3), A3, and Rule 3, we have

(4) $GW| \equiv <ID_i, N_i >$

According to M2, we have

(5) $S_j \lhd\ < U_i| \equiv N_i, T_2 >_{\kappa_j}$

In accordance with (5), A4, and Rule 1, we have

(6) $S_j\ | \equiv GW| \sim < U_i| \equiv N_i, T_2 >$

In accordance with (6), A5, and Rule 2, we have

(7) $S_j\ | \equiv GW| \equiv (U_i| \equiv N_i)$

In accordance with (7), A6, and Rule 3, we have

(8) $S_j| \equiv U_i| \equiv N_i$

In accordance with (8), and $SK = T_\beta(N_i)$, we have

(9) $S_j| \equiv U_i| \equiv (U_i \xleftrightarrow{SK} S_j)$ **Goal 1**

In accordance with (9), A7, and Rule 3, we have

(10) $S_j| \equiv (U_i \xleftrightarrow{SK} S_j)$ **Goal 2**

According to M3, we have

(11) $GW \lhd <N_s, L_i, N_i >_{\kappa_j}$

In accordance with (11), A8, and Rule 1, we have

(12) $GW| \equiv S_j| \sim <N_s, L_i, N_i >$

In accordance with (12), A9, and Rule 2, we have

(13) $GW| \equiv S_j| \equiv <N_s, L_i >$

In accordance with (13), A10, and Rule 3, we have

(14) $GW| \equiv <N_s, L_i >$

According to M4, we have

(15) $U_i \lhd < N_S, S_j| \equiv U_i \xleftrightarrow{SK} S_j, N_i >_{A_i}$

In accordance with (15), A11, and Rule 1, we have

(16) $U_i| \equiv GW| \sim <N_S, S_j| \equiv U_i \xleftrightarrow{SK} S_j, N_i >$

In accordance with (16), A12, and Rule 2, we have

(17) $U_i\ | \equiv GW| \equiv <N_S, S_j| \equiv U_i \xleftrightarrow{SK} S_j >$

In accordance with (17), A13, and Rule 3, we have

(18) $U_i| \equiv S_j| \equiv (U_i \xleftrightarrow{SK} S_j)$ **Goal 3**

In accordance with (18), A14, and Rule 3, we have

(19) $U_i| \equiv (U_i \xleftrightarrow{SK} S_j)$ **Goal 4**

B. FORMAL SECURITY ANALYSIS IN RO MODEL

On the basis of the security model introduced by Wang and Wang [32], we demonstrate that our scheme is provably secure.

1) SECURITY MODEL

Participants: The entities of authentication scheme for WMSNs comprise the user U_i, the gateway GW, the medical sensor node S_j. Every principal involves multiple instances, i.e., U_i^a, GW^a, and S_j^a.

Queries: The adversary is allowed to make the following queries.

Execute (U_i^a, GW^a, S_j^a)*:* It corresponds to the passive attack. The adversary gets the exchanged messages in public channel through this query.

Send $(U_i^a/GW^a/S_j^a, m)$*:* It corresponds to the active attack. The adversary masquerades as an entity to send a message m. If m is valid, the oracle returns a response message.

Reveal (U_i^a, S_j^a)*:* If the entity U_i^a or S_j^a does not have a session key SK, the oracle sends back an invalid symbol $\perp$. Otherwise, it sends back SK.

Corrupt (U_i^a, z)*:* The adversary is able to get at most two kinds of user authentication factors through this query.

In case that $z = 1$, the oracle discloses the password of U_i^a.

In case that $z = 2$, the oracle discloses the parameters of U_i^a's smart card.

In case that $z = 3$, the oracle discloses the biometric of U_i^a.

Corrupt (GW^a, S_j^a)*:* It is used to test forward secrecy. The oracle returns the secret key of gateway and the medical sensor node to the adversary.

Test (U_i^a, S_j^a)*:* It is employed to test the semantic security of session key. The adversary is capable of asking this query at most once. If U_i^a or S_j^a is fresh (see below) and has a session key SK, the oracle flips a coin b. In case $b = 1$, SK is sent back to the adversary. Otherwise, an equal-length random string is sent back to the adversary. If U_i^a or S_j^a is not fresh, it returns $\perp$.

Freshness: The instance U_i^a or S_j^a is fresh, if it satisfies

1. The instance is accepted, and generates a session key SK.
2. The adversary does not ask Corrupt (GW^a, S_j^a) query or Reveal (U_i^a, S_j^a) query.

Semantic Security: If the adversary is able to distinguish whether the value answered by Test (U_i^a, S_j^a) query is the session key or not, we say the adversary breaks the semantic security. The advantage that the adversary $\mathcal{A}$ wins the game is defined as:

$$Adv_P^{ake}(\mathcal{A}) = 2Pr\left(b' = b\right) - 1.$$

We say the authentication scheme is semantically secure, if the advantage for any adversary is ignorable.

2) FORMAL SECURITY ANALYSIS

Theorem 1: Let the frequency distribution of users' passwords conform to Zipf's law [31]. Suppose that the polynomial-time adversary $\mathcal{A}$ can ask at most q_e Execute queries, q_s Send queries, q_h Hash queries, and q_b Biohashing queries. The advantage that $\mathcal{A}$ breaks the semantic security of our scheme is

$$Adv_P^{ake}(\mathcal{A}) \leq \frac{q_h^2 + 6q_s}{2^{l_1}} + \frac{q_b^2 + 2q_s}{2^{l_2}} + \frac{(q_s + q_e)^2}{p} + 2C' * q_s^{s'} + 2q_h Adv_P^{CHDHP}.$$

where l_1, l_2 are the bit length of hash value, biohashing value, respectively. D_{PW} denotes the password space. C' and s' are the parameters of Zipf distribution. Adv_P^{CHDHP} denotes the advantage that $\mathcal{A}$ solves CHDHP. Take the Tianya password data set [36] for an example, $|D_{PW}| \approx 13$ *million*, $C' = 0.062239$, $s' = 0.155478$.

The Proof: The games G_i $(0 \leq i \leq 6)$ are defined to get $Adv_P^{ake}(\mathcal{A})$. $Pr[S_i]$ denotes the probability that $\mathcal{A}$ correctly guesses the values of b in G_i.

G_0 : This game emulates the real attack. Consequently, we have,

$$Adv_P^{ake}(\mathcal{A}) = 2\left(Pr[S_0]\right) - 1. \tag{1}$$

G_1: In G_1, a hash list Λ_H and a biohashing list Λ_{bH} are created for modeling the hash oracle and the biohashing oracle. When the adversary makes a hash query $H_1(\gamma)$, the oracle uses γ to search Λ_H. If there exists the hash value of γ in Λ_H, it answers the hash value. Otherwise, it sends back a random number ψ to the adversary, and stores (γ, ψ) in Λ_H. The biohashing oracle is simulated similarly with the hash oracle. Obviously, G_1 and G_0 are indistinguishable. We have

$$Pr[S_0] - Pr[S_1] = 0. \tag{2}$$

G_2 : In this game, if the following collisions occur, the game aborts.

(1) There is a collision on hash values or biohashing outputs, the probability is $q_h^2/2^{l_1+1} + q_b^2/2^{l_2+1}$.

(2) There is a collision on message transcripts, the probability is $(q_s + q_e)^2/2p$.

We have

$$|Pr[S_1] - Pr[S_2]| \leq \frac{q_h^2}{2^{l_1+1}} + \frac{q_b^2}{2^{l_2+1}} + \frac{(q_s + q_e)^2}{2p}. \tag{3}$$

G_3 : G_3 aborts if $\mathcal{A}$ guesses C_i, K_i, M_i, L_i without asking hash query. The probability is no more than $q_s/2^{l_1}$. We have

$$|Pr[S_2] - Pr[S_3]| \leq q_s/2^{l_1}. \tag{4}$$

G_4 : G_4 aborts if $\mathcal{A}$ guesses authentication parameter A_i directly. The probability is no more than $q_s/2^{l_1}$. We have

$$|Pr[S_3] - Pr[S_4]| \leq q_s/2^{l_1}. \tag{5}$$

G_5 : G_5 aborts if $\mathcal{A}$ has calculated A_i by means of Corrupt (U_i^a, z) query. There are three cases involved.

In case Corrupt $(U_i^a, z = 1, 2)$. The probability that $\mathcal{A}$ guesses user's biometric is no more than $q_s/2^{l_2}$.

In case Corrupt $(U_i^a, z = 2, 3)$. The probability that $\mathcal{A}$ guesses user's password is no more than $C' * q_s^{s'}$.

In case Corrupt $(U_i^a, z = 1, 3)$. The probability that $\mathcal{A}$ guesses the value of B_i is less than $q_s/2^{l_1}$.

We have

$$|Pr[S_4] - Pr[S_5]| \leq q_s * \left(\frac{1}{2^{l_1}} + \frac{1}{2^{l_2}}\right) + C' * q_s^{s'}. \tag{6}$$

G_6 : In this game, the private hash oracles $H_1{}'$ instead of the hash oracle H_1 is employed to compute L_i. As $H_1{}'$ is unavailable to the adversary. Consequently, we have

$$Pr[S_6] = \frac{1}{2}. \tag{7}$$

G_6 and G_5 are indistinguishable, unless $\mathcal{A}$ asks the hash query $H_1(SK \| N_S)$. We use Λ_1 to denote this event. Thus, we have

$$|Pr[S_5] - Pr[S_6]| \leq Pr[\Lambda_1]. \tag{8}$$

If $\mathcal{A}$ has asked the hash query $H_1(SK \parallel N_S)$, there must be a tuple including SK in Λ_H. Through randomly choosing in Λ_H, the probability that we get SK is $\frac{1}{q_h}$. SK is a solution of CHDHP, hence we have

$$Pr[\Lambda_1] \leq q_h Adv_P^{CHDHP}. \tag{9}$$

In the light of (1)-(9), we have

$$Adv_P^{ake}(\mathcal{A}) \leq \frac{q_h^2 + 6q_s}{2^{l_1}} + \frac{q_b^2 + 2q_s}{2^{l_2}} + \frac{(q_s + q_e)^2}{p} + 2C' * q_s^{s'} + 2q_h Adv_P^{CHDHP}. \tag{10}$$

C. INFORMAL ANALYSIS

We prove that our scheme can withstand known attacks and achieve desired properties in this section.

1) RESISTANCE TO OFF-LINE GUESSING ATTACK

Suppose that $\mathcal{A}$ attempts to guess user's identity and password, under the circumstances the biometric and the smart card are compromised. $\mathcal{A}$ chooses a pair of (ID_i^*, PW_i^*) from dictionary space, computes $V_i^* = H_1(H_1(ID_i^* \parallel PW_i^* \| H_2(b_i^*))mod\,\tau$, checks if $V_i^* = V_i$. However, our scheme employs the fuzzy validation value V_i as suggested in [32]. When $\tau = 2^8$, and ID_i, PW_i are both 64 bits, there are $\frac{2^{64}*2^{64}}{2^8}$ pairs of identity and password conforming to $V_i^* = V_i$. In addition, our scheme employs the "honeywords" technique [32] to prevent online guessing attack. The smart card and GW store a random number o_i. If the adversary compromises the smart card, he can obtain o_i. When GW receives a login request generated using the correct o_i along with an erroneous A_i. GW regards that it comes from an attacker who has compromised user's smart card. GW uses a counter *Cou* to record the suspicious login. When the number of suspicious login reaches the preset maximum value, such as 10, the smart card is suspended. Consequently, our scheme is secure against off-line guessing attack, even the biometric and smart card are compromised.

2) RESISTANCE TO REPLAY ATTACK

In the messages $\{F_i, C_i, T_1\}$ and $\{E_i, K_i, T_2\}$, the timestamp mechanism is used to prevent replay attack. The timestamps T_1, T_2 are involved in the hash values C_i, K_i, it makes sure that they are not tampered with. The messages $\{N_s, L_i, M_i\}$ and $\{N_s, L_i\}$ are generated using N_i, the recipients can verify the freshness of messages based on the nonce α. For the messages $\{F_i, C_i, T_1\}$ and $\{E_i, K_i, T_2\}$, the timestamps are essential to verify the freshness of messages. For the messages $\{N_s, L_i, M_i\}$ and $\{N_s, L_i\}$, the freshness of messages can be verified based on the nonce α. They do not use timestamps any more. It helps to improve efficiency.

3) RESISTANCE TO SESSION-SPECIFIC TEMPORARY INFORMATION ATTACK

In our scheme, the session key is computed based on $SK = T_\beta(N_i) = T_{H_1(A_i\|\alpha)}(N_S)$. In case of getting the nonce α, A_i is still required to compute $T_{H_1(A_i\|\alpha)}(N_S)$. To get A_i, the adversary needs to compromise the master key of GW or break the smart card, the password, and the biometric of U_i. In case of getting the nonce β, N_i is still required to compute $T_\beta(N_i)$. To retrieve N_i, $\mathcal{A}$ needs to compromise GW's secret key μ, ν or S_j's secret key κ_j. $\mathcal{A}$ can not compute $T_{H_1(A_i\|\alpha)}(N_S)$ or $T_\beta(N_i)$. Therefore, our scheme is secure against such an attack.

4) FORWARD SECRECY

When the master key *mk* is disclosed, $\mathcal{A}$ computes $\kappa_j = H_1(SID_j \parallel mk)$, $N_i = E_i \oplus H_1(\kappa_j\|T_2)$. However, to derive SK from N_i, N_S, there is no alternative but to solve CHDHP. Hence, our scheme preserves forward secrecy.

5) RESISTANCE TO SESSION KEY DISCLOSURE ATTACK

To compute $SK = T_\beta(N_i) = T_{H_1(A_i\|\alpha)}(N_S)$, $\mathcal{A}$ needs to get N_i, β or $H_1(A_i\|\alpha)$. To retrieve N_i, $\mathcal{A}$ has to compromise the secret key μ, ν or κ_j. Moreover, To retrieve β from N_s, $\mathcal{A}$ needs to solve CHLDP. To get $H_1(A_i\|\alpha)$, A_i and α are required. α is a random number only known to U_i. To get A_i, the adversary needs to compromise the master key of GW or break the smart card, the password, and the biometric of U_i. $\mathcal{A}$ cannot compute $T_\beta(N_i)$ or $T_{H_1(A_i\|\alpha)}(N_S)$, therefore $\mathcal{A}$ cannot disclose the session key in our scheme.

With the help of Rabin cryptosystem and chaotic maps, the secure session key is established at a minimum cost. As analyzed above, under no circumstances can the session key be revealed by $\mathcal{A}$.

6) RESISTANCE TO KNOWN KEY ATTACK

In our scheme, the session key is established based on the random numbers α, β and the secret A_i. A_i is protected by CHLDP and hash function. Even $\mathcal{A}$ has obtained the previous session key, he cannot get A_i. Without α, β, A_i, $\mathcal{A}$ is unable to compute the session key.

7) RESISTANCE TO FORGERY ATTACK

In the messages $\{F_i, C_i, T_1\}$, $\{E_i, K_i, T_2\}$, $\{N_s, L_i, M_i\}$, to ensure message integrity and identity of the sender, the hash values C_i, K_i, L_i are generated using the transmitted parameters along with the authentication value A_i or the secret key κ_j. To forge a message, the adversary has to reveal A_i or κ_j. Besides, to forge the message $\{N_s, L_i\}$, the adversary chooses a random number β, and computes $N_s = T_\beta(x)$. However, to compute L_i, $\mathcal{A}$ needs to compromise μ, ν or κ_j to retrieve N_i. As A_i, κ_j, μ, ν are unavailable, our scheme is secure against forgery attack.

8) RESISTANCE TO MAN-IN-THE-MIDDLE ATTACK

$\mathcal{A}$ can intercept messages from public channel. However, as A_i, κ_j, μ, ν are unavailable, $\mathcal{A}$ is unable to generate valid messages to deceive any two communicating parties. Therefore, our scheme is resistant to man-in-the-middle attack.

9) USER ANONYMITY

In our scheme, only GW who knows μ, ν is able to retrieve ID_i from F_i. In addition, F_i changes with the nonce α in each session. The adversary $\mathcal{A}$ cannot track the user action. Consequently, the proposed scheme preserves user anonymity.

10) RESISTANCE TO DE-SYNCHRONIZATION ATTACK

As the hash values C_i, K_i, M_i, L_i are employed to ensure message integrity. If $\mathcal{A}$ modifies the parameters of a message and sends the modified message to the receiver, the modified message will not be verified to be valid. In addition, if a message is blocked by $\mathcal{A}$, as user's authentication parameters

TABLE 3. Security attributes of the relevant schemes.

Security attributes	Soni et al. [27]	Mao et al. [24]	Li et al. [37]	Our Scheme
User anonymity	√	√	√	√
Resist privileged insider attack	√	√	×	√
Resist man-in-the-middle attack	√	√	×	√
Resist off-line guessing attack	√	√	√	√
Resist session key disclosure attack	√	√	√	√
Resist forgery attack	√	√	×	√
Resist replay attack	√	√	×	√
Resist known session-specific temporary information attack	√	×	×	√
Forward secrecy	×	√	√	√
Three-factor security	×	√	×	√
Sensor node capture attack	×	√	√	√

are not changed, the user can continue to access the medical sensor nodes.

11) RESISTANCE TO PRIVILEGED INSIDER ATTACK

The user never discloses his password or biometric to GW in the registration request. In addition, as A_i is unknown to the medical sensor node, the medical sensor node cannot impersonate the user or GW successfully. As κ_j is unknown to the user, the user cannot impersonate the medical sensor node or GW successfully. Consequently, our scheme can withstand this attack.

12) RESISTANCE TO SENSOR NODE CAPTURE ATTACK

Assume that $\mathcal{A}$ compromises the sensor node S_j, $\mathcal{A}$ obtains the secret key κ_j and the identity SID_j. However, with κ_j and SID_j, $\mathcal{A}$ is unable to reveal the secret parameter A_i or the identity of user, as they are protected with hash function and symmetric encryption. Furthermore, $\mathcal{A}$ is unable to reveal the master key mk of the gateway, as hash function is irreversible. The secret key μ, ν is kept secret by the gateway. Besides, the random number β is only known to S_j. Without β, $\mathcal{A}$ is unable to compute the established session key between U_i and S_j. $\mathcal{A}$ cannot reveal any secret parameter based on κ_j and SID_j, hence our scheme is secure against sensor node capture attack.

13) THREE-FACTOR SECURITY

We demonstrate that our scheme provides three-factor security as follows.

1) As analyzed in off-line guessing attack, when the smart card and the biometric are compromised, $\mathcal{A}$ is unable to reveal the password.
2) Suppose that $\mathcal{A}$ obtains user's password as well as smart card. However, the calculation of hash function is irreversible, $\mathcal{A}$ is unable to reveal $H_2(b_i)$ from V_i.
3) Suppose that $\mathcal{A}$ obtains user's password as well as biometric. He attempts to disclose the parameters of the smart card. However, as A_i is protected by the hash function, $\mathcal{A}$ is unable to retrieve the critical parameter B_i.
4) A_i is unavailable, therefore $\mathcal{A}$ is unable to impersonate the legitimate user successfully.

VI. SECURITY AND PERFORMANCE COMPARISON

We provide the comparative analysis of our scheme and some representative schemes [24], [27], [37] in this section. When evaluating the computation and communication overheads, we concern with the login and authentication phase.

Based on the adversary model introduced by Wang *et al.* [29], we cryptanalyze the relevant schemes and present the analysis results in Table 3. We note that only our scheme fulfils all security attributes. While Soni *et al.*'s scheme [27] suffers from sensor node capture attack, no forward secrecy, and the violation of three-factor security. Li *et al.*'s scheme [37] is vulnerable to various weaknesses like forgery attack, man-in-the-middle attack, and replay attack, etc. Mao *et al.*'s scheme [24] provides many security attributes, but is flawed with known session-specific temporary information attack.

We evaluate the computation and communication overheads of the relevant schemes and present the results in Table 4. Specifically, T_H, T_{BH}, T_P, T_M, T_Q, T_C, T_F represent a hash operation, a biohashing operation, a point multiplication operation, a modular square operation, solving a quadratic residue, the calculation of Chebyshev polynomial, the execution of probabilistic generation function of fuzzy extractor, respectively. The computing time of "XOR" operation is ignorable. According to [38]–[40], the computation time of T_H, T_{BH}, T_P, T_M, T_Q, T_C, T_F are 0.5 ms, 21.02 ms, 63.075 ms, 1.896 ms, 3.481 ms, 21.02 ms, 63.075 ms, respectively. Our scheme requires $1T_{BH} + 5T_H + 2T_C + 1T_M$ in user end, $6T_H + 1T_Q$ in gateway, $4T_H + 2T_C$ in medical sensor node. The total running time of our scheme is $21.02 + 15 * 0.5 + 4 * 21.02 + 1.896 + 3.481 = 117.977$ms. The total running time of the relevant schemes [24], [27], [37] are 515.6 ms, 456.525 ms, 387.95 ms, respectively.

To evaluate the communication overhead, we assume that the timestamp, the random number, the user identity, the identity of sensor node, the hash value, and the

TABLE 4. Computing and communication overheads.

	Computing cost			Running time (ms)	Communication cost (bits)
	User (ms)	GW (ms)	Sensor (ms)		
Soni et al. [27]	$13T_H + 3T_P + 1T_F$ (258.8)	$12T_H + 3T_P$ (195.225)	$5T_H$ (2.5)	456.525	2272
Mao et al. [24]	$10T_H + 3T_P$ (194.225)	$7T_H + 3T_P$ (192.725)	$5T_H + 2T_P$ (128.65)	515.6	2048
Li et al. [37]	$8T_H + 2T_P + 1T_F$ (193.225)	$7T_H + 1T_P$ (66.575)	$4T_H + 2T_P$ (128.15)	387.95	1792
Our scheme	$1T_{BH} + 5T_H + 2T_C + 1T_M$ (67.456)	$6T_H + 1T_Q$ (6.481)	$4T_H + 2T_C$ (44.04)	117.977	2304

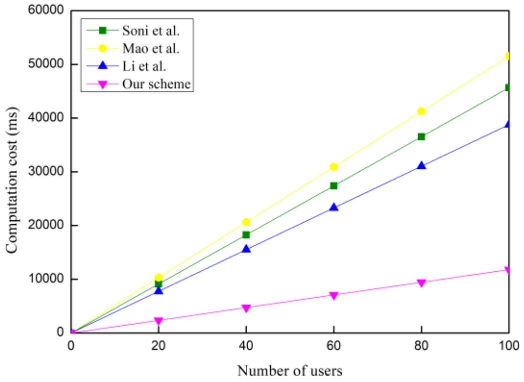


FIGURE 5. The total computation cost comparison.

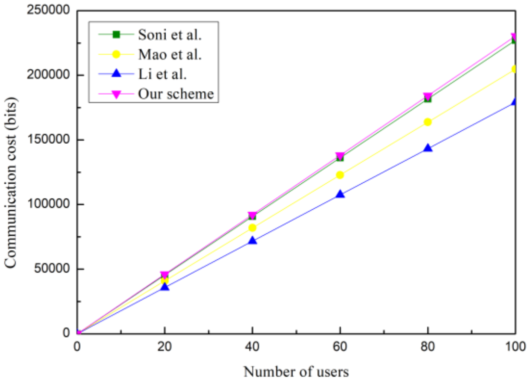


FIGURE 6. The total communication cost comparison.

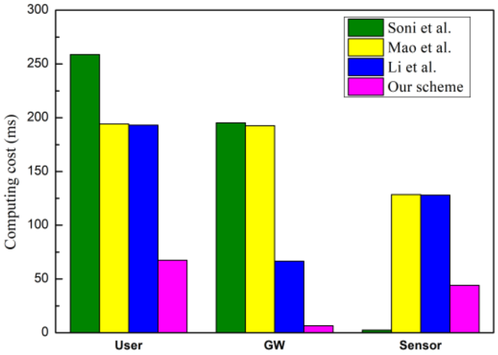


FIGURE 7. Computing cost comparison in each communication end.

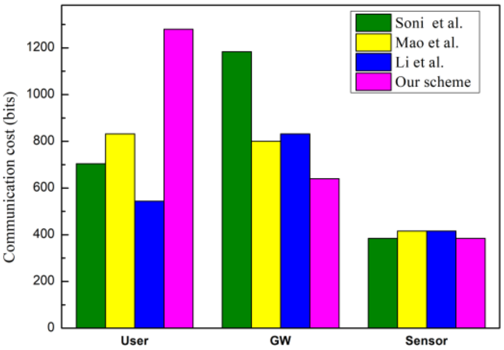


FIGURE 8. Communication cost comparison in each communication end.

Chebyshev polynomial are 128 bits. The point on elliptic curve group is 160 bits. The large integer ω is 1024 bits. Our scheme involves four messages, i.e., $\{F_i, C_i, T_1\}$, $\{E_i, K_i, T_2\}$, $\{N_s, L_i, M_i\}$, and $\{N_s, L_i\}$. C_i, K_i, M_i, L_i are hash values. N_s is a Chebyshev polynomial. E_i is generated by the XOR operation of a Chebyshev polynomial and a hash value. F_i is the result of modular square. T_1, T_2 are timestamps. The total communication overhead of our scheme is $128 * 10 + 1024 = 2304$ bits. The total communication overheads of the relevant schemes [24], [27], [37] are 2048 bits, 2272 bits, 1792 bits, respectively.

To present the comparison results more intuitively, we give the total computing overhead comparison and the total communication overhead comparison when the number of users ranges from 0 to 100 in Figure 5 and Figure 6. As shown in Figure 5, our scheme is more efficient than the relevant schemes. As shown in Figure 6, the total communication overhead of our scheme is slightly inferior to the relevant schemes, as Rabin cryptosystem is employed to enhance the security.

We present the comparisons of computing and communication overheads of each communication end in Figure 7 and Figure 8. It indicates that our scheme is not at a disadvantage except in the communication overhead of user end, as the Rabin encryption operation is performed in user end. Our scheme performs better, particularly for the resource-constrained sensor node. In terms of the computation cost of the sensor node, our scheme is second only to Soni *et al.*'s scheme. In terms of the communication cost of the sensor node, our scheme is equal to Soni *et al.*'s scheme and is superior to the other schemes. But Soni *et al.*'s scheme has weaknesses like sensor node capture attack. We note that, in Mao *et al.*'s scheme, the sensor node delivers the response message to the user directly. As the user generally is far away from the sensor node, the long-distance message transmission will increase quite a lot of energy consumption.

In summary, our scheme has lowest computation cost. Our scheme is slightly inferior to other schemes in communication overhead, as Rabin cryptosystem is employed to enhance the security. Moreover, the security of our scheme is better than the relevant schemes. Among these schemes, the security of Mao *et al.*'s scheme is closest to our scheme. But the computing overhead of Mao *et al.*'s scheme is 4.37 times more than our scheme. In addition, our scheme has high efficiency for the resource-constrained sensor node. Hence, our schemes is superior to the relevant schemes.

VII. CONCLUSION

In this paper, we reveal that Soni *et al.*'s scheme has weaknesses like sensor node capture attack, no forward secrecy, and the violation of three-factor security. To enhance the security and efficiency, we propose a novel scheme using Rabin cryptosystem and chaotic maps, in which we establish secure session key at a minimum cost. We use several security analysis methods to verify the correctness and security of our scheme. BAN logic analysis confirms that our scheme provides mutual authentication and session key agreement. The formal analysis in RO model shows that our scheme achieves semantic security. Moreover, the heuristic analysis indicates that our scheme is in accord with the security requirements of WMSNs. The comprehensive performance comparisons demonstrate that our scheme is better than the relevant schemes both in security and efficiency. Besides, our scheme incurs low energy consumption for the sensor node. Our scheme is more applicable to WMSNs. In the future, we plan to extend this work for multi-gateway wireless sensor networks.

REFERENCES

[1] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for E-Health systems in IoT," *Future Gener. Comput. Syst.*, vol. 96, pp. 410–424, Jul. 2019.

[2] O. Mir, J. Munilla, and S. Kumari, "Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 79–91, Jan. 2017.

[3] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3597–3604, Dec. 2012.

[4] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[5] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.

[6] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for E-Health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.

[7] C.-C. Chang, W.-Y. Hsueh, and T.-F. Cheng, "A dynamic user authentication and key agreement scheme for heterogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 447–465, Jul. 2016.

[8] W. Meng, Y. Wang, D. S. Wong, S. Wen, and Y. Xiang, "TouchWB : Touch behavioral user authentication based on Web browsing on smartphones," *J. Netw. Comput. Appl.*, vol. 117, pp. 1–9, Sep. 2018.

[9] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4081–4092, Sep. 2018.

[10] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," *Comput. Netw.*, vol. 73, pp. 41–57, Nov. 2014.

[11] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for mobile cloud computing," *Future Gener. Comput. Syst.*, vol. 62, pp. 190–195, Sep. 2016.

[12] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, Jan. 2016.

[13] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Depend. Sec. Comput.*, vol. 12, no. 4, pp. 428–442, Jul. 2015.

[14] J. Yu, G. Wang, Y. Mu, and W. Gao, "An efficient generic framework for three-factor authentication with provably secure instantiation," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2302–2313, Dec. 2014.

[15] T. Hayajneh, B. J. Mohd, M. Imran, G. Almashaqbeh, and A. V. Vasilakos, "Secure authentication for remote patient monitoring with wireless medical sensor networks," *Sensors*, vol. 16, no. 4, p. 424, 2016.

[16] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Electr. Eng.*, vol. 63, pp. 182–195, Oct. 2017.

[17] M. Shuai, B. Liu, N. Yu, and L. Xiong, "Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Jun. 2019, doi: 10.1155/2019/8145087.

[18] A. K. Das and A. Goswami, "A secure and efficient Uniqueness-and-Anonymity-Preserving remote user authentication scheme for connected health care," *J. Med. Syst.*, vol. 37, no. 3, p. 9948, Jun. 2013.

[19] P. Kumar, S.-G. Lee, and H.-J. Lee, "E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.

[20] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, Feb. 2015.

[21] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2643–2655, Oct. 2016.

[22] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 80, pp. 483–495, Mar. 2018.

[23] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.

[24] D. Mao, L. Zhang, X. Li, and D. Mu, "Trusted authority assisted three-factor authentication and key agreement protocol for the implantable medical system," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–16, Jul. 2018, doi: 10.1155/2018/7579161.

[25] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.

[26] Y. Chen, Y. Ge, Y. Wang, and Z. Zeng, "An improved three-factor user authentication and key agreement scheme for wireless medical sensor networks," *IEEE Access*, vol. 7, pp. 85440–85451, 2019, doi: 10.1109/ACCESS.2019.2923777.

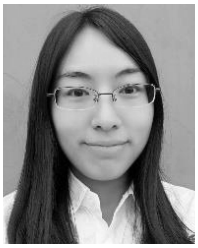
[27] P. Soni, A. K. Pal, and S. H. Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote healthcare system," *Comput. Methods Programs Biomed.*, vol. 182, Dec. 2019, Art. no. 105054.

[28] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons Fractals*, vol. 37, no. 3, pp. 669–674, Aug. 2008.

[29] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101619.

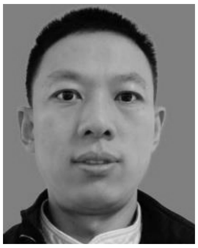
[30] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.
[31] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
[32] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 4, pp. 708–722, Sep. 2016.
[33] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on Smart-Card-Based password-authenticated key agreement in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1767–1775, Jul. 2014.
[34] V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. R. Sekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation," *Future Gener. Comput. Syst.*, vol. 100, pp. 938–951, Nov. 2019.
[35] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[36] D. Wang and P. Wang, "On the implications of Zipf's law in passwords," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2016, pp. 111–131.
[37] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.
[38] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended chebyshev chaotic maps," *IEEE Trans Ind. Informat.*, vol. 14, no. 11, pp. 4815–4828, Nov. 2018.
[39] S. Roy, S. Chatterjee, A. Kumar Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2884–2895, Aug. 2018, doi: 10.1109/JIOT.2017.2714179.
[40] Z. Zhou, P. Wang, and Z. Li, "A quadratic residue-based RFID authentication protocol with enhanced security for TMIS," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 9, pp. 3603–3615, Sep. 2019.

GUOAI XU received the Ph.D. degree in signal and information processing from the Beijing University of Posts and Telecommunications, China, in 2002. He was a Professor, in 2011. He is currently the Associate Director of the National Engineering Laboratory of Security Technology for Mobile Internet, School of Cyberspace Security, Beijing University of Posts and Telecommunications. His research interests include software security and data analysis.



FEIFEI WANG received the M.S. degree in computer science and technology from Henan Polytechnic University, China, in 2016. She is currently pursuing the Ph.D. degree in information security with Beijing University of Posts and Telecommunications, China. Her research interests include authentication technologies and mobile security.

MIAO ZHANG received the Ph.D. degree in signal and information processing from the Beijing University of Posts and Telecommunications, China, in 2007. He is currently an Associate Professor with School of Cyberspace Security, Beijing University of Posts and Telecommunications. His research interests include mobile security and software security.



JUNHAO PENG received the Ph.D. degree from the Beijing University of Posts and Telecommunications, China, in 2008. He is currently a Professor with School of Mathematics and Information Science, Guangzhou University. His research interests include mobile security and cryptography.

• • •