

Article

A Rivest–Shamir–Adleman-Based Robust and Effective Three-Factor User Authentication Protocol for Healthcare Use in Wireless Body Area Networks

Kaijun Liu ^{1,†}, Guosheng Xu ^{1,2,†} , Qiang Cao ^{1,2,*} , Chenyu Wang ^{1,2}, Jingjing Jia ^{1,2}, Yuan Gao ^{1,2} and Guoai Xu ^{1,2,3}

¹ School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China; liukaijun@bupt.edu.cn (K.L.); guoshengxu@bupt.edu.cn (G.X.); wangchenyu@bupt.edu.cn (C.W.); jiajingjing@bupt.edu.cn (J.J.); yuan_gao@bupt.edu.cn (Y.G.); xga@hit.edu.cn (G.X.)

² Key Laboratory of Trustworthy Distributed Computing and Service (MoE), Beijing 100876, China

³ School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen 518055, China

* Correspondence: scq@bupt.edu.cn

† These authors contributed equally to this work.

Abstract: In healthcare, wireless body area networks (WBANs) can be used to constantly collect patient body data and assist in real-time medical services for patients from physicians. In such security- and privacy-critical systems, the user authentication mechanism can be fundamentally expected to prevent illegal access and privacy leakage occurrences issued by hacker intrusion. Currently, a significant quantity of new WBAN-oriented authentication protocols have been designed to verify user identity and ensure that body data are accessed only with a session key. However, those newly published protocols still unavoidably affect session key security and user privacy due to the lack of forward secrecy, mutual authentication, user anonymity, etc. To solve this problem, this paper designs a robust user authentication protocol. By checking the integrity of the message sent by the other party, the communication entity verifies the other party's identity validity. Compared with existing protocols, the presented protocol enhances security and privacy while maintaining the efficiency of computation.

Keywords: authentication; healthcare; Rivest–Shamir–Adleman (RSA); hash function; wireless body area networks (WBANs)



Citation: Liu, K.; Xu, G.; Cao, Q.; Wang, C.; Jia, J.; Gao, Y.; Xu, G. A Rivest–Shamir–Adleman-Based Robust and Effective Three-Factor User Authentication Protocol for Healthcare Use in Wireless Body Area Networks. *Sensors* **2023**, *23*, 8992. <https://doi.org/10.3390/s23218992>

Academic Editor: Naveen Chilamkurti

Received: 18 September 2023

Revised: 23 October 2023

Accepted: 30 October 2023

Published: 5 November 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the development and maturity of wireless communication technologies, wireless networks have been widely used to obtain specific information; this has a profound impact on how we live, work, and play. It is well known that wireless body area networks (WBANs), as a promising application of wireless networks in healthcare, have attracted significant attention with their foreseeable potential to improve the quality of healthcare services. As defined in the IEEE 802.15.6 standard [1], WBANs are composed of wearable, implantable, and invasive intelligent electronic devices around the human body; currently, most wireless medical devices operate under the 2.4 GHz band [2].

As shown in Figure 1, electroencephalogram (EEG) sensors can monitor different types of brain waves. Electromyography (EMG) sensors can test muscle activity. Electrocardiogram (ECG) sensors can detect the electrical transmissions of the heart. Pulse oximeter (POT) sensors can measure hemoglobin in the blood. These health facilities, i.e., EEG, EMG, ECG, and POT sensors, have been used to assist physicians in empowering the functions of human gait analysis, postoperative rehabilitation monitoring, sleep quality detection, and respiratory disease prevention [3]; then, they enable physicians to provide timely medical services without geographical limitations.

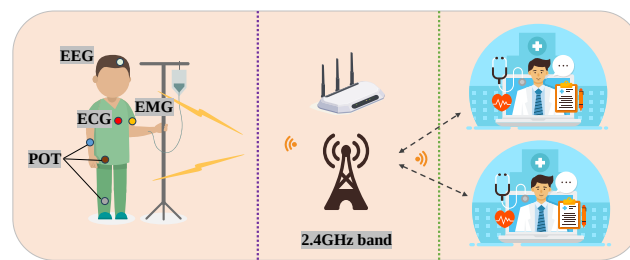


Figure 1. Network model of WBANs.

However, the openness of wireless communication undoubtedly runs the risk of unfettered illegal access, which may, on the one hand, distort professional diagnosis and treatment and, on the other hand, leak patients' personal vital and sensitive physiological data. With so much real-time data traveling from body area sensor nodes to physicians, just as much attention must be paid to security and privacy issues as vaccine research and the elimination of COVID-19 [4].

Luckily, a user authentication mechanism—as a first line of defense for information security that identifies the authenticity of users—is required to protect these key real-time medical data from unauthorized access. As with wireless medical sensor networks (WMSNs) [5], WBANs consist of ad hoc sensor networks, which are continuously carried by patients, connected to their bodies, to sample patient body data. Specifically, the authentication for WBANs involves three indispensable participating entities (shown in Figure 2): a user (U), a gateway node (GWN), and a series of body area sensor nodes (BASNs). The U is often the physician who holds the smart card, the GWN can be a personal digital assistant (PDA), which can be charged, and the BASNs are suitably deployed in patients' bodies and continuously collect medical data [6]. After the mutual authentication among the three entities, a negotiated session key between the user and BASNs will be generated with the help of the GWN.

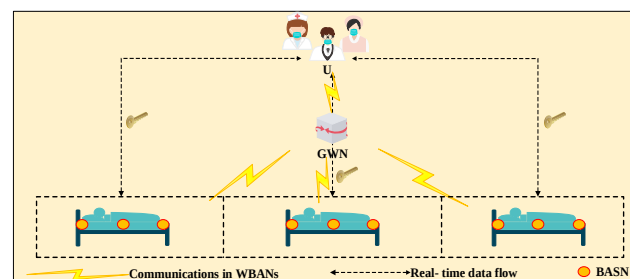


Figure 2. System architecture of WBANs in healthcare.

However, considering the security threats (such as no forward secrecy for the session key, no user anonymity, and inevitable attacks) in existing WBAN-oriented authentication schemes and the financial expenses of energy-constrained sensor nodes, designing a solution that both strengthens efficiency and security and achieves a good balance between efficiency and security is a challenge [7]. For this challenge, we use the Rivest–Shamir–Adleman (RSA) cryptosystem [8] to only protect the secret values; we do not involve RSA in the computation of session keys to preserve efficiency, and add secret values and the “modulus” operation to enhance security. Then, we consider a three-factor authentication scheme, which can be more suitable for WBANs with limited resources.

Motivations and Contributions

WBANs, with the guard of the authentication mechanism, can avoid unauthorized access from malicious attackers. However, existing alternatives show deficiency, either in terms of superior performance or robust security. In addition, a greater number of solutions compromise security in favor of higher efficiency. This compromise prompts the

design of an efficient user authentication scheme with robust security. Accordingly, three indispensable research works listed below are our research contributions:

- (1) The design of a user authentication protocol for WBANs.

Firstly, we show the detailed user authentication system model for WBANs and then give a complete, three-factor (namely smart card, password, and user's personal biometric information) user authentication protocol, which can obtain mutual authentication from the user, the gateway, and the BASNs. Meanwhile, this protocol offers a user-friendly property whereby the user can locally change or update their password without interacting with the gateway, and can enable BASN deletion/addition at will.

- (2) A detailed security analysis for the proposed protocol.

Second, by preserving the user anonymity, a session key is securely established by the user and BASNs. After that, the proposed protocol is demonstrated to be provably secure by the formal security in the random-or-real model. Moreover, a heuristic security analysis has been carried out to show that the proposed protocol can obtain various desirable features and be resistant to all known attacks.

- (3) The complete performance comparisons for the proposed scheme.

Third, performance comparisons—covering storage, communication, and computation costs—between our protocol and other existing relevant protocols have been performed. It is clear that the presently proposed protocol can obtain a better balance between efficiency and security than the alternatives.

To give readers a road map of what to expect in the subsequent sections, the rest of this paper is organized as follows. The related works are introduced in Section 2, and preliminary works are shown in Section 3. The designed protocols are detailed in Section 4. In Section 5, a full security analysis is presented for the proposed protocol, including performance evaluation. A final conclusion is made in Section 6.

2. Related Work

Kumar et al. [9] were the first to propose an authentication protocol for securing communications in medical healthcare. From then on, a large number of related authentication protocols were developed to enhance the protocol security and performance efficiency [10–17].

In one of the proposed research works, Mo et al. [10] highlighted that common attacks (password guessing attack; desynchronization attack) still threaten the security of the designed protocols. Then, they gave some countermeasures to thwart the vulnerabilities, e.g., using the “modulus” operation to resist the password guessing attack, and making the parameters unchanged to resist desynchronization attacks. Similarly, Khan et al. [11] examined and pointed out that their analyzed scheme cannot guarantee the security of passwords and had no forward secrecy of the session key and no user anonymity [11]. Following this, based on the achievement of [11], Khan et al. [12] offered an improved user authentication scheme for healthcare applications, and they showed that their scheme can be more robust than other analyzed schemes.

In 2013, He et al. [13] listed seven functionality requirements of the authentication solution and then presented a robust anonymous authentication protocol for healthcare. Lately, the work in [14] found that He et al.'s scheme had an incorrect authentication and session key agreement phase and that there was no wrong password detection mechanism. Then, they introduced biometric information as the third authentication factor and designed a three-factor authentication solution to remove the drawback of the scheme in [13]. However, Das et al. [15] showed that the scheme presented in [14] could not resist the privileged-insider attack or the sensor node capture attack; then, they developed a more secure biometric-based user authentication scheme. This was more secure than the schemes proposed in [13,14], in which the additional BAN logic AVISPA tool had been used to prove the security of their proposed scheme.

Focusing on securing the communication in wireless healthcare sensor networks, the authors of [16] presented a three-factor user authentication and key agreement protocol.

Their work considered a more user-friendly property for re-registration to accommodate cases in which a user may have lost their smart card or their smart card was stolen. Aiming to resolve security issues in telecare medicine information systems, Ostad et al. [17] developed an enhanced, anonymous, and unlinkable user authentication and key agreement protocol; here, the protocol can provide perfect forward secrecy, patient anonymity, and unlinkability. However, the security of the password could not be preserved, because, in their protocol, the patient directly submitted the bare information OPW_p to the server; this can enable the server to easily guess their password.

Afterwards, for securing the authentication in WBANs, Zhang et al. [18] proposed a privacy-preserving authentication protocol between the user and the telecare medical server, and the session key can be used for forward secrecy by using the chaotic map; however, their scheme inevitably suffered from user identity leakage and password guessing attacks (i.e., the insider attacker guesses PW_i^* and then checks whether $PW_i^* = W_i \oplus ID_i \oplus Z_i \oplus h(ID_i \oplus PW_i^* \oplus V_i \oplus h(ID_i \oplus PW_i^*))$).

Very interestingly, for authentication with access control in medical settings, Soumya Banerjee et al. [19] designed a user authentication and session key exchange protocol, in which any physician with their medical department and professional title will only obtain mutual authentication from the designated sensing devices, while anyone who has been revoked or whose authentication credential is overdue cannot obtain authentication anymore. However, we find that their scheme will be under threat due to an absence of forward secrecy, leaving it vulnerable to the password guessing attack and the node capture attack [20].

In a cloud-of-things-centered wearable device monitoring system, based on the Chinese Remainder Theorem [21] (CRT), the research work in [22] presented a secure user authentication with access control scheme whose functionality is similar to the work in [19], in which an observation highlights that, for the forward secrecy, they adopted a principle wherein the long-term key does not need to be involved in constituting the session key. However, significantly more storage resources are consumed in their scheme, which should be optimized.

Using the well-known RSA-based cryptosystem, Dharminder et al. [23] propounded an RSA-based authentication protocol for two communication entities: the user and the telecare server, whereas security flaws—including vulnerabilities to the password-guessing attack, the absence of forward secrecy, and the absence of user anonymity—should be mitigated.

To solve the session key's forward secrecy, Mahdi Fotouhi et al. [24] offered a robust WBAN-oriented authentication scheme. Their scheme can obtain perfect forward secrecy (PFS) by adopting the secret and updated dynamic authentication credential (DAC) parameters [25], whereas considering the adversary as an administrator of the gateway means that their scheme is defeated in internal anonymity [26]; meanwhile, a very large amount of storage resources are consumed to store indispensable information, including the user data and hundreds or thousands of medical devices.

In contrast to the general centralized system architecture, to mitigate the single point of failure and the trust problem, a blockchain-based authentication scheme [27] was proposed. In their scheme, through the certificate-free-authentication key agreement, each PDA from the WBANs acquires authentication through blockchain nodes, and then these security-critical medical data will be stored in the blockchain. Through blind signature technology, each node can verify the authenticity of an entity that wants to query the medical data.

In 2021, Masud et al. [28] used the physical unclonable function (PUF) [29] and designed a robust user authentication and key establishment scheme, where their scheme can attain perfect anonymity through a very large challenge–response pair. However, to preserve forward secrecy, all entities in the scheme must run the operation of verification at least twice during the authentication phase.

To obtain a superior authentication performance, a lightweight WBAN-oriented scheme [30] was proposed; in this process, a session key is established in the sensor node and the Hub node. However, a deficiency was shown in that there was no mutual authentication among the three

entities (access point, hub node, and sensor node); this creates obstacles when encountering real-world applications. Then, Xie et al. of [31] analyzed that the protocol [30] cannot resist a stolen-verifier attack and has no perfect forward secrecy. Then, a robust patient monitoring authentication scheme based on elliptic curve cryptography (ECC) [32] was proposed, and the formal security proof demonstrates the security of their scheme. However, it still lacks mutual authentication between the relay node and sensor node.

To obtain mutual authentication among all entities, Narwal et al. in [33] demonstrated mutual authentication among three entities (sensor node, mid node, and chief node) in their paper. However, their scheme still weakens the session key's forward secrecy and resistance against the node capture attack. Focusing on the WBAN scenario, the authors of [34] offered a mutual authentication protocol for securing the communication between body sensor units (BSUs) and administrator (Adm); here, the session key can be used for forward secrecy. However, the anonymity of identity should be improved if one considers the GWN as an insider attacker.

In summary, existing alternatives show deficiencies, either in terms of superior performance or robust security. Furthermore, a greater number of solutions compromise security in favor of higher efficiency. It is necessary to design an authentication protocol with higher efficiency and while preserving robust security.

3. Preliminaries

3.1. System Model

The system model shown in Figure 3 consists of three entities: the physicians, the gateway node (GWN), and a series of body area sensor nodes (BASNs). Furthermore, the GWN computes and then transmits messages between physicians and BASNs; BASNs are constantly carried on a patient's body and collect real-time data from the body. Furthermore, the physicians comprise entities who directly access the data from the BASNs to monitor patients and then provide timely medical service.

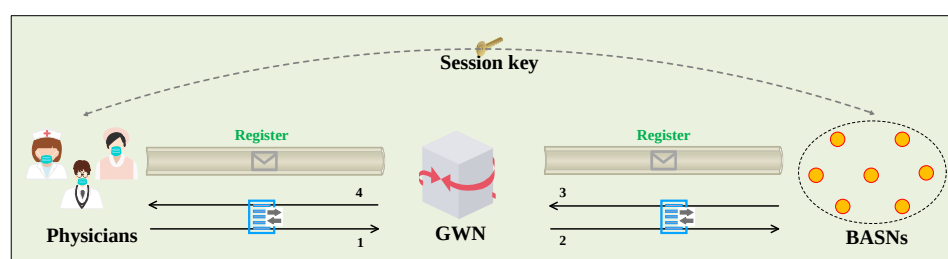


Figure 3. System model in the proposed scheme.

Note that, in Figure 3, information packets in the secure channel are transmitted during the registration phase, and information packets in the public channel from **number 1 to number 4** are transmitted during the authentication and key agreement phase. We then introduced the implementation of authentication and key agreement among the three entities. In the beginning, the GWN initiates the authentication system and then generates a long-term key, a secret key value, and other public parameters. Then, when a physician (denoted by U_i) registers in the GWN through the secure channel, they send the registration request to the GWN, and then the GWN sends a smart card securely to the U_i (information packets shown on the left). For the registration of the BASNs, which also occurs through the secure channel, these nodes only need to submit their identities to the GWN, and then they can receive the identity-related secret values from the GWN's calculations (information packets shown on the right).

In the following authentication, firstly, the U_i submits a login request to the GWN (**number 1**); the GWN then verifies the identity of the U_i based on the login request and sends the verification message to the BASNs (**number 2**). After receiving the verification message, the BASNs first verify the GWN and calculate a message which consists of a

session key and relevant authentication parameters, and then send this message to the GWN (**number 3**). After obtaining the message from the BASNs, the GWN verifies the BASNs and sends the message with the newly embedded session key to the U_i . Finally, the U_i authenticates the GWN, and obtains key parameters from the received message; then, it recomputes the session key (**number 4**).

3.2. RSA Cryptosystem

As a public key cryptography, the Rivest–Shamir–Adleman (RSA) encryption and decryption algorithm [8], based on the hardness problem of a large-number factorization problem, is described below with an example of a message sender S sending a message m to a message receiver R .

- **Initiation:** Message receiver R selects two large prime numbers p, q , computes $n = p \times q$ and Euler's totient function of n , i.e., $\varphi(n) = (p - 1) \times (q - 1)$. Then, R chooses an integer e meeting $\gcd(e, \varphi(n)) = 1$, and computes $d \equiv e^{-1} \pmod{\varphi(n)}$. As a result, R is public (e, n) and keeps the private key d secret.
- **Encryption:** Message sender S takes a message m and computes an encryption $c = m^e \pmod{n}$ with R 's public key e . Then, S sends the cipher c to R .
- **Decryption:** Upon receiving the cipher c , R decrypts $m = c^d \pmod{n}$ with their own private key d .

3.3. Threat Model

The Dolev–Yao model [35]—which depicts the adversary's capacity—has been widely applied to analyze the security of the authentication protocol. Now, the newest research work [20] further summed up the capabilities of adversaries aiming to fully assess the proposed schemes. Then, in this more sophisticated threat model, an attacker $\mathcal{A}$ can be described to have seven capacities (A-), as outlined below:

- **(A-1)** $\mathcal{A}$ can fully control the open channel and then intercept, modify, insert, and delete any messages transmitted in the open channel.
- **(A-2)** $\mathcal{A}$ can enumerate all items offline in the Cartesian product of the identity space and the password space $D_{id} \times D_{pw}$ within the polynomial time.
- **(A-3)** To a three-factor user authentication scheme, $\mathcal{A}$ can compromise the following two of three authentication factors: (a) user's password; (b) data in the smart card; and (c) user's biometric information.
- **(A-4)** $\mathcal{A}$ can obtain previous session keys established between the physician (user) and body area sensor node (BASN).
- **(A-5)** $\mathcal{A}$ can grasp GWN's secret key when we consider the system's eventual failure.
- **(A-6)** $\mathcal{A}$ can break some BASNs, i.e., extracting the sensitive data stored therein, and control the broken BASN to join the next newly communication of GWN, other users, and body area sensor nodes.
- **(A-7)** $\mathcal{A}$ may register as a legitimate user or as the administrator of the GWN, only when the security of the user's password is assessed.

4. The Proposed Protocol

In this part, the following indispensable phases covering the user/body area sensor node registration, user/body area sensor node mutual authentication, password change, and body area sensor node deletion and addition constitute a robust RSA-based three-factor user authentication and key agreement protocol. Furthermore, we reinforce the session key's security and user anonymity from the points below:

1. To achieve forward secrecy, the session key will be computed from the secret values of user and BASNs, rather than the general GWN's long-term key x . Although the adversary grasps x , they cannot corrupt the session key. Furthermore, the RSA-based encryption and decryption algorithm will only be used to protect secret values

of user and BASNs, but not involving the computation of session key to preserve the efficiency.

- To preserve user anonymity, in the registration phase, the user only submits the hashed value A_0 to GWN, and no real identity information has been exposed to adversary (i.e., identity protection); on the other hand, in the verification phase, the dynamic pseudo identity PID_i will be allocated to the user. The randomness of PID_i confuses the adversary to decide whether two sessions are from the same user (i.e., untraceability).

To facilitate an understanding of the proposed protocol for readers, the notations used in this paper are explained in Table 1.

Table 1. Notations of symbols in our scheme.

Symbols	Descriptions	Symbols	Descriptions	Symbols	Descriptions
U_i	i th physician	GID	GWN's identity	MS_j	j th BASN
PW_i	Password of U_i	x	GWN's long-term key	MIS_j	MS_j 's identity
$\Rightarrow$	The secure channel	$\rightarrow$	The public channel	$\oplus$	The XOR operation
ID_i	Unique identity of U_i	$BKG(\cdot)$	Biometric key generation	x_j	Secret value of MS_j
PID_i	Pseudo-identity of U_i	bio_i	Biometric information of U_i	$X Y$	The concatenate operation

Next, we provide a detailed description of the proposed protocol.

4.1. System Setup Phase Run by GWN

Given a security parameter n , the GWN chooses a long-term key $x \in \{0, 1\}^n$ and keeps x secret.

4.2. Registration Phase of User and BASN

The registration phase enables the user and the body area sensor nodes (BASNs) to finish the registration of related identity information in the terminal of the GWN; meanwhile, the user and the BASNs receive feedback from the GWN to be ready for future identity authentication. Specifically, two parts are involved—one for the body area BASN and another one for the user/physician (U_i).

For the registration of each body area a sensor node called MS_j , MS_j sends its identity MIS_j to the GWN by the secure channel. Upon receiving the registration request from MS_j , the GWN computes $x_j = h(MIS_j||x)$ and then feeds back x_j to MS_j also by the secure channel. Meanwhile, the GWN publishes a revocation list L_{revoke} which will store the identity of deleted sensor nodes.

For the new user, U_i , to register, they need to follow the three following steps with the help of the GWN.

- Step 1.** $U_i \Rightarrow GWN : A_0$. U_i chooses their own ID_i, PW_i and a random value r , and computes $HPW_i = h(ID_i||PW_i) \bmod n_0$, $A_0 = HPW_i \oplus r$. Then, the U_i sends the value A_0 to the GWN through the secure channel.
- Step 2.** $GWN \Rightarrow U_i : \{PID_i, BKG(\cdot), A_1, Cou\}$. Through the received A_0 , GWN firstly generates a pseudo-identifier, PID_i , computes $V_i = h(PID_i||x)$, $A_1 = V_i \oplus A_0$, and then injects the values $PID_i, BKG(\cdot), A_1, Cou$ to the smart card, in which the "Cou" means the maximal times (such as 3). This allows the user to try to login using the smart card if they forget the right password. Lastly, GWN also feeds back the smart card to U_i by the secure channel.
- Step 3.** After obtaining the smart card from the GWN, the U_i inputs their biometric information bio_i into the smart card, and the smart card further computes $V_i = A_0 \oplus A_1$, $V_{ii} = BKG(bio_i)$ and $A_2 = h(ID_i||PW_i||V_i||V_{ii}) \bmod n_0$. In the end, the smart card updates $A_1 = V_i \oplus HPW_i$ and stores $\langle PID_i, BKG(\cdot), A_1, A_2, Cou \rangle$.

4.3. User Login Phase

In the login phase, the U_i needs to be verified by the smart card. Once the smart card verifies the U_i 's legitimacy, the U_i successfully logs in using the smart card, and the smart card generates an authentication request for the U_i . Finally, the smart card transmits this request packet to the GWN. Specifically, the U_i enters (ID_i^*, PW_i^*) and their own biometric information bio_i^* , then the smart card computes $HPW_i^* = h(ID_i^* || PW_i^*) \bmod n_0$, $V_i^* = HPW_i^* \oplus A_1$, $V_{ii}^* = BKG(bio_i^*)$, and a verifier $A_2^* = h(ID_i^* || PW_i^* || V_i^* || V_{ii}^*) \bmod n_0$, and checks whether $A_2^* = A_2$; here, A_2 has been stored in the smart card during the registration phase (step 3). If $A_2^* \neq A_2$, then the smart card terminates this session and sets $Cou = Cou + 1$ at the same time. If Cou exceeds a certain value, such as 3, then this smart card is directly suspended until the physician U_i re-registers by the gateway. Otherwise, the smart card shares the registration information V_i ; meanwhile, the terminal of the user (e.g., personal computer, laptop) initializes a pair of RSA parameters (e_i, d_i) , where " e_i " is the public key and " d_i " is the private key, and selects a random value $r_u \in Z_p^*$ —some body area sensor node MS_j —with the identifier, MIS_j , which the U_i needs to acquire, and extracts the time stamp T_1 . Then, it computes the following values: $B_1 = h(V_i || e_i \oplus h(r_u || T_1))$, $B_2 = MIS_j \oplus h(PID_i || h(r_u || T_1))$. Next, the verifier obtains $B_3 = h(PID_i || MIS_j || h(r_u || T_1) || e_i)$. In the end, the U_i sends the request packet $\{PID_i, B_1, B_2, B_3, T_1\}$ to the GWN in the open channel. It is worth noting that, in computing B_1 , to keep the ' $\oplus$ ' operation running properly, the size of $h(V_i) || e_i$ is equal to the size of $h(r_u || T_1)$; through this, 0 is added in the upper part of $h(r_u || T_1)$.

4.4. Verification Phase of the User, the GWN, and the BASNs

In the verification phase, all three entities—the U_i , the GWN, and the MS_j —will verify each other's identities, and then the U_i and the MS_j negotiate a session key, SK , to protect secret information in future communications.

- Step 1.** $GWN \rightarrow MS_j : \{B_4, B_5, B_6, T_2\}$. Given the login response from the U_i , the GWN first checks whether $|T_c - T_1| < \Delta T$; here, T_c and ΔT are the current timestamp and the time gap, respectively. If so, then the GWN computes $V_i^* = h(PID_i || x, h(r_u^* || T_1) || e_i^* = B_1 \oplus h(V_i^*), MIS_j^* = B_2 \oplus h(PID_i || h(r_u^* || T_1))$. The GWN checks whether $MIS_j^* \in L_{revoke}$. If so, then the authentication request for MIS_j^* (i.e., MIS_j) is not valid, and the GWN neglects this login request. Otherwise, the GWN further computes $B_3^* = h(PID_i || MIS_j^* || h(r_u^* || T_1) || e_i^*)$. Furthermore, the GWN checks whether $B_3^* = B_3$; if not, then this session concludes. Otherwise, the GWN selects a nonce or a random value $r_g \in Z_p^*$, extracts the timestamp T_2 , and then obtains: $x_j = h(MIS_j || x)$, $B_4 = h(x_j || MIS_j) \oplus e_i || r_g || h(r_u || T_1)$ and $B_5 = MIS_j || h(V_i) \oplus h(x_j || r_g)$, $B_6 = h(h(r_u || T_1) || r_g || x_j || MIS_j || T_2)$. Then, the GWN sends the information packet $\{B_4, B_5, B_6, T_2\}$ to MS_j in the open channel.
- Step 2.** $MS_j \rightarrow GWN : \{B_7, B_8, B_9, B_{10}, T_3\}$. Through the request from the GWN, the body area sensor node MS_j first checks whether $|T_c - T_2| < \Delta T$; if not, then this session is concluded. Otherwise, MS_j obtains: $e_i^* || r_g^* || h(r_u^* || T_1) = B_4 \oplus h(x_j || MIS_j)$, $MIS_j^* || h(V_i^*) = B_5 \oplus h(x_j || r_g^*)$. Then, it further computes $B_6^* = h(h(r_u^* || T_1) || r_g^* || x_j || MIS_j^* || T_2)$. Next, MS_j checks whether $B_6^* = B_6$; if not, then this session is concluded. Otherwise, MS_j chooses a nonce $r_s \in Z_p^*$, extracts timestamp T_3 , and computes $r_s' = (r_s)^{e_i}$ and $SK = h(h(r_u || T_1) || r_s || h(V_i))$, $B_7 = MIS_j \oplus h(r_g)$, $B_8 = r_s' || h(SK || r_g) \oplus x_j$, $B_9 = h(r_s' || h(SK || r_g) || x_j || T_3)$. Next, the verifier obtains $B_{10} = h(SK || r_g) \oplus x_j \oplus h(r_s' || SK)$. Finally, MS_j sends the information packet $\{B_7, B_8, B_9, B_{10}, T_3\}$ to the GWN in the open channel.
- Step 3.** $GWN \rightarrow U_i : \{B_{11}, B_{12}, B_{13}\}$. Upon obtaining $B_7, B_8, B_9, B_{10}, T_3$, the GWN first checks whether $|T_c - T_3| < \Delta T$; if not, then this session is concluded. Otherwise, the GWN computes $MIS_j^* = B_7 \oplus h(r_g)$ and checks whether $MIS_j^* \in L_{revoke}$. If so, then this denotes that the authentication session from MIS_j^* (i.e., MIS_j) is not valid, and the GWN neglects this request. Otherwise, the GWN further computes

$x_j^* = h(MIS_j^* || x), r_s'^* || h(SK^* || r_g^*) = B_8 \oplus x_j^*$ and $B_9^* = h(r_s'^* || h(SK^* || r_g^*) || x_j^*) || T_3$, and checks whether $B_9^* = B_9$; if so, then the GWN further computes $h(r_s' || SK) = B_{10} \oplus h(SK || r_g) \oplus x_j$ and then selects a new pseudo-identifier PID_i^{new} , computes $V_1^{new} = h(PID_i^{new} || x), B_{11} = V_i^{new} \oplus V_i$, and $B_{12} = PID_i^{new} || r_s' \oplus h(V_i^{new} || h(r_u || T_1)), B_{13} = h(V_i^{new} || h(r_s' || SK))$. Next, the GWN transmits $\{B_{11}, B_{12}, B_{13}\}$ to the physician, U_i .

- **Step 4.** When receiving feedback from the GWN, the U_i computes $V_i^{new*} = B_{11} \oplus V_i, PID_i^{new*} || r_s'^* = B_{12} \oplus h(V_i^{new*} || h(r_u || T_1)), r_s^* = (r_s'^*)^{d_i}$ with a private key, d_i ; then, $SK^* = h(h(r_u || T_1) || r_s^* || h(V_i)), B_{13}^* = h(B_{13}^{new*} || h(r_s'^* || SK^*))$. After that, the U_i checks whether $B_{13}^* = B_{13}$; if so, then the U_i accepts SK^* as SK. Furthermore, they update $A_1^{new} = V_i^{new} \oplus HPW_i, A_2^{new} = h(ID_i || PW_i || V_i^{new} || V_{ii}) \bmod n_0$. Finally, the U_i replaces the smart card's old parameters $\{PID_i, A_1, A_2\}$ with newly $\{PID_i^{new}, A_1^{new}, A_2^{new}\}$.

4.5. User Password Change Phase

The password change phase enables the user to update their password at will. Specifically, it consists of two parts: user identity verification, finished by the smart card; update parameters covering PW_i, A_1, A_2 , finished by the user. That is, the U_i only submits their old or frequently used password to the smart card, as shown in the login phase. After the smart card verifies the U_i 's legitimacy—through checking whether $A_2^* = A_2$ —the smart card allows the U_i to choose a new PW_i^{new} , and updates the $HPW_i^{new} = h(ID_i || PW_i^{new}) \bmod n_0, A_1^{new} = HPW_i^{new} \oplus V_i, A_2^{new} = h(ID_i || PW_i^{new} || V_i || V_{ii}) \bmod n_0$. Lastly, the smart card replaces A_1, A_2 with A_1^{new}, A_2^{new} .

4.6. Body Area Sensor Node Deletion Phase

Given that some nodes may be compromised or run out of their limited energy, let us take MS_j ; at this time, the GWN directly revokes this sensor node and puts MS_j 's identity MIS_j into a revocation list L_{revoke} . Lastly, the GWN broadcasts L_{revoke} to all communication entities within the WBANs.

4.7. Body Area Sensor Node Addition Phase

In this part, the proposed protocol offers a dynamic node addition phase to meet the real-time data collection persistently from the patient. When a new MS_t needs to be added into the existing architecture, the GWN only assigns an identifier MIS_t and computes $x_t = h(MIS_t || x)$ to MS_t . Then, the new body area sensor node MS_t stores the corresponding x_t in its secure memory.

5. Analyses of the Proposed Protocol

Here, we provide analyses of the proposal, including a security analysis and a performance analysis. The security analysis involves a provable proof security and a heuristic analysis, which shows that our scheme can be robust. Then, the performance analysis includes comparisons of our designed scheme with other new WBAN-oriented schemes, to indicate that the proposed protocol can be applied in real-world uses.

5.1. Formal Security Analysis of The Proposed Protocol

As an effective method to prove the semantic security of the protocol, the formal security analysis covers two aspects. That is, given the adversary model shown in Section 3, we need to (1) firstly provide some introductions for formal proof and then state the security objectives of the protocol in Section 5.2; (2) second, in Section 5.3, we provide Theorem 1 to determine the advantages of adversary breaking for the session key in the protocol.

5.2. Introductions for Formal Proof

In the proposed protocol **P**, three participants (a physician— U_i ; a gateway node—GWN; body area sensor node— MS_j) are involved. Initially, the simulator uses the RSA encryption and decryption algorithm over two large primes p, q , where $|p| = |q|$. Next, the U_i obtains their own information $\{ID_i, PW_i, Bio_i\}$ and smart card

containing $\{PID_i, BKG(\cdot), A_1, A_2, Cou\}$; the GWN generates a long-term key x ; the MS_j keeps the identity secret key pair MIS_j, x_j .

During the proof, the three entities will instantiate U_i , GWN, and MS_j with $\Pi_{u_i}^u, \Pi_{GWN}^g, \Pi_{MS_j}^m$, respectively. Furthermore, these instances can be uniformly marked as Π^t if there is no need to tell the three instances apart. Furthermore, if the input message is valid/incorrect or null, then the state of the instance as an oracle will reach accept/reject, or return " $\perp$ ", which means that there is no response for the input.

Here, we provide some terms used in this proof.

- *Accepted state*: When an instance Π^t receives the last expected protocol message, an instance Π^t obtains an accepted state. In this session, all ordered concatenation communicated messages decide on the session identifier.
- *Partnering*: Here, mutually authenticated Π^{t_1}, Π^{t_2} are partnering, if Π^{t_1}, Π^{t_2} simultaneously satisfy the following criteria: (1) both have an accepted state; (2) both share the same identification; (3) both Π^{t_1}, Π^{t_2} are the mutual partners of each other.
- *Adversary*: Based on the information received by initiating the query oracles and controlling the simulator, an adversary $\mathcal{A}$ attempts to compromise the security of the authentication messages and rebuild the session key in protocol $\mathbf{P}$. Some queries $\mathcal{A}$ that can launch are the following:
 - *Execute*($\Pi_{u_i}^u, \Pi_{GWN}^g, \Pi_{MS_j}^m$). This query can be run to simulate the entire authentication process, and $\mathcal{A}$ will obtain communicated messages among U_i , GWN and MS_j .
 - *Send*(Π^t, l). $\mathcal{A}$ can launch an active attack against a participating instance Π^t with a message l . Furthermore, if Π^t received the valid l , then the simulator gives a response to $\mathcal{A}$. Otherwise, the simulator ends the query.
 - *Reveal*(Π^t). This query means that $\mathcal{A}$ can grasp the session key calculated by Π^t (and its partner).
 - *Corrupt*($\Pi_{u_i}^u, \alpha$). In this query, $\mathcal{A}$ can obtain the corresponding authentication factors stored by the user, U_i , according to the value α . That is, the oracle exposes the password ($\alpha = -1$), the data stored in the smart card ($\alpha = 0$), and the biometric information Bio_i ($\alpha = 1$), respectively, to $\mathcal{A}$.
 - *Corrupt*(Π_{GWN}^g). For this query, the long-term key x could be known by $\mathcal{A}$.
 - *Corrupt*($\Pi_{MS_j}^m$). $\mathcal{A}$ in this query can obtain the secret value of MS_j .
- *Freshness*: If the session key between the U_i and the MS_j has not been revealed to $\mathcal{A}$ using *Reveal*, then the instance $\Pi_{u_i}^u$ or Π_{GWN}^g or $\Pi_{MS_j}^m$ can be fresh.
- *Test*(Π^t): In this test query, $\mathcal{A}$ is capable of querying only once. By the protocol $\mathbf{P}$, the instance Π^t can, accordingly, only be $\Pi_{u_i}^u$ or $\Pi_{MS_j}^m$. Formally, if instance Π^t has not computed a session key or Π^t cannot be fresh, or *Test*(Π^t) has been queried before, then the *test* query outputs " $\perp$ " (null). Otherwise, the oracle will flip the unbiased coin b . If $b = 1$, the adversary $\mathcal{A}$ receives the real session key. If $b = 0$, then $\mathcal{A}$ obtains a random string that has the same length as the real session key.
- *Semantic Security*: Given a protocol $\mathbf{P}$, a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ has requested new instances for a series of queries including the execute query, the send query, the corrupt query, and the test query. Now, $\mathcal{A}$ desires to break the protocol $\mathbf{P}$ by guessing the value of b in the test query and outputting a guessing value b^* . Let $Succ(\mathcal{A})$ denote the event that $\mathcal{A}$ guesses b^* correctly b , i.e., $b^* = b$. The advantage of $\mathcal{A}$ breaking the semantic security of protocol $\mathbf{P}$ over the session key can be defined as follows:

$$Adv_{\mathcal{A}}^{\mathbf{P}} = 2\Pr[Succ(\mathcal{A})] - 1.$$

5.3. Semantic Security Proof of The Protocol

In this part, we show the proposed protocol's semantic security evaluation in the view of a theorem.

Theorem 1. Let $\mathbf{P}$ be the proposed protocol, $|D|$ be the space of a password, and n be the system security parameter. After making a series of queries—including execute-query q_e times, send query q_s times, hash query q_h times, and bio-hashing query $q_{BKG(\cdot)}$ times—the advantage $Adv_{\mathcal{A}}^{P,D}$ of $\mathcal{A}$ breaking the semantic security of SK in $\mathbf{P}$ is less than

$$\frac{q_h^2 + 6q_s}{2^{l_1}} + \frac{(q_s + q_e)^2}{p} + \frac{q_{BKG(\cdot)}^2 + 2q_{BKG(\cdot)}}{2^{l_2}} + 2(C'q_{send}^{s'} + Adv_{\mathcal{A}}^{RSA}(n))$$

Proof. By the games chain, involving Game₁–Game₈, we now prove that the adversary's advantage in breaking the semantic security of session key is factually negligible. Furthermore, set $Succ_i$ to the event in which $\mathcal{A}$ successfully guesses the b in the test query of Game_k, where $k = 1, 2, \dots, 8$.

Game₁: this game simulates a real attack by the random oracle. A bit b is then randomly chosen at the beginning of this game. Thus,

$$Adv_{\mathcal{A}}^{P,D} = 2\Pr[Succ_1] - 1 \quad (1)$$

Game₂: this game shapes a hash list Ω_h and a $BKG(\cdot)$ list $\Omega_{BKG(\cdot)}$. Say that $\mathcal{A}$ initiates a hash query $h(\gamma)$, then the hash oracle Θ_h takes γ to retrieve Ω_h . If a hash value $h(\gamma)$ is retrieved in Ω_h , then Θ_h responds the hash value. Otherwise, a random string ψ will be sent to $\mathcal{A}$; meanwhile, (γ, ψ) is stored in Ω_h .

For $BKG(\cdot)$'s oracle $\Theta_{BKG(\cdot)}$, its simulation is simulated in the same way as the hash oracle Θ_h . By the known list in this game, $\mathcal{A}$ performs the *Test*-query to tell the real session key and the random value apart. For $SK = h(h(r_u || T_1) || r_s || h(V_i))$, secret values only include U_i 's r_u , V_i , and MS_j 's r_s . Hence, $\mathcal{A}$ has no way to compute SK and to distinguish whether $b = 0$ or $b = 1$ other than to guess.

Thus, compared to Game₁, $\mathcal{A}$'s chance of winning Game₂ does not increase the $\mathcal{A}$'s advantage despite its eavesdropping attack, i.e.,

$$\Pr[Succ_2] = \Pr[Succ_1] \quad (2)$$

Game₃: In this game, $\mathcal{A}$ can execute an active *send* query or *hash* query to try to persuade a communication entity to accept a forged message. Compared with Game₁ and Game₂, $\mathcal{A}$'s advantage may be enhanced by finding the collision to generate a valid message. That is, if the following collisions occur, then this game aborts.

- (i) A collision can be found in the hash values or $BKG(\cdot)$'s outputs, and the probability is $\frac{q_h^2}{2^{l_1+1}}$ or $\frac{q_{BKG(\cdot)}^2}{2^{l_2+1}}$, where l_1 and l_2 denote the length of the output by the hash function and $BKG(\cdot)$, respectively.
- (ii) Another collision which can be found is on the choice of random numbers r_u, r_g, r_s ; the probability is $\frac{(q_s + q_e)^2}{2p}$.

Thus, we have:

$$|\Pr[Succ_3] - \Pr[Succ_2]| \leq \frac{q_h^2}{2^{l_1+1}} + \frac{q_{BKG(\cdot)}^2}{2^{l_2+1}} + \frac{(q_s + q_e)^2}{2p} \quad (3)$$

Game₄: In this game, $\mathcal{A}$ wants to guess B_3, B_6, B_9, B_{13} without asking the hash query. Obviously, we obtain:

$$|\Pr[Succ_4] - \Pr[Succ_3]| \leq \frac{q_s}{2^{l_1}} \quad (4)$$

Game₅: In this game, $\mathcal{A}$ tries to guess A_2 without asking the hash query. Similarly, we can obtain:

$$|\Pr[Succ_5] - \Pr[Succ_4]| \leq \frac{q_s}{2^{l_1}} \quad (5)$$

Game₆: In this game, by the corrupt $(\Pi_{u_i}^u, \alpha)$ query, $\mathcal{A}$ computes A_1 . There are three cases we need to consider.

- Case 1, i.e., corrupt $(\Pi_{u_i}^u, \alpha = -1, 0)$: the probability that $\mathcal{A}$ guesses the user's biometric information is less than $\frac{q_{BKG}(\cdot)}{2^{l_2}}$.
- Case 2, i.e., corrupt $(\Pi_{u_i}^u, \alpha = 1, 0)$: in the technology of "fuzzy keywords + honeywords", the probability that $\mathcal{A}$ guesses the physician's password is no more than $C'q_{send}^{s'}$ [36,37]. Here, C' and s' are constants, depending on the password dataset, and can be gained through linear regression. Take the Gmail password dataset [38] as an example, $C' = 0.020963$, $s' = 0.225653$.
- Case 3, i.e., corrupt $(\Pi_{u_i}^u, \alpha = -1, 1)$: the probability that $\mathcal{A}$ guesses values of A_1 is less than $\frac{q_s}{2^{l_1}}$.

Therefore, we obtain:

$$|\Pr[Succ_6] - \Pr[Succ_5]| \leq C'q_{send}^{s'} + \frac{q_s}{2^{l_1}} + \frac{q_{BKG}(\cdot)}{2^{l_2}} \quad (6)$$

Game₇: This game describes the attack that $\mathcal{A}$ aims to compromise the body area sensor node MS_j by performing the corrupt $(\Pi_{MS_j}^m)$ oracle, and then $\mathcal{A}$ obtains the secret value x_j and further r'_s . However, $\mathcal{A}$ cannot retrieve r_s from r'_s , since there is no PPT solution to break the hardness of large number factorization problem [8]. Therefore, we can yield:

$$|\Pr[Succ_7] - \Pr[Succ_6]| \leq Adv_{\mathcal{A}}^{RSA}(n) \quad (7)$$

Game₈: In this attack, $\mathcal{A}$ tries to calculate SK . At this time, $\mathcal{A}$ cannot query the oracle *execute* query, *send* query and *Corrupt* query any more. Similarly to the analysis of Game₇, $\mathcal{A}$ cannot compute r_s from r'_s . In other words, $\mathcal{A}$'s advantage in Game₈ is equal to the advantage in Game₇. Thus, we can have:

$$\Pr[Succ_8] = \Pr[Succ_7] \quad (8)$$

Until now, we can obtain that $\mathcal{A}$ has no non-negligible advantage other than $\frac{1}{2}$, and so $\Pr[Succ_8] = \frac{1}{2}$. From Equations (1)–(8) and triangular inequality, we yield the following deduction with $\Delta = 2(C'q_{send}^{s'} + Adv_{\mathcal{A}}^{RSA}(n))$:

$$\begin{aligned} Adv_{\mathcal{A}}^{P,D} &= 2\Pr[Succ_1] - 1 \\ &= 2\Pr[Succ_8] - 1 + 2(\Pr[Succ_1] - \Pr[Succ_8]) \\ &\leq \frac{q_h^2 + 6q_s}{2^{l_1}} + \frac{(q_s + q_e)^2}{p} + \frac{q_{BKG}(\cdot)^2 + 2q_{BKG}(\cdot)}{2^{l_2}} + \Delta \end{aligned} \quad (9)$$

As a conclusion, one can see that, if the adversary desires to break the semantic security of a session key, then the advantage of this adversary can only be negligible, $Adv_{\mathcal{A}}^{P,D}$, which is less than $\frac{q_h^2 + 6q_s}{2^{l_1}} + \frac{(q_s + q_e)^2}{p} + \frac{q_{BKG}(\cdot)^2 + 2q_{BKG}(\cdot)}{2^{l_2}} + 2(C'q_{send}^{s'} + Adv_{\mathcal{A}}^{RSA}(n))$. $\square$

5.4. Heuristic Security Analysis of The Proposed Protocol

The heuristic method [7] does not involve any complex formula. It is a very effective and simple method, which can conduct a concise security analysis of the protocol. In this part, our designed protocol provides not only desired attributes, but is also resistant against a variety of known attacks.

- **Mutual authentication.** The proposed scheme can obtain mutual authentication, since the U_i and the GWN authenticate each other bidirectionally by checking whether $B_3^* = B_3$ and $B_{13}^* = B_{13}$, respectively. Then, through the MS_j checking whether $B_6^* = B_6$ and the GWN seeing that $B_9^* = B_9$, the GWN and the MS_j can authenticate each other.
- **Session Key Agreement.** The session key agreement means that no one can solely pre-compute the session key without interacting with another entity. Factually, in the proposed scheme, $SK = h(h(r_u||T_1)||r_s||h(V_i))$ contains the indispensable part from the U_i (the secret parameter r_u) and the MS_j (the secret parameter r_s), and so our scheme meets this well-defined attribute.
- **Forward Secrecy.** Forward secrecy holds if the past built session keys are still secure, on the condition that the long-term secret—i.e., the GWN's x —is corrupted. As a matter of fact, suppose that the attacker knows x , and further that they can obtain the PID_i from the open channel and then compute $V_i = h(PID_i||x)$, and then obtain $h(r_u||T_1)$. Even so, it is vitally important to note that they cannot retrieve the r_s because of the hardness of the large number's factorization in RSA [8]. That is, we can obtain forward secrecy.
- **User Anonymity.** User anonymity mainly consists of user identity protection that cannot be figured out by the adversary and the user's un-traceability, which guarantees that the adversary can neither determine who the user is nor distinguish whether two occurrences of data interaction are by the same user. For identity protection, in the registration phase, the U_i only submits A_0 to the GWN, so it does not directly extract the identity information for the adversary, even if the GWN is destroyed. The PID_i cannot be used to deduce the identity of a user during the authentication phase, and so the adversary cannot capture the user's identity ID_i . As for the un-traceability of the user, the randomness of PID_i breaks the statistical property, which effectively confuses the adversary in their attempt to determine whether two data behaviors are from the same entity.
- **Password Guessing Attack.** There are two password guessing attacks that result from the verification value: one is in a smart card (attack I) and the other is the verification value in a public channel (attack II). For attack I, even if the adversary knows the verification values A_1, A_2 in the smart card, they cannot check the correctness of the guessed PW_i^* and ID_i^* , because of the congruence of the "modulus" operation in HPW_i and A_2 . For attack II, the password-related verification value only is attributed to B_1 . Although the adversary obtains B_1 and even owns A_1 , they cannot verify the correctness of the guessed PW_i^* and ID_i^* , because the indeterminacy and congruence of the "modulus" operation confuses the adversary in their attempt to decide which of the guessed values (ID_i^*, PW_i^*) is correct [39].

Additionally, according to the research work of [39], the space of the adversary to guess the identity and the password is $\frac{|D_{id}| \times |D_{pw}|}{n_0}$, where $2^4 \leq n_0 \leq 2^8, |D_{pw}| = |D_{id}| = 10^6$. So, the valid password and identity cannot be effectively guessed by the adversary, since the $\frac{|D_{id}| \times |D_{pw}|}{n_0} \approx 2^{32}$ is larger than the finite value Cou , which denotes the time data of the smart card, leading to login failure for the adversary. Thus, the proposed protocol is safe against password-guessing attacks.

- **Body area sensor node impersonation attack.** The adversary in this attack [7] is mainly the legitimate inside user. The user could obtain the body area sensor node's secret key x_j , leading to a faulty session key for the next new physician. Factually, this adversary cannot extract this secret x_j from B_7, B_8, B_{10} , since they cannot obtain the value r_g of the GWN. So, this attack in the proposed scheme has no favorable space.
- **Desynchronization attack.** Generally, after the session key is established, U_i , GWN, and MS_j have no need to update any parameters, and so the desynchronization attack is impossible. However, the U_i in our scheme needs to change their pseudo-identity PID_i to PID_i^{new} and B_1 to B_1^{new} , and then check whether $h(B_1^{new*}||h(r_s'^*||SK^*)) = B_{13}$. Luckily,

it is verifying the correctness of B_{13} that guarantees the synchronization update of PID_i and B_1 .

- **Replay attack.** The adversary in the replay attack usually sends old messages to obtain the verification of the participants. In the proposed protocol, the U_i , the GWN, and the MS_j choose random numbers r, r_u, r_g , and r_s , respectively, to ensure the freshness and independence of the exchanged messages in each session. As a result, the adversary cannot obtain authentication from another through the replay attack.
- **Verifier-stolen attack.** For an adversary using verifiers to launch an attack, since there is no verifier table associated with the user being stored in the GWN, the verifier-stolen attack cannot occur.
- **Privileged insider attack.** In this attack, the adversary (even a corrupted GWN) can extract the real or bare identity information of a legitimate user in the registration phase. Factually, the U_i just submits an A_0 that encapsulates the ID_i to the GWN, rather than the bare ID_i . Therefore, the identity of the user can be protected in this attack.
- **Node capture attack.** This attack denotes that the adversary has the node's secret value, x_j , and then retrieves A_3 and A_4 . However, this adversary cannot re-calculate the session key, SK, unless they can effectively solve the problem of the large number's factorization.
- **Denial of service (DoS) attack.** In the proposed scheme, even if the adversary may render BASN unavailable by repeatedly replaying the old message B_4, B_5, B_6, T_2 , the BASN firstly verifies whether the time gap meets $|T_c - T_2| > \Delta T$ or not. If so, then the BASN directly terminates this session. Furthermore, even though the adversary updates the timestamp T_2 to make $|T_c - T_2| < \Delta T$, the BASN also ignores this session, because of the following verification failure of value B_6 , where B_6 can only be derived by the original timestamp. Thus, this DoS attack makes no sense. Similarly, the terminal of the GWN can resist the DoS attack.
- **Man-in-the-middle (MITM) attack.** In our protocol, suppose that the adversary [40] listens to and blocks the user's login message $PID_i, B_1, B_2, B_3, T_1$, the response message B_{11}, B_{12}, B_{13} from the GWN, and extracts all the parameters of the smart card. To issue a man-in-the-middle (MITM) attack, the adversary must forge another new message flow $PID_i^*, B_1^*, B_2^*, B_3^*, T_1^*, B_{11}^*, B_{12}^*, B_{13}^*$ or replay the old messages. As discussed above, the proposed scheme can resist an impersonation attack and replay attack. That is, it is not possible for the adversary to be authenticated by both the user and the gateway. Hence, the proposed scheme is resistant against the MITM attack.
- **Session-specific temporary information attack.** This attack happens if the adversary learns the value of session key by obtaining short-term information like random values or nonces, r_u, r_s . However, in our scheme, apart from the nonces, the long-term information like V_i constitutes an SK, and so this attack is infeasible for adversaries.

5.5. Performance Analyses in Functionality and Consumed Cost

In this section, we provide details on the detailed performance analyses covering the functionality comparisons and cost comparisons among the WBAN-oriented user authentication schemes.

For a long time, indispensable valuable design criteria have been used to effectively evaluate the advantages and disadvantages of extant authentication protocols; meanwhile, these provide guidance for designing a good protocol that obtains a balance between performance and security. In accordance with the new criteria [20] and according to our security analyses shown above, Table 2 describes 10 detailed criteria, comprising five ideal (E_*) attributes and five security (C_*) attributes.

Table 2. Ten criteria for evaluating authentication schemes.

Short-Term			Definition in WBANs
Ideal Attributes	E ₁	Password friendly	Users are allowed to choose and locally change their passwords at will.
	E ₂	Sound repairability	The BASN can join the network dynamically and the smart card can be revoked.
	E ₃	Key agreement	The user and BASN should and must negotiate a session key after the authentication.
	E ₄	Mutual authentication	All participants should verify each other's identities.
	E ₅	No password verifier table	Password-related parameters are only stored by the user.
Security Attributes	C ₁	User anonymity	The users' identities can neither be calculated nor tracked by the adversary.
	C ₂	No password exposure	In the registration phase, the privileged participants (usually the administrator of the gateway) cannot obtain the users' password.
	C ₃	Forward secrecy	The agreed session key cannot be acquired by $\mathcal{A}$ even when the long-term key of gateway is compromised.
	C ₄	Resistance to known attacks	The protocol can resist the impersonation attack, offline guessing attack, desynchronization attack, replay attack, stolen verifier-attack, unknown key share and known key attack, DoS attack, and node capture attack. Note that, in these attacks, $\mathcal{A}$ does not compromise the smart card or the BASB anymore.
	C ₅	Resistance to smart card loss attack	$\mathcal{A}$ failed to attack the protocol via a user's smart card.

Furthermore, in Table 3, for the five ideal attributes, it can be observed that all schemes meet E₂, i.e., sound repairability. However, a difference appears in the remaining four attributes. Specifically, scheme [31] does not involve the "password" as an authentication factor and so there is no comparison to be made (denoted by '-'). However, the scheme presented by [28] shows weakness in E₃, with no secret user or sensor node constituting the session key.

Table 3. Functionality comparisons.

Schemes	Ref.	E ₁	E ₂	E ₃	E ₄	E ₅	C ₁	C ₂	C ₃	C ₄	C ₅
Masud et al. (2021)	[28]	✓	✓	✓	✓	✓	✓	×	×	×	×
Nyangaresi et al. (2022)	[34]	-	✓	✓	✓	-	×	-	✓	×	✓
Xie et al. (2023)	[31]	-	✓	✓	×	-	×	-	✓	×	-
Ours	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

For the five security attributes, the sensor node capture attack threatens the session key's security, which indicates that [28,31,34] cannot meet C₄. In the scheme of [28], the user's password security and the session key's forward secrecy cannot be guaranteed, since the adversary can easily initiate an effective password guessing attack and compromise the GWN. This implies that the scheme presented in [28] cannot meet C₂, C₃, or C₅. For the schemes presented in [31,34], the GWN can grasp the identities of communication entities, which makes it easy for the attacker to obtain identity values by corrupting the GWN. Accordingly, the works presented in [31,34] do not meet C₁. Meanwhile, in the scheme presented by [31], no one verifies the identity of the relay node, and so E₄ cannot be achieved.

Our scheme is thus superior to the alternatives. That is, by using the technology of the RSA algorithm, the dynamic assigning of the pseudo identity, and "the modulus" operation, our scheme successfully fulfills the 10 criteria.

Next, we present a comparison among the consumed overheads, covering the storage–communication–computation costs. To obtain a comprehensive evaluation of the overhead comparisons, Table 4 pre-defines the reasonable reference length of all the terms for the compared schemes [28,31,34].

Table 4. The length of all terms.

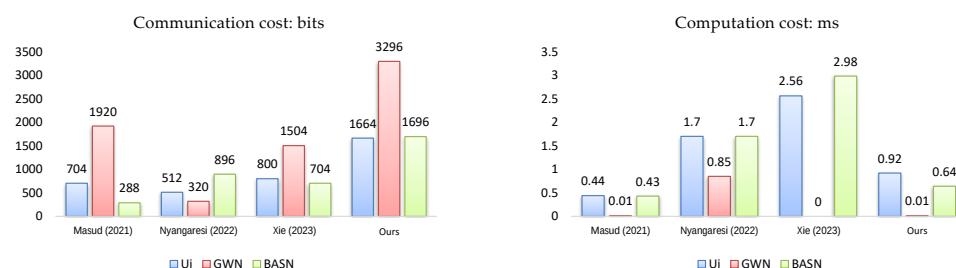
Symbols	Bits	Symbols	Bits
Module (n_0)	32	ECC point (p)	160
Counter (c)	32	Hash value (h)	160
Timestamp (T)	32	Secret value (x)	160
Entities' identity (ID)	128	Random/nonce (r)	160
Challenge–response pair (CRP)	128	Public key of RSA pk	1024
Biometric key generation ($BKG(\cdot)$)	160	Symmetric ciphertext size (enc)	256

In Table 5, for the aspect of storage costs consumed, one can see that the user, the gateway, and the BASN in our protocol need 640 bits, 320 bits, and 160 bits, respectively. However, the storage costs of these three entities in other schemes are unavoidably influenced by the following parameters: N (the number of challenge–response pairs in [28]); m (the number of users), n (the number of BASNs), and m' (the number of relay nodes) in [31]. Please note that, in [31], from the flow of mutual authentication and key agreement phase in Figure 2 of [31], the role of SN_j can be seen as that of the U_i , the role of MS can be seen as that of the $BASN$, and the role of RN can be seen as that of the GWN . Thus, more storage costs (i.e., total $128N(2m + n) + 640(m + n) + 416$ in [28] and $128(m' + n) + 928$ in [31]) will be consumed as the parameters increase. Overall, the proposed protocol is advantageous compared with the compared schemes.

Table 5. Comparison of storage costs.

Schemes	Ref.	Storage Cost: Bits		
		U_i	GWN	BASN
Masud et al. (2021)	[28]	288	$128N(2m + n) + 640(m + n)$	128
Nyangaresi et al. (2022)	[34]	640	480	640
Xie et al. (2023)	[31]	$128(m' + n) + 160$	0	768
Ours	–	640	320	160

As for the communication costs comparison shown in Figure 4, it can be seen that our protocol consumes more communication costs than other compared schemes in order to meet all the attributes shown in Table 3; other schemes save in communication costs, but subsequently weaken the security of the authentication protocol.

**Figure 4.** Comparison of communication and computation costs in all schemes [28,31,34].

As for the computation costs, since the login phase and the verification phase are frequently run through a user authentication protocol, we provided the cryptography computation costs of these two phases. Then, by running the test algorithm on compiler CLion (version 2023.2) in the Windows 11 operating system with 12th Intel core i7-12700H, 16G memory, where the compiler was developed by JetBrains, located in Prague, Czech Republic, we determined that the estimated time of the 1024-bit RSA modular exponentiation is 0.63 ms and the time for the scalar multiplication of the ECC is 0.85 ms. Furthermore, for

other cryptography functions, the time for the BKG is 0.29 ms [41], the time for the hash function (SHA-1) is 0.00069 ms [42], and the time for the PUF is 0.43 ms [43]. As shown in Figure 4, the time consumption values from the user and the BASN in our scheme were 0.92 ms and 0.64 ms, respectively. These show the potential for reducing the user's and the BASN's computation costs by 64% and 79% in comparison with the scheme presented by [31].

In summary, as evidenced by the provable security demonstrated in Section 5.3 and the heuristic analysis demonstrated in Section 5.4, our proposed mechanism can ensure the mutual authentication, forward secrecy of the session key, and user anonymity, while resisting all known attacks. As demonstrated by the performance analyses presented in Section 5.5, we show that the proposed protocol meets the 10 design criteria; other schemes show deficiencies in the provision of the key agreement (E_3), the mutual authentication (E_4), and the security criteria from C_1 to C_5 . Combined with Figure 4 and Table 5, one can see that the costs of storage and computation are superior to the schemes presented by [28,34]. Hence, we can determine that the proposed protocol outperforms the baseline protocols.

6. Conclusions

The authentication mechanism has always been an effective method of guaranteeing the security of data sharing for WBANs. In this paper, based on the RSA encryption and decryption algorithm, we propose a robust three-factor authentication protocol for WBANs. Through detailed security proofs and heuristic analyses, we prove that the proposed protocol can resist various known attacks. Finally, the performance analyses were evaluated to show that the costs of storage and computation are superior to the schemes proposed by [28,34]; specifically, our proposal can reduce the user's and the BASN's computation costs by 64% and 79%, respectively, compared to the scheme proposed in [31], which indicates that our protocol would be more suitable for WBANs with limited resources. For our future research, we will focus on the authentication of WBANs in the architecture of decentralized identity (DID) through blockchain.

Author Contributions: Validation, methodology, writing—original draft, K.L. and G.X. (Guosheng Xu); writing—review and editing, Q.C., C.W., and G.X. (Guoai Xu); validation, Y.G. and J.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was mainly funded by the National Natural Science Foundation of China under grant of No.: 62102042 and the National Key Research and Development Program of China under grant No.: 2021YFB3101500.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hernandez M.; Kohno R.; Kobayashi T.; Kobayashi T. New revision of IEEE 802.15.6 wireless body area networks. In Proceedings of the 2022 16th International Symposium on Medical Information and Communication Technology (ISMICT), Lincoln, NE, USA, 2–4 May 2022.
2. Cornet, B.; Fang, H.; Ngo, H.; Edward W. Boyer; Boyer W.; Wang H. An overview of wireless body area networks for mobile health applications. *IEEE Netw.* **2022**, *36*, 76–82. [\[CrossRef\]](#)
3. Nyangaresi, V. Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks. *Ad Hoc Netw.* **2023**, *142*, 103117. [\[CrossRef\]](#)
4. Ambarkar, S.; Shekokar, N. Toward smart and secure IoT based healthcare system. In *Internet of Things, Smart Computing and Technology: A Roadmap Ahead. Studies in Systems, Decision and Control*; Dey N., Mahalle P., Shafi P., Kimabahune V., Hassanien A. Eds.; Springer: Cham, Switzerland, 2020.
5. Alemdar, H.; Ersoy, C. Wireless sensor networks for healthcare: A survey. *Comput. Netw.* **2019**, *54*, 2688–2710. [\[CrossRef\]](#)
6. Liu, X.; Zhang, R.; Zhao, M. A robust authentication scheme with dynamic password for wireless body area networks. *Comput. Netw.* **2019**, *161*, 220–234. [\[CrossRef\]](#)

7. Zou, S.; Cao, Q.; Wang, C.; Huang Z.; Xu G. A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home in IoT. *IEEE Syst. J.* **2021**, *16*, 4938–4949. [\[CrossRef\]](#)
8. Rivest, R.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [\[CrossRef\]](#)
9. Kumar, P.; Lee, G-S; Lee, J-H. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors* **2012**, *12*, 1625–1647. [\[CrossRef\]](#)
10. Mo, J.; Hu, Z.; Lin, Y. Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks. *Secur. Commun. Netw.* **2020**, *2020*, 5047379. [\[CrossRef\]](#)
11. Khan, M.; Kumari, S.; Singh, P. Cryptanalysis of an efficient-strong authentication protocol (E-SAP) for healthcare applications using wireless medical sensor networks. *KSII Trans. Internet Inf. Syst.* **2013**, *7*, 967–979.
12. Khan, M.; Kumari, S. An improved user authentication protocol for healthcare services via wireless medical sensor networks. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 347169. [\[CrossRef\]](#)
13. He, D.; Kumar, N.; Chen, J.; Lee C.; Chilamkurti N.; Yeo S. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Syst.* **2013**, *21*, 49–60. [\[CrossRef\]](#)
14. Li, X.; Niu, J.; Kumari, S.; Liao J.; Liang W.; Khan M. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. *Secur. Commun. Netw.* **2016**, *9*, 2643–2655. [\[CrossRef\]](#)
15. Das, A.; Sutrala, A.; Odelu, V.; Goswami A. A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks. *Wirel. Pers. Commun.* **2017**, *94*, 1899–1933. [\[CrossRef\]](#)
16. Challa, S.; Das, A.; Odelu, V.; Kumar N.; Kumari, S.; Khan M.; Vasilakos A. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Comput. Electr. Eng.* **2018**, *69*, 534–554. [\[CrossRef\]](#)
17. Ostad-Sharif, A.; Abbasinezhad-Mood, D.; Nikooghadam, M. An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. *Int. J. Commun. Syst.* **2019**, *32*, e3913. [\[CrossRef\]](#)
18. Zhang, L.; Zhu, S.; Tang, S. Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. *IEEE J. Biomed. Health Inform.* **2017**, *21*, 465–475. [\[CrossRef\]](#)
19. Banerjee, S.; Odelu, V.; Das, A.; Srinivas, J.; Kumar N.; Chattopadhyay, S.; Choo K. A provably secure and lightweight anonymous user authenticated session key exchange scheme for internet of things deployment. *IEEE Internet Things J.* **2019**, *6*, 8739–8752. [\[CrossRef\]](#)
20. Wang, C.; Wang, D.; Tu, Y.; Wang H.; Xu G. Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 507–523. [\[CrossRef\]](#)
21. Pei D.; Salomaa A.; Ding C. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptograph*; World Scientific: Singapore, 1996.
22. Srinivas, J.; Das, A.; Kumar, N.; Rodrigues J. Cloud centric authentication for wearable healthcare monitoring system. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 942–956. [\[CrossRef\]](#)
23. Dharminder, D.; Mishra, D.; Li, X. Construction of RSA-based authentication scheme in authorized access to healthcare services. *J. Med. Syst.* **2020**, *44*, 6. [\[CrossRef\]](#)
24. Fotouhi, M.; Bayat, M.; Das, A.; Far H.; Pournaghi S.; Doostari M. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Comput. Netw.* **2020**, *177*, 107333. [\[CrossRef\]](#)
25. Yang, Z.; He, J.; Tian, Y.; Zhou J. Faster authenticated key agreement with perfect forward secrecy for industrial internet-of things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6584–6596. [\[CrossRef\]](#)
26. Boyd, C.; Mathuria, A.; Stebila, D. *Protocols for Authentication and Key Establishment*; Springer: Berlin/Heidelberg, Germany, 2020.
27. Mwitende, G.; Ali, I.; Eltayieb, N.; Wang B.; Li F. Authenticated key agreement for blockchain-based WBAN. *Telecommunication Systems.* **2020**, *74*, 347–365. [\[CrossRef\]](#)
28. Masud, M.; Gaba, G.; Alqahtani, S.; Muhammad G.; Gupta B.; Kumar P.; Ghoneim A. A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care. *IEEE Internet Things J.* **2021**, *8*, 15694–15703. [\[CrossRef\]](#)
29. Kumar, S.S.; Guajardo, J.; Maes, R.; Schrijen, G.-J.; Tuyls, P. The Butterfly PUF: Protecting IP on Every FPGA. In Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Washington, DC, USA, 30 April–4 May 2008; pp. 67–70.
30. Alzahrani, B.; Irshad, A.; Albeshri, A.; Alsubhi K. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. *Wirel. Pers. Commun.* **2021**, *117*, 47–69. [\[CrossRef\]](#)
31. Xie, Q.; Liu, D.; Ding, Z.; Tan X.; Han L. Provably Secure and Lightweight Patient Monitoring Protocol for Wireless Body Area Network in IoHT. *J. Healthc. Eng.* **2023**, *2023*, 4845850. [\[CrossRef\]](#)
32. Kobitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [\[CrossRef\]](#)
33. Narwal, B.; Mohapatra, A. SAMAKA: Secure and Anonymous Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks. *Arab. J. Sci. Eng.* **2021**, *46*, 9197–9219. [\[CrossRef\]](#)
34. Nyangaresi, V. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In Proceedings of the 2022 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 20–22 July 2022.
35. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [\[CrossRef\]](#)

36. Wang, D.; Wang, P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 708–722. [[CrossRef](#)]
37. Wang, D.; Zou, Y.; Dong, Q.; Song Y.; Huang X. How to Attack and Generate Honeywords. In Proceedings of the 43rd IEEE Symposium on Security and Privacy (IEEE S&P), Francisco, CA, USA, 23–25 May 2022; pp. 489–506.
38. Wang, D.; Cheng, H.; Wang, P. Zipf’s Law in Passwords. *IEEE Trans. Inf. Forensic Secur.* **2017**, *12*, 2776–2791. [[CrossRef](#)]
39. Liu, K.; Zhou, Z.; Cao, Q.; Xu G.; Wang C.; Gao Y.; Zeng W.; Xu G. A Robust and Effective Two-Factor Authentication (2FA) Protocol Based on ECC for Mobile Computing. *Appl. Sci.* **2023**, *13*, 4425. [[CrossRef](#)]
40. Qiu, S.; Wang, D.; Xu, G.; Kumari S. Practical and Provably Secure Three-Factor Authentication Protocol Based on Extended Chaotic-Maps for Mobile Lightweight Devices. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1338–1351. [[CrossRef](#)]
41. Wu, F.; Li, X.; Xu, L.; Vijayakumar P.; Kumar N. A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks with IoT Notion. *IEEE Syst. J.* **2021**, *15*, 1120–1129. [[CrossRef](#)]
42. Wang, C.; Wang, D.; Xu, G.; He D. Efficient Privacy-Preserving User Authentication Scheme with Forward Secrecy for Industry 4.0. *Sci. China-Inf. Sci.* **2022**, *65*, 1–15. [[CrossRef](#)]
43. Kumar, D.; Jain, S.; Khan, A.; Pathak P. An improved lightweight anonymous user authenticated session key exchange scheme for Internet of Things. *J. Ambient Intell. Humaniz. Comput.* **2020**, *14*, 5067–5083. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.