Hindawi
Security and Communication Networks
Volume 2017, Article ID 4167549, 8 pages
https://doi.org/10.1155/2017/4167549

Research Article

Efficient Anonymous Authenticated Key Agreement Scheme for Wireless Body Area Networks

Tong Li,[1] Yuhui Zheng,[2] and Ti Zhou[1]

[1]*School of Engineering Science, University of Chinese Academy of Sciences, Beijing 100049, China*
[2]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*

Correspondence should be addressed to Ti Zhou; zhouti@sdu.edu.cn

Received 5 September 2017; Accepted 18 October 2017; Published 21 November 2017

Academic Editor: Lianyong Qi

Wireless body area networks (WBANs) are widely used in telemedicine, which can be utilized for real-time patients monitoring and home health-care. The sensor nodes in WBANs collect the client's physiological data and transmit it to the medical center. However, the clients' personal information is sensitive and there are many security threats in the extra-body communication. Therefore, the security and privacy of client's physiological data need to be ensured. Many authentication protocols for WBANs have been proposed in recent years. However, the existing protocols fail to consider the key update phase. In this paper, we propose an efficient authenticated key agreement scheme for WBANs and add the key update phase to enhance the security of the proposed scheme. In addition, session keys are generated during the registration phase and kept secretly, thus reducing computation cost in the authentication phase. The performance analysis demonstrates that our scheme is more efficient than the currently popular related schemes.

1. Introduction

With the progress of society and the development of science and technology, people's health-care requirements are improved continuously. In the area of health-care, people are no longer satisfied with the traditional pattern of posttreatment, and hope that there is a new model achieving preventive early diagnosis and early treatment. As the population aging process accelerates and the number of older people increases, the need for surveillance of chronic diseases is increasing. The elderly can detect their own health anytime and anywhere, without having to go to the hospital. This can not only make a diagnosis and give treatment timely according to the patient's condition, but also reduce the cost of medical treatment and hospital burden. On the other hand, with the rapid development of wireless communication technology, the integration of physiological sensors and embedded computing technology, the health-care as the main application purpose of wireless body area networks (WBANs) has appeared correspondingly. WBANs act as an important branch of wireless sensor networks that provide a convenient and low-cost method for health monitoring of chronic patients.

WBANs can long-term monitor and record human health signals. WBANs mainly consist of wearable or implanted biomedical sensors and portable personal device, which can collect relevant physiological parameters such as heart rate, blood pressure, and blood sugar. WBANs achieve real-time or long-term monitoring of the relevant physiological parameters to provide timely and accurate data for doctors' diagnosis. The concept of WBANs was first introduced by Zimmerman in 1996 [1]. Later, several variations of WBANs were presented in the literature. The papers [2, 3] present a wireless EEG/ECG system using noncontact sensors to monitor human EEG and ECG data. The relevant sensors [4, 5] can provide patients with timely warning of the disease and remind the patient to be treated early. In addition, blood glucose in diabetic patients is monitored by micro blood glucose sensors. When the blood glucose value is lower than a certain value, the miniature syringe placed on the patient will inject insulin to control the level of the blood glucose in time.

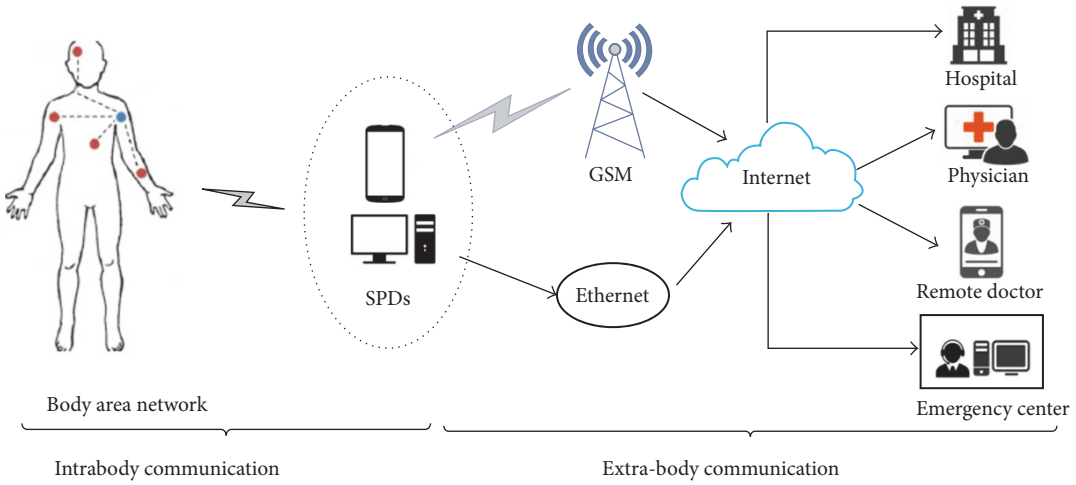

Figure 1: A typical wireless body area networks.

The working mechanism of WBANs is using sensors and networks to acquire user's data as well as doing operation of the data like sensing, storing, processing, and transmitting [6]. As is shown in Figure 1, the overall architecture of WBANs can be divided into two tiers. The first tier is the intrabody communication, which refers to the communication between sensor nodes and the smart portable device (SPD) held by the patient. The other is the extra-body communication, which refers to the whole network of the server. This tier enables SPD to communicate with the remote application provider (AP) such as the hospital, remote doctor, and medical institutions [7]. Our concern in this paper is to enhance the security of the extra-body communication.

The data collected or transmitted in WBANs are very sensitive and important because these data are the basis of clinical diagnostics. Besides, the open wireless network environment makes the application of WBANs face many security risks and threats. Therefore, the protection of client's privacy is the most concerned about the client. Such as in telemedicine applications, the client may need anonymous access to medical services. Doctors only need to know the physiological information related to the patient's condition and cannot acquire the client's privacy information, such as the user's name and ID number. Therefore, in the WBANs medical applications, we should use the relevant cryptographic algorithms to encrypt the user's privacy information to achieve users and medical institutions anonymous authentication and to ensure that the privacy information is not disclosed when the user is receiving medical services.

Key agreement and mutual authentication are two fundamental building blocks for meeting the security and privacy requirements [8, 9]. More specifically, key agreement is needed to establish a session key between AP and the client for ensuring the confidentiality and integrity of the information in transmission [10]. Mutual authentication requires that only the authorized WBANs client and AP are authenticated at the same time. Taking into account the importance of privacy security and resource constraint, we design an efficient and anonymous authenticated key agreement scheme for WBANs. Our contributions can be summarized as follows:

(i) By analyzing the existing authenticated key agreement scheme, we propose a novel certificateless authenticated key agreement scheme for WBANs, which is cost-effective and achieves many security requirements. The proposed scheme is based on an efficient and provably secure signature scheme from bilinear pairings [11, 12] and an identity-based authenticated key agreement protocol [13].

(ii) Most of the authentication protocols for WBANs generate the session key during the authentication phase, and our scheme generates the session key in the registration phase and stores it secretly. Therefore, when the WBANs client authenticates himself/herself to a requested AP, they do not need to establish the session key; thus, this design reduces the computation cost.

(iii) The proposed scheme implements the function of key update, which avoids the repeated use of the same session key. The WBANs client can update their session key freely.

This paper is organized as follows. We discuss related works in Section 2. Section 3 briefly describes the basic definition of the bilinear pairing and BDH assumption. Section 4 introduces the system model of our authenticated key agreement scheme for WBANs and lists several security requirements that need to be met. We describe the proposed scheme for WBANs in Section 5. We perform the security analysis for the proposed scheme in Section 6. Section 7 discusses computation cost of the proposed scheme. We make concluding remarks in Section 8.

2. Related Works

Because the patient health data is sensitive and face many security threats in open wireless network environment, thus

the protection of patient's privacy is an important issue. Over the last few years, many authentication schemes for WBANs have been proposed for practical applications.

In 2012, Liu et al. presented a remote anonymous authentication protocol to enable client terminals and application to securely access WBANs services [14]. Liu et al. also presented a pair of efficient and light-weight authentication protocols to enable remote WBANs clients to anonymously enjoy health-care service in 2013 [15]. However, Xiong demonstrated that their signature schemes fail to resist the public key replacement attack. Moreover, Liu et al. authentication protocols cannot offer forward security and scalability [16].

Zhao [17] discovered that the protocols of Liu et al. are insecure when the verifier table is disclosed. To improve security and efficiency, Zhao proposed an identity-based efficient anonymous authentication scheme for WBANs. However, Zhao's scheme cannot provide real anonymity because the users' pseudo identities are constant value and the adversary could tract the users; then Wang and Zhang proposed a new anonymous authentication scheme for WBANs [18]. Security analysis shows that the proposed scheme could overcome weakness in previous scheme.

He reviewed the Liu et al. scheme [15] and pointed out that it is not secure for medical applications by proposing an impersonation attack. Afterwards, they proposed a new anonymous authentication scheme for WBANs and proved that is provably secure [19]. In 2017, Xiao et al. proposed a novel certificateless anonymous remote authentication protocol featured with efficient revocation [7], and this is the first time considering the revocation functionality of anonymous remote authentication for the WBANs. In 2015, Shen et al. proposed an enhanced secure sensor association and key management protocol based on elliptic curve cryptography and hash chains for WBANs [20]. Their protocol achieves mutual authentication and secure communication between sensor nodes, the patient controller, and health-care worker. Because the computation ability of medical sensors and controller nodes in WBANs is very limited, we proposed an efficient certificateless authenticated key agreement scheme for WBANs.

3. Preliminaries

In this section, the basic definition and properties of the bilinear pairing and the Bilinear Diffie-Hellman (BDH) assumption [21] are briefly introduced.

3.1. Bilinear Pairing. Let $\mathbb{G}_1$ be a cyclic additive group with a prime order q, and let $\mathbb{G}_2$ be a cyclic multiplicative group with the same order q. P is an arbitrary generator of $\mathbb{G}_1$.

Suppose that the discrete logarithm problem (DLP) is hard in $\mathbb{G}_1$ and $\mathbb{G}_2$. A bilinear pairing is a map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ which satisfies the following properties:

3.1.1. Bilinear. For all $P, Q, R \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$, we have

$$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab},$$
$$\hat{e}(P + R, Q) = \hat{e}(P, Q)\hat{e}(R, Q),$$
$$\hat{e}(P, R + Q) = \hat{e}(P, R)\hat{e}(P, Q).$$

3.1.2. Nondegenerate. If $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_1$, then $\hat{e}(P, Q)$ is a generator of $\mathbb{G}_2$, which also implies $\hat{e}(P, Q) \neq 1$.

3.1.3. Computability. There is a computable algorithm to get $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

As is shown in [22], the modified Tate pairing on a supersingular elliptic curve is such a bilinear pairing.

3.2. The Bilinear Diffie-Hellman (BDH) Assumption. Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two groups of prime order q. Let $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be an admissible bilinear map. We have $\{P, aP, bP, cP\} \in \mathbb{G}_1$ and compute $\hat{e}(P, Q)^{abc}$, where a, b, c are randomly chosen from $\mathbb{Z}_q^*$. An algorithm is said to solve the BDH problem with an advantage of ε if

$$\Pr\left[\mathcal{A}(P, aP, bP, cP) = \hat{e}(P, P)^{abc}\right] \geq \varepsilon. \quad (1)$$

We assume that the BDH problem is hard, which means there is no polynomial time algorithm to solve BDH problem with nonnegligible probability.

4. Problem Statement

In this section, some security requirements that should be reached in the proposed scheme are stated. Then, the system model of our authenticated key agreement scheme is introduced.

4.1. Security Requirements. There are some security requirements which need to be met in the design of the certificateless authenticated key agreement scheme for WBANs [23].

4.1.1. Anonymity. This requirement ensures that an adversary does not get the identities of legal users in authentication process. Sensor nodes detection, collection, and transmission of data are closely related to the user in WBANs. These data refer to the user's private information, so users want to enjoy their own wireless medical services, and at the same time their privacy will not be disclosed to the unauthorized illegal third party. Therefore, the purpose of anonymity is to protect the user from being compromised when enjoying the service.

4.1.2. Forward Secrecy. In case that the private key of users or AP is compromised, the attacker could not effectively generate the forward session key, the confidentiality of previous session keys is still fulfilled, and we called this condition forward secrecy.

4.1.3. Unlinkability. It indicates that any third party except the client and AP is unable to learn whether two different protocol sessions are initiated by the same user. In other words, the adversary cannot distinguish whether he has seen the same WBANs client twice.

4.1.4. Mutual Authentication. This requirement is used to confirm the legitimacy of the user's and AP's identity in WBANs, so as to achieve the purpose of identifying and preventing illegal third parties from participating in communications. For example, in medical WBANs applications,

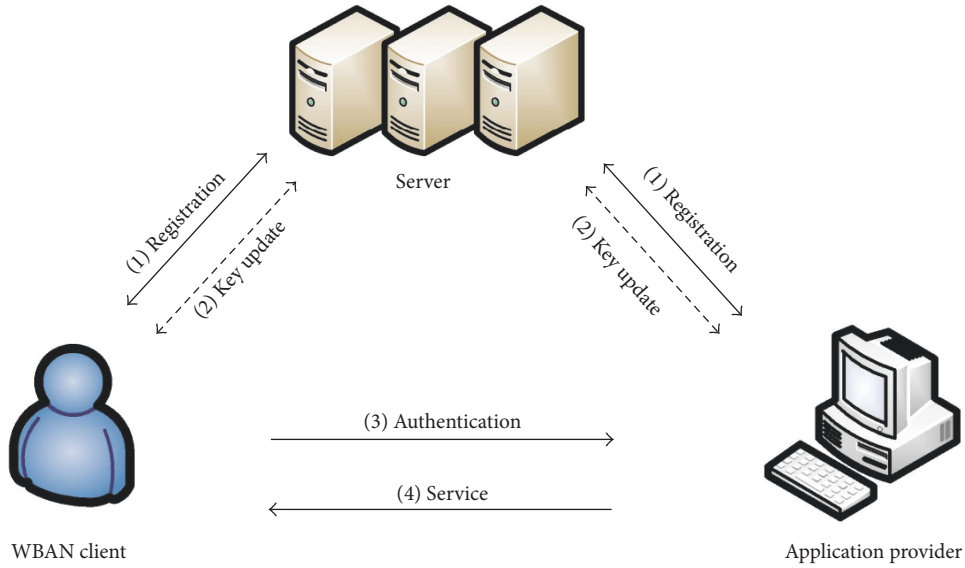

Figure 2: Working flow of the proposed authenticated key agreement protocol.

the authentication scheme enables AP to identify illegal third parties and ensures that only an authorized user accesses services from AP.

4.1.5. Session Key Establishment. Upon a successful mutual authentication process, a session key is established between the WBANs users and the application provider for secure subsequent communication. This session key is used to encrypt physiological data while requesting and accessing services from an AP.

4.1.6. Nonrepudiation. The user cannot deny that he/she enjoys the service provided by application providers, while service providers cannot deny that they provide a certain service for the user. The user computes the signature information with the application provider for authentication; once the authentication is successful, the user cannot deny that he/she has accessed the medical service.

4.2. System Model. The proposed system consists of three types of entities. The working flow between them is illustrated in Figure 2, which has the following process [24].

(i) Server: the server is similar to a completely trusted third party and responsible for system initialization. Moreover, it is in charge of the registration of WBANs clients and application providers (APs). Specifically, the server acts as a key generating center, whose responsibility is to generate system parameters and the secret keys for the client and AP.

(ii) WBANs client: the WBANs client is monitored by the server and enjoys medical services though smart portable devices or a smart phone. Before accessing some services offered by AP, the client should be registered with the server and preloaded with the public parameters.

(iii) Application provider (AP): application providers may be hospitals, clinics, or any other medical institutions. It also should be registered with the server and preloaded with public parameters before they offer some health-care monitoring and treatments remotely to WBANs clients.

5. Proposed Scheme

In this section, an efficient certificateless authenticated key agreement scheme for WBANs is proposed, and our scheme involves three entities; they are the WBANs client, the server, and the application provider, respectively. In addition, this scheme consists of the initialization, registration, authentication, and key update phases. In the registration phase, the client submits some personal information to the server; then the server generates partial private key for user and some related parameters. After that, the server sends them to the client in a secure channel. This phase is carried out only once, unless the client reregisters. Upon accomplishment of the registration phase, the client is able to access the server in the authentication phase. This phase can be performed as many times as needed. In the key update phase, the client can update his session key and change his pseudonym by interacting with the server.

5.1. Initialization. The server performs the following operations firstly. Given a security parameter l, the server chooses two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same prime order $q > 2^l$ and a modified Weil pairing map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. $\mathbb{G}_1$ is a cyclic additive group, and $\mathbb{G}_2$ is a cyclic multiplicative group. P is a generator of groups $\mathbb{G}_1$.

(a) Let $g = \hat{e}(P, P)$; then the server selects two distinct cryptographic hash functions $H_1: \{0,1\}^* \to Z_q^*$ and $H_2: \{0,1\}^* \times \mathbb{G}_1 \to Z_q^*$.

(b) The server generates a random number $s \in Z_q^*$ as its master key and computes its public key $P_{\text{pub}} = sP \in \mathbb{G}_1$.

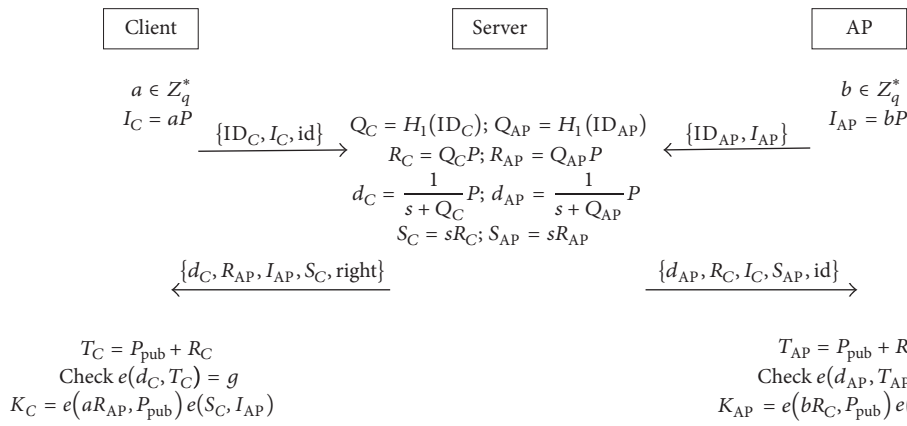

Figure 3: Working flow of the registration phase.

Afterwards, the server picks a message authentication code $\mathrm{MAC}_{(\cdot)}(\cdot)$.

(c) The server publishes the system parameter $\mathrm{listparams} = \{l, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, g, P_{\mathrm{pub}}, H_1, H_2, \mathrm{MAC}_{(\cdot)}(\cdot)\}$ to the WBANs clients and APs; however, s is kept in secret.

5.2. Registration. Each client needs to perform the following operations (shown as Figure 3) with the server once before he or she can access the AP for medical services. Likewise, an application provider should first perform this phase with the server once before it can provide services to the clients.

(a) The client generates a pseudonym $\mathrm{id} = \{0,1\}^*$ as his identity when he needs to authenticate with AP and picks a random number $a \in Z_q^*$ secretly. After that, this client computes $I_C = aP$ and sends the message $\{\mathrm{ID}_C, I_C, \mathrm{id}\}$ to the server in a secure channel. Note that ID_C is the real identity of the client.

(b) AP associated with identity $\mathrm{ID}_{\mathrm{AP}}$ selects a secret value $b \in Z_q^*$ and computes $I_{\mathrm{AP}} = bP$ and then sends its identity $\mathrm{ID}_{\mathrm{AP}}$ and I_{AP} to the server in a secure channel.

(c) Once the server receives this client's message $\{\mathrm{ID}_C, I_C, \mathrm{id}\}$ and the message $\{\mathrm{ID}_{\mathrm{AP}}, I_{\mathrm{AP}}\}$ from AP, it first verifies that their identities are valid or not and defines the client's right and then computes $Q_C = H_1(\mathrm{ID}_C)$, $R_C = Q_C P$, $S_C = sR_C$, and $d_C = (1/(s + Q_C))P$. Among them, d_C is the partial private key of the client. Likewise, the server also computes $Q_{\mathrm{AP}} = H_1(\mathrm{ID}_{\mathrm{AP}})$, $R_{\mathrm{AP}} = Q_{\mathrm{AP}} P$, $S_{\mathrm{AP}} = sR_{\mathrm{AP}}$, and $d_{\mathrm{AP}} = (1/(s + Q_{\mathrm{AP}}))P$. Afterwards, the server sends the message $\{d_C, R_{\mathrm{AP}}, I_{\mathrm{AP}}, S_C, \mathrm{right}\}$ and the message $\{d_{\mathrm{AP}}, R_C, I_C, S_{\mathrm{AP}}, \mathrm{id}\}$ to the client and AP in secret, respectively.

(d) After receiving the message $\{d_C, R_{\mathrm{AP}}, I_{\mathrm{AP}}, S_C, \mathrm{right}\}$ from the server, the client first computes $T_C = P_{\mathrm{pub}} + R_C$ and verifies the message's validity by checking whether the formula $\hat{e}(d_C, T_C) = g$. If it holds, the client generates the session key $K_C = \hat{e}(aR_{\mathrm{AP}}, P_{\mathrm{pub}})\hat{e}(S_C, I_{\mathrm{AP}})$. Now the client stores K_C, d_C, right, and T_C in a registration table secretly.

(e) Likewise, upon receiving the server's message $\{d_{\mathrm{AP}}, R_C, I_C, S_{\mathrm{AP}}, \mathrm{id}\}$, AP first computes $T_{\mathrm{AP}} = P_{\mathrm{pub}} + R_{\mathrm{AP}}$ and checks its correctness by checking whether $\hat{e}(d_{\mathrm{AP}}, T_{\mathrm{AP}}) = g$.

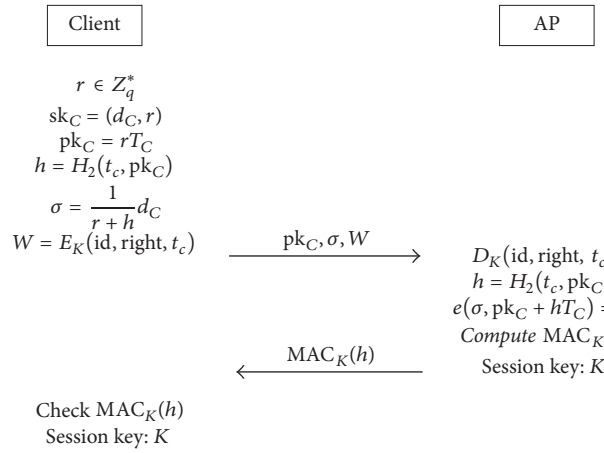

Figure 4: Working flow of the authentication phase.

If the formula holds, AP generates the session key $K_{\mathrm{AP}} = \hat{e}(bR_C, P_{\mathrm{pub}})\hat{e}(S_{\mathrm{AP}}, I_C)$. Therefore, the common session key is $K = K_C = K_{\mathrm{AP}} = \hat{e}(aR_{\mathrm{AP}} + bR_C, sP)\hat{e}(S_{\mathrm{AP}}, I_C)$ Afterwards, AP stores the common session key K and R_C secretly.

5.3. Authentication. In this phase, as shown in Figure 4, the client and AP can authenticate each other by performing the below process.

(a) The client chooses a random number $r \in Z_q^*$ and sets r as his secret value and then outputs a pair (d_C, r) as the client's private key. That is, the client's private key $\mathrm{sk}_C = (d_C, r)$ is the pair consisting of the partial private key and the secret value. Afterwards, the client generates his public key $\mathrm{pk}_C = rT_C$ and computes $h = H_2(t_C, \mathrm{pk}_C)$, $\sigma = (1/(r + h))d_C$, where t_C denotes the current timestamp. The client encrypts id, right, and t_C with the session key generated during the registration phase; this process denotes $W = E_K(\mathrm{id}, \mathrm{right}, t_C)$. The client sends the message $\{\mathrm{pk}_c, \sigma, W\}$ to AP.

(b) Upon receiving $\{\mathrm{pk}_c, \sigma, W\}$, AP gets $(\mathrm{id}, \mathrm{right}, t_C)$ by using the session key K to decrypt W. AP calculates $h = H_2(t_C, \mathrm{pk}_C)$ and checks whether the equation $\hat{e}(\sigma, \mathrm{pk}_C + hT_C) = g$ holds. If it does not hold, AP rejects the client's

request. Otherwise, AP computes the authentication code $\mathrm{MAC}_K(h)$ and sends the code to the client. In addition, the session key has been generated during the registration phase and kept secretly in the database.

The correctness of the verification algorithm $\hat{e}(\sigma, \mathrm{pk}_C + hT_C) = g$ is proved as follows:

$$\begin{aligned}\hat{e}\left(\sigma, \mathrm{pk}_C + hT_C\right) &= \hat{e}\left(\sigma, rT_C + hT_C\right)\\ &= \hat{e}\left(\sigma, r\left(P_{\mathrm{pub}} + R_C\right) + h\left(P_{\mathrm{pub}} + R_C\right)\right)\\ &= \hat{e}\left(\frac{1}{(r+h)(s+Q_C)}P, (r+h)(s+Q_C)P\right)\\ &= \hat{e}(P,P) = g.\end{aligned} \tag{2}$$

(c) Once receiving the response message $\mathrm{MAC}_K(h)$, the client checks the integrity of the authentication code. If the result is negative, the user quits the current session. Otherwise, the client will authenticate AP and regard K as the session key in the later communication.

5.4. Key Update. The key update phase is provided to allow the client and AP to change their session key freely. When the client wants to update his/her session key, he/she first needs to go through the authentication phase to make sure that the past session key is valid and then updates the session key by reregistering with the server. More specifically, the client selects a new random number a^* and computes $I_C^* = a^* P$ and then sends I_C^* to the server. Likewise, AP updates the session key with the same steps. Afterwards, the client and AP replace K with K^* and store K^* secretly.

6. Security Analysis

In this section, the security analysis of the proposed scheme is presented. The security properties of the proposed scheme can be listed as follows.

6.1. Client Anonymity. The real identity of the requesting client cannot be revealed by any third party, including the application provider [25, 26]. As specified in Section 5, in the registration phase, the client sends his/her pseudonym to the server. Afterwards, the server sends this pseudonym id to AP in a secure channel; then AP stores id as the client identity. AP does not know the client real identity. In the authentication phase, the client encrypts his pseudonym id using the session key K and sends it to AP. Only AP can decrypt it with K. On the other hand, even if the adversary gets the client's pseudonym, he/she still cannot know the client's real identity ID_c. Moreover, the client pseudonym id is dynamic; the user can update the pseudonym by reregistering. Therefore, the proposed protocol achieves client anonymity.

6.2. Forward Secrecy. Forward secrecy indicates that the session keys agreed upon in previous sessions remain undisclosed even when the long-term secret key of the participants is disclosed [27]. In the proposed scheme, the long-term secret keys of the client and AP are S_C and S_{AP}, respectively. Even if S_C and S_{AP} are disclosed, the adversary cannot compromise the session key in the past. Because the adversary cannot get the secret values a, b and the server's master keys.

6.3. Unlinkability. In each run of our authenticated key agreement protocol, the message $\{\mathrm{pk}_c, \sigma, W\}$ that the client sends to AP is different. More specifically, in each authentication phase, r is a secret random number and the public key pk_C and the signature σ are different. t_C is a current timestamp, so $\mathrm{MAC}_K(h)$ is also unique in each session. Therefore, the adversary cannot learn whether two authentication sessions involve the same client.

6.4. Mutual Authentication. In the registration phase of the proposed scheme, the client and the server perform mutual authentication through the formula $\hat{e}(d_C, T_C) = g$ and the identity of the client ID_C. Because the message in the registration phase is transmitted over a secure channel, only the legitimate client has the knowledge of Q_C and computes $T_C = P_{\mathrm{Pub}} + Q_C P$. AP and the server are authenticated in the same way to prevent the adversary from sending junk information to AP constantly. In authentication phase, only the requested AP can authenticate the accessing user by checking user's signature σ, and AP verifies whether the formula $\hat{e}(\sigma, \mathrm{pk}_C + hT_C) = g$ holds. Among them, σ is generated by the secret value r and the hash value h. In addition, h is related to t_C, which can only be recovered by AP. The client authenticates AP by the authentication code $\mathrm{MAC}_K(h)$, because $h = H_2(t_C, \mathrm{pk}_C)$ is related to t_C, and the session key K is kept secret by the client and AP. Overall, the proposed scheme accomplishes mutual authentication between the client and AP.

6.5. Session Key Establishment. Beside mutual authentication, another critical task is to establish the session key to protect the health information in transit. In registration phase, we used the smart key agreement scheme which uses the Weil pairing to generate the session key; K can only be shared by AP and the client. The session key $K = \hat{e}(aR_{\mathrm{AP}} + bR_C, sP)$ between the AP and the user is generated by the secret random values a and b from the client and AP. More specifically, the common session key depends on the identities Q_C, Q_A of the client and AP, the master key s of the server, and two ephemeral keys a, b. So that the adversary cannot get K. Therefore, the proposed scheme for WBANs could provide session key establishment.

6.6. Nonrepudiation. When the client requests a service from the server, then he/she sends his signature σ to the server. In the certificateless cryptographic mechanism, the user's private key sk_C consists of two parts. The first part is the secret value r selected by the client randomly, and the other part is the partial private key d_C provided by the server. The adversary cannot forge this signature without knowing the user's private key. Therefore, once the authentication between the client and AP is successful, AP will provide services for the client and this client cannot deny that he had requested services from the AP and enjoyed services. Similarly, when AP receives the client's request message, pk_c, σ, and W, then

Table 1: Comparison of computation cost in the registration phase.

Scheme	Client	AP
Xiong's	$1T_{\text{mul}}$	$1T_{\text{mul}}$
Jiang et al.'s	$1T_{\text{mul}} + 1T_h$	$1T_{\text{mul}} + 1T_h$
Our	$2T_{\text{mul}} + 1T_{\text{add}} + 2T_b$	$2T_{\text{mul}} + 1T_{\text{add}} + 2T_b$

Table 2: Comparison of computation cost in the authentication phase.

Scheme	Client	AP
Xiong's	$5T_{\text{mul}} + 2T_{\text{add}} + 5T_h$	$3T_{\text{mul}} + 4T_{\text{add}} + 3T_h$
Jiang et al.'s	$3T_{\text{mul}} + 4T_h + 1T_k + 1T_b$	$3T_{\text{mul}} + 4T_h + 1T_k + 1T_b$
Our	$2T_{\text{mul}} + 1T_h + 1T_k$	$1T_h + 1T_k + 1T_b$

it uses the session key to decrypt W. Afterwards, the server can get t_C and computes $h = H_2(t_C, \text{pk}_C)$ and then sends $\text{MAC}_K(h)$ to the client to complete the authentication. Since any third party cannot get the session key, so AP cannot deny that he has provided services to the user.

7. Performance Analysis

On account of the resource limited system for WBANs, we analyze the computational cost of the proposed scheme in this section. We also give comparison of the proposed scheme with He and Jiang's schemes in terms of computational complexity.

For convenience, we give the definition of the notations used in this section as follows:

(1) T_{mul}: the execution time of a elliptic curve point multiplication operation

(2) T_K: the execution time of a symmetric key encryption/decryption operation

(3) T_h: the execution time of a hash function operation

(4) T_{add}: the execution time of a point addition operation

(5) T_b: the execution time of a bilinear map operation

The comparison of computation cost among related schemes is summarized as the following two tables. In Table 1, we compare our scheme with Xiong [16] and Jiang et al.'s [27] schemes in the registration phase. In the authentication phase, the comparison results in terms of computational cost are summarized in Table 2. Although the computational cost of Xiong and Jiang et al.'s schemes is lower than our scheme in the registration phase. However, the registration phase is carried out only once, unless the client reregisters. In the authentication phase, our scheme is more efficient than the other two schemes and this phase can be performed as many times as needed. In addition, Jiang et al.'s and Xiong's schemes do not have the key update phase. If the session keys of their protocols are compromised, then their protocols are insecure. In order to improve the shortcomings of Jiang et al.'s and Xiong's schemes, the proposed scheme add the key update phase. The client and AP can update their session keys freely to enhance the security of the communication between the client and AP.

8. Conclusion

Due to the limited computing capability and storage resource of sensor nodes in WBANs, we propose an efficient anonymous authenticated key agreement scheme for WBANs in this paper. The proposed scheme can reduce the computational cost at the client side in the authentication phase. In addition, we add the key update phase in the scheme to guarantee the security of the session key. In order to provide the real anonymity of clients, we use the pseudonym to replace the user's real identity when the user requests the service from AP. The client can update the pseudonym by reregistering, so that the client pseudonym is dynamic. Moreover, the proposed scheme satisfies a set of security properties, such as forward secrecy, unlinkability, and nonrepudiation. The performance analysis shows that our scheme is more efficient than Xiong's scheme [16] and Jiang et al.'s scheme [27] in the authentication phase. It can be concluded that the proposed scheme can be well utilized in practical WBANs application scenarios.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] T. G. Zimmerman, "Personal area networks: Near-field intrabody communication," *IBM Systems Journal*, vol. 35, no. 3-4, pp. 609–617, 1996.

[2] Y. M. Chi and G. Cauwenberghs, "Wireless non-contact EEG/ECG electrodes for body sensor networks," in *Proceedings of the International Conference on Body Sensor Networks (BSN '10)*, pp. 297–301, Singapore, June 2010.

[3] A. Sapio and G. R. Tsouri, "Low-power body sensor network for wireless ECG based on relaying of creeping waves at 2.4GHz1," in *Proceedings of the 2010 International Conference on Body Sensor Networks, BSN 2010*, pp. 167–173, Singapore, June 2010.

[4] Z. Wang, F. Xiao, N. Ye, R. Wang, and P. Yang, "A See-through-wall system for device-free human motion sensing based on battery-free RFID," *ACM Transactions on Embedded Computing Systems*, vol. 17, article 6, no. 1, pp. 1–21, 2017.

[5] H. Zhu, F. Xiao, L. Sun, R. Wang, and P. Yang, "R-TTWD: Robust device-free through-the-wall detection of moving human With WiFi," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, pp. 1090–1103, 2017.

[6] G. Xie, G. Zeng, Z. Li, R. Li, and K. Li, "Adaptive dynamic scheduling on multifunctional mixed-criticality automotive cyber-physical systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 6676–6692, 2017.

[7] F. Xiao, L. Sha, Z. Yuan, and R. Wang, "VulHunter: A discovery for unknown Bugs based on Analysis for known patches in industry internet of things," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 99, pp. 1–13, 2017.

[8] J.-H. Yang and C.-C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Computers & Security*, vol. 28, no. 3-4, pp. 138–143, 2009.

[9] T.-T. Truong, M.-T. Tran, and A.-D. Duong, "Improvement of the more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC," in *Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA '12)*, pp. 698–703, Fukuoka, Japan, March 2012.

[10] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, 2017.

[11] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 390–394, 2009.

[12] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2402–2415, 2017.

[13] N. P. Smart, "Identity-based authenticated key agreement protocol based on Weil pairing," *IEEE Electronics Letters*, vol. 38, no. 13, pp. 630–632, 2002.

[14] J. Liu, Z. Zhang, R. Sun, and K. S. Kwak, "An efficient certificateless remote anonymous authentication scheme for wireless body area networks," in *Proceedings of the 2012 IEEE International Conference on Communications, ICC 2012*, pp. 3404–3408, can, June 2012.

[15] J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2013.

[16] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 12, pp. 2327–2339, 2014.

[17] Z. Zhao, "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, article 13, 7 pages, 2014.

[18] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *Journal of Medical Systems*, vol. 39, no. 11, article 136, 2015.

[19] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[20] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu, and X. Sun, "Enhanced secure sensor association and key management in wireless body area networks," *Journal of Communications and Networks*, vol. 17, no. 5, pp. 453–462, 2015.

[21] B. Dan and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Springer Berlin, Heidelberg, Germany, 2001.

[22] I. F. Blake, G. Seroussi, and N. P. Smart, "Advances in elliptic curve cryptography," vol. 22, no. 03, 2005.

[23] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "A survey on wireless body area network: Security technology and its design methodology issue," in *Proceedings of the 2nd IEEE International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2015*, India, March 2015.

[24] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communications Survey & Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[25] Z.-T. Li, Q. Chen, G.-M. Zhu, Y.-J. Choi, and H. Sekiya, "A low latency, energy efficient MAC protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 946587, 9 pages, 2015.

[26] Z. Tang, A. Liu, Z. Li, Y.-J. Choi, H. Sekiya, and J. Li, "A trust-based model for security cooperating in vehicular cloud computing," *Mobile Information Systems*, vol. 2016, Article ID 9083608, 22 pages, 2016.

[27] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth," *Journal of Medical Systems*, vol. 40, no. 11, article no. 231, 2016.