Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2011, Article ID 282986, 10 pages
doi:10.1155/2011/282986

Research Article

A Biometric Key Establishment Protocol for Body Area Networks

Lin Yao,[1] Bing Liu,[1] Guowei Wu,[1] Kai Yao,[2] and Jia Wang[1]

[1] *School of Software, Dalian University of Technology, Dalian 116023, China*
[2] *Library Information Center, Shenyang University of Technology, Shenyang 110178, China*

Correspondence should be addressed to Guowei Wu, wgwdut@dlut.edu.cn

Received 14 March 2011; Accepted 19 May 2011

Current advances in semiconductor technology have made it possible to implant a network of biosensors inside the human body for health monitoring. In the context of a body area network (BAN), the confidentiality and integrity of the sensitive health information is particularly important. In this paper, we present an ECG (electrocardiogram)-signal-based key establishment protocol to secure the communication between every sensor and the control unit before the physiological data are transferred to external networks for remote analysis or diagnosis. The uniqueness of ECG signal guarantees that our protocol can provide long, random, distinctive and temporal variant keys. Biometric Encryption technique is applied to achieve the mutual authentication and derive a non-linkable session key between every sensor and the control unit. The correctness of the proposed key establishment protocol is formally verified based on SVO logic. Security analysis shows that our protocol can guarantee data confidentiality, authenticity and integrity. Performance analysis shows that it is a lightweight protocol.

1. Introduction

Current advances in semiconductor technology have made it possible to implant some sensor nodes inside the human body for health monitoring. In such a deployment scenario of sensors, some wearable sensors called biometric sensors or biosensors will be usually located on the body surface to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants. These biosensors form a wireless network between themselves, which is called the body area network (BAN) [1–3]. Before the physiological data detected are passed on to external networks for remote analysis, diagnosis, or treatment, these data must be transferred to a single body control unit (CU) such as the sink node worn on the human body. Thus, data transmission can be classified into three levels [4]: (1) between the CU and every biosensor in the BAN; (2) between the CU and a remote server; (3) between the remote server and the physicians.

While the communication rate specifications in a BAN are typically low, the security requirements are stringent, especially when sensitive medical data are exchanged. It should be impossible for an adversary to eavesdrop, inject, and modificate these sensitive data. Privacy laws and regulations also mandate that security and privacy must be guaranteed when the patient-related data are created, transferred, stored, and processed in the BAN [5]. On one hand, authentication between a biosensor and CU must be performed over the network. Without the successful authentication, an attacker may pretend to be a user and transmit false data to the CU, which may lead a wrong diagnosis. On the other hand, data encryption is also important to prevent an attacker from sniffering or modificating these sensitive data. Therefore, a common session key is needed to secure the communication.

There are two classical personal authentication approaches in traditional cryptosystems: (1) knowledge-based approach; (2) token-based approach. Token or knowledge is prone to be forgotten, lost, stolen, or duplicated. Either approach cannot represent the unique user. Compared with knowledge-based approach and token based approach, biometrics can represent the uniqueness of one user. However, the conventional biometric characteristics such as iris, fingerprint, or face are static biometrics. A novel kind of biometric traits, such as heart rate variability, interpulse interval, and other features of electrocardiogram and photoplethysmogram, has been recently studied as a new identification approach [4]. In our protocol, ECG as the dynamic biometrics is utilized to authenticate between a biosensor and CU. The idea of using ECG comes from the observation that the human body is dynamic and complex and the physiological state of a subject is quite randomness and time variance [6]. ECG is typically collected and utilized in many recognition applications, which is in accordance with the data minimization principle [7].

In order to ensure data confidentiality and privacy, cryptographic algorithms are classified into symmetric and asymmetric algorithms. Asymmetric algorithms require more computation resources and storage resources compared with symmetric algorithms. Asymmetric key or public key cryptography is unsuitable in BAN, because sensor nodes are limited in power, computational capacities, and memory. In our protocol, we prefer the symmetric cryptographic algorithm. Based on the Biometric Encryption [8, 9], a symmetric cryptographic key is established between every biosensor and CU.

In our previous work, we have proposed a key establishment protocol, named by ESKE, based on ECG signals combining with the fuzzy vault scheme [10]. When a CU authenticates a biosensor, it will send a message including the real biometric points and some chaff points. As soon as receiving the message, the biosensor will calculate the similarity between its own set of points and the set of points from the CU. If a sufficient number of points can match within a certain threshold, the biosensor will be proved legal. Then, a session key will be established. In order to improve the match accuracy, more chaff points should be transmitted, which consumes more bandwidth. At the same time, the forward secrecy and backward secrecy cannot be guaranteed. Based on our previous work, Biometric Encryption technique instead of the fuzzy vault scheme is adopted to lock the session key at one end and unlock it at the other end. As biosensors have stringent constrains of power, memory, and computation capability, high effective security technology should be implemented. When we design our key establishment protocol, security and resource constraints must be balanced.

The remainder of this paper is organized as follows. In Section 2, we describe the related work. In Section 3, we give a brief introduction to Biometric Encryption. We present the proposed scheme in Section 4. The formal verification of its correctness is presented in Section 5. The security and performance analysis are given in Section 6. Finally, we conclude the paper in Section 7.

2. Related Work

With the advance of computer and networking technology convergence trends, pervasive computing is regarded as key technology to assist real-time medical and healthcare information service with the help of deploying sensors [11, 12]. A number of theoretical and technical approaches are proposed [11, 13–21]. But only a framework approach to balance the security and the limited resources of biosensors is proposed in the above papers, lacking the real experiments on the human body signals.

Several security solutions have been proposed to protect the BAN security. Four kinds of solutions are classified in [22]: TinySec, hardware encryption, elliptic curve cryptography and biometric methods.

TinySec [23] is proposed as a solution to achieve link layer encryption in the BAN. In the TinySec approach, packets are encrypted by a group key shared among biosensors. The group key is programmed into every sensor before the sensor network is deployed. If one biosensor discloses the key or it acts as an attacker, all the information in the BAN will be disclosed.

Hardware [22] encryption is an alternative approach of TinySec. In the BAN, there is a radio chip supporting only the encryption algorithms on every biosensor. The base station shares the encryption key with every biosensor, and only the base station can decrypt the traffic. The base station collects data from the whole network and usually acts as a gateway to other networks. Therefore, it can be considered as a single point of failure. If an adversary mounts several DoS attacks, the whole WSN will be collapsed. Another drawback is that hardware encryption is highly dependent on the specific platform. Not all the biosensors produced by the different manufactures can support the platform.

Elliptic curve cryptography is a public-key cryptography approach based on the algebraic structure of elliptic curves over finite fields. It has been used in the wireless sensor network recently [24, 25]. Even though elliptic curve cryptography is feasible for sensor nodes, its energy requirements are still orders of magnitude higher compared to those of symmetric cryptosystems [22]. For example, some works [26, 27] are considered as costly due to high processing requirements. Some symmetric key distribution techniques [28, 29] require predeployment and adjust the topology when the BAN changes, which causes high computation cost because the topology of a BAN changes frequently.

Biometrics derived from the human body to secure the keying material is firstly proposed by Cherukuri in 2003 [30]. The mechanism adopts the error-correcting codes and the multiple biometrics to secure the key. Compared with the traditional asymmetric key algorithms, this technique can reduce the cost of computation and communication. In this paper, no implementation details are given. For example, how to collect the relevant biometric data and how to examine their variation with time for individuals are not expounded. The authors proposed a biometric based distributed key management approach for BAN, but only a system architecture is given without detail experiments on physiological signals [31].

Time information of heartbeats as an excellent biometric characteristic can be used to secure the BAN by Poon et al. [32, 33]. A biometric trait generated from a sequence of interpulse interval is also to secure the BAN [33]. The interpulse interval can be derived from two sources, namely, ECG and photoplethysmogram (PPG) time series. On one hand, the interpulse interval is used to secure the transmission of the encryption key between biosensors. On the other hand, it is also used as an identity for mutual authentication between biosensors. But the experiments show that the average Hamming distance between the keys generated from ECG or PPG for the same subject is 60 or 65 bits, even though the keys are long and random. The main reason is that the physiological signals from ECG and PPG have high correlation without the same values, so the keys generated by ECG and PPG have different values. Based on the ECG signals, other schemes have been proposed for key distribution and authentication [34]. The major challenge for ECG is that biometrics derived from physiological features possesses the high degree of noise and variability inherently present in these signals. As a result, fuzzy methods are needed to enable proper operations with adequate performance in terms of false acceptance rate (FAR) and false rejection rate (FRR) [35].

The fuzzy vault scheme has so far been primarily applied to biometric authentication, such as fingerprints and iris images [36–38]. Fuzzy vault scheme is not specific to sensor networks but serves as a significant support to solve the problem of securing biosensor networks. Minhthang gave a comparative study on fuzzy vault [35]. The experiment results show that fuzzy vault scheme is suitable for securing a fuzzy key. The performance of fuzzy vault system is dependent on an error-correction code, so the specification of the error-correction code makes the design rather inflexible. Fuzzy vault is used by Agrafioti to secure the key generation between the biosensors in the BAN [7], but the computational complexity is high.

Fuzzy vault system is also used in PKSA, a scheme for authenticated pairwise key agreement between two nodes in BANs [6]. PKSA can solve the susceptivity of synchronization and feature reordering issues in [34]. The session key between two nodes is locked by using physiological signal features and fuzzy-vault cryptographic primitive and is unlocked by the receiver according to the physiological signal features measured at the other end. The key is encoded in a polynomial, which must be reconstructed based on a set of correct points to unlock the key. The polynomial degree is linear with the key length, because the key insists of the coefficients of the polynomial. If the key is too short, it is easy to guess by attackers. If the key is too long, it will take the receiver node more cost to compute the polynomial because of the presence of chaff points.

Similar to fuzzy vault, Biometric Encryption technique can be used to keep the biometrics privacy and generate a cryptographic key from biometrics [39]. Compared with fuzzy vault, the chaff points are not necessary to transmit, so the limited bandwidth in the BAN can be saved. Based on Biometric Encryption, we have designed an intradomain mutual authentication and key establishment protocol scheme [9] and an interdomain mutual authentication and key establishment protocol scheme for pervasive computing [40].

3. Preliminaries

In this section, Biometric Encryption technique will be introduced in brief.

Compared with the two classical personal authentication approaches, knowledge based approach and token based approach, Biometrics can represent the uniqueness of a user through electronic examinations of his or her physiological characteristics such as iris, fingerprint, or face and/or through behavioral characteristics. Conventional biometric identification typically consists of an enrollment stage and a verification stage. During the enrollment stage, a user's biometric template is gathered and stored in the plaintext. During the verification stage, the user's biometrics sampled on the spot is matched against the stored biometric template to verify his or her identity. If the stored biometric template of a user is compromised, there could be severe consequences for the user because the biometric template lacks revocation mechanisms.

With the proliferation of information exchange across the internet and the storage of sensitive data, cryptography has been an important technique to achieve the data confidentiality. Cryptographic algorithms are available to secure the information. Cryptographic algorithms are divided into symmetric algorithms and public-key algorithms. However, regardless of whether a symmetric or a public-key system is deployed, the system security is dependent on the key secrecy. If a key is too short, it will be guessed easily. If a key is strong enough, the large size of a key is difficult to remember. It is infeasible for a user to enter the key each time correctly. The encrypted key can be stored on a computer's hard device, but it must be protected securely.

In order to protect the users' biometric templates and keys, Mytec Technologies Inc proposed Biometric Encryption technique. Accordingly, biometric cryptosystems were originally developed for the purpose of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features [39]. A biometric cryptosystems also have a two-stage process: the enrollment stage and the verification stage [9, 38], as shown in Figure 1. During the enrollment stage, the biometric image is bound with a cryptographic key to create data as Bioscrypt. We refer to it as a key binding biometric cryptosystem. During the verification stage, the biometric image on the spot is combined with the Bioscrypt to recover the key. We refer to it as a key generation biometric cryptosystem.

Bioscrypt does not reveal any information about the key or biometric feature; that is, it is computationally hard to decode the key without any knowledge of the user's biometrics and vice versa. Consequently, Bioscrypt provides an excellent privacy protection. The key itself is completely independent of biometrics and can always be changed or updated. Even if the key is ever compromised, the biometrics cannot be leaked. Moreover, the key can be easily modified. In a conclusion, Biometric Encryption can not only secure a cryptographic key, but also protect the user's biometric template.

4. A Biometric Key Establishment Protocol

4.1. System Model. Our application scenario is shown in Figure 2. The notions used in describing the protocol are listed in Table 1.

Multihop communication in a BAN is most commonly used than a single hop communication in order to consume less power. The multihop structure is extremely suitable for wireless networks, especially appropriate for BAN, because each node does not require more transmitted power. Each

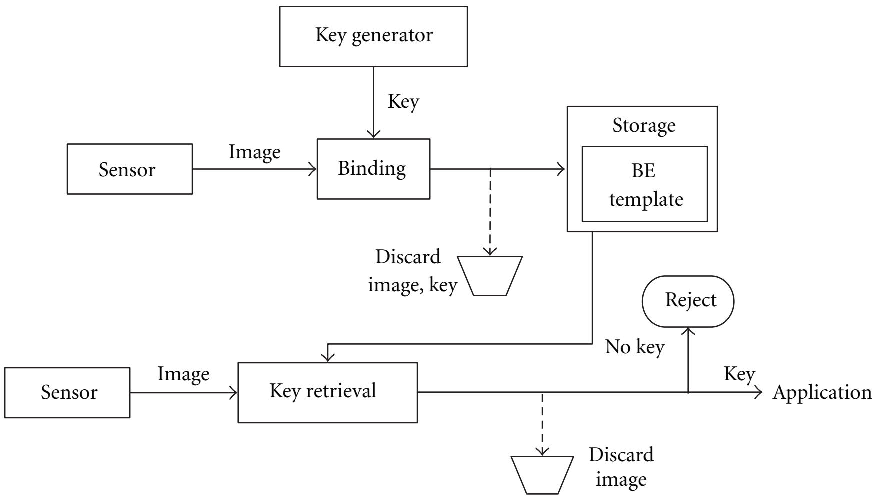


Figure 1: The process of biometric encryption.

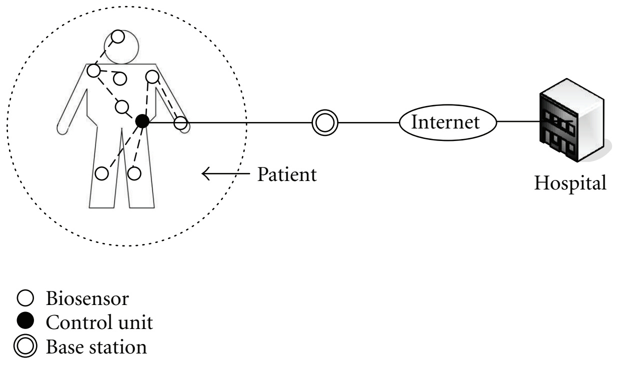


Figure 2: The system model of BANs.

Table 1: Notation table.

Symbols	Meaning
S_j	The jth biosensor
CU	Control unit
h	A secure one-way hash function
r	A random number preallocated to S_j and CU
$\{m\}_K$	A message m is encrypted by the Key K.
Na	A random number
L	The length of a random number
C_H, C_{XOR}	The computation cost of the hash function and the XOR operation
v	The order of polynomial in PSKA

node collects data and transports data to the CU via a multihop network. CU aggregates the data and sends to the remote server. All the nodes except the sink node are called biosensors. In this multihop tree, every biosensor must be authenticated by CU before transmitting the detected data. The purpose of our scheme aims to provide a mutual trust between every biosensor and CU. At the same time, a session key is generated to secure the subsequent traffic. In our experiments, ECG as the biometircs is collected and utilized. Our protocol includes two phases in Figure 3: the key binding stage and key generation stage. During key binding, a session key is bound with ECG to produce Bioscrypt. During key generation, CG can recover the session key with Bioscrypt.

4.2. Key Binding. A random number r is preallocated to CU and S_j. S_j can generate a session key to secure the subsequent traffic between CU and S_j according to the following four steps [9].

(1) S_j collects ECG signals and filters them by wavelet transform. Then, these signals are processed by discrete hashing based on the random number r [41]. Discrete hashing is described as the following.

   (a) The equidistant coordinates of peak are extracted from the filtered signals, marked as (k_{xi}, k_{yi}), $i = 1, \ldots, n$, to form a feature vector ($w_i = [k_{xi} \mid k_{yi}]$). These signals are represented in a vector format, $w \in R^n$, with n denoting the feature length of w.

   (b) Use r to generate m orthonormal pseudorandom vectors, $\{r_i \in R^n \mid i = 1, 2, \ldots, m\}$ and $m \leq n$.

   (c) Compute the inner product $\{t^i \in T \mid i = 1, 2, \ldots, m\}$ between r and w.

   (d) Compute a, m-bit code: $b^i = 0$ if $t^i \leq 0$; $b^i = 1$ if $t^i > 0$.

(2) Reed-Solomon codes are designed to correct the errors (bit differences) within the reference and test signals. Reed-Solomon codes are block-based error-correcting codes with a wide range of applications in digital communications and storage [9].

(3) Biometric template is secured by XOR process as is shown in (1). σ is Bioscrypt:

$$h(b, Na) \oplus \text{Key} = \sigma. \tag{1}$$

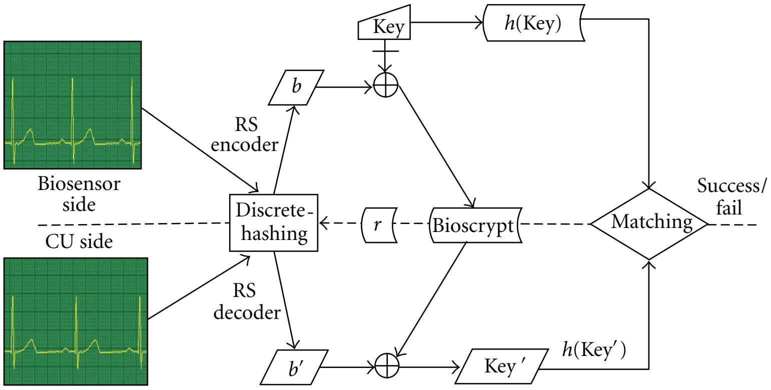


Figure 3: Biometric cryptosystem.

Fourthly, h(Key) as the session key is stored by the sensor while b and the filtered signals are discarded.

4.3. Key Generation. The key generation phase is comprised of the following four steps.

(1) S_j sends the following message: $S_j \rightarrow \text{CU} : \{\sigma, Na\}_{h(r)} || \{r_i\}_{h(\text{Key})}$.

(2) Because r is preallocated to CU and S_j, CU can decrypt $\{\sigma, Na\}_{h(r)}$ to get σ and Na.

(3) CU collects ECG signals filtered by using wavelet transform. These signals are also processed by discrete hashing. Reed-Solomon code is applied too. Key$'$ can be got in (2):

$$\sigma \oplus h(b', Na) = \text{Key}'. \qquad (2)$$

(4) CU sends the following message to S_j : CU $\rightarrow$ S_j: $\{r + 1\}_{h(\text{Key}')}$.

(5) If h(Key) and h(Key$'$) are equal, S_j can decrypt $r + 1$ correctly.

By these five steps, S_j and CU authenticate each other successfully and h(Key) is negotiated as the session key.

5. Correctness Verification

In order to ensure our protocol function correctly, the correctness of the proposed scheme is formally verified based on the SVO logic [42]. SVO logic is based on a unification of four of its logic predecessors and is relatively simple to use. SVO is a logic of belief. The intended use of SVO is to describe the beliefs of trustworthy parties involved in our protocol and the evolution of these beliefs as a consequence of communication while preserving correspondence with the original description of our protocol. In our protocol, both CU and S_j will share a fresh. In this section, the correctness of our proposed scheme is formally verified based on the SVO logic.

The symbols in SVO logic have been introduced in detail [43]. We adopt SVO to prove that both parties ascertain that they are sharing a fresh session key and both are sure that the same belief is held by the other side. Here, both CU and S_j obtain a new key, Key. Therefore, the verification goals are CU believes $S \overset{\text{Key}+}{\longleftrightarrow} \text{CU}$ and S believes $S \overset{\text{Key}+}{\longleftrightarrow} \text{CU}$ Furthermore, they believe that the new key is a fresh session key. So the verification goals are CU believes fresh(Key) and S believes fresh(Key).

First, the messages exchanged should be formalized. Then, premise sets should be figured out previously. We prove the key security from the standpoint of CU, and the process for S_j can be done right in the same way.

The Formalized Messages:

M1: $S \rightarrow \text{CU} : \{\{\sigma, Na\}_{h(r)}, \{r_i\}_{h(\text{Key})}\}$,

M2: $\text{CU} \rightarrow S : \{r_i + 1\}_{h(\text{Key}')}$.

The Premise Sets:

P1: S believes fresh(Na),

P2: S believes $S \overset{r}{\longleftrightarrow} \text{CU}$,

P3: CU believes $\text{CU} \overset{r}{\longleftrightarrow} S$,

P4: CU believes CU has $\{r, u\}$,

P5: S believes S has $\{r, Na, \sigma, \text{Key}\}$,

P6: CU believes $PK_\delta(\text{CU}, u)$,

P7: S believes S controls $\{Na, \text{Key}\}$,

P8: CU believes (CU received $\{\{\sigma, Na\}_{h(r)}, \{r_i\}_{h(\text{Key})}\}$ $\supset$ CU received $\{\{\sigma, \text{fresh}(Na)\}_{h(r)}, \{r_i\}_{h(\text{Key})}\}$),

P9: S believes S received $\{r_i + 1\}_{h(\text{Key}')}$.

The first assumption P1 states that S_j trusts the freshness of its random number. P2 and P3 state that each principal believes their sharing random number is secure. P4 and P5 show what they have. P7 states that the principal controls the generation of the agreement key and its random number. P8 and P9 show the comprehension of CU and S_j. The verification procedures from CU's standpoint are listed as follows.

Certification Process (from CU's Standpoint):

R1: S believes $PK_{\delta}(S, \sigma, Na)$ // by M1, P7,

R2: CU believes CU $\overset{\text{Key}}{\longleftrightarrow}$ S // by R1, P6, Ax5, Net,

R3: CU believes (CU received $\{\sigma, \text{fresh}(Na)\}$) // by P2, P8, Ax7,

R4: CU believes CU $\overset{\text{Key}-}{\longleftrightarrow}$ S // by R2, P3, R3, R1, Ax13, Net,

R5: CU believes $\{S$ says (S sees Key)$\}$ // by M2, Ax1, Ax3, Ax17, MP,

R6: CU believes CU $\overset{\text{Key}+}{\longleftrightarrow}$ S // by R4, R5, Net,

R7: CU believes fresh(Na) // by P8, Ax1, Ax7,

R8: CU believes fresh(Key) // by R7, Ax18.

R6 and R8 show that our protocol has reached the anticipated aim. Therefore, the protocol achieves the goal of establishing a new session key for the two participants.

6. Security and Performance Analysis

In this section, we analyze the security and performance of our protocol.

6.1. Security Analysis

Data Confidentiality. The health information is so sensitive that it is important to prevent the privacy from being accessed by unauthorized entities. In our protocol, every biosensor and CU can generate a unique key to secure the traffic between them, so data confidentiality can be assured and the third party cannot decrypt it.

Data Authenticity. Data Authenticity is the property of the data by which the recipient can verify and trust that the claimed sender is a legitimate one. It is very important for BAN to prevent an illegitimate entity from masquerading as a legal one. In our protocol, the data is encrypted by h(Key) and only legal party can decrypt it.

Data Integrity. Data integrity is a property so that malicious intermediaries cannot modificate the transmission data. If a malicious entity modifies the exchange message, it will be discarded by any receiver as the message digest code cannot match due to the difference.

Mutual Authentication. The proposed scheme provides mutual trust to every bisosensor and CU. The mutual authentication is based on ECG, and a session key will be produced after authentication. The whole process has been proved by SVO.

Multiple/Cancellable/Revocable Key. Biometric Encryption can guarantee that different Bioscrypt can be got by binding the same biometrics with different keys. In our protocol, $\sigma = h(b, na) \oplus \text{Key}$ represents Bioscrypt. Even if one σ is compromised, another σ can be generated soon by binding with a new key. Biometric Encryption makes it possible to change or recompute σ easily. That is, the session key h(Key) may be revoked and replaced by newly generated one calculated from the same biometrics.

Nonlinkability. The session key h(Key) is not relevant to ECG signals and other elements. As discussed in Section 4, the session keys are independent and nonlinkable.

Forward Security. Forward Secrecy guarantees that a passive adversary who knows a contiguous subset of old session keys cannot discover subsequent session keys. In our scheme, the session key h(Key) is produced randomly by the biosensor and bound with the ECG. Thus, an adversary will have no idea of the old session keys because of the non-linkability between the session keys.

Backward Security. Backward Secrecy guarantees that a passive adversary who knows a contiguous subset of session keys cannot discover preceding the session keys. Because the session key is unlinkable, our scheme can achieve backward secrecy.

Replay Attack/Data Freshness. In order to prevent the replay attack, some time stamp or random numbers can be filled into the message to provide data freshness.

Online/Offline Guessing Attack. It is clear that a passive eavesdropper would not be able to compute the shared session key, unless he knows both the ECG signal and the random number.

The comparisons on the security features among our previous work ESKE [10], PSKA [6], and our protocol are shown in Table 2. In PSKA and ESKE, fuzzy vault scheme is adopted and the real points and fuzzy points are transferred to the receiver in plaintext. Therefore, data confidentiality, integrity, and authenticity cannot be ensured. Biometric Encryption can provide multiple, cancellable or revocable keys and non-linkability, while fuzzy vault scheme does not have this feature. Only our protocol is verified by SVO, while other works have not been proven. The table shows that our protocol can provide better security.

6.2. Performance Analysis. We evaluate our protocol using ECG physiological signal, because ECG has been found to specifically exhibit desirable characteristics for BAN applications [33]. There are existing sensor devices for medical applications, manufactured with reasonable costs, that can record these interpulse interval sequences. In our experiment, a QT database is used [44, 45], which consists of 549 holter recordings from 294 persons. These signals are sampled at 1 KHz with 16-bit resolution and over 100 fifteen-minute two-lead ECG recordings. There are onset, peak, and end markers for P, QRS, T, and U waves from 30 to 50 selected beats in each recording. The experiment platform is Matlab. In our experiments, ECG signals are processed by the wave

Table 2: Comparisons on protocol security.

Security features	PKSA [6]	ESKE [10]	Our protocol
Data confidentiality	N	N	Y
Data integrity/authenticity	N	N	Y
Mutual authentication	Y	Y	Y
Multiple/cancellable/ revocable key	N	N	Y
Nonlinkability	N	N	Y
Forward security	Y	N	Y
Backward security	Y	N	Y
Replay attack/data Freshness	Y	Y	Y
Online/offline guessing attack	Y	Y	Y
Correctness verification	N	N	Y

transform. Wavelet coefficients of different scales can be calculated by multilayer wavelet decomposition of ECG, which can remove the noise correlation coefficient and retain the useful signal components. Moreover, different rhythms have different frequencies, so multiresolution analysis separate the frequencies.

6.2.1. Distinctiveness of h(Key). An important requirement is that the physiological signals can distinguish people, which ensures that the session key $h(\text{Key})$ cannot be unlocked by the sensors of another person. Therefore, the physiological signals for sensors on the same subject must be clearly distinctive from those on the different subjects. FRR and FAR are used to measure the authentication accuracy. FRR is the frequency with which a genuine user is not correctly recognized and hence denied access. FAR is the frequency with which an impostor is accepted as a genuine user. If a system can accept all the ECG of right people, it will have a desirably low FRR. If a system cannot reject all the wrong people, it will have a higher FAR.

In Figure 4, we compare the FAR between our scheme and our previous work [10]. It shows that our scheme can achieve more lower FAR.

6.2.2. Robustness of h(Key). Because of the person's uniqueness, it is extremely difficult to steal and use other people ECG and it is equally difficult for an individual to mimic someone else's heart signals as they are the outcome of a combination of several sympathetic and parasympathetic factors of the human body. Thus, the session key $h(\text{Key})$ is robust and antiattack. When the key length is 128, 64, or 32 bits, the results in Figure 5 show that these keys are distinct for different subjects or the same subject at different time. The results also show that the session keys are nonlinkability. Even if an attacker is able to reveal one key, he cannot guess other keys because the key does not carry extra information to reveal other encryption keys. From Figure 5, we also can see that the entropy of the keys ranges from 0.586 to 1, which means that our protocol possesses more uncertainty and a higher privacy level.

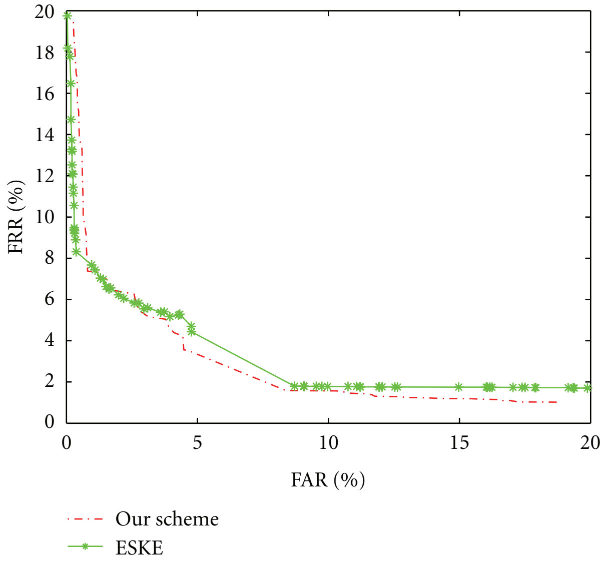


Figure 4: FAR versus FRR.

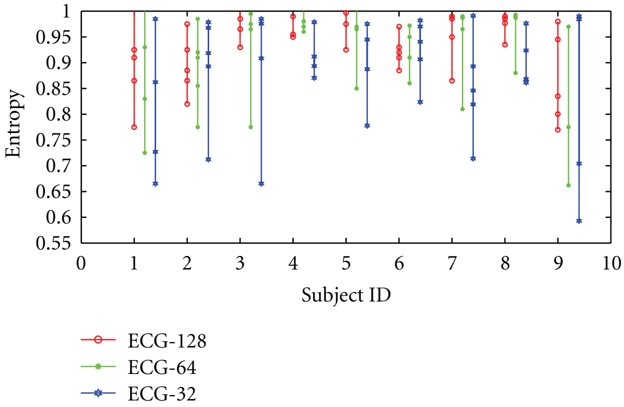


Figure 5: The entropy of different length keys.

6.2.3. Computation and Storage Overhead. Every biosensor must store some fix and temporary parameters whose unit is byte or bit as shown in Table 3. In ESKE, a biosensor needs to store the session key and the public key of CU as fix parameters and some random numbers as temporary parameters. In PSKA, a biosensor should need the polynomial coefficients as the session key and its own identifier as the fix parameters, and some other temporary parameters. In our protocol, a biosensor stores the session key and the random r as fix parameters, w, t, b, and Na as temporary parameters.

The computation analysis in Table 4 focuses on encryptions and decryptions of asymmetric or symmetric algorithms, hash operations, XOR operation, calculated polynomial, and inner product. In ESKE, only a hash operation, a XOR operation, two public-key encryption operation in sending messages, a symmetric encryption operation to verify key, and $n+1$ times computation of distances between

Table 3: Storage overhead.

	Fix storage	Temporary storage
ESKE [10]	L	$(m+nm+1)L$
PSKA [6]	$(v+1)L+L$	$(2n+2m+1)L$
Our protocol	$mn+L$	$n+2m+2L$

Table 4: Computation overhead.

	ESKE [10]	PSKA [6]	Ours protocol
Hash operation	1	1	1
XOR operation	1	0	1
Asymmetric operation	2	1	0
Symmetric operation	1	1	2
Polynomial operation	0	$m+n$	0
Inner product operation	$n+1$	0	m

the vectors are needed. In PSKA, a hash operation to compute the message digest code, $n+m$ times computation of polynomial, and a public-key encryption operation in sending messages are needed. In our scheme, a hash operation and a XOR operation are needed to compute Bioscrypt; two symmetric operations and m times of inner product are needed.

From Tables 3 and 4, we can see that our scheme shows higher superior in storage and computation overhead compared with ESKE and PSKA. Therefore, our new scheme significantly reduces computational and storage overhead.

7. Conclusion

In this paper, we have presented a biometic key establishment scheme to protect the confidentiality and integrity of the sensitive health information. Our protocol attempts to solve the problem of security and privacy in BANs. It also aims to securely and efficiently generating and distributing the session key between a biosensor and CU.

Our protocol is based on Biometric Encryption. The primary contributions of this paper are summarized as follows.

(1) ECG is used to bind and generate a session key, which can guarantees that the key is long, random, distinctive, and temporal variant.

(2) Biometric Encryption technique is applied to derive multiple and nonlinkable keys from the same ECG signal.

(3) The correctness of the proposed scheme is formally verified based on SVO logic. Security and performance analysis show that our protocol cannot only guarantee data confidentiality, authenticity, and integrity, but also resist malicious attacks efficiently.

In the future work, we will continue to optimize our algorithm to balance safety and security.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China under Grants no. 60703101 and no. 60903153 and the Fundamental Research Funds for the Central Universities.

References

[1] E. Jovanov, A. Milenkovic, C. Otto, and P. C. de Groen, “A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation,” *Journal of NeuroEngineering and Rehabilitation*, vol. 2, no. 1, 2005.

[2] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, “Security and privacy for implantable medical devices,” *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30–39, 2008.

[3] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones et al., “Sensor networks for emergency response: challenges and opportunities,” *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16–23, 2004.

[4] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, “A biometrics based security solution for encryption and authentication in tele-healthcare systems,” in *Proceedings of the 2nd International Symposium on Applied Sciences in Biomedical and Communication Technologies, (ISABEL ’09)*, pp. 1–4, Bratislava, Slovakia, November 2009.

[5] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, “Security issues on wireless body area network for remote healthcare monitoring,” in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, (SUTC ’10)*, pp. 327–332, Newport Beach, Calif, USA, June 2010.

[6] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, “PSKA: usable and secure key agreement scheme for body area networks,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2010.

[7] F. Agrafioti, F. M. Bui, and D. Hatzinakos, “On supporting anonymity in a BAN biometric framework,” in *Proceedings of the16th International Conference on Digital Signal Processing, (DSP ’09)*, pp. 787–792, Santorini, Greece, July 2009.

[8] A. Adler, “Vulnerabilities in Biometric Encryption Systems,” *Lecture Notes in Computer Science*, vol. 3546, no. 1, pp. 211–228, 2005.

[9] L. Yao, X. W. Kong, G. Wu, Q. N. Fan, and C. Lin, “A privacy-preserving authentication scheme using biometrics for pervasive computing environments,” *Journal of Electronics*, vol. 27, no. 1, pp. 68–78, 2010.

[10] L. Yao, B. Liu, K. Yao, G. W. Wu, and J. Wang, “An ecg-based signal key establishment protocol in body area network,” in *Proceedings of the Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, pp. 233–238, October 2010.

[11] J. Woods, “The five styles of sensory applications,” Gartner Research, 2006.

[12] M. M. M. B. Amer and M. I. M. Izraiq, “System with intelligent cable-less transducers for monitoring and analyzing biosignals,” *European Patent Application*, 2007.

[13] W. R. Jih, S. Y. Cheng, J. Y. J. Hsu, and T. M. Tsai, “Context-aware access control in pervasive healthcare,” in *Proceedings of the EEE’05 Workshop: Mobility, Agents, and Mobile Services (MAM)*, Hong Kong, China, March 2005.

[14] K. Adam, B. Price, M. Richards, and B. Nuseibeh, “A privacy preference model for pervasive computing,” in *Proceedings of the Euro mGov 2005*, Brighton, UK, July 2005.

[15] G. Zhang and M. Parashar, "Context-aware dynamic access control for pervasive applications," in *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference, (CNDS '04)*, Western MultiConference (WMC), San Diego, Calif, USA, January 2004.

[16] D. Jea, I. S. Yap, and M. B. Srivastava, "Context-aware access to public shared devices," in *Proceedings of the HealthNet 2007: The First International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments*, Puerto Rico, USA, June 2007.

[17] M. Tentori, J. Favela, and M. D. Rodriguez, "Privacy-aware autonomous agents for pervasive healthcare," *IEEE Intelligent Systems*, vol. 21, no. 6, pp. 55–62, 2006.

[18] M. Haque and S. I. Ahamed, "Security in pervasive computing: current status and open issues," *International Journal of Network Security*, vol. 3, no. 3, pp. 203–214, 2006.

[19] S. C. Shin, C. Y. Ryu, J. H. Kang et al., "Realization of an e-health system to perceive emergency situations," in *Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, (EMBC '04)*, vol. 2, pp. 3309–3312, San Francisco, Calif, USA, September 2004.

[20] R. Bose, A. Helal, S. Lim, and V. S. Sivakumar, "Virtual sensors for service oriented intelligent environments," in *Proceedings of the 3rd IASTED International Conference on Advances in Computer Science and Technology, (ACST '07)*, Phuket, Thailand, April 2007.

[21] S. Lim, S. Kang, and J. Sohn, "Modeling multiple agent based cryptographic key recovery protocol," in *Proceedings of the 19th Annual Computer Security Applications Conference, (ACSAC '03)*, pp. 119–128, Las Vegas, Nev, USA, December 2003.

[22] M. Mana, M. Feham, and B. A. Bensaber, "Trust key management scheme for wireless body area networks," *International Journal of Network Security*, vol. 12, no. 2, pp. 61–69, 2011.

[23] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, (SenSys '04)*, pp. 162–175, Baltimore, Md, USA, November 2004.

[24] M. Guennoun, M. Zandi, and K. El-Khatib, "On the use of biometrics to secure wireless biosensor networks," in *Proceedings of the 3rd International Conference on Information and Communication Technologies: From Theory to Applications, (ICTTA '08)*, pp. 1–5, Damascus, Syria, April 2008.

[25] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: testing the limits of elliptic curve cryptography in sensor networks," in *Proceedings of the 5th European Conference on Wireless Sensor Networks*, pp. 305–320, Bologna, Italy, February 2008.

[26] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in *Proceedings of the International Workshop on Wireless Sensor Networks and Applications, (WSNA '03)*, pp. 141–150, San Diego, Calif, USA, September 2003.

[27] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in *Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, (SECON '04)*, Santa Clara, Calif USA, October 2004.

[28] F. Adelstein, S. K. S. Gupta, G. G. Richard, and L. Schwiebert, *Fundamentals of Mobile and Pervasive Computing*, McGraw-Hill, New York, NY, USA, 2005.

[29] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security, (CCS '03)*, vol. 2, pp. 500–528, Washington, DC, USA, October 2003.

[30] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proceedings of the International Conference on Parallel Processing Workshops*, pp. 432–439, Kaohsiung, Taiwan, October 2003.

[31] S. M. K.-U.-R. Raazi, H. Lee, S. Lee, and Y.-K. Lee, "Bari+: a biometric based distributed key management approach for wireless body area networks," *Sensors*, vol. 10, no. 4, pp. 3911–3933, 2010.

[32] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[33] S. D. Bao, C. C. Y. Poon, L. F. Shen, and Y. T. Zhang, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 6, pp. 772–779, 2008.

[34] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 529879, 16 pages, 2008.

[35] F. M. Bui and D. Hatzinakos, "Secure methods for fuzzy key binding in biometric authentication applications," in *Proceedings of the 42nd Asilomar Conference on Signals, Systems and Computers, (ASILOMAR '08)*, pp. 1363–1367, Pacific Grove, Calif, USA, October 2008.

[36] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Proceedings of the Audio- and Video-Based Biometric Person Authentication (AVBPA '05)*, vol. 3546, pp. 310–319, Hilton Rye Town, NY, USA, July 2005.

[37] E. S. Reddy and I. R. Babu, "Authentication using fuzzy vault based on iris textures," in *Proceedings of the 2nd Asia International Conference on Modelling and Simulation, (AMS '08)*, pp. 361–368, Kuala Lumpur, Malaysia, May 2008.

[38] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the International Symposium on Information Theory*, vol. 38, pp. 237–257, Seattle, Wash, USA, July 2006.

[39] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 579416, 17 pages, 2008.

[40] L. Yao, L. Wang, X. W. Kong, G. W. Wu, and F. Xia, "An inter-domain authentication scheme for pervasive computing environment," *Computers and Mathematics with Applications*, vol. 60, no. 2, pp. 234–244, 2010.

[41] A. T. B. Jin, D. C. L. Ngo, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[42] C. Meadows, "Formal methods for cryptographic protocol analysis: emerging issues and trends," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 1, pp. 44–54, 2003.

[43] P. Syverson and I. Cervesato, "The logic of authentication protocols," *Foundations of Security Analysis and Design*, vol. 2171, pp. 63–136, 2001.

[44] P. Laguna, R. G. Mark, A. Goldberg, and G. B. Moody, "Database for evaluation of algorithms for measurement of QT and other waveform intervals in the ECG," *Computers in Cardiology*, vol. 27, pp. 673–676, 1997.

[45] A. L. Goldberger, L. A. N. Amaral, L. Glass et al., "PhysioBank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. 215–220, 2000.

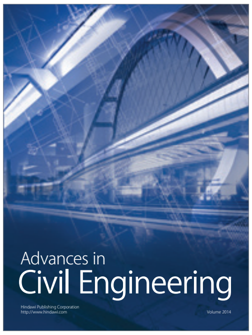
Journal of
Engineering

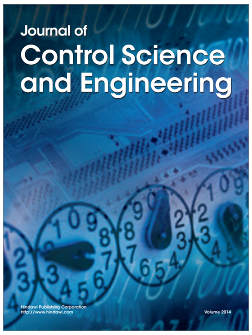
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

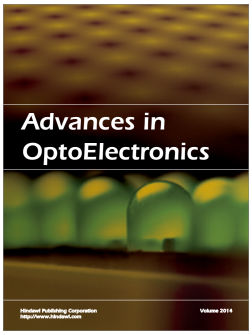
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

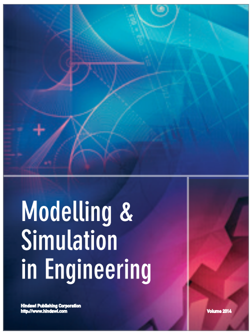
Journal of
Robotics

Journal of
Electrical and Computer Engineering

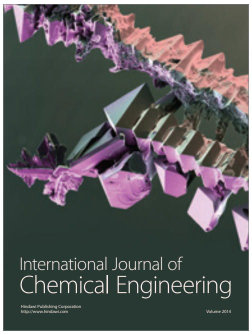

Advances in
OptoElectronics

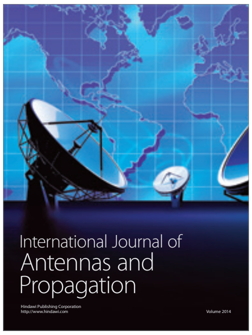
VLSI Design

International Journal of
Navigation and Observation

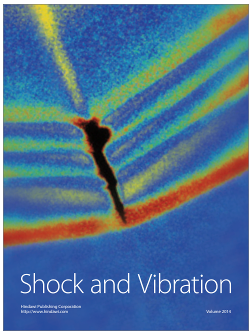

Modelling &
Simulation
in Engineering

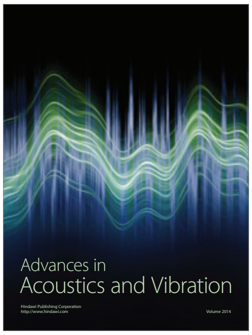
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration