BDK: Secure and Efficient Biometric based Deterministic Key Agreement in Wireless Body Area Networks*

Jun Zhou, Zhenfu Cao, Xiaolei Dong
Department of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai, 200240, China
zhoujun_tdt@sjtu.edu.cn, {zfcao, dong-xl}@cs.sjtu.edu.cn

ABSTRACT

Wireless body area networks (WBANs) have been widely adopted to efficiently monitor patients' realtime health condition for medical treatment and emergency handling. Key agreement with the properties of plug-n-play and transparency for WBANs is indispensably required to establish the secure communication channels among body sensors. Existing works mainly focus on exploiting the technique of fuzzy vault to allow body sensors deployed on the same human body can securely establish a pairwise key at a high probability, where the authentic extracted biometric characteristics and the chaff points are indistinguishable from the adversaries' view except a brute attack. However, it simultaneously brings about a large body of additional overhead for dealing with the redundancy. In this paper, a secure and efficient biometric based deterministic key agreement for WBANs is proposed by exploiting the overlap between the biometric characteristics collected by body sensors. The pairwise keys for WBANs can be definitely negotiated by the interactions between body sensors embedded in the same human body. The security depends on the underlying one way trapdoor function rather than the coffer/vault size. Extensive simulations and comparisons illustrate the efficiency and practicability of our proposed construction BDK and the advantages over the state-of-the-art with stronger resilience, less storage, computational and communication overhead.

Keywords

Wireless body area networks, biometric based deterministic key agreement, security and privacy, efficiency

1. INTRODUCTION

Wireless body area network (WBAN) is a potential technology for efficiently monitoring, collecting and transmitting the patients' realtime health information to the healthcare provider to obtain timely and precise medical treatment from the professional physicians. Its substantial development owes to the rapid progresses in the fields of wireless sensor networks and biometric computing [1] [2]. It generally comprises a set of body sensors embedded on, in or around the patients' human bodies that monitor the biometric characteristics such as the heart beating, body temperature and blood pressure, and cooperate to aggregate the raw health data to the patients' hand-held data sinks, dramatically alleviating the risks patients took on the way between their residences and hospitals and greatly enhancing the medical healthcare quality.

However, WBANs are confronted with the unprecedented security and privacy challenges since the patient health information is highly related to the patients' privacy and their leakage would significantly impedes the profound adoption of the WBANs as a cornerstone of the whole e-healthcare system. Specifically speaking, wireless communication in WBANs is vulnerable to kinds of sophisticated attacks such as eavesdropping and modification, which would lead to serious discrimination and wrong diagnosis against the patients. Therefore, how to secure the wireless communication in WBANs critically requires our solutions.

Key agreement provides an efficient way to guarantee the data confidentiality and the authentication among the body sensors. However, the traditional pairwise key establishment [4,7] in sensor networks cannot be directly applied to WBANs for its heavy predistribution cost. To adapt to the resource-constrained property of WBANs and support the quick responses from the healthcare providers especially in the emergency cases, it is required to make the underlying WBAN possess the properties of plug-n-play and transparency in essence. Recently, a series of physiological signal based key agreement schemes [3,5,6,9-11] for WBANs have been proposed by exploiting the matching biometric signals sampled on different body sensors deployed on the same patient. They not only secure the communications in WBANs, but considerably reduce the latency brought about by the re-initialization and body sensor deploy adaption due to the patient's dynamic health conditions. However, the existing works mainly focused on exploiting the technique of fuzzy vault [8] and its variations to realize the key agreement, which leads to significant storage, computational and communication overhead on body sensors. Both the probability of successful key agreement and its security depend on the coffer/vault size (i.e. the number of characteristic points and chaff points) rather than polynomially-computational hard problems utilized in cryptography. In this paper, a secure and efficient biometric-based deterministic key agreement scheme in WBANs is proposed.

The proposed secure and efficient biometric-based deterministic key agreement scheme BDK mainly comprises the following phases. (1) Each body sensor respectively collects specific biometric characteristics from different locations from the same patient human body. (2) After being processed, the biometric characteristics

*

BODYNETS 2013, September 30-October 02, Boston, United States

DOI 10.4108/icst.bodynets.2013.253731

are additively blinded by the sponsoring sensor and transmitted to the reacting one. (3) The latter performs the privacy-preserving comparison between the biometrics collected by two entities and sends the result to the sponsoring node. (4) The sponsoring body sensor deciphers the comparing result and establishes the pairwise key with the other party if the number of shared biometric characteristics exceeds the specific threshold pre-determined by the W-BAN system. The main contributions are described as follows.

(1) A secure and efficient biometric-based deterministic key agreement scheme BDK in WBANs is proposed. It realizes the definite and authenticated pairwise key agreement among body sensors once the number of shared biometrics exceeds a certain threshold.

(2) The security of the proposed BDK relies on the computational hardness of reversing underlying one-way trapdoor functions rather than the number of extracted biometric characteristics and the chaff points that are exploited to prevent the adversary to distinguish the authentically extracted biometrics from the redundancy.

(3) The performance analysis illustrates the efficiency and practicability of our proposed BDK w.r.t. significantly reduced storage, computational and communication overhead by avoiding introducing chaff points.

The remainder of this paper is organized as follows. The related work is introduced in Sec. 2, followed by the network architecture and the security model in Sec. 3. In Sec. 4, the proposed secure and efficient biometric based deterministic key agreement scheme BDK in WBANs is presented. Then, security analysis and performance evaluations are respectively given in Sec. 5 and Sec. 6. Finally, we conclude our paper in Sec. 7.

2. RELATED WORK

A series of research [2,3,5,6,9-11] have focused on the security and privacy issues w.r.t. WBANs, which mainly deal with the data encryption, pairwise key agreement between body sensors and the access control to patient health information collected by WBANs. Additionally, key agreement to establish the secure communication channel between body sensors serves as the cornerstone for other two security requirements.

The biometric based key agreement in WBANs is firstly proposed by S. Cherukuri et al. [2]. Two body sensors deployed at different parts of the same human body respectively collect the same kind of biometric characteristics to establish the shared pairwise key by utilizing the simple error correction code to adapt the biometrics generated by different body sensors. Afterwards, S. D. Bao et al. introduced the Inter-Pulse-Interval (IPI) to negotiate the session key in WBANs based on the assumption that the hamming distance of the pairwise keys generated from the same patient is significantly lower than that generated from different patients [3]. However, K. K. Venkatasubramanian et al. indicated by experiment that the hamming distances of the underlying IPI produced from the same human body and different human bodies are not distinguished enough to generate the pairwise keys w.r.t. one specific patient and prevent the encrypted private patient health information from exposure to other unauthorized patients or adversaries [9]. The utilized error correction code cannot solve the problem well due to the translational and rotational errors introduced when the biometric IPI is encoded into binary strings.

On the other hand, the technique of fuzzy fault [8] is widely adopted in key agreement in WBANs [9,10]. A set of chaff points are introduced by one body sensor to anonymize the authentic points derived from the biometric characteristics collected from the human body and together to constitute the vault. The other body sensor can successfully establish the pairwise key if and only if the size of the intersection between the vault and his own collected biometrics meets a certain threshold. However, K. K. Venkatasubramanian et al. claimed that it is likely for the adversary to guess the authentic points from the vault transmitted in its plaintext and recover the original polynomial selected by the sponsoring body sensor. PSKA [9] utilized the physiological signals photoplethysmogram (PPG) and electrocardiogram (EKG) to allow neighboring body sensors within the same WBAN to agree a symmetric key in an authenticated manner. OPFKA [10] devised a ordered-physiological-feature-based key agreement based on the observation that the secret biometric features generated by a body sensor is ordered and only the body sensor that generates it can be aware of this order. Both constructions are devised by using the fuzzy vault (or its variation coffer) and claimed to enhance its security level. However, the technique of fuzzy vault essentially throws the key agreement for WBANs into a dilemma that if the size of the vault becomes larger by introducing more chaff points, the difficulty of the adversary to distinguish the authentic points from the chaff ones dramatically increases; but the collisions between the biometric characteristics collected by the reacting body sensor and the chaff points added by the sponsoring sensor, namely the false rejection rate, also increase simultaneously. Therefore, how to devise a secure and efficient biometric based deterministic key agreement for WBANs is a challenging open problem.

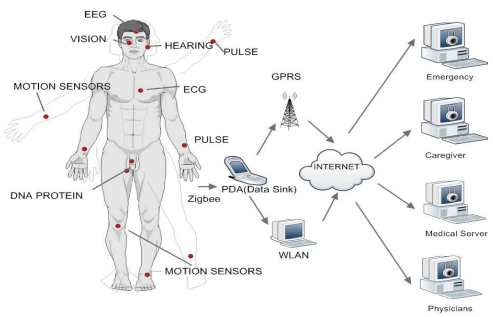

Figure 1: Architecture of WBANs

In this paper, a secure and efficient biometric based deterministic key agreement BDK for WBANs is proposed. Special additive and multiplicative blinding techniques are respectively exploited by each pair of body sensors to negotiate the pairwise key even without the need to recover the intersection between two biometric sets if and only if the size of the intersection exceeds a certain threshold. Additionally, avoiding chaff points significantly reduces the storage, computational and communication overhead for the resource-constrained body sensors, and allows the key agreement to be definite (without false rejection). Finally, the enhanced security depends on the computational difficulty in reversing the underlying one way trapdoor functions, instead of the size of the vault.

3. NETWORK ARCHITECTURE AND SECURITY MODEL

WBAN is generally deployed on, in or around the patient human bodies to monitor and collect the realtime biometric characteristics and the environmental parameters to cooperatively contribute to the patient health information. All these information is aggregated to the patient's hand-held data sink at a regular interval and further transmitted to the healthcare provider for efficient medical treatment. Fig. 1 illustrates the architecture of WBANs. It is assumed that the body sensors possess the ability to monitor appropriate biometric characteristics and only the body sensors physically attached to the human body can perform the feature collection task. We also assume that all the body sensors cannot be compromised without detection and the adversary can sponsor eavesdropping, spoofing or interjection attacks. The adversary also tries to achieve the established pairwise key from other patient's body if the selected biometric characteristic does not have enough uniqueness for each person. Specifically speaking, the security of our proposed BDK depends on the computationally hardness of the underlying one way trapdoor function. The chosen plaintext attack (CPA) security can be formally defined as follows.

Initialization Phase: On input 1^k, the adversary queries a key generation oracle. The key generation oracle $\mathcal{O}^{KGen}$ computes $(f, f^{-1}, d) \leftarrow_R Initilization(1^k)$ and gives back PK_f to $\mathcal{A}$ as the response. d refers to the underlying ring $\mathbb{R}_p$, where p is the big prime of the length k.
Query Phase: The adversary submits a message $m \in \mathbb{R}_p$ to encryption oracle $\mathcal{O}^E$, and the simulator gives back the ciphertext $c \leftarrow Encryption(1^k, PK_f, m)$ as the response. It is noted that since the underlying one way trapdoor function is publicized, this operation can also be performed by the adversary himself.
Challenge Phase: The adversary submits two messages $m_0, m_1 \in \mathbb{R}_p$ to the simulator, where $|m_0| = |m_1| = k$. On input m_0, m_1, the simulator flips a coin and randomly selects $\beta \in_R \{0, 1\}$ and outputs $c^* \leftarrow_R Encryption(1^k, PK_f, m_\beta)$ as the challenge ciphertext to the adversary.
Guess Phase: The adversary outputs $\beta' \in \{0, 1\}$. If $\beta' = \beta$, we mean the adversary has successfully defeated the proposed BDK.

Definition 1. Assume the CPA advantage of the adversary $\mathcal{A}$ against the proposed BDK at the security parameter k to be $AdvCPA_{\mathcal{A}(t,n(k))}(k) = |Pr[\beta' = \beta] - \frac{1}{2}|$ in the attack game described above, where $n(k)$ is the size of the biometric characteristic vector. Then, we say our proposed BDK is secure against chosen plaintext attack if and only if for all probabilistic and polynomially-bounded adversary $\mathcal{A}$ running in time at most t,

$$AdvCPA_{\mathcal{A}(t,n(k))}(k) \leq \epsilon(k),$$

where $\epsilon(k)$ is negligible in k.

4. THE PROPOSED BDK

In this section, a secure and efficient biometric-based deterministic key agreement BDK for WBANs is proposed. It mainly comprises the following five phases, namely feature generation, feature blinding, feature exchange, feature matching and feature acknowledgement. Different from the existing works, the proposed BDK allows pairs of body sensors to deterministically negotiate a pairwise key if there exists a set of shared biometric characteristics, the size of which is no less than the predefined threshold selected by the system. Additionally, it is not required for each body sensor to recover the shared biometrics themselves to decide the intersection, significantly reducing the computational cost of key agreement in WBANs. Finally, since the proposed deterministic BDK avoids introducing chaff points widely adopted in the state-of-the-art, the false rejection rate (FRR), the storage, computational and communication overhead can be all dramatically optimized for resource-constrained body sensors. The details of the proposed BDK are described as follows.

Feature Generation: For comparison convenience, the feature generation steps resemble the associated operations in PSKA [9] and OPFKA [10]. Firstly, both body sensors sample the biometric-based characteristics in a loosely synchronized way with a specific sampling rate during a fixed time period. Then, these collected samples are divided into multiple windows, on each of which the Fast Fourier Transformation (FFT) is performed and the FFT coefficients are passed through a selected peak detection function with the form $< K_x^i, K_y^i >$ as its output. K_x^i, K_y^i respectively refer to the FFT point where the peak is observed as the x-axis value and the corresponding FFT coefficient as the y-axis value, and i is the index of the peak. Then, each pair of $< K_x^i, K_y^i >$ is quantized and transformed into a binary string with the form $[K_x^i | K_y^i]$ as a feature. After that, a hash function $H_0 : \{0, 1\}^* \rightarrow \mathbb{R}_p$ where p is a big prime is selected and performed on $[K_x^i | K_y^i]$ to derive $[k_x^i | k_y^i]$. The parameters utilized in feature generation are carefully selected according to the kinds of biometric characteristics collected by body sensors (i.e. we use IPI signals in our proposed BDK). FFT peaks are chosen as features for its expression simplicity and precision, therefore, they can be exploited to distinguish the biometric features sampled in the same WBAN or different WBANs from different patients and become a natural tool for body sensor authentication and key agreement. Finally, the biometric features monitored by body sensors A and B can be respectively represented by two vectors with the size of n (i.e. the number of indexes where the peaks are observed): $\vec{a} = (a_1, a_2, \cdots, a_n)$ and $\vec{b} = (b_1, b_2, \cdots, b_n)$ where $a_i = [k_x^{A,i} | k_y^{A,i}], b_i = [k_x^{B,i} | k_y^{B,i}]$.

Feature Blinding and Exchange: In this step, both the sponsoring body sensor B and the reacting body sensor A respectively blind their processed biometric characteristics using different kinds of encryptions. The purpose is to facilitate each party to discover the indexes of the shared biometric characteristics and prevent the adversary from extracting the private health information of the patient. Firstly, body sensor B randomly selects $R_B \in_R \mathbb{R}_p$, computes

$$\begin{aligned} &\vec{b}^{bld} = (b_1 + R_B, b_2 + R_B^2, \cdots, b_n + R_B^n), \\ &B_0 = MAC(ID_B \parallel ID_A \parallel \vec{b}^{bld}) \\ &= MAC(ID_B \parallel ID_A \parallel b_1 + R_B \parallel \cdots \parallel b_n + R_B^n), \end{aligned} \quad (1)$$

where MAC is the message authentication code and transmits $(ID_B, ID_A, \vec{b}^{bld}, B_0, N_0)$ to body sensor A where $N_0 \in_R \mathbb{R}_p$ is the random nonce.

After checking whether $B_0 = MAC(ID_B \parallel ID_A \parallel \vec{b}^{bld})$, body sensor A randomly selects $R_A \in_R \mathbb{R}_p$, computes

$$\begin{aligned} \vec{a}^{bld} &= (R_A(b_1^{bld} - a_1), R_A^2(b_2^{bld} - a_2), \cdots, R_A^n(b_n^{bld} - a_n)), \\ A_0 &= MAC(ID_A \parallel ID_B \parallel \vec{a}^{bld}) = MAC(ID_A \parallel ID_B \parallel \\ &\quad R_A(b_1^{bld} - a_1) \parallel \cdots \parallel R_A^n(b_n^{bld} - a_n)), \end{aligned} \quad (2)$$

where b_i^{bld} refers to the i-th component of sensor B's blinded biometric vector $\vec{b}^{bld}$ and transmits $(ID_A, ID_B, \vec{a}^{bld}, A_0)$ back to body sensor B.

Finally, after checking whether $A_0 = MAC(ID_A \parallel ID_B \parallel$

$\vec{a}^{bld}$), body sensor B computes

$$R_{A,i} = \frac{a_i^{bld}}{R_B^i}, \quad (3)$$

where a_i^{bld} refers to the i-th component of sensor A's blinded biometric vector $\vec{a}^{bld}$ and R_B is the random number selected by B. It is noted that if there exist shared processed biometric characteristics between body sensors A and B, the following condition that $R_{A,i} = R_A^i$ would be satisfied at the corresponding index i. Therefore, if body sensor B discovers a subset $\{R_{A,i}^{'}\} \subseteq \{R_{A,i}\}(i = 1, 2, \cdots, n)$ satisfies the above-mentioned condition, we would conclude that those elements in $\vec{b}$, the indexes of which are comprised in the set $\{R_{A,i}^{'}\}$, are the shared biometric characteristics between A and itself. In order to compare the equality of the corresponding biometric characteristics, the prime modular p should be selected big enough so that the values of all the processed biometric characteristics satisfy $a_i < p, b_i < p, a_i^{bld} < p, b_i^{bld} < p$. Therefore, the random number $R_A < p$ is also uniquely determined. The matching index discovering process can be detailed in Algorithm 1.

Algorithm 1 Discovery Algorithm for shared biometric characteristics

Data: There exists a judging set $\{R_{A,i}\}$, from which body sensor B wants to derive a index set of the shared biometric characteristics $IndSet$. All the shared biometric characteristics and their corresponding elements in $R_{A,i}^{'}(i = 1, 2, \cdots, n)$ possess the same indexes. Initially, set $IndSet = \phi$ and T is the pre-defined threshold.

Begin

1: **for** each $R_{A,i}$ **do**
2: Body sensor B derives R_A by computing the i-th root $R_{A,i}^{rt}$ of $R_{A,i}$,
3: Calculates $R_{A,i}^{RT} = \{R_{A,i}^{rt}, (R_{A,i}^{rt})^2, \cdots, (R_{A,i}^{rt})^n\}$,
4: Computes the intersect $R_{A,i}^{IST} = R_{A,i}^{RT} \cap \{R_{A,i}\}$,
5: Computes the cardinality of $R_{A,i}^{IST}$,
6: **if** $|R_{A,i}^{IST}| \geq T$ **then**
7: Adds the corresponding indexes i of the elements in $\{R_{A,i}\}$ that are also located in $R_{A,i}^{IST}$ to $IndSet$;
8: **else**
9: i=i++;
10: **end if**
11: **end for**Outputs $IndSet$.

End

Until now, body sensor B derives the subset $B \subseteq \{b_i\}$, each element of which possesses the index located in $IndSet$ and calculates the pairwise key as $K_{B,A} = H_1(B_1 \parallel \cdots \parallel B_{|IndSet|})$, where $B_i \in B$ are arranged according to the ascending series of their corresponding indexes and H_1 is also a hash function mapping $H_1 : \{0,1\}^* \rightarrow \mathbb{R}_p$.

Feature Matching and Acknowledgement: In this step, body sensor B computes

$$ISTM = MAC(ID_B \parallel ID_A \parallel K_{B,A} \parallel B \parallel IndSet) \quad (4)$$

and sends $(ID_B, ID_A, Indset, ISTM)$ to A. After receiving the message from B, body sensor A derives the subset $A \subseteq \{a_i\}$, each element of which possesses the index located in $IndSet$ and checks whether $|A| \geq T$ holds. If it does, body sensor A calculates the pairwise key as $K_{A,B} = H_1(A_1 \parallel \cdots \parallel A_{|IndSet|})$, and verifies whether

$$ISTM = MAC(ID_B \parallel ID_A \parallel K_{A,B} \parallel A \parallel IndSet) \quad (5)$$

holds. If it does, body sensor A returns $(ID_A, ID_B, MAC(ID_A \parallel ID_B \parallel K_{A,B} \parallel N_0))$ to B. After verification, body sensors B and A use the established pairwise key $K_{B,A}(= K_{A,B})$ to secure the wireless communications between them.

Remark: In the proposed key agreement BDK described above, it is required the biometric characteristics collected from body sensors A and B are perfectly ordering which means there exists only an opportunity for $a_i = b_i$ with the same index i (i.e. it is the same assumption as OPFKA [10] which can be naturally satisfied by the essence of the biometric characteristics). If it is required to perform random permutation on the blinded biometric vectors $\vec{a}^{bld}$ and $\vec{b}^{bld}$ before transmitting to the other party or the underlying biometric characteristics are monitored or collected disorderly, for each element a_i in $\vec{a}$, it is necessary for body sensor A to compute

$$\vec{a}^{bld,'} = (R_A(b_1^{bld} - a_i), R_A^2(b_2^{bld} - a_i), \cdots, R_A^n(b_n^{bld} - a_i)) \quad (6)$$

in the feature blinding phase. Accordingly, B is required to perform $R_{A,i}^{'} = \frac{a_i^{bld,'}}{R_B^j}(j = 1, 2, \cdots, n)$ for each element $a_i^{bld,'}$ in vector $\vec{a}^{bld,'}$. Therefore, both the storage, computational and communication overhead would increase from $O(n)$ to $O(n^2)$.

5. SECURITY ANALYSIS

5.1 Security Proof

In this section, we give the formal security proof for two kinds of data encryptions (additive blinding and multiplicative blinding) exploited by both body sensors to blind their own private health information and prevent exposure from the adversaries. The main idea can be outlined as follows. Firstly, we give the formal security proof resilient to chosen plaintext attack (CPA) w.r.t. the following variations $C_I = (C_1^I, C_{2,1}^I, \cdots, C_{2,n}^I)(I \in \{A, B\})$ of the two encryptions adopted in our construction by introducing a one-way trapdoor function as

$$\begin{aligned} &C_1^B = f(R_B), && C_1^A = f(R_A), \\ &C_{2,1}^B = m_1 + R_B, && C_{2,1}^A = m_1 R_A, \\ &C_{2,2}^B = m_2 + (R_B)^2, && C_{2,2}^B = m_2 (R_A)^2, \\ &\cdots, && \cdots, \\ &C_{2,n}^B = m_n + (R_B)^n, && C_{2,n}^A = m_n (R_A)^n. \end{aligned} \quad (7)$$

Then, it is straightforwardly to deduce our proposed construction BDK at least possesses the CPA security presented above, since if we omitted the one-way trapdoor functions in either encryption form, it would only leak less information about R_B, R_A to the adversary. In the following, we give the formal security proof of the additive blinding and the proof of multiplicative blinding is similar. The details of the security proof are described as follows.

THEOREM 1. *Let $\mathcal{A}$ be a malicious adversary defeating our proposed BDK with a nonnegligible advantage defined as $AdvCPA_{\mathcal{A}(t,n(k))}(k) = \epsilon^{',t,n(k)}$, where $n(k)$ refers to the total number of elements included in the biometric characteristic vector and k is the security parameter. There exists a simulator $\mathcal{B}$ who can use $\mathcal{A}$ to invert the one-way trapdoor function with the probability:*

$$\epsilon \geq n(k)\epsilon^{',t,n(k)}.$$

PROOF. The proof is by contradiction. we mean the adversary defeating our proposed BDK with permutations when he successfully recovers the biometric characteristic vector $\vec{b} = (b_1, \cdots, b_n)$ of size n. Let $\mathcal{A}$ be a malicious adversary defeating our proposed BDK with a nonnegligible advantage defined as $\epsilon^{'}, t, n(k)$, where $n(k)$ refers to the size of the biometric characteristic vector and k is the security parameter. We construct a simulator $\mathcal{B}$ that can utilize $\mathcal{A}$ to reverse the underlying one way trapdoor function when $(f, f^{-1}, \mathbb{R}_p) \leftarrow \mathcal{G}(1^k)$; $R_B \leftarrow \mathbb{R}_p$; $y \leftarrow f(R_B)$. The simulator $\mathcal{B}$ also defines the encryption C_B as what we previously explained. If the encryption oracle $\mathcal{O}^E$ is asked an $R_B^i (i = 1, \cdots, n(k))$ such that $f(R_B) = y$, the simulator outputs R_B and halts. Otherwise, the simulator $\mathcal{B}$ selects $\alpha \leftarrow y \parallel s$ where $s \leftarrow_R \mathbb{R}_p$ and gives back to the adversary $\mathcal{A}$ as the response. (e.g. It is noted that since the underlying one way trapdoor function is publicized, the encryption oracle can also be operated by the adversary himself.) Meanwhile, the simulator $\mathcal{B}$ watches the oracle queries that $\mathcal{A}$ makes to see whether there exists any oracle query $R_B^i (i = 1, \cdots, n(k))$ for which $f(R_B) = y$ holds. If there exists, $\mathcal{B}$ outputs R_B.

Then, the adversary $\mathcal{A}$ submits two messages $m_0, m_1 \in \mathbb{R}_p$ where $|m_0| = |m_1| = k$, and the simulator $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and returns the encryption of m_β as the challenge ciphertext c^*.

Let A_k be the event that the adversary $\mathcal{A}$ asks the query $R_B = f^{-1}(y)$. The adversary $\mathcal{A}$ has no advantage in distinguishing m_0 and m_1 in the case that he does not query the encryption oracle $\mathcal{O}^E$ at $R_B^i (i = 1, \cdots, n(k))$ satisfying $R_B = f^{-1}(y)$. Additionally, the permutation operation also makes the adversary correctly decide the R_B's position w.r.t. the associated element in the biometric characteristic vector with the probability of $Pr[\mathcal{A}succeeds|A_k] = \frac{1}{n(k)}$. Therefore,

$$\begin{aligned} & \frac{1}{2} + \epsilon^{'}, t, n(k) \\ & = Pr[\mathcal{A}succeeds|A_k]Pr[A_k] + Pr[\mathcal{A}succeeds|\bar{A_k}]Pr[\bar{A_k}] \\ & \leq \frac{1}{n(k)} Pr[A_k] + \frac{1}{2}. \end{aligned} \quad (8)$$

Thus, we can arrive at $\epsilon = Pr[A_k] \geq n(k)\epsilon^{'}, t, n(k)$ must be also nonnegligible and namely the simulator $\mathcal{B}$ successfully inverts the underlying one way trapdoor function f. □

The formal security proof w.r.t. the multiplicative blinding resembles to the proof we presented above. Therefore, the proposed secure and efficient biometric based deterministic key agreement for WBANs is proved to be secure in the model we set in Sec. 3.

5.2 Security Comparison

In this subsection, we evaluate the security level of our proposed BDK by comparing the computational cost required for the adversary to successfully attack the key agreement constructions possessing the same security levels with the existing work. In the state-of-the-art, the technique of fuzzy vault and its variations are widely adopted to construct physiological signal based key agreement schemes for WBANs and their security mainly rely on the fact that the hiding of the authentic biometric characteristics among a much larger chaff points with the same value ranges, makes identifying the authentic points to recover the polynomial selected by the sponsoring body sensor very difficult. Only the authorized body sensors deployed on the same patient human body can collect the relevant biometric characteristics and distinguish the authentic points from the chaff ones. However, it is required for the adversary to search each point in the vault to obtain the agreed pairwise key. Therefore, the security of the current work mainly depends on the size of the fuzzy vault.

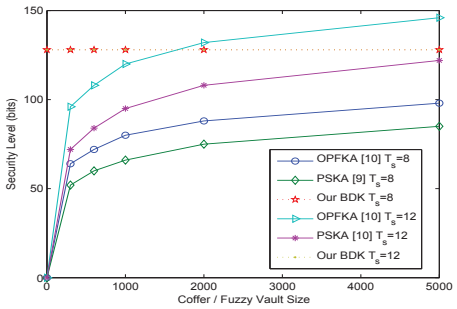

Figure 2: Security Comparison among PSKA [9], OPFKA [10] and Our Proposed BDK

On the contrary, the security of our proposed key agreement scheme BDK depends on the computational hardness of the underlying one way trapdoor function, namely the secrecy of the private key. For ease of comparison, we transform the computational cost into its counterpart of sponsoring brute-forcing attack to a private key with specific length. Fig. 2 illustrates the security level comparisons among PSKA [9], OPFKA [10] and our proposed BDK w.r.t. specific computational cost. It is obviously observed that the security levels of [9] and [10] increase as the size of the fuzzy vault increases, while the security level of our proposed BDK remains constant, independent of the fuzzy vault size and much higher than the other two constructions [9] and [10]. Although OPFKA [10] possesses higher security level than PSKA [9] w.r.t. the same size of fuzzy vault, when the number of the shared biometric characteristics $T_s = |R_{A,i}^{IST}| = 8$, the security level of OPFKA [10] cannot achieve our proposed BDK as the vault size increases even to 5000. When $T_s = |R_{A,i}^{IST}| = 12$, the security level of OPFKA [10] meets the level of our proposed BDK as the vault size increases to about 1650. Therefore, we can arrive at the conclusion that our proposed BDK achieves a much higher security level with dramatically reduced overhead.

5.3 Message Exchange and Acknowledgement

The biometric based interactions between a pair of body sensors also cannot allow the adversary to extract the negotiated pairwise key. The reasons are mainly described as follows.

Firstly, in each biometric characteristic message exchange, ID_B and ID_A respectively identify the identities of the sponsoring and reacting body sensors. The random number N_0 ensures the freshness of the received message. Additionally, the adversary cannot sponsor replay attack or forgery attack. The former refers to the adversary retransmits the old messages including the outdated biometric characteristics belonging to previous time slots; while the latter refers to the adversary tries to establish a pairwise key with one body sensor by using the biometric characteristics collected from different human bodies. However, none of them can successfully pass the MAC verification. Finally, the proposed BDK with

permutation operations can still prevent the adversary from computing the agreed pairwise key even he recovers the shared biometric characteristics between a pair of body sensors.

6. PERFORMANCE EVALUATION

In this section, we perform the extensive simulations to illustrate the practicability and efficiency of our scheme by using EKG signals. The proposed secure and efficient biometric based deterministic key agreement scheme BDK in WBANs is evaluated from the following aspects by comparison with the existing work: (1) long and random keys; (2) storage, computational and communication overhead; and (3) distinctiveness and temporal variance.

(1) Long and random keys. The established pairwise keys among body sensors are negotiated by the interactions between the sponsoring sensor and the reacting sensor through performing an underlying hash function on the shared biometric characteristics. Therefore, the length and randomness of the pairwise keys can be guaranteed.

(2) Storage overhead. For comparison convenience, it is assumed that ID_B and ID_A respectively take 16 bytes. The authentic biometric characteristic points and the chaff points introduced in PSKA [9] and OPFKA [10] take 20 bits each. The index takes 1 byte and the random nonce N_0 and the MAC takes 16 bytes each. Therefore, the storage overhead for each body sensor in our proposed BDK is

$$STCOST = 2(|ID_B|+|ID_A|)+2.5|M|+|Idx|+|N_0|+2|MAC|, \quad (9)$$

where $|M|$ refers to the number of authentic biometric characteristic points. If we use $|N|$ to represent the number of chaff points introduced in PSKA [9] and OPFKA [10], $|R| = |M| + |N|$ denotes the total size of the fuzzy vault in [9] or the coffer size in [10]. It is obviously observed that the majority of the storage is taken up by the biometric set M and the vault/coffer set R. Since different feature generation method is adopted in PSKA [9], it is required to use 36 bits to represent each point in their construction. Fig. 3 illustrates the storage comparison among PSKA [9], OPFKA [10] and our proposed BDK. It shows that to transmit the same number of collected biometric characteristics between the pair of body sensors for negotiating the pairwise key, the storage overhead of our proposed BDK is significantly reduced compared to the existing work [9] and [10] and best adapts to the scenario of WBANs. Moreover, the more the authentic biometric characteristics are collected, the more obvious this advantage will become.

(3) Communication overhead. The communication overhead mainly depends on the steps of feature exchange and feature acknowledgement. It can be straightforwardly concluded that the communication overhead of our proposed BDK is dramatically reduced since no chaff points are introduced to guarantee the security of the underlying pairwise key agreement scheme. The communication comparison resembles the storage illustrated in Fig. 3.

(4) Computational overhead. We mainly focus on modular exponentiation and multiplicative operations required in the underlying key agreement scheme for WBANs since the computational cost of additive operations can be omitted compared to the former two. It is assumed that the private key of the one way trapdoor function exploited in our proposed BDK is 128-bit long. To achieve the same security level, it is required for OPFKA [10] to possess the coffer size of 1600 under the condition that the number of shared biometric characteristics $T_s = 12$. However, with the same vault size in PSKA [9], it is required to increase the number of shared biometric characteristics to $T_s = 15$ to meet the defined security level. In our evaluations, t_e and t_m respectively refer to the time required for modular exponentiation and multiplicative operations. The computational overhead of PSKA [9] mainly relies on the polynomial evaluation in the vault creation phase and the polynomial reconstruction in the vault unlocking phase. Thus, for each body sensor, it is respectively required to perform at least $300 * t_e + 330 * t_m$ computational cost in PSKA [9] to successfully establish a pairwise key. On the other hand, without using error correction codes and reconstructing polynomials, OPFKA [10] possesses less computational overhead than PSKA [9] and our proposed BDK; however, this goal is only achieved by sacrificing significant storage overhead for chaff points to meet the same security level. The computational overhead of our proposed BDK mainly depends on the biometric characteristic blinding and debinding operations respectively in the phase of feature blinding and exchange. It is required for each body sensor in our proposed BDK to have a total amount of $22 * t_e + 24 * t_m$ computational cost to successfully establish an agreed key. Although the computational cost is slightly heavier than OPFKA [10], without introducing the chaff points, under the same security level, the storage overhead on each body sensor would be dramatically reduced as what has been illustrated in Fig. 3.

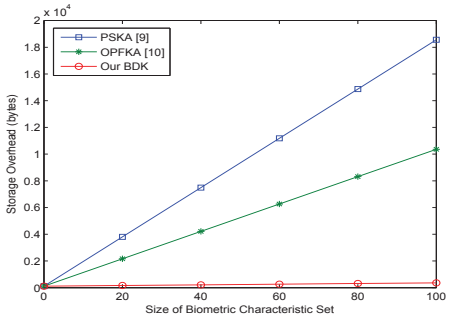

Figure 3: Storage Comparison among PSKA [9], OPFKA [10] and Our Proposed BDK

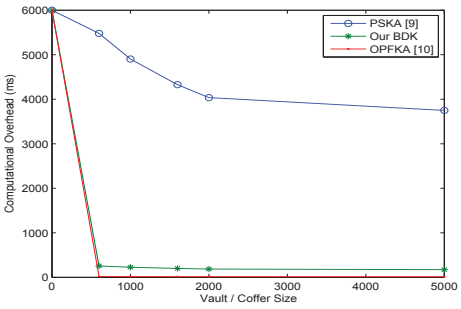

Figure 4: Computation Comparison among PSKA [9], OPFKA [10] and Our Proposed BDK

We conduct the experiments by exploiting PBC [16] and MIRACLE [17] libraries running on Linux platform with 2.93GHz processor to study the computational overhead. The experimental re-

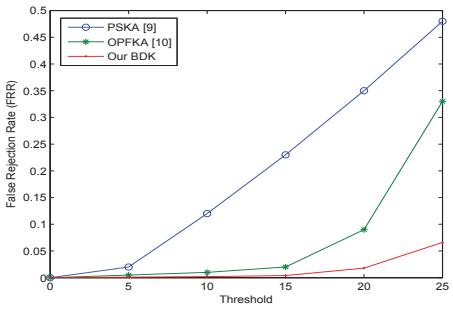

Figure 5: False Rejection Rate Comparison among PSKA [9], OPFKA [10] and Our Proposed BDK

sults show a single exponentiation and multiplicative operation in $\mathbb{R}_p$ with $|p| = 512$-bit long almost respectively costs 7.6 ms and 6.2 ms. Fig. 4 illustrates the computational comparison between PSKA [9], OPFKA [10] and our proposed BDK. It shows that the computational overhead of PSKA [9] decreases as the vault/coffer size increases, since to achieve the same security level, it is require to possess more shared biometric characteristics between body sensors, namely the degree of the underlying polynomial selected by the sponsoring sensor would be higher, when the vault size is small. For comparison convenience, it is obviously observed that when the same number of shared biometric characteristics T_s is required in PSKA [9] and our proposed BDK, our computational overhead is dramatically reduced since only $T_s - 1$ modular exponentiation and T_s multiplicative operations in $\mathbb{R}_p$ are required for each body sensor, alleviating the complex polynomial evaluation and reconstruction.

(5) Distinctiveness and temporal variance. Distinctiveness refers to the property that the biometric characteristics collected from one patient can be significantly distinguished from the ones collected from other patients, which prevents the adversary from launching forgery attack. There are also two metrics to evaluate the distinctiveness, namely the false rejection rate and the false acceptance rate. The former refers to the probability that two sensors in the same WBAN fail to negotiate a shared pairwise key, while the latter refers to the probability that two sensors deployed in different WBANs successfully establish a session key or the asynchronously collected biometric characteristics are exploited to successfully establish a session key between body sensors (e.g. The property of time variance represents the randomness of the generated biometrics and can be utilized to evaluate the resilience to replay attacks).

The false acceptance rate of our proposed BDK is comparable to OPFKA [10] since the same feature generation method is exploited. Fortunately, our proposed BDK possesses lower false rejection rate than PSKA [9] and OPFKA [10] since we remove the need of chaff points to ensure certain security levels. Therefore, the probability of the collisions between the chaff points and the biometric characteristics collected by the reacting body sensor is significantly reduced. Fig. 5 illustrates the false rejection rate comparison between PSKA [9], OPFKA [10] and our proposed BDK.

7. CONCLUSIONS

In this paper, a secure and efficient biometric based deterministic key agreement for WBANs is proposed by exploiting the overlap between the biometric characteristics collected by body sensors. The pairwise keys for WBANs can be definitely agreed by the interactions between body sensors within the same WBAN. We give the formal security proof depending on the underlying one way trapdoor function rather than the vault/coffer size. Extensive simulations and comparisons illustrate the efficiency and practicability of our proposed construction BDK and the advantages over the state-of-the-art with stronger resilience, lower false rejection rate, less storage, computational and communication overhead.

8. ACKNOWLEDGMENTS

This work was supported by the National Program on Key Basic Research Project (973 Program) and National Natural Science Foundation of China under grant 2012CB723401, 61161140320 and 61033014.

9. REFERENCES

[1] L.Gatzoulis and I. Iakovidis, *Wearable and Portable E-health Systems*, IEEE Engineering in Medicine and Biology Magazine, vol. 26, no. 5, pp. 51-56, 2007.

[2] 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 Proc. IEEE Int'l Conf. Parallel Processing Wksp., pp. 432-439, Oct. 2003.

[3] S. D. Bao, C.C.Y. Poon, Y.T. Zhang and L.-F. Shen, *Using the Timing Information of Hearbeats as an Entity Identifier to Secure Body Sensor Network*, IEEE Transactions on Information Technology in Biomedicine, vol. 12, no. 6, pp. 772-779, 2008.

[4] L. Eschenauer and V. Gligor, *A Key Management Scheme for Distributed Sensor Networks*, Proc. of the 9th ACM Conf. on Computer and Communication Security, pp. 41-47, ACM Press, New York, 2002.

[5] J. Zhou, Z. Cao, X. Dong, X. Lin and A. V. Vasilakos, *Securing m-Healthcare Social Networks: Challenges, Countermeasures and Future Directions*, IEEE Wireless Communications, Accepted.

[6] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, *SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for E-health Systems*, IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 365-378, May 2009.

[7] J. Zhou and M. He, *An Improved Distributed key Management Scheme in Wireless Sensor Networks*, In 9th. International Workshop of Information Security Applications 2008-WISA 2008, September, 2008.

[8] A. Juels, and M.Sudan, *A Fuzzy Vault Scheme*, Proc. of IEEE Int. Symp. on Info. Theory, pp. 408, 2002.

[9] 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, Jan. 2010.

[10] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao and D. Chen, *OPFKA: Secure and Efficient Ordered Physiological Feature-based Key Agreement for Wireless Body Area Networks*, IEEE INFOCOM 2013.

[11] J. Zhou and Z. Cao, *TIS: A Threshold Incentive Scheme for Secure and Reliable Data Forwarding in Vehicular Delay Tolerant Networks*, In IEEE GLOBECOM 2012.