# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities


WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

## Interested in publishing with us?
## Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter 11

# Physiological Signal Based Biometrics for Securing Body Sensor Network

Fen Miao, Shu-Di Bao and Ye Li

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/51856

## 1. Introduction

Nowadays, the constraints in the healthcare of developing countries, including high population growth, a high burden of disease prevalence, low health care workforce, large numbers of rural inhabitants, and limited financial resources to support healthcare infrastructure and health information systems, accompanied with the improvement of potential of lowering information and transaction costs in healthcare delivery due to the explosively access of mobile phones to all segments of a country, has motivated the development of mobile health or m-health field. M-health is known as the practice of medical and public health supported by mobile devices such as mobile phones and PDAs for delivering medical and healthcare services. Thus, the popularity of m-health can be subjected to the development of wearable medical devices and wireless communication technology. In order to fully utilize wireless technology between the wearable medical devices, the concept of body sensor network (BSN), which is a kind of wireless sensor network around human body, was proposed in 2002.

### 1.1. Body sensor network

BSN, which has great potential in being the main front-end platform of telemedicine and mobile health systems, is currently being heavily developed to keep pace with the continuously rising demand for personalized healthcare. Comprised of sensors attached to the human body for collecting and transmitting vital signs, BSN is able to facilitate the joint processing of spatially and temporally collected medical data from different parts of the body for resource optimization and systematic health monitoring. In a typical BSN, each sensor node collects various physiological signals in order to monitor the patient's health status no matter their location and then instantly transmit all information in real time to the

INTECH
open science | open minds

© 2012 Miao et al.; licensee InTech. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

medical server or the doctors. When an emergency is detected, the physicians will immediately inform the patient through the computer system by providing appropriate messages or alarms. By this way, BSN is preferred in monitoring patients in environments lack of medical doctors, such as home and workplaces. Fig.1 presents a simplified example of a BSN application scenario in a mobile health system. Sensor nodes on or inside the human body and a Master Node (MN), are connected to form a BSN. Medical information collected by different sensors in a BSN will be sent to the MN for data fusion and then to personal server for pre-processing before being forwarded to a central server for further analysis or the physicians for care giving via various forms of communications such as wireless personal area network (WPAN), wireless local area network (WLAN) and wide area network (WAN).

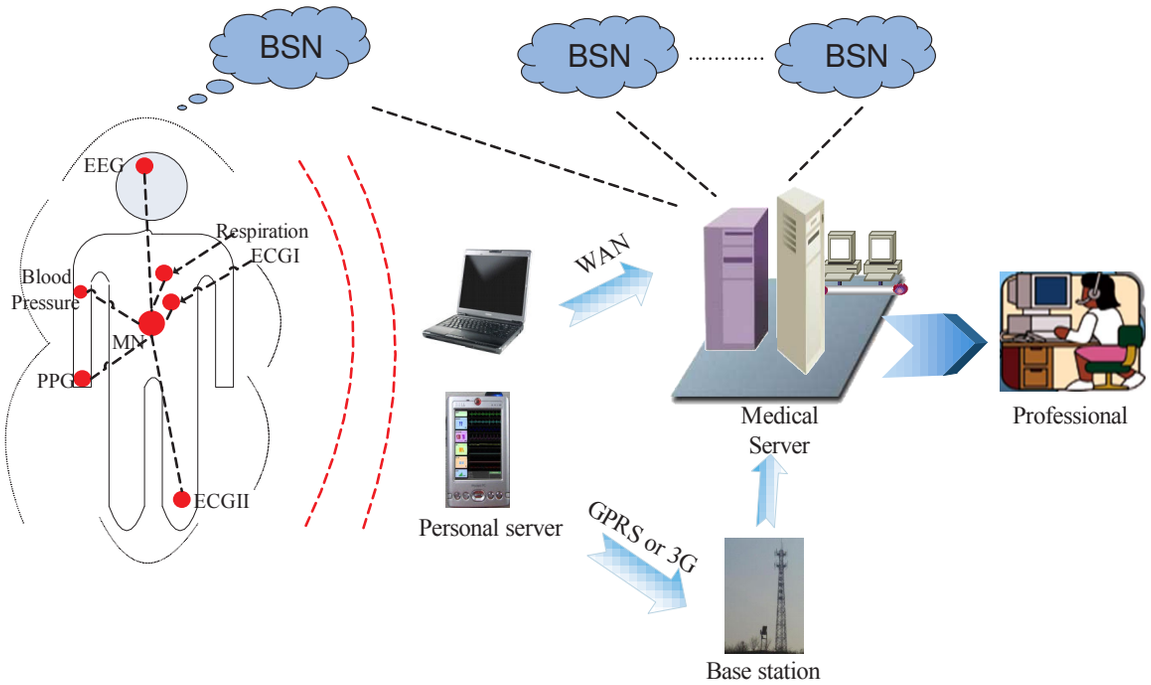


**Figure 1.** An application scenario of BSN

## 1.2. Security challenge in BSN

As mandated by privacy laws and regulations, such as the Health Information and Portability Accountability Act (HIPAA) (Bowen et al, 2005) and the European Union Directive 2002/58/EC (2002), wireless standards with medical applications have to have a high level of reliability to guarantee the security of patients' information and the privacy of healthcare history. To ensure the security of the overall mobile health system, BSN as an important end, should be protected from different attacks such as eavesdropping, injection and modification. However, it is a nontrivial task due to stringently limited processing capability, memory, and energy, as well as lack of user interface, unskilled users, longevity of devices, and global roaming for most sensor nodes.

http://dx.doi.org/10.5772/51856

Symmetric cryptography, in which communication parties must possess a shared secret key via an invulnerable key distribution solution prior to any encryption process, is a promising approach to relieve the stringent resource constraints in BSN. Existing key distribution techniques for large-scale sensor networks, such as random-key pre-distribution protocols (Gligor et al, 2002; Perrig et al, 2003) and polynomial pool-based key distribution (Ning et al, 2003), require some form of pre-deployment. However, given the progressively increasing deployments of BSN, these approaches may potentially involve considerable latency during network initialization or any subsequent adjustments, due to their need for pre-deployment. In addition, it obviously discourages people, such as family members, to share sensors between themselves because whenever there is need to add or change a body sensor, the user has to configure a new initial key to ensure that the new sensor can securely communicate with the existing ones. Therefore, a new series of key distribution solutions without any form of initial deployment to provide plug and play security is desirable for BSNs.

### 1.3. Novel biometrics for BSN security

As well known, the human body physiologically and biologically consists of its own transmission systems such as the blood circulation system, thus, how to make use of these secured communication pathways available specifically in BSN to secure it is a good idea (Poon et al, 2006). It is undoubtedly practical in securing BSN with a telemedicine or m-health application, as nodes of these BSN would already comprise biosensors for collecting medical data, which could be physiological characteristics uniquely representing an individual. If these intrinsic characteristics can be used to verify whether two sensors belong to the same individual, the use of physiological signals to identify individuals and secure encryption key transmission with resources-saving is feasible. Building upon this initial idea, a family of lightweight and resource-efficient biometrics-based security solutions, which are based on time-variant physiological signals, has been proposed for the emerging BSN with a dual purpose of individual identification and key transmission. It is different from traditional biometrics, where the physiological or behavioural characteristics are static and merely used to automatic identify or verify an individual. The utilized biometric traits in traditional biometric systems should have the characteristics of universality, distinctiveness, permanence, effectiveness, invulnerability and so on, while the physiological characteristics should be dynamic at different times to ensure the security of key transmission in BSN.

As depicted in Fig.2, in biometrics solution the physiological signals of human body, such as electrocardiograph (ECG) and photoplethysmograph (PPG), were used to generate the entity identifier (EI) of each node for identifying nodes and then protecting the transmission of keying materials by a key hiding/un-hiding process. It is based on the fact that EIs generated simultaneously from the same subject are with high similarity, while those generated non-simultaneously or from different subjects are with significant differentiation.

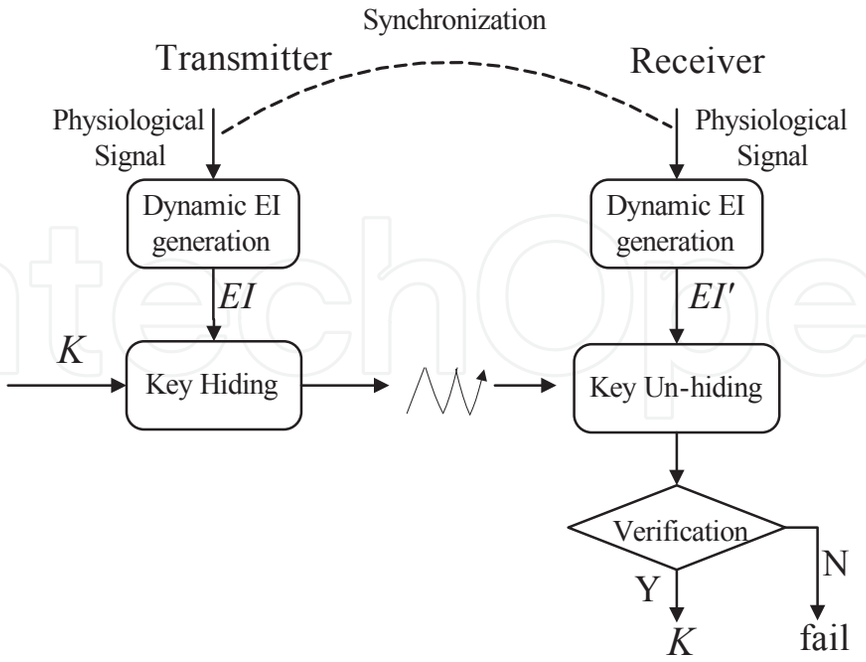


**Figure 2.** Workflow of biometrics-based security solution

*1.3.1. Dynamic EI generation*

The timing information of heartbeats was demonstrated by Bao et al (2005) to be a possible biometric characteristic to be used in proposed entity authentication scheme due to its chaotic nature, which can ensure the dynamic random performance of the generated EIs and then the security performance for BSN. Thus, the authors proposed to use Inter-Pulse-Interval (IPI) to generate EIs for securing the distribution of keying materials. A rigorously information-theoretic secure extraction scheme to properly extract the randomness of ECG signal, mainly from the IPI information, was proposed by Xu et al (2011). It was demonstrated that there are two advantages of using IPI to secure BSN. Firstly, it can be derived from multiple physiological signals such as electrocardiograph (ECG) and photoplethysmograph (PPG) by measuring the time difference between peaks in the signals. Secondly, it has been demonstrated that EIs generated from a series of IPI values passed the selected randomness tests from the National Institute of Standards and Technology (NIST) standards, and thus show an acceptable degree of randomness. However, an R-wave detection process is required before IPI measurement, which not only increases the computational complexity, but also leads to the uncertain performance because the accuracy of R-wave detection seriously affects the performance of IPI-based security system. In addition, 32 IPIs need to be utilized to generate a 128-bit EI, which means about 30 seconds of ECG/PPG measurements are required before cryptographic keys can be securely distributed. To overcome these problems, the frequency-domain characteristics of physiological signals (FDPS), was proposed by Gupta et al (2010) to be a promising biometric characteristic due to its real-time performance, where 5 seconds measurement is enough to generate EIs. Also, there is no need of R-wave

http://dx.doi.org/10.5772/51856

detection in FDPS-based EI generation scheme. However, the poor randomness and recognition rate performance are the bottlenecks of using FDPS to generate EIs and need to be broken through to ensure the security performance of BSN.

*1.3.2. Fuzzy method based key distribution solution*

Since intrinsic characteristics captured simultaneously at different parts of the same subject have slight differences, fuzzy methods should be deployed on the transmitter/receiver for an increased tolerance in acceptable differences to protect the transmission of keying materials using generated EIs. Fuzzy commitment scheme proposed by Juels (2002), which works effectively in the case that the generated EIs are all sequential and with the same length, is employed in BSN security due to its low computational complexity, low memory occupied, as well as convenience to be implemented. However, Fuzzy commitment scheme is not appropriate while the feature points in EIs are un-ordered or with missing values due to its requirement for correspondence of features in terms of order. To address this issue, Juels and Sudan (2006) proposed the fuzzy vault scheme, which offers attractive properties in terms of security, changeable key, and flexibility, and thus has been a good candidate for biometrics based cryptographic systems. It has been applied in different traditional biometric systems, for example, fingerprint, face, and Iris biometric systems for better performance than fuzzy commitment. Though fuzzy vault scheme was also adopted in biometrics based BSN security in more and more studies, it is noted that (Miao et al, 2010) the scheme is not good enough to achieve stable performance if the generated EIs are with dynamic random patterns in bit difference. Also, fuzzy vault has its drawbacks of low recognition rate due to not considering the inequality of the number of features in EIs generated from the two communication parties.

This chapter will describe the aspects of this kind of new biometrics with focus on the state-of-the-art biometric solutions for BSN security. In Section 2, the schemes of generating EIs from physiological signals based on both time-domain and frequency-domain information will be presented, followed by the performance evaluation as being a dynamic individual identifier to differentiate different subjects. Secondly, the usage of such generated EIs for securing BSN, i.e. key transmission schemes, will be detailed with a performance comparison of different schemes designed according to EIs' specific characteristics in Section 3. In Section 4, we conclude this chapter with an illustration of different biometric solutions in BSN security, where some issues need to be further studied will be emphasized.

## 2. Entity identifier generation schemes

EI generation scheme is the most important issue should be addressed in the biometrics solutions because the security of BSN depends heavily on the characteristics of EIs generated. As described in Section 1, the state-of-the-art EI generation schemes are mainly classified into two categories, one is based on the time-domain information of physiological signals (TDPS) and the other is based on the frequency-domain information (FDPS). In this section,

we will illustrate the two schemes separately with a detail performance evaluation on their advantages and disadvantages.

### 2.1. TDPS-based EI generation scheme

IPI is the most commonly used timing information in TDPS-based EI generation scheme. Fig.3 presents the experimental protocol of IPI-based EI generation scheme and the application of EIs for node identification. In IPI-based EI generation scheme, each node extracts the time-domain information by calculating a series of IPIs from its own recorded cardiovascular signal such as ECG and PPG based on a synchronization signal initiated by the master node, which can be denoted as $\{IPI_i \mid 1 \le i \le N\}$. IPI-based EI generation process is then deployed on the series of IPIs of each end to generate its own EI. The EIs generated simultaneously from the transmitter and the receiver are with high similarity for the same subject, while high dissimilarity for different subjects or generated non-simultaneously, and thus can be used to identify nodes by comparing the Hamming distance between two EIs.

As depicted in Fig.3, given a sequence of IPI values, the IPI-based EI generation process for the transmitter/receiver is comprised of the following three processes: accumulation & modulo, contraction mapping and Gray coding. Give $N$ consecutive individual IPIs, a series of multi-IPIs can be obtained as follows:

$$\left\{ mIPI_i = \sum_{n=1}^{i} IPI_n \;\middle|\; 1 \le i \le N \right\} \tag{1}$$

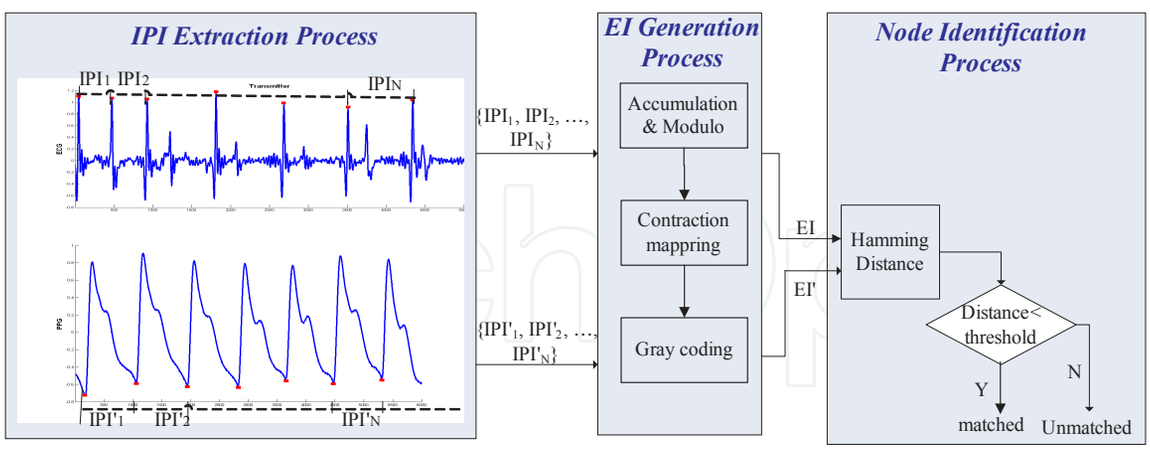


**Figure 3.** Experimental Protocol of TDPS-based EI generation scheme and node identification

To randomize the monotonically increasing multi-IPIs, a modulo operation is further introduced, i.e. $(mIPI_i) \bmod (2^L)$, where $L$ is a positive integer referred to as the modulo parameter. To compensate measurement differences among different BSN nodes, the modulo result is further transformed into a small integer $q$ by a contraction mapping $\hat{f} : [0, 2^L) \to [0, 2^q)$, i.e.,

http://dx.doi.org/10.5772/51856

$$\hat{f}(m)=\left\lfloor \frac{m}{2^{(L-q)}} \right\rfloor \quad (2)$$

where $L > q$ and $\lfloor . \rfloor$ returns the largest integer less than or equal to $m/2^{(L-q)}$. Finally, to increase the noise margin of measurements, the Gray code scheme is employed to get binary EIs. The generated EI can be expressed as $EI = I_1 \| I_2 \cdots \| I_{L-1} \| I_N$, where $I_i$ is generated from a corresponding $mIPI_i$ with the bit length of $q$. Such generated EIs have a bit length of $N \times q$.

### 2.2. FDPS-based EI generation scheme

Fig.4 presents a demonstration of the experimental protocol of FDPS-based EI generation scheme and the application of EIs for node identification with PPG as the physiological signal. In state-of-the-art FDPS-based EI generation schemes, nodes in the same BSN obtained independently the same physiological signal in a loosely synchronized manner, at a specific sampling rate for a fixed duration. An EI generation process is then deployed on the signal acquired from each end to generate its own EI. In order to realize node identification and the security of keying materials, the EIs generated simultaneously from the transmitter and the receiver should be with high similarity for the same subject, while high dissimilarity for different subjects or generated non-simultaneously. Therefore, the EIs can be used to identify nodes by comparing the distance between two EIs. Different from TDPS-based EI generation scheme, the distance of EIs measured here cannot be Hamming distance, the reason of which will be explained in Section 2.3.

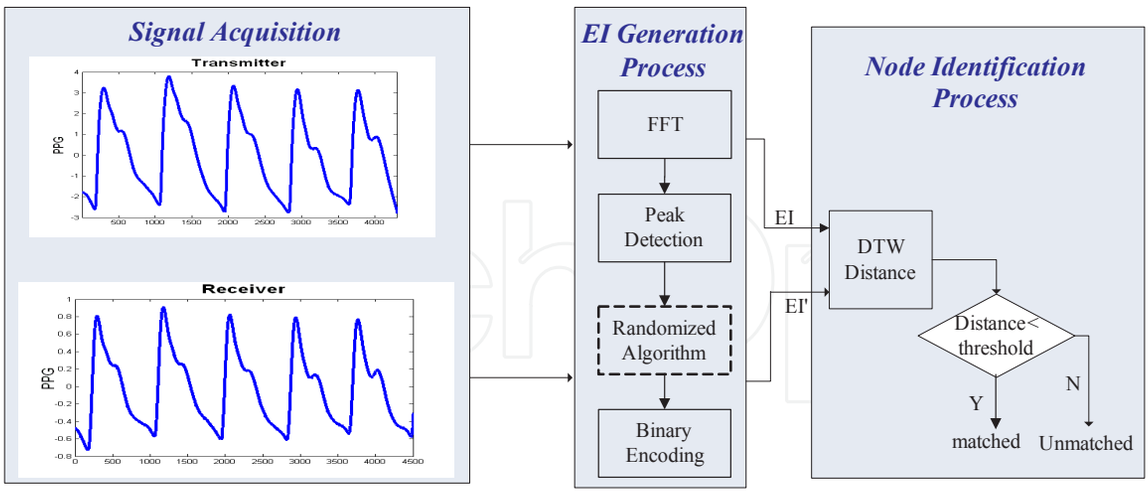


**Figure 4.** Experimental Protocol of FDPS-based EI generation scheme and node identification

As depicted in Fig.4, an entire FDPS-based EI generation process is comprised of a Fast Fourier Transform (FFT) process, a peak detection process, a randomized algorithm in some situations and a binary encoding process. In the previous FDPS-based EI generation process proposed by Gupta *et al* (2010), the samples collected are divided into several windows and

a FFT is performed on each of these parts, denoted as Multi-Windows generation scheme. A combination with the form of $<K_x^i, K_y^i>$ is derived through the peak detection process deployed on the FFT coefficients, where $K_x^i$ is the FFT point at which peak is observed, $K_y^i$is the corresponding FFT coefficient values, and $i$ is the index of the peaks. Each of the peak-index and peak-value are quantized and converted into a binary string and concatenated to form an EI, which can be denoted as $EI = \{f^1, f^2, \cdots f^N\}$, where $f^i = [K_x^i, K_y^i]$, $1 \le i \le N$, $N$ is the number of indexes where peaks are observed, which varies upon situation. However, based on what we learned from experimental analysis, $K_y^i$ is not a good resource to generate EIs because the amplitudes of physiological signals can be easily affected by a lot of measurement factors, such as the degree of skin exposure to sensor nodes.

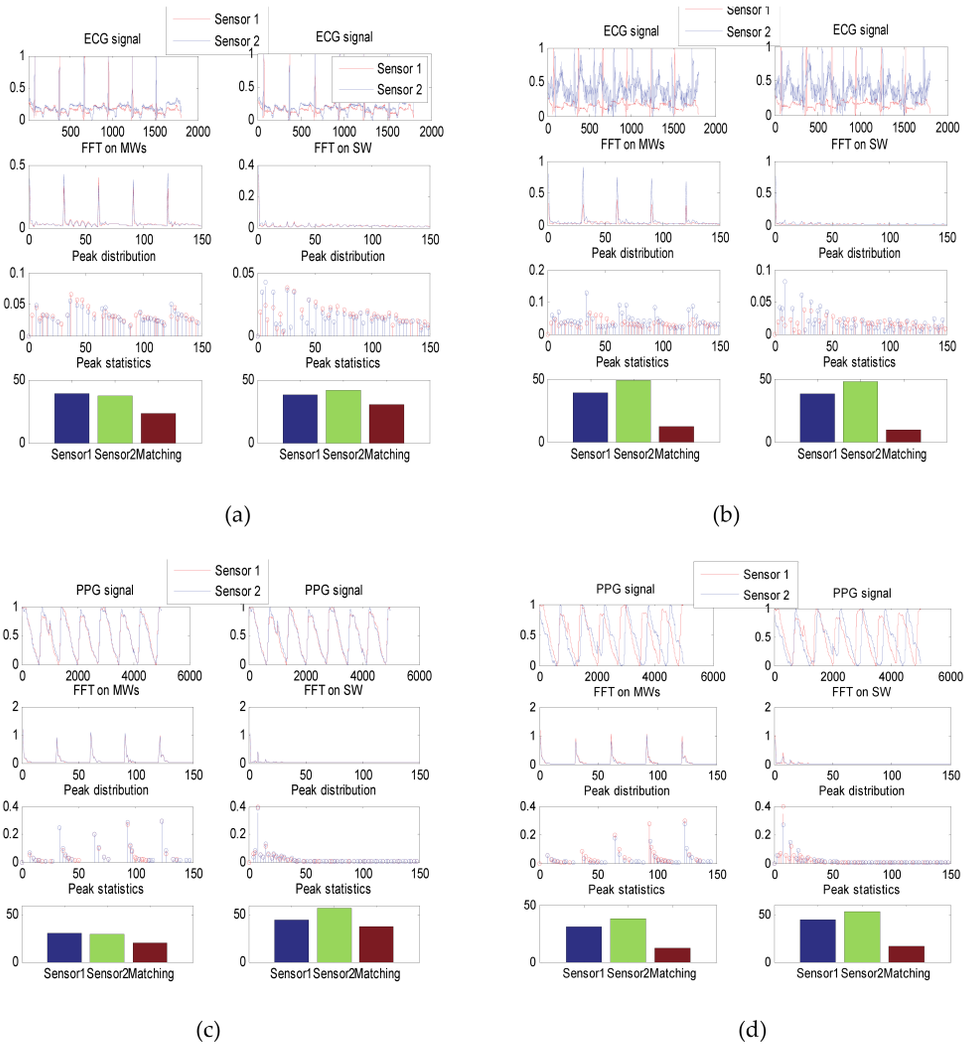


**Figure 5.** Multi-Windows versus Single-Window feature points generation process: (a) Same subject with ECG; (b) Different subjects with ECG; (c) Same subject with PPG; (d) Different subjects with PPG

http://dx.doi.org/10.5772/51856

Therefore, a Single-Window (SW) method to generate EIs was proposed by Miao *et al* (2011) aiming for a significant improvement in recognition performance and increase in randomness performance. Firstly, FFT is directly performed on the physiological signal in a loosely synchronized manner, at a specific sampling rate for a fixed duration, such as 5 seconds. Then, each peak-index, i.e. $<K_x^i>$, of the first $M$ points of FFT coefficients is selected and concatenated to form a set of feature points $F=\{K_x^1, K_x^2, \cdots K_x^N\}$, where $N$ is the number of indexes where peaks are observed, which varies upon situation. Before binary encoding process, a randomized algorithm is designed to overcome the bottleneck of randomness performance. Fig.5(a) and Fig.5(b) indicate an example of the differences between Multi-Windows (MWs) and Single-Window (SW) methods before randominzed algorithm with ECG signals collected by two nodes on one single subject and from two different subjects, respectively, while Fig.5(c) and Fig.5(d) indicate an example of the differences with PPG signals. It can be seen from Fig.5 that the number of peaks generated from nodes on the same subject has a higher number of matchings in terms of peak-index compared to those from different subjects; however, there is no such findings with FFT coefficients. In addtion, compared with MWs method, the SW method presents a larger matching rate, which is defined as the rate between the number of matched peaks and the number of the detected peaks, for the same subject and smaller matching rate for different subjects, no matter what kind of physiological signal is.

Obviously, all of the integer values of feature points are ascending and within a certain scale, which would bring about the bottleneck of the randomness performance and security weakness. Therefore, a randomized algorithm similar to Linear Congruential Generator (LCG), which is a kind of pseudorandom number generator, is deployed to randomize $F$ and form a new set $F'$, i.e.,

$$\begin{aligned} F' &= \{(bK_x^1 + c)\bmod 2^p,\ (bK_x^2 + c)\bmod 2^p,\ \cdots (bK_x^N + c)\bmod 2^p\} \\ &= \{f_1,\ f_2 \cdots,\ f_N\} \end{aligned} \tag{3}$$

where $2^p$ is the "modulus" and $p$ is a positive integer referred to as modulo parameter, $b \geq 0$ is the "multiplier", $0 \leq c < 2^p$ is the "increment". The selection of $b$, $c$, $p$ is directly related to the randomness performance of $F$. In the randomized algorithm, it is recommended that the most optimal relationship between $b$, $c$, $p$ is as followings:

$$\begin{cases} b = \lfloor 2^{p/2} \rfloor + 1 \\ c = 2\beta + 1,\ c \Big/ 2^p = (1 \Big/ 2 - \sqrt{3} \Big/ 6) \end{cases} \tag{4}$$

where $\beta \geq 0$, $\lfloor x \rfloor$ returns the largest integer less than or equal to x. Then, a permuted feature points set is generated with the form of $F'' = RandomPermute(f_1, f_2, \cdots, f_N) = (f'_1, f'_2, \cdots f'_N)$ by randomly permuting the order of

each point $f_i$. The generated EI can be expressed as $EI = I_1 \| I_2 \cdots \| I_{N-1} \| I_N$, where $\|$ is a concatenation operation. Each block of EI, i.e., $I_i$ is the binary result of a corresponding $f_i'$. The bit length of $I_i$ is $p$, and thus, the bit length of EI is $N \times p$.

### 2.3. Performance evaluation

To demonstrate the performance of different EI generation scheme, we conduct the performance evaluation in terms of randomness performance and group similarity. The performance comparison will be given to systematically illustrate the advantages and disadvantages of different schemes with two experiments. In the first experiment (Exp. I), the experimental data to be used for performance evaluation include ECG and PPG from 14 healthy subjects, where ECG was captured from the three fingers of each subjects and two channels of PPG were captured from the index fingers of the two hands, respectively. For each subject, the three channels of signals were captured simultaneously for 2-3min. All the three channels of signals were used to generate TDPS-based EIs, while two channels of PPG were used to generate FDPS-based EIs. In the second experiment (Exp. II), there were in total 85 clinical subjects from the hospital and two channels of physiological signals (including one-channel ECG and one-channel PPG) with a duration of 40 seconds were simultaneously recorded from each subject on three or four days within two-month period.

#### *2.3.1. Randomness performance analysis*

The randomness performance of binary sequences can be evaluated using a variety of randomness tests. Beacause of the length limitation in the generated binary EIs from each subject, several tests from the National Institute of Standards and Technology (NIST) standards were selected, including frequency (monobit) test, frequency test within a block, cumulative sums test, runs test, and approximate entropy test with the decision rule of 1% level.

| Test | Pass rate | |
|---|---|---|
| | FDPS-based EIs $b=23$, $c=109$, $p=9$ | TDPS-based EIs |
| Frequency Test | 99.219% | 100% |
| Frequency Test within a Block (M=10) | 100% | 100% |
| Runs Test | 99.219% | 100% |
| Cumulative Sums Test | 100% | 100% |
| Approximate Entropy Test | 99.219% | 100% |

**Table 1.** Randomness test results

Table 1 shows the randomness test results of TDPS-based EIs and FDPS-based EIs, where the randomizing parameters in FDPS-based EI generation scheme were set as $b=23$, $c=109$, $p=9$. It can be seen that all bit streams generated based on TDPS and most of

FDPS-based EIs passed the selected tests, and TDPS-based EIs show a better randomness performance than FDPS-based EIs.

### *2.3.2. Group similarity analysis*

The similarity between any pair of TDPS-based EIs generated simultaneously by sensors on the same individual can be analyzed with the Hamming distance. Fig.6 depicts the Hamming distance distribution of EIs with $L$ =8, $N$ =16, $q$=3. It can be seen that more than 95% of the Hamming distances between TDPS-based EIs are less than 10, and thus shows a good group similarity performance with the two experiments. Therefore, the proposed scheme is applicable in both healthy people and clinical subjects.

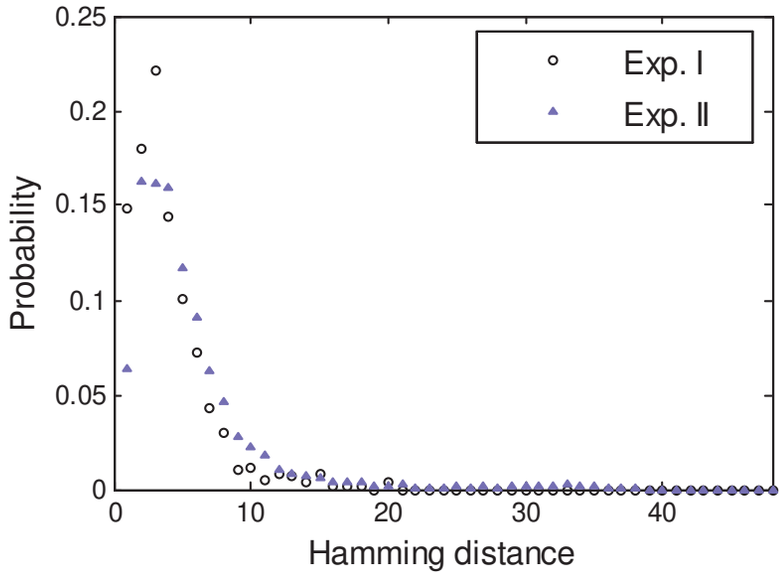


**Figure 6.** Similarity analysis with the Hamming distance ($L$ =8, $N$ =16, $q$=3)

Different from TDPS-based EIs, FDPS-based EIs cannot be analyzed with the Hamming distance due to the unequal length of generated EIs and matching points at different orders. As shown in Fig.7, the feature sets generated at the transmitter/receiver of the same subject after randomized algorithm have some common points, such as 174, 225, 156 at different orders, and thus direct Hamming distance in sequence can not reflect the real matching performance.

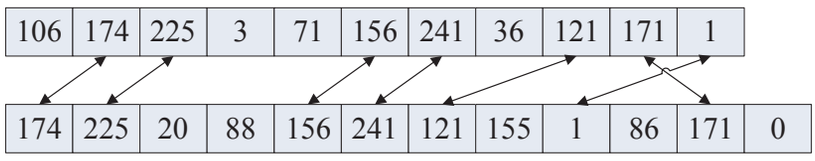


**Figure 7.** Feature points set generated at the transmitter/receiver of the same subject

Therefore, dynamic time warping (DTW) distance was selected to measure the group similarity between any pair of EIs generated from the same subject. DTW is an algorithm for measuring similarity between two sequences that vary in time or speed, which meets the characteristics of the EIs generated from FDPS. It is able to find an optimal match between two given sequences with certain restrictions. The sequences are "warped" non-linearly in the time dimension to determine a measure of their similarity independent of certain non-linear variations in the time dimension. Let $s_1$ and $s_2$ be two vectors with lengths of $m$ and $n$. The goal of DTW is to find a mapping path $\{(p_1, q_1), (p_2, q_2), \cdots, (p_k, q_k)\}$ such that the distance on this mapping path $\sum_{i=1}^{k} |s_1(p_i) - s_2(q_i)|$ is minimal.

Fig.8 depicts the DTW distance distribution of EIs generated from the true pairs, i.e., two nodes on the same individual, with the SW and MWs methods on PPG data, respectively. It can be seen that with the SW EI generation scheme, 98% of the DTW distance between true pairs are less than 90, compared with 82% with the MWs, and thus exhibit a better performance of group similarity than those with MWs.

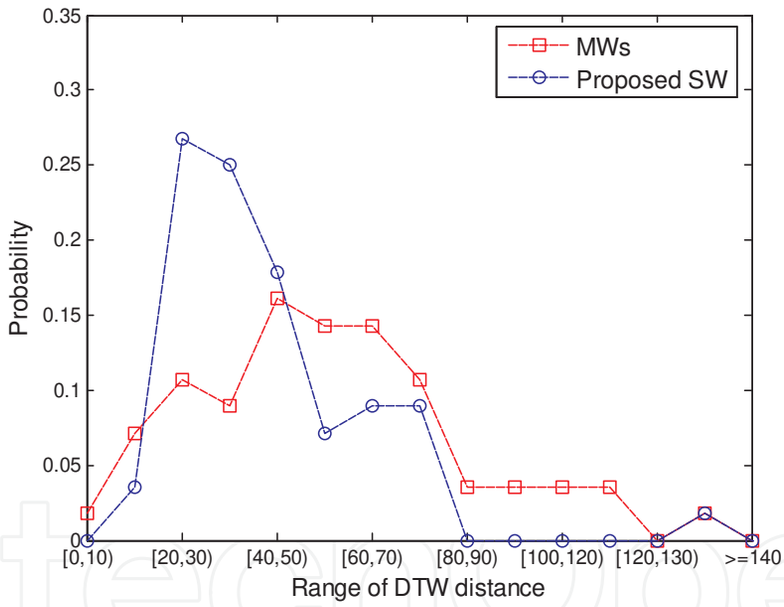


**Figure 8.** DTW distance distribution of FDPS-based EIs of the true pairs.

*2.3.3. Performance comparison between two EI generation schemes*

In order to realize high recognition rate, the generated EIs should have the characteristics of effectiveness (being able to be generated fast and easily), robustness (resistance to uncertainty), randomness, distinctiveness (being similar for same subjects and differentiate for different subjects). Firstly, as about 30 seconds of ECG/PPG measurements are required to generate a 128-bit EI based on TDPS while only 5 seconds based on FDPS, and an R-wave detection is needed in TDPS-based EI generation scheme for the IPI measurement, which in-

creases the computational complexity, the FDPS-based EIs shows a better effectiveness performance than TDPS. Secondly, the accuracy of R-wave detection affects the recognition performance of TDPS-based EIs heavily. For example, once a negative R-wave is detected or a positive R-wave is missed in one end, the EIs from true pairs will be dissimilar. Therefore, there would be a requirement for the given TDPS-based EI generation scheme that, the physiological signals shall be with an acceptable quality for peak detection. Though FDPS-based EI generation may also require a good signal quality, there is no evidence that the requirement is more constrict while compared to the TDPS-based one. Thirdly, from both the randomness performance and group similarity analysis, TDPS-based EIs shows a better performance than FDPS-based. In conclusion, TDPS-based EIs is superior in randomness and distinctiveness performance, while FDPS-based EIs is superior in effectiveness and robustness performance.

## 3. Key distribution solution

As presented in the workflow of the biometrics security in Section 1.3, the EIs can not only be used to identify individuals, but also be used to protect the transmission of keying materials. The key distribution process in biometrics security model works as follows: one of the two sensors, called transmitter, hides the random symmetric key generated by its own using an EI obtained from the physiological signal. This hidden key is sent over to another sensor, called receiver, which uses its own version of EI to recover the random key after compensating for the differences between its EI and the one used by the transmitter. The most common fuzzy methods used in biometrics security solution until now are fuzzy commitment and fuzzy vault, dependent on the characteristics of the EI generated. In this section, the two fuzzy methods application will be detailed with a discussion of the specific fuzzy method to be adopted for TDPS-based EIs and FDPS-based EIs according to their characteristics.

### 3.1. Fuzzy commitment scheme applied in BSN security

The block diagram of key distribution solution between communication parties based on the fuzzy commitment scheme is presented in Fig.9. Let $K \in \{0,1\}^k$ and $\hat{K} \in \{0,1\}^n$ represent the cryptographic key need to be protected and its corresponding error-correction codeword, respectively, $EI \in \{0,1\}^n$ represent the EI value at the transmitter used to protect keying materials, and $h : \{0,1\}^n \to \{0,1\}^l$ be a one-way hash function. The fuzzy commitment scheme is defined as $F(K, EI) = (h(K), K \oplus EI)$, where $\oplus$ is the bitwise XOR operation. To decommit $F(\hat{K}, EI)$ using a witness $EI'$ at its own end, the receiver computes $K' = f(EI' \oplus (\hat{K} \oplus EI)) = f(\hat{K} \oplus (EI' \oplus EI))$, where $f$ is the relevant error-correction decoding process. If $h(K') = h(K)$, then the decommitment is successful and $K'$ is the correct key $K$. Otherwise, $EI'$ is an incorrect witness that is not close enough to the original encrypting witness $EI$. It is obvious that the EI used in such a security model must be sequential and with the same length. In fact, in order to realize high-level security performance, $EI$ used in

fuzzy commitment must have the performance of distinctiveness and time-variance to ensure the invulnerability.

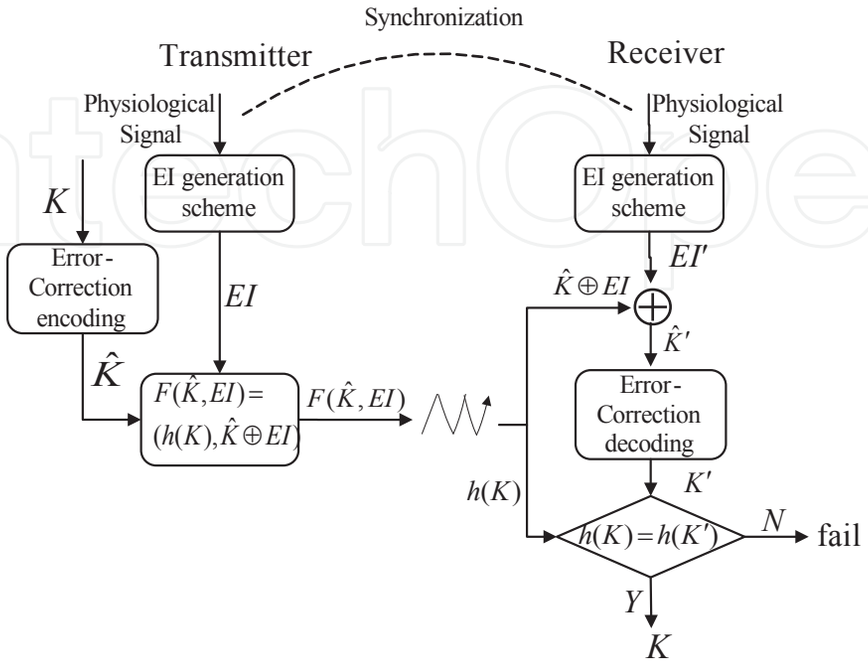


**Figure 9.** Key distribution solution based on fuzzy commitment scheme

### 3.2. Fuzzy vault scheme applied in BSN

Fig.10 gives the block diagram of key distribution solution between communication parties based on the fuzzy vault scheme applied in BSN security. In fuzzy vault based key distribution scheme, let $K \in \{0,1\}^n$ represent the cryptographic key need to be protected, $a_i \in \{0, 1\}^k$, $i=1 \cdots M$ represent the binary biometric features derived from the generated EI used to protect keying materials. A polynomial $P(x)=c_m x^m + c_{m-1} x^{m-1} + c_{m-2} x^{m-2} + \cdots c_1 x + c_0$ is created for binding of $K$ and $a_i \in \{0, 1\}^k$, $i=1 \cdots M$ by segmenting $K$ as its coefficients with the form of $K=c_m \| c_{m-1} \| c_{m-2} \| \cdots \| c_0$, where $m$ is the degree of the polynomial. The polynomial $P(x)$ is then evaluated on each of the feature points $X_i$, where $X_i$ is an integer number corresponds to binary feature $a_i$. The generated pairs $\{(X_i, P(X_i)), i=1 \cdots M\}$ are termed the genuine set $G$. Then the transmitter generates the chaff points set $C=\{(u_j, v_j),\ j=1 \cdots N_c\}$, where $N_c \gg M$, $u_j \neq X_i$ and each pair does not lie on the polynomial, i.e. $v_j \neq f(u_j)$. The final vault is constructed by taking the union of the two sets, i.e. $G \cup C$, combined with the message authentication code (e.g. MD5, SHA1)of $K$, denoted as $MAC(K)$, and pass through a scrambler so that it is not clear which are the feature points and which are the chaff points. The receiver decodes the fuzzy vault using binary biometric features $a'_i \in \{0, 1\}^k$, $i=1 \cdots M$ derived from the EI generated by itself by searching for the

matchings in the fuzzy vault. All the candidate points are identified together with their pair values in the vault to form a set $S$. Let $U$ denotes the number of pairs in $S$. To reconstruct the polynomial with $m$ degree, all possible combinations of $m+1$ points are identified, with a total number of $\binom{U}{m+1}$ combinations. Each of the possible combinations is used to recover the polynomial using Lagrange interpolating technique. The coefficients in the generated polynomial is mapped back and concatenated in the same order as encoding to generate an n-bit code $K'$. The cryptographic key $K$ can be retrieved while the message authentication code of $K'$ equals to $MAC(K)$ if the two EIs generated at both ends are with high similarity.

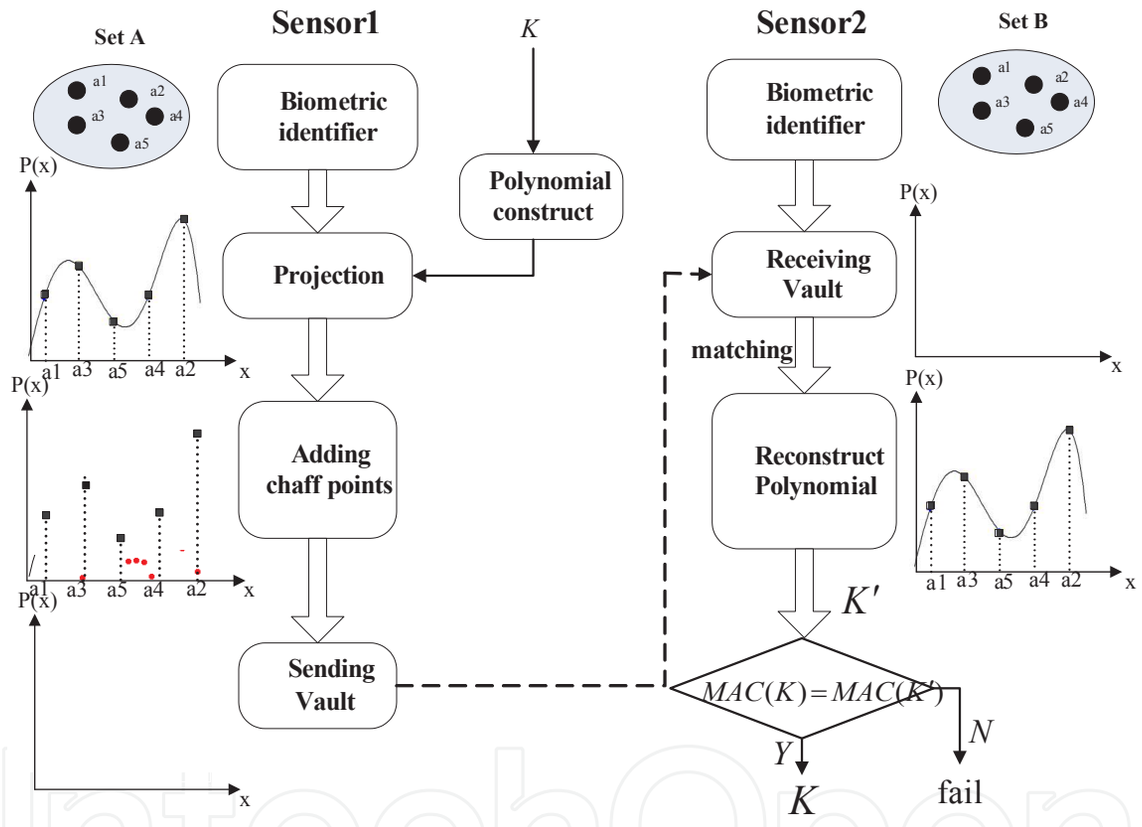


**Figure 10.** Key distribution solution based on fuzzy vault scheme

### 3.3. Performance comparison between different application scenarios

In order to realize high recognition performance and security, a suitable key distribution solution should be selected based on the specific characteristics of EIs generated based on TDPS and FDPS. In this section, we conduct a series of experiments to evaluate the performance of different key distribution solutions. Firstly, a detailed recognition performance in terms of False Accept Rate (FAR)/False Reject Rate (FRR) is conducted for different EI generation scheme with different key distribution solution to demonstrate the suitable key distribution solution for different EIs generated. Then, the security performance of different fuzzy

methods are presented. At last, the computational complexity performances are conducted for different key distribution solutions with the appropriate EI generation scheme.

*3.3.1. FAR/FRR performance*

FAR and FRR are two important indexes to evaluate the recognition rate performance of a biometric system, where FAR is the probability that a system incorrectly matches the input pattern from false pairs, FRR is the probability that a system fails to detect a match between the true pairs. The most suitable fuzzy method for different EIs should achieve a minumum half total error rate (HTER) that equals (FAR+FRR)/2.

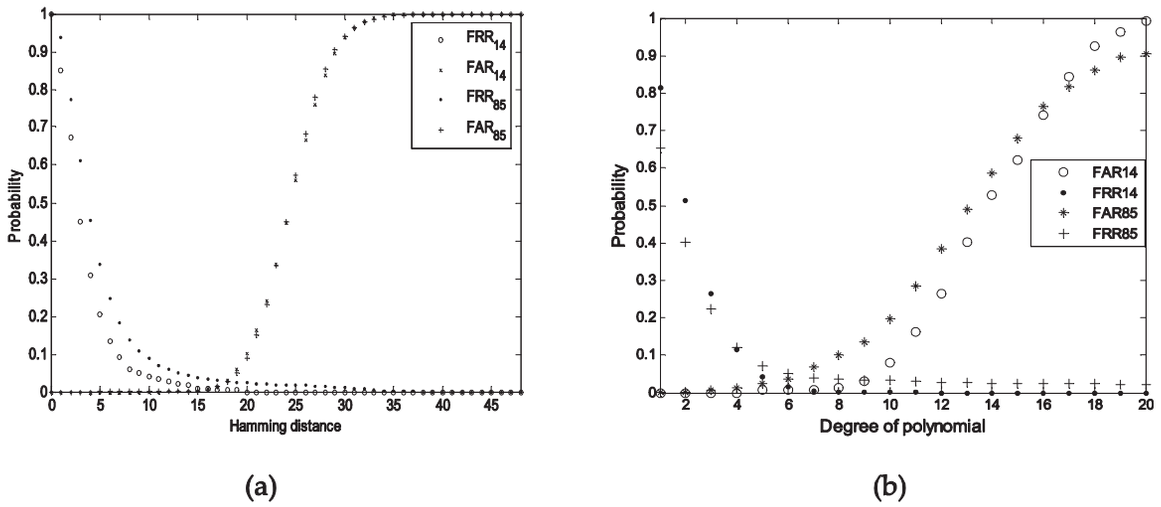


**Figure 11.** FAR/FRR curves with TDPS-based EIs. (a) Fuzzy commitment scheme; (b) Fuzzy vault scheme

For TDPS-based EIs, we conduct our performance evaluation based on data from two experiments described in Section 2.3. In Exp.I, i.e. there were in total 14 healthy subjects and three channels of physiological signals (including 1-channel ECG and 2-channel PPG) with a duration of 2-3 minutes were simultaneously recorded from each subject. In Exp.II, there were in total 85 clinical subjects and two channels of physiological signals (including one-channel ECG and one-channel PPG) with a duration of 40 seconds were simultaneously recorded from each subject on three or four days within a two-month period. Data from the both experiments are with 12-bit A/D resolution and at a sampling rate of 1000 Hz. Fig.11(a) depicts the FAR/FRR curves with fuzzy commitment scheme, where FRR is the rate at which the two EIs generated from the same subject during the same period are unmatched, i.e. Hamming distance is larger than a specific threshold, FAR is the rate at which the two EIs generated from the different subjects or during different periods are matched, i.e. Hamming distance is larger than a specific threshold. Fig.11(b) depicts the FAR/FRR curves with fuzzy vault scheme, where FRR is the rate at which the two EIs generated from the same subject during the same period are unmatched, i.e. matching number is smaller than a predefined degree of polynomial, FAR is the rate at which the two EIs generated from the different subjects or during different periods are matched, i.e. matching number is smaller than a prede-

http://dx.doi.org/10.5772/51856

fined degree of polynomial. It can be seen that the fuzzy commitment scheme shows a better recognition performance with a minumum HTER of less than 1.46% and 3.19% on 14 and 85 subjects, compared to 3.4% and 5.6% with fuzzy vault scheme. The results indicate that the fuzzy commitment scheme is superior to fuzzy vault scheme in different settings, such as the lab and the clinical setting, for TDPS-based EIs.

As presented in Section 2.3.2, the two feature sets generated based on FDPS from the transmitter and receiver are with different numbers of points and it is common to have matching points at different orders of the two sets, thus fuzzy commitment scheme is not suitable for FDPS-based EIs due to its requirement for correspondence of features in terms of order. Therefore, fuzzy vault scheme is probably the only approriate solution to protect the transmmission of keying materials with FDPS-based EIs. The data we used for performance evaluation include ECG data of 20 subjects from the physioBank database (http://www.physionet.org/physiobank), including 10 healthy people and 10 people with different kinds of diseases, which were simultaneously collected from two leads on each subject at a sampling rate of 360 Hz, and two-channel PPG data at a sampling rate of 1000 Hz from 14 subjects in Exp.I Fig.12 depicts the FAR/FRR curves with fuzzy vault scheme. It can be seen that fuzzy vault shows an recognition performance with a minumum HTER of 5.2% and 8.9% on ECG and PPG, respectively.

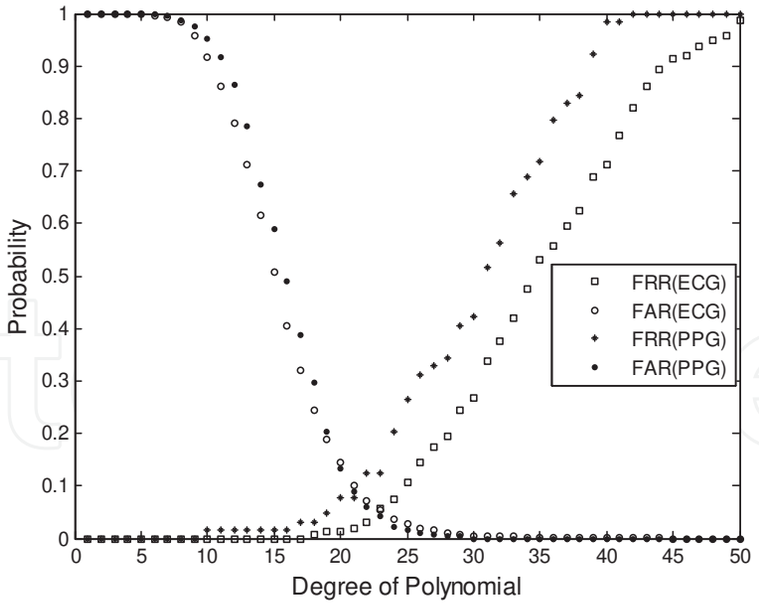


**Figure 12.** FAR/FRR curves with FDPS-based EIs based on fuzzy vault scheme

From the above analysis we can see, fuzzy commitment scheme is suitable for TDPS-based EIs while fuzzy vault scheme for FDPS-based EIs. In addition, TDPS-based solution shows a better recognition rate performance than FDPS-based one.

*3.3.2. Security analysis*

Suppose the EIs generated are random enough, the security issues in the proposed key distribution solution primarily exist during its package exchange process by brute-forcing the key ($K$) or EI directly. Therefore, to ensure the security of the key distribution protocol, the information contained in EI must be larger than that in $K$.

For fuzzy commitment scheme, an eavesdropper can try out each bit of $K$ by brute-force attack. Also, he can try out most of bits in EI to reconstruct the same $K$. Suppose the length of $K$ is $l$, the computation requirement of directly attack on $K$ in terms of its equivalence to brute-forcing a key of a particular length (bits) is $l$. The number of attempts by attacking EI depends on the length of $K$ and the ability of its corresponding error-correction. Take Reed-Solomon as the error-correction code for example, a redundancy code of $2\times t$ bits should be attached to correct $t$-bit errors, thus the length of EI should be equal to$l+2\times t$. As the error-correction code can correct $t$-bit errors, an attempt of $l+2\times t-t=l+t$ bits can reconstruct $K$ successfully. In conclusion, the computation requirement in terms of its equivalence to brute-forcing a key of a particular length (bits) is $\min(l, l+t)=l$. In another word, the security of fuzzy commitment depends on the security of $K$ directly.

For fuzzy vault scheme, except for brute-forcing $K$ directly, an eavesdropper can record the vault and try to construct the hidden polynomial from it. As described above, the computation requirement of directly attack on $K$ is $l$. Suppose the degree of the polynomial is $m$, as the feature points are hidden among a much larger number of chaff points, whose values are randomly distributed in the same range in some situation, an adversary is able to try out each group of $m+1$ points in the vault to get the correct polynomial, the average attempts are $\binom{L}{m+1}\Big/2$, where $L$ is the vault size and $L \le 2^p$. Thus, the security of vault is a balance act between the vault size $L$ and the degree of the polynomial $m$, but subject to $p$ and $l$. In conclusion, the computation requirement in terms of its equivalence to brute-forcing a key of a particular length (bits) is $\min(\log_2^{\binom{L}{m+1}}, l)$. The security of the vault for different values of $m$ and different number of vault size in the condition $l=128$ and $p=9$ is presented in Fig.13. For ease of understanding, we represent this computation requirement in terms of its equivalence to brute-forcing a key of a particular length (bits). As expected, increasing the number of chaff points increases the security provided by the vault, but the security is subject to $p$ and $l$. Higher the order of the polynomial means higher security, where more common feature points shall be hold by two ends.

*3.3.3. Computational complexity*

As described in Section 3.3.1, the suitable fuzzy method for TDPS-based EIs is fuzzy commitment while fuzzy vault for FDPS-based EIs. We estimate the cost performance of proposed key distribution solutions in terms of computational complexity, including time complexity and space complexity.

http://dx.doi.org/10.5772/51856

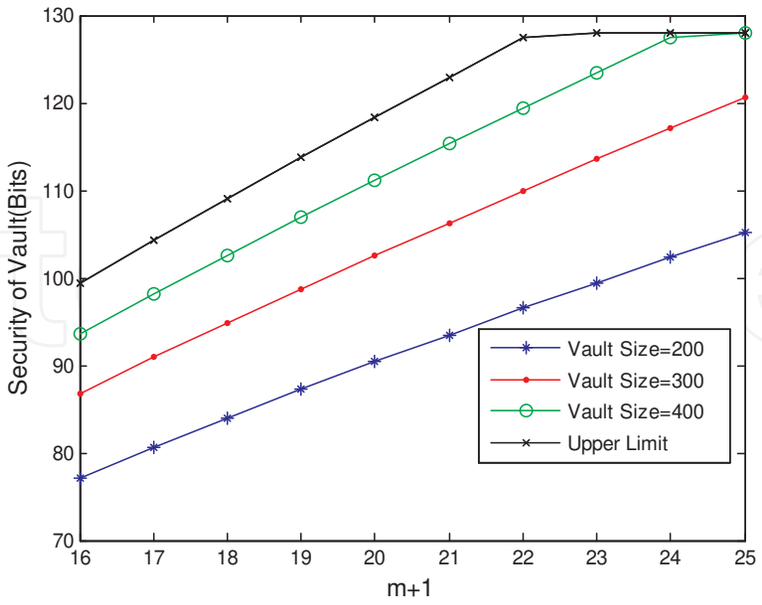


**Figure 13.** Security of fuzzy vault scheme

The time complexity involved in TDPS-based key distribution solution requires the following tasks: 1)R-wave detection; 2) IPI-based EI generation process; 3) Error-correction encoding process; 4) Error-correction decoding process. From the FAR/FRR performance analysis we can see, the Hamming distance to achieve minimum HTER is about 18. Thus, from the security analysis, in order to ensure the security of 128 bits, an EI of 164 bits should be generated. Take $q$=4 for example, 41 IPIs should be calculated, which means 42 R-waves should be detected. Take difference threshold algorithm for example, which has the minimum computational complexity in R-wave detection algorithms, the time complexity of R-wave detection process on $n$ points is $O(n)$. It was demonstrated by Bao et al (2009) that the time complexity for IPI-based EI generation process is $O(N^2)$, where $N$ is the number of IPIs used. Take Reed-Solomon as the error-correction code, the time complexity for the encoding process is $O(N.q)$, and for the decoding process based on Berlekamp–Massey algorithm the time complexity is $O((N.q)^2)$. As $q$ is a fixed number, the time complexity of proposed solution can be expressed as $O(n+N^2)$. The space complexity is estimated in terms of memory required for implementing proposed schemes. Excluding the dynamic occupied memory due to R-wave detection process and error-correction encoding/decoding process, the primary static components in the transmitter is $F(\hat{K}, EI)$ while $F(\hat{K}, EI)$ and $EI'$ in the receiver, and the overall memory required is 84 bytes.

The time complexity involved in FDPS-based key distribution solution requires the following tasks: 1) FFT computation; 2) Peak detection; 3) EI generation; 4) Key hiding (polynomial evaluation); 5) Key un-hiding (Lagrange interpolation). For the FFT computation process performed on $n$ points, the time complexity is $O(n\log n)$. As $M$ points of FFT coefficients that are selected to perform a peak detection process, the time complexity for peak detection is

$M$, where $M=150$ in our experiment. EI generation scheme includes an addition operation and a modulo operation on each feature point. The number of feature points depends on peak indexes detected, the time complexity of EI generation process is $O(\beta M)$, where $\beta$ is the rate between peaks detected and the FFT coefficients selected and thus $0<\beta<1$. The polynomial evaluation in key hiding process would require $48\times m(m+1)/2$ operations, so the time complexity of key hiding process is $48\times m(m+1)/2$. It is demonstrated by J.P. Berrut that the improved Lagrange interpolation, i.e., Barycentric interpolation, requires only $O(m)$ operations as opposed to $O(m^2)$ for evaluating the Lagrange basis individually. Therefore, the time complexity of key un-hiding process is reduced to $O(\binom{N_2}{m+1}m)=O(m)$, where $N_2$ is the number of feature points generated at the receiver. As $m$ and $M$ are fixed numbers, the time complexity of proposed solution can be expressed as $O(n\log n)$. From the FAR/FRR performance analysis we can see, the degree of polynomial to achieve minimum HTER is about 23. Thus, in order to realize the security of 128 bits, the vault size should be larger than 400. Excluding the dynamic occupied memory due to FFT process and randomized process, the primary static components of the memory required are the physiological features (9 bit values, about 48 for PPG and ECG for example) and their polynomial projects (12 bit values), chaff points (400 for example to realize the security of 128 bits, 9 bit x-values and 12 bit y-values). The overall memory required is 4.854KB.

Table 2 gives the detailed computational complexity of the TDPS-based and FDPS-based key distribution solution, separately. It can be seen that TDPS-based key distribution solution is superior in space complexity with only 84B of memory required, compared to 4.854KB for FDPS-based solution.

| Computational complexity | | | Task | Value |
|---|---|---|---|---|
| TDPS-based with fuzzy commitment | Time complexity $O(n+N^2)$ | Transmitter $O(n+N^2)$ | R-wave detection | $O(n)$ |
| | | | IPI_based EI generation process | $O(N^2)$ |
| | | | Error correction encoding | $O(N.q)$ |
| | | Receiver $O(N^2)$ | Error correction decoding | $O((N.q)^2)$ |
| | Static space complexity (84B) | Transmitter (34B) | $\hat{K}\oplus EI$ | 18B |
| | | | hash(K) | 16B |
| | | Receiver (50B) | $F(\hat{K}, EI)$ | 34B |
| | | | $EI'$ | 16B |

| Computational complexity | | | Task | Value |
|---|---|---|---|---|
| FDPS-based with fuzzy vault | Time complexity $O(n\log n)$ Static space complexity (4.854KB) | Transmitter $O(n\log n)$ | FFT computation | $O(n\log n)$ |
| | | | Peak detection | $M = 150$ |
| | | | Randomized process | $O(\beta M)$ |
| | | | Key hiding | $48 \times m(m+1)/2$ |
| | | Receiver $O(m)$ | Key un-hiding (Polynomial reconstruction) | $O(\binom{N_2}{m+1} m) = O(m)$ |
| | | Transmitter (2.302KB) | Chaff points (i.e. 400) | 2.05KB |
| | | | Feature points (i.e. 48) | 252B |
| | | Receiver (2.552KB) | Vault (i.e. 448) | 2.302KB |
| | | | Feature points (i.e. 48) | 252B |

**Table 2.** Computational complexity

## 4. Conclusion

In the biometrics solution for BSN security, physiological signals within human body are used to generate dynamic EIs, which is not only used to realize node identification, but also protect the transmission of keying materials. In this chapter, the procedures of biometric solutions for securing BSN, including the EI generation scheme and relevant key distribution solution, have been described. From the experimental results we can see that, TDPS-based EI generation scheme is superior in randomness and recognition performance, while FDPS-based scheme has advantage on its real-time performance and robustness. The two common used fuzzy methods, including fuzzy commitment scheme and fuzzy vault scheme, also have their own advantages and disadvantages. Fuzzy commitment can achieve low computation complexity and low memory occupied, but it is not suitable for EIs that are un-ordered or with different length. Fuzzy vault scheme can be suitable to most of cases, but with a high computation complexity and memory occupied. To realize high recognition performance, fuzzy commitment should be selected for TDPS-based EIs, called TDPS-based solution, while fuzzy vault for FDPS-based EIs, called FDPS-based solution. There are a lot of issues need to be further studied to make it applicable into practical BSN platforms.

The challenges of TDPS-based solution primary exist in the EI generation process, where a signal of about 30s is needed to generate a 128-bit EI. Firstly, how to increase the positive detection rate of R-wave with lower computational complexity or design a more robust EI generation scheme being little influenced by the precision of R-wave should be studied to in-

crease the robustness performance of the solution. Secondly, a faster EI generation scheme based on minimum number of IPIs should be addressed to increase its real-time performance.

For FDPS-based solution, the randomness performance of generated EIs, the computational complexity and the recognition rate pose great challenges to its application. Because the less satisfying randomness performance of EIs would bring about the security issue to the overall solution, how to make generated EIs as random as possible while not affecting its recognition rate is an issue should be addressed. In addition, the high computational complexity especially the space complexity brought by large amount of chaff points should be decreased to satisfy the stringent restriction of processing power, memory and energy for most sensor nodes. And what is the most important is that the recognition rate shall be significantly increased to make the solution applicable.

In some cases, not all of the physiological sensors that need to communicate with each other can obtain the needed information, such as IPI or same kind of physiological signals. Thus, how to extract a common feature from other kinds of physiological signal, such as respiration and blood pressure, might be further studied.

## Author details

Fen Miao, Shu-Di Bao and Ye Li

Key Laboratory for Biomedical Informatics and Health Engineering, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China

## References

[1] J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg (2005). *An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule*, Nat. Inst Stand. Technol., NIST Spec. Publ. 800-66, Gaithersburg, MD.

[2] The European Parliament and the council of The European Union (Jul. 2002). *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector,* Official J. Eur. Communities, pp. L201/37-47.

[3] L. Eschenauer and V. Gligor (2002). *A key-management scheme for distributed sensor networks*, Proceedings of the 9th ACM Conf. on Computer and Communication Security, pp.41–47.

[4] H. Chan, A. Perrig, D. Song (2003). *Random key predistribution schemes for sensor networks*, in: proceedings of the 2003 IEEE Symposium on security and privacy, May 11-15, pp. 197-213.

[5] D. Liu, P. Ning (2003). *Establishing pariwise keys in distributed sensor networks,* proceedings of the 10th ACM Conference on Computer and Communication, pp. 42-51.

[6] S. Cherukuri, K. K. Venkatasubramanian, S. K. S. Gupta (2003). *BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body,* Proc. IEEE International Conference Parallel Processing Workshop, pp.432−439.

[7] S. D. Bao, Y. T. Zhang, and L. F. Shen (2005). *Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems,* Proc. 27th IEEE Int'l. Conf. Eng. Med. and Bio. Soc., Shanghai, China.

[8] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, and L. F. Shen (2008). *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.

[9] Fengyuan Xu, Zhengrui Qin et al, *IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian,* IEEE INFOCOM 2011.

[10] C. C. Y. Poon, Y. T. Zhang, S. D. Bao (2006). *A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health,* IEEE Communication Magazine, pp.73-81.

[11] K. K. Venkatasubramanian, A. Banerjee, S. K. S. Gupta (2008). *Plenthysmogram-based secure inter-sensor communication in body sensor networks,* Proc. of IEEE Military Communiations, pp.1−7.

[12] K. K. Venkatasubramanian, A. Banerjee, S. K. S. Gupta (2010). *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.

[13] F. Miao, L. Jiang, Y. Li, Y. T. Zhang (2009). *Biometrics based novel key distribution solution for body sensor networks,* Proc. Annual Conference of IEEE-EMBS, pp.2458−2461.

[14] A. Juels, M. Wattenberg (1999). *A fuzzy commitment scheme,* Proceedings of 6th ACM conference on Computer and Communication Security.

[15] A. Juels, M. Sudan (2006). *A fuzzy vault scheme,* Design Codes and Cryptography, Vol. 38, no. 2, pp. 237-257.

[16] U. Uludag, S. Pankanti, A. K. Jain (2005). *Fuzzy vault for fingerprints,* In: Kanade T, Jai AK, Ratha NK. Proc. of the 5th Int'l Conf. on AVBPA. Berlin: Springer-Verlag, pp. 310−319

[17] Y. Wang, K. Plataniotis (2007). *Fuzzy vault for face based cryptographic key generation,* In: Proc. of the Biometrics Symp. Berlin: Springer-Verlag, pp. 1−6.

[18] Y. Lee, K. Bae, S. Lee, K. Park, J. Kim (2007). *Biometric key binding: fuzzy vault based on iris images,* In: Lee SW, Li SZ eds. Proc. of the ICB 2007. LNCS 4642, Berlin: Springer-Verlag, pp.800−808.

[19] F. Miao, S. D. Bao, Y. Li (2010). *A Modified Fuzzy Vault Scheme for Biometrics-based Body Sensor Networks Security,* IEEE Globecom.

[20] S. D. Bao and Y. T. Zhang (2005). *A new symmetric cryptosystem of body area sensor networks for telemedicine,* in 6th Asian–Pacific Conference on Medical and Biological Engineering.

[21] Miao, F., Bao, S. D., & Li, Y. A Novel Biometric Key Distribution Solution with Energy Distribution Information of Physiological Signals for Body Sensor Networks Security. IET Information Security. Accepted.

[22] J.P. Berrut, L. Trefethen. *Barycentric Lagrange Interpolation.* SIAM Review 46 (3): 501–517,2004.

[23] Lin Yao, Bing Liu, Guowei Wu et al. *A Biometric Key Establishment Protocol for Body Area Networks, International Journal of Distributed Sensor Networks*, 2011.

IntechOpen