31st Annual International Conference of the IEEE EMBS
Minneapolis, Minnesota, USA, September 2-6, 2009

Biometrics Based Novel Key Distribution Solution for Body Sensor Networks

Fen Miao, Lei Jiang, Ye Li and Yuan-Ting Zhang, *IEEE Fellow*

***Abstract*—The security of wireless body sensor network (BSN) is very important to telemedicine and m-healthcare, and it still remains a critical challenge. This paper presents a novel key distribution solution which allows two sensors in one BSN to agree on a changeable cryptographic key. A previously published scheme, fuzzy vault, is firstly applied to secure the random cryptographic key generated from electrocardiographic (ECG) signals. Simulations based on ECG data from MIT PhysioBank database, produce a minimum half total error rate (HTER) of 0.65%, which demonstrates our key distribution solution is promising compared with previous method, with HTER of 4.26%.**

***Keywords*— BSN, Biometrics, Fuzzy Vault, Security**

I. INTRODUCTION

The development of telemedicine and m-health is an effective solution to relieve the contradictions between the huge demand and the lack of physicians, which arises from the increasing aging population and chronic patients. The Body Sensor Network (BSN), which can be used as the terminal part in telemedicine, should be developed. As is shown in Fig. 1, a typical BSN consists of some biomedical sensors and a personal server, which works as a signal collector. The physiological signals collected by different sensors, will be sent to the personal server and then to external networks for remote diagnosis. As a result, it is very important that the personal medical and health information collected by the biosensors should be kept in privacy [1]. In another word, how to protect the physiological data against eavesdropping, injection, and modification, is a critical problem that should be seriously considered in BSN. That is, the security issues of BSN should never be ignored.

There are a lot of works about the generic sensor networks. Perrig et al. [2] presented a set of protocols that satisfy the requirements of security, such as confidentiality and authenticity for traditional sensor networks. Unfortunately, the traditional security scheme can't be used in BSN directly because biosensors are limited in battery lifetime, computation and communication capabilities, especially for those biosensors implanted in human body. Thus novel specific security mechanisms must be developed for BSN.

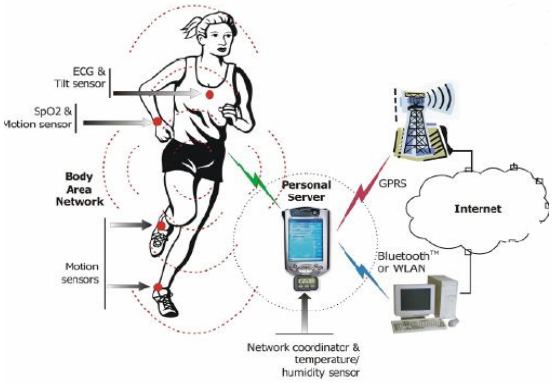

Fig.1 System model

A novel biometric solution was firstly presented in [3] to resolve the security problem in BSN. The biometrics solution is superior in low power consumption and computation complexity. Biometrics used in this study refers to the technology of measuring and analyzing the physiological data within the human body for authentication purposes. It is different from traditional biometrics, where the patterns used are captured on a specific part of the body surface, such as finger prints, eye retinas and irises, voice patterns, facial patterns, and hand measurements. There are still many issues referred to biometrics technology which should be studied such as effective key distribution method between two sensors. However, previous works on key distribution method have lower flexibility and higher half total error rate (HTER).

This paper focuses on the security of key distribution in BSN (see Fig. 1). A novel biometrics based key distribution solution, which allows two sensors in a BSN to agree on a changeable cryptographic key, is proposed. Compared with traditional scheme, our solution is superior in security performance, HTER and flexibility, which can be verified from our experiments.

The remainder of this paper is organized as follows. Section II provides a brief review of the related work. The details of the proposed methods are proposed in section III. In section IV, we present the experimental results based on the MIT PhysioBank database, and demonstrate the effectiveness of our solution. Section V provides conclusion and future works.

II. RELATED WORK

There is not much biometrics related work done on the security of BSN. Cherukuri et al [3] suggested to use

The authors are with the Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen, 518067, China (e-mail: fen.miao@sub.siat.ac.cn; lei.jiang@sub.siat.ac.cn; ye.li@sub.siat.ac.cn).

Yuan-Ting Zhang is both with the Shenzhen Institute of Advanced Technology Chinese Academy of Sciences, Shenzhen, 518067, China, and with Biomedical Engineering at the Chinese University of Hong Kong, Hong Kong, China (e-mail: ytzhang@ee.cuhk.edu.hk) .

physiological parameters with higher level of entropy (e.g., blood glucose, blood pressure, temperature) to generate the key for data encryption and decryption. Unfortunately, further detailed work hasn't been done. The timing information of heart-beats was adopted as biometric trait due to its chaotic nature. Building upon this initial idea, the authors in [4] [5] [6] propose the use of Inter-Pulse-Interval (IPI) to generate cryptographic keys. Since the biometric traits are captured at different parts of the body and have slight variations, a fuzzy commitment scheme [7] was suggested to overcome the variation and increase the tolerance. Based on the fuzzy commitment scheme and the secure key transmission in [8], a key distribution scheme was proposed by Bao et al. [9]. The scheme has error-tolerant capability while ensuring the security of key transmission. Though the IPI meets all the requirements as biometrics, it has a principal drawback that it will take about half a minute of measurement to generate relevant key, which makes it considerably slow for the real-time requirements of BSN. The authors in [10] proposes a novel ECG-based key agreement method based on the frequency domain of ECG, a measurement for 5 second of ECG is enough to generate a key, it can satisfy the real-time requirements of BSN.

Further, the effectiveness of using error correction codes to tolerant large variations is yet to be studied. The former fuzzy commitment scheme requires a strict correspondence of features in terms of order. To overcome this problem, Juels and Sudan [11] introduced the fuzzy vault scheme. The fuzzy vault scheme offers attractive properties in terms of security (proven information-theoretic secure), changeable key (generated randomly), and flexibility (working with unordered set). So it is a good candidate for biometrics based cryptographic systems. In this paper, the fuzzy vault scheme is firstly used in BSN security.

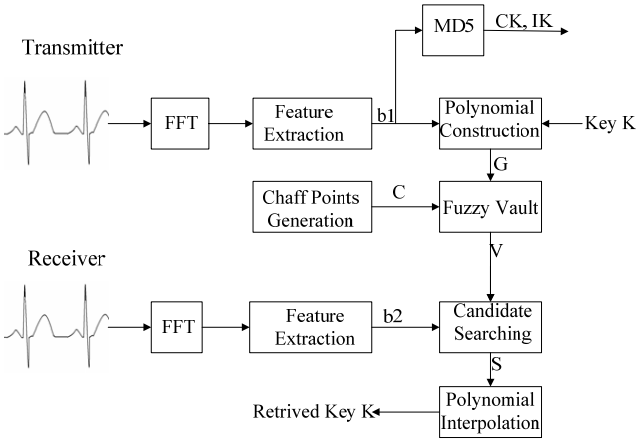

Fig. 2 Block diagram of proposed method

III. PROPOSED SOLUTION

In this section, the ECG based key generation and distribution method is presented for BSN. Fig. 2 depicts the block diagram of the proposed solution. A set of biometrics features is first extracted from the ECG signals. The extracted features are then quantized and mapped to binary representation for feature points matching. The produced binary features and the randomly generated key from ECG are bound by fuzzy vault scheme to ensure the security of the cryptographic key.

3.1 Feature Extraction and key generation method

In this paper, the frequency domain analysis of ECG signals is adopted to generate the features [10]. This is because the frequency components of physiological signals, at any given time, have similar values irrespective of where they are measured on the body. A time-domain analysis showed that the values of two ECG signals measured at different parts of the body (at different leads) have similar trend but diverse values. The feature generation is executed by the two sensors, by sampling the ECG signal simultaneously, at a specific sampling rate for a fixed duration of time (360Hz and 3 seconds, respectively in our case). In order to remove measurement artifacts, the signal is smoothed by removing the frequency components that do not contribute much to the overall power of the signal. The 3 second sample of the ECG signal (producing 1080 samples) is then divided into 3 parts of 360 samples each. A Fast Fourier Transform (FFT) is then performed on each of these parts. The first 180 FFT coefficients (due to the symmetric nature of the spectrum) of each of the 3 parts are concatenated to form a feature vector F of 540 coefficients.

To extract features from F, it is then quantized into a binary stream. By this way, we divide F into 20 blocks each containing 27 coefficients. The 27 coefficients in each block are then quantized into binary. We choose to quantize F in small blocks in order to capture the small variations in spectrum. The quantization produces 4 bit binary value for each coefficient, resulting in 20, 108 bit blocks $b_{1i}(i = 1, 2, ...20)$ and $b_{2i}(i = 1, 2, ...20)$ at each of the communicating sensors.

Key generation is a very important factor in security solution, and generally costs much computational resource. In our biometrics-based cryptosystem, the information of physiological signals is not only used to generate 'witness' to ensure the secure transmission of the key, but also utilize to generate the key. Once the feature vector $b_i(i = 1, 2, ...20)$ has been generated at an arbitrary sensor, it can be used to form the basis of the final key, including cipher key *CK* and integrity key *IK* . In our solution, each block is hashed by a one-way hash function to generate relevant keys. The commonly used hash functions, such as MD5 and SHA256, are adopted in our design to generating the key with a length of at least 128bits.

3.2 Key distribution method

Secure communication between sensors in BSN requires the presence of identical cryptographic keys at the communication units. In this section we present an ECG based key distribution method for enabling two sensors in a BSN to agree upon a common key.

3.2.1 Fuzzy vault scheme

Juels and Sudan [11] proposed to use Reed-Solomon (RS) codes for error correction. In this paper, a similar scheme

proposed in [12] is adopted for fuzzy vault encoding and decoding.

The fuzzy vault matching process in our solution is comprised of the following steps.

The transmitter:

Step1: Create an 8-order polynomial $f(x)=c_8x^8+c_7x^7+\cdots c_1x+c_0$ by encoding the secret 128-bit K as the coefficients c_0-c_8. The bit string K is the initial key in our cryptosystem that needs to be protected and linked with the biometric signal.

Step2: Project extracted feature $b_{1i}(i=1,2,...M)$ onto the polynomial to generate vault points $G=\{X_{1i},f(X_{1i}),i=1...M\}$, where X_{1i} is an integer number corresponds to the binary feature b_{1i}.

Step3: Randomly create chaff point set $C=\{(a_j,b_j),j=1...N_c\}$, where N_c □ $M, a_j\neq X_{1i}$, and each pair does not lie on the polynomial, i.e., $b_j\neq f(a_j)$.

Step4: The final vault is constructed by taking the union of the two set $G\cup C$ and pass through a scrambler so that it is not clear which are the feature points and which are the chaff points $\{V=(\mu_k,\nu_k),k=1...M+N_c\}$.

The receiver:

Step5: Project extracted feature at the receiver $b_{2i}(i=1,2,...M)$ to the vault space and search for the matching in the fuzzy vault V. The candidate points set $\{S=(\mu_k,\nu_k),k=1...M\}$ will be generated in the receiver end.

Step6: The polynomial can be reconstructed as: $f(x)=\sum_{i=1}^{9}f_i(x)$ given an identified combination $\{(\mu_1,\nu_1),(\mu_2,\nu_2),...,(\mu_9,\nu_9)\}$ where $f_i(x)=\nu_i\prod_{j=1,j\neq i}^{9}\frac{x-\mu_j}{\mu_i-\mu_j}$.

Step7: The coefficients in the generated polynomial is mapped back and concatenated in the same order. The 128-bit binary string K can be retrieved if the decoding process is successful.

Based on the above steps, the simulation results for fuzzy vault matching process with 200 chaff points and 9 feature points are presented in Fig. 3. It can be observed that the same subject is well matched while the different ones are separated.

3.2.2 Key agreement method

The fuzzy vault scheme ensures the security of a random 128-bit binary string K. Now that keys CK and IK have been generated at the communication sensors, which is presented in section 3.1, they should be transmitted in a secure way. The block diagram of cryptographic key agreement is shown in Fig.4. To do so, the communication entities exchange the following messages:

$$s1\rightarrow s2:<R=(U=K\oplus CK,MAC(K,U))>$$

Here $s1$ is the transmitter sensor and $s2$ is the receiver sensor, CK is the cryptographic key generated at the transmitter, MAC is the message authentication code, which will be used to detect adversaries. The receiver first verifies the MAC when the message is received. If the verification is successful, the node extract CK by XOR-ing K, which is derived from the fuzzy vault decoding process, with U. If the process is successful, the key CK can be derived, otherwise not. The same process is done on the integrity key IK.

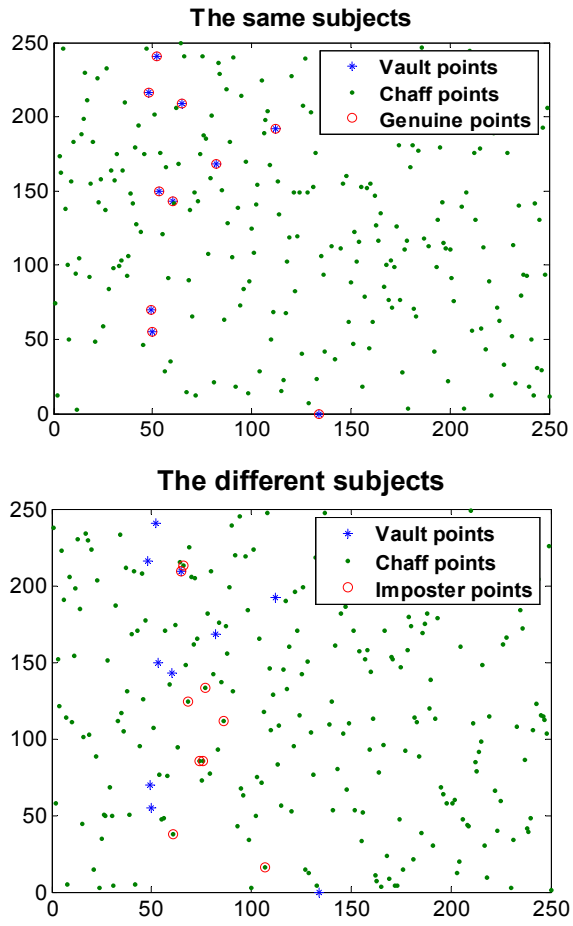

Fig.3 Demonstration of fuzzy vault matching

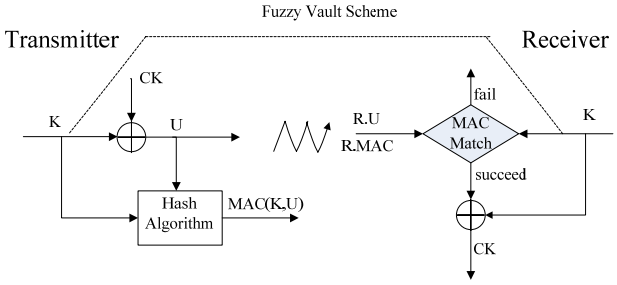

Fig.4 Block diagram of cryptographic key agreement

IV. EXPERIMENTAL TESTING RESULTS

To evaluate the performance of proposed methods, we conducted our experiments based on MIT PhysioBank

database (http://www.physionet.org/physiobank/). Each data was sampled at 360Hz, there is one ECG value every 3 msec.

Similar to the generic biometric verification systems, we evaluated the performance of the proposed biometric approach by three types of errors: false accept rate (FAR), false reject rate (FAR) and the half total error rate (HTER=1/2(FAR+FRR)). The binary features $b_{1i}(i=1,2,...20)$ and $b_{2i}(i=1,2,...20)$ are extracted from sensors that are about to communicate. The experiments are performed on $M=9-20$ number of binary features of 30 subjects, with 200 chaff points. Fig. 5 depicts the receiver operating curve as the function of M. It can be observed that as the M increases, FAR increase and FRR decrease. The selected polynomial requires 9 matched points. If the number of available points increases, the possibility of matching will increase. Table I details the obtained error rates with respect to different number of binary features M of 30 subjects. In our experiments, the best results obtained in terms of HTER is 0.65%, with FAR=0.8% and FRR=0.5%, at M=19. Compared with traditional solution in [13] with HTER of 4.26%, while FRR=6.46% and FAR=2.06%, it is clear that the proposed method produces promising results in terms of HTER. The simulation results demonstrate that the fuzzy vault scheme is superior in biometric based security application.

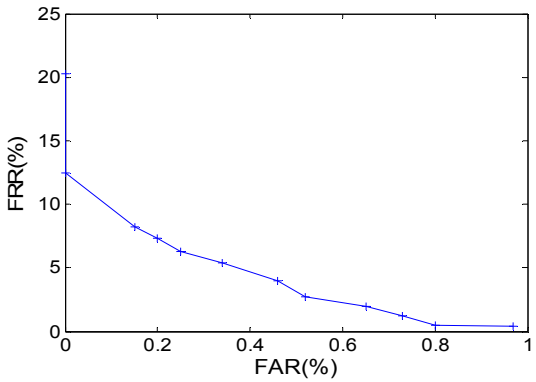

Fig.5 Receiver operating as a function of M

TABLE I. Error rates (%) obtained with different M

		FRR	FAR	HTER
M	9	20.25	0	10.125
	10	12.45	0	6.225
	11	8.25	0.15	4.2
	12	7.35	0.20	3.775
	13	6.28	0.25	3.265
	14	5.4	0.34	2.37
	15	4	0.46	2.23
	16	2.7	0.52	1.61
	17	2	0.65	1.325
	18	1.25	0.73	0.99
	19	0.5	0.80	0.65
	20	0.42	0.97	0.695

V. CONCLUSION AND DISCUSSION

In this paper, the fuzzy vault scheme is firstly applied to biometrics based key distribution solution in BSN. A set of biometric features are extracted from the ECG signals in frequency domain. The extracted binary features and the randomly generated keys from ECG are bound by fuzzy vault scheme to ensure the security of the cipher keys. Experiment results on real ECG data of MIT PhysioBank database produces a minimum HTER of 0.65%, which shows that our scheme is promising compared with previous method, with HTER of 4.26%.

In the future, we will implement the scheme on BSN development kit with a reasonable number of nodes, and then analyze the performance of our scheme in terms of security and power consumption.

REFERENCES

[1] Health Insurance Portability Accountability Act (HIPAA)

[2] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security Protocols for Sensor Networks", in Proceedings of the 7th Annual International Conference on Mobile Computing and Networks (MOBICOM 2001), July 2001.

[3] 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," Proc. IEEE Int'l Conf. Parallel Processing Wksp., 6–9 Oct. 2003, pp. 432–439

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, Vol. 47, No. 6, June 2004. W.-K. Chen, Linear Networks and Systems (Book style).Belmont, CA: Wadsworth, 1993, pp. 123–135.

[5] J. Bhattacharya, R. P. Kanjilal, "Assessing determinism of photoplethysmographic signals", IEEE Trans. On Systems, Man, and Cybernetics-part A systems and humans, vol. 29, pp. 406-410, 1999.

[6] S. D. Bao, Y. T. Zhang, L. F. Shen, "A New Symmetric Cryptosystem of Body Area Sensor Networks for Telemedicine", in Proc. 6th Asian-Pacific Conference on Medical and Biological Engineering, 2005.

[7] A. Juels, M. Wattenberg, "A Fuzzy Commitment Scheme", in Proceedings of 6th ACM conference on Computer and Communication Security, 1999.

[8] S. D. Bao, Y. T. Zhang, and L. F. Shen, "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, Sept. 2005

[9] S. D. Bao, L. F. Shen, Y. T. Zhang, "Biometrics Based Security Solution for Wireless Body Area Sensor Networks", in Proc. Dynamics of Continuous Discrete and Impulsive Systems, 2005.

[10] Krishna Kumar Venkatasubramanian,Ayan Banerjee, and Sandeep K.S Gupta, "EKG-based Key Agreement in Body Sensor Networks", IEEE,2008.

[11] A. Juels, and M.Sudan, "A fuzzy vault scheme", Proc. Of IEEE Int. Symp. On Info. Theory, pp. 408, 2002.

[12] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for finger-prints", Proc. Of Int. conf. on Audio and Video based Biometric Person Auth., pp. 310-319, 2005.

[13] Carmen C. Y. Poon, Yuan-Ting Zhang, and Shu-Di Bao, "A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health", IEEE Communication Magazine, vol. 44, no. 4, pp. 73-81, 2006.