35th Annual International Conference of the IEEE EMBS
Osaka, Japan, 3 - 7 July, 2013

A Compensation Method to Improve the Performance of IPI-based Entity Recognition System in Body Sensor Networks

Shu-Di Bao, *Member*, *IEEE*, Zhong-Kun He, Rong Jin, and Peng An

***Abstract*—Security of wireless body sensor networks (BSNs) with telemedicine applications remains a crucial issue. A family of novel biometrics schemes has been recently proposed for node recognition and cryptographic key distribution without any pre-deployment in BSNs, where dynamic entity identifiers (EIs) generated from physiological signals captured by individual sensor nodes are used for nodes to recognize each other. As the recognition performance of EIs determines the maximal performance that can be achieved in such biometric systems, several kinds of EI generation schemes have been proposed. The inter-pulse intervals based EI generation scheme is more promising for such applications in actual scenarios because of its acceptable recognition performance. However, it was found that such generated EIs by true pairs of nodes, i.e. two nodes from the same BSN, have some error pattern which could be considered while doing node recognition or key distribution for an improved success rate. To address the problem, this work proposes an error-correcting code based compensation method which can be easily combined together with the key distribution process to achieve an improved recognition performance. Results of statistical analysis with experimental data collected from 14 subjects show that the bit difference between EIs from true pairs of nodes can be effectively reduced with the proposed method.**

I. Introduction

Mobile health technology used to manage chronic and acute conditions will become ubiquitous across healthcare infrastructures. As a front-end platform for physiological data collection in mobile health systems, body sensor network (BSN) enables wireless communications between several miniaturized body sensor units and a single body central unit worn at the human body [1]. To protect the vital medical information from unauthorized usage for personal advantage or fraudulent acts, a family of novel biometrics methods [2-13] has been recently proposed to achieve automatic node recognition and cryptographic key distribution without any pre-deployment in BSN.

Different from traditional biometrics, which refers to the automatic recognition of individuals based on their physiological or/and behavioral characteristics [14], the biometrics method concerned in this study is to make use of the communication channels already available on or in the human body, i.e., the bio-channels, for securing wireless communications within BSN. To be brief, it is achieved by generating dynamic entity identifiers (EIs) from physiological data collected in real time at each node, which are then used for node recognition as well as key distribution. A biometric trait that can be used for securing BSN must be distinctive and time-variant. The trait should be sufficiently different on any two individuals when copies of it are captured simultaneously. At the same time, it should change with time and have a high degree of randomness so that copies of it captured at different times would not match even if they are obtained from the same individual. As EIs generated from physiological data simultaneously captured at different locations of the body using different sensors have slight variations, fuzzy schemes, such as fuzzy commitment scheme and fuzzy vault scheme [15-16], have to be deployed to ensure that nodes in the same BSN can recognize each other. To improve the recognition performance of the system, a better matching performance of biometric EIs generated at different nodes of BSN is strongly desired.

The existing schemes of biometric EI generation utilize the cardiovascular signals that are readily available in body sensors for health monitoring. Both time domain and frequency domain information of cardiovascular signals have been studied. It was reported that the inter-pulse intervals (IPI) based EI generation scheme, compared to others, is more promising for such applications in actual scenarios because of its good recognition performance compared to other generation schemes. However, it was also found that the error distribution of such generated EIs from true pairs has a certain pattern, which could be taken into account for node recognition [17-18].

In this study, we aim to reduce the difference between IPI-based EIs from true pairs and thus improve the recognition performance of the system. The performance in terms of false acceptance rate and false rejection rate will be evaluated with experimental data collected from 14 subjects. The remainder of this paper is organized as follows. In Section II, the IPI based EI generation scheme and the error pattern of EIs from true pairs are briefly introduced. In Section III, the error-correcting code based compensation method is proposed, followed by experimental analysis in Section IV. A conclusion is finally given in Section V.

*Research supported by the National Nature Science Foundation of China (No. 61102087), Ningbo Nature Science Foundation (No. 2012A610024 & No. 2011A610186), and Shenzhen Key Basic Research Program (No. JC201005270257A).

S. D. Bao is with Ningbo University of Technology, Ningbo 315016, China, and Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China (phone: 86-574-87081299; e-mail: sdbao@ieee.org).

Z. K. He, R. Jin and P. An are with Ningbo University of Technology, Ningbo 315016, China (e-mail: hzk@nbut.cn; rong_jin@163.com; anp04@126.com).

II. IPI-BASED EI GENERATION SCHEME AND TRUE-PAIR ERROR ANALYSIS

A. IPI-based EI Generation Scheme

The generation scheme of network-wide IPI based EIs is depicted in Fig. 1 [7]. To begin with, a node in BSN, usually the master node with less resource constraint, sends out a synchronization signal indicating the beginning of network-wide EI generation. Upon receiving the synchronization signal, other nodes in the same BSN begin to record at least one cardiovascular signal. The initiating node also begins the signal recording at the same time. Each node calculates a sequence of IPIs (unit in millisecond) from its own recorded cardiovascular signal, which can be denoted as $\{IPI_i \mid 1 \le i \le L\}$. Afterwards, an accumulation operation is performed to the sequence of IPIs followed by modulo operation, i.e. $(mIPI_i) \bmod (2^p)$. To compensate measurement differences among nodes in the same BSN, the modulo result is further transformed into a smaller integer by a contraction mapping

$\hat{f} : [0,2^p) \to [0,2^q)$,

i.e. $\hat{f}(m) = \lfloor m / 2^{(p-q)} \rfloor$, where $m \in [0,2^p)$, $p > q$, and $\lfloor \cdot \rfloor$ returns the largest integer less than or equal to $m/2^{(p-q)}$. Finally, to increase the noise margin of measurements, the classical binary reflected Gray code scheme is employed to get binary EIs.

The generated EI can be expressed as $EI = I_1 \| I_2 \cdots \| I_{L-1} \| I_L$, where $\|$ is a concatenation operation. Each block of EI, i.e. I_i, is originally generated from a corresponding multi-IPI ($mIPI_i$). The bit length of I_i is q, and thus the bit length of EI is $L \cdot q$.

B. Error Patten between True-Pair EIs

In this content, true-pair EIs means they are synchronously generated by two nodes within the same BSN, and all other pairs of EIs are false-pair EIs, including those generated by two nodes from different BSNs or those asynchronously generated by nodes within the same BSN. In the IPI-based EI generation scheme, the employment of Gray code is important to reduce the bit errors between true-pair EIs due to its specific feature, i.e. there is only one bit changes state between neighboring codewords. Table I shows the probability at which the bit changes state between neighboring codewords, from which it can be seen that the least significant bit has the largest probability of state changing while comparing any pair of neighboring codewords. Analysis results with experimental data were consistent with the theoretical values. For example, while q was set to 3 or 4, the probability that every q^{th} bit of EIs from true pairs happened to be different from each other was quite large, which however is not desirable.

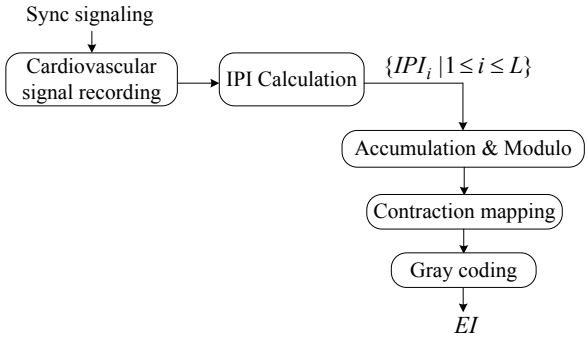

Figure 1. Generation scheme of binary biometric EIs from IPIs[7]

TABLE I. THEORETICAL PROBABILITY OF BIT CHANGING STATE BETWEEN NEIGHBORING CODEWORDS

Bit Length of Gray Code	Probability of Bit Changing State (left: the most significant bit)
4	(2, 2, 4, 8)/16
3	(2, 2, 4)/8
2	(2, 2)/4

C. Distance Analysis of True-Pair EIs

To further check the difference between true-pair EIs, a statistical analysis of bit differences between true-pair EIs was carried out with the experimental data involving 14 health subjects. Details of the experimental protocol can be found in Section IV. Results of statistical analysis were obtained based on every EI block, i.e. I_i mentioned in Section II.A. Fig. 2 shows some of the results while the parameter q of EI generation scheme was set to 4. As can be seen from the figure, most blocks of true-pair EIs have no more than 1-bit difference. Therefore, the aim of this study is to find a method to effectively compensate the single bit difference between true-pair EI blocks.

III. METHOD

Suppose there are two nodes communicating with each other, each of which has generated its own binary EIs with the scheme described in Section II.A. The basic idea behinds the compensation method is to make use of error-correcting code to correct the single bit with different values between two synchronous EI blocks.

Let $C_i(n,k)$ represent an error-correcting code with ω bits of error-correcting ability, where the lengths of codewords and information bits are n and k, respectively. I_i and I_i' with a bit length of q represent two synchronous blocks of EIs from a true pair of nodes, where q is the

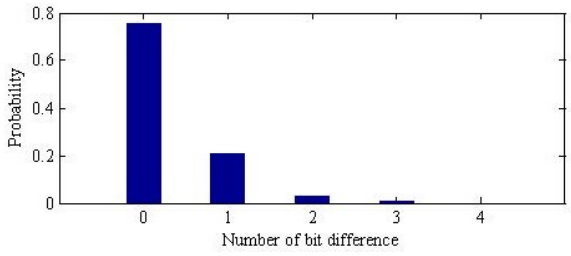

Figure 2. Statistical results of bit difference between true-pair EI blocks (q=4)

parameter q in the above mentioned EI generation scheme. The relationship between these parameters is that

$$\begin{cases} k = q \\ n = \omega \cdot k \end{cases} \tag{1}$$

The process of single-bit error compensation for each EI block is described as follows. Firstly, one of the two nodes, noted as A, sends out a binary sequence m_A with a bit-length of $L \cdot n$, i.e.,

$$\begin{aligned} m_A = & (\overbrace{I_1 \| \cdots \| I_1}^{\omega}) \oplus c_1(n,k) \\ & \cdots \\ & \| (\overbrace{I_i \| \cdots \| I_i}^{\omega}) \oplus c_i(n,k) \\ & \cdots \\ & \| (\overbrace{I_L \| \cdots \| I_L}^{\omega}) \oplus c_L(n,k) \end{aligned} \tag{2}$$

where L is the number of EI blocks, i.e., the number of IPIs used to generate EI, and each error-correcting code $c_i(n,k)$ is randomly selected.

Upon receiving the message m_A, the other node, noted as B, starts to compensate any single-bit difference for each block of its own EI by the following steps. Firstly, it separates the received binary message m_A into L segments and also prepares the L segments of its own EI. Then it does binary XOR operation for each EI block, i.e.,

$$\begin{aligned} & ((\overbrace{I_i \| \cdots \| I_i}^{\omega}) \oplus c_i(n,k)) \oplus (\overbrace{I'_i \| \cdots \| I'_i}^{\omega}) \\ & = (\overbrace{I_i \oplus I'_i \| \cdots \| I_i \oplus I'_i}^{\omega}) \oplus c_i(n,k) \end{aligned} \tag{3}$$

According to the results of XOR operation, the node B is able to estimate the number of different bits between I_i and I'_i, find out and then correct the bit of I'_i if there is only one-bit difference between the two blocks. Finally, all L segments with correction will be concatenated to obtain a corrected EI.

The compensation process is also depicted in Fig. 3. There are two aspects to be considered while designing the compensation process. On the one hand, the compensation must be effective, which needs accurate judgment on the single-bit errors. This will be demonstrated later by experimental data analysis in the next section. On the other hand, the security of EIs will never be compromised during the compensation process because $k = q$, i.e., the bit length of information of the error-correcting code must be no less than the bit length of EI blocks, which means the message m_A transmitted in the air interface does not expose information to any third-party.

IV. Performance Evaluation

A. Experimental Data

We used data collected from an experiment with 14 healthy subjects, the original purpose of which was to simultaneously capture electrocardiogram (ECG) and photoplethysmogram (PPG) for the estimation of blood pressure. ECG was captured from the three fingers of the subjects and two channels of PPG were captured from the index fingers of the two hands, respectively. For each subject, the three signals were captured simultaneously for 2–3 minutes. Fig. 4 depicts a segment of simultaneously captured ECG and PPG. Peak-to-peak intervals of ECG and foot-to-foot intervals of PPG were calculated.

B. False Acceptance–False Rejection Performance

False acceptance (FA, also known as false match) and false rejection (FR, also known as false non-match) were used to characterize the two aspects of EIs. Fig. 5 depicts the FA-FR curves of EIs generated by the IPI-based scheme with and without the proposed compensation method while q was set to 4, where false acceptance rate (FAR) was the rate at which two EIs generated from difference subjects or at a different time were matched, and false rejection rate (FRR) was the rate at which two EIs generated from the same subject

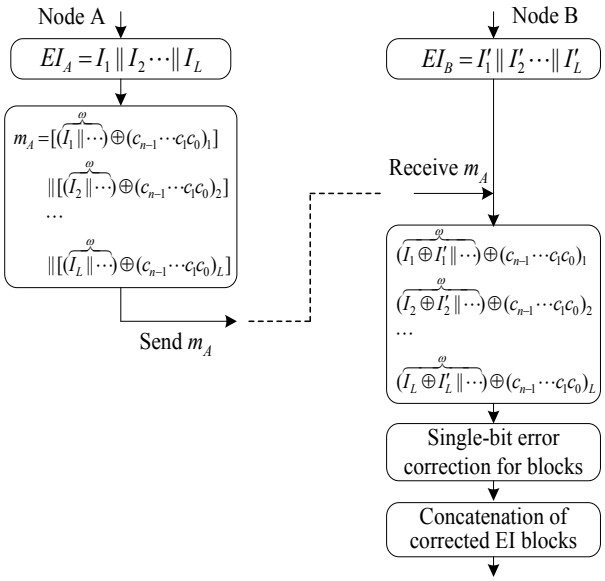

Figure 3. The compensation process for EI blocks

TABLE II. Minimum HTER Associated with Compensation Method for the Node Recognition System

Signals	Threshold (bit)		Mini. HTER (%)	
	w	w/o	w	w/o
ECG-PPG1	18	19	0.17	0.58
ECG-PPG2	16	18	0.50	1.02
PPG1-PPG2	18	19	0.78	1.82

Note: q=4; the bit length of EI is 64. 'w' and 'w/o' mean with or without the compensation method, respectively.

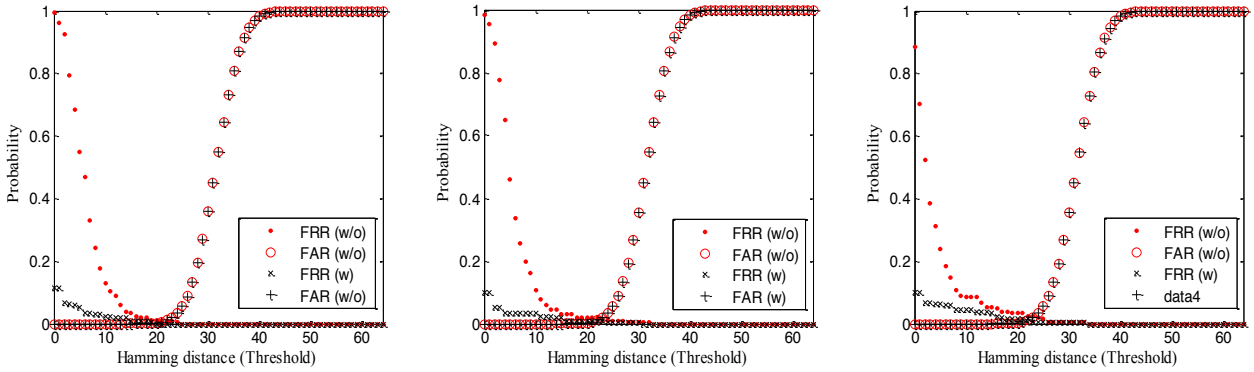

Figure 5. FA-FR curves of EIs with or without the proposed compensation method (q = 4). (a) ECG-PPG1. (b) ECG-PPG2. (c) PPG1-PPG2.

during the same period of time were unmatched. Table II shows the minimum half total error rate (HTER) that equals (FAR+FRR)/2. Compared to one of our previous studies that used the same set of raw data, this study was able to achieve a lower minimum HTER and thus a better recognition performance.

V. Conclusion

Physiological signals that are readily available at nodes of BSN can be used to generate dynamic entity identifiers for node recognition and cryptographic key distribution within the same BSN. The inter-pulse intervals based entity identifier generation scheme has its advantage in terms of recognition performance. However, it was found that such generated EIs of nodes from the same BSN have some error pattern which could be considered to further improve the recognition rate. In this study, we have proposed an error-correcting code based compensation method to address the error pattern problem of true-pair EIs generated by the IPI-based scheme. The results of our experimental analysis demonstrate the effectiveness of the proposed method in terms of single-bit difference elimination between synchronous blocks of true-pair EIs, which thus results in a better performance of node recognition.

Acknowledgment

This work thanks for the experimental data provided by the Joint Research Center for Biomedical Engineering, The Chinese University of Hong Kong.

References

[1] G. Z. Yang, *Body Sensor Networks*. London: Springer-Verlag, 2006, pp. 4–13.

[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," *Proc. IEEE Int'l Conf. Parallel Processing Workshop*, 2003, pp. 432−439.

[3] S. D. Bao, L. F. Shen, and Y. T. Zhang, "A novel key distribution of body area networks for telemedicine," *Proc. IEEE Int'l Workshop on Biomedical Circuits and Systems*, 2004, pp. 17–20.

[4] 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. Annual Conference of IEEE-EMBS*, Shanghai, China, 2005, pp. 2255–2258.

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

[6] S. D. Bao, C. Y. Poon, Y. T. Zhang, and L. F. Shen, "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, 2008, pp. 772–779.

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

[8] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in Body Sensor Networks," *Proc. INFOCOM Workshops*, 2008, pp.1−6.

[9] F. M. Bui and D. Hatzinakos, "Biometric Methods for Secure Communications in Body Sensor Networks: Resource-Efficient Key Management and Signal-Level Data Scrambling," *EURASIP Journal on Advances in Signal Processing*, 2008, pp.1−16.

[10] K. K. Venkatasubramanian, A. Banerjee, 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, 2010, pp. 60–68.

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

[12] F. Miao, S. D. Bao and Y. Li, "A modified fuzzy vault scheme for biometrics-based body sensor networks security," *Proc. IEEE Global Telecommunications Conference*, 2010, pp. 1−5.

[13] C. Z. Cao, C. G. He, S. D. Bao and Y. Li, "Improvement of fuzzy vault scheme for securing key distribution in body sensor network," *Proc. Annual Conference of IEEE-EMBS*, 2011, pp. 3563−3567.

[14] A. Ross, S. Pankanti, "Biometrics: a tool for information security," *IEEE Transaction on Information Forensics and Security*, vol. 1, no. 2, 2006, pp. 125–143.

[15] A. Juels, M. Wattenberg, "A fuzzy commitment scheme," *Proc. 6th ACM conference on Computer and Communication Security*, 1999, pp. 28–36.

[16] A. Juels, M. Sudan, "A fuzzy vault scheme," *Design Codes and Cryptography*, vol. 38, no. 2, 2006, pp. 237−257.

[17] T. Hong, S. D. Bao, Y. T. Zhang, and P. Yang, "An improved scheme of IPI-based entity identifier generation for securing body sensor networks," *Proc. Annual Conference of IEEE-EMBS*, 2011, pp. 1519−1522.

[18] S. D. Bao, "A Matching Performance Study on IPI-Based Entity Identifiers for Body Sensor Network Security," *Proc. IEEE Int'l Conf. on Biomedical Engineering and Informatics* , 2012.