33rd Annual International Conference of the IEEE EMBS
Boston, Massachusetts USA, August 30 - September 3, 2011

An Improved Scheme of IPI-based Entity Identifier Generation for Securing Body Sensor Networks

Tian Hong, Shu-Di Bao, *Member, IEEE*, Yuan-Ting Zhang, *Fellow, IEEE*, Ye Li, *Member, IEEE*, and Ping Yang, *Member, IEEE*

***Abstract*—Securing body sensor network (BSN) in an efficient manner is very important for preserving the privacy of medical data. Protecting data confidentiality, integrity and to authenticate the communicating nodes are basic requirements to secure BSN. The existing method to generate entity identifier (EI) from inter-pulse intervals (IPIs) of heartbeats has its advantages in authenticating and identifying nodes, which however was found in this study that such generated EIs are not so resistant to attacks because of potential error patterns. This paper presents an improved scheme of IPI-based EI generation to eliminate the error patterns. The performance of randomness and node identification, i.e. false acceptance rate and false rejection rate, is experimentally evaluated. The results indicate that compared with the existing one, the new scheme is effective to eliminate the error patterns and thus more tolerant to attacks, while there is no compromise on the randomness level and identification performance.**

I. Introduction

Body sensor network (BSN) has emerged as a new technology to provide continuous monitoring of a patient's physiological and contextual parameters by utilizing a network of miniaturized, low cost, wireless and wearable or implantable biosensors [1-2]. It will play an important role in future health system which has key trends include the evolution from disease centric to patient centric care, the delocalization of care from hospitals to home, and a focus on prevention rather than cure [3]. Instead of being measured face-to-face, health-related parameters of BSN's user can be monitored remotely, continuously, and in real time, which greatly increase the efficiency of healthcare.

As BSNs are basic platforms to collect and transmit sensitive health data, it is essential to ensure the security of them, especially their wireless communications. Failure to secure BSNs will possibly lead to violations of patient privacy, or even lead to wrong diagnosis and treatment [4]. It is a challenge to implement traditional security infrastructures in BSNs due to several limitations associated with BSNs such as computation, storage and bandwidth constraints. Biometrics method has been demonstrated as a promising way to efficiently secure wireless communications in BSN, where human body itself was taken as a communication channel of biological data [5-6]. As some of the biological data are unique to individuals while also time variant, they could potentially be an identifier of the owner of BSN.

The idea of using biometrics to secure inter-sensor communications was first introduced in [7]. Based on this initial idea, it was demonstrated in [8-10] that time-domain information, e.g. inter-pulse intervals (IPIs) of electrocardiogram (ECG) or photoplethysmograph (PPG), and frequency-domain information of cardiovascular signals can be used as biometric characteristic to generate entity identifier (EI) for node identification and also intra-network security in BSN. Because IPI can be readily collected from sensors with functions of cardiovascular signal detection, the use of such a kind of characteristic has advantages over frequency-domain information, which would require the same kind of signal to be collected and thus has more limitations for actual deployments.

In this paper, a statistical analysis will be carried out to check if there is any consistent error pattern of EIs generated from the existing method [11] using IPI as the biometric characteristic, which may lead to a reduced difficulty of attacks. EIs from both true pairs and false pairs will be statistically analyzed, where true pair means a pair of nodes that shall be expected to communicate with each other in the same BSN, while false pair means nodes from different BSNs. Based on the theoretical and experimental analysis, an improved scheme of IPI-based EI generation which is able to efficiently eliminate the error pattern will be proposed.

The remainder of this paper is organized as follows. In Section II, we briefly introduce the existing method to generate EIs from IPIs of heartbeats. In Section III, detailed statistical analysis method of error pattern is given, and error pattern of EIs generated from the existing method is analyzed with experimental data, followed by an improved scheme of IPI-based EI generation in Section IV. In section V, the performance evaluation of the improved scheme is carried out, including error pattern analysis, randomness level, as well as false acceptance rate and false rejection rate. Finally, conclusions are given in Section VI.

This work was supported in part by National Basic Research Program 973 (No. 2010CB732606), Key Basic Research Program of Shenzhen, China (No. JC201005270257A), and Guangdong Innovation Team Fund for Low-cost Health Technologies.

The authors are with the Institute of Biomedical and Health Engineering, Shenzhen Institutes of Advanced Technology, and Key Lab for Health Informatics, Chinese Academy of Sciences (email: tian.hong@siat.ac.cn, sd.bao@siat.ac.cn, ytzhang@ee.cuhk.edu.hk, ye.li@siat.ac.cn, ping.yang@siat.ac.cn)

Y. T. Zhang is also with the Joint Research Centre for Biomedical Engineering, Department of Electronic Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong.

Please direct correspondence to Dr. Bao (phone: +86-755-86392200; fax: +86-755-8639229; email: sd.bao@siat.ac.cn)

II. Related Works

It has been demonstrated that the hamming distance of EIs from nodes in different BSNs, or called false pairs, is quite large, while those simultaneously obtained by nodes in the same BSN, or called true pairs, is small enough [8-9]. Therefore, the EIs can be used for nodes to recognize if the peer end is with the same BSN as itself. The existing generation scheme of EI is depicted in Fig. 1. Firstly, nodes of the same BSN record one cardiovascular signal at the same time. Then each node calculates a series of IPIs from its own recorded cardiovascular signal, which can be denoted as $\{IPI_i | 1 \le i \le L\}$. After that, an accumulation operation is performed to the series of IPIs, followed by the modulo operation, i.e. $mIPI_i \pmod{2^p}$.

To compensate measurement differences among different nodes, the modulo result is further transformed into a smaller integer by a contraction mapping:

$$f(m) = floor(\frac{m}{2^{p-q}}), m \in [0, 2^p), q < p \tag{1}$$

where floor returns the largest integer less than or equal to $m / 2^{(p-q)}$. Finally, to increase the noise margin of measurement, the classical binary reflected Gray code is employed to get binary EIs.

The generated EI can be expressed as $EI=I_1|I_2|\ldots|I_L$, where | is a concatenation operation. Each block of EI, I_i, for example, is generated from a corresponding $mIPI_i$. The bit length of I_i is q, and thus the bit length of EI is $L \cdot q$ [11].

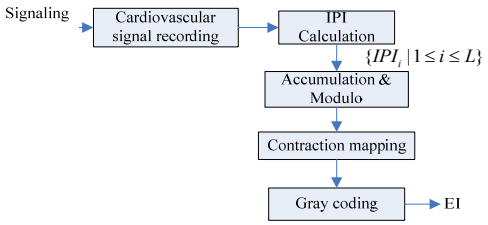


Fig. 1. The existing scheme of entity identifiers generation [10]

III. Error Pattern Analysis of Entity Identifiers

A. Method of Statistical Analysis

Because such generated EIs are used for node recognition as well as keying material protection, the performance study about EIs shall include pair-based error pattern while not only traditional biometrics evaluation method, i.e. false rejection rate (FRR) and false acceptance rate (FAR). The error pattern is defined as the bit pattern that EIs in binary simultaneously generated by nodes in the same BSN differs from each other, or EIs otherwise generated are identical to each other.

According to the definition of error pattern, there are two kinds of pair-based error pattern. One is the error pattern of EIs from true pairs, i.e. two EIs that are generated simultaneously by two nodes in the same BSN. Another is the error pattern of EIs from false pairs, i.e. two EIs that are generated from two different BSNs or at a different time.

In this study, a statistical analysis method will be carried out to evaluate pair-based error pattern of EIs. Given a data pool of EIs generated by the method described in Section II, the error pattern of EIs from true pairs is statistically analyzed as follows. Assume that there are in total T true pairs of EIs, denoted as $\{EI_i, EI_i'\}(1 \le i \le T)$, and each EI has a bit length of N and is denoted as $EI_{ik}(1 \leqslant k \leqslant N)$. The probability of bit error for true pairs is calculated as

$$e_1(k) = \frac{\sum_{i=1}^{T}(if(EI_{ik} \ne EI_{ik}'))}{T}, 1 \le k \le N \tag{2}$$

where the function $if(\cdot)$ returns 1 if the condition satisfies, or 0 otherwise. The result of $e_1(k)$ shows the probability that the two EIs from true pairs do not match each other at the k^{th} bit.

Assume that there are in total F false pairs of EIs, denoted as $\{EI_i, \widetilde{EI}_i\}(1 \le i \le F)$. The probability of bit error for false pairs is calculated as

$$e_2(k) = \frac{\sum_{i=1}^{F}(if(EI_{ik} = \widetilde{EI}_{ik}))}{F}, 1 \le k \le N \tag{3}$$

where the function $if(\cdot)$ is the same as above. The result of $e_2(k)$ shows the probability that the two EIs from false pairs match each other at the k^{th} bit.

Ideally, $e_1(k)$ shall be 0 if two EIs from true pairs match each other exactly, and $e_2(k)$ shall be 0.5 if the data pool is big enough. Therefore, it shall be expected that $e_1(k)$ is close to 0 while $e_2(k)$ is close to 0.5. Besides, there should be no consistent pattern both in $e_1(k)$ and $e_2(k)$.

B. Error Pattern Analysis of Entity Identifiers

The experimental data, including one-channel ECG and one-channel PPG, were captured from 10 subjects (aged 25.6±1.4 years). Both ECG and PPG were captured from the 10 subjects for a period of 5 minutes when they sat on a chair quietly, with a sampling rate at 1000 Hz and A/D resolution at 16 bit. For error pattern analysis of true pairs, EI pairs were generated from simultaneously segmented ECG and PPG signals captured from the same subject, while for error pattern analysis of false pairs; EI pairs were generated from ECG signals captured from two different subjects.

According to the analysis results reported in [10], we will focus on analyzing the effect of parameters p and q on the error pattern of EIs, while setting the value of L to 32. Based on the captured ECG and PPG signals, 100 true and false EI pairs were generated, respectively, i.e. T=100 and F=100. The results of $e_1(k)$ and $e_2(k)$ calculated by Equations (2) and (3), are shown in Fig. 2 and Fig. 3, respectively.

It can be seen from Fig. 2 that it happens consistently that the q^{th} bit of each q-bit block has a relatively high value of $e_1(k)$ regardless of the value of p. In other words, there is a high probability that every q^{th} bits of two EIs from a true pair cannot match each other, which however is not expected. On the other hand, there is no consistent error pattern for false pairs as expected. The calculated results are shown in Fig. 3.

IV. IMPROVED SCHEME OF IPI-BASED EI GENERATION

Though the consistent error pattern of EIs from true pairs does not reduce the randomness of entity identifiers, it will reduce the difficulty of attacks given the bit length of EI is fixed, and thus the security level to a certain extend. In other words, since it is with a significantly high probability that every q^{th} bit of EIs may not be matched for true pairs; attackers may not have to guess the values of those bits while trying brute-force attacks.

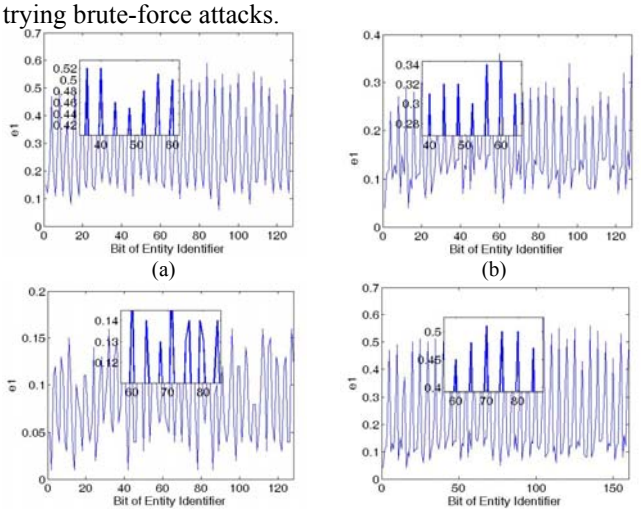


Fig. 2. Mismatched bits of entity identifiers from true pairs: (a) p=7, q=4; (b) p=8, q=4; (c) p=9, q=4; (d) p=8, q=5.

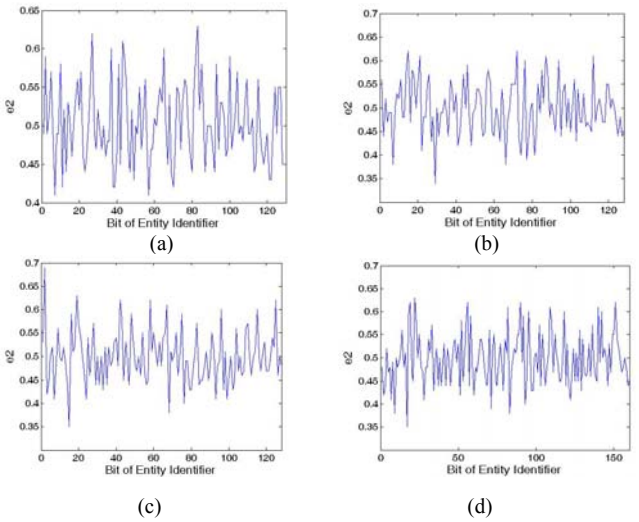


Fig. 3. Matched bits of entity identifiers from false pairs: (a) p=7, q=4; (b) p=8, q=4; (c) p=9, q=4; (d) p=8, q=5.

To address this problem, an improved scheme of EI generation is proposed to eliminate the error pattern, as illustrated in Fig. 4. Based on the existing EI generation scheme described in Section II, after gray coding, a 2-bit random number generated from two consecutive IPIs is used to reorder I_i and I_{i+1}, which are generated from corresponding $mIPI_i$ and $mIPI_{i+1}$. The reordering result is denoted as I_i', and the EI generated by this improved scheme can be expressed as $EI = I_1' \,|\, I_2' \,|\cdots|\, I_L'$.

Each random number is generated from two consecutive IPIs and used to control the reordering of the Gray code, which is however directly concatenated to generate EI in the existing method. Firstly, a mean value of the L IPIs, denoted as m, is calculated. Then each of the L IPIs is compared with m, if the value of IPI_i is greater than m, the coding result is 1, or otherwise 0. Each two consecutive coding bits are concatenated to be a 2-bit random number.

The 2-bit random number is then used to control the reordering of I_i and I_{i+1}. In other words, a 2-bit random number is used twice for reordering of two Gray codes in the same way. The reordering is actually the exchange of two bits, i.e. the lowest significant bit and the bit that the random number selects. For example, if the random number is '10', it means that the lowest significant bit, i.e. 1st bit, and the 3rd bit will be exchanged.

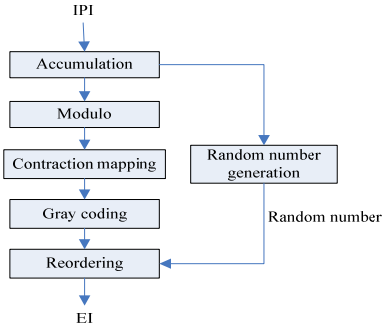


Fig. 4. Improved scheme of IPI-based entity identifier generation

V. PERFORMANCE EVALUATION OF THE IMPROVED SCHEME

The same experiment data as described in Section III is used to evaluate the performance of entity identifier generated by the improved scheme. For simplicity, here the parameters are set as L=32, p=8, and q=4.

A. Error Pattern Analysis of Entity Identifiers

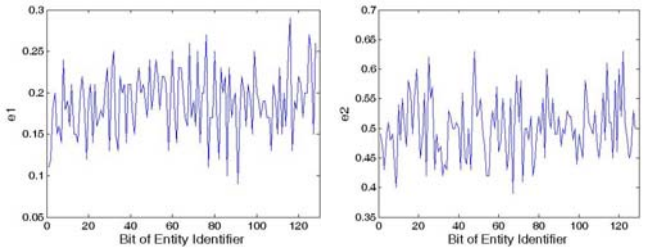
EI pairs used in Section III are reordered to analyze the effectiveness of the improved scheme for eliminating error pattern. As L=32, p=8, and q=4, the generated EIs have a bit length of 128, i.e. N=128. 100 true and false EI pairs were generated, respectively, i.e. T=100 and F=100. The results of $e_1(k)$ and $e_2(k)$ are shown in Fig. 5.

With comparison to Fig. 2, which shows that EIs generated from the existing scheme possess a consistent error pattern for true pairs that the 4th bit of each 4-bit block has a relatively high value of $e_1(k)$ when the value of q is 4. On the other hand, it can be seen from Fig. 5 that there is no any consistent error pattern both for true and false pairs. To summarize, the improved EI generation scheme is effective in removing the error pattern.

B. Randomness Evaluation

According to the National Institute of Standards and Technology (NIST), there is a variety of randomness tests can be used to evaluate the randomness performance of binary sequences. Because of the bit length limitation of EIs, 6 tests of NIST standards were chosen to evaluate the randomness of EIs, including frequency test, frequency test within a block,

runs test, test for the longest run of ones in a block, serial test and cumulative sums test [12]. For comparison, EIs generated by both the existing and the improved scheme are tested. Results show that EIs generated by the improved scheme show an acceptable degree of randomness as the existing scheme.



(a) (b)

Fig. 5. Error analysis of entity identifiers generated by the improved scheme: (a) from true pairs; (b) from false pairs.

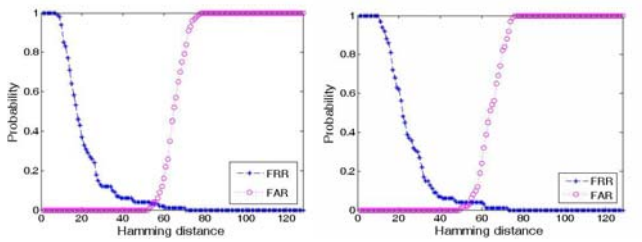
C. False Acceptance and False Rejection Performance

False acceptance and false rejection, as two types of errors, were used to evaluate the performance of node identification. False rejection rate (FRR) was the rate that two EIs simultaneously generated by two nodes in the same BSN were unmatched, and false acceptance rate (FAR) was the rate that two EIs generated from two different BSNs or at a different time were matched. The half total error rate (HTER) defined as (FRR+FAR)/2 was also analyzed.

Fig. 6 depicts the FRR and FAR curves of EIs generated by the existing and improved schemes. By comparing Fig. 6(a) and (b), it can be found that there is no significant difference between FAR and FRR of EIs generated by these two schemes. It can also be seen from Fig. 7 that, though at the hamming distance from 10 to 40, the HTER of EIs generated by the improved scheme is a little bit bigger than the HTER with the existing scheme, the minimum HTER, which normally determines the decision-making threshold, is the same.

VI. Conclusion

In this study, the error pattern that exists in the EIs generated by the method proposed in [10] was studied with experimental data using a statistical method. The analysis results show that it is with high probability that the bit difference between true EI pairs, i.e. two EIs generated simultaneously by nodes from the same BSN, has a consistent pattern, which indicates a reduced security level given the certain bit length of EI. An improved scheme of EI generation is then proposed in order to eliminate the error pattern. The performance of randomness and node identification, i.e. false acceptance rate and false rejection rate, is experimentally evaluated. The results indicate that compared with the existing one, the new scheme is effective to eliminate the error patterns with no compromise on the randomness level and identification performance, and thus is more anti-attackable.



(a) (b)

Fig. 6. FRR and FAR curves of EIs: (a) by the existing scheme; (b) by the improved scheme.

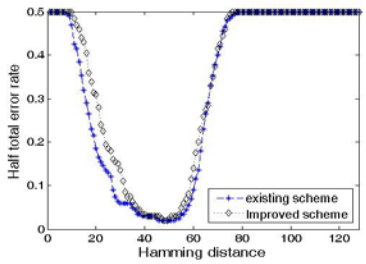


Fig. 7. HTER comparison for the existing and improved schemes.

References

[1] B. Lo and G. Z. Yang, "Body sensor networks-research challenges and opportunities," *IET*, 2007, pp. 26-32.

[2] T. camilo, R. Oscar and L. Carlos, "Biomedical signal monitoring using wireless sensor networks," *Communications*, LATINCOM'09. IEEE Latin-American Conference, 2009, pp. 1–6.

[3] B. Gyselinckx, R. Vullers, C. V. Hoof, J. Ryckaert, R. F. Yazicioglu, P. Fiorini, and V. Leonov, "Human++: Emerging technology for body area networks," *Very Large Scale Integration, IFIP International Conference*, 2007, pp. 175-180.

[4] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *Wireless Communications, IEEE*, 2010, pp. 51-58.

[5] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, "Security of body sensor networks", *Body Sensor Network,* New York: Springer-Verlag, 2006, pp. 195–206.

[6] M.Guennoun, M. Zandi, and K.EI-Khatib, "On the use of biometrics to secure wireless biosensor networks," *ICTTA 3rd International Conference*, 2008, pp. 1-5.

[7] F. Hao, R. Anderson, and J. Daugman, "Combing crypto with biometrics effectively," *IEEE Computer Society*, 2006, pp. 1081-1088.

[8] S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," *In Proc. Of Wireless Security and Privacy Workshop*, 2003, pp. 432–439.

[9] C. C. Y. Poon, S. D. Bao, Y. T. Zhang, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, 2006, 44(4): 73–81.

[10] S. D. Bao, Y. T. Zhang, and L. F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," *Engineering in Medicine and Biology 27th Annual Conference*, Shanghai, China, 2005, pp. 2255–2258.

[11] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Transactions on Information Technology in Biomedicine*, 2008 12(6):772–779.

[12] A. Rukhin *et al.* ,"A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Nat. Inst. Stand. Technol., NIST Special Publication 800-22*, Gaithersburg, MD, 2001.