Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 3403456, 11 pages
https://doi.org/10.1155/2018/3403456

Research Article

Muscle Activity-Driven Green-Oriented Random Number Generation Mechanism to Secure WBSN Wearable Device Communications

Yuanlong Cao,[1] Guanghe Zhang,[1] Fanghua Liu,[1] Ilsun You,[2] Guanglou Zheng,[3] Oluwarotimi Williams Samuel,[4,5] and Shixiong Chen[4,5]

[1]*Jiangxi Normal University, Nanchang, China*
[2]*Department of Information Security Engineering, Soonchunhyang University, Asan, Republic of Korea*
[3]*Security Research Institute, Edith Cowan University, Perth WA 6027, Australia*
[4]*Chinese Academy of Sciences (CAS), Key Laboratory of Human-Machine Intelligence-Synergy Systems, Shenzhen, China*
[5]*Institutes of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China*

Correspondence should be addressed to Ilsun You; ilsunu@gmail.com

Received 13 April 2018; Accepted 27 June 2018; Published 19 August 2018

Academic Editor: Ding Wang

Wireless body sensor networks (WBSNs) mostly consist of low-cost sensor nodes and implanted devices which generally have extremely limited capability of computations and energy capabilities. Hence, traditional security protocols and privacy enhancing technologies are not applicable to the WBSNs since their computations and cryptographic primitives are normally exceedingly complicated. Nowadays, mobile wearable and wireless muscle-computer interfaces have been integrated with the WBSN sensors for various applications such as rehabilitation, sports, entertainment, and healthcare. In this paper, we propose MGRNG, a novel muscle activity-driven green-oriented random number generation mechanism which uses the human muscle activity as green energy resource to generate random numbers (RNs). The RNs can be used to enhance the privacy of wearable device communications and secure WBSNs for rehabilitation purposes. The method was tested on 10 healthy subjects as well as 5 amputee subjects with 105 segments of simultaneously recorded surface electromyography signals from their forearm muscles. The proposed MGRNG requires only one second to generate a 128-bit RN, which is much more efficient when compared to the electrocardiography-based RN generation algorithms. Experimental results show that the RNs generated from human muscle activity signals can pass the entropy test and the NIST random test and thus can be used to secure the WBSN nodes.

1. Introduction

Over the last few years, the growing interest in the wireless body sensor network (WBSN) has resulted in thousands of peer-reviewed publications. Significant results in this area have enabled many medicine and healthcare applications. A WBSN interconnects tiny and wireless sensor nodes and devices worn on or implanted in the human body that have the capability to acquire physiological signals such as electrocardiography (ECG) [1, 2], electromyography (EMG) [3], and electroencephalography (EEG) [4], as well as data about the physical state of individuals which include walking, running, and seating [5–7]. A wide spectrum of WBSNs applications that include different kinds of wearable devices has been developed and applied for, e.g., physical fitness monitoring, and chronic diseases monitoring. Figure 1 illustrates the most typical usage scenarios for a WBSN-based rehabilitation system with wearable devices. In such a rehabilitation system, the EMG signals can be collected by wearable WBSN devices from an injured patient's upper arm, processed and then used to control an artificial limb in order to facilitate the injured or disabled people's daily works and lives.

Although the WBSN technologies bring obvious and attractive benefits to facilitate people's life activity, there are many concerns and challenges to be addressed. The first important concern of WBSN is related to security and privacy

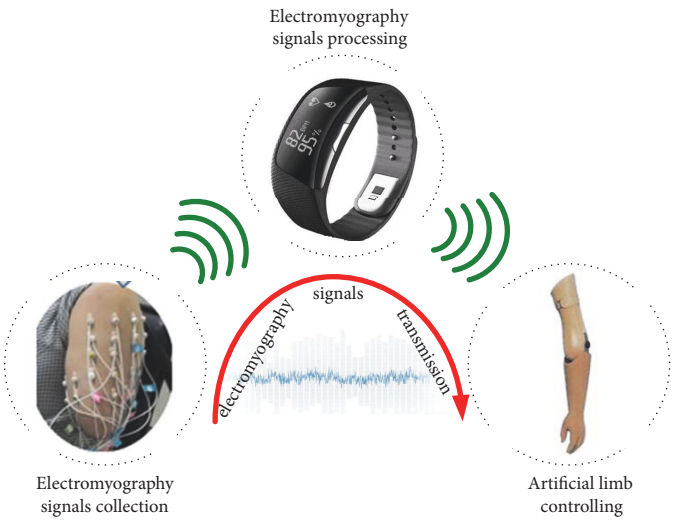

Figure 1: A WBSN-based rehabilitation system with the EMG signals collection, processing, and artificial limb controlling.

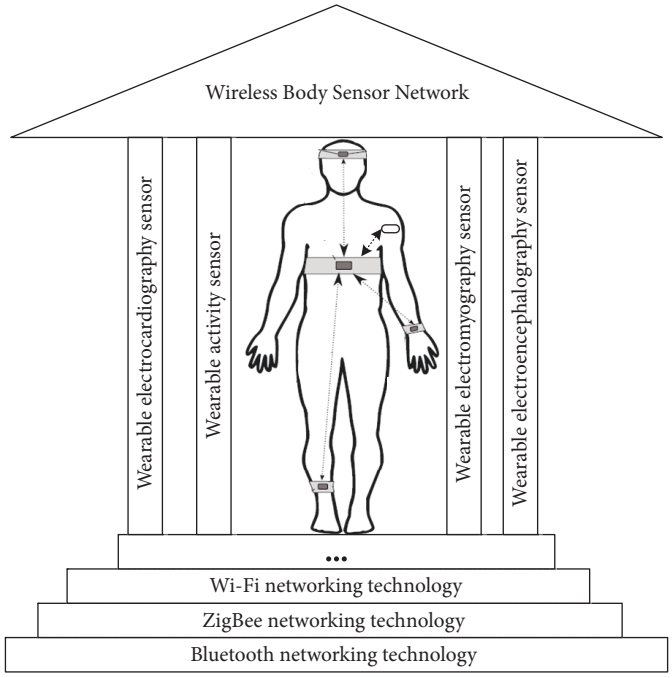

Figure 2: A basic structure of wireless body sensor networks.

challenges. A typical WBSN system consists of a number of wearable biomedical sensors or wireless muscle-computer interfaces worn on or even implanted in a single person; it also involves a base station which can be a wearable computer, a smart watch, or a smart phone. The base station is responsible for collecting physiological signals from a patient through wearable biomedical sensors placed on a human by using of Wi-Fi, ZigBee, and/or Bluetooth networking technologies (as shown in Figure 2). However, due to limited bandwidth resource and computing capabilities, wearable WBSN devices provide less security and authentication system (in comparison to traditional personal computers, laptops, and other computing devices). Consequently, we have reason to believe that attacks targeting wearable WBSN devices with the aim of malicious disruption or worse will rise. As numerous wearable devices make their way into the WBSNs with a much more open structure, they undoubtedly bring a WBSN system of security and privacy challenges.

Aside from the wearable devices, there will also be a rise in the number of targeted attacks focused on interrupting WBSN signal transmission or even stealing personal data. In a WBSN system, wearable devices generally have limited

storage and computation capabilities, they require to pair with other wearable electronic devices to perform most functions. In other word, a WBSN system is more like a tiny switching system [8, 9]. In such a system, a wearable WBSN device needs to communicate with other computing devices (e.g., a mobile phone and a wearable personal computer) via Wi-Fi, Bluetooth, or ZigBee connections for the data to be processed. During the communications between a wearable device and a computing device, these personal data should be properly protected from all forms of security threats posed by potential attackers, since the data normally contains sensitive health information [10–14]. The unauthorized usage of the data will breach the users' privacy and could be even harmful to their life.

The second concern of WBSN is the energy consumption problem. In the WBSN systems, a wearable device generally has extremely limited energy capacity and is frequently constrained by the volume of energy resource available in its battery. Moreover, a wearable device is not a standalone device as it needs to send the collected biomedical data to a computing device using Bluetooth, Wi-Fi, or ZigBee networking technology, which means that apart from the energy consumption of data collection an energy-constrained wearable device needs to spend a considerable amount of energy resource for the biomedical packet transmission. The high power consumption of wearable devices will limit the WBSN lifetime because if one or more wearable devices run out of battery, the whole WBSN system may fail to work. Therefore, a promising WBSN-based design has to take into consideration energy overhead and optimization policy [15].

In this paper, we propose a novel muscle activity-driven green-oriented random number generation mechanism (MGRNG) which uses the human muscle activity as green energy resource to generate random numbers (RNs). The RNs can be used to enhance the privacy of wearable device communications and secure WBSNs for rehabilitation purposes. To this end, we study a different type of physiological signal for the random number (RN) generation purpose, that is, the EMG signals recorded from the muscle(s) via a surface or intramuscular electrode(s) placed on the muscle(s) [3]. The method was tested on 10 healthy subjects as well as 5 amputee subjects with 105 segments of simultaneously recorded surface electromyography signals from their forearm muscles. The proposed MGRNG requires only one second to generate a 128-bit RN, which is much more efficient when compared to the electrocardiography-based RN generation algorithms.

The remainder of this paper is organized as follows. In Section 2, a problem statement with a clear description of the security and privacy issue in a WBSN system is presented in order to explain our motivation. Section 3 presents the EMG signal-based RN generation algorithm, describes the experimental settings and determines performance metrics in order to evaluate the proposed EMG-based RN generation scheme. Section 4 evaluates and analyzes the performance of the proposed solution. Section 5 discusses the limitations of the work and gives some interesting directions for future work. Section 6 concludes the paper.

2. Problem Statement

Nowadays, with the widespread use of WBSNs, the shapes and functionalities of WBSN devices are evolving dramatically. Among them, wearable devices are becoming even more important as sales of wearable devices continue to see year-over-year growth [17]. Typically, wearable WBSN devices facilitate the daily life and works. Unfortunately, wearable WBSN devices become a vulnerable and attractive target of most attacks because of the lack of security mechanisms [18]. Moreover, a wearable WBSN device becomes more and more lucrative target because it collects and shares an amount of sensitive personal data with third-parties [19]. Therefore, wearable WBSN devices bring much more threats to the WBSN systems and make them face more serious security and privacy challenges [20, 21].

In a WBSN system, data collected from the wearable biomedical sensors or other wearable devices is often transmitted to a mobile phone or other portable devices where it is stored and processed in order to provide real-time feedback for users in different areas of applications [22]. However, the personal data collected by wearable WBSN devices may be illegally used by potential attackers [23]. Figure 3 presents a scenario that the health information of individuals maliciously is manipulated by an attacker. As the figure shows, a wearable electromyography sensor transmits the collected personal electromyography data to a wearable watch for data processing and artificial limb controlling. However, the artificial limb can be out of control because of malicious manipulation caused by an attacker.

Apart from malicious manipulation, personal data and biomedical information collected and processed by connected wearable WBSN devices are also increasingly becoming a main target of attacks. A fresh survey has revealed that there is a rise in the number of targeted attacks focused on stealing personal data from the wearable WBSN devices connected to the computing devices [24]. Figure 4 presents a scenario that the health information of individuals is intercepted by potential attackers. Although the amount of personal data and biomedical information collected and processed in the WBSN systems grows daily, these data and information with extremely valuable can be easily captured by hackers and vanished into the black market due to the lack of security and authentication system in the WBSN systems [25, 26].

Considering the fact that health information of individuals is subject to interception and manipulation by potential attackers, the security of data at rest and in transit is a major challenge in the abovementioned WBSN applications. Existing traditional asymmetric security methods such as Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), and symmetric methods including Advanced Encryption Standard (AES) and Rivest Cipher 5 (RC5) are of high computational complexity. Hence, these algorithms cannot be directly applied to the WBAN systems since they have limited computing resources. To develop an efficient security mechanism for WBSN systems, previous studies have proposed the use of features extracted from physiological signals

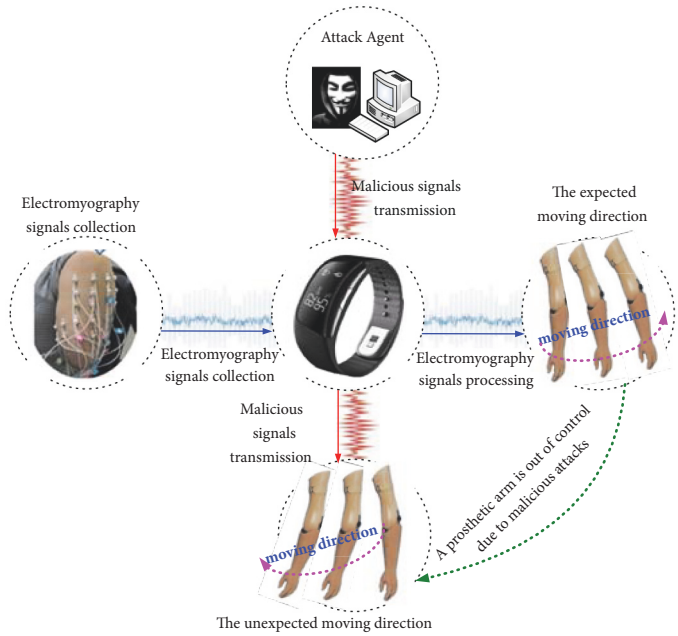

Figure 3: The health information of individuals is subject to manipulation by potential attackers: an example.

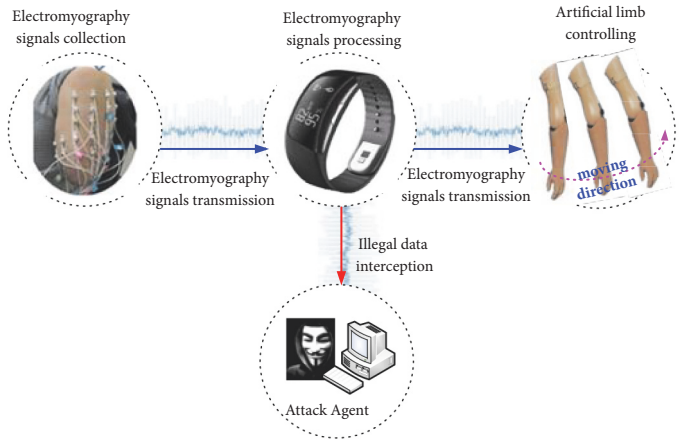

Figure 4: The health information of individuals is subject to interception by potential attackers: an example.

like ECG and EEG collected via wireless sensors and wearable devices for random number generation.

Currently, most of the random numbers generated from ECG features are based on the process of Interpulse Intervals (IPIs) extracted from the signal [16]. In previous studies, a method using IPIs to encode 128-bit random number sequence with reasonable randomness performance shows that if a single IPI is encoded into 4-bits, then at least 32 IPIs have to be extracted from the ECG signal. This implies that the WBSN sensor nodes need to successfully detect at least 33 consecutive heartbeats [16]. Considering that the normal sinus rhythm of an adult lies between 60 and 100 beats per minute (bpm), generating a 128-bit of random number sequence would require about 20 seconds. Hence, the IPI-based methods may not be suitable for real-time applications of WBSN systems since it requires a considerable amount of time.

Furthermore, recent WBSN efforts are devoted to generating random numbers for securing the data associated with WBSN devices, by exploiting the characteristics of EEG signals [4]. Although their research reports reveal that the EEG-based method is comparable to the existing ECG-based methods, it is important to note that the EEG-based random number generation method has a number of issues which may limit its application in real-time systems. These issues are as follows: (a) processing acquired EEG signals requires a relatively high computing resources because the signals have poor signal-to-noise ratio; (b) EEG signal acquisition would generally require precise deployment of dozens of electrodes around the head and the use of various gels, saline solutions,

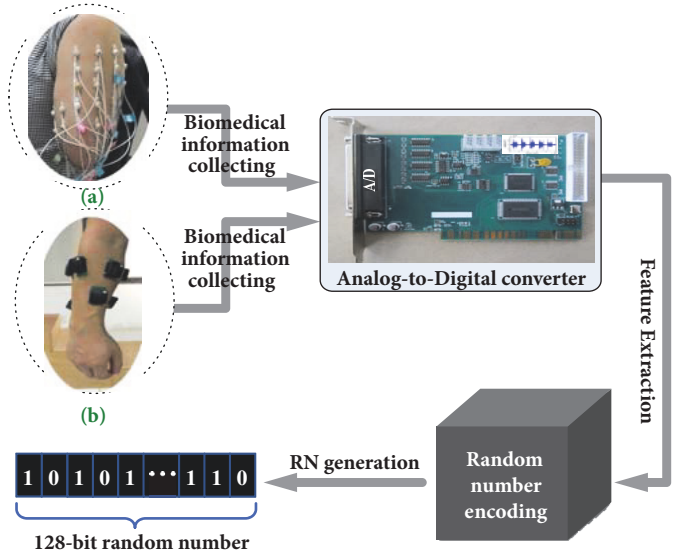

Figure 5: The architecture of MGRNG system.

and/or pastes to keep the electrodes in place, which would severely affect the daily life of the individual and make the user feel uncomfortable.

Compared to the abovementioned IPI-based methods, EMG signals sampled at the rate of 1000Hz can be used to generate a 128-bit random sequence with only one second. More importantly, in comparison to the EEG, EMG signals require less computing resources with a simplified data collection procedure. In this paper, we propose MGRNG, a novel random number generation algorithm which is based on features extracted from EMG recordings. The randomness of the 128-bit RNs was exhaustively examined by using the entropy metric. We believe that these EMG-based RNs can be further used to protect both data at rest and in transit in a WBSN system. More specifically, our solution makes important contributions in the following aspects:

(i) It introduces a green-oriented RN generation method which exploits the human muscle activities as energy resources to generate RNs and improve on wearable device communication by being more energy efficient.

(ii) It designs a fast RN generation scheme which generates a 128-bit random sequence in a timely fashion. The muscle activity-based RNs can be further used to enhance the security and privacy in WBSNs.

3. MGRNG Detail Design

This paper is devoted to exploring the possibility of resolving a critical security issue associated with data storage and transmission among the wearable devices and nodes in WBSN systems. To this end, we propose a novel security method dubbed as MGRNG. MGRN contributes to generating an EMG-based 128-bit RN for secure communication over WBSN systems. Figure 5 presents the architecture of MGRNG, which reveals how the EMG signals are collected (from the upper arm of an amputee subject and the forearm of a healthy subject), then processed, and encoded for RN generation.

3.1. EMG-Based RN Generation. In the MGRNG solution, there are five stages included to generate RN: (i) EMG signal collection, (ii) EMG signal sampling, (iii) EMG signal segmenting, (iv) feature extraction, and (v) RN generation. Figure 6 shows the technological processes of EMG signal-based RNs generation scheme in MGRNG. A detailed description of each of these five stages is presented as follows in order to help the readers understand easily:

(i) *EMG Signal Collection*: In MGRNG, the EMG signals are collected from an upper arm of an amputee subject and forearm of a healthy subject through wearable biomedical sensors placed on these subjects.

(ii) *EMG signal sampling*: The analog EMG signals are converted into digital EMG signals by using an Analog-to-Digital (A/D) converter, and every EMG signal is sampled at the rate of 1000Hz.

(iii) *EMG Signal Segmenting*: These collected EMG signals are divided into 128 segments in order to further used for 128-bit RNs generation.

(iv) *Feature Extraction*: There are many methods can be used for signal denoising and EMG signal extraction. In this study, we choose the wavelet analysis method for signal denoising and EMG signal extraction since as a mature technology, wavelet analysis has proven to be invaluable in signals analysis and processing. More details on the wavelet analysis method can be found in [27].

(v) *RN Generation*: Encoding these extracted EMG features generates a sequence of random numbers (a 128-bit RN) for the purpose of secure WBSN communications.

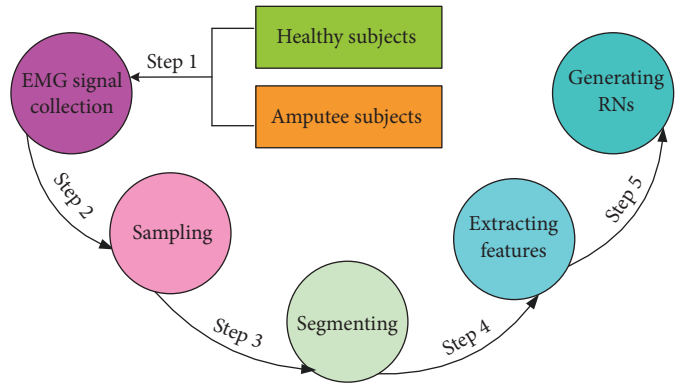

Figure 6: The technological processes of EMG signal-based RN generation.

Definition:
S_{list}: all subjects who are volunteers for EMG collection
WS_{list}: all wearable sensor used to acquire the EMG signals
ES_{list}: all the EMG signals collected from subjects
for $(i = 1, i \leq \text{count}(S_{list}), i++)$ **do**
  for $(j = 1, j \leq \text{count}(WS_{list}), j++)$ **do**
    execute EMG signal acquisition;
  end for
end for
for $(k = 1, k \leq \text{count}(ES_{list}), k++)$ **do**
  take the EMG signal sample;
  divide EMG signals into 128 segments;
  extract EMG features using wavelet analysis method;
  encode the EMG features to generate 128-bit RNs.
end for

Algorithm 1: EMG-based RN generation algorithm.

In this study, we use 256 EMG signals from each subject to generate a number of RNs which are of different lengths. Each EMG signal was encoded into different bits to result in RNs of length varying from 512 bits to 2816 bits. Then the RNs were divided into 128 bit segments. To this end, we developed an algorithm with MATLAB programming tool to detect and exclude the invalid data segments in the EMG recordings. Afterwards, the features were extracted from the preprocessed EMG signals and utilized to generate 128-bit RNs, and a total of 105 (15 subjects including 10 healthy subjects (HS) and 5 disabled subjects (DS), and each subject has 7 sensors) RNs were generated. The experimental protocols were approved by the Shenzhen Institutes of Advanced Technology Institutional Review Board, Chinese Academy of Sciences. All the subjects agreed and gave written informed consent as well as permission for the publication of their photographs and data for scientific and educational purposes. The pseudo code of the EMG-based RN generation algorithm is presented in Algorithm 1.

From Algorithm 1, it can be seen that the EMG-based RN generation method would at least have the following advantages: (i) an EMG is a very low-risk procedure, (ii) the EMG signals can be easily acquired from muscle activities, (iii) compared with most of the traditional pseudorandom number generation solution [7], the EMG-based RN generation method neither requires a random seed nor complex computation operations, and (iv) compared with the classic ECG/EEG-based number generation solutions [4, 16], the EMG-based RN generation method requires less computing resources and shorter time to generate RNs. For these reasons, we believe that the proposed EMG-based RN generation method will become a promising technology used to generate RNs for securing data confidentiality in WBSNs.

3.2. Performance Metric Determination. Considering the fact that the entropy is an important metric to measure and reflect the randomness and uncertainty of matter in a system, in this paper, we select entropy as the performance metric to measure and evaluate the randomness of the EMG-based RNs. We calculate the entropy values for these generated EMG-based RNs by using the following formula:

$$S = -K \times \sum_{i=1}^{N} P_i \ln\left(P_i\right), \tag{1}$$

where K is a constant, P_i is the uncertainty (probability) of the i^{th} RN, and N is the number of RNs.

Moreover, in order to further convince the effectiveness of these generated RNs, we calculate the mean entropy value and standard deviation of RNs generated from each EMG sensor placed on every subject. Assuming the obtained entropy values are $e_1, e_2, e_3, \cdots, e_m$, we calculate the mean value of the entropies by using the following formula:

$$\overline{E_M} = \frac{1}{M} \times \sum_{i=1}^{M} e_i, \tag{2}$$

where E_i is an entropy value, M is the number of entropy values, and $\overline{E_M}$ is the mean entropy of RNs generated from each EMG sensor.

Formula (2) is a general formula for the mean entropy value calculation. In order to reduce the computational complexity, we use an iterative method (see (3)) to calculate the mean entropy value:

$$\overline{E_{M+1}} = \frac{\overline{E_M} \times M + e_{M+1}}{M+1}, \tag{3}$$

We use the previous mean entropy $\overline{E_M}$ and the new entropy value e_{M+1} to calculate the current mean entropy value $\overline{E_{M+1}}$. This means that the current mean entropy is updated according to the newly recorded entropy values.

Similarly, the general formula for calculating the standard deviation (SD) is presented in the following:

$$\sigma_M = \sqrt{\frac{\sum_{i=1}^{M} \left(e_i - \overline{E_M}\right)^2}{M-1}}, \tag{4}$$

Equation (4) is a general formula for calculating the SD value. In order to reduce the computational complexity, we also calculate the SD value utilizing an iterative method presented in the following formula:

$$\sigma_{M+1} = \sqrt{\frac{\sigma_M^2 \times (M-1)}{M} + \frac{\left(e_{M+1} - \overline{E_M}\right)^2}{M+1}}, \tag{5}$$

By using (5), we can calculate the new SD σ_{M+1} using only four variables: the previous SD σ_M, the previous mean entropy value $\overline{E_M}$, the current entropy value e_{M+1}, and the previous records of entropy M.

The mean entropy and the entropy SD values obtained from (3) and (5) can be used as references for evaluating the randomness and effectiveness of these generated EMG-based RNs. Furthermore, we also use 15 tests provided by the US National Institute of Standards and Technology (NIST) to validate the performance of RNs [7]. Specifically, we implement the five commonly used NIST tests (see Table 1) as part of effort to further examine the randomness of our proposed method. In other words, the five NIST tests have been used in this work for evaluating the randomness of the 128 bit RNs and the pass rates have been defined as the ratio of the numbers of p value greater than 0.01 divided by the total generated RNs.

It is worthy to note that the NIST suite consists of 15 different tests [3–5], and some of them require the length of the RNs to be no less than 1,000,000 bits. In this study, we only focus on evaluating an EMG-based RN with a length of only 128 bits; thus we just utilize the five commonly used NIST tests (namely, F Test, B Test, R Test, L Test, and A Test) to verify the randomness of the generated RNs. Moreover, interested readers can refer to our previous work [16] for more detail information on how the NIST tests are conducted for the generated RNs.

Table 1: The five most commonly used NIST tests.

Test cases	Descriptions
F Test	The frequency test
B Test	The frequency test block
R Test	The runs test
L Test	The longest runs ones block test
A Test	The approximate entropy test

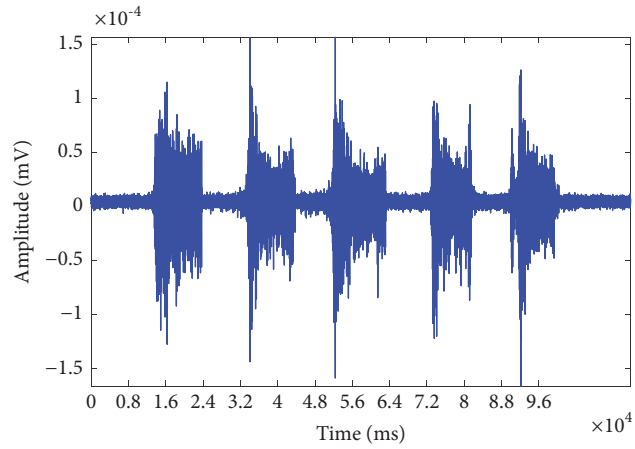

Figure 7: The EMG amplitudes between time $t = 0$ ms and $t = 10$ ms.

4. Results and Analysis

In order to generate 128 bit EMG-based RNs and then evaluate the randomness of them, we pull the EMG samples from total 15 subjects including 10 healthy subjects (HS) and 5 disabled subjects (DS); each subject has 7 wearable biomedical sensors to gather the EMG signals. Figure 7 presents the EMG amplitudes collected from one of these subjects (only EMG amplitudes between time $t = 0$ ms and $t = 10$ ms are illustrated in the figure in order to better show the results).

After EMG feature extraction, feature encoding and RN generation, we calculate the entropy values for these generated RNs by using (1). From the obtained entropy values shown in Table 2, it was observed that the entropy values of the generated RNs varied from 0.9887 to 0.9998 among the 7 EMG sensors for a representative healthy subject. Meanwhile, for an arbitrarily selected amputee, an entropy value that ranged between 0.9914 and 1.0000 was recorded for the generated RNs based on EMG recordings from the seven sensors.

Table 2: The entropy of RNs generated from EMG signals extracted from seven sensors (a healthy subject vs. an amputee subject).

No.	A healthy subject	An amputee subject
1	0.9887	0.9937
2	0.9998	1.0000
3	0.9914	0.9993
4	0.9998	0.9972
5	0.9914	0.9956
6	0.9984	0.9914
7	0.9972	0.9937

Table 3: The entropy of each sensor of health and disabled subjects.

No.	MEHS	VHS	MEAS	VAS
1	0.9967	1.88×10^{-5}	0.9968	6.80×10^{-6}
2	0.9861	3.02×10^{-5}	0.9913	1.70×10^{-5}
3	0.9959	1.51×10^{-4}	0.9964	7.10×10^{-6}
4	0.9948	1.03×10^{-5}	0.9962	5.28×10^{-5}
5	0.9996	2.80×10^{-6}	0.9976	9.13×10^{-5}
6	0.9952	9.40×10^{-6}	0.9967	1.61×10^{-3}
7	0.9973	1.74×10^{-5}	0.9981	1.50×10^{-6}

Table 4: The entropy of each sensor of health and disabled subjects.

Name	Mean of entropy	Variance of entropy
Health subjects (our Best)	0.9996	2.80×10^{-6}
Amputee subjects (our Best)	0.9981	1.50×10^{-6}
Subjects with myocardial infarction [6]	0.9902	2.31×10^{-6}
Subjects with other CVD [6]	0.9899	2.96×10^{-6}
Healthy subjects [6]	0.9893	3.46×10^{-6}

Table 3 presents the average entropy of RNs generated from each EMG sensor (i.e., from sensor 1 to sensor 7) placed on 10 healthy and 5 amputee subjects. It shows that the mean entropy of RNs generated from 10 healthy subjects (MEHS) varies from 0.9861 to 0.9996. Meanwhile, the mean entropy of RNs generated from 5 amputee subjects (MEAS) varies from 0.9913 to 0.9981. The overall average entropy of both categories of subjects per sensor varied from 0.9887 to 0.9986 (i.e., from sensor 1 to sensor 7). The variance of health subjects (VHS) varied from 2.80×10^{-6} to 1.51×10^{-4}, and the variance of amputee subjects (VAS) varied from 1.50×10^{-6} to 1.61×10^{-3}. Moreover, by comparison with the mean entropy values, we found that the mean of entropy of RNs generated from EMG signals in our proposed approach is better than binary previously study [6], as shown in Table 4.

Additionally, we implemented the five most commonly used NIST tests (F Test, B Test, R Test, L Test, and A Test) as part of effort to clarify the randomness of our proposed method. We found out through experiment that, the pass rates of the five NIST tests varied from 0.9857 to 1.0000 for the healthy subjects and from 0.9714 to 1.0000 for the amputee subjects, as shown in Figures 8 and 9, respectively.

Through analyzing the results, we can observe that the entropy values of RNs generated from the representative healthy and amputee subjects shown in Table 2 are observed to be close to 1.00, which reflects a perfect randomness as well as a perfect performance. Also, similar performance can be observed when the entropy of the entire 105 RNs is computed. By comparing the RNs generated from the sensors deployed at different positions of the body, the obtained entropy results show that there is no distinctive difference between RNs from any two sensors. This implies that the EMG sensor position has no effect on the randomness of generated RNs.

Furthermore, we investigate the randomness of the RNs generated based on the features extracted from EMG recordings of the healthy and amputee subjects and then compare the results obtained for both categories of subjects. The rationale behind comparing the RNs of healthy and amputee subjects is because WBSN systems have been widely applied for both the healthcare and the sports training. In healthcare, rehabilitation devices such as the prostheses are now commonly available to help amputees regain their arm functions. And the EMG signal patterns obtained from the amputated arm have been reported to be different from that obtained from the intact arm [28–30]. In this regard, we compare the randomness of the RNs generated from the healthy and amputated subjects to see if the variations in EMG signal patterns between both categories of subjects would be different. From the comparison, it can be observed that there is no distinctive difference between the RNs of the

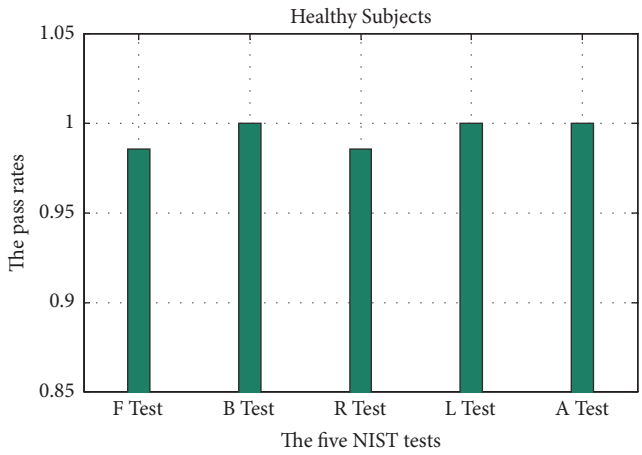

Figure 8: The pass rates of 128-bit RNs using five NIST tests (RNs generated from EMG of healthy subjects).

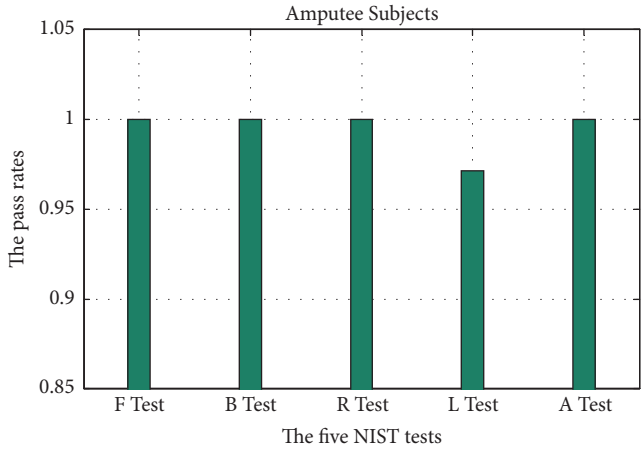

Figure 9: The pass rates of 128-bit RNs using five NIST tests (RNs generated from EMG of disabled subjects).

healthy and amputee subjects. We can see from this result that our proposed method is robust and could be used to secure the data in WBSN systems regardless of the health status of the user (whether the user is healthy or not).

We also compare the pass rates of the RNs generated by the proposed EMG-based RN generation method with those resulted from the Interpulse Intervals- (IPIs-) based RN generation method [16] (the pass rates of the 128-bit RNs generated from IPIs of 20 healthy subjects have been tested). In order to make the comparison more reasonable, the pass rates of RNs from healthy subjects generated by the EMG-based RN generation method and the IPIs-based RN generation method are illustrated only, as shown in Figure 10. As the figure shows, the proposed EMG-based RN generation method outperforms the IPIs-based RN generation method in all cases in terms of RN pass rate. The subfigure in Figure 10 shows the cumulative average pass rates of the two methods. As the subfigure shows, the EMG-based RN generation method achieves a better pass rate in comparison with the IPIs-based RN generation method. More specifically, the average pass rate of the EMG-based RN generation method is about 3.54% higher than that of the IPIs-based RN generation method.

5. Discussion

In Section 4, we demonstrated how the proposed EMG-based RNs generation method is robust, we also investigated the randomness of the EMG-based RNs, and we believe that the EMG-based RNs can be used to enhance the privacy of wearable device communications and secure the data in WBSN systems. In this section, we discuss the limitations of the work and explore some potential directions for future research:

(i) Despite the promising results achieved by the proposed EMG-based RNs generation method, it may not be applicable to persons with neuromuscular disorder, who lack the ability to provide EMG signals from which RNs could be generated.

(ii) It is unknown whether the proposed EMG-based RNs generation method would be robust to variation in muscle contraction level. Therefore, we plan to investigate this issue in our future study.

(iii) It is unknown what the capabilities of the EMG-based RNs are allowed to an attacker. Our future work will study the existing threat models [31] and further define a proper threat model to assess the security capabilities of a WBSN system with the EMG-based RNs.

(iv) It is also unknown whether the proposed EMG-based RNs generation mechanism can be used in the promising anonymous mutual authentication protocols for wearable sensors. This is a very interesting topic and will be carried on in our future research.

(v) As discussed in the previous section, we consider five different NIST tests that could be used to validate the randomness of RNs of 128-bit length. However, as a secure RN generator, it should be better to pass all the 15 NIST tests. We will extend our proposal and evaluate the randomness under those test cases.

(vi) In addition, we believe that a WBSN system with the promising collaboration computing and multipathing technologies [32–36] is an interesting topic worth further investigation. In our future work, we will also apply these promising technologies to optimize the performance of the WBSN systems.

6. Conclusion

In this paper, we present a novel EMG-based RN generation method which uses the human muscle activity as green energy resource to generate 128 bit RNs for securing data communication in a WBSN system. Compared to the previously proposed methods that used ECG features to generate RNs for securing the data in WBSN systems [16], our EMG-based approach could generate random numbers with comparable performance and high speed of generation

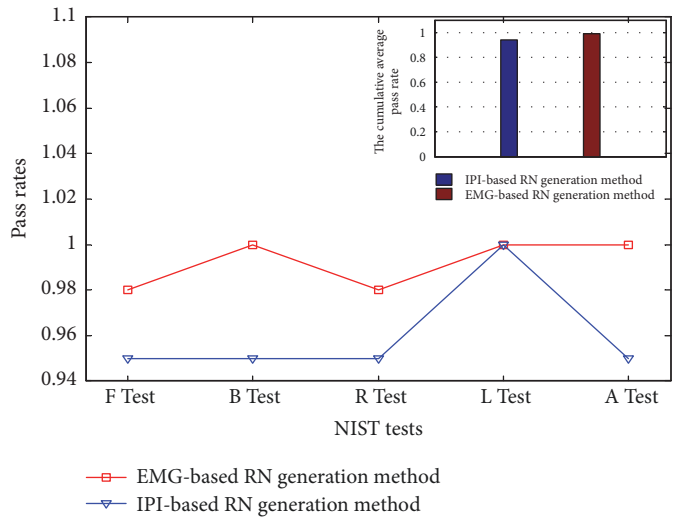

Figure 10: Pass rates of the EMG-based RN generation method as compare to the IPI-based RN generation method [16].

(128 bit per second). In addition, the proposed surface EMG-based RNs generation method can be used for real-time applications for a WBSN system since the signal from a single EMG sensor would be sufficient to provide the required RNs based on our experimental results. In addition, unlike the EEG-based RNs generation method that is sensitive to sensor position as placed on the scalp of a subject, our proposed EMG-based approach is insensitive to sensor location on the muscle, which is an advantage over the recently proposed EEG-based approach [4]. The results from five NIST statistical tests reveal that the RNs generated by our method can potentially be used as authentication identifiers or encryption keys for securing WBSNs.

Data Availability

Some data were omitted due to a confidentiality agreement between the research team and the Shenzhen Institutes of Advanced Technology Institutional Review Board, Chinese Academy of Sciences.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

The first two authors contributed equally to this work and share the first authorship.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant no. 61562043 and by the Soonchunhyang University Research Fund. The authors would like to thank the members of the School of Computer and Information Engineering, Jiangxi Normal University, as well as the members of the Research Center for Neural Engineering, Institute of Biomedical and Engineering, Shenzhen Institutes of Advanced Technology, and Chinese Academy of Sciences for their assistance in the experiments.

References

[1] C. 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, pp. 73–81, 2006.

[2] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proceedings of the 27th IEEE Conference on Computer Communications (IEEE INFOCOM Workshops)*, pp. 1–6, IEEE Xplore, Phoenix, AZ, USA, April 2008.

[3] G. Zhang, O. Samuel, F. Liu et al., "Electromyogram-Based Method to Secure Wireless Body Sensor Networks for Rehabilitation Systems," in *Proceedings of the 39th Annual International Conference of the IEEE Engineering in Medicine Biology Society (EMBC17)*, pp. 1246–1249, JeJu Island, S. Korea, 2017.

[4] J. F. Valenzuela-Valdes, M. A. Lopez, P. Padilla, J. L. Padilla, and J. Minguillon, "Human Neuro-Activity for Securing Body Area Networks: Application of Brain-Computer Interfaces to People-Centric Internet of Things," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 62–67, 2017.

[5] Y.-L. Zheng, X.-R. Ding, C. C. Y. Poon et al., "Unobtrusive sensing and wearable devices for health informatics," *IEEE Transactions on Biomedical Engineering*, vol. 61, no. 5, pp. 1538–1554, 2014.

[6] O. W. Samuel, X. Li, Y. Geng et al., "Resolving the adverse impact of mobility on myoelectric pattern recognition in upper-limb multifunctional prostheses," *Computers in Biology and Medicine*, vol. 90, pp. 76–87, 2017.

[7] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST 800-22, 2001.

[8] Y. Zhang, P. Shi, C.-C. Lim, H. Zhu, J. Hu, and Y. Zeng, "Chaotification of a class of linear switching systems based on a Shilnikov criterion," *Journal of The Franklin Institute*, vol. 354, no. 13, pp. 5519–5536, 2017.

[9] Y. Zhang, X. Liu, H. Zhang, and C. Jia, "Constructing chaotic systems from a class of switching systems," *International Journal of Bifurcation and Chaos*, vol. 28, no. 2, 1850032, 9 pages, 2018.

[10] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2010.

[11] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless Communications Magazine*, vol. 17, no. 1, pp. 80–88, 2010.

[12] M. Li, W. J. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications Magazine*, vol. 17, no. 1, pp. 51–58, 2010.

[13] *Summary of Health Insurance Probability and Accountability Act (HIPAA), U.S. Dept. of Health and Human Services, Washington, DC, 2003*.

[14] The European Parliament and the Council of the European Union, "Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Union, vol.L201, pp.37-47, 2002.

[15] F. Song, D. Huang, H. Zhou, H. Zhang, and I. You, "An Optimization-Based Scheme for Efficient Virtual Machine Placement," *International Journal of Parallel Programming*, vol. 42, no. 5, pp. 853–872, 2014.

[16] G.-H. Zhang, C. C. Y. Poon, and Y.-T. Zhang, "Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 1, pp. 176–182, 2012.

[17] S. Seneviratne, Y. Hu, T. Nguyen et al., "A Survey of Wearable Devices and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2573–2620, 2017.

[18] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, 2015.

[19] X. Fafoutis, L. Marchegiani, G. Z. Papadopoulos, R. Piechocki, T. Tryfonas, and G. Oikonomou, "Privacy leakage of physical activity levels in wireless embedded wearable systems," *IEEE Signal Processing Letters*, vol. 24, no. 2, pp. 136–140, 2017.

[20] Y. Shi, X. Wang, and H. Fan, "Light-weight white-box encryption scheme with random padding for wearable consumer electronic devices," *IEEE Transactions on Consumer Electronics*, vol. 63, no. 1, pp. 44–52, 2017.

[21] S. Wang, R. Bie, F. Zhao, N. Zhang, X. Cheng, and H.-A. Choi, "Security in wearable communications," *IEEE Network*, vol. 30, no. 5, pp. 61–67, 2016.

[22] F. Song, Y. Zhou, Y. Wang, T. Zhao, I. You, and H. Zhang, "Smart collaborative distribution for privacy enhancement in moving target defense," *Information Sciences*, 2018.

[23] J. Liu and W. Sun, "Smart Attacks against Intelligent Wearables in People-Centric Internet of Things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 44–49, 2016.

[24] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via RSS trajectory matching between wearable devices," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 802–817, 2018.

[25] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. R. Choo, and Y. Park, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, 2018.

[26] F. P. Diez, D. S. Touceda, J. M. Sierra Cámara, and S. Zeadally, "Toward self-authenticable wearable devices," *IEEE Wireless Communications Magazine*, vol. 22, no. 1, pp. 36–43, 2015.

[27] MATLAB Wavelet Toolbox User's Guide. https://www.mathworks.com/help/wavelet/examples.html.

[28] G. Zheng, G. Fang, R. Shankaran et al., "Multiple ECG Fiducial Points-Based Random Binary Sequence Generation for Securing Wireless Body Area Networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 3, pp. 655–663, 2017.

[29] M. J. Cler and C. E. Stepp, "Discrete Versus Continuous Mapping of Facial Electromyography for Human-Machine Interface Control: Performance and Training Effects," *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, vol. 23, no. 4, pp. 572–580, 2015.

[30] D. Brunelli, E. Farella, D. Giovanelli, B. Milosevic, and I. Minakov, "Design considerations for wireless acquisition of multichannel sEMG signals in prosthetic hand control," *IEEE Sensors Journal*, vol. 16, no. 23, pp. 8338–8347, 2016.

[31] D. Wang and P. Wang, "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[32] F. Song, Y.-T. Zhou, K. Kong, Q. Zheng, I. You, and H.-K. Zhang, "Smart collaborative connection management for identifier-based network," *IEEE Access*, vol. 5, pp. 7936–7949, 2017.

[33] Z. Ai, Y. Zhou, and F. Song, "A Smart Collaborative Routing Protocol for Reliable Data Diffusion in IoT Scenarios," *Sensors*, vol. 18, no. 6, p. 1926, 2018.

[34] Y. Cao, F. Song, Q. Liu, M. Huang, H. Wang, and I. You, "A LDDoS-Aware energy-efficient multipathing scheme for mobile cloud computing systems," *IEEE Access*, vol. 5, pp. 21862–21872, 2017.

[35] F. Song, Z. Ai, J. Li et al., "Smart Collaborative Caching for Information-Centric IoT in Fog Computing," *Sensors*, vol. 17, no. 11, p. 2512, 2017.

[36] Z. Ai, Y. Liu, F. Song, and H. Zhang, "A Smart Collaborative Charging Algorithm for Mobile Power Distribution in 5G Networks," *IEEE Access*, vol. 6, pp. 28668–28679, 2018.