Towards Using Physiological Signals as Cryptographic Keys in Body Area Networks

Duygu Karaoğlan Altop
Faculty of Engineering & Natural Sci.
Sabancı University
İstanbul, TURKEY
duyguk@sabanciuniv.edu

Albert Levi
Faculty of Engineering & Natural Sci.
Sabancı University
İstanbul, TURKEY
levi@sabanciuniv.edu

Volkan Tuzcu
Department of Pediatric Cardiology
İstanbul Medipol University
İstanbul, TURKEY
vtuzcu@gmail.com

***Abstract*—Body Area Networks (BANs) are the most important building stone of pervasive healthcare, which enables remote, continuous and real-time health monitoring. Biosensors, constituting the BANs, collect highly sensitive medical information from their hosts and communicate these data. Considering the nature of the wireless medium, the privacy requirements of the individuals and the extreme energy and storage limitations of the biosensors, BANs require a light-weight and secure key management infrastructure. It has been suggested that the security of a BAN can be guaranteed using the body itself as the communication channel by means of bio-cryptography. Explicitly, physiological parameters generated from different body parts are used to protect the data exchanged among the biosensors. In this paper, we (i) define a novel physiological parameter generation technique, and (ii) identify and evaluate an appropriate physiological parameter that can be used in a bio-cryptographic key management protocol, namely the inter-pulse interval (IPI). For experimental data analysis, we use the blood pressure (BP) signal, for the first time in the literature, together with the electrocardiogram (ECG) and photoplethysmogram (PPG) signals. Our results show that the IPI values derived from the ECG, PPG and BP signals are good candidates of physiological parameters that can be used as cryptographic keys in order to ensure secure key management in BANs.**

***Keywords*—Cryptographic Key Generation; Body Area Networks; Physiological Signals; Key Management; Network Security; Bio-cryptography**

I. Introduction

Healthcare concerns with the maintenance or restoration of an individual's health by preventing or treating well-being through medical services. With the use of pervasive computing, healthcare systems can be constituted so as to monitor a patient's health status in real-time, continuously and remotely. While using pervasive healthcare, physical presence of the health professionals are required only during emergencies; meaning that there is no restriction on the time and space of the patient monitoring process. Body Area Networks (BANs), whose infrastructure is as depicted in Figure 1, are the principal enabling technology for pervasive healthcare [1]–[3]. They provide effective, efficient and accurate monitoring of the vital body signals through the use of interconnected wearable *biosensors*, without disturbing the daily lives of the patients.

In fact, the general infrastructure of a BAN also consists of (i) a central server, in which the collected data is stored, (ii) health professionals, who may try to access the stored data, and (iii) an aggregating device, which transports the aggregated data to the central server. Whereat, BANs include two types of communications: (i) *intra-BAN* and (ii) beyond-BAN communication. The former addresses the communication between the biosensors (including the aggregating device), while the latter defines secure data sharing over the central server, which indeed is out of the scope of this paper.

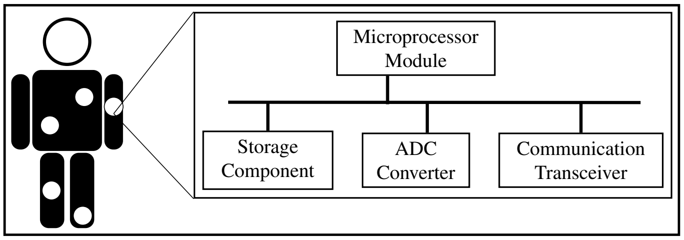

Fig. 1: Body Area Network Infrastructure

Biosensors collect sensitive personal medical data from patients and communicate these data through wireless medium, which exposes a potential for both passive and active attacks [4]. Besides, loosing such information may also lead to privacy leakage [5], [6]. Therefore, secure data protection and secure node-to-host association mechanisms are required before any data transmission [7]. However, due to the crucial power and memory constraints of the biosensors, establishing and maintaining the security of the exchanged data is not a trivial problem. Conventional solutions for generic sensor networks are not applicable in BANs. Essentially, bio-cryptography best suits with the light-weight security protocol requirement, since the BANs are context-aware networks. Using bio-cryptographic approaches, security of the network can be provided in a plug-n-play way; neither a network setup nor a key predistribution mechanism will be needed. On top of it, re-keying will be done automatically. Cryptographic keys can be generated within the network on the fly, when and as needed, through the use of the data collected by the biosensors.

This work was supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under grant 114E557.

Duygu Karaoğlan Altop was supported by TÜBİTAK BİDEB 2211-C.

PervasiveHealth 2015, May 20-23, Istanbul, Turkey

DOI 10.4108/icst.pervasivehealth.2015.260074

Key establishment requires the communicating entities to have something only they know and it is the physiological signals of the individuals in the context of using bio-cryptography in BAN security. In this respect, random numbers generated from the physiological signals derived from different body parts is used to protect the exchanged data.

At this point, the choice of the physiological parameter to be used is of great importance. Physiological signals captured at different parts of the same subject, which will be used to compute the physiological parameter of the security protocol, should be highly correlated independent of the source of measurement and should be chaotic in nature. When the physiological parameters constructed at different biosensors match with each other, it is a very important indication that these biosensors belong to the same host. This outcome avoids potential interference attacks among different BANs and provides secure node-to-host association naturally. In this paper, we propose a novel physiological parameter generation technique and identify an appropriate physiological parameter together with the related physiological signals that can be used in a bio-cryptographic key management protocol designed to secure the BAN communication. Our contributions include: (i) defining a new physiological parameter generation method, (ii) for the first time in the literature, using the blood pressure (BP) signal to generate a physiological parameter, (iii) demonstrating the suitability of the inter-pulse interval (IPI) values derived from the electrocardiogram (ECG), photoplethysmogram (PPG) and BP signals on generating cryptographic keys, and (iv) experimentally analyzing the quality and performance of the generated keys.

The rest of this paper is organized as follows. Section II provides detailed information on the physiological signals that are viable to be used in a security protocol. In Section III, we explore our novel approach on generating physiological parameters and in Section IV, we evaluate the performance and quality of the generated physiological parameters to decide on their applicability on being used as cryptographic keys in BANs. Section V investigates the bio-cryptographic approaches proposed in the literature to secure the BAN communications and their physiological parameter generation methods. Finally, in Section VI, we conclude the paper and provide insights for future work.

II. Suitable Physiological Signals

In a remote health monitoring system, medical professionals generally keep track of the ECG, BP, oxygen saturation (via PPG) and body temperature (BT) signals of the patients. Each of these vital signs has a different device specifically designed for the required recording and each of these devices has a specific place on the human body to be attached. Therefore, in a generic remote health monitoring system, patients should be using at least 4 biosensors. In order for these biosensors to exchange data securely using a bio-cryptographic infrastructure, each biosensor should be able to sense the physiological signal(s) used while generating the predefined physiological parameter. Hence, the choice of the physiological signal(s) to be adopted for physiological parameter generation depends on the ability of the biosensors on retrieving the relevant data. Additionally, this choice also depends on the fact that the generated physiological parameter should meet the requirements of being used as a cryptographic key [8]. First of all, it should be universal; meaning that the biometric trait should be measurable from every user of the system. Secondly, it should be different for different users, at any given time. The reason behind this requirement is not to be able to retrieve any data secured using the biometric features of one person with another person's biometric features. Thirdly, it should be time varying; meaning that it should be different for the same user, at different times. In other words, it should be indistinguishable *only for simultaneous captures* so that the keys can be renewable. Finally, it should be cryptographically random in order to provide security.

Heart rate variability (HRV) measures the intervals between the heart beats. It is the analysis of the beat-to-beat alterations of the heart rate. HRV meets the requirements of a physiological parameter being used as a cryptographic key: (i) it is universally measurable, (ii) it is unique for individuals [9], (iii) it is chaotic in nature [10], and (iv) it is characterized by a bounded random process [11]. Being readily available in several kinds of physiological signals like ECG, PPG and BP, HRV can be approved to be a good candidate for a security providing physiological parameter. The features that can be extracted from HRV include:

- (Normalized) Temporal distances between the fiducials of the physiological signals (difference between the peak points of the signal on the x-axis) [9], [12], [13]
- (Normalized) Amplitude distances between the fiducials of the physiological signals (difference between the peak points of the signal on the y-axis) [12], [13]
- IPI of the physiological signals [8], [14]–[16]
- Frequency features of the physiological signals [17]–[22]

Frequency-domain analysis includes spectral methods, while time-domain analysis determines the heart rate at any point in time between successive complexes [23]. Considering a *specific* physiological signal, frequency-domain analysis of two signals measured at different parts of the human body have similar values independent of the point of measurement, in contrast to time-domain analysis, which results in similar trend but a little diverse values [22]. In light of this fact, frequency-domain methods should be preferred to time-domain ones when short-term recordings are of interest, in order not to increase the overall latency of the system [23]. However, using frequency-domain features of HRV as the physiological parameter of a security protocol necessitates the biosensors to collect the same kind of physiological signals from their hosts. A similar inference can also be made for the (normalized) temporal and/or amplitude distances between the fiducials of the physiological signals, which depend on the physiological signal itself. For instance, the fiducials of the ECG signals and the fiducials of the PPG signals are different from each other. Therefore, none of these HRV features are viable to be used as the physiological parameter of a security protocol, as in the way that they have been proposed in the literature.

On the other hand, IPI, which is the time elapsed between the successive nerve impulses, can be extracted from the HRV derived from any cardiovascular signal, with close values. Hence, the IPI feature of the HRV is readily available in all of the physiological signals required in a remote health monitoring system, except for the BT signal, as depicted in Figure 2. Nevertheless, a BT sensor can be attached to each of the other biosensors capturing the ECG, PPG and BP signals, since the device used to measure the BT signal is far simple and cheaper than the devices used to measure the other signals. Therefore, it can be deduced that the IPI of the HRV is the most suitable physiological feature and the ECG, PPG and BP signals are the most suitable physiological signals to be used in a bio-cryptographic security infrastructure designed for BANs.

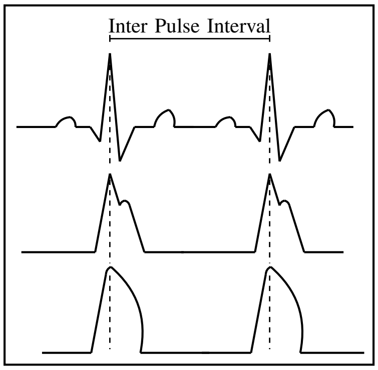

Fig. 2: Ideal ECG (top), PPG (middle) and BP (bottom)

III. Proposed Physiological Parameter Generation Technique

In this section, we describe our physiological parameter generation technique, which is visualized in Figure 3 and defined as in Algorithm 1, where the utilized symbols are listed in Table I. This technique can be applied on the ECG, PPG and BP signals in order to derive IPI-based physiological parameters that can be used as cryptographic keys.

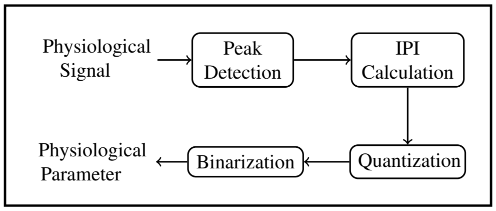

Fig. 3: Proposed IPI-based Physiological Parameter Generation Technique

Algorithm 1 Pseudocode of the Proposed IPI-based Physiological Parameter Generation Technique

```
INPUT: $Signal$, $l$, $g$, $min$, $max$, $s$, $n$
OUTPUT: $PhysParam$
$P = FindPeakLocations(Signal)$
for all $i \in \{1, ..., l\}$ do
    $IPI_i^{init} = P_{i+1} - P_i$
end for
$IPI = zeros\ (l/g)$
$k = 1$
for $i = 1 : g : l$ do
    for all $j \in \{1, ..., g\}$ do
        $IPI(k) = IPI(k) + IPI^{init}(i + j - 1)$
    end for
    $k = k + 1$
end for
$len_{part} = floor\ (max - min)/s$
$part = zeros\ (len_{part})$
$code = zeros\ (len_{part} + 1)$
for all $i \in \{1, ..., len_{part}\}$ do
    $part(i) = min + i * s$
    $code(i) = i \bmod 2^n$
end for
$IPI^{quant} = Quantization\ (IPI, part, code)$
$PhysParam = GrayEncoding\ (IPI^{quant})$
```

TABLE I: Symbols used in Physiological Parameter Generation and Evaluation

Symbol		***Description***
$IPI_{(a,b),i}^{(c,d),j}$	i	IPI index
	a, b	User index
	j	Signal type $\in sig = \{ECG, PPG, BP\}$
	c, d	Start time index of IPI
l		Length of the initial IPI sequence
g		Size of the IPI groups
s		Step size for quantization
min, max		Minimum and maximum values of an IPI
n		Bit length of a quantized and binarized IPI
$D_{(d,s,t)}$	D	Distance between physiological parameters
	d	of different hosts
	s	of the same host at same time
	t	of the same host at different times
FAR		False Accept Rate
FRR		False Reject Rate
HTE		Half Total Error Rate
FAR_{HTE}, FRR_{HTE}		FAR and FRR at HTE
t		Expected value of the elapsed time to generate two matching physiological parameters

First of all, the peak points of the sensed ECG, PPG and BP signals are determined using a generic peak detection function. Then, IPI sequences of length l are generated by computing the time elapsed between the adjacent $(l + 1)$ peak points. After that, in order to decrease the effect of the measurement errors, each IPI sequence is divided into groups of length g and the elements in each group are summed up. At the end of this process, the constructed IPI sequences are of the form IPI_i^j, where $1 \leq i \leq l/g$ defines the IPI index and $j \in \{ECG, PPG, BP\}$ defines the related physiological signal. For instance, if $l = 6$, $g = 2$, and the initial IPI sequence is $\{6, 8, 6, 3, 8, 9\}$, then we have $IPI^j = \{14, 9, 17\}$.

Thereafter, these IPI sequences are quantized in order to further decrease the measurement errors. Here, we apply a circular uniform quantization method, in which the value range of the IPI sequences, $min <= IPI_i^j <= max$ $(\forall i, j)$, are partitioned into blocks using a step size, s, and each partition is mapped to a value from the set $\{0, 1, \ldots, 2^{128/(l/g)} - 1\}$, circularly, where l/g is length of the constructed IPI sequence. We determine the min and max values for the IPI sequence range using 5 minute ECG, PPG and BP recordings of 50 different individuals that are obtained from PhysioBank MIMIC II Waveform database [24]. For instance, if $min = 1$, $max = 40$, $s = 4$ and $l/g = 64$, then the partitions are defined as $\{1 - 4, 5 - 8, \ldots, 37 - 40\}$ and the IPI values that appear in the first, fifth and ninth partitions are assigned to 0, the ones that appear in the second, sixth and tenth partitions are assigned to 1, and so forth.

Finally, Gray encoding, i.e. $\{0, 1, 2, 3\} \mapsto \{00, 01, 11, 10\}$, is applied on the resulting quantized IPI sequences in order to increase the error margin of the physiological parameters generated in different BANs. For instance, if $IPI = \{14, 9, 17\}$ and $n = 2$, then the resulting quantized IPI sequence will be $\{3, 2, 0\}$ and the encoded physiological parameter will be $\{10, 11, 00\}$.

At the very end of the physiological parameter generation method described above, a 128 bit binary sequence is generated as the physiological parameter.

IV. Performance Analysis

In this section, we analyze the performance of the generated physiological parameters in terms of their randomness, distinctiveness, temporal variance and error rates. We conduct our experiments on the ECG, PPG and BP signals obtained from the publicly available PhysioBank MIMIC II Waveform database [24]. We downloaded 5 minutes of data (per subject), sampled at 125 Hz, from 50 different subjects. Each recording includes a simultaneous measurement of all ECG, PPG and BP signals.

We randomly selected 10 different starting points to compute IPI sequences with lengths $l = 32$, $l = 64$ and $l = 128$, from each of the aforementioned signals. These IPI sequences are then used to generate 5 different physiological parameters:

- IPI sequences of length 32 and 64 are used as they are ($g = 1$ and $l = 32$ or $l = 64$);
- IPI sequences of length 64 and 128 are divided into groups of 2 ($g = 2$ and $l = 64$ or $l = 128$);
- IPI sequences of length 128 are divided into groups of 4 ($g = 4$ and $l = 128$)

We implemented and analyzed our physiological parameter generation methods using Matlab. As discussed in the below subsections one by one, results of the evaluation metrics show that most of the generated physiological parameters meet the requirements of being used as cryptographic keys.

A. Randomness

Being random is one of the requirements of a physiological parameter for it to be used as a cryptographic key. In order to evaluate the randomness of the generated IPI-based physiological parameters, we use the Shannon's entropy, which is computed as in Equation 1, where $P(\cdot)$ is the probability mass function. According to this evaluation metric, the randomness level of the input sequence increases as H approaches to 1.

$$H = -\sum_i P(IPI_i) log_2 P(IPI_i) \tag{1}$$

Table II shows the average randomness of the generated physiological parameters, where l is the length of the initial IPI sequence, g is the group size and s is the step size. Results reveal that the physiological parameters generated using the accumulated IPI sequences appear to be more random than the ones that are generated using the singleton sequences, for most of the step size values. For instance, the physiological parameters generated using $l = 64$ and $g = 2$ or $l = 128$ and $g = 4$ are more random than the ones generated using $l = 32$ and $g = 1$. Among the generated 36 different physiological parameters, 23 of them ($\sim 64\%$), the ones with a Shannon's entropy of greater than 0.7, are applicable to be used as cryptographic keys.

TABLE II: Randomness of the IPI-based Physiological Parameters - Underlined values indicate that the corresponding physiological parameters have high level of randomness.

s **l, g**	**2**	**3**	**4**	**5**	**6**	**7**
32, 1	$\underline{0.91}$	0.37	$\underline{0.85}$	$\underline{0.99}$	$\underline{0.87}$	$\underline{0.99}$
64, 1	0.65	0.43	0.39	$\underline{0.99}$	0.39	$\underline{0.99}$
64, 2	$\underline{0.99}$	$\underline{0.96}$	$\underline{0.86}$	0.53	$\underline{0.85}$	$\underline{0.84}$
128, 2	$\underline{0.99}$	$\underline{0.95}$	$\underline{0.91}$	$\underline{0.72}$	0.51	0.42
128, 4	$\underline{0.96}$	$\underline{0.89}$	$\underline{0.86}$	$\underline{0.79}$	$\underline{0.99}$	0.69

B. Distinctiveness

Another requirement of a physiological parameter for being used as a cryptographic key is that it should be different for different users, at any given time. This requirement also implies that the two physiological parameters generated at the same time by the two different biosensors of the same host should have similar values. In order to evaluate the distinctiveness of the generated IPI-based physiological parameters, we use the average Hamming distance metric, as defined in Equation 2, where D_s is the distance between the physiological parameters that are generated from the same host, D_d is the distance between the physiological parameters that are generated from different hosts, $|sig|$ is the length of the utilized physiological signal set, a and b defines the subject indexes, i defines the IPI index, and j and k defines the signal types.

Figure 4 shows the average differences between the generated physiological parameters, where l is the length of the initial IPI sequence, g is the group size and s is the step size. In order for the generated physiological parameters to

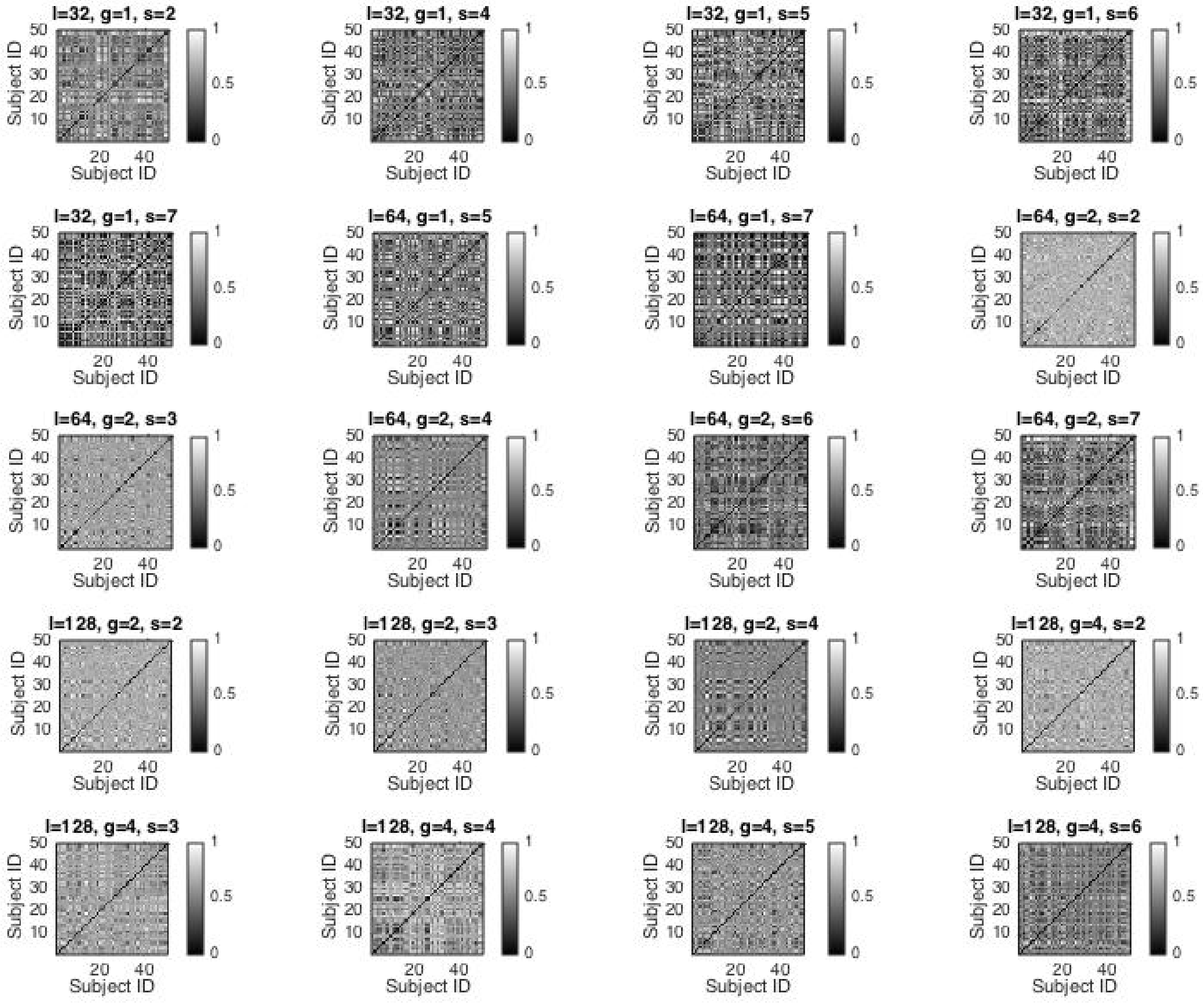

Fig. 4: Distinctiveness of the IPI-based Physiological Parameters - In each sub-figure, diagonal and non-diagonal cells hold the average Hamming distances between the IPI-based physiological parameters generated from the same host and from different hosts, respectively. The value at the cell (x, y) is the average Hamming distance between the physiological parameters of the x^{th} and y^{th} hosts and the darkness of this cell represents the proximity of these physiological parameters, i.e., if the average Hamming distance is close to 0, then the cell will be darker, indicating that the related physiological parameters are identical.

be distinctive for different users, Hamming distances between the IPI-based physiological parameters that are generated from the same host (diagonal cells), should be as dark as possible, i.e. close to 0, and Hamming distances between the ones that are generated from different hosts (non-diagonal cells), should be as light as possible, i.e. close to 1. Results show that the average Hamming distance between the IPI-based physiological parameters derived by different BANs' biosensors are quite large, while the average Hamming distance between the IPI-based physiological parameters derived simultaneously by the same BAN's biosensors are very low. Results also show that using the accumulated IPI sequences better separates different users than using the singleton IPI sequences, independent of the step size, considering the fact that the color tone difference between the diagonal and non-diagonal cells indicates the degree to which the interpersonal distinction can be accomplished.

$$\begin{aligned} D_s &= \left(\sum_{a=b, j \neq k} (|IPI_{a,i}^{j} - IPI_{b,i}^{k}|) \right) / \binom{|sig|}{2} \\ D_d &= \left(\sum_{a \neq b} (|IPI_{a,i}^{j} - IPI_{b,i}^{k}|) \right) / \, |sig|^2 \end{aligned} \tag{2}$$

C. Temporal Variance

Being different for the same user at different time intervals is another requirement for a physiological parameter to be used as a cryptographic key. Temporal variance evaluates the similarity between the two physiological parameters that are generated by the biosensors of the same BAN at different time intervals. In order to evaluate the temporal variance of the generated IPI-based physiological parameters, we define a new metric: the average *temporal ratio* metric, which identifies whether the average Hamming distance between the physiological parameters that are generated from the same host at different time intervals, D_t, is close to the average Hamming distance between the physiological parameters that are generated from the same host at the same time, D_s, or from different hosts, D_d. This metric is evaluated as defined in Equation 3, where D_s and D_d are as given in Equation 2, and D_t is as given in Equation 4, where $|sig|$ is the length of the utilized physiological signal set, c and d defines different start times, i defines the IPI index, and j and k defines the signal types. According to this temporal ratio metric, having R value that is greater than 1 implies that the generated physiological parameters will not match with each other, meaning that they have temporal variance.

$$R = \frac{D_s - D_t}{D_d - D_t} \tag{3}$$

$$D_t = \left(\sum_{c \neq d} (|IPI_i^{c,j} - IPI_i^{d,k}|) \right) / \, |sig|^2 \tag{4}$$

Table III shows the average temporal ratio of the generated physiological parameters, where l is the length of the initial IPI sequence, g is the group size and s is the step size. Results reveal that the physiological parameters that are generated using the singleton IPI sequences do not have temporal variance, except for the one with $l = 64$ and $s = 2$, which was already eliminated because of the randomness level it exhibits. Among the 18 physiological parameters that are generated using the accumulated IPI sequences, 14 of them ($\sim$ 78%) are applicable to be used as cryptographic keys.

TABLE III: Temporal Variance of the IPI-based Physiological Parameters - Underlined values indicate that the corresponding physiological parameters have temporal variance.

s **l, g**	**2**	**3**	**4**	**5**	**6**	**7**
32, 1	0.71	0.43	0.36	0.29	0.27	0.23
64, 1	$\underline{1.31}$	0.66	0.88	0.47	0.42	0.46
64, 2	$\underline{4.99}$	$\underline{2.62}$	$\underline{1.45}$	$\underline{1.47}$	0.58	0.48
128, 2	$\underline{3.98}$	$\underline{2.55}$	$\underline{1.42}$	$\underline{1.24}$	$\underline{1.09}$	0.78
128, 4	$\underline{2.63}$	$\underline{2.07}$	$\underline{1.41}$	$\underline{1.21}$	$\underline{1.17}$	0.87

D. Error Rates

Performance of the biometric systems are generally evaluated using the *False Accept Rate* (FAR), which is the percentage of the imposters accepted by the system, and the *False Reject Rate* (FRR), which is the percentage of the genuines rejected by the system. In the context of bio-cryptographic key generation, FAR corresponds to the percentage of the matched physiological parameters that should be unmatched, while FRR corresponds to the percentage of the unmatched physiological parameters that should be matched. Equal Error Rate (EER), on the other hand, is defined as the rate at which the FAR and FRR are equal to each other. Basically, EERs of different systems are compared so as to pick the one with the lowest EER as the most accurate system. The EER value of a system can be obtained through the Receiver Operating Curve (ROC) that plots the characterization of the trade-off between the FAR and FRR.

Figure 5 shows the ROCs for the generated IPI-based physiological parameters, which are resolved to be applicable for being utilized as cryptographic keys in consequence of the above discussions, with respect to different threshold values, where l is the length of the initial IPI sequence, g is the group size, s is the step size. In each subfigure, the point at which the ROC and the black dotted linear line intersects defines the EER of the related technique. Table IV, on the other hand, includes the statistics derived from the related data, where FAR_{HTE} and FRR_{HTE} are the FAR and FRR values at the half total error rate, $HTE = (FAR{+}FRR)/2$, and t is the expected value of the time elapsed to generate two matching physiological parameters, which is computed as in Equation 5, where 0.0142 is the common IPI of adults in minutes.

$$t = \frac{1}{1 - FRR_{HTE}} * l * 0.0142 \tag{5}$$

Results reveal a trade-off between the delay of generating two matching physiological parameters and the security level of the system. For instance, according to the EER values, the physiological parameter that is generated with $l = 128$, $g = 4$ and $s = 6$ performs better than the other two, which has the highest expected delay.

TABLE IV: Statistical Information of the IPI-based Physiological Parameters

l, g	**s**	**EER**	$\mathbf{FAR_{HTE}}$	$\mathbf{FRR_{HTE}}$	**t (minute)**
64, 2	4	0.135	0.139	0.131	0.97
128, 2	5	0.096	0.111	0.081	1.91
128, 4	6	0.059	0.058	0.060	1.92

V. Related Work and Discussions

Approaches for securing the communication among the biosensors by means of bio-cryptography consists of feature extraction and fuzzy cryptography. Fuzzy cryptography can be divided into three categories [25]: (i) fuzzy commitment based key binding, (ii) fuzzy vault based key binding, and (iii) key generation. In the former two methods, biosensors use the physiological parameters, which are derived from the sensed signals, to conceal a shared key, while in the last method, they use the computed physiological parameters as the shared key itself. In all of these approaches, biosensors simultaneously sense a predefined set of physiological signals for a predefined

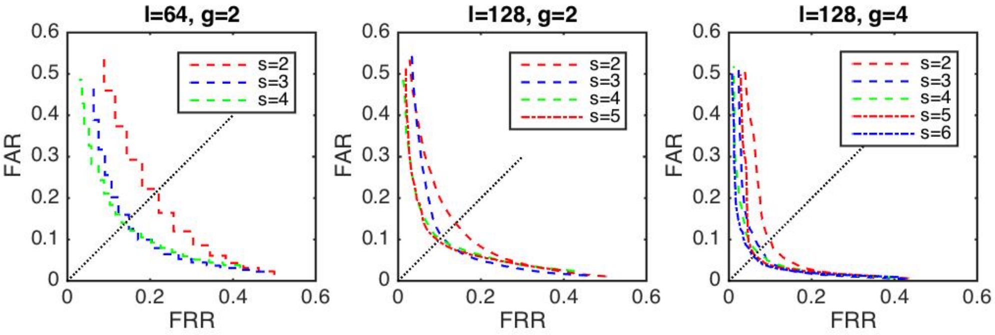

Fig. 5: ROCs for the IPI-based Physiological Parameters

period of time and generate pseudorandom numbers from these signals. The pseudorandom number generation process includes feature extraction, which can be done by either frequency-domain or time-domain analysis.

Venkatasubramanian et al. [17], [18], Banerjee et al. [20], Zhang et al. [21] and Miao et al. [19] propose fuzzy vault based bio-cryptographic key binding protocols and Venkatasubramanian et al. [22] propose a bio-cryptographic key generation protocol that are specifically designed for BANs. In each of these proposals, frequency-domain features of either ECG or PPG signals are utilized as the physiological parameter. The authors first divide the corresponding signal into x overlapping windows of y samples each. Then, they perform y point FFT (Fast Fourier Transform) on each of these parts and pass the first z FFT coefficients of the x windows through a peak detection function. Finally, they quantize the peak index and peak value pairs into binary strings, according to the standard deviations and means of these values, and concatenate them. The most important drawback of these protocols is that the authors assume that all of the BAN nodes are capable of measuring the predefined physiological signal, either ECG or PPG. In fact, using frequency-domain features induces this drawback, as also discussed in Section 2.

Besides, Bao et al. propose a fuzzy commitment based key distribution protocol [15] and an entity authentication protocol [14], in which the IPI values derived from the PPG signals are used as the physiological parameters. In their proposals, the authors use adaptive segmentation to divide the value range of the IPI sequence into segments and map the values in each segment into binary words. Poon et al. [8] further evaluate the performance of this physiological parameter generation approach, using both ECG and PPG signals, with respect to their error rates. In their subsequent work, Bao et al. [16] propose another physiological parameter generation method that can be used in a bio-cryptographic security protocol. In this method, the authors first divide the ECG and PPG signals into segments so that each segment contains 16 IPI values. Then, they add up the IPI values of each segment, randomize these values by computing their 2^p modulus and divide the resulting modulus values by 2^{p-q} to compensate measurement differences. The authors argue that the physiological parameters generated using the individual and multi-level IPI sequences have comparable randomness and distinctiveness. They also compare the error rates of the physiological parameters generated using the multi-level IPI sequences with the results of their previous work [14] and indicate that this technique can provide a lower minimum HTE, which is 0.0283. Nevertheless, the latency of this method is very high, i.e. $16 * 16 = 256$ IPI values are required to generate a 64 bit physiological parameter, and with the provided error rates it takes ~ 3.7 minutes to generate two matching physiological parameters. On the contrary, our protocol can generate two matching 128 bit physiological parameters in ~ 1.92 minutes at maximum, as also mentioned in Section IV-D. In a bio-cryptographic security infrastructure designed for BANs, in order for the cryptographic keys to be generated from the captured physiological signals *in real-time*, the delay of the key generation process should be at minimum.

An alternative physiological parameter generation method is also proposed by Xu et al. [26], in which the IPI values derived from the ECG signals are used. The authors adopt Gray encoding and map each IPI value to a 4 bit binary word using uniform quantization, where the quantization levels are decided based on the mean and standard deviation of a 15 minute recording of an ECG signal. The authors state that the generated physiological parameters pass the first 9 randomness evaluation tests provided by the NIST test suit [27]. They also express that the generated physiological parameters possess both distinctiveness and temporal variance, according to a Hamming distance evaluation. Unfortunately, this work does not include the relevant numerical data for the experimental performance results.

VI. Conclusions and Future Work

BANs are the most important building stone of pervasive healthcare, enabling continuous, remote and real-time patient monitoring through the use of biosensors. These small wearable sensing devices are limited in energy and storage, and they collect very important and sensitive personal information. Therefore, light-weight security solutions are required for

BANs in order both to preserve the privacy of the user and to provide the security of the exchanged data. In this paper, we propose a novel physiological parameter generation technique and demonstrate the performance of the generated IPI-based physiological parameters in terms of their randomness, distinctiveness, temporal variance and error rates. Results show that, when appropriate parameters are used in the generation process, physiological parameters computed from the IPI sequences derived from the ECG, PPG and BP signals are applicable to be used as cryptographic keys in a bio-cryptographic security protocol designed for BANs.

Our future work includes the design and analysis of a new bio-cryptographic key management protocol that does not possess the deficiencies of the existing ones, which are analyzed in detail in [25]. Our aim will be to comprise a security infrastructure that can provide privacy preservation with low communication and computational overheads and low key generation latency. We will also evaluate the performance of the generated physiological parameters when used in the existing key binding and key generation based bio-cryptographic security infrastructures and compare the results with that of ours.

References

[1] J. O'Donoghue and J. Herbert, "Profile based sensor data acquisition in a ubiquitous medical environmet," in *Proceedings of the Pervasive Computing and Communications Workshops (PerComW)*. IEEE Computer Society, Washington, Pisa, Italy, 13–17 March 2006, pp. 570–574.

[2] G.-Z. Yang, *Body Sensor Networks*, 1st ed. London: Springer-Verlag, 2006.

[3] U. Varshney, "Pervasive healthcare and wireless health monitoring," *Mobile Networks and Applications*, vol. 12, no. 2/3, pp. 113–127, 2007.

[4] M. S. Siddiqui and C. S. Hong, "Security issues in wireless mesh networks," in *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE)*. IEEE Computer Society, Washington, Seoul, Korea, 26–28 April 2007, pp. 717–722.

[5] R. J. Anderson, "A security policy model for clinical information systems," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Washington, Oakland, CA, 6–8 May 1996, pp. 30–43.

[6] A. Bhargava and M. Zoltowski, in *Proceedings of the International Workshop on Database and Expert Systems Applications (DEXA)*. IEEE Computer Society, Washington, Prague, Czech Republic, 1–5 September 2003, pp. 956–960.

[7] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16–23, 2004.

[8] C. 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.

[9] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to identify individuals," *Pattern Recognition*, vol. 38, no. 1, pp. 133–142, 2005.

[10] K. Vibe, J.-M. Vesin, and E. Pruvot, "Chaos and heart rate variability," in *Proceedings of the International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*. IEEE Press, Portland, Montreal, Canada, 20–23 September 1995, pp. 1481–1482.

[11] S. Lu, J. Kanters, and K. H. Chon, "A new stochastic model to interpret heart rate variability," in *Proceedings of the International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*. IEEE Press, Portland, Cancun, Mexico, 17–21 September 2003, pp. 2303–2306.

[12] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: A new approach in human identification," *IEEE Transactions on Instrumentation and Measurement*, vol. 50, no. 3, pp. 808–812, 2001.

[13] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric recognition," *Eurasip Journal on Advances in Signal Processing*, vol. 2008, pp. 19:1–19:11, 2008.

[14] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Proceedings of the 27th Annual International Conference of the IEEE-EMBS on Engineering in Medicine and Biology Society*, China, 1–4 September 2005, pp. 2455–2458.

[15] S.-D. Bao, L.-F. Shen, and Y.-T. Zhang, "A novel key distribution of body area networks for telemedicine," in *Proceedings of the IEEE International Workshop on Biomedical Circuits and Systems*. IEEE Press, Portland, Singapore, 1–3 December 2004, pp. 1–20.

[16] S.-D. Bao, C. 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, pp. 772–779, 2008.

[17] 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.

[18] K. K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*. IEEE Press, Portland, San Diego, CA, 16–19 November 2008, pp. 1–7.

[19] F. Miao, L. Jiang, Y. Li, and Y.-T. Zhang, "Biometrics based novel key distribution solution for body sensor networks," in *Proceedings of the International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS)*. IEEE Press, Portland, Minneapolis, MN, 3–6 September 2009, pp. 2458–2461.

[20] A. Banerjee, K. Venkatasubramanian, and S. K. S. Gupta, "Challenges of implementing cyber-physical security solutions in body area networks," in *Proceedings of the Fourth International Conference on Body Area Networks*. ICST, Belgium, LA, California, 1–3 April 2009, pp. 18:1–18:8.

[21] Z. Zhang, H. Wang, A. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070–1078, 2012.

[22] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proceedings of the IEEE International Conference on Computer Communications Workshop (INFOCOM)*. IEEE Press, Portland, Phoenix, AZ, 13–18 April 2008, pp. 1–6.

[23] Task Force of the European Society of Cardiology the North American Society of Pacing Electrophysiology, "Heart Rate Variability: Standards of measurement, physiological interpretation, and clinical use," *European Heart Journal*, vol. 17, pp. 354–381, 1996.

[24] D. Kreiseler and R. Bousseliot, "Automatisierte EKG-Auswertung mit Hilfe der EKG-Signaldatenbank CARDIODAT der PTB," *Biomedizinische Technik/Biomedical Engineering*, vol. 40, no. 1, pp. 319–320, 2009.

[25] D. Karaoğlan and A. Levi, "A survey on the development of security mechanisms for body area networks," *The Computer Journal*, vol. 57, no. 1, pp. 1484–1512, 2014.

[26] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *Proceedings of the IEEE INFOCOM*, Shanghai, China, 10–15 April 2011, pp. 1862–1870.

[27] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "Statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards & Technology, Tech. Rep., 2010.