Secure Key Generation Using Gait Features for Body Sensor Networks

Yingnan Sun, Charence Wong, Guang-Zhong Yang, and Benny Lo

***Abstract*— With increasing popularity of wearable and Body Sensor Networks technologies, there is a growing concern on the security and data protection of such low-power pervasive devices. With very limited computational power, BSN sensors often cannot provide the necessary data protection to collect and process sensitive personal information. Since conventional network security schemes are too computationally demanding for miniaturized BSN sensors, new methods of securing BSNs have proposed, in which Biometric Cryptosystem (BCS) appears to be an effective solution. With regards to BCS security solutions, physiological traits, such as an individual's face, iris, fingerprint, electrocardiogram (ECG), and photoplethysmogram (PPG) have been widely exploited. However, behavioural traits such as gait are rarely studied. In this paper, a novel light-weight symmetric key generation scheme based on the timing information of gait is proposed. By extracting similar timing information from gait acceleration signals simultaneously from body worn sensors, symmetric keys can be generated on all the sensor nodes at the same time. Based on the characteristics of generated keys and BSNs, a fuzzy commitment based key distribution scheme is also developed to distribute the keys amongst the sensor nodes.**

I. INTRODUCTION

With the aim of providing pervasive health monitoring, Body Sensor Networks (BSN) capture and process sensitive personal information, such as physiological data, life style preferences, etc. Such information could be targeted by hackers to cause harm to the users [1]. With no user interface and limited computational power in the sensor node, security solutions for BSN have to be light weight, energy efficient and autonomous. A widely researched security solution for BSNs is biometric cryptosystem (BCS), which utilizes biometrics, such as ECG, PPG, and fingerprints, to secure the body sensing signals [2]. The primary advantages of employing biometrics are twofold. First, biometrics can be easily collected by body worn sensor nodes, which means that no key pre-deployment is required; second, biometrics are unique and permanent [3], which makes it especially suitable for user authentication.

The state-of-the-art BCSs employ Fast Fourier Transform (FFT) [4], [5] and Discrete Wavelet Transform (DWT) [6] to extract frequency and spatial coefficients from ECG signals captured by BSN sensor nodes, which are then used to generate binary sequences to form a common secret key for the secure network communication. However, as frequency domain analysis is computationally demanding, the proposed schemes are often too complex for real time processing in miniaturized BSN sensor nodes. Another approach is to use the variations of Inter-pulse Intervals (IPI) of consecutive ECG pulses; this particular approach has been exploited by [7]–[9]. IPI-based BCS approaches are relatively light weight in comparison to FFT and DWT key generation schemes. Although ECG and PPG signals are available to many wearable devices and mobile phones, the majority of wearable devices are often unable to obtain correct ECG or PPG measurement without user intervention. With the aim of developing a security scheme for BSN, we propose the use of gait biometrics for key generation for BSN. The scheme is based on gait acceleration signals measured by accelerometers, which are readily available in most wearable devices and mobile phones. The scheme is capable of generating and distributing secret keys amongst sensor nodes without complex frequency domain analysis.

Gait acceleration signals as a biometric behavioural trait has been proposed for authentication [10] and recognition [11], [12]; however, the feasibility of adopting gait in BCSs requires further investigation. An automatic key generation scheme based on gait was proposed by [13], [14], in which Independent Component Analysis (ICA) is applied to separate accelerations produced from leg motions and arm swing motions. As previously mentioned, complex frequency domain analysis introduces high computation overheads to the security system; therefore, the scheme may not be suitable for typical BSN sensors. In addition to the design complexity, the key generation scheme in [13] requires a number of message exchanges during key establishment, which results in more overheads in the channel. Another device-to-device authentication scheme using gait was recently proposed in [15], where gait fingerprint bits are extracted from energy level difference between each gait cycle and the average gait cycle. In a similar work [16], the secret key is generated from a set of extracted features in both time and frequency domains from gait signals. In addition to the high computation overheads of FFT and Discrete Cosine Transform (DCT) analysis in this scheme, the error rate of the generated key will rapidly increase if the key size is greater than 40 bits.

This paper proposes a novel light-weight symmetric key generation scheme based on gait events timing from acceleration signals. The rest of the paper is organized as follows: Section II presents the details of the proposed scheme, system models, gait event extraction algorithms, and experimental set-up. An evaluation of the proposed scheme along with a discussion relating to the results are provided in Section III, while the final section provides the conclusions, discussions, and future works.

Yingnan Sun, Charence Wong, Guang-Zhong Yang and Benny Lo are with the Hamlyn Centre, Imperial College London, London SW7 2AZ, UK, e-mail:{y.sun16, charence.wong05, g.z.yang, benny.lo}@imperial.ac.uk

978-1-5090-6244-7/17/$31.00 ©2017 IEEE

II. METHODS

A. System Modelling and Experimental Set-up

As shown in Fig. 1, a typical BSN employs the star topology, where sensor nodes only communicate directly with the network coordinator, which is often a mobile phone. Sensor information is then aggregated by the coordinator before being forwarded to the server via Wi-Fi or a mobile network.

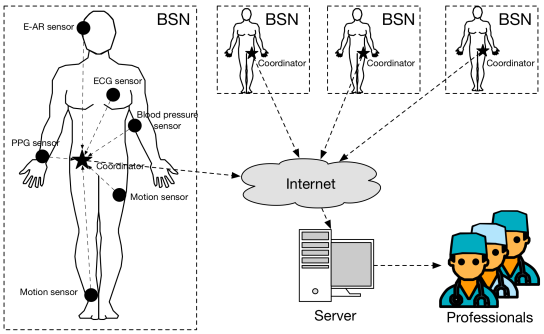


Fig. 1. Design of a typical BSN system

Our key generation and distribution scheme is focused on securing wireless communication amongst a network of sensors worn by a user, where gait acceleration signals can be obtained directly from the sensor node with its embedded accelerometer. Fig. 2 illustrates the acceleration signal of an entire gait cycle on a sensor worn on the back, which consists of a right step and a consecutive left step, along the Superior-Inferior (SI) axis. There are seven key gait events: right heel contact, left toe off, heel off, left heel contact, right toe off, feet adjacent, and tibia vertical. The timing of each gait event varies from cycle to cycle, which is used in the proposed scheme for generating the biometric key. For the ease of explanation, ECG pulse naming convention is applied to label one gait cycle as indicated in Fig. 2: right or left heel contact in a gait cycle is denoted as P wave; right or left foot flat pulse is named QRSTU complex, while valley S represents the toe-off event, the pulse in the mid-stance phase between toe-off and heel off is labelled as T, and finally heel off event is named as U. Gait events often have a slight variation between each gait cycle, so that they can all be used to generate random binary sequences. Although any of the gait events can be used in the proposed scheme, only R peaks are used for the explanation in the rest of the paper.

For data collection, we used two iPhones and an e-AR sensor in our experiments, while acceleration data was captured and recorded in each device separately. The e-AR sensor is an ear-worn activity recognition sensor, designed for gait analysis [17]. The data was then downloaded onto a computer for processing. The proposed key generation and distribution scheme was implemented, simulated and evaluated using Matlab R2016b. To evaluate the performance of the scheme, we have first conducted an experiment with one iPhone placed on the lower back and another placed on the front of the waist of each subject, and about 300 steps were collected from 5 test subjects. A second experiment was conducted with one iPhone placed on the lower back and the other iPhone placed on the right upper arm of each subject. Finally, a third experiment was carried out by placing one iPhone on the lower back and the e-AR sensor on right ear of the test subjects.

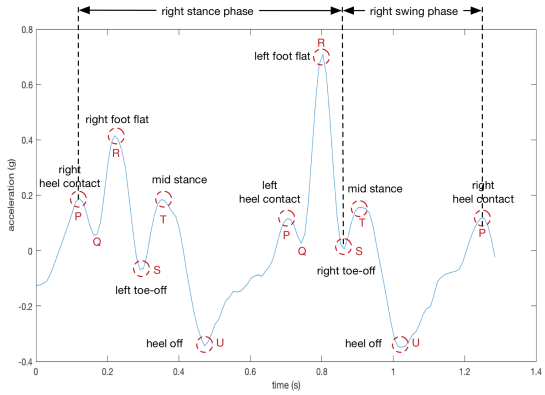


Fig. 2. Gait acceleration data in the inverted gravity direction

B. Signal Preprocessing

Acceleration signals collected by a sensor node are captured in respect of its own orientation and coordinate system; therefore, to extract accurate gait features from body worn sensors, the acceleration signals have to be projected onto the same coordinate system [13]. In the proposed scheme, rotation matrix $\mathbb{R}^{3\times3}$ is multiplied to the 3-axis acceleration signals, denoted as Acc_x, Acc_y, Acc_z, to project the acceleration signals onto the common world coordinate system:

$$\begin{bmatrix} Acc_N \\ Acc_E \\ Acc_{-G} \end{bmatrix} = \mathbb{R} \begin{bmatrix} Acc_x \\ Acc_y \\ Acc_z \end{bmatrix} \tag{1}$$

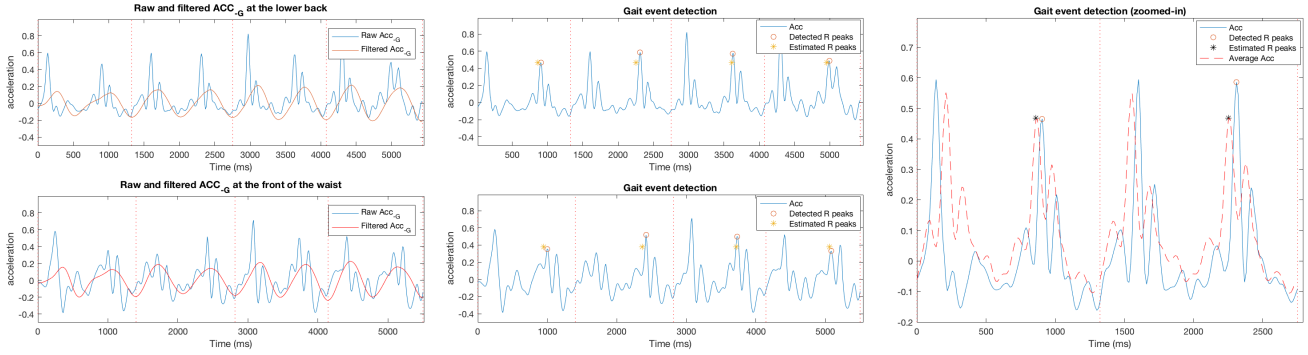
where Acc_N, Acc_E, and Acc_{-G} are acceleration signals along North, East, and inverted gravity directions in the world coordinate system; and rotation matrix $\mathbb{R}$ is derived from the quaternion vector $\mathbf{q} = [w,x,y,z]^T$ provided by iOS API using

$$\mathbb{R} = \begin{bmatrix} 1-2(y^2+z^2) & 2(xy-wz) & 2(xz+wy) \\ 2(xy+wz) & 1-2(x^2+z^2) & 2(yz-wx) \\ 2(xz-wy) & 2(yz+wx) & 1-2(x^2+y^2) \end{bmatrix} \tag{2}$$

The quaternion vector $\mathbf{q}$ can be calculated from raw gyroscope data as followings: [18]

$$\mathbf{q} = \begin{bmatrix} w \\ x \\ y \\ z \end{bmatrix} = \begin{bmatrix} cos(\frac{\alpha}{2})cos(\frac{\beta}{2})cos(\frac{\gamma}{2}) + sin(\frac{\alpha}{2})sin(\frac{\beta}{2})sin(\frac{\gamma}{2}) \\ cos(\frac{\alpha}{2})sin(\frac{\beta}{2})cos(\frac{\gamma}{2}) - sin(\frac{\alpha}{2})cos(\frac{\beta}{2})sin(\frac{\gamma}{2}) \\ sin(\frac{\alpha}{2})cos(\frac{\beta}{2})cos(\frac{\gamma}{2}) + cos(\frac{\alpha}{2})sin(\frac{\beta}{2})sin(\frac{\gamma}{2}) \\ cos(\frac{\alpha}{2})cos(\frac{\beta}{2})sin(\frac{\gamma}{2}) - sin(\frac{\alpha}{2})sin(\frac{\beta}{2})cos(\frac{\gamma}{2}) \end{bmatrix} \tag{3}$$

where α, β, and γ are the raw 3-axis gyroscope signals recorded alongside with acceleration signals. By projecting the sensor signals onto the same coordinate system, the



(a) (b) (c)

Fig. 3. Gait cycle and gait event detection

accuracy of the gait event detection can be improved significantly, even though, the proposed key generation scheme can work without projection, as it mainly relies on the timing information.

In the proposed scheme, only Acc_{-G} is considered due to the fact that gait events can be directly extracted from the acceleration signal in the $-G$ direction.

C. Gait Cycle and Gait Event Detection

A low pass filter with a cut-off frequency of 10Hz is applied to Acc_{-G}, as indicated in Fig. 3(a), to identify and split repetitive gait cycles in Acc_{-G}. 10Hz is chosen as the cut-off frequency because human motion has no significant effects on frequencies above 10Hz [15]. Assuming N gait cycles are found, the detected gait cycles

$$\mathbf{a} = [a_1, ..., a_i, ..., a_N]$$

are then interpolated or decimated to the same length, $\overline{T}$, and the average gait cycle $\overline{\mathbf{a}}$ is obtained. Then, the desired R peak $(\overline{t}, \overline{y})$ in $\overline{\mathbf{a}}$ can be found. $\overline{t}$ stands for the average time from the start to the desired R peak in each gait cycles, and $\overline{y}$ is the average magnitude of those R peaks. However, in each gait cycle, the estimated time from the start of a gait cycle to the estimated R peak, $\widetilde{t}_i$, has to be adjusted as

$$\widetilde{t}_i = \frac{T_i}{\overline{T}}\overline{t}$$

where $i = 1, ..., N$. T_i is the interval of $\mathbf{a}$, and $\overline{T}$ is the interval of $\overline{\mathbf{a}}$:

$$\overline{T} = \left\lfloor \frac{1}{N}\sum_{i=1}^{N} T_i \right\rfloor$$

On the other hand, $\overline{y}$ can be used directly as the estimated magnitude of the R peaks, $\widetilde{y}_i = \overline{y}$ because human gait is highly repetitive and gait events are likely to occur at the same positions in every gait cycle as indicated in Fig. 3. To simplify the representation of the estimated R peaks, it is represented as

$$\widetilde{p}_i = (\widetilde{t}_i, \widetilde{y}_i)$$

Next, all R the peaks, $\mathbf{p} = [\mathbf{p}_1, ..., \mathbf{p}_i, ..., \mathbf{p}_N]$, in Acc_{-G} are detected, and $\mathbf{p}_i = [p_{i_1}, ..., p_{i_m}, ..., p_{i_M}]$ represents the detected peaks in one interval T_i. Only the peaks closest to $\widetilde{p}_i$ are selected as the actual R peaks. The selected R peak corresponds to each interval T_i is represented as:

$$\hat{p}_i = \arg\min_{p_{i_m}} |p_{i_m} - \widetilde{p}_i|$$

Finally, the selected R peaks in the entire signal ACC_{-G} is shown as

$$\hat{\mathbf{p}} = [\hat{p}_1, ..., \hat{p}_i, ..., \hat{p}_N]$$

where $\hat{p}_i$ is the final selected peak in the i^{th} gait cycle. During data collection, subjects were instructed to walk at a normal constant speed. However, even at normal speed, temporal variations still exist between each gait cycle, which is the source of the randomness in the generated binary sequences. $\hat{p}_i$ will likely drift from the estimated time $\widetilde{t}$ and magnitude $\widetilde{y}$ as shown in Fig. 3(b) and 3(c), which are the two example results of the R peak detection algorithms.

Algorithm 1 Pseudo code for binary sequence generation

Require: $ACC \leftarrow$ Acceleration sample
$n \leftarrow$ Codeword length $f \leftarrow$ Sampling frequency
$q \leftarrow$ Bits generated per gait cycle

function GENBS(ACC,n,f,q)
  $accT \leftarrow$ PEAK_DETECTION(ACC)
  for i=1 to $length(accT)$-1 **do**
    $IPI(i) \leftarrow accT(i+1) - accT(i)$
  end for
  $IPI \leftarrow mod(round(IPI/(m \times 1000/f)), 2^q)$
  $grayIPI \leftarrow bin2gray(IPI, 'qam', 2^q)$
  $R \leftarrow de2bi(grayIPI, '$left-msb$')$
  $[rr, cc] \leftarrow size(R)$
  $reshapeR \leftarrow reshape(R^T, [1\ rr \times cc])^T$
  $S \leftarrow S(1:n)$
  return S
end function

D. Key Generation

Upon receiving the synchronization signal from the coordinator, all the sensor nodes and the coordinator in the same BSN will start recording 3-axis gait acceleration signals, and the signals will be projected onto the world coordinate

system using Eq. 1. Then, the R peak detection algorithm will be applied to the acceleration signal Acc_G to find the timing of R peaks $accT$, and the inter-pulse interval IPI is calculated. Next, as $accT$ is in milliseconds, IPI is divided by $m \times \frac{1000}{f_s}$ and a round operation is applied afterwards. Round and modulo operations are also applied to IPI to quantize it into 2^q levels. To improve the bit agreement rate, IPI is mapped onto gray coded $grayIPI$ using the Matlab function $bin2gray$, and an integer to binary Matlab function $de2bi$ is applied to $grayIPI$, producing a binary matrix $R^{q\times N}$. Finally, $R^{q\times N}$ is reshaped into $reshapeR^{1\times q\cdot N}$ using Matlab function $reshape$, and the first n bits are used for generating binary sequence S. n is the codeword length used in the BCH scheme. The procedures are summarized in Algorithm 1.

Algorithm 2 Pseudo code for the network simulation

Require: $k \leftarrow$ Key length $n \leftarrow$ Codeword length
$f \leftarrow$ Sampling frequency
$q \leftarrow$ Bits generated per gait cycle
$ACC \leftarrow$ Device 1 acceleration sample
$S \leftarrow \text{GENBS}(ACC, n, f, q)$ ▷ Algorithm 1
$K \leftarrow randi([0\ 1], 5, k)$
$Kgf \leftarrow gf(K)$ ▷ Galois field array
$Kecc \leftarrow$ bchenc(Kgf,n,k)
for i = 1 to 5 **do**
    Ken[i,:] = Kecc[i,:] $\bigoplus$ S ▷ Commitment
end for
$ACC' \leftarrow$ Device 2 acceleration sample
$S' \leftarrow \text{GENBS}(ACC', n, f, q)$
for i = 1 to 5 **do**
    K'ecc[i,:] = Ken[i,:] $\bigoplus$ S' ▷ Decommitment
end for
$[K', numerr] \leftarrow bchdec(K'ecc, n, k)$
$e \leftarrow 0$
for i = 1 to 5 **do**
    for j = 1 to k **do**
        if $K'[i,j] \neq K[i,j]$ **then** $e \leftarrow e+1$
        end if
    end for
end for

E. Key Distribution And Network Simulation

The fuzzy commitment [19] was widely adopted in BCSs [7], [16]; in comparison to the fuzzy vault scheme, it is less complex and computationally demanding in terms of key concealing and revealing while yielding a superior False Acceptance Rate (FAR) performance [20]. Therefore, the fuzzy commitment scheme with BCH codes is adopted in the proposed scheme. The network simulation is described in Algorithm 2, illustrating how the key is encoded and decoded by the transmitter and the receiver, respectively. On the transmitter, the secret $K^{5\times k}$ is a randomly generated binary matrix, and it is encoded by BCH codes with the parameters of (n,k,t), where n is the codeword length, k is the length of K, and t is the maximum error correction capability of a valid BCH pair $[n,k]$. A codeword length long binary sequence S is generated by the proposed key generation scheme, and an XOR operation is performed between each row of K_{ecc} and S to encrypt the secret K into cipher-text K_{en}. On the receiver, an XOR operation is applied to each row of K_{en} and S' to obtain K'_{ecc}, which is then decoded by the BCH decoder, producing K'. Finally, the bit difference e is calculated by comparing K' and K.

TABLE I
THEORETICAL MAXIMUM SECURITY OF THE GENERATED BINARY SEQUENCES IN DIFFERENT SAMPLING FREQUENCIES AND SETTINGS

f_s (Hz)	maximum secure bits	gait cycles required		gray coding
		31-bit BS	127-bit BS	
50	2	16	64	Y
100	4	8	32	Y
250	16	2	4	Y
500	20	2	7	N

III. EVALUATION AND RESULTS

Table. I presents the summary of the settings for achieving theoretical maximum security of the generated binary sequences in different sampling frequencies. The theoretical maximum secure bits generated per gait cycle is calculated as

$$maximum\ secure\ bits = \left\lfloor \frac{\lfloor \overline{\sigma} \rfloor}{m \times \frac{1000}{f_s}} \right\rfloor \tag{4}$$

where the average standard deviation $\overline{\sigma}$ of IPI in three experiment is 40.8, m is set to 1, and the sampling frequency f_s is 100. Gray code mapping is only available when $\frac{1000}{f_s}$ can be divided by 2^q with no remainder.

TABLE II
BIT AGREEMENT RATES (BAR) OF THE GENERATED BINARY SEQUENCES IN TERMS OF DIFFERENT M AND Q SETTINGS

settings		Bit agreement rate (%)			
m	q	Exp. I	Exp. II	Exp. III	Inter-class
1	4	64.2	65.2	58.4	51.4
	5	66.6	69.7	65.0	52.0
2	3	65.8	64.3	59.6	51.8
	4	68.0	73.9	65.2	52.6
3	3	67.3	74.3	63.2	53.2
	4	79.1	79.7	67.8	54.2
5	3	73.6	78.6	70.9	53.3
	4	79.8	87.9	78.4	66.1
10	3	83.6	88.7	84.4	69.5
	4	85.9	91.5	86.1	67.7

The results from three experiments are summarized in Table. II. In Experiment I, one iPhone was placed on the lower back while the other one on the front of the waist of 5 test subjects walking in normal speed, and the sampling

frequency was 100Hz. In Experiment II, one iPhone was placed on the lower back while the other one was attached to the right upper arm of the subjects with the same settings in Exp. I. In Experiment 3, only one iPhone was placed on the lower back while the E-AR sensor was placed on the right ear of the subjects, and the sampling frequency of 100Hz was used on both devices. The experimental results suggest that scheme with m=3 and q=5 is the best configuration for the proposed scheme. The bit agreement rates in Exp. III are lower than Exp. I and Exp. II, which is mainly due to the measurement errors introduced by Bluetooth wireless transmission delays, unstable sampling rates, and noise due to head movements.

IV. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented our novel light-weight symmetric key generation scheme based on the timing information of gait. We have designed and simulated the proposed scheme using Matlab R2016b and analyzed the average bit agreement rates between the keys generated during the experiments. With the setting of m=3 and q=4, the BAR is about 79% (except for Exp. III), which means the encrypted secret K can be corrected by BCH codes (n=127, k=15, t=27). In our future work, we would like to expand our database, increase the number of sensor nodes on the subjects, conduct a detailed security analysis, and investigate other binary sequence extraction techniques that could utilize all 3-axis acceleration signals, to improve the performance of the proposed scheme.

V. ACKNOWLEDGEMENT

This research is supported by EPSRC project - SenTH - PETRAS -IoT EP/N023242/1 Cyber Security of the Internet of Things.

REFERENCES

[1] B. P. L. Lo, H. Ip, and G. Z. Yang, "Transforming Health Care: Body Sensor Networks, Wearables, and the Internet of Things," *IEEE Pulse*, vol. 7, no. 1, pp. 4–8, 2016.

[2] Z. Guo, N. Karimian, M. M. Tehranipoor, and D. Forte, "Hardware security meets biometrics for the age of IoT," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016, pp. 1318–1321.

[3] P. Campisi, "Security and Privacy in Biometrics: Towards a Holistic Approach," in *Security and Privacy in Biometrics*, Springer, 2013, ch. 1, pp. 1–23.

[4] F. Miao, L. Jiang, Y. Li, and Y. T. Zhang, "A Novel Biometrics Based Security Solution for Body Sensor Networks," in *International Conference on Biomedical Engineering and Informatics*, 2009, pp. 1–5.

[5] S. N. Ramli, R. Ahmad, and M. F. Abdollah, "Electrocardiogram (ECG) signals as biometrics in securing Wireless Body Area Network," in *International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 2013, pp. 536–541.

[6] H. A. Garcia-Baleon, V. Alarcon-Aquino, and O. Starostenko, "A wavelet-based 128-bit key generator using electrocardiogram signals," in *IEEE International Midwest Symposium on Circuits and Systems*, 2009, pp. 644–647.

[7] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, and E. Dutkiewicz, "An ECG-based Secret Data Sharing scheme supporting emergency treatment of Implantable Medical Devices," in *International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2014, pp. 624–628.

[8] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, and L. F. Shen, "Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 6, pp. 772–779, 2008.

[9] 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.

[10] G. Cola, M. Avvenuti, A. Vecchio, G. Z. Yang, and B. Lo, "An unsupervised approach for gait-based authentication," in *International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, 2015, pp. 1–6.

[11] Y. Zhang, G. Pan, K. Jia, M. Lu, Y. Wang, and Z. Wu, "Accelerometer-Based Gait Recognition by Sparse Representation of Signature Points With Clusters," *IEEE Transactions on Cybernetics*, vol. 45, no. 9, pp. 1864–1875, 2015.

[12] P. Meharia and D. P. Agrawal, "The Able Amble: Gait Recognition Using Gaussian Mixture Model for Biometric Applications," in *ACM International Conference on Computing Frontiers*, New York, NY, USA, 2015, pp. 1–5.

[13] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie-Talkie: Motion-Assisted Automatic Key Generation for Secure On-Body Device Communication," in *ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2016, pp. 1–12.

[14] G. Revadigar, C. Javali, W. Xu, W. Hu, and S. Jha, "Secure key generation and distribution protocol for wearable devices," in *IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, 2016, pp. 1–4.

[15] D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf, "BANDANA - Body Area Network Device-to-device Authentication using Natural gAit," in *IEEE Conference on Pervasive Computing and Communications*, 2017.

[16] T. Hoang and D. Choi, "Secure and Privacy Enhanced Gait Authentication on Smart Phone," *The Scientific World Journal*, May 2014.

[17] D. Jarchi, B. Lo, E. Ieong, D. Nathwani, and G. Z. Yang, "Validation of the e-AR sensor for gait event detection using the parotec foot insole with application to post-operative recovery monitoring," in *International Conference on Wearable and Implantable Body Sensor Networks*, 2014, pp. 127–131.

[18] N. Mohssen, R. Momtaz, H. Aly, and M. Youssef, "It's the Human That Matters: Accurate User Orientation Estimation for Mobile Computing Applications," in *Nternational Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2014, pp. 70–79.

[19] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.

[20] G. Zheng, G. Fang, M. A. Orgun, and R. Shankaran, "A comparison of key distribution schemes using fuzzy commitment and fuzzy vault within wireless body area networks," in *IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2015, pp. 2120–2125.