



# An Artificial Neural Network Framework for Gait-Based Biometrics

Yingnan Sun , *Student Member, IEEE*, and Benny Lo , *Senior Member, IEEE*

**Abstract**—As the popularity of wearable and the implantable body sensor network (BSN) devices increases, there is a growing concern regarding the data security of such power-constrained miniaturized medical devices. With limited computational power, BSN devices are often not able to provide strong security mechanisms to protect sensitive personal and health information, such as one’s physiological data. Consequently, many new methods of securing wireless body area networks have been proposed recently. One effective solution is the biometric cryptosystem (BCS) approach. BCS exploits physiological and behavioral biometric traits, including face, iris, fingerprints, electrocardiogram, and photoplethysmography. In this paper, we propose a new BCS approach for securing wireless communications for wearable and implantable healthcare devices using gait signal energy variations and an artificial neural network framework. By simultaneously extracting similar features from BSN sensors using our approach, binary keys can be generated on demand without user intervention. Through an extensive analysis on our BCS approach using a gait dataset, the results have shown that the binary keys generated using our approach have high entropy for all subjects. The keys can pass both National Institute of Standards and Technology and Dieharder statistical tests with high efficiency. The experimental results also show the robustness of the proposed approach in terms of the similarity of intraclass keys and the discriminability of the interclass keys.

**Index Terms**—Wearable security, gait biometrics, artificial neural network, data privacy, wireless communications, IoT security.

## I. INTRODUCTION

RECENT wireless communication technology advancements have facilitated the development of light-weight, low-energy, miniaturized sensor nodes to be worn on human body or implanted in the body, thus, forming a network of body worn sensors (i.e. Body Sensor Networks (BSN)), and associated wireless networking technology which is known as the Wireless Body Area Network (WBAN) defined by the IEEE standard 802.15.6 [1]. Operating mainly in ISM (Industrial, Scientific and Medical) bands, wireless channels in WBANs are

Manuscript received May 9, 2018; revised June 20, 2018; accepted July 21, 2018. Date of publication August 2, 2018; date of current version May 6, 2019. This work was supported by EPSRC project—SenTH+PETRAS IoT EP/N023242/1 Cyber Security of the Internet of Things. (Corresponding author: Yingnan Sun.)

The authors are with the Hamlyn Centre, Imperial College London, London SW7 2AZ, U.K. (e-mail: y.sun16@imperial.ac.uk; benny.lo@imperial.ac.uk).

Digital Object Identifier 10.1109/JBHI.2018.2860780

opened to anyone with matched radio interface configurations, and thus attackers can eavesdrop or even participate within the wireless communication amongst WBAN sensor nodes [2]. As a result, a high level data protection is a necessity for BSNs, whereby the protection of patients’ data from unauthorized access is of paramount importance. However, due to the very limited computational power, the lack of an user interface, and the low battery power design of BSN sensors, security solutions for wearable and implantable sensors are required to be light-weight and robust. Physiological signals, such as Electrocardiogram (ECG), Photoplethysmography (PPG), and behavioral characteristics, such as voice [3], and gait [4], can be captured by BSN sensors, thus, providing opportunities for Biometric Cryptosystems (BCS) to be applied as channel encryption, device authentication, and key distribution methods for securing WBANs. The state-of-the-art BCSs are mainly designed based on extracting binary keys from ECG signals [5], [6] for WBAN channel encryption and authentication. However, ECG sensors are expensive and cumbersome to use, as they require two or more electrodes to be directly attached onto the body and have to be with at least a few centimeters apart to measure the potential differences generated by the cardiac cycle. Long term use of such electrodes could cause irritation and poor contacts result in inaccurate ECG readings. In addition, most ECG-based BCSs require high sampling frequencies to capture the fiducial points in ECG waveforms, which could drain the battery power of the BSN sensors.

Alternatively, gait signals can also be used as the common source for generating secret keys for symmetric BCSs. Gait refers to the walking pattern of a person and it has been shown that gait signature is a reliable biometric for security applications [7]–[9]. Gait signals can be captured by using Inertial Measurement Units (IMUs), which are less expensive and much smaller than ECG sensors, and many wearable and implantable devices are already embedded with an IMU or inertial sensor. The challenge of using gait signals as the common entropy sources for generating secret binary keys for BSN applications is that the IMU signals collected from sensors located at different positions are less correlated, compared to ECG signals. As initially discovered by Cornelius *et al.* [10], a good correlation exists between gait signals collected from different body positions, including hands and legs, however, it is not sufficient to extract high similarity random numbers. Without applying any method to increase the correlations between the IMU signals at different positions, only a fraction of common features from the different IMU signals can be used to extract secret keys for securing the

on-body wireless channels, which will significantly hinder the reliability of gait based biometric. For example, a gait-based authentication scheme BANDANA [11] can only extract 4 bits per gait cycle from the IMU signals. Another gait-based authentication scheme [12] using Fast Fourier Transform (FFT) can only extract one bit per second on average (around 1.2 bits per gait cycle) from IMU signals. Our proposed security scheme is capable of generating 13 bits per gait cycle, outperforming the state-of-the-art gait-based key generation and authentication schemes.

Therefore, we propose the use of Artificial Neural Network (ANN) to estimate IMU signals on the chest from IMU signals from other body positions, to increase the correlations among the IMU signals at different body positions, such as head, wrist, and thigh. Using the correlated IMU signals estimated by the ANN, sensors located at different body positions are capable of extracting secret keys with high similarity for symmetric encryption of wireless channels among them. ANN is used in the proposed security scheme due to its flexibility (can be easily retrained) and light-weight (compared to deep learning approaches). The ANN framework only has 1 hidden layer with 10 hidden nodes, which can be easily implemented in the iOS [13] or Android [14] based wearable devices. Xu *et al.* [15] have also proposed a gait-based automatic key generation protocol, in which an Independent Component Analysis (ICA) approach is applied to separate acceleration signals produced by torso movement and arm swing motions. Xu's work only considered placing the coordinator on the chest position, but in practical, coordinators, such as mobile phones, are often placed in the pockets (thigh positions). Our proposed ANN framework is more flexible in terms of where the network coordinator can be placed on the body. In the experiment, the proposed biometric security scheme was tested on 7 different body positions, namely head, upperarm, chest, waist, wrist, thigh, and shin. The coordinator can be placed at any of the aforementioned major body positions. Majority of the gait-based biometric security schemes require fixed network coordinator positions [7]–[9], [15], [16], whereas the proposed security scheme can be applied on the wearable devices located at any body positions.

In this paper, we propose an ANN framework for gait biometrics for symmetric encryption, using signal energy variations with an ANN-based gait signal estimation algorithm, to secure wireless channels among wearable medical and healthcare devices and on-body network coordinators. The proposed security scheme can generate encryption keys with high level of uniqueness, freshness, robustness, and efficiency, compared with the state-of-the-art gait-based approaches. Our contributions in this paper are summarized as follows:

- 1) gait-based biometric/security scheme for securing wireless channels of wearable devices and coordinators;
- 2) ANN framework for IMU signal estimation to increase the correlations among different on-body positions [17];
- 3) analysis of the security strength of the proposed security scheme against common attacks on biometrics

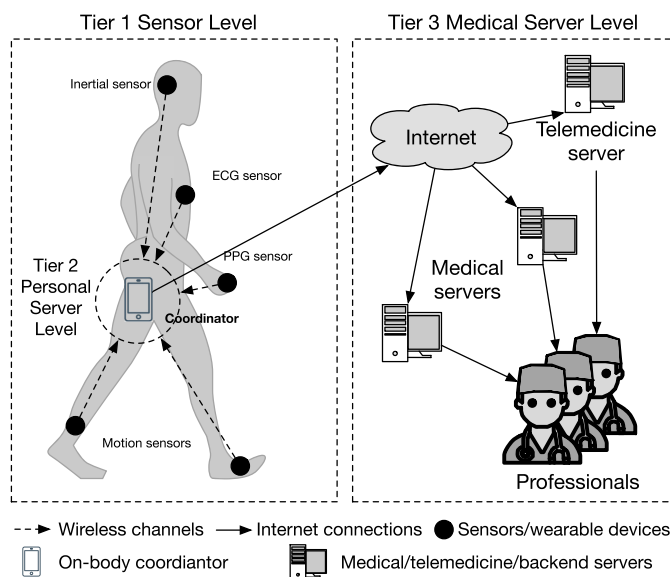


Fig. 1. A typical 3-tier BSN-based healthcare system.

## II. METHODOLOGY

### A. System Modeling

Fig. 1 illustrates a typical 3-tier BSN-based healthcare system [18], where the sensor data, such as skin temperature and blood pressure readings, collected from patients are forwarded to medical servers by gateway devices or personal servers, which is often an on-body coordinator (ex. a smart-phone). The wireless communications between the personal servers to the medical servers are often secured by computer network security measures, such as the Secure Sockets Layer (SSL). However, there is very limited protection for the wireless communications among the sensors and the personal servers. Our proposed security scheme is designed to symmetrically encrypt the wireless channels among sensors and the on-body coordinator with the secret keys extracted from the estimated IMU signals. As sensors and the coordinator are placed on the same body, they can simultaneously capture the gait IMU signals when the user is walking. Then the ANN framework can be applied to increase the correlations, and improve the reliability of the security scheme. Gait is defined as the walking pattern of a person, and gait signals in this paper refer to the acceleration and angular velocity captured by the IMU sensors during the walking motion. Gait signals can also be recognized as a behavior biometric trait, with both time-domain features, such as instantaneous signal energy variation, and frequency-domain features, such as FFT coefficients. An advantage of using behavioral biometric traits, including gait, rather than using physical biometric traits, such as fingerprints, is that the binary keys generated at different time intervals will be sufficiently different, thus providing freshness and randomness to the security scheme. As such, our proposed scheme uses gait signals as the common source for the on-body or implantable sensors to generate secret keys for the symmetric BCS.

However, the main challenge of using gait signals as the common source for key generation is that the gait signals captured

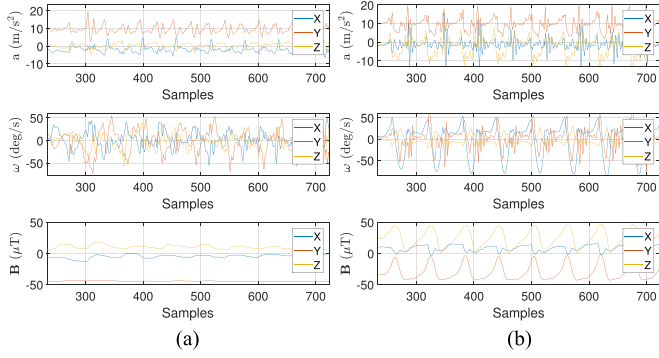


Fig. 2. IMU outputs at the chest and shin positions,  $a$  = acceleration,  $\omega$  = angular velocity, and  $B$  = magnetic field. (a) IMU outputs at the chest. (b) IMU outputs at the shin.

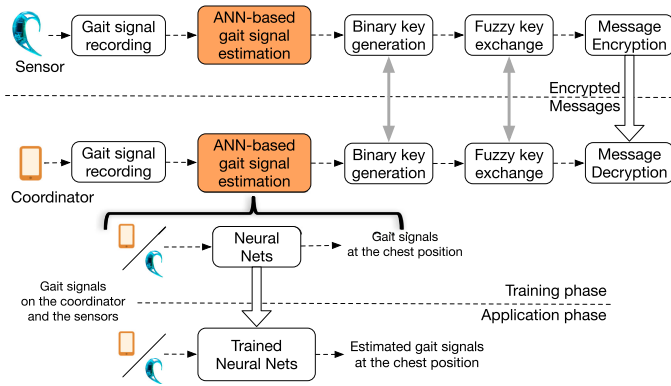


Fig. 3. Overview of the proposed security scheme.

by the sensors positioned at different locations on the body will have different patterns as shown in Fig. 2. The discrepancies between the sensor signals are often introduced by body movements such as arm and leg swings. As stated in [15], the frequency of acceleration introduced by arm swing overlaps with the frequency of the torso movement, so they cannot be separated simply by applying filters. To solve this problem, we propose the use of ANN-based gait signal estimation [19] to project the gait signals acquired from body worn sensors onto the chest, to minimize the gait signal differences among sensors and improve the performance of the security scheme. The estimated gait signals will have similar signal patterns and energy variations, from which similar binary keys can be extracted for the symmetric BCS approach. This is illustrated in Fig. 3, where an overview of the proposed security scheme is presented.

As presented in the bottom of Fig. 3, the scheme requires a training phase, where ANNs on the sensors and the coordinator are trained using the ground truth gait signals captured by the sensors attached to the chests. The ANNs will require reinforcement training if the sensor is moved to a new position. Such training can be conducted in the set up phase of a BSN system, and the trained scheme can then be applied as most of the wearable and implantable devices are worn or fixed to the targeted positions; for instance, a smart watch will always be worn on the wrist. Moreover, complex tasks like the training of ANNs can be carried out by a high performance cloud server

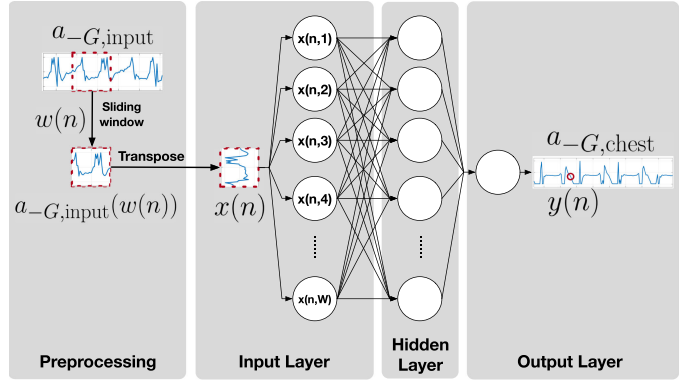


Fig. 4. ANN-based gait signal estimation.

and the trained model can then be transferred onto the sensors for on-node processing, therefore, the power consumption can be minimized while maintaining a sufficient level of security. The proposed security scheme consists of four main functional blocks: a signal recording block, an ANN-based gait signal estimation block, a binary key generation block, and a fuzzy key exchange block. For secured communications, sensors and the coordinator will perform the functions of these blocks sequentially to establish an encrypted channel for data exchange. Meta information including gait cycles and reliability vectors (from which the secret keys cannot be guessed) will be exchanged in the binary key generation block, and individual secret keys will be corrected in the fuzzy key exchange block as indicated using the gray double-headed arrows in Fig. 3.

## B. ANN-Based Gait Signal Estimation

The ANN-based gait signal estimation block consists of a pre-processing layer, an input layer, a hidden layer with 10 hidden nodes, and an output layer. In the training phase, the acceleration in the inverted gravity direction,  $a_{-G,chest}$ , captured by the sensors on the chest are set as the training targets. Although the accelerometer has 3 axes and the orientation of the sensors are often not aligned with the anatomical plans of the users, the inverted gravity direction can be easily detected by choosing the axis which has the largest mean value, as gravity is mostly capture on that axis of the accelerometer. In the proposed security scheme, only the acceleration in the inverted gravity direction is used to demonstrate the feasibility of the scheme, and  $a_{-G}$  will be referred as the gait signal in the rest of the paper. The gait signals,  $a_{-G,input}$ , captured by the coordinator and the sensors except the ones on the chests are set as the training inputs. The training dataset consists of the training inputs and the training target that collected on the same subject and at the same time. Assuming there are  $N$  samples in the training target, each sample in the training dataset, represents features extracted from sliding window with size  $W$  in the training inputs, as illustrated in Fig. 4. Thus, there are  $\frac{W}{2} + N + \frac{W}{2}$  features in the training inputs for  $N$  samples in the training dataset.

Assuming the red circle in the training target in the output layer represents the  $n^{th}$  sample, and the red dash rectangle on the training inputs is the associated sliding window,  $w(n)$ . The

training input for the  $n^{th}$  sample is given by

$$x(n) = [a_{-G,input}(w(n))]^T \quad (1)$$

where  $w(n) \in [n - \frac{W-1}{2}, n + \frac{W-1}{2}]$ . The training inputs for the entire training set can be expressed as

$$\mathbb{X} = [x(1), x(2), \dots, x(n), \dots, x(N)] \quad (2)$$

whereas the training target set is

$$Y = [y(1), y(2), \dots, y(n), \dots, y(N)] \quad (3)$$

where  $y(n)$  is the  $n^{th}$  sample in the training targets.

An ANN has to be trained for each sensor other than those worn on the chest. In the application phase, the inputs follows the same format as the training inputs  $\mathbb{X}$ , whereby the outputs of the ANNs are the estimated gait signals projected on the chest, denoted as  $\hat{a}_{-G,chest}$ . By estimating chest gait signals on both the coordinator and the sensors, they would obtain much similar gait signals as the common source, as shown in Fig. 10, from which binary keys with high similarity can be generated using the algorithms presented in section III-C. The impact of the ANN-based gait signal estimation block is analyzed and presented in section IV-B-3.

### C. Binary Key Generation

Since the binary key generation block is performed on the coordinator and the sensors, its algorithms have to be lightweight. The algorithm only contains three modules: a gait cycle detection module, a binary sequence extraction module, and a reliability bit extraction module.

1) **Gait Cycle Detection:** the gait cycle detection module is adopted from [17], in which a low pass filter is applied to  $\hat{a}_{-G,input}$ . The cut-off frequency of the low pass filter is set to 3 Hz, because the average gait frequency is between 1.7 and 2.7 Hz [16]. Every two consecutive valley is considered as the boundary between two adjacent gait cycles, as indicated with the red vertical lines in Fig. 5b, where two gait cycles are presented for illustration. After the gait cycle detection module, the original gait signal  $\hat{a}_{-G,input}$  is filtered by a 10 Hz low-pass filter which is shown as the blue dash line in Fig. 5c, to remove any noise. Assuming  $J$  gait cycles are found, the detected gait cycles are then interpolated or decimated to the same length,  $T$ , which is the averaged number of samples in all gait cycles for each subject. The normalized gait cycles are denoted as

$$\mathbf{c} = [c_1, c_2, \dots, c_j, \dots, c_J] \quad (4)$$

where  $c_j = [\hat{a}_1, \hat{a}_2, \dots, \hat{a}_t, \dots, \hat{a}_T]^T$  and  $\hat{a}_t$  represents the  $t^{th}$  sample in  $\hat{a}_{-G,chest}$ .

2) **Binary Sequence Extraction:** to calculate signal energy variations,  $\mathbf{c}$  is divided into  $U$  groups, and each group contains  $L$  gait cycles. The gait cycle group is represented as

$$\mathbf{C} = [C_1, C_2, \dots, C_\mu, \dots, C_U] \quad (5)$$

where  $C_\mu = [c_\mu, c_{\mu+1}, \dots, c_{\mu+l}, \dots, c_{\mu+L}]$ . Then, all the averaged gait cycle,  $\alpha$ , for  $\mathbf{C}$  is represented as

$$\alpha = [\alpha_1, \alpha_2, \dots, \alpha_\mu, \dots, \alpha_U] \quad (6)$$

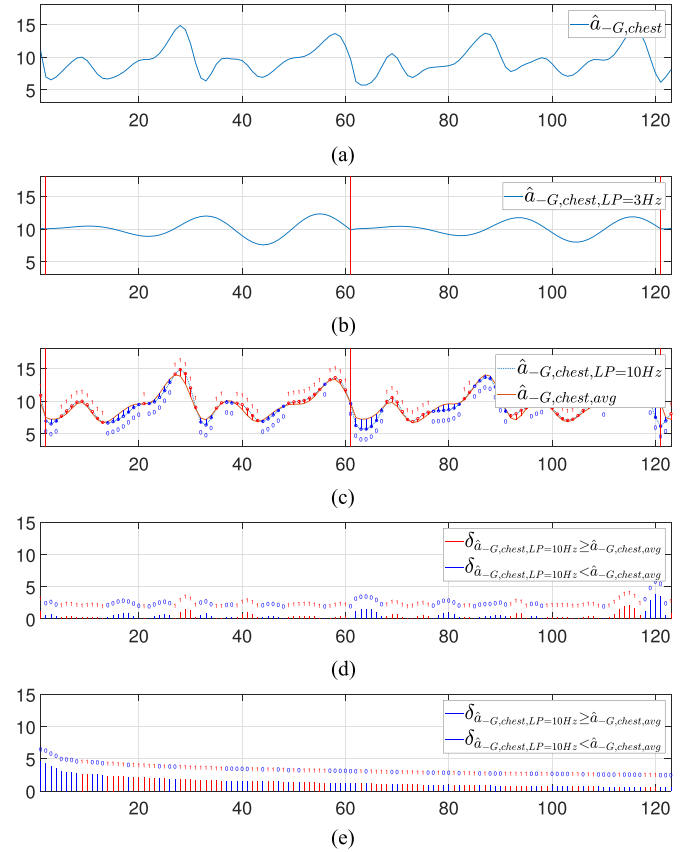


Fig. 5. Illustration of the binary key generation block. (a) Gait signal  $\hat{a}_{-G,chest}$  ( $m/s^2$ ). (b)  $\hat{a}_{-G,chest}$  ( $m/s^2$ ) filtered by the 3 Hz low-pass filter. (c) Bit extraction by comparing  $\hat{a}_{-G,chest}$  filtered by the 10 Hz low pass filter and the averaged  $\hat{a}_{-G,chest}$ . (d) Energy difference,  $\delta$ , between  $\hat{a}_{-G,chest,LP=10Hz}$  and  $\hat{a}_{-G,chest,avg}$ . (e) Re-indexed binary keys using the associated reliability vectors.

where  $\alpha_\mu = \frac{1}{L} \sum_{l=1}^L c_{\mu+l}$ .

The signal energy difference,  $\delta$ , between  $\mathbf{c}$  and  $\alpha$  can be calculated using

$$\delta_{\mu l} = c_{\mu+l} - \alpha_\mu \quad (7)$$

as a gait cycle  $c$  contains  $T$  samples, the signal energy difference for the  $t^{th}$  individual sample in the  $l^{th}$  gait cycle of the  $\mu^{th}$  gait cycle group is  $\delta_{\mu lt}$ , which can be used for generating a bit,  $b_{\mu lt} \in \{0, 1\}$ , using

$$b_{\mu lt} = \begin{cases} 1, & \delta_{\mu lt} \geq 0 \\ 0, & \text{otherwise} \end{cases} \quad (8)$$

Finally, the  $\mu^{th}$  binary key,  $\mathbf{b}_\mu$ , containing  $(L \cdot T)$  bits, is formed using the bits generated from the  $\mu^{th}$  gait cycle group  $C_\mu$ . The process is illustrated in Fig. 5c, where 1 is extracted from the red circles which are the samples whose signal energy is higher or equal to that of the averaged gait cycle, and 0 otherwise. The binary sequence extraction itself cannot generate highly randomized keys with respect to the corresponding binary sequences generated on other sensors. To address the problem, the extracted bits are re-indexed by the associated reliability vectors.

3) **Reliable Bit Extraction:** the calculation of the reliability is adopted from Schurmann *et al.* [11], where a reliability vector is defined as the descending index vector of the absolute values of the signal energy differences. The absolute values of the signal energy difference for the  $\mu^{th}$  gait cycle group  $C_\mu$  can be represented as

$$\Delta_\mu = [|\delta_{\mu 1}|, |\delta_{\mu 2}|, \dots, |\delta_{\mu \eta}|, \dots, |\delta_{\mu(L.T)}|] \quad (9)$$

and it is rearranged in a descending order to produce the associated reliability vector

$$\mathbf{r}_\mu = [r_{\mu 1}, r_{\mu 2}, \dots, r_{\mu \eta}, \dots, r_{\mu(L.T)}] \quad (10)$$

where  $r_{\mu \eta} \geq r_{\mu \eta + 1}$ . The generated binary keys are re-indexed using the reliability vectors as illustrated in Fig. 5d and Fig. 5e. Bits generated from higher signal energy differences are more reliable, as they have higher chances to be identical to the corresponding bits on different sensors [11]. The final binary keys are the top  $n$  reliable bits in each gait cycle group, and  $n$  matches the codeword length in the Bose-Chaudhuri-Hocquenghem (BCH) error correction codes in the fuzzy key exchange block.

#### D. Fuzzy Key Exchange

In the fuzzy key exchange block, we adopt the fuzzy commitment scheme [20], which has been previously used in biometric-based security systems [9]. To correct the bit errors introduced by the dissimilarity of the intra-class keys, BCH error correction codes [21] is adopted in the fuzzy key exchange block. The codeword length,  $n$ , and the minimum distance,  $d_{min}$ , of the binary  $t$ -error-correcting BCH codes can be defined by two positive integers  $m$  ( $m \geq 3$ ) and  $t$  ( $t < 2^{m-1}$ ) satisfying

$$n = 2^m - 1 \text{ and } d_{min} \geq 2t + 1 \quad (11)$$

where  $t$  is the maximum number of bit errors that is correctable by the corresponding BCH codes. The second parameter  $k$  in a BCH pair  $(n, k, t)$  is the message length that satisfies

$$n - k \leq mt \quad (12)$$

subsequently the length of the parity bits is  $p = n - k$ . A Galois field array  $GF(2)$  is created from the  $k$ -bit secret message  $K$ , which is then encoded by the BCH encoder on the sender to create a codeword  $c$ . A codeword length long binary key  $b$  is generated by the binary key generation block, and an XOR operation is performed between  $c$  and  $b$  to encrypt the codeword  $c$  into cipher-text  $c_{commit}$ . The data requester receives  $c_{commit}$ , which is then decrypted by an XOR operation with  $b'$ , which is the binary key generated on the requester, to obtain  $c'$ .  $c'$  is then decoded by the BCH decoder, producing  $K'$  and bit error  $e$ . Finally, if  $e \leq t$ , the decoding process on the requester is a success, thus, an acknowledgement is sent back to the sender to establish a secure channel, and messages will be directly decrypted by the BCH-corrected key. On the other hand, if  $e > t$ , the requester requests a new key for the commitment and the process will be repeated until it meets  $e \leq t$ . The process of the fuzzy key exchange block is illustrated using flowcharts in Fig. 6.

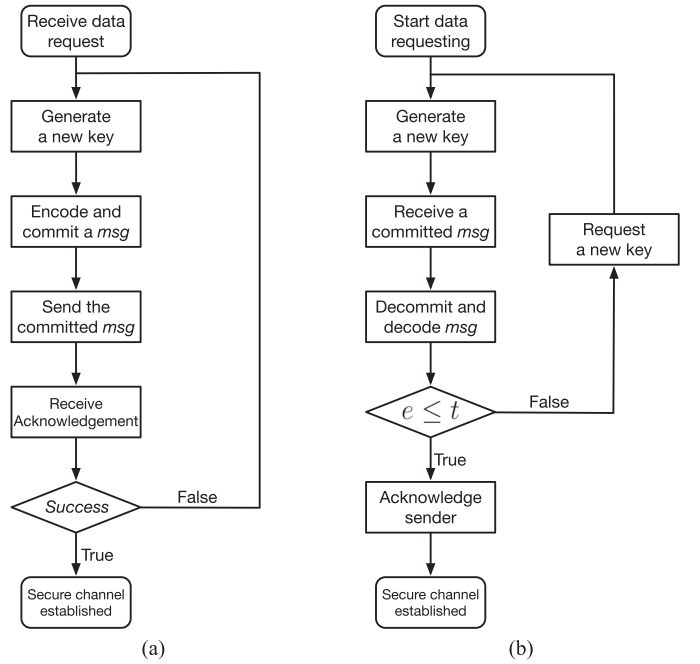


Fig. 6. Flowcharts of the fuzzy key exchange block. (a) Sender. (b) Requester.

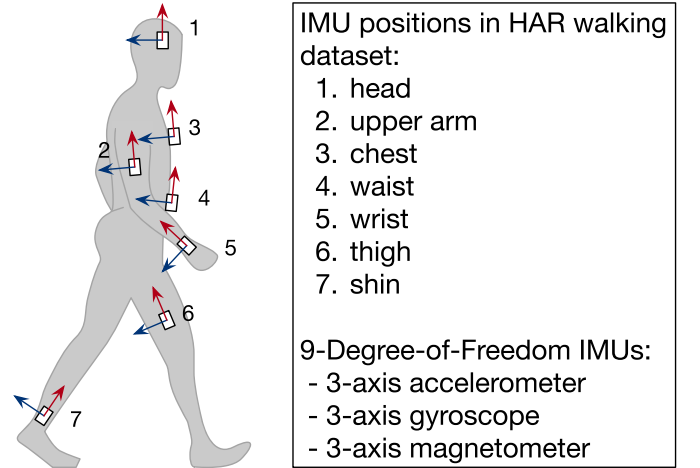


Fig. 7. HAR walking dataset.

### III. EXPERIMENTS AND RESULTS

#### A. Experimental Set-Up and Dataset

To assess the performance of the proposed security scheme, we evaluated the scheme with a series of experiments, using a walking dataset containing recordings of 15 subjects (age  $31.9 \pm 12.4$ , height  $173.1 \pm 6.9$  cm, weight  $74.1 \pm 13.8$  kg, 8 males and 7 females) from the Real World Human Activity Recognition (HAR) dataset [22]. The HAR dataset is designed for activity recognition research, and therefore it has activity recordings such as walking, sitting, and running. In our experiments, only the walking dataset was used. In this walking dataset, 7 sensors were worn by the subjects at different body locations, namely the head, upperarm, chest, wrist, waist, thigh, and shin, as illustrated in Fig. 7. As there is only one recording at one sensor position

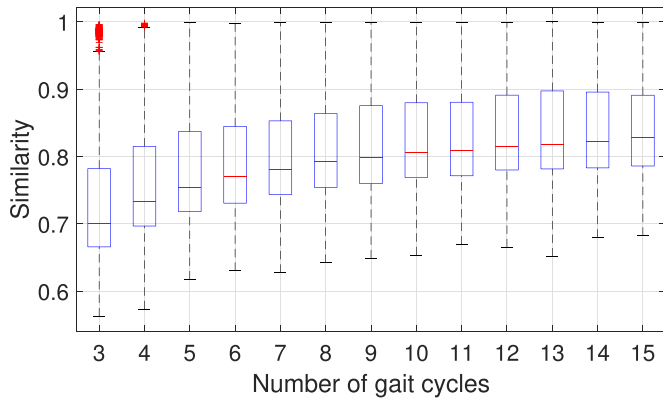


Fig. 8. Averaged similarity between 128-bit binary keys generated simultaneously from two sensors on different sensor positions of the same subject (intra-class group).

for each subject in the HAR walking dataset, we divided each sensor's recording into three equal-length subsets, and employed a  $k$ -fold cross validation method (with  $k = 3$ ): to train the ANNs, one subset of data is used and the other two subsets are used to test the proposed scheme. Instead of listing independent accuracy of each validation, the mean and standard deviation of accuracy from the  $k$ -fold cross validation are provided, as box charts, to show the robustness of the approach. As there are only marginal differences between the validations, the results from the validations are grouped together as box charts to show the results of the experiment.

In the HAR walking dataset, the sensors on each subject capture gait signals independently according to their own software clocks, therefore, the gait signal recordings were not synchronized and have different lengths of samples. To solve this issue, we re-sampled the 7 gait recordings to the same length for each subject using two timestamps of the subject's sensor on the chest. One timestamp was selected at the beginning of each recording when the subject has not started walking, and the other one was selected at the end of each recording when the subject has stopped walking. As aforementioned in section III-B, only the acceleration in the inverted gravity direction was used as the gait signals in our experiments.

## B. Group Similarity Evaluation

1) *Number of Gait Cycles*: as there are 60 samples in each gait cycle on average, to generate one 128-bit key in the binary key generation block, a minimum number of 3 gait cycles,  $N_{gc} = 3$ , is required. However, to reliably generate 128-bit keys with high similarity within the intra-class group, at least 8 gait cycles are required, as shown in Fig. 8. Intra-class keys refer to the keys generated on the same subject from two different sensors at the same time interval, whereby inter-class keys refer to the keys generated either on different subjects, or on the same subject but at different time intervals. In the experiment,  $N_{gc} = 10$  was chosen to be used to generate each 128-bit key, as it can provide sufficient intra-class similarity while maintain a high key generation rate at the same time.

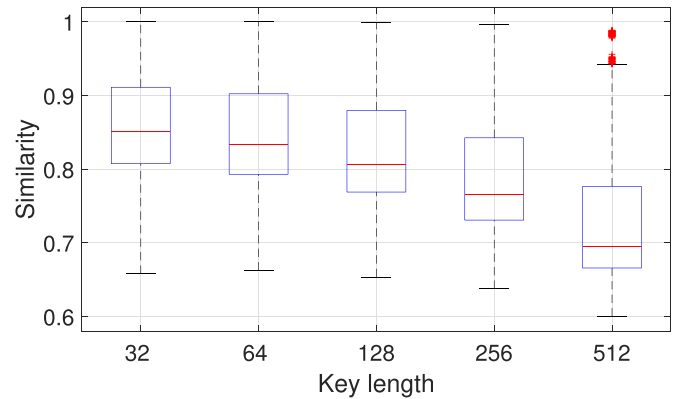


Fig. 9. Averaged similarity between intra-class keys at different key lengths. The keys were generated by reordering binary sequences using reliability vectors and cutting off at the key lengths.

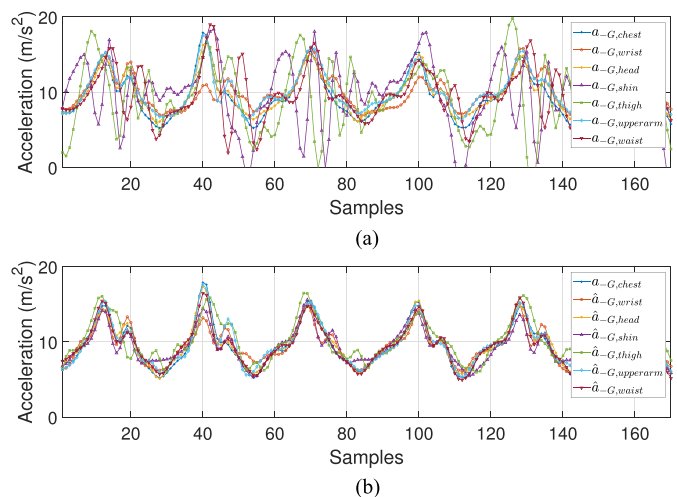


Fig. 10. Illustration of the ANN-based signal estimation. (a) Raw gait acceleration signals ( $a_{-G}$ ). (b) Estimated gait acceleration signals ( $\hat{a}_{-G}$ ).

2) *Key Length*: the similarity of the intra-class keys decreases with the increase of the key length, as shown in Fig. 9, where the box charts of the intra-class similarity of the 32, 64, 128, 256, and 512-bit reliable keys, generated when  $N_{gc} = 10$ , are shown. Reliable keys refer to the keys re-indexed with the associated reliability vectors. 128 was chosen as the key length used in the experiment as it provides larger number of possible keys to prevent brute force attacker from exhausting it in a short time, meanwhile, providing sufficient intra-class similarity and high inter-class distinctiveness.

3) *ANN-Based Gait Signal Estimation*: as aforementioned, the challenge of using gait signals as the common source for generating secret keys for symmetric-BCSs is that the gait signals captured by different sensors at different locations on the body have different patterns, as shown in Fig. 2 and Fig. 10a. In our proposed security scheme, an ANN is designed to project and estimate the gait signals (captured by sensors positioned at different body positions) onto the chest. Therefore, the estimated signals,  $\hat{a}_{-G}$ , on each position would be similar to each other as shown in Fig. 10b. The results of using the ANN-based gait signal estimation block is illustrated in Fig. 11, where

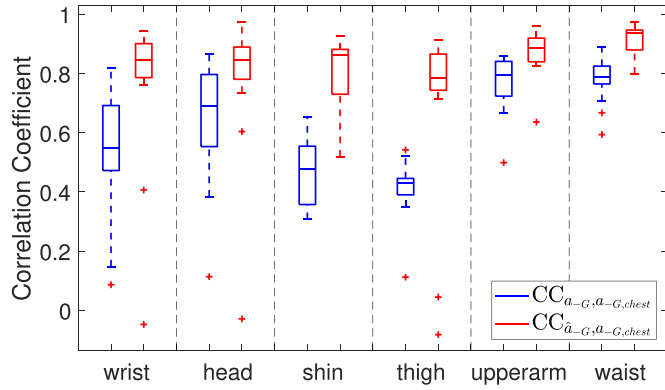


Fig. 11. CCs between the raw gait signals at other positions and chest gait signals (blue boxes), and CCs between estimated gait signals, using trained ANNs, at other positions and the chest gait signals (red boxes).

correlation coefficients (CC) between raw gait signals at various positions and chest gait signals are represented as blue boxes, and CCs between estimated gait signals at various positions and chest gait signals are represented as red boxes. CC, also known as Pearson's correlation coefficient, is a method of assessing linear relationship between two continuous variables [23], and CC has often been used for measuring how close an estimator, such as joint angles over time, is to the ground truth measured in gait analysis research [24]. According to [25], a value of CC in the range of 0.5 to 0.7 indicates a moderate correlation, in the range of 0.7 to 0.9 indicates a high correlation, and in the range of 0.9 to 1 indicates a very high correlation. As shown in Fig. 11, the ANN-based gait signal estimation block improves the correlation between gait signals from chest and other positions from moderate correlations to high or very high correlations (where the averaged CCs for six sensor positions are all above 0.7), leading to improvements on the intra-class similarity results. There are 4 CC results in the estimated signals which are below 0.2 (no correlation) and would lead to low intra-class similarity. Hence, the keys generated from these gait signals, 4 out of 90, were excluded from the final results. The ANN-based estimation block fails to improve the CC results because the raw signals do not have any correlation (below 0.2) to the chest gait signals.

The impact of the ANN-based gait signal estimation is further illustrated in Fig. 12, where blue boxes are the intra-class similarity between one sensor position to the rests without the ANN-based gait signal estimation block and red boxes are the ones with the ANN-based gait signal estimation block. It is clear that the intra-class similarity improves at every sensor position in Fig. 12, especially for those on the wrist, shin, and thigh positions. As aforementioned in section III-E, the binary BCH error correction coding scheme is adopted in the proposed security scheme for correcting bit errors between intra-class keys. BCH encoder only allows its code word length to be equal to  $n = 2^m - 1$  for any integer  $m$  between 3 and 16 [21]. When  $m = 7$ ,  $n = 2^7 - 1 = 127$  is the closet codeword length as the keys have a key length of 128. A number of valid BCH pairs  $(n, k, t)$ , which could be used in the fuzzy key exchange block, are listed in Table I. Therefore, the minimum similarity between the encryption key and the decryption key required by BCH

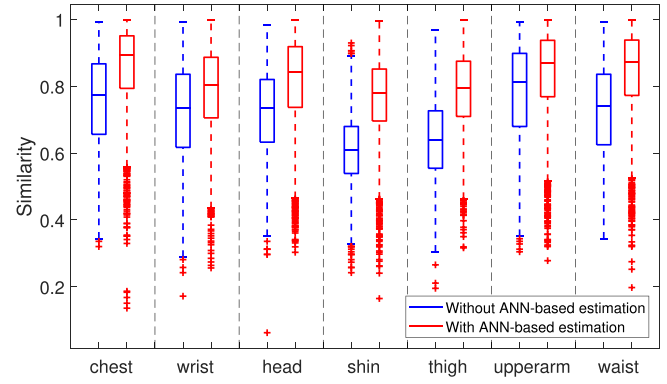


Fig. 12. Similarity of the keys generated at various positions against the keys generated at the rest of the positions.

TABLE I  
POTENTIAL BINARY BCH  $(N, K, T)$  PAIRS

n	k	t	Min similarity
127	29	21	83.46%
127	22	23	81.89%
127	15	27	78.74%
127	8	31	75.60%

TABLE II  
PROBABILITY (IN PERCENTAGE) OF MESSAGES ENCRYPTED BY INTRA-CLASS KEYS GENERATED ON ONE POSITION TO BE SUCCESSFULLY DECODED BY FOUR BCH DECODER PAIRS  $(N, K, T)$  ON THE REST OF THE SENSOR POSITIONS (ANN=WITH THE ANN-BASED GAIT SIGNAL ESTIMATION BLOCK, RAW=WITHOUT THE ANN-BASED GAIT SIGNAL ESTIMATION BLOCK)

	$(127, 29, 21)$		$(127, 22, 23)$		$(127, 25, 27)$		$(127, 8, 31)$	
	raw	ANN	raw	ANN	raw	ANN	raw	ANN
chest	34.38	65.98	37.95	69.34	46.42	76.18	53.95	81.60
wrist	25.37	41.76	29.45	46.39	36.59	55.16	44.65	63.53
head	22.76	52.21	26.94	56.39	36.11	65.23	45.35	71.57
shin	1.31	30.96	2.16	36.30	4.38	47.37	8.07	57.75
thigh	4.77	36.35	6.59	41.45	11.54	52.11	18.27	61.46
upperarm	43.98	60.41	48.16	64.15	55.89	71.29	62.43	77.83
waist	26.02	60.20	30.06	64.00	39.35	72.28	47.23	78.29

decoder to successfully decode the encrypted messages is 75.6%. The probabilities of successful fuzzy key exchanges with or without the ANN-based gait signal estimation block on various sensor positions are listed in Table II. Without the ANN-based gait signal estimation block, the probabilities of the keys generated on the shin and thigh positions to be accepted by other sensors are 8.07% and 18.27% for the BCH pair  $(127, 8, 31)$ , which is very inefficient. With the ANN-based estimation, their probabilities reach to 57.75% and 61.46% respectively, which are sufficiently improved.

Assuming a successful fuzzy key exchange in a series of attempts is an independent event, the probability of a successful

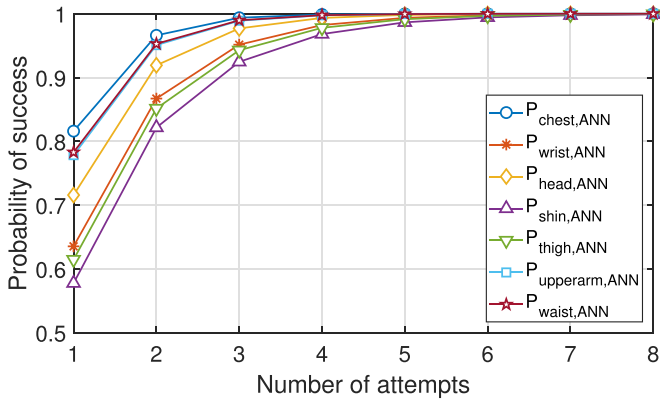


Fig. 13. Probability of successful fuzzy key exchanges on various positions to the rest of positions in different number of attempts.

TABLE III

DETAILED AVERAGED POSITION-TO-POSITION INTRA-CLASS SIMILARITY OF 128-BIT KEYS GENERATED FROM 15 SUBJECTS

	chest	wrist	head	shin	thigh	upper arm	waist
chest	1.00	0.85	0.87	0.79	0.81	0.90	0.93
wrist	0.83	1.00	0.77	0.71	0.73	0.85	0.81
head	0.86	0.77	1.00	0.74	0.80	0.85	0.84
shin	0.79	0.72	0.75	1.00	0.77	0.75	0.78
thigh	0.80	0.73	0.80	0.76	1.00	0.82	0.80
upperarm	0.90	0.86	0.86	0.74	0.82	1.00	0.86
waist	0.93	0.82	0.84	0.78	0.81	0.86	1.00

fuzzy key exchange after the  $n^{\text{th}}$  attempt is calculated as

$$P_n = \sum_{i=1}^n P_{\text{success}} \times (1 - P_{\text{success}})^{n-1} \quad (13)$$

where  $P_{\text{success}}$  is the probability of a successful fuzzy key exchange for an individual attempt. Using Eq. (13), the probabilities of success against the number of attempts for the BCH pair (127, 8, 31) are calculated and shown in Fig. 13. At all 7 positions, a successful fuzzy key change occurs on the second, third, and fourth attempt reach 80%, 90%, and 95% respectively, with the ANN-based gait signal estimation. As  $N_{gc} = 10$ , each attempt requires 10 gait cycles, and the proposed method can provide at least 95% successful rates for all sensor positions using 40 gait cycles.

A detailed comparison amongst position-to-position intra-class similarity, averaged for all the subjects in the HAR walking dataset, is presented in Table III. The averaged similarity between wrist and shin and between wrist and thigh are 72% and 73% respectively, which are the lowest similarity values in the position-to-position comparison. This can also be seen in Fig. 12. It is due to the fact that shin and thigh gait signals are less correlated with chest gait signals, as shown in Fig. 11.

4) **Reliability:** the impact of reordering keys using associated reliability vectors has also been investigated and the results are

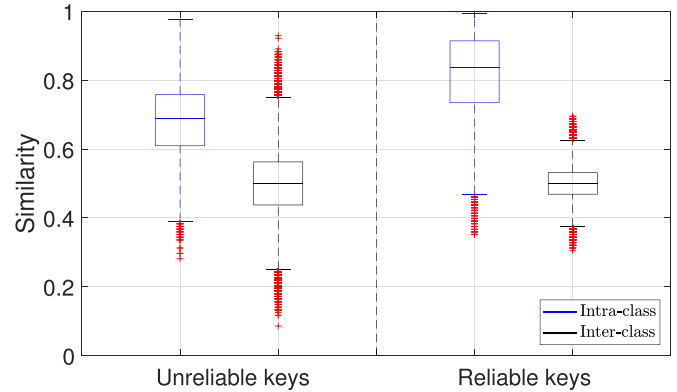


Fig. 14. Similarity of intra-class group and inter-class group. Unreliable keys are the 128-bit keys generated without reordering by their reliability vectors, while reliable keys are the reordered unreliable keys using their associate reliability vectors.

shown in Fig. 14, where the left two boxes are the similarity for the intra-class and inter-class unreliable keys, and the right two boxes are the similarity for the intra-class and inter-class reliable keys. It is clear that reliable keys produce higher similarity for intra-class keys and better distinctiveness for inter-class keys, which means the inter-class similarity distribution is less dispersed. In addition, although we chose 128-bit reliable keys in the experiments to demonstrate the feasibility of our proposed security scheme, longer key length can also be adopted as presented in Fig. 9. The mean intra-class similarity for 256-bit keys is 78.13%, when  $N_{gc} = 10$ , indicating that 256-bit keys can be used but with less efficiency (requires more attempts to achieve high probabilities of successful key exchanges). Longer key length can provide better distinctiveness between inter-class keys due to its further concentrated normal distribution of inter-class similarity, and provide more secure bits in each key. For example, using the BCH pair (255, 9, 63) in the fuzzy key exchange block would provide 192 secure bits, whereas using the BCH pair (127, 8, 31) would provide 96 secure bits.

### C. Uniqueness and Freshness of Generated Keys

Uniqueness and freshness can be interpreted as the distinctiveness between inter-class keys, which are generated from either different subjects, same subject but sensors are worn at different positions, or same person wearing the same sensors but at different time. The purpose of this analysis is to quantify how distinctive the inter-class keys are, and it is achieved by analyzing the distribution of the Hamming Distance (HD) for the inter-class keys and vitalizing the generated binary keys. A HD between two binary keys,  $\mathbf{b}_a$  and  $\mathbf{b}_b$ , of the same length, is equal to the number of bits in which the two binary keys differ from one another [26].  $HD = 0$  means two binary keys are identical, while  $HD = 1$  means two binary keys are completely different from one another [27]. For sufficiently long binary keys, the distribution of HD should be a normal distribution with a mean close to 50% [28]. As shown in Fig. 15, the probability of HD of the inter-class keys generated in the experiments follows a normal distribution with the mean of 49.96%, which is very close to 50%. Moreover, the lower bound of the HD distribution



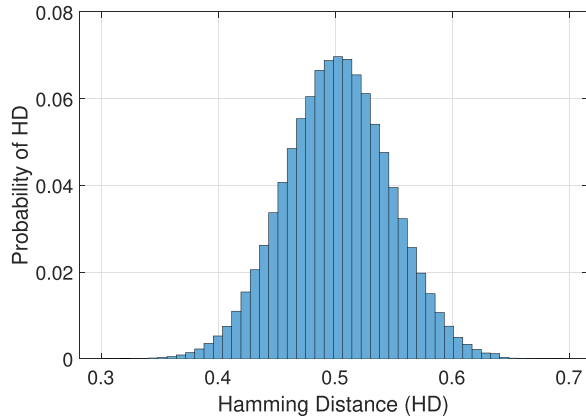


Fig. 15. Probability distribution of hamming distance of any two inter-class 128-bit keys generated from all 15 subjects, with the mean distance of 49.96%.

is around 0.3, which indicates that no key will be falsely accepted. This result demonstrates the robustness of the proposed biometrics against brute force attacks.

#### D. Randomness Evaluation

To protect the proposed security scheme from brute-force attacks, it is vital that the generated keys process high randomness. Therefore, we evaluated the randomness of the keys generated in the experiments using the entropy analysis, the NIST randomness test, and the Dieharder battery test.

1) *Entropy Analysis*: the generated keys in the experiments were tested with the entropy analysis. Shannon entropy is a measure of uncertainty of binary sequences [29]. The uncertainty refers to the possibilities of the next event being any mutually exclusive events are equal. The entropy of the binary keys, which contains two mutually exclusive events  $\{0, 1\}$ , can be calculated using [30]

$$H(\{0, 1\}) = -P(0)\log_2 P(0) - P(1)\log_2 P(1) \quad (14)$$

where  $P(0)$  is the probability of 0s and  $P(1)$  is the probability of 1s. The results of the entropy analysis for 128-bit keys generated from all the subjects in the HAR walking dataset are shown in Fig. 16. Although the entropy varies from subject to subject, a large majority of the keys have entropy above 0.99, which indicates that no pattern of 0s and 1s dominates in the keys generated from any subjects.

2) *NIST Randomness Test*: the National Institute of Standards and Technology (NIST) randomness test suite has also been used widely by researchers [15], [28], [31] to detect deviations of a binary sequence from randomness [32]. We tested all the 600-bit ( $60 \times 10$ ) keys, re-indexed using associated reliability vectors, generated in the experiments when  $N_{gc} = 10$  using NIST tests, and the results are listed in the Table IV. The minimum pass rate for each statistical test is approximately 96%, therefore, all tests have passed the tests. The P-values in Table IV are from the uniformity tests for these statistical tests, and  $P > 0.0001$  indicates the p-values from the

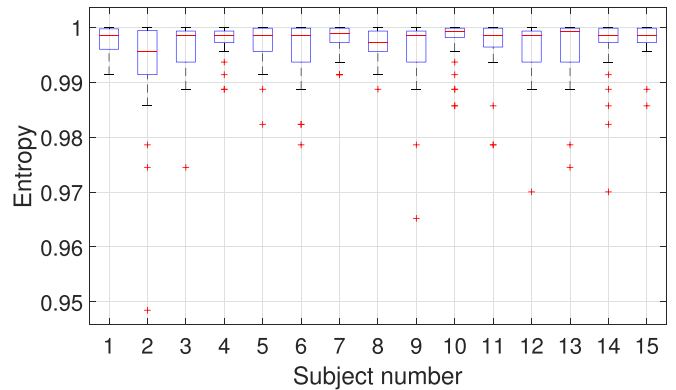


Fig. 16. Shannon entropy of 128-bit keys for 15 subjects in the HAR walking dataset ( $N_{gc} = 10$ ).

TABLE IV  
NIST STATISTICAL TEST RESULTS

Statistical test	P-value	Proportion	Pass/Fail
Frequency	0.595549	99%	Pass
Block Frequency	0.739918	98%	Pass
Cumulative Sums <sup>+</sup> (2)	0.282961	98%	Pass
Runs	0.224821	100%	Pass
Longest Run	0.867692	99%	Pass
FFT	0.554420	100%	Pass
Approximate Entropy	0.851383	98%	Pass
Non-Overlapping Template <sup>+</sup> (148)	0.136742	97%	Pass
Serial <sup>+</sup> (2)	0.457748	99%	Pass
Linear Complexity	0.137282	96%	Pass

corresponding statistical test are uniformly distributed on the interval  $[0, 1)$  [33].

3) *Dieharder Test*: all the keys generated in the experiments were also run through a series of Dieharder statistical tests [34], and the p-value distributions of 21 runs of the Dieharder tests are shown in Fig. 17. If a p-value from a Dieharder statistical test is below 0.001, it can be considered as it fails the test, however, p-values are expected equals or below 0.05 (weak) 5% of the time. The results in Fig. 17 shows no incident of failure in any tests and a few incidents where  $p \leq 0.05$  as expected. Furthermore, the p-values of all the tests are well distributed over the interval  $[0, 1)$ , indicating the keys have passed all the Dieharder statistical tests.

One of the common concerns for biometric security is the uniqueness of the biometrics for different users (inter-class) and for different access request attempts, which are considered as intra-class for most biometric approaches, but they are considered as inter-class in the proposed security scheme. Only the keys generated on the same user and at the same time are considered as intra-class keys. This approach gives the proposed security scheme freshness and robustness against attacks using the correlations between two attempts, which traditional biometric schemes do not provide.

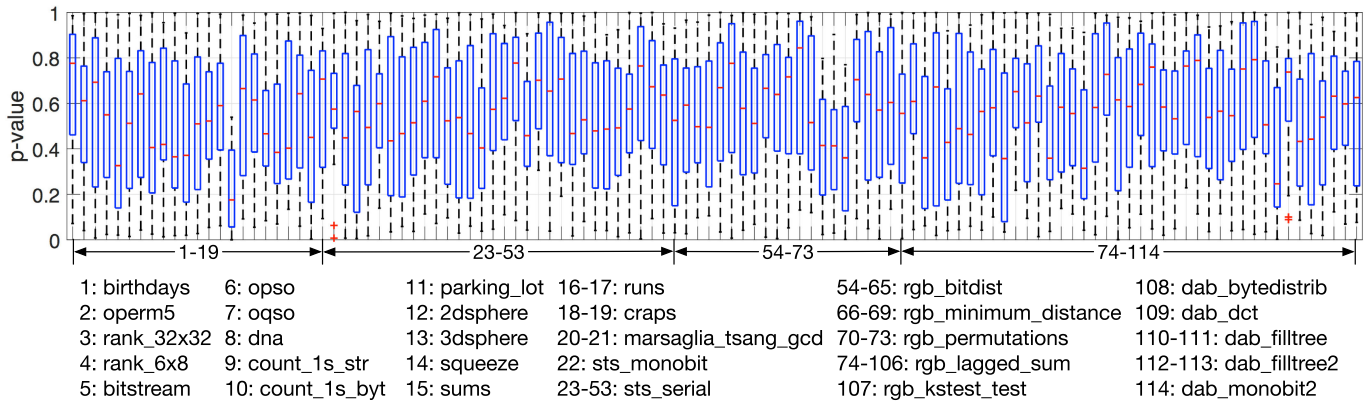


Fig. 17. Distribution of p-values in the Dieharder statistical test results.

#### IV. DISCUSSION

Possible attack scenarios and adversarial analysis against the proposed security scheme are discussed in this section.

##### A. Security Model

1) **Brute Force Attacks:** A brute force attack is a trial-and-error attack used to exhaust the space of possible keys, which means to try out all possible keys to decode the messages that the attacker have intercepted. As the BCH error correcting code with the pair (127, 8, 31), which can correct up to 31-bit errors in the keys, is used in the fuzzy key exchange block, there are  $127-31 = 96$  secure bits, resulting in the number of all possible keys to be  $\mathbb{F}_2^{96}$ . Therefore, it is recommended to renegotiate a new key as quickly as possible to prevent the secured channel from being exposed. If the attacker successfully obtained one of the keys using brute force attacks, only the messages encrypted by that key are exposed. As all the keys possess the property of high distinctiveness, the attacker cannot use the exposed key to predict any other keys.

2) **Dictionary Attacks:** besides brute force attacks, dictionary attacks are also very popular methods used by among hackers in recent years [35]. Therefore, it is a requirement for any biometric cryptosystems to be resilient to dictionary attacks. Although they have not been tested using no user-specific dictionaries, the keys generated in our experiments produced uniform distributions of p-values in the majority of the Dieharder statistical tests, which includes many commonly used dictionaries, such as birthdays and DNA. Thus, the proposed security scheme is resilient to common dictionary attacks.

3) **Attaching Device:** the attacker can also attach a malicious device to the victims to try to obtain the secured keys. However, the malicious device requires a fully-trained ANN, specifically to the position it attached to, in order to extract binary keys acceptable to other legitimate BSN devices. If the attacker intends to train ANNs for the malicious device, at least two malicious devices must be attached to the target position and another one on the chest at the same time. This process is difficult for attackers to execute successfully without being noticed by the victims.

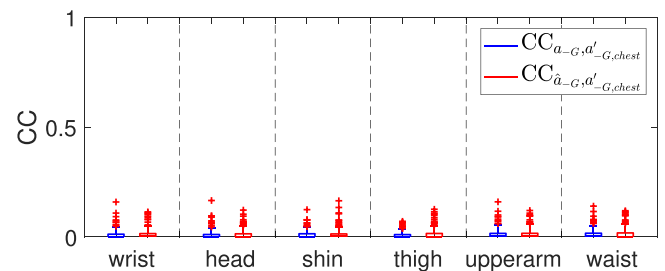


Fig. 18. CCs between impersonators and victims (blue boxes), and CCs between impersonators and victims when using victims' trained neural networks (red boxes).

4) **Impersonation Attacks:** impersonation attacks in gait biometrics have been studied extensively in the literature [36]–[38]. Muaaz and Mayrhofer [38] demonstrated that a zero effort or a mimicry impersonation attack on gait biometric is unlikely be able to compromise the IMU-based gait authentication systems. Furthermore, previous studies have shown that during impersonation attacks, impersonators could lose regularity between steps, increasing the difficulty of the impersonation. Fig. 18 shows that when using victims' neural networks, the zero-effort impersonation does not increase the CC results nor improve chances of the impersonation.

5) **Freshness:** another big concern when adopting fuzzy commitment or fuzzy vault scheme into the any biometric-based security schemes would be “with the unavoidable information leak, is it resilient to the attacks targeting the correlations or correspondence between two or multiple keys generated from the same biometric instance”. Previous studies [39], [40] have demonstrated that fuzzy commitment or fuzzy vault schemes are vulnerable against many attacks (i.e. Decodability [39], record multiplicity, surreptitious key-inversion, and novel blended substitution [41]). In general, such vulnerability comes from the fact that the dependency of binary features has been neglected in many research, resulting in overestimation in the security levels of such schemes [42]. For instance, if the keys are extracted using frequency domain features, such as FFT, from the same face or fingerprint, they are likely to contain similar patterns of 1 s and 0 s. In our proposed scheme, temporal gait features are used for generating encryption keys with a high level of

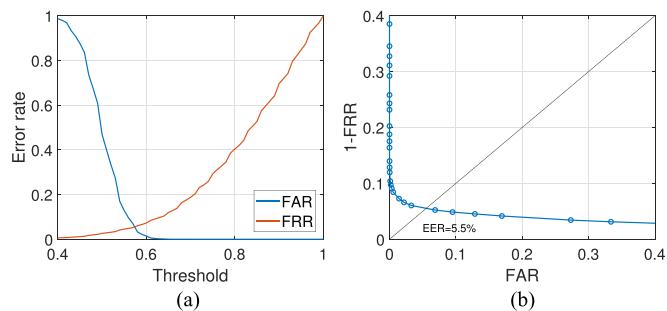


Fig. 19. Use the proposed security scheme as biometric device-to-device authentication. (a) FAR & FRR. (b) ROC.

freshness. Because temporal features are time-variant, producing distinctive keys even in a short period of time. As shown in Fig. 14 and 15, the keys generated using proposed security scheme process high distinctiveness and a good probability distribution of hamming distance, meeting the strict condition for fuzzy commitment scheme to be used safely.

6) *Efficiency*: the number of the gait cycles required for generating one 128-bit key is sufficiently reduced compared with our previous work [17], in which 32 gait cycles are required for one 128-bit key, and BANDANA, in which 48 gait cycles are required. The proposed security scheme only requires 10 gait cycles for one 128-bit key, which is 68.75% and 79.17% more efficient than our previous work and BANDANA respectively. The averaged number of samples in one gait cycle after re-sampled to 50 Hz in the HAR walking dataset is 60, thus, the averaged time for one gait cycle is  $60 \times \frac{1}{50} = 1.2$  s. When  $N_{gc} = 10$ , the averaged time required for generating one 128-bit key is 12 s, and the averaged output rate of the binary key generation block is  $128 \times \frac{1}{12} = 10.7$  bps. The proposed security scheme is based on gait biometric, it will only generate new keys when the user is walking. Hence, the same key will be used if the user is performing other activities.

## B. Authentication

The proposed security scheme can be used as traditional biometric device-to-device authentication with different thresholds instead of fixing it to the constant  $t$ . Fig. 19a and Fig. 19b present the performance of such authentication usage using False Agreement Rate (FAR), False Rejection Rate (FRR), and Receiver Operating Characteristic (ROC) curves. Equal Error Rate (EER) is 5.5% when the threshold is set to 0.57. However, the generated keys cannot be used for channel encryption, as the fuzzy commitment scheme is not applicable at the EER point. After authentication, a new set of encryption keys must be used based on the mutual agreement between the sender and the receiver.

## V. CONCLUSION

In this paper, we proposed a novel gait-based security scheme with ANN for securing wireless communications for wearable and implantable healthcare devices. The use of ANN-based gait signal estimation block for estimating gait signals on the chest from those captured by sensors worn on the other body positions

has been proposed and significant improvement on the performance of the proposed security scheme has been shown from the experimental results. The probability of a successful intra-class fuzzy key exchange using the BCH pair (127, 8, 31) within 4 attempts for all sensor positions reach 95%, and inter-class keys possess the property of high distinctiveness, with a mean Hamming Distance of 49.96% for all 15 subjects in the HAR walking dataset. The experimental results have demonstrated the feasibility and the robustness of our proposed security scheme and its resilience against common attacks. With its low computational power design and the use of gait signals from IMUs, the proposed scheme could provide the needed for secured communications for wireless pervasive healthcare systems.

## REFERENCES

- [1] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, IEEE Std 802.15.6-2012, 2012.
- [2] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "A survey on wireless body area network: Security technology and its design methodology issue," in *Proc. Int. Conf. Innovations Inf., Embedded Commun. Syst.*, 2015, pp. 1–5.
- [3] M. Khitrov, "Talking passwords: Voice biometrics for data access and security," *Biometric Technol. Today*, vol. 2013, no. 2, pp. 9–11, 2013.
- [4] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2010, pp. 306–311.
- [5] 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 Trans. Inf. Technol. Biomed.*, vol. 12, no. 6, pp. 772–779, Nov. 2008.
- [6] A. D. C. Chan, M. M. Hamdy, A. Badre, and V. Badee, "Wavelet distance measure for person identification using electrocardiograms," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 2, pp. 248–253, Feb. 2008.
- [7] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2012, pp. 16–20.
- [8] 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 Trans. Cybern.*, vol. 45, no. 9, pp. 1864–1875, Sep. 2015.
- [9] T. Hoang, D. Choi, and T. Nguyen, "Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme," *Int. J. Inf. Security*, vol. 14, no. 6, pp. 549–560, 2015.
- [10] C. T. Cornelius and D. F. Kotz, "Recognizing whether sensors are on the same body," *Pervasive Mobile Comput.*, vol. 8, no. 6, pp. 822–836, 2012.
- [11] D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf, "BANDANA Body area network device-to-device authentication using natural gait," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun.*, 2017, pp. 190–196.
- [12] D. Oberoi, W. Y. Sou, Y. Y. Lui, R. Fisher, L. Dinca, and G. P. Hancke, "Wearable security: Key derivation for Body Area sensor Networks based on host movement," in *Proc. IEEE 25th Int. Symp. Ind. Electron.*, 2016, pp. 1116–1121.
- [13] B. Kerimbaev, "Neural Networks in iOS 10 and macOS," 2016. [Online]. Available: <https://www.bignerdranch.com/blog/neural-networks-in-ios-10-and-macos/>
- [14] L. Matney, "Google introduces Neural Networks API in developer preview of Android 8.1," 2017. [Online]. Available: <https://techcrunch.com/2017/10/25/google-introduces-neural-networks-api-in-developer-preview-of-android-8-1/>
- [15] W. Xu, C. Javali, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Gait-Key: A gait-Based shared secret key generation protocol for wearable devices," *ACM Trans. Sensor Netw.*, vol. 13, no. 1, pp. 1–27, Jan. 2017.
- [16] G. Revadigar, C. Javali, W. Xu, A. V. Vasilakos, W. Hu, and S. Jha, "Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2467–2482, Oct. 2017.
- [17] Y. Sun, C. Wong, G. Z. Yang, and B. Lo, "Secure key generation using gait features for body sensor networks," in *Proc. IEEE 14th Int. Conf. Wearable Implantable Body Sensor Netw.*, 2017, pp. 206–210.

- [18] F. Miao, L. Jiang, Y. Li, and Y. T. Zhang, "Biometrics based novel key distribution solution for body sensor networks," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, 2009, pp. 2458–2461.
- [19] Y. Sun, G.-Z. Yang, and B. Lo, "An artificial neural network framework for lower limb motion signal estimation with foot-mounted inertial sensors," in *Proc. IEEE Conf. Body Sensor Netw.*, 2018, pp. 132–135.
- [20] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. ACM Conf. Comput. Commun. Security*, 1999, pp. 28–36.
- [21] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, 2nd ed. Cambridge, MA, USA: MIT Press, 1972.
- [22] T. Szytler, H. Stuckenschmidt, and P. Wolfgang, "Position-aware activity recognition with wearable devices," *Pervasive Mobile Comput.*, vol. 38, pp. 281–295, 2017.
- [23] D. G. Altman, *Practical Statistics for Medical Research*, 1st ed. London, U.K.: Chapman and Hall, 1990.
- [24] S. Tadano, R. Takeda, and H. Miyagawa, "Three dimensional gait analysis using wearable acceleration and gyro sensors based on quaternion calculations," *Sensors*, vol. 13, no. 7, pp. 9321–9343, 2013.
- [25] D. E. Hinkle, W. Wiersma, and S. G. Jurs, *Applied Statistics for the Behavioral Sciences*, 5th ed. Boston, MA, USA: Houghton Mifflin, 2002.
- [26] Encyclopedia.com, "Hamming distance," 2017. [Online]. Available: <http://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/hamming-distance>
- [27] D. K. Altop, A. Levi, and V. Tuzcu, "Towards using physiological signals as cryptographic keys in body area networks," in *Proc. 9th Int. Conf. Pervasive Comput. Technol. Healthcare (PervasiveHealth)*, 2015, pp. 92–99.
- [28] G. Zheng *et al.*, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Informat.*, vol. 21, no. 3, pp. 655–663, May 2017.
- [29] S. R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho, "Low-latency approach for secure ECG feature based cryptographic key generation," *IEEE Access*, vol. 6, pp. 428–442, 2017.
- [30] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.
- [31] S. Yin, C. Bae, S. J. Kim, and J.-S. Seo, "Designing ECG-based physical unclonable function for security of wearable devices," in *Proc. 39th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, 2017, pp. 3509–3512.
- [32] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications (SP 800-22 Rev. 1a)," National Inst. Standards Technol., Gaithersburg, MD, U.S.A., Tech. Rep., 2010.
- [33] M. Sys, Z. Riha, V. Matyas, K. Marton, and A. Suci, "On the interpretation of results from the NIST statistical test suite," *Romanian J. Inf. Sci. Technol.*, vol. 18, no. 1, pp. 18–32, 2015.
- [34] R. G. Brown, "Dieharder: A random number test suite," 2004. [Online]. Available: <https://webhome.phy.duke.edu/rgb/General/dieharder.php>
- [35] R. Millman, "Brute force and dictionary attacks up 400 percent in 2017," 2018. [Online]. Available: <https://www.scmagazineuk.com/amp/brute-force-dictionary-attacks-400-percent-2017/article/1473168>
- [36] D. Gafurov, E. Snekenes, and P. Bours, "Spoof attacks on gait authentication system," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 491–502, Sep. 2007.
- [37] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be Spoofed?" in *Proc. 21st Int. Conf. Pattern Recognit.*, 2012, pp. 3280–3283.
- [38] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: From authentication to imitation," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3209–3221, Nov. 2017.
- [39] B. Tams, "Decodability attack against the fuzzy commitment scheme with public feature transforms," *arXiv:1406.1154v3*.
- [40] C. Rathgeb and A. Uhl, "Statistical attack against fuzzy commitment scheme," *IET Biometrics*, vol. 1, no. 2, pp. 94–104, 2012.
- [41] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," in *Proc. Biometrics Symp.*, 2007, pp. 1–6.
- [42] X. Zhou, A. Kuijper, R. Veldhuis, and C. Busch, "Quantifying privacy and security of biometric fuzzy commitment," in *Proc. Int. Joint Conf. Biometrics*, 2011, pp. 1–8.