Accelerometer-Based Key Generation and Distribution Method for Wearable IoT Devices

Fangmin Sun, *Member, IEEE*, Weilin Zang, Haohua Huang, Ildar Farkhatdinov and Ye Li*, *Senior Member, IEEE*

***Abstract*—With the fast development of wearable IoT devices, their applications are becoming more and more pervasive, ranging from social networking, payment, and navigation to health and activity monitoring. The security of the communication between these devices is essential to protect the transmitted sensitive information from tampering and eavesdropping. With the integration of accelerometers into wearable IoT devices, the gait-based biometric cryptography technology has emerged as a data securing tool for wearables. This paper proposes a light-weight noise-based group key generation method, which utilizes the noise signals imposed on the raw acceleration signals to generate an M-bit key with high randomness and bit generation rate. Moreover, a signed sliding window coding (SSWC)-based common feature extraction method was designed to extract the common feature for sharing the generated M-bit key among devices worn on different body parts. Finally, a fuzzy vault-based group key distribution system was implemented and evaluated using a public dataset. The performed comprehensive analysis of the proposed key generation and distribution method proved that the binary keys generated via the introduced noise-based procedure have high entropy and can pass both the NIST and Dieharder statistical tests with high efficiency. The experimental results obtained prove the robustness of the proposed SSWC-based common feature extraction method in terms of the similarity and discriminability of intra- and inter-class features, respectively.**

***Index Terms*— Communication security, gait, body area network, secret key generation, key distribution**

Manuscript received XXXX; revised XXXX; accepted XXXX.

This study was sponsored by the National Key R&D Program of China with grant number 2018YFB1307005; National Natural Science Foundation of China with grant numbers 61702497 and 61902388; Joint Fund of NSFC and Guangdong Province with grant number U1801261; Strategic Priority CAS Project with grant number XDB38040200; Basic research project of Shenzhen Science and Technology Innovation Commission with grant number JCYJ20180703145002040 and JCYJ20190807161805817; Major Projects from General Logistics Department of People's Liberation Army with grant number AWS13C008.

Fangmin Sun, Weilin Zang, Haohua Huang and Ye Li* are with the Joint Engineering Research Center for Health Big Data Intelligent Analysis Technology, Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen, China.

Haohua Huang is also with the University of Chinese Academy of Sciences, Beijing, China.

Ildar Farkhatdinov is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, UK.

Corresponding author: Ye Li (e-mail: ye.li@siat.ac.cn)

I. Introduction

Recent years witnessed a remarkable growth in the variety and number of wearable IoT devices. The application of wearable IoT devices becomes more and more pervasive, ranging from social networking, payment, navigation, to health and activity monitoring [1]. A typical application scenario of the wearable IoT devices is shown in Fig.1. Various kinds of personal data concerning health status, social data, daily activity, bank accounts, etc., are collected and wirelessly transmitted to the mobile gateway by wearable IoT devices [2, 3]. Due to the privacy and sensitivity features of personal data and the wireless nature of the communication, the security of communication between these devices is essential to protect the transmitted data from being eavesdropped, tampered, or injected with malicious commands, while data sharing has to be kept strictly among body-worn devices that belong to the same user [4, 5].

Fig.1. Typical application scenarios of wearable IoT devices

However, due to the limited power and computing resources of wearable IoT devices, traditional channel encryption methods such as the Diffie-Hellman (D-H) peer-to-peer key exchange algorithm, Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc., cannot be directly applied to wearable devices [6]. The personal identification number (PIN) is currently used as an authentication method for some mobile devices like cellphones, but it is not suitable for small-sized

wearable IoT devices, which usually have no input interface [7].

Since the conventional security schemes proposed for computers are too computationally demanding for miniaturized wearable IoT devices [8], new methods of securing body sensor networks (BSNs) have been offered, in which a biometric cryptosystem (BCS) is considered a quite effective solution [9]. The biometrics-based approach avoids memory overload and obviates expensive computation, insofar as biometric traits are already available in the wearable device. With regards to BCS security solutions, such physiological characteristics as an individual's face, iris and fingerprints have already been widely applied to the identity authentication of mobile devices, but these biometric features are vulnerable to theft and duplication. In contrast, the recently emerged bioencryption technology uses real-time physiological biometrics such as the electrocardiogram (ECG) [10-12] and photoplethysmogram (PPG) [13-15] to generate the random key to secure private information. However, these physiological biometrics require specialized sensors to be in physical contact with the human body, which can make the user uncomfortable. Moreover, the sampled signal quality can be easily interfered with by the external environment and human activity [16].

Nowadays, with the availability of the integrated inertial measurement units (IMU) in wearable IoT devices, such behavioral traits as gait, keyboard tapping, etc. are gaining much attention for their noninvasive and unique features [17, 18]. In many types of wearable IoT devices, it is more convenient to extract the gait signal than other physiological signals like ECG and PPG.

Due to human gait uniqueness and non-variability over time, it has been utilized for user authentication or identification of wearable IoT devices in multiple previous studies [19-22]. These studies used gait information to protect the security of the wearable devices by providing a gait-based access control mechanism; however, the safety of the data transmitted between devices was not guaranteed. Wazid et al. proposed a key agreement and management scheme for implantable and wearable medical devices [23, 24] and used the formal security verification and informal security analysis to prove their scheme's security against known attacks.

Acceleration-based symmetric key generation method was first proposed by Bichler et al. to encrypt the communication in wireless body area networks [25]. In their scheme, the devices have to be shaken together to ensure that they can generate the same symmetric key based on the acceleration signal caused by the shake. This direction was followed by Mayrhofer et al., who proposed a secure pairing scheme of mobile devices that exploited the joint movement caused by simultaneous shaking as a shared secret to realizing the secure pairing of devices [27]. Further, Sun et al. proposed the IPIs (Inter-Pulse Intervals) based random number generation method for securing the communication of wearable IoT devices [28, 29]. However, the key generation rate of this method was too low, as they used the gait cycles instead of sample points to extract the random binaries. Alternatively, Xu et al. designed a symmetric secret key generation scheme that allowed two legitimate devices to establish a common cryptographic key by exploiting users' gait characteristics [30, 31]. In contrast to the above shake-based key generation methods, gait-based ones require no human intervention and are more user-friendly. Bruesch et al. provided a comprehensive discussion of the security properties of pairing schemes, including the efficiency of the quantization and authentication algorithms, statistical properties of the generated sequences, and the possible threats and security levels of the system, etc. [32].

Recently, Wu et al. proposed a novel machine learning framework that uses an auto-encoder to help one device predict the gait observations at another remote device attached to the same body and generate the key using the predicted sensor data [33]. However, this method is not flexible because once the sensor's position changes, a new predicting model target for the new sensor position needs to be trained.

From another view of point, Revadigar et al. presented a gait-based group key generation and distribution scheme for body area networks [26]. The on-board accelerometer sensor and the unique walking style of the user were used to generate random binaries by M-ary coding algorithms. Although sample points were used for key generation in this scheme, the guard band inserted between two consecutive quantization levels decreased the key generation rate. Moreover, the common information extraction algorithms used for sensors and coordinator placed on body parts other than chest is too energy and time-consuming.

We proposed an acceleration-based key generation and distribution method for wearable IoT devices based on the above survey and comparative analysis of available techniques. The coordinator takes advantage of the noise randomness to generate a group key and uses the common feature of the gait signal sampled from different body parts to distribute the key to other sensor nodes on the same body. The motivation for this study can be summarized as follows:

1. Due to the privacy and sensitivity features of personal data and the wireless nature of the communication, the security of the communication between these devices is essential to protect the transmitted data from being eavesdropped, tampered, or injected with malicious commands, while data sharing has to be kept strictly among body-worn devices that belong to the same user.

2. The available robust security solutions are not suitable for wearable devices. Firstly, conventional security schemes proposed for computers are too computationally demanding for miniaturized wearable IoT devices. Secondly, there are some deficiencies in data acquisition, anti-jamming and anti-attack of the recently emerging physiological biometrics-based bio-encryption technology.

3. With a decrease of in the cost and size of the acceleration sensors, more and more wearable IoT devices are

integrated with accelerometers for monitoring the human daily activities. The behavioral biometrics based bio-encryption methods are gaining much attention for their noninvasive and unique features.

4. Despite numerous advantages of accelerometer-based bio-encryption methods over conventional ones, their significant improvement is still required, including such features as the key randomness and the key distribution success rate.

The rest of this paper is organized as follows. The relavant recent works are discussed in Section II. The overview of the proposed security system for wearable IoT devices is introduced in Section III. The noise-based key generation method and gait characteristic-based common information extraction method are described in Section IV. The design of the fuzzy vault-based key distribution protocol is presented in Section V. The system performance concerning the key randomness, bit generation rates, and common information similarity are evaluated in Section VI. Finally, the conclusions are drawn, and the direction of follow-up studies outlined in Section VII.

II. Background

With the development of wearable IoT devices, their information security became the object of multiple studies. In this section, related works on biometric cryptographic systems and gait based key generation and distribution methods are summarized and analyzed.

A. Random bit sequence generation methods

To provide strong security of wearable IoT devices, a good random number generator (RNG) is essential. RNG is a critical component in any cryptographic system, producing random numbers to be used for both asymmetric and symmetric key generation, block cipher initialization vectors, one-time padding, digital signatures, and password storage [34].

There are two basic types of RNGs: true random number generators (TRNG) and pseudo-random number generators (PRNG). PRNGs are widely used in cryptographic systems as they can easily generate not truly random numbers at high speeds. However, PRNGs are vulnerable to brute-force attacks if the seed selection is faulty. To solve this problem, many state-of-the-art practical PRNGs use seeds generated by TRNGs to enhance the entropy and security level. However, the hardware-based TRNG methods, which require special integrated circuits to be embedded into the devices, are not suitable for wearable IoT decices due to their limited power and computational resources [35].

In recent years, several researchers used physiological signals to generate secure keys. For example, Pirbhulal et al. used IPIs of heartbeats to generate the random binary sequence for wireless BSNs, which incorporated a finite monotonic increasing sequence generation mechanism of IPIs and a cyclic block encoding procedure that extracted entropic bits from each IPI [13]. However, the heartbeat rate of a healthy person varies between 60-100 beats/min, as the above method uses the unpredictable change of IPIs to generate a random binary sequence, so the random bits generation rate is usually lower than the heartbeats rate. Miao et al. used the PPG and ECG signals to generate the key and secure the BSN [15]. However, the sampled signal quality was found to be deteriorated by the external environment. Human gait, due to its uniqueness and non-variability over time, has started to be utilized for securing wearable IoT devices in numerous studies [16-29], and is becoming an emerging research field.

B. Security key distribution method

The key distribution techniques are established based on two cryptographic primitives, namely the fuzzy commitment [35] and fuzzy vault [36] schemes. These two primitives have been widely investigated for the purpose of biometric key distribution, and their applicability to wearable device security has been analyzed by numerous studies [26, 35, 38]. These techniques used physiological or behavioral signals as common information to distribute and extract the key securely. The similarity of the common information is a key factor that influences the key distribution success rate.

Since each person has his/her own walking style, including the stride length and the stepping frequency, the gait signal collected at different body parts has a remarkable similarity, insofar as sensors placed in different body locations capture the same signal. Thus, gait features have been exploited to construct the vault and unlock it.

However, due to the complexity of body movements, devices placed in different body locations will capture different acceleration signals due to the movement of other body parts (such as arms), and this becomes the key challenge when exploiting the common gait signal for key fuzzy vault-based key distribution.

Fig. 2 depicts the acceleration signal in the gravity direction captured by devices placed at different body locations when the user was walking. It was infeasible to use the raw motion signals captured by the sensors to generate a common secret key directly. To address this challenge, we used the principal component analysis technique to separate the signals produced from gait and arm swing and apply the SSWC-based peak coding method to extract the common gait feature for fuzzy vault-based key distribution.

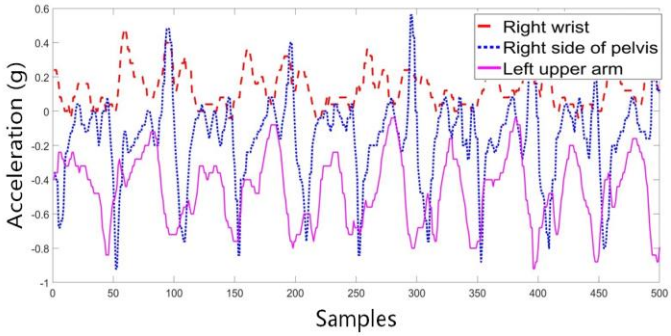


Fig.2. Acceleration signal from different body parts in the gravity direction captured by devices worn at different body locations when the user was walking

C. *Challenges and contributions*

Despite a significant progress made in previous studies, developments, the following problematic issues in the gait-based key generation and distribution methods need to be solved for their further large-scale application:

1. Generating a robust random key sequence: using the gait signal to generate a random key sequence directly would reduce the randomness due to the periodicity of human gait. Under the limited computing and energy resources, improving the randomness of the gait-based secret key is quite a challenge.

2. Extracting common information for key distribution: to distribute the generated key among all legitimate devices secretly, the common information shared by all devices should be extracted to lock and unlock the vault. Unlike the ECG or PPG signals sampled from different body parts which have a strong similarity, the acceleration signals sampled from different body parts are quite different due to the movement of other body parts (such as arms). Hence, extracting common information from acceleration signals sampled from different body locations is a more challenging problem, as compared to the ECG based methods.

To resolve the above problems, a light-weight noise-based random number generation method and a signed sliding window coding (SSWC) based common information extraction method were proposed in this work. In addition, the M-bit key distribution system was designed based on the fuzzy vault algorithm, and its performance was validated with a public dataset. The main contributions of this work can be summarized as follows.

1. A light-weight noise-based key generation method with high randomness and bit generation rate was proposed. The key generation rate (100bps in this study) for the proposed method is as high as the signal sampling rate when using no multilevel coding schemes.

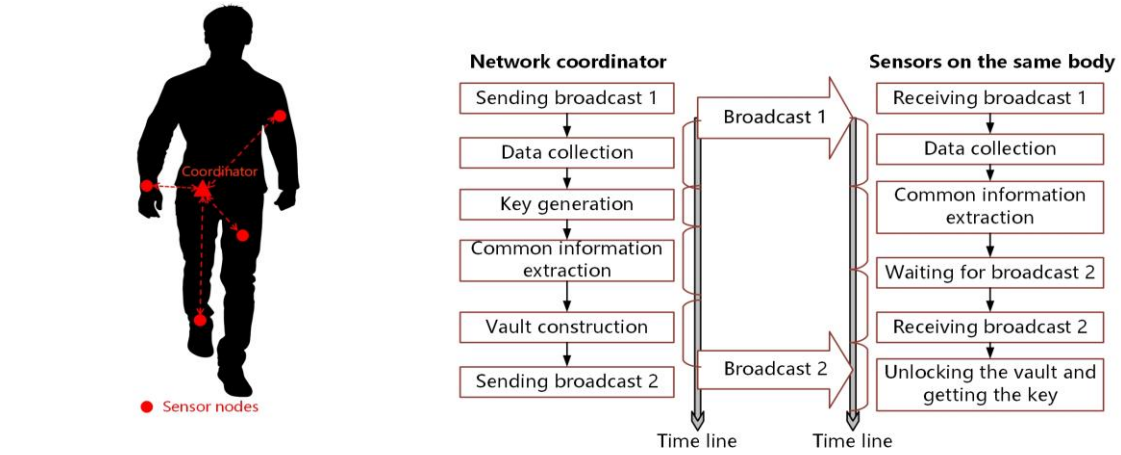
2. The energy and time consumption of the proposed methods was significantly reduced. The energy and time consumed by the coordinator for key generation, common information extraction, and vault construction are 4.95mJ and 3.84ms, which reduced the energy and time consumption by 61% and 98.2%, respectively, as compared to [26].

3. An SSWC-based common information extraction method was proposed to lock and unlock the vault in the key distribution process. Time scale and frequency scale information was fused to extract the common features. The average intra-body similarity of common features extracted from sensors on different body locations was 0.92, while the average inter-body similarity was just 0.39 (λ=0.5), which proved its excellent ability of detecting whether the sensors were worn on the same body or not.

4. A fuzzy vault-based key distribution method was proposed to share the generated key among sensors on the same body. Based on the proposed common information extraction, and the fuzzy vault construction framework, the average key distribution success rate reached 0.95.

III. SYSTEM OVERVIEW

In this section, the system overview of the proposed key generation method is presented. The system consists of a hub node and several sensor nodes. The hub node is usually a smartphone, which acts as a controller and a signal processor. The sensor nodes transmit the sampled various kinds of information to the hub node and execute the instructions issued by the hub node. In the network, the hub node generates the secret key using the accelerometer and pre-shares with legitimate sensor nodes through a fuzzy vault. The legitimate sensor nodes extract the key using the common gait feature received from the vault. The proposed wearable sensor network is shown in Fig.3 (a).



(a) Overview of the proposed wearable sensor network

(b) Overview of the network access process

Fig. 3. The overview of the system and the proposed methods

The overview of the proposed key generation and distribution system is depicted in Fig.3 (b). The network coordinator first sends a broadcast packet through the public channel to start the processes of key generation and distribution.

The broadcast1 contains the information on time duration *T* for the next data collection. The coordinator and sensors, which need to join the network, start to collect the acceleration data upon receiving the broadcast packet for the next *T* duration. Then, the coordinator uses the collected data to generate the random group key and extract the common information. After hiding the group key in a vault constructed using the common information, the coordinator integrates the vault with another broadcast packet and sends it to sensors. When sensors receive the second broadcast packet, they unlock the vault using the common information they extracted from the collected acceleration data and get the group key hidden in the vault. The definitions of parameters used in the proposed system are listed in Table I.

TABLE I. DEFINITIONS OF THE SYSTEM PARAMETERS

Parameter	Description
M	The length of key bits
w_t	The window size of the time scale
λ	The coefficient used to calculate the window size
N	The polynomial order
L	The length of the acceleration signal used to extract common information
v	The vault size

In the following sections, the key generation methods, the common information extraction method, and the fuzzy vault-based key distribution method are described in detail.

IV. KEY GENERATION METHOD

In this section, we introduce the noise-based M-bit key generation method, including the noise extraction method based on the zero-phase Butterworth filter, the coding method, and the M-bit key generation method. The main idea of the proposed method was inspired by the fact that the noise superimposed on the regular gait signal, which mainly caused by the irregular motion of human body parts and the nearby environment (such as electromagnetic interference and power frequency interference), possesses the characteristic of randomness and uncertainty, and is a good source of entropy.

Noteworthy is that the accelerometer's noise is random, which makes it a good entropy source to generate the random binary sequence. A noise-based random key generation method was designed, and the common gait information was extracted to share the key among the devices worn on the same body. The proposed scheme can improve the user experience significantly, as walking is a normal activity, and the wearable IoT devices can access the network automatically when the user is walking.

A. Overview of the noise-based key generation algorithm

The proposed key generation method is presented in Algorithm 1. It includes five main steps: filtering, normalization, noise extraction, coding according to the noise level, and downsampling to enhance the randomness. First, the three-axis acceleration signal (ACCx, ACCy, and ACCz) is filtered through a specially designed zero-phase filter, and the amplitudes of raw and filtered signals are normalized. Then, the noise is extracted via the difference between the raw and filtered signals. The random bit sequences are generated according to the noise level and the XOR operator is applied to the RBS to enhance the randomness of the sequences. Finally, the M-bit random key is generated by down-sampling the generated sequence.

Algorithm1: M bits Key generation method

Input:

Acceleration data: ACCx, ACCy, ACCz
Sample frequency: f_s
Cutoff frequency: f_c
Key length: M

Procedure:

```
1. filter=Filter design (fs,fc);
2. ACC#_filtered = filter(ACC#); % # represent x, y and z
3. diff# = ACC#-ACC#_filtered; %compute the signal noise
4. Len=length(ACCx);
5. For i = 1:len
6. if diff# >= 0 % coding according to the value of the signal noise
7. key_#(i)= 1;
8. else
9. key_#(i)=0;
10.End for
11.key=bitxor(key_x, key_y, key_z);% Perform XOR operation to improve the
   randomness
12.w=floor(len/M);
13.For j=w:w:M*w %down sampling and generating the M bits key
14.key_M(j/w)=key(j);
15.End for
```

Output:

M bits random key : key_M

B. Zero-phase filtering process

An accurate noise signal extraction is the key to the noise-based key generation method. However, the phase shift caused by the conventional filter makes it very difficult to extract the noise signal.

Keeping the phase and amplitude of the signal undistorted is a key factor to precisely extract the noise superimposed on the gait signal. For this purpose, we designed a zero-phase four-order low-pass Butterworth filter to remove the high-frequency noise. As the average gait frequency is between 1.7 and 2.7 Hz, the cut-off frequency of the designed filter is set to 3 Hz. The flowchart of the zero-phase filtering process is shown in Fig. 4.

The three-axis raw acceleration signals (represented by *r_sig*) are first inputted into the designed low-pass Butterworth filter. Then, the first output filtered signal *f_sig* is reversed and converted to the time-reversed signal *rev_f_sig*. The latter is inputted into the above filter and reversed again to yield *rev_ff_sig* with a zero-phase distortion.

Figure 5(a) presents an example of zero-phase filtering results: as compared to the raw signal, the phase of the filtered

one remains unchanged, but the amplitude is largely attenuated by the square of the filter's response magnitude.

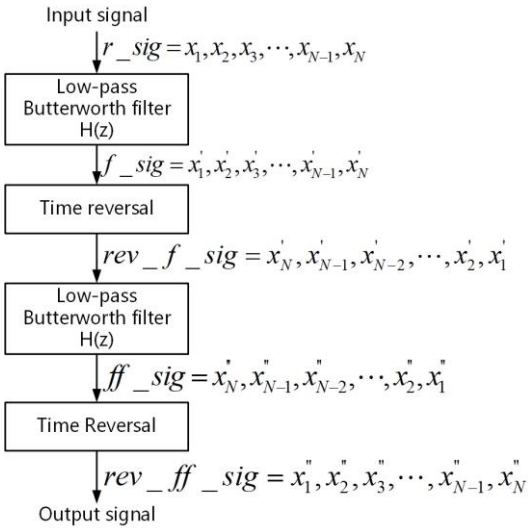


Fig.4. Flowchart of the zero-phase filtering process

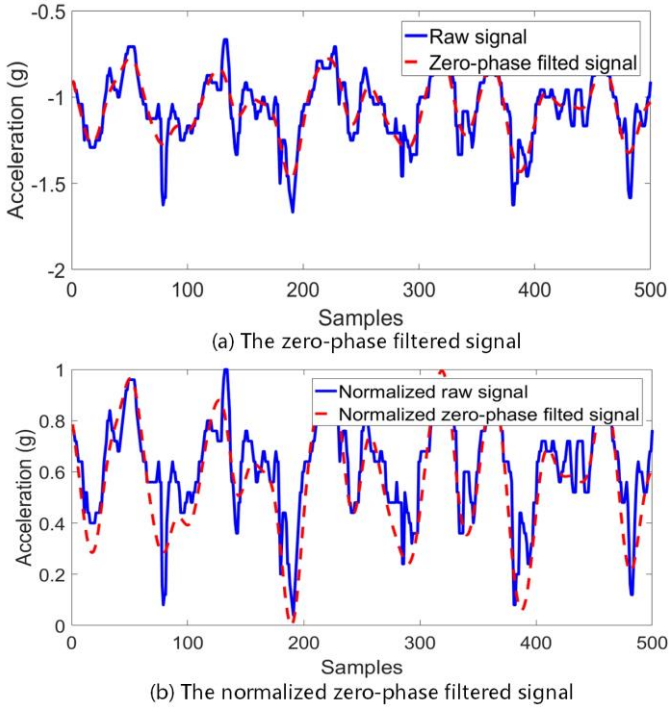


Fig.5. An example of zero-phase filtered signal and its normalization

C. *Noise extraction and coding*

To compensate for the attenuation of signal amplitude, the magnitudes of signals *r_sig* and the *ff_sig* are normalized before calculating their difference. As seen in Fig. 5 (b), the difference between the amplitudes of *r_sig* and *ff_sig* was reduced by the above normalization procedure.

Next, the noise *n-sig* is calculated via the difference between the raw and filtered signals as follows:

$$n\_sig = r\_sig - ff\_sig \tag{1}$$

For the coding process, three binary sequences would be generated, according to the noise value imposed on the three-axis acceleration. If *n_sig* is negative, the binary is set at "1"; otherwise, it is set at "0". After the same process is performed for the three-axis acceleration signal, values of *key_x*, *key_y*, and *key_z* are calculated, as shown in Fig.6.

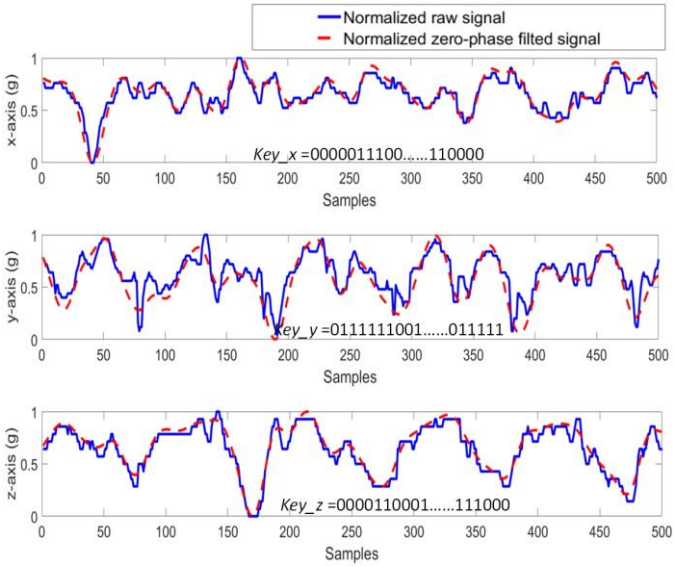


Fig.6. Coding by the *n-sig* value

To enhance the generated key randomness, the XOR operation is performed for *key_x*, *key_y*, and *key_z*.

$$key = key\_x \oplus key\_y \oplus key\_z \tag{2}$$

According to the length of the acceleration signal used to generate the secret key, one can further enhance the randomness by downsampling the binary sequence. Finally, the wearable IoT device generates the M-bit secret key *key_M*, which will be used to secure the data transmitted through the wireless channel.

V. SSWC-BASED GAIT COMMON INFORMATION EXTRACTION METHOD

The common gait feature information shared by all sensor nodes worn on the same body is used to lock and unlock the vault. The intra-similarity of the extracted common information is a very important factor for key distribution.

During walking, the raw acceleration measured by multiple body-worn devices is the result of the user's gait as well as the movement of individual body parts, e.g., feet and arms, and hence, devices located in different places experience different accelerations, as shown in Fig.2. However, from the time scale, positions of the peak points caused by heel-strike events and though/valley points caused by toe-off events are identical. So, in this section, the time scale information of the gait features is extracted as common information, and a signed slide window coding (SSWC)-based method is designed and used to extract the common information shared by all nodes on the same body. Before the SSWC-based common information extraction, the raw signal is firstly preprocessed by the principal component analysis (PCA) method to reduce the dimensionality of the

acceleration signal.

A. Data preprocessing

For the data preprocessing, the high-frequency noise was first reduced by a low-pass Butterworth filter with a 3 Hz cut-off frequency. In order to reduce the impact of the irregular motion of other body parts on common gait information extraction, the sampled acceleration signal was first preprocessed by a low-pass filter and the principal component analysis (PCA) algorithm. The PCA could effectively extract the signal caused by gait from the raw signals, whereas the first component of the signal represented the motion caused by gait. According to our test results, the contribution rate of the first component was exceeded 90%.

The *r_signal* is composed of the three-axis acceleration signals. The format of the *r_signal* is given by Eq.(3). The PCA analysis results are formulated in Eq.(4), where *E* and *E(:,1)* correspond to eigenvectors of *r_signal* and maximum eigenvalues, respectively.

$$r\_signal = \begin{bmatrix} acc\_x_1 & acc\_x_2 & \cdots & acc\_x_M \\ acc\_y_1 & acc\_y_2 & \cdots & acc\_y_M \\ acc\_z_1 & acc\_z_2 & \cdots & acc\_z_M \end{bmatrix} \quad (3)$$

$$pca\_signal = E(:,1)^{'} * r\_signal \quad (4)$$

The signal after the PCA process is depicted in Fig.7. The peak points of the *pca_signal* are caused by toe-off events while the valley points are caused by heel-strike events. The occurrence time of the two gait events detected by different sensors is of high consistency. Therefore, in this study, the occurrence time of the toe-off and heel-strike events was used to generate the common information, as well as to construct and deconstruct the fuzzy vault.

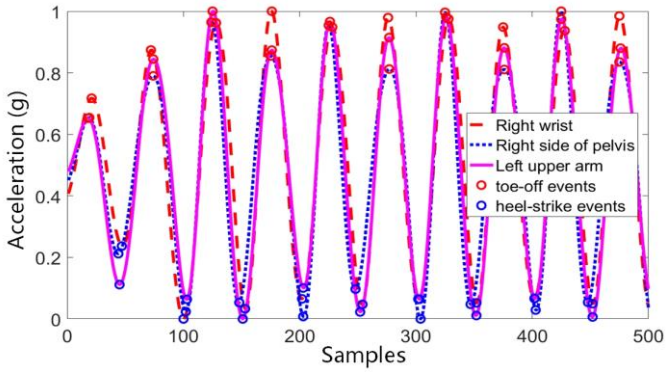


Fig.7. The PCA results of the acceleration signal sampled from different body parts

B. SSWC-based common information extraction

In this section, the proposed signed slide window coding (SSWC) method is described. Firstly, the *pca_signal* is inputted into the fast Fourier transformation (FFT) model to calculate the step frequency f_{step}, and then the window size for SSWC-based common feature extraction is set according to f_{step}. It can be seen in Fig.8 that frequency peaks of signals sampled from three different body parts are very similar.

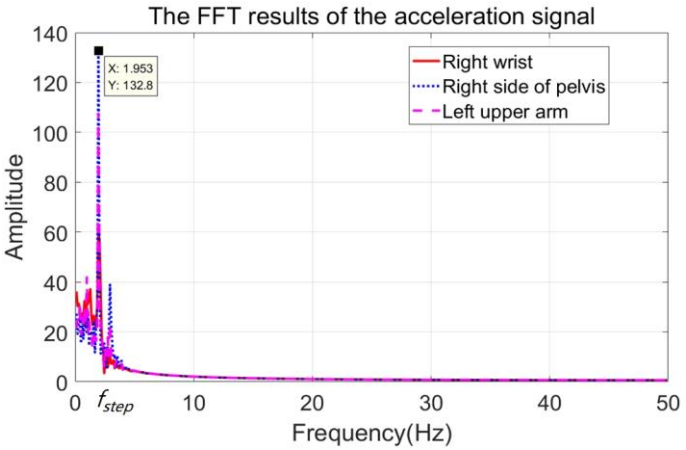


Fig. 8. The FFT results of the pca_signal sampled from different body parts

The sliding window size w_t for SSWC-based common information extraction is defined as follows:

$$w_t = \left\lfloor \lambda * \frac{f_s}{f_{step}} \right\rfloor \quad (5)$$

where f_s is the sampling frequency, f_{step} is the detected step frequency, λ is a parameter set according to the application scenarios. The range of λ is (0,1], whereas smaller values of λ correspond to higher the security level and computing complexity.

In the proposed SSWC quantization method, the existing peak and valley points in the N_{th} window, if any, are coded as *N* and –*N*, respectively. In the absence of such peak or valley points in the window, the latter just slides forward. One of the quantization examples is depicted in Fig. 9. We set the window size factor λ= *0.1*5.

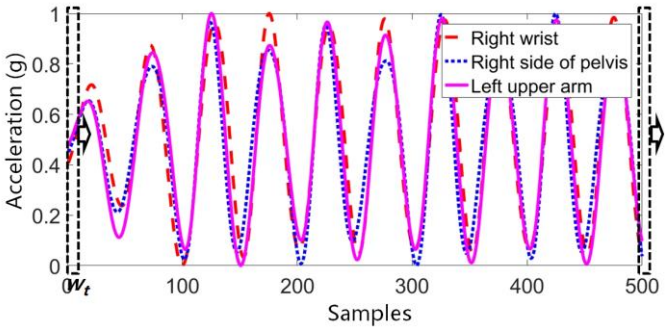


Fig.9. Non-overlapping signed sliding window coding of the peak value.

VI. KEY DISTRIBUTION METHOD

Fuzzy vault is a theoretically secure cryptographic construct for hiding a secret key in vault *V* by using a set *A*. The vault can be unlocked only by another set *B* that sufficiently overlaps with *A*.

The proposed fuzzy vault-based key distribution method mainly includes two procedures: the vault locking process and the vault unlocking one. The workflow of the key distribution algorithm is presented in Fig.10.

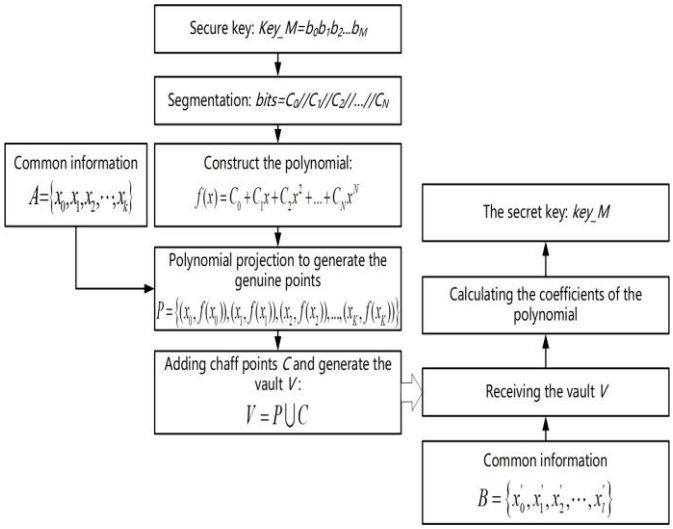


Fig.10 Fuzzy vault-based secrete key distribution process

A. *Vault construction*

The fuzzy vault construction process mainly includes the following steps, as shown in Fig.10:

1. Data segmentation: in order to conceal the random binary key sequence in the vault, the binary sequence is segmented into *N*, and

$$\text{bits} = C_0 // C_1 // C_2 // \cdots // C_N \tag{6}$$

2. Polynomial construction: the segmented values are used as coefficients to construct an *N*-order polynomial *f(x)*.

$$f(x) = C_0 + C_1 x + C_2 x^2 + \ldots + C_N x^N \tag{7}$$

3. Vault construction: using the common information *A* extracted in the previous subsection, the mapping of common information on polynomials is computed to obtain *P*. Then, a large number of chaff points are added, and the fuzzy vault is constructed. Finally, the coordinator sends the constructed fuzzy vault *V* to the sensor nodes.

The projection of set *A* on polynomial *p* is calculated to obtain the set *P = (A, f(A))*. A large set of random chaff points *C* that excludes set *A* of elements and does not intersect with polynomial *p* is constructed to obtain the vault via Eq.(10). Vault *V* will be a large set of points, in which secret points of *P* are masked by random chaff points (noise). The chaff points are added to *V* in such way that they cannot be distinguished from *P* using the statistical analysis:

$$A = \{x_0, x_1, x_2, \cdots, x_k\} \tag{8}$$

$$P = \{(x_0, f(x_0)), (x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_K, f(x_K))\} \tag{9}$$

$$V = P \cup C \tag{10}$$

B. *Unlocking the vault*

For the vault unlocking process, when sensor nodes receive the vault sent by the coordinator, they use the common information *B* extracted from the acceleration signal to reconstruct the polynomials and then get the key concealed in the polynomials.

$$B = \{x_0', x_1', x_2', \cdots, x_l'\} \tag{11}$$

VII. EVALUATION

In this section, we design experiments to test the performance of the proposed key generation and distribution methods. For the key generation methods, the randomness and bit generation rate are mainly considered. For the key distribution rates, we mainly analyze the correlation coefficient among the common data extracted from different body parts. The Pearson correlation coefficient (PCC) is used to evaluate the intra- and inter-similarity of common information.

A. *Performance of the key generation method*

For key extraction between a pair of wireless devices, the bit mismatch rate is defined as the number of bits that do not match between two devices divided by the total number of secret bits extracted. For group key extraction, it is defined as the averaged bit mismatch rate from all pairs of devices in the group.

1. Randomness test

For the randomness of the generated binary sequence, the NIST (National Institute of Standards and Technology) and the Dieharder tests were conducted to assess the randomness performance. The latest NIST-STS version 2.1.2 included 15 tests, each of which was designed to test a pre-defined null hypothesis. The tested sequence was random and designated by H_0. It also produced a probability value (p-value) in the range of the interval [0, 1]. If the p-value was larger than the threshold, H_0 was accepted; otherwise, H_0 was rejected [38]. However, limited by the length of the generated binary sequence, we selected several tests from NIST to perform the randomness evaluation. The test results are listed in Table II.

Dieharder statistical tests consisted of tests from Diehard and many improved tests from NIST [39]. The distribution of p-values of 100 runs of the Dieharder tests for the dataset sampled from the right wrist is shown in Fig. 11. If a p-value from the Dieharder statistical test is below 0.001, the test is considered as failed. However, p-values are expected not to exceed 0.05 (weak) 5% of the time. The results showed no failure incidents in any tests and included a few incidents where $p \leq 0.05$ was expected. Furthermore, the p-values of all tests were well-distributed over the interval [0, 1], indicating that keys successfully passed all the Dieharder statistical tests.

TABLE II: P-VALUE RESULTS OF THE NIST STATISTICAL TESTS

NIST Test	p-value	
	Right wrist	**Right side of the pelvis**
Frequency	0.890121	0.869021
Block frequency	0.730901	0.887932
FFT	0.233295	0.678987
Runs	0.212568	0.689091
Longest run	0.476970	0.744939
Entropy	0.989152	0.996787
Serial	0.517388	0.897461
Non-overlapping template	0.367982	0.476098
Cumulative sums forward	0.873556	0.901933
Cumulative sums reverse	0.657120	0.790993

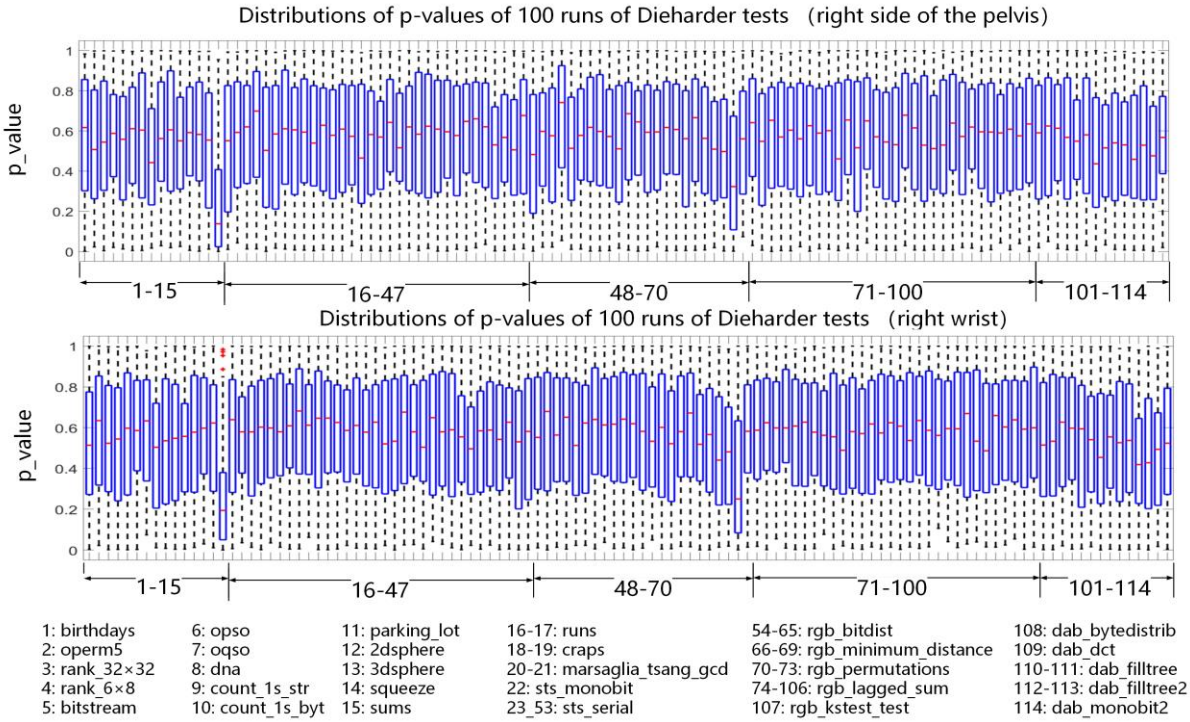


Fig.11. The distribution of p-values in the Dieharder tests

2. Bit generation rate

The bit generation rate represents the number of secret bits extracted per measurement. It denotes the average number of bits generated from acceleration samples per unit time and is usually measured in bits per second (bps). This metric evaluates how fast the coordinator can generate secret bits.

As we used no complex multilevel coding methods, the bit generation rate of the proposed noise-based key generation method was only affected by the sampling rate of the acceleration signal. The maximum bit generation rate was the same as the sampling rate (100bps in this study). It took less than 2 seconds to generate a 128-bit key.

Further, we compared the bit generation rate with three related works. The comparative analysis results listed in Table III strongly indicate that the proposed method, which uses no multilevel coding schemes, such as the m-ary, exhibits the bit generation rate outperforming those of three related key generation methods used for comparison. In particular, the first method was the IPIs-based key generation method proposed by Sun et al. [29] using the variation between the lengths of each

gait cycle to generate the binary sequence. As the gait frequency is far lower than the sampling frequency, its bit generation rate is still very low, although multi bits were assigned to each cycle in the quantization process. The second one was the symmetric key generation method proposed by Xu et al. [31], which implied coding the acceleration sample point itself to generate the random binary sequence. In the third method proposed by Revadigar et al. [26], the bit match rate and the bit sequence randomness were improved by using a multilevel quantization scheme, where a small band called 'guard band' was inserted between two consecutive quantization levels. The samples in the guard band were excluded during quantization, which would reduce the bit generation rate.

TABLE III: BIT GENERATION RATES OF THE PROPOSED METHOD AND THREE OTHER ONES [26, 29, 31]

	Sampling rate (Hz)	Method	Parameters	Bit generation rate (bps)	Time to generate a 128-bit key (s)
This study	100	Noise-based key generation	/	100	1.28
Sun et al. [29]	100	IPIs-based key generation	/	/	≈ 16 (32 gait cycles)
Xu et al. [31]	100	m-ary quantization	*m=2*	28	4.6
			m=4	37	3.5
			m=8	43	3
Revadigar et al. [26]	50	m-ary quantization	*m=2* $\alpha^{1*}=0.5$ *W²*=50*	25	5.12
			m=8 $\alpha^{1*}=0.5$ *W²*=50*	75	1.71
			m=32 $\alpha^{1*}=0.5$ *W²*=50*	125	1.02

1: α is the guard band- to-data ratio*
2: W is the size of the non-overlapping moving window*

B. Performance of the key distribution method

In this section, the factors that influence the key distribution are discussed, and the key distribution success rate is evaluated for different scenarios. Firstly, the similarity of the common information extracted from different body parts is compared and analyzed.

1. The similarity of the common information

The Pearson correlation coefficient (PCC) was used to evaluate the similarity of the common information extracted from different body parts. PCC shows the linear relationship between two sets of data. Its value is ranged between -1 and +1, where −1 implies the total negative linear correlation, 0 corresponds to no linear correlation, and +1 is the total positive linear correlation. The following equation is used to derive PCC.

$$\rho_{x,y}=\frac{\mathrm{cov}(x,y)}{\sigma_x\sigma_y}=\frac{E((x-\mu_x)(y-\mu_y))}{\sigma_x\sigma_y} \tag{12}$$

where *Cov* is the covariance between *x* and *y*, σ_x and σ_y are the standard deviations of *x* and *y*, respectively, μ_x and μ_y are the mean values of *x* and *y*, respectively, while *E* is the expectation.

The correlation between datasets is a measure of their relation closeness. The PCC between the common information extracted from different body parts reflects their similarity. The intra-similarity (of different body parts of the same subject) and the inter-similarity (of different body parts of different subjects) were analyzed.

Firstly, in order to test the similarity of the common information extracted from sensors worn on different body parts, we used the PCC to evaluate the intra- and inter-similarities of the extracted common information when the window size factor λ varied from 0.1 to 1.

The test results on the PCC between different body parts (Fig.12) implied that the correlation coefficient grew with the window size. This finding was quite expected: when the window widened, peaks or valleys of different sensor signals were more likely to be in the same window.

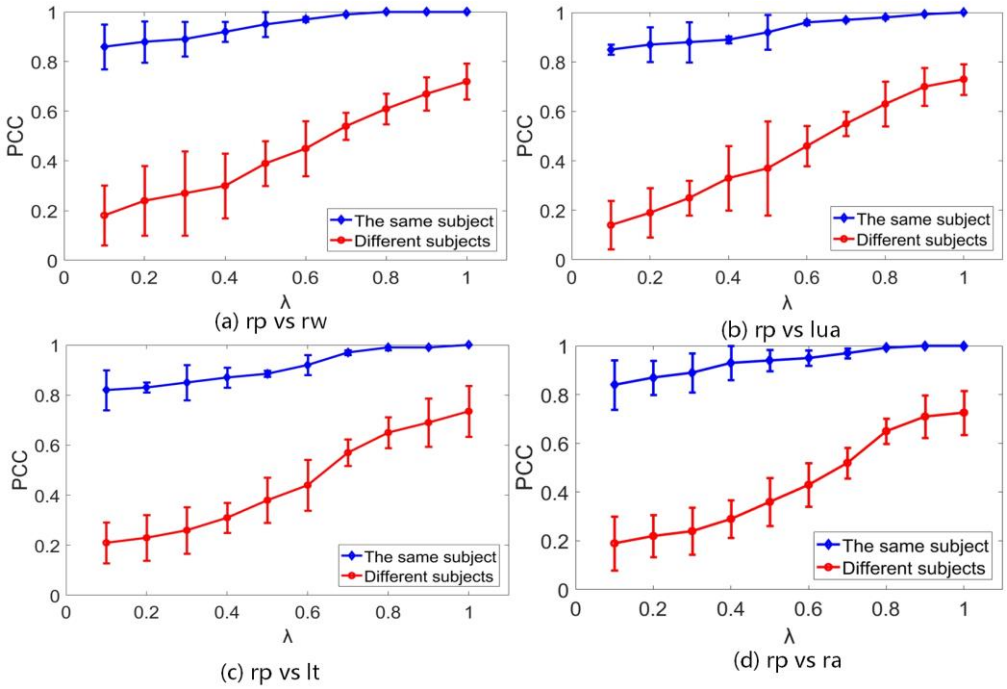


Fig.12. Comparison of the similarity of time scale common information extracted from different body parts of the same subject and different subjects versus the window size: w_t

2. The key distribution success rate

Besides, the key distribution success rate was tested to evaluate the overall key distribution performance. In this experiment, 500 samples of acceleration signals were collected by the hub node and sensor nodes synchronously. Then, a 128-bit binary key sequence ($b_1, b_2, \ldots, b_{128}$) was first generated in the hub node, and a 16 order polynomial function was constructed using segments of the generated 128-bit binary key sequence as its coefficients, $C_i=b_{(8*i+1)}, b_{(8*i+2)}, \ldots, b_{(8*i+8)}$, where $i=0, 1, \ldots, 16$. The hub and the sensor node extracted their own common information through the previously collected 500 samples of acceleration signals using the proposed SSWC method with $\lambda=0.15$. Then the hub node sent the common information concealed in the vault with size of 300 to the sensor nodes through a public channel. The sensor nodes attempted to reconstruct the eight-order polynomial using their own common information on receiving the vault.

First, we tested the key distribution success probability using the open dataset ZJU-GaitAcc shared by [17]. The ZJU-GaitAcc dataset contains the gait acceleration series of 175 subjects. 153 of which are present in two sessions (Session 1 & 2). For each subject, six records are included in one session, where each record contains five gait acceleration series simultaneously measured at the right wrist (rw), left upper arm (lua), right side of the pelvis (rp), left thigh (lt), and right ankle (ra), respectively. In this experiment, we used the acceleration data of the 153 subjects in session 1 to test the key distribution success probability. For each subject, the sensor placed on the right side of the pelvis acted as a hub node and generated a 128-bit binary key sequence using the data collected in the first record. Then, the hub node distributed the key sequence to other sensor nodes through the proposed fuzzy vault-based key distribution method. The intersection between the common information datasets extracted by the hub node and the sensor nodes was computed. If the size of the intersection dataset exceeded the polynomial order, the key distribution was a success, otherwise, it was failed. As there were six records for each subject, if the key was not successfully shared between the hub and sensor nodes, the next record was used to generate another common information datasets and make another attempt to distribute the binary key sequence through the fuzzy vault. The probabilities of success against the number of attempts for the sensors placed in different body locations (the hub node being placed on the pelvis right side) were calculated and plotted in Fig. 13. The results obtained show that the average success rate after a single attempt is about 0.95, and after four attempts, the success rate reaches 1.

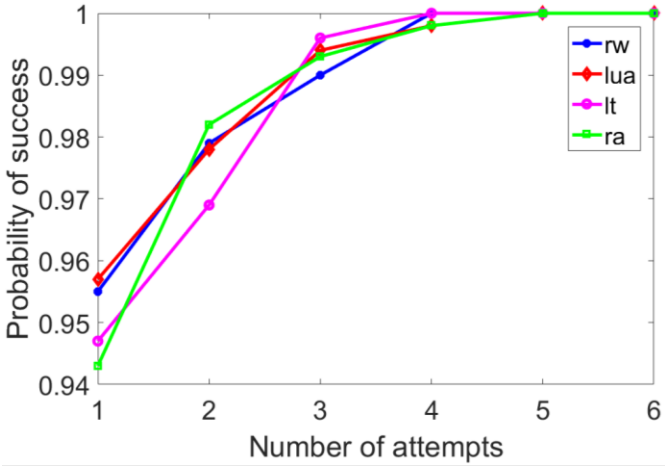


Fig. 13. Key distribution success probability tested on ZJU-GaitAcc dataset

Further, we used the real word dataset RealWorld (HAR) shared by [42, 43] to test the robustness of the proposed

methods. This dataset was collected in real-world scenarios and covers six kinds of sensor data of 8 common activities: climbing stairs down and up, jumping, lying, standing, sitting, running/jogging, and walking. There were fifteen subjects (eight males and seven females) enrolled in the data collecting process. The participants' statistical characteristics were: age 31.9±12.4, height 173.1±6.9, and weight 74.1±13.8. For each activity, the acceleration of seven body positions (chest, forearm, head, shin, thigh, upper arm, and waist) was recorded simultaneously. According to our test purpose, only walking acceleration data of each subject was used for this experiment. The sampling frequency of the acceleration signal for walking is 50Hz, and the length of the acceleration signal for each subject is about ten minutes. Firstly, we removed the data collected in the first two minutes after the start to reduce the interference in the start-up phase of the experiment. Then, the next 3000 samples (about 1 minute long) were extracted and divided into six sections with equal length.

The acceleration data collected on the waist were used to generate the key and construct the vault. In contrast, the acceleration data collected on the other body positions in the same section was used to unlock the vault and recover the key hidden in it. If the key was not successfully distributed through the acceleration data in the first section, the next section of acceleration data was used to generate another common information dataset and make another try to distribute the binary key sequence through the fuzzy vault. The key distribution success probabilities against the number of attempts for the sensors placed in different body locations (the waist sensor was used as the hub) were calculated and plotted in Fig. 14. We can see from the results that the distribution success probability after a single attempt was 0.94, being slightly lower than that obtained on the ZJU-GaitAcc dataset. The reason for the performance degradation is that the complex walking environments (non-flat ground condition, etc.) and the motion of other body parts (head, hand, etc.) deteriorated the gait signal's consistency sampled from different body positions.

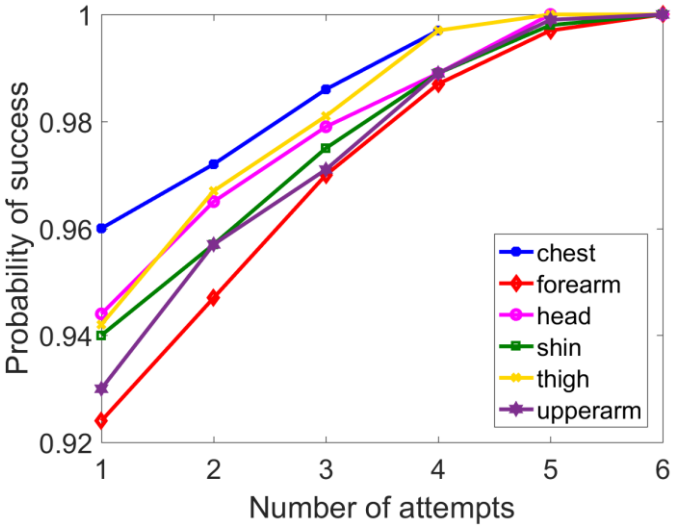


Fig 14. Key distribution success probability tested on RealWorld (HAR) dataset

C. *Resource consumption analysis*

In this section, we evaluated the light-weight feature of the proposed method from the perspective of resource (including energy and time) consumption. The proposed noise-based key generation algorithm, SSWC-based gait common information extraction algorithm, and the fuzzy vault locking and unlocking algorithm were first converted to Android application programs. Next, the Trepn Profiler diagnostic tool [40] designed by Qualcomm was used to test the energy and time consumption of the proposed algorithms when generating and distributing a 128-bit binary key. The energy and time consumptions of the proposed algorithms are summarized in Table IV. We further compared the resource consumption of the coordinator and the sensor with the model proposed in [26]. The comparison results are listed in Table V. One can see that, although the energy and time consumptions of the sensor in our work exceeded those of the chest-worn sensor in [26], the total energy and time consumption of the coordinator and the sensor were much lower than those in [26]. Besides, as the wrist-worn sensor needs to extract the gait signal from the sampled complex signal using the independent component analysis algorithm, the energy and time consumption of the wrist-worn sensor in [26] significantly exceeded ours.

TABLE IV: ENERGY AND TIME CONSUMPTION TEST RESULTS

Algorithm	Energy (mJ)	Time (ms)
Key generation algorithm	0.1207	0.1331
Gait common information extraction algorithm	4.7911	3.6763
Vault locking algorithm	0.0398	0.0277
Vault unlocking algorithm	0.0467	0.0302

TABLE V: COMPARISON RESULTS OF ENERGY AND TIME CONSUMPTION WITH [26]

Device	Energy (mJ)	Time (ms)
Coordinator (this study)	4.9516	3.8371
Sensor (this study)	4.8378	3.7065
Coordinator [26]	12.7713	208.782
Chest-worn sensor [26]	0.0720	0.6820
Wrist-worn sensor [26]	364.7503	486.4320

D. *Security analysis*

1. Vault security

In this section, we discuss the security level of the vault. The security offered by the vault depends on the vault size (v) and the constructed polynomial order (N). More chaff points added to the vault and higher order of the constructed polynomial increase the vault security level. The latter can be calculated as follows:

$$security\ level = log_2(C_v^N) \quad (13)$$

The test results obtained for different vault sizes and polynomial orders are shown in Fig.15.

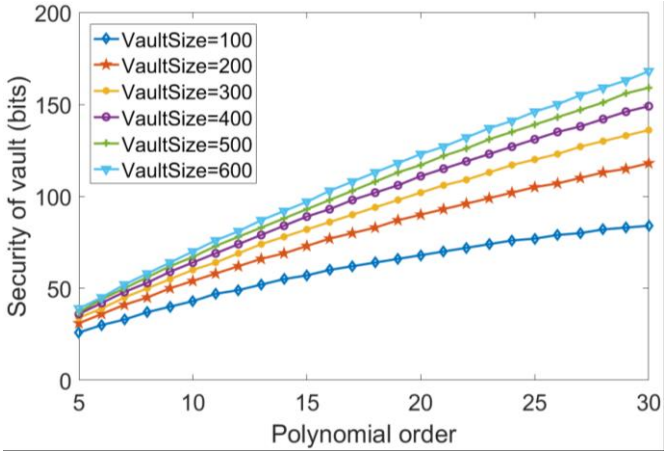


Fig. 15 Security level test results for different vault sizes (100 to 600)

2. Anti-imitation attack ability

In order to further evaluate the security performance of the proposed methods, we designed imitation attack experiments and analyzed the mimicking attack threats.

In these experiments, 8 subjects were recruited and subdivided into 4 groups as shown in Table VI. Two subjects with a similar body shape (height and weight) or their walking style are naturally similar were selected in each group to act as a genuine user and his/her imitator (adversary). To achieve better mimicking effects, the adversaries were asked to imitate the walking style of the genuine users during the experiments. At the same time, two (wrist- and waist- worn) IMU sensors with a 100Hz sampling frequency [41] were used to collect the walking acceleration data of the genuine user and the adversary simultaneously. The test scenario is illustrated by Fig. 16.

TABLE VI: GROUPING AND PHYSICAL PARAMETERS OF THE TEST SUBJECTS

Group	Subject	Gender	Age (yrs)	Height (cm)	Weight (kg)
G 1	Sbj. 1	F	29	163	50
	Sbj. 2	F	37	164	55
G 2	Sbj. 3	M	30	157	62
	Sbj. 4	M	30	170	56
G 3	Sbj. 5	M	29	172	70
	Sbj. 6	M	36	174	80
G 4	Sbj. 7	F	32	165	56
	Sbj. 8	M	33	170	63

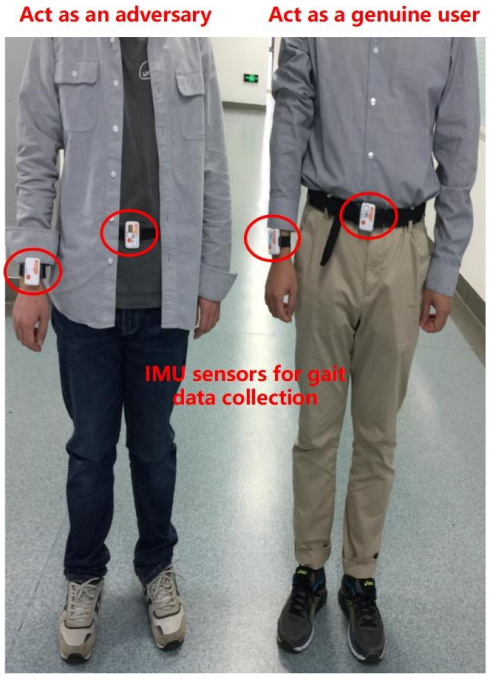


Fig. 16 The imitation attack test scenario: genuine user and his/her gait imitator (adversary)

For the threats' model analysis, we considered the following two scenarios. The first one envisaged that the adversaries would try to generate the same key as genuine users of the same group by using their own acceleration signal through mimicking the walking style of the genuine user. For this scenario, the hamming distance (HD) between the keys generated by the genuine user and the adversary was used to evaluate the anti-imitation attack ability of the proposed methods.

The acceleration signals collected by the IMU sensors worn on the wrist and waist were used to generate a 128-bits key, respectively, based on the proposed noise-based random key generation method. Then, the HD between the keys generated by genuine users and adversaries in the same group was computed, as shown in Fig. 17. The results indicate that the average HDs between keys generated from IMU sensors worn on the wrist and waist were 81 and 88 bits, respectively. Thus, the proposed noise-based random key generation method effectively prevented the adversaries to achieve the true key by mimicking the walking style of genuine users.

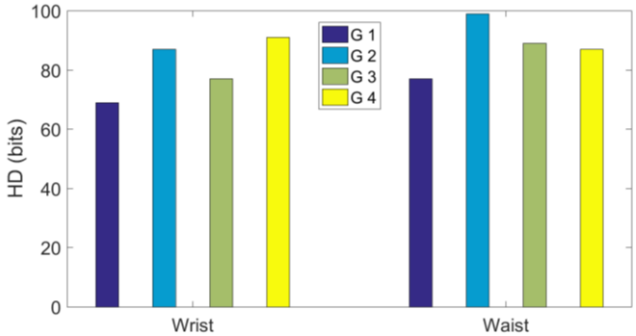


Fig. 17 The HD between the keys generated by the genuine users and their adversaries

The second scenario implied that the adversary would attempt to extract the key from the vault transmitted by the

genuine user through the public channel using his/her own gait feature through mimicking the walking style of the genuine user.

In this test, a 128-bit binary key sequence and S (S=20) gait common information ($gc_1, gc_2,\ldots,gc_S$) were generated using the proposed methods based on the wait-worn acceleration sensor signal collected by the genuine user. Then, a 16-order polynomial function $f(x)$ was constructed using segments of the generated 128-bit binary key sequence as its coefficients, and the genuine pairs of values $(gc_i, f(gc_i))$ which could be used to unlock the vault was computed by substituting the common gait information into the polynomial. A software random number generator was used to generate chaff points pairs that were not present in the polynomial function $f(x)$, and genuine pairs and the generated chaff point pairs were merged and mixed to form a vault with a size of 300. The adversaries tried to unlock the vault using the common gait information extracted from their own acceleration sensors. In the absence of the application program for the sensor nodes, the performance was evaluated offline using the acceleration data collected in advance. It was assumed that the adversary nodes had no prior knowledge on the key length and the polynomial order, so the recovered key length could differ from that of the true/genuine key. We modified the similarity index (SI) defined in [26] to evaluate the similarity between the recovered and genuine keys via Eq. (13).

$$SI = \frac{|genuine\ Key \cap recovered\ Key|}{|genuine\ Key|} \quad (13)$$

Here, SI varies between 0 and 1. Higher values indicate that the genuine and recovered key have more common elements. SI will be 1 if the recovered key is a subset of the genuine key and contains no chaff points.

The SI values between (i) the genuine key generated by the waist-worn acceleration of the genuine user and those recovered via his/her wrist-worn acceleration sensor, (ii) the genuine key generated by the waist-worn acceleration of the genuine user and those recovered by the waist- and wrist-worn acceleration of the adversary, were computed and plotted in Fig. 18. These test results strongly indicate that it is hard for any adversary to recover the genuine key by mimicking the walking style of the genuine user.

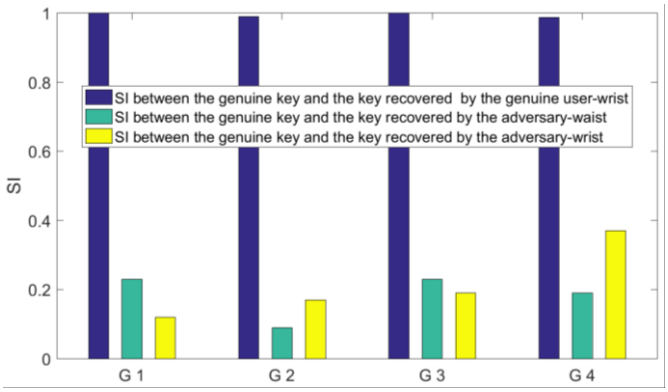


Fig. 18 The values of SI for the genuine and recovered keys

VIII. Conclusion and Future Work

This paper proposed a light-weight noise-based M-bit key generation method for wearable IoT devices. We designed a zero-phase filter to extract the noise imposed on the regular gait signal. As the noise has the properties of randomness and uncertainty, the binary sequence generated based on the noise value has good randomness and high entropy. For sharing the generated key among different wearable IoT devices in the same body area network, an SSWC-based common feature extraction method was first designed to extract the gait common information from acceleration signals sampled by different wearable IoT device. Next, fuzzy vault-based key distribution methods were used to secretly transmit the generated key among wearable IoT devices in the same body. A comprehensive analysis of the proposed key generation and distribution method proved that the binary keys generated via the introduced noise-based procedure have high entropy and can pass both the NIST and Dieharder statistical tests with high efficiency. The experimental results proved the robustness of the proposed SSWC-based common feature extraction method in terms of the similarity and discriminability of intra- and inter-class features, respectively.

For future research, the realistic scenarios' online tests for gait-based key generation and distribution should be performed. The active attacks, including walking posture imitation and machine vision-based gait synthesis should be taken into consideration. The follow-up studies are envisaged to apply multi-biometric fusion-based secure methods to further enhance the security level of wearable devices.

References

[1] M. Chen, S. Gonzalez, A. V. Vasilakos, H. Cao, V. C. Leung. Body area networks: A survey. Mobile Networks and Applications. 16(2), pp.171-93, 2011.

[2] R. A. Khan and A. S. K. Pathan. The state-of-the-art wireless body area sensor networks: A survey. International Journal of Distributed Sensor Networks, 14(4), pp.1-23, 2018.

[3] S. Hiremath, G. Yang, K. Mankodiya. Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), 2014.

[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 20(8), pp.2481-501, 2014.

[5] O. Arias, J. Wurm, K. Hoang, Y. Jin. Privacy and security in internet of things and wearable devices. IEEE Transactions on Multi-Scale Computing Systems, 1(2), pp.99-109, 2015.

[6] M. Lee, K. Lee, J. Shim, S. J. Cho, J. Choi. Security threat on wearable services: Empirical study using a commercial smartband. IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), pp.1-5, 2016.

[7] A. J. Perez and S. Zeadally. Privacy issues and solutions for consumer wearables. It Professional, 20(4), pp.46-56, 2017.

[8] Y. Yang, X. Liu, R. H. Deng, Y. Li. Lightweight sharable and traceable secure mobile health system. IEEE Transactions on Dependable and Secure Computing, 17(1), pp.112-126, 2020.

[9] U. Uludag, S. Pankanti, S. Prabhakar, A. K. Jain. Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 92(6), pp.948-960, 2004.

[10] G. Zheng, R. Shankaran, W. Yang, C. Valli, L. Qiao, M. Orgun, and S. Mukhopadhyay. A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices. IEEE Sensors Journal, 19(3), pp.1186-1198, 2018.

[11] Z. Zhang, H. Wang, A. V. Vasilakos, H. Fang. ECG-cryptography and authentication in body area networks. IEEE Transactions on Information Technology in Biomedicine. 16(6), pp.1070-8, 2012.

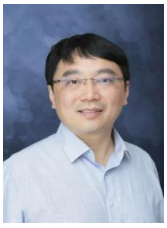
[12] K. K. Venkatasubramanian, A. Banerjee, S. K. S. Gupta. PSKA: Usable and secure key agreement scheme for body area networks. IEEE Transactions on Information Technology in Biomedicine, 14(1), pp.60-68, 2010.
[13] S. Pirbhulal, H. Zhang, W. Wu, S. C. Mukhopadhyay, Y. Zhang. Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. IEEE Transactions on Biomedical Engineering, 65(12), pp.2751-2759, 2018.
[14] G. Zhang, C. Poon, Y. 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, 16(1), pp.176-182, 2012.
[15] F. Miao, S. Bao, Y. Li. Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security. IET Information Security, 7(2), pp.87-96, 2013.
[16] F. Sun, C. Mao, X. Fan, Y. Li. Accelerometer-based speed-adaptive gait authentication method for wearable IoT devices. IEEE IoT Journal, 6(1), pp. 820-830, 2018.
[17] Y. Zhang, G. Pan, K. Jia, M. Lu, Y. Wang, Z. Wu. Accelerometer-based gait recognition by sparse representation of signature points with clusters. IEEE Transactions on Cybernetics, 45(9), pp.1864-1875, 2015.
[18] M. Abuhamad, A. Abusnaina, D. Nyang, D. Mohaisen. Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Survey. arXiv preprint arXiv:2001.08578. 2020 Jan 23.
[19] H. Zhao, Z. Wang, S. Qiu, J. Wang, F. Xu, Z. Wang Y. Shen. Adaptive gait detection based on foot-mounted inertial sensors and multi-sensor fusion. Information Fusion, 52, pp.157-166, 2019.
[20] W. Xu, G. Lan, Q. Lin, S. Khalifa, M. Hassan, N. Bergmann, W. Hu. KEH-gait: Using kinetic energy harvesting for gait-based user authentication systems. IEEE Transactions on Mobile Computing, 18(1), pp.139-152, 2019.
[21] F. Sun, W. Zang, R. Gravina, G. Fortino, Y. Li. Gait-based identification for elderly users in wearable healthcare systems. Information Fusion, 53, pp.134-144, 2020.
[22] M. Wazid, A. K. Das, V. Bhat, A. V Vasilakos. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. Journal of Network and Computer Applications, 150(2020), pp.102496, 2020.
[23] M. Wazid, A. K. Das, N. Kumar, M. Conti, A. V. Vasilakos. A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE journal of biomedical and health informatics. 22(4), pp.1299-309, 2017.
[24] M. Wazid, A. K. Das, A. V. Vasilakos. Authenticated key management protocol for cloud-assisted body area sensor networks. Journal of Network and Computer Applications. 123, pp.112-26, 2018.
[25] D. Bichler, G. Stromberg, M. Huemer, M. Löw. Key generation based on acceleration data of shaking processes. In International Conference on Ubiquitous Computing, pp. 304-317. Springer, Berlin, Heidelberg, 2007.
[26] G. Revadigar, C. Javali, W. Xu, A. V. Vasilakos, W. Hu, S. Jha. Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. IEEE Transactions on Information Forensics and Security, 12(10), pp.2467-2482, 2017.
[27] R. Mayrhofer and H. Gellersen. Shake well before use: Intuitive and secure pairing of mobile devices. IEEE Transactions on Mobile Computing, 8(6), pp.792-806, 2009.
[28] Y. Sun and B. Lo. Random number generation using inertial measurement unit signals for on-body IoT devices. IET Conference on Living in the Internet of Things: Cybersecurity of the IoT, pp.28-9, 2018.
[29] Y. Sun, W. Charence, G. Z. Yang, B. Lo. Secure key generation using gait features for body sensor networks. In 2017 IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN), pp. 206-210, 2017.
[30] W. Xu, G. Revadigar, C. Luo, N. Bergmann, W. Hu. Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In 2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), pp. 1-12, 2016.
[31] 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 Transactions on Sensor Networks. 13(1), pp.1-6, 2017.
[32] A. Bruesch, L. Nguyen, D. Schürmann, S. Sigg, L. C. Wolf. Security properties of gait for mobile device pairing. IEEE Transactions on Mobile Computing, 19(3), pp.697-710, 2020.
[33] Y Wu, Q Lin, H Jia, M Hassan, W Hu. Auto-Key: Using Autoencoder to Speed Up Gait-based Key Generation in Body Area Networks. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 4(1), pp.1-23, 2020.
[34] A. Ometov, P. Masek, L. Malina, R. Florea, J. Hosek, S. Andreev. Feasibility characterization of cryptographic primitives for constrained (wearable) IoT devices. IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), pp.1-6. 2016.
[35] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and Communications Security, pp. 28-36, 1999.
[36] A. Juels and M. Sudan. A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2), pp.237-257, 2006..
[37] C. Li, J. Hu, J. Pieprzyk. A new biocryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion. IEEE Transactions on Information Forensics and Security, 10(6), pp.1193-1206, 2015.
[38] A. Rukhin. A statistical test suite for random and pseudorandom number generators for cryptographic applications (SP 800-22 Rev. 1a). Tech. Rep. Gaithersburg, MD, U.S.A.: National Institute of Standards and Technology, 2010.
[39] R. G. Brown. Dieharder: A Random Number Test Suite. 2004.
[40] M. A. Hoque, M. Siekkinen, K. N. Khan, Y. Xiao, S. Tarkoma. Modeling, profiling, and debugging the energy consumption of mobile devices. ACM Computing Surveys (CSUR), 48(3), pp1-40, 2015.
[41] Shimmer 3: http://www.shimmersensing.com/products/
[42] T. Sztyler, H. Stuckenschmidt. On-body localization of wearable devices: An investigation of position-aware activity recognition. IEEE International Conference on Pervasive Computing and Communications (PerCom), pp.1-9, 2016.
[43] https://sensor.informatik.uni-mannheim.de/

Fangmin Sun (M'20) received her B.S. degree in the Measurement and Control Technology and Instruments from Xian Electronic Technology University in 2010 and her doctoral degree at the State Key Laboratory of Transducer Technology Institute of Electronics, Chinese Academy of Sciences in 2015. She is currently an associate professor at Shenzhen Institute of Advanced Technology (SIAT). Her research interests include multi sensor information fusion, activity recognition and gait analysis, wearable perception and computing.

Weilin Zang received B.S. and M.S. degrees in communication engineering from Guilin University of Electronic Technology, Guilin, China, in 2006 and 2009 respectively and his doctor degree in Research Center for Biomedical information Technology in Shenzhen Institutes of advanced Technology (SIAT), Chinese Academy of Sciences in 2018. His main research interests include wireless body area networks and resource allocation in wireless communications.

Haohua Huang received his B.S degree in the Measurement and Control Technology and Instruments from Guilin University of Electronic Technology, Guilin, China, in 2017. He is currently a M.S. candidate in Computer Technology from University of Chinese Academy of Sciences. His research interests include machine learning and wearable computing.

Ildar Farkhatdinov is a lecturer (assistant professor) in robotics at the School of Electronic Engineering and Computer Science, Queen Mary University of London. Before joining QMUL, he was a research associate at Imperial College of London. He has received the B.Sc. in automation and control from the Moscow State University of Technology STANKIN, Moscow, Russia, the M.Sc. in mechanical engineering from the KoreaTech University South Korea, and the Ph.D. in robotics from the Sorbonne University, France. His research interests are assistive robotics and physical human-robot interaction.



Ye Li (M'09-SM'19) is a professor in Shenzhen Institute of Advanced Technology (SIAT), Chinese Academy of Sciences. He received the B.S. and M.S. degrees in electrical engineering from University of Electronic Science and Technology of China, Chengdu, China, in 1999 and 2002, respectively. In 2006, he received the Ph. D. degree in electrical engineering from Arizona State University, AZ, US. In 2007, Dr. Li worked in Cadence Design Systems, Inc., San Jose, CA, the U.S. Since 2008 he is the Director of the Research Center for Biomedical Information Technology in SIAT. His research interests include body sensor networks, wearable computing, and health data mining.