Imperial College London,
Department of Computing

# Securing Body Sensor Networks and Pervasive Healthcare Systems

Yingnan Sun

Supervised by Dr. Benny Lo

Submitted in part fulfilment of the requirements for the degree of
Doctor of Philosophy in Computing of Imperial College London
and the Diploma of Imperial College London, July 2019

I hereby declare that:

- this thesis is the record of original work, that has been carried out by me,
- all other referenced work is appropriately referenced,
- this thesis has not been submitted in any previous application for a higher degree,
- I truthfully documented all methods, data and operational procedures,
- I have not manipulated any data,
- I have identified all persons who have substantially supported me in my work in the acknowledgements.

I understand that the above written work may be tested electronically for plagiarism.

# Abstract

With increasing popularity of wearable and Body Sensor Network (BSN) technologies, there is a growing concern on the security and data protection of such low-power ubiquitous devices. With very limited computational power, BSN sensors often cannot provide the necessary data protection on the sensitive personal health information they collect and process. Biometrics, such as face and fingerprint, have been widely used for securing computer systems and mobile devices, however, such methods have issues. For instance, the capturing of the biometric is quite intrusive and previously collected data or compromised data can be reused by attackers.

The aim of the thesis is to tackle the challenges of collecting biometrics pervasively with miniaturised BSN nodes, and ensuring the data freshness of a BSN security system, by investigating innovative ways of using behavioural biometrics. It is hypothesised that behavioural biometrics, such as Electroencephalographic (EEG) and walking patterns (gait) can be used for unobtrusive encryption of BSN wireless communication channels and secure the BSN-based healthcare systems.

A person's brain wave signal, also known as EEG signal, is nearly impossible to mimic and can be easily collected with EEG headsets without user intervention; therefore, it is suitable to be used as biometrics for securing BSNs. Due to the complex nature of EEG signals, the state-of-the-art manually feature extraction methods often cannot utilise the full potential of the underlying features neural activities in the EEG signals. Therefore, to explore the potential of using EEG for securing BSN-based healthcare systems and to improve the performance of the current EEG-based authentication systems, the use of deep learning approaches is investigated.

Although EEG-based security systems perform exceptionally well, EEG headsets are still very expensive and cumbersome in size. To reduce the costs of the security systems, the walking pattern of a person, called gait, is investigated as a biometric for securing BSNs. Gait is one of the most promising behavioural biometric traits for securing wireless communications between BSN sensors and coordinators. This thesis presents the work in resolving issues in using gait for BSNs, especially the challenge of using less correlated gait signals collected from sensors located at different positions for the common entropy sources of Biometric Cryptosystems (BCS). In this context, a novel light-weight symmetric key generation scheme based on the timing information of gait and fuzzy commitment scheme is proposed. The effect of gait-based soft biometrics is also investigated, namely age and gender. Through analysing a large gait database with inertial sensor data, and the results show that age and gender information can be accurately estimated using only gait signals. The recognised age and gender information can be used to improve current gait-based security systems.

Next, with the advances of Artificial Intelligence (AI) for the healthcare applications, many wearable devices and BSN sensors are now able to perform on-node inferencing. The challenge of less correlation between gait signals at different body positions can be tackled by machine learning techniques. An Artificial Neural Network (ANN) framework has been developed for estimating gait signals on the shin and thigh positions from gait signals collected on the ankles. The work shows the possibility of using ANNs to project gait signals captured from one body position to onto another position. Therefore, based on this finding, the ANN framework is proposed to improve the previously proposed gait-based key generation scheme, where gait signals collected on the head, upperarm, wrist, waist, thigh, and shin positions are all projected onto the chest position so that the transformed signals are highly correlated and more similar secret keys can be extracted by devices at those positions.

From our experiments on using biometrics for securing BSNs, it is also found that the freshness of gait signals can be used to generate random numbers by removing the low frequency periodical components in the signals. The last part of the thesis investigate the use of gait signals as the entropy source for Random Number Generators (RNG), and a novel random number generation method is proposed for securing on-body IoT devices based on temporal signal variations of the outputs of the Inertial Measurement Units (IMU) worn by the users while walking. The proposed method has been tested with two inertial gait datasets and passed four well-known randomness test suites, namely NIST-STS, ENT, Dieharder, and RaBiGeTe.

# Acknowledgements

I would like to express my very great appreciation to my supervisor Dr. Benny Lo, for his guidance and support whenever I ran into troubles with my research during the past three years. His willingness to give his time so generously has been very much appreciated. Advice and comments given by Prof. Guang Zhong Yang has been a great help in the writing of chapters related to gait-based security. Completing this thesis would have been much more difficult without the support and friendship provided by the other members of the Hamlyn Centre, and I must express my deepest appreciation to them for their help. I would particularly like to thank my colleague Frank Lo for his contribution and comments on the writing of Chapter 3, I am in debt to him. Last but not least, I am profoundly grateful to my parents and my wife for providing me with constant support and encouragement throughout my years of study. This accomplishment would not have been possible without them.

To my family.

# Contents

# List of Tables

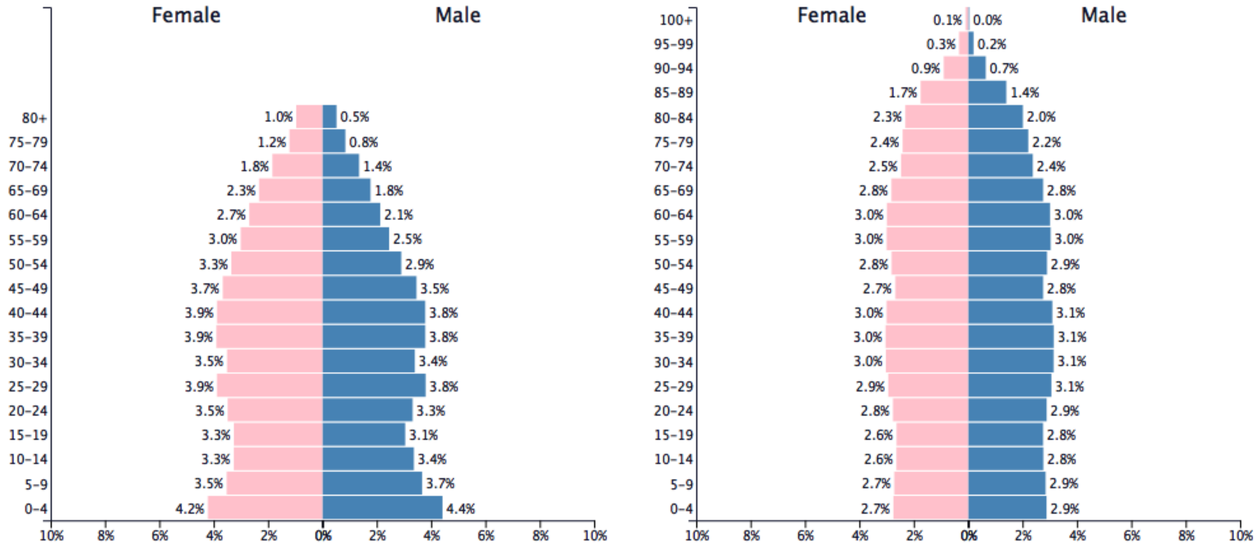
# List of Figures

# Chapter 1

# Introduction

Due to the demographic shift, elderly population will account more than a third of the overall population in the UK by 2050, as shown in Fig. 1.1. Given the rising cost of care and the severely under resource of the healthcare services, the current health care systems will no longer be able to provide quality care to the older people who require living assistance or medical attention. Technological solutions are being sought to help alleviating the growing healthcare crisis, and one target is an autonomic health monitoring system. Such system would require pervasive and autonomous low-level self-management to reduce labour costs and increase scalability to meet the potential demand of millions of users. Recent wireless technology advancements have enabled the introduction of lightweight, low energy, miniaturised sensor nodes to be worn by users or placed in the surrounding of users to form a network system known as the Body Sensor Networks (BSNs). BSN can be applied for a wide range of applications including sports, entertainment, and most importantly, healthcare.

BSN can play a critical role in shifting current healthcare systems to more scalable solutions by providing low cost and autonomic wireless networks with sensors that continuously monitor the health of the elderly population and patients who are suffering from Parkinson's disease, cardiovascular diseases, and other chronic diseases. These patients may have experienced early-stage symptoms but often not realise the severity of their diseases. With continuous monitoring of patients by wearable sensors in the BSN-based healthcare systems, early signs of deterioration can be detected and early intervention can be introduced. However, this can only be achieved when the BSN systems can be



(a) UK age pyramid in 1950

(b) UK age pyramid in 2050

Figure 1.1: UK age pyramid representing the population of aged people[1]

self-managed with only high-level supervision from network operators. With each patient wearing multiple BSN devices, the scale of the sensing network could be massive and it will become humanly impossible to manage and administrate. More importantly, any data collected from patients must be fully protected throughout its life cycle, which includes the wireless transmissions between the BSN sensors and their coordinators.

Applying proper security measures to the current BSN-based healthcare systems can prevent attackers from eavesdropping vital personal information and intervening in therapeutic treatment/care plans by manipulating patients' long-term physiological data. Traditionally, encryption keys for wireless communications among BSN sensors and coordinators are pre-distributed, which have been proven to be unsafe. A more promising solution is to distribute new keys, i.e. session keys, when a new communication link is established. The system would use a trustworthy third-party for generating and managing keys using asymmetric cryptography, but it is too computational intense for low power miniaturised BSN sensors.

Biometrics is another promising approach to secure BSN networks, and classic biometrics such as face and fingerprint have been widely used for securing mobile devices. However, there are still many concerns when applying to BSNs, for instance, the intrusiveness of the data capturing methods and

[1] "Population Pyramids of the World from 1950 to 2100" by PopulationPyramid.net, available from https://www.populationpyramid.net/united-kingdom/

the prevention of the previously collected data or compromised data being reused by attackers.

This thesis aims to tackle the technical challenges in protecting BSN-based healthcare systems, such as to collect biometric traits pervasively, and to ensure the security systems are aware of data freshness, by investigating innovative ways of using behavioural biometrics. To this direction, it is hypothesised that behavioural biometrics, especially Electroencephalographic (EEG) and walking patterns (gait) can be used for unobtrusive encryption of BSN wireless communication channels and secure the BSN-based healthcare systems.

## 1.1 Motivation and Objectives

Biometric traits such as face and fingerprint are difficult to capture using BSN sensors, therefore, EEG and gait biometrics are investigated in this thesis, because both of them can be collected by BSN sensors, such as EEG headsets and Inertial Measurement Units (IMUs), without user interventions. Although much research has been carried out on EEG and gait biometrics, there are still many issues and challenges hindering their adoption as main security measures in practice. This thesis is focused on introducing new solutions to EEG and gait biometrics research to address the challenges.

### 1.1.1 Motivation for EEG biometrics

A wearable EEG headset can capture the neural activities or signals in the brain, which can be used as biometric measurements for user identification applications. EEG biometrics have several advantages over other traditional biometrics, such as fingerprints. First, EEG signals depend largely on the person's brain structure and association with the person's current memory, mood, stress and mental state; therefore, a person's EEG signal is unique, constantly changing, and nearly impossible to mimic. Secondly, to capture a user's EEG signals, an EEG capturing device has to be attached or worn on the user's head and the user also has to be conscious, which greatly reduce the chances of malicious attacks. Thirdly, EEG signals can provide a wider range of features from both time and frequency domains, in the meantime, the signals captured in different time intervals will be of different patterns. Such high level of freshness provided by the EEG signal indicates its potentials in the user identification applications.

Although with the aforementioned advantages over other biometrics, EEG has not been widely used in security systems due to its cumbersome settings and high noise sensitivity. However, the new generation of EEG headsets are smaller and more accessible with less EEG electrodes than clinical EEG machines. Targeting for the new generation of EEG headsets, this thesis investigates the application of deep learning methods to minimise the number of EEG electrodes needed for user identification while maintaining the performance of the system.

### 1.1.2 Motivation for gait biometrics

Although EEG-based security systems perform exceptionally well, EEG headsets are still very expensive and cumbersome in size. Gait biometrics is studied in this thesis as it can be easily captured by IMUs, which are ubiquitous and low cost, and can be easily embedded into any BSN sensors. Gait, similar to other widely adopted biometric traits, is unique, fresh, and difficult to mimic, which makes it very suitable for biometric security applications. There are mainly two ways of capturing a person's gait: either using a camera, or using IMUs attached to the person to sense the movements. The former method has been greatly exploited and used in real world security systems, whereas the later method is still being researched. Although camera-based user authentication systems are widely adopted, it is not suitable for BSN-based healthcare systems. The reasons are twofold: first, the system will not be able to capture the gait of the person, if the persons are not in sight of the camera or occluded by an object or another person; secondly, the initial and maintenance costs of installing cameras in the building is too high. On the other hand, IMU-based gait biometrics can provide more cost effective security measures to the healthcare systems, and it could also provide better scalability and ubiquitous than camera based gait biometrics.

However, many challenges are still needed to be addressed for IMU-based gait biometrics, and one of the main challenges for using gait signals to generate secret binary keys for BSN applications is that the IMU signals collected from sensors located at different positions are less correlated. This is due to motions from different segments of the body, such as arm swing and leg swing. In this thesis, it is hypothesised that gait signal differences introduced by the motion of body segments can be reduced or eliminated by machine learning and deep learning techniques.

### 1.1.3 Key research challenges and objectives

In this thesis, the use of gait and EEG biometrics is researched for securing wireless communications among BSN sensors and coordinators, as well as securing BSN-based healthcare systems. The existing healthcare systems often have insufficient security measures and are vulnerable for network attackers. To develop biometric-based security schemes for BSN and healthcare systems, many challenges still need to be tackled. In this thesis, some key issues are addressed, and the key research challenges and objectives are summarised as follows:

- To identify suitable feature extraction techniques for EEG and gait biometrics;
- To develop methods to increase signal correlations between gait signals collected from BSN sensors worn at different body positions;
- To develop methods for generating real-time random binary sequences as secret keys for symmetric cryptographic systems;
- To investigate stochastic properties of the gait signals by removing low frequency periodic components of the signals for generating random numbers.

## 1.2 Thesis structure

The thesis starts with an introduction of the challenges that current healthcare systems are facing, and the motivation for implementing EEG and gait biometrics for the healthcare systems. In chapter 2, a review on BSN and healthcare systems is first presented. The review provides an overview of the key challenges of implementing EEG and gait biometrics in the power and resource constrained wireless network environments. A detailed literature review on BSN security is then presented, which outlines security requirements, threats, the state-of-the-art security schemes, and followed by a discussion on the open issues and challenges. Then, a detailed review on the gait analysis is presented. By investigating the state-of-the-art methodologies applied in the gait analysis, a new perspective on how to tackle the challenges of applying gait biometrics in BSN security is presented. The following chapters describe the novel methodologies designed and developed to tackle the aforementioned issues and challenges.

To secure BSN-based healthcare systems, a novel EEG-based user identification system is proposed in Chapter 3, where 1D-convolutional Long Short-Term Memory (LSTM) approach is applied and presented in detail. The system extracts the spatiotemporal features resided in the EEG signals which outperforms the state-of-the-art deep learning approaches, and it can be used to reduce the number of EEG channels required by the systems, subsequently reducing the costs of the systems and improve its usability.

Chapter 4 presents a novel light-weight symmetric key generation scheme using gait event timing as the common entropy source for cryptography. Moreover, the influence of gender and age for gait biometrics is also analysed in this chapter. By performing gender and age recognition using only inertial sensors, a new perspective on applying soft biometrics in the respect of securing miniaturised BSN sensors is provided.

Following the concept on soft biometrics, Chapter 5 describes a new approach developed to improve the symmetric key generation scheme by applying an Artificial Neural Network technique to increase the correlations among gait signals collected from BSN sensors located at different body positions. The chapter consists of two parts: the first part presents a novel lower limb motion estimation method using two inertial sensors attached to the ankles; and the second part extends the proposed method to generate higher correlations among gait signals collected from different positions, which is then used as the common entropy source for cryptography.

Chapter 6 introduces the research on using gait signals for generating random numbers. In this respect, a novel random number generation method is proposed in this chapter for securing on-body BSN devices based on temporal signal variations of gait signals. The method is rigorously tested and passed using four widely adopted randomness test suites.

In the last chapter of the thesis, a summary of thesis achievements is presented, follow by the discussions on future directions in the research of EEG and gait biometrics.

## 1.3 Contributions

The thesis contributes to the research of biometric security, specifically on the EEG and gait biometrics for securing body sensor networks and pervasive healthcare systems. The original technical contributions of this thesis include:

- A novel 1D-convolutional LSTM approach for EEG-based user identification for securing BSN-based healthcare systems;
- A novel light-weight symmetric key generation scheme based on gait event timing (temporal features) from inertial signals for securing wireless communications among BSN sensors and coordinators;
- A deep learning approach designed for gender and age recognition using a single inertial sensor attached to the lower back of the subjects;
- An Artificial Neural Network (ANN) framework for lower limb motion signal estimation, which can be used for sensor reduction in real-time gait analysis as well as increasing correlations of gait signals from different body positions;
- An improved key generation scheme based on ANN-based gait signal estimation and fuzzy key exchange;
- A novel random number generation method using gait signals and stochastic signal energy variation for on-body Internet of Things (IoT) devices.

The work presented in this thesis has resulted in a number of publications in peer reviewed journals and international conference proceedings. The publications directly related to the work presented in this thesis are as follows:

1. Y. Sun, F. Lo and B. Lo, “EEG-based Identification with 1D-Convolutional Long Short-Term Memory Neural Networks,” *Expert Systems with Applications*, vol. 125, pp. 259-267, Elsevier, July 2019

2. Y. Sun, F. Lo and B. Lo, “Machine Learning Approaches on Gait Biometrics for Securing BSN-based Healthcare Systems,” *The IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*, Special Session, May 2019

3. Y. Sun, F. Lo and B. Lo, “A Deep Learning Approach on Gender and Age Recognition using a Single Inertial Sensor,” *IEEE 16th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, May 2019

4. Y. Sun and B. Lo, “An Artificial Neural Network Framework for Gait Based Biometrics.” *IEEE journal of biomedical and health informatics*, vol. 32, pp. 987-998, May 2019

5. Y. Sun and B. Lo, “Random Number Generation Using Inertial Measurement Unit Signals for On-Body IoT Devices,” *Living in the Internet of Things: Cybersecurity of the IoT-2018*, IET, March 2018

6. Y. Sun, G.-Z. Yang, and B. Lo, “An Artificial Neural Network Framework for Lower Limb Motion Signal Estimation with Foot-Mounted Inertial Sensors,” *IEEE 15th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 132-135, March 2018

7. Y. Sun, C. Wong, G. Z. Yang, and B. Lo, “Secure key generation using gait features for Body Sensor Networks,” *IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 206-210, March 2017

Other relevant publications from the author, which may be of interest to readers but not directly related to the works described in this thesis are listed as follows:

1. F. Lo, J. Qiu, Y. Sun and B. Lo, “A Novel Vision-based Approach for Dietary Assessment using Deep Learning View Synthesis,” *IEEE 16th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, May 2019

2. R. Rother, Y. Sun and B. Lo, "Internet of Things based Pervasive Sensing of Psychological Anxiety via Wearable Devices under Naturalistic Settings," *Living in the Internet of Things: Realising the socioeconomic benefits of an interconnected world*, IET, May 2019

3. J. Howes, Z. Wang, J. Zhan, H. Zhang, Y. Sun, and B. Lo, "Pervasive Sensing of Distress using Wearable Devices for People with Dementia," *The IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*, May 2019

4. F. Lo, Y. Sun and B. Lo, "Depth Estimation based on a Single Close-up Image with Volumetric Annotations in the Wild: A Pilot Study," *IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, July 2019

5. J. Qiu, F. Lo, Y. Sun and B. Lo, "Mining Discriminative Food Regions for Accurate Food Recognition," *British Machine Vision Conference (BMVC)*, September 2019

6. F. Lo, Y. Sun, J. Qiu, and B. Lo. "Food Volume Estimation Based on Deep Learning View Synthesis from a Single Depth Map," *Nutrients*, vol.10, no.12, December 2018

# Chapter 2

# Literature Survey

In healthcare, significant improvements in efficiency and quality of care are expected from the diverse range of developments in Internet of Things (IoT). In particular, smart wearable and implantable sensors has attracted much interest in recent years due to the advances in microelectronics, materials, and biosensor design. The rapid development of IoT, however, has meant that the security and safety of these systems often have received insufficient attention. The consequences of inadequate security in healthcare system can be, for instance, compromised patients' privacy due to eavesdropping, and disruption of normal operations of wearable or implantable devices due to active attacks. In 2015, a study by HP Fortify found the 10 most popular smartwatches (at the time) all had security vulnerabilities from insufficient authentication or authorisation, lack of data transmission encryption, insecure interfaces, insecure software/firmware, and privacy concerns (Rawlinson, 2015). Authentication, for example, is the process of confirming identity. All systems should only be accessed by authorised and authenticated users or devices. Insufficient authentication protection could allow attackers to enter the system and gain access to private and personal data of the users.

User/device authentication is important to a system, as it can ensure that the data is correctly attributed and information in the systems is only accessible to the authorised entities. In the context of healthcare system, the ability to authenticate the user of a wearable sensor could be used to establish the integrity of the data, such as activity information for obese patients, and authentication would also be used to safeguard patients' privacy by ensuring that information, such as the patients' electronic medical records (Evans, 1999), is only accessible to the authorised and authenticated users, such as the patients' general practitioners. Network and system security is a well-established field, and extensive security protection schemes and methods are available to protect computer systems and networks. For example, public-key cryptosystems such as Rivest-Shamir-Adleman (RSA) (Kravitz, 1993) and Digital Signature Algorithm (DSA) (Barrett, 1986) which are commonly used in securing computer networks.

However, many of such schemes and methods cannot be applied for IoT devices due to the limitation of low power and low computational capability (Jonsson and Tornkvist, 2017; WISeKey, 2017). Compare to typical IoT devices, wearable and implantable medical and healthcare devices are often designed with very low computational power and battery capacities, as they have to be miniaturised in size. Medical and healthcare IoT devices have to store and process personalised health data, and some devices even have actuation functions to support the users' health (ex. insulin pump). Therefore, the level of security required for IoT health devices is expected to be much higher than typical IoT and computing devices (Turner, 2018). Yet, security and threats are often overlooked in the design of medical devices and healthcare systems (Davis, 2019; Dolmatov, 2019).

With the rapid development of IoT technologies, more and more medical and healthcare devices are internet connected, and most devices are designed to transmit and store the data in the cloud waiting to be further processed and analysed, such as Health-CPS (Zhang, Qiu, et al., 2017) and UbeHealth (Muhammed et al., 2018). This advancement enables the medical carer to provide faster and more accurate responses to the patients that are being monitored by the medical and healthcare devices. However, it also introduces risks of users' data stored in the cloud servers being abused or stolen (Scammell, 2019). The privacy of the users' data, especially users' personal data must be well protected. Yet, many examples of security breaches of cloud servers from large enterprises, such as Facebook (Hutchinson, 2018) and Yahoo (Garun, 2017), raise the question: can users' sensitive health data really be protected? In fact, more and more hackers are targeting medical servers and eHealth systems, because personal health data is very valuable in the illegal/black markets (Yao, 2017). Therefore, medical servers require even stronger security measures, which inevitably increases the costs of creating, running, and maintaining these services.

In addition to developing countermeasures to attacks, post-attack measures also need to be well considered. Financial information, such as credit card security codes, can be made invalid and useless quickly (Fazzini, 2019), but personal health data can reveal a person's current health conditions (Brooks, 2019). When such data is stolen in a security breach, the retrieval and elimination of the stolen data is critical and must be accomplished. To protect patients' data, strong regulations and severe penalties must be in place from governments and healthcare organisations. The Information Commissioner's Office (ICO) could only fine a company which is responsible for a data breach up to 500,000 pounds previously; however, with the newly introduced General Data Protection Regulation (GDPR), ICO is now able to fine a company based on the company's profits. For example, British Airways was suspected to be fined up to 183 million pounds, due to a data breach of 500,000 users from its website and mobile app (Pratley, 2019). In addition, according to the GDPR, any incidents of data breaches in the healthcare systems must be reported promptly (ICO, 2019). It also forces healthcare providers to introduce proper security measures for their healthcare services.

## 2.1 Body Sensor Network

### 2.1.1 BSN-based Healthcare Systems

BSN-based healthcare systems often consist of 3 tiers, sensor level, personal server level, and medical server level as indicated in Fig. 2.1, such as (Kantoch, 2013; Lu, Lin, and Shen, 2012; Yeh, 2016). Medical devices and sensors are located in the sensor level, which form a local network, often referred as Body Sensor Networks. BSN can employ a star network topology, where medical devices and sensors can only communicate with the network coordinator/gateway, which is often located in the personal server level; or a mesh network topology, where medical devices and sensors can communicate with each other if required. Wireless technology standards including Bluetooth Low Energy (BLE) (Singh and Ricke, 2016), Wi-Fi (Li, Qi, et al., 2011), Wireless Body Area Network (WBAN) (Wu et al., 2017), Near-Field Communication (NFC) (Masuda, Noda, and Shinoda, 2018), and Radio-Frequency IDentification (RFID) (Wang, Gu, et al., 2016), are often employed for wireless communications in the sensor and personal server levels. BLE, Wi-Fi and WBAN support star and mesh network topologies, whereas NFC and RFID can only support ultra-low energy, device-to-device close proximity direct communications, which are often used by implantable devices.

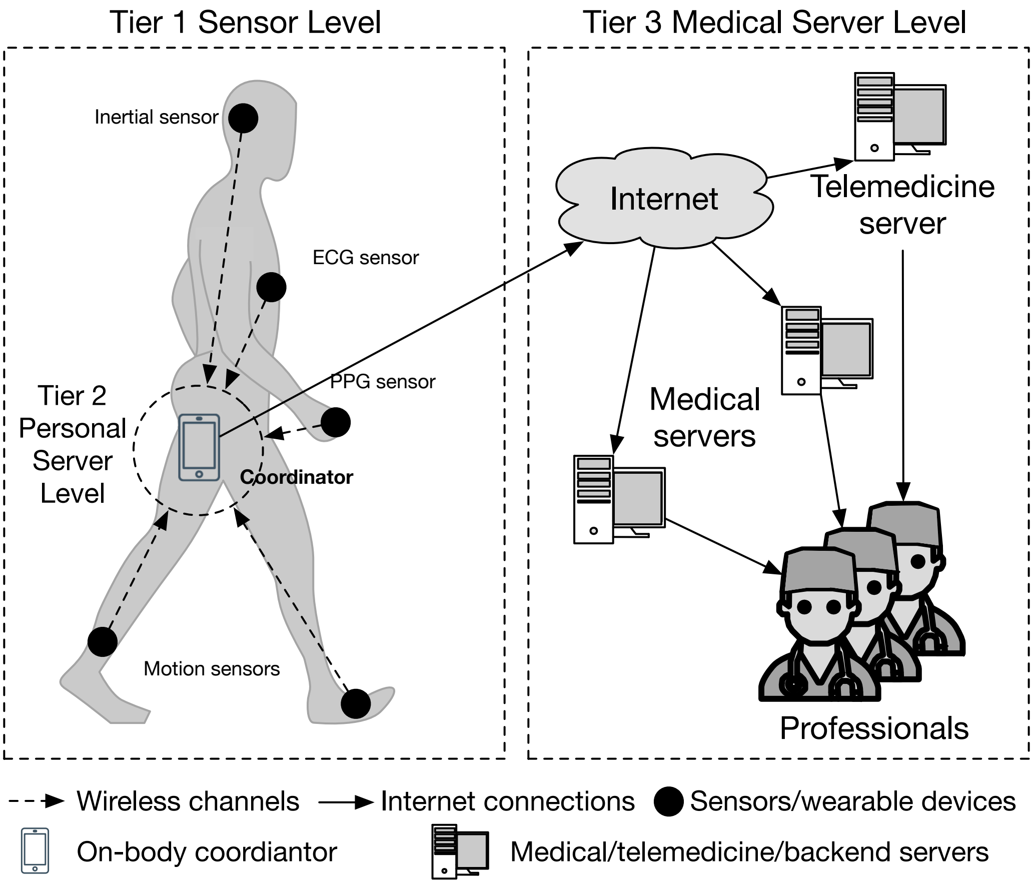


Figure 2.1: Illustration of a 3-tier BSN/IoT-based healthcare system (Sun and Lo, 2018b)

Physiological data collected by the medical devices will be sent to personal servers, which can be on-body devices, such as smart phones and tablets, or off-body devices, such as Wi-Fi routers and BLE gateways. The purposes of personal servers are to process and store patients' data locally before sending to the centralised servers in the medical server level. A personal server is required to be able to operate normally when the network connection to the medical servers is lost. The aggregated patients' data will be forwarded to the databases located in the medical server level. Medical personnel, such as doctors, are able to access patients' data remotely, providing prompt advice to the patients. Algorithms and computer programs for early diagnoses and rehabilitation progress assessments can also be run on the medical servers with patients' consents. Many BSN/IoT-based healthcare systems have been proposed for continuous patient monitoring in the last decade, but many of them do not adopt any security and privacy measures in their designs or left out as future work, such as Code-

Blue (Malan et al., 2004), UbiMon (Ng, Lo, et al., 2004), MobiCare (Chakravorty, 2006), SleepSense (Zhuang et al., 2015) and BiGRA (Vu et al., 2018). These work have focused more on other technical challenges such as power consumption and usability, rather than the security of the systems and the privacy of patients' data. Recently proposed BSN/IoT-based healthcare systems, such as BSN-Care (Gope and Hwang, 2016) and (Yeh, 2016), have adopted encryption and authentication schemes into their designs.

### 2.1.2 Network Design Challenges

A protocol is a set of rules that governs the exchange or transmission of data between devices (OED, 2019). A routing protocol is inherited from traditional networks, where it specifies how network routers exchange data with one another, disseminating information that enables them to select routes between any two nodes in the same network or in different networks. Routing protocols in wireless networks are more complex than those used in wired networks in many respects, including network topology, power conservation, and channel effectiveness. Thus, transferring data between nodes is not the only functionality required from routing protocols in wireless networks.

#### 2.1.2.1 Postural Body Movements

On-body sensors are often moving as a group, as the patients under diagnosis or users under monitoring are often not stationary, resulting in frequent changes in network topology and components (Shin and Joe, 2015). Routing protocols in BSNs should be adaptive to both repetitive and unpredictable changes in the quality of communication links between sensor nodes (Zheng, Zheng, et al., 2018). Link quality varies as a function of time against postural body movements (Maskooki et al., 2011), which can be utilised in routing protocols to conserve energy. For example, a transmission power control scheme based on gait cycle for BSNs has been proposed in (Zang and Li, 2017), where transmission time is optimised by matching link quality changes due to walking. On the other hand, there are also unpredictable changes of link quality due to signal blockage by clothes or bags that intensify channel attenuation.

#### 2.1.2.2 Temperature Rise

Antenna radiation absorption and power consumption of node circuitry are the two sources than cause temperature rise in sensor nodes (Tang, Tummala, et al., 2005a). Radio energy can also be absorbed by the tissues which could heat up the tissues, attenuate the signals, and cause skin or tissue burns (Tang, Tummala, et al., 2005b). Therefore, transmission and computing power in sensor nodes should be considered in the design of routing protocols, and extra attention should be paid for designing protocols for implant sensor nodes, as excessive heat can cause discomfort and damage nearby tissues and organs.

#### 2.1.2.3 Energy Efficiency

Routing protocols in BSNs should be designed to optimise the energy efficiency for both local energy consumption on sensor nodes and overall network lifetime. Energy efficiency is a crucial element of BSNs, as it determines the size of the devices, the lifetime of the system, and the usability of the devices. For instance, surgeries will be required for implant sensor nodes to replace batteries, and such surgeries are risky and very expensive. Typical implantable devices, such as pacemakers, should have the battery lifetime of at least 10 to 15 years to enable the user to live a normal life (Uslan et al., 2012). For wearable sensor nodes, frequently charging or replacing batteries hinders the usability of the devices.

#### 2.1.2.4 Transmission Range

Short transmission range along with the postural body movements could lead to the problems of disconnection and re-partitioning amongst sensor nodes in BSNs (Quwaider and Biswas, 2009). The number of sensor nodes on a patient or a user should be minimised to reduce discomfort, which results in fewer routes to neighbour sensor nodes. Therefore, if the connecting sensor node is out of range, packets will have to be routed through an alternative path resulting in higher energy consumption and longer time for the packets to reach the destination. In BSNs, if the alternative path includes one or more implantable devices, the routing protocol must be able to decide whether to take this alternative path based on the importance of the contents in the packets.

#### 2.1.2.5 Heterogeneous Environment

In most BSN applications, different types of sensor nodes from a variety of medical equipment vendors are required to measure different physiological signals of patients or users. Therefore, routing protocols have to be designed to tackle the challenges of heterogeneous environments in many BSN applications. To solve this problem, many BSN platforms and frameworks have been proposed for medical devices from different vendors to work together, such as DexterNet (Kuryloski et al., 2009) and SPINE (Gravina et al., 2010).

#### 2.1.2.6 Quality of Service

Real time life-critical BSN applications, such as Electrocardiogram (ECG) sensing, are both data loss sensitive and time critical, and the Quality of Service (QoS) requirements of such applications must be met (Liang and Balasingham, 2007; Zang and Li, 2017). However, implant sensor nodes have limited memory and computational capability, which means routing protocols have to consider QoS measures such as retransmission and error correction strategies without inducing additional computational load on the sensor nodes.

## 2.2 Security for Body Sensor Network

### 2.2.1 Security Requirements

Security requirements for the IoT-based healthcare systems are similar to typical IoT-based infrastructures, therefore, security requirements, including the Confidentiality-Integrity-Availability (CIA) principle (Samonas and Coss, 2014), for wireless communications and information security must be met. IoT-based healthcare systems have many additional security requirements, such as device localisation (Huang, Zhou, et al., 2016) and self-healing (Lo, Panousopoulou, et al., 2014a), which can also contribute to the security of the systems. The functionalities of each tier of the IoT-based healthcare systems are different, which means each tier requires different security measures to be in place.

#### 2.2.1.1 Data Level

**Confidentiality** Storage of patient health data must comply with legal and ethical privacy regulations, such as GDPR, in which only authorised individuals can have access to those data. To prevent breaches of data, adequate measures must be adopted to ensure the confidentiality of the health data associated with individual patients. The importance of such measures cannot be overemphasised, especially as, stolen by cyber criminals, the data could be used for malicious purposes, causing the patient to suffer not from only privacy violation, but also possible financial and reputational damages (Ismail, 2018).

**Integrity** The purpose of the data integrity requirement is to ensure that the data arriving at the intended destination have not been compromised in any way during the wireless transmission (Pearlman, 2019). Attackers could gain access to and modify patient data by taking advantage of the broadcast characteristic of the wireless network, which could lead to severe implications in life-threatening cases. To guarantee that the data have not been compromised, the capacity to detect potential unauthorised distortions or manipulations is critical. Therefore, appropriate mechanisms of data integrity must be implemented in the system to prevent alteration of transferred data by network attacks such as Man-in-the-Middle (Publico, 2017), viruses and malware (Swain, 2009).

**Availability** Services and data must be accessible when they are required to the authorised users. Such services and data, provided by the medical sensor nodes, will become inaccessible if an attacker captures or compromises a sensor node. Any missing data or services could lead to life threatening incidents, such as failing to provide prompt care in the case of a heart attack. Therefore, to minimise the risk of availability loss, the healthcare applications must be in the always-on operation to ensure data availability, which is regulated by GDPR (Bienkowski, 2018).

#### 2.2.1.2 Sensor Level

The security and privacy of the sensors in the sensor level are the most challenging components in the 3-tier IoT-based healthcare system, due to the lack of computational capability and power constraint of the medical devices and sensors (Al Ameen, Liu, and Kwak, 2012). The trend in sensor level security is to put most of the computations in the personal server level instead, and the security measures are required to be light-weight and less communication overheads in the sensor level.

**Channel encryption** Wireless channel encryption is essential to the confidentiality and integrity in the Confidentiality-Integrity-Availability (CIA) principle (Samonas and Coss, 2014). Encryption ensures that the wireless transmitted data cannot be comprehended by eavesdroppers without valid decryption keys. It also prevents attackers to alter the encrypted data without being noticed by the receivers ensuring the integrity of the patients' personal data. The encryption of data can be implemented in the network layer, such as (Raza, Duquennoy, et al., 2011), an end-to-end IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) extension over Internet Protocol Security Framework (IPsec); in the transport layer, such as in (Raza, Trabalza, and Voigt, 2012), an end-to-end 6LoWPAN extension over Datagram Transport Layer Security (DTLS) for Constrained Application Protocol (CoAP); and in the application layer, including the biometric-based methods (Bao, He, et al., 2013; Schurmann et al., 2017; Xu, Revadigar, et al., 2016).

**Tamper-proof hardware** Medical and healthcare devices, especially ambient sensors, can be stolen physically, which leads to security information, such as keys, being exposed to attackers. Furthermore, the stolen devices can be reprogrammed by attackers and redeployed to the system, which enable the attacker to listen to communications in the network without being noticed (Nilges, 2015). Therefore, physical theft of medical devices is a severe security threat and must be addressed in the IoT-based healthcare systems. One of the solutions to such problems is to use tamper-proof hardware or trusted platform model (Morris, 2011). Medical devices in the systems should at least have tamper resistant integrated circuits, preventing codes loaded on the devices being read by third parties once being deployed.

**Localisation** Researchers are focusing on two types of sensor localisation, on-body sensor position and sensor's/patient's location in an indoor environment. The former sensor localisation is typically designed to identify whether the sensors are worn at the desired positions, for instance, on the wrist. Such on-body sensor position identification is of vital importance for applications such as activity recognition (Saeedi et al., 2014). The latter sensor localisation, also known as Location of Things (LoT) (Shit et al., 2018), is designed to locate the sensor and the patient wearing the sensor in a room or in a building. Some of the techniques for LoT are centroid (Chen, Huang, et al., 2008), connectivity (Liu, Wang, et al., 2005), cluster (Li and Hu, 2003), and path planning (Koutsonikolas, Das, and Hu, 2007). In addition, due to the nature of the IoT-based healthcare systems, medical devices may join and disconnect from the network very frequently. Therefore, a real-time intrusion detection measure is required, if the network allows its sensors to leave and rejoin irregularly. An example of such measure is SVELTE (Raza, Wallgren, and Voigt, 2013), a 6LoWPAN-based intrusion detection method which can be implemented on the personal server level, reporting malicious nodes to the network administrators.

**Self-healing** Self-healing, one the seven self-* properties of Autonomic Computing (Kephart and Chess, 2003) and Autonomic Sensing (Lo, Panousopoulou, et al., 2014b), is of great importance in the IoT-based healthcare systems, as medical devices shall operate normally, when the network is under attacked. To achieve self-healing, an IoT system should be able to detect and diagnose the attacks, and apply corresponding security mechanisms (Stankovic, 2014) with minimal human intervention. Self-healing methods deployed should also be light-weight, in terms of communication overheads to the network and computational complexity to the medical and healthcare devices. An example of self-healing architecture for IoT is proposed in (Almeida, Ribeiro, and Moreno, 2015), where a dendritic cells algorithm is applied in the network to detect network attacks.

**Over-the-air programming** Over-the-air (OTA) programming or updating (Hoffman, 2003) has become a popular method to update an IoT system with a large number of sensor nodes, which raises security concerns, such as malicious sensor nodes listening to updates and forging identities into the network (Califano, 2018). OTA can be part of the self-healing mechanism, updating security rules for the network instantly. To implement OTA programming properly, security measures must be made to prevent OTA updates being exploited by attackers. An example solution is one-time programs (Goldwasser, Kalai, and Rothblum, 2008), which is a computational paradigm where the program sent to the receiver can only be executed once by the targeted sensor node and then self-destructs.

**Forward and Backward Compatibility** This is also a key requirement in real-time healthcare applications where faulty medical sensors are replaced promptly with new ones. Forward compatibility is characterised by the fact that new messages cannot be read by existing medical sensors, if their transmission occurs after the sensors have left the network. Conversely, in backward compatibility, messages that have been transmitted earlier cannot be read by a sensor just joined the network (Spacey, 2016).

#### 2.2.1.3 Personal Server Level

As patients' data is often stored and aggregated in the personal server level before being forwarded to the medical servers in the IoT-based healthcare systems (Bromwich and Bromwich, 2016; Murgia, 2017), it is essential to ensure that the data is well protected while on the personal servers. Generally, two types of authentication schemes must be deployed to provide security and privacy in the personal server level, namely device/sensor authentication and user/patient authentication.

**Device authentication** A personal server (i.e. a smart phone) shall perform authentication before accepting data sent from the medical devices and sensors. A device authentication scheme should be able to establish secured/encrypted communications for data confidentiality and integrity (Crilly and Muthukkumarasamy, 2010). False information from malicious devices about patients' physical conditions could have severe negative impacts on the clinical diagnosis and care decisions, therefore, device authentication must be implemented in all BSN-based healthcare systems. Device authentication is mutual between personal servers and sensors, but the majority of the computation should be performed on the personal servers, as they often have more computational capability than the medical devices and sensors.

**User authentication** The data stored either temporarily or permanently on the personal servers should only be accessed by the patients and/or authorised medical staff such as caregivers, therefore, effective user/patient authentication schemes are required (Davis, 2018; Kogetsu, Ogishima, and Kato, 2018). Personal servers in the BSN-based healthcare systems should also support emergency access of the data, if the patients are in critical conditions, such as having a stroke or a seizure. The user authentication schemes are required to be robust and protected against attackers. A popular solution to user authentication in the personal server level is the use of biometrics, which is particularly applicable in the IoT-based healthcare systems, as most of the biometrics can be easily collected from medical and healthcare devices (Kogetsu, Ogishima, and Kato, 2018; Orme, 2019).

#### 2.2.1.4 Medical Server Level

Two of the most important requirements on the security and privacy of patients' data in the medical server level are: only authorised devices and personnel have access to the data; and the data itself must be encrypted at all time when stored in the databases (Azeez and Van der Vyver, 2018). Failure to meet either requirement could potentially lead to patients' personal health data being leaked, and severe penalty by ICO, enforced by GDPR (Pratley, 2019). With more and more paper-based medical records being replaced by Electronic Medical Record (EMR) or Electronic Health Record (EHR), security concerns with the medical servers storing EMRs and EHRs are growing (Preidt, 2018; Raposo, 2015). Over 230 millions data breaches have benn reported in the healthcare, medical providers and medical insurance services since 2005 (Privacyrights, 2018).

**Access control** To ensure only authorised devices and personnel have access to the medical servers, effective and selective access control schemes must be deployed. It is not feasible to ask permission or consent of a patient every time a data access request is made; therefore, the service providers of the medical servers should provide selective access control for patients, i.e. allowing them to choose which data can be shared without permissions and which third parties, such as companies (Quinn, 2016) and researchers (Welpton, 2018), can gain access to their data. A popular solution of selective access control is Attribute-Based Encryption (ABE) (Goyal et al., 2006), which is categorised as public-key cryptography where the secret keys are generated from attributes (i.e. received signal strength, location, and channel frequency). Access trees in the ABE solutions can be selectively constructed with a set of attributes, so that only a set of attributes that satisfies the tree will be granted access to the encrypted data.

Medical servers should also be able to update the access control policy efficiently. Many cloud security measures require the change of encryption keys when updating access control policy (Murugesan and Bojanova, 2016), which requires decryption and re-encryption of the data in the medical servers and in the personal servers. Therefore, a scalable and less redundant policy update scheme should be deployed to reduce or eliminate the computational overheads in cryptography. A popular solution is the 2-layer over-encryption (Di Vimercati et al., 2007), where policy updates can be made in Surface Encryption Layer (SEL) while a further encryption is imposed by the data owners in Base Encryption Layer (BEL). Furthermore, emergency access control should also be supported in the medical servers, either by disabling security measures over patient's data or by granting a third-party emergency access. For example, Proxy Re-Encryption (PRE) (Blaze, Bleumer, and Strauss, 1998) can be used to convert data encrypted by a patients' public key into encrypted data, which can be decrypted by a third party without revealing patients' data.

**Key Management** The development of secure applications depends on key management protocols, whose goal is to implement and distribute cryptographic keys to sensor nodes (Xiao et al., 2007). Trusted server, key pre-distribution, and self-enforcing protocols are the three major categories of key management protocols (Kumar and Mukesh, 2013). Trusted server protocols achieve key agreement within the network based on a trusted base station. When there is no restriction on resource gateways, these types of protocols are deemed appropriate for hierarchical networks. However, the trusted server protocols are inadequate for critical applications like those related to healthcare because a whole network failure could paralyse a trusted server in a real-time environment (Ng, Sim, and Tan, 2006).

Key pre-distribution protocols rely on symmetric key cryptography to store secret keys within the network prior to its deployment. These types of protocols, such as (Chakrabarti, Maitra, and Roy, 2006; Du et al., 2005; Liu, Wei, and Liu, 2009; Qin et al., 2014; Subash and Divya, 2011), are more appropriate for resource-limited sensor networks because their implementation is straightforward and are not very complex computationally. Self-enforcing protocols are based on public-key infrastructure and are advantageous because they ensure robust security, scalability, and memory efficiency. Modifications must be made to the public key algorithms, such as RSA (Jonsson and Kaliski, 2003) to be optimised for wireless networks in terms of the computations (Gulen, Alkhodary, and Baktir, 2019). In addition, it has been demonstrated by some that protocols based on Elliptic Curve Cryptography (ECC) are appropriate for resource-limited networks (Ng, Sim, and Tan, 2006).

**Trust Management** Trust means that there is a two-way association between two reliable nodes, such as a sensor node and a network coordinator, that share data with one another (Rosenblatt, 2011). Similarly, one study (Boukerche and Ren, 2009) explained trust as the extent to which a node is secured and dependable when it interacts with another node. Distributed collaboration between the nodes of a network must be in place for wireless healthcare applications. In this regard, the level of trust of a node can be determined with trust management systems, which are important particularly as the trust assessment of a node's behaviour, such as the delivery and quality of data, is essential in healthcare applications (Kumar and Lee, 2012). Nevertheless, to clarify how trustworthy the various nodes are, WBANs are required to implement trust management for real-time healthcare applications (Meng et al., 2018).

**Resistance to DoS Attacks** Table 2.1 lists all the Denial of Service (DoS) attacks against WBAN health care applications (DHS, 2014; Kumar et al., 2014). Attackers can use high-energy signals to stop the network from operating properly, such as jamming attacks (Sufyan, Saqib, and Zia, 2013) in the physical layer. The whole network communication could be blocked or sufficiently degraded if the jamming signal is sufficiently strong (Liu, 2012). Attackers may also cause deferrals in communication by breaching the medium access control protocol (Hamza et al., 2016). There are many approaches proposed in safeguarding and self-repairing the network against such attacks, such as evasion defence (Xu, Wood, et al., 2004) and competition strategies (Noubir and Lin, 2003), but they are all at early stage of research (Xu, Ma, et al., 2006). Therefore, more research is required to develop secure DoS attack counteracting strategies for real-time healthcare applications based on wireless body area networks, due to the mobile nature of these applications.

Table 2.1: DoS attacks at each routing protocol layer

| Layers | DoS attacks |
|---|---|
| Physical layer | Jamming |
| | Node tampering |
| MAC layer | Collision and unfairness |
| | Denial of sleep |
| Network layer | Spoofing,<br>replaying, and wormhole |
| | Homing |
| | Hello floods |
| Transport layer | Flooding |
| | De-synchronisation |
| Application layer | Overwhelming sensors |
| | Reprogramming attacks |
| | Route-based DoS |

### 2.2.2 Security Threats

With the internet and wireless connectivity, the new generation of medical devices are facing new challenges in security threats (Al Ameen, Liu, and Kwak, 2012). Instead of medical equipment securely installed in hospital wards or laboratories, the new generation of medical and healthcare devices are worn by or implanted in patients such that they can be monitored in their own home and carry around with them. The majority of the new medical devices have wireless connectivity and can be connected seamlessly with smartphones. These internet connected devices could suffer the same security threats as other IoT devices. The devices can be captured by attackers and important user and personal health information can be exposed to the adversary. Their wireless communication can be attacked by other common IoT attacks, such as malicious code injection (Yang, He, et al., 2015), false data injection (Yang, Lin, Yu, et al., 2015), replay attacks (Mo and Sinopoli, 2009; Zhao and Ge, 2013), crypt-analysis attacks (Zhang, Gu, et al., 2010), side channel attacks (Yang, Wu, and Karri, 2004), eavesdropping (Zhao, Yu, et al., 2016), interference, sleep deprivation (Andrea, Chrysostomou, and Hadjichristofi, 2015; Sarkar and Roy, 2011), Denial of Service (DoS) attacks (Maheswari et al., 2016; Mahmoud et al., 2015), spoofing attacks (Andrea, Chrysostomou, and Hadjichristofi, 2015), sinkhole attacks (Soni, Modi, and Chaudhri, 2013), wormhole attacks (Lee, Clark, et al., 2013), man in the middle attack (Padhy, Patra, and Satapathy, 2011), Sybil attacks (Newsome et al., 2004), malicious virus/worms, etc. Much research has been conducted in defending IoT and BSN devices, and many security schemes, such as the RAEED protocol proposed by Maheswari et al. (2016) can be adopted in health IoT device communication to avoid DoS attacks.

As all medical devices have to handle personal and physiological data of the users, the impact of security attacks on the users could be more direct and severe compared to other IoT systems. Wireless connected implantable devices are designed to manage cardiac functions, insulin functions, nerve stimulation, etc. and equipped with electrodes, pumps and other actuators. Malicious attacks on such devices could be fatal. As most medical devices are only equipped with minimal security protection, these devices can easily be hacked (Rahman, 2018). For example, Radcliffe demonstrated that he can hack into an insulin pump 150 feet away and disable the device or instruct the device to inject excessive amount of insulin (Kaplan, 2011). Cyber-security has become an important issue for the Food and Drug Administration (FDA) in the United States, and the FDA has issued recommendations to medical device manufacturers to review their cyber-security practices (Klonoff, 2015).

There are always new approaches and methods to attack computer devices, and computers have to be constantly updated with patches and anti-virus libraries to protect themselves against malicious attacks. However, unlike computer networks where patches or virus update can easily be injected into the systems, wearable and implantable medical devices often do not have sufficient network bandwidth and resources to update their firmware regularly (Olavsrud, 2016). The majority of these health devices cannot be shut down and wait for security experts to find the anti-virus or patches to recover the devices after the attacks. Given that security attacks can be considered as unavoidable, in addition to introducing security protection mechanisms in IoT health devices, self-recovery or self-protection schemes have to be designed in the medical devices to enable them to recover themselves, maintain essential functions, and protect stored information when the devices are under attack (Cole, Carlton, and Trinh, 2017).

### 2.2.3 Security Schemes

In this section, a few main security schemes applicable for wearable and implantable medical devices are discussed. Although the majority of the security schemes are designed for cloud computing or IoT devices, such as (Choudhury et al., 2011; Wang, Wang, et al., 2010), many of such security schemes can potentially be applied for the new generation of medical and healthcare devices in the era of IoT.

#### 2.2.3.1 Biometric Authentication

Different types of authentication and factors can be used to confirm identity. Facts can be knowledge factors, such as user's secrets, ownership factors, etc., which are verifiable objects that the user possesses, or inherent factors, which are characteristics of the user (Turner, 2016). Most commercial IoT devices currently available for monitoring health and well-being, such as smartwatches, use numeric or alphanumeric passwords for authentication, instead of biometric authentication (Looper, 2019). The use of near-field communication technologies, such as radio frequency identification (RFID) tags, to identify devices and users is also discussed in some surveys (He and Zeadally, 2015; Khoo, 2011).

For healthcare IoT, researchers are exploring the use of biometric inherent factors that are unique to the user, such as fingerprints (Bohan et al., 2013), ECG (Miao et al., 2009a), motion (Xu, Revadigar, et al., 2016), voice (Monrose et al., 2000), and EEG (Huang, Hu, et al., 2019) as it is assumed that these factors are more challenging for an attacker to compromise, especially in comparison to the short passwords commonly used in smartwatches. Such biometric-based security schemes in BSN should meet the requirements stated in Table. 2.2.

Biometric-based security systems often perform two types of actions, namely identification and verification. Identification is the matching of a sample against all the samples in the database, whereas, verification is the matching of a sample against one person's samples in the database (Goode, 2018).

Table 2.2: Characteristics of biometric traits and the requirements of biometric authentication schemes (Guennouni, Mansouri, and Ahaitouf, 2019)

| Characteristics | Explanations |
|---|---|
| Universal | All potential users can use the system |
| Unique | Each user must be differentiated |
| Measurable | The system must be able to collect/measure the biometrics |
| Acceptable | The sampling process must be user-friendly |
| Circumvention | The system must prevent attackers bypassing itself |

Fig. 2.2 is a block diagram of general biometric authentication systems, which is retrieved from (Dharavath, Talukdar, and Laskar, 2013).

As it can be seen from Fig. 2.2, there are two phases, enrolment and matching, in the biometric authentication systems. In the enrolment phase, subjects register their biometric samples or a feature vector extracted from their samples into the database. The recorded biometric samples will be processed into a template or a feature vector and compared against the stored templates or feature vectors. The new template or feature vector will be discarded if it matches with any existing ones in the database. If a match is not found, the new template or feature vector will be stored into the database. In the matching phase, similar process is performed. The subject will be authenticated only if his/her sample matches one or many templates or feature vectors of the claimed identity. If not, the authentication attempt will be rejected by the system. It's worth mentioning that the person must be physically present in front of the biometric authentication systems; otherwise, another person can use any pre-recorded samples to bypass the system.

To assess the performance of biometric authentication systems, some likelihood-based performance metrics, as listed in Table. 2.3, are commonly used (Thakkar, 2017). A trade-off will be made between False Acceptance Rate (FAR) and False Rejection Rate (FRR) by choosing a decision threshold value $t$ for the biometric authentication systems, as shown in Fig. 2.3 (a). If the matching score $s$ is larger or equal than $t$, the authentication is considered to be successful. If $s$ is smaller than $t$, the authentication is failed and the person is considered to be an impostor. The higher the decision threshold $t$ is, the more secure the biometric authentication systems are, and $t$ is often chosen based on the security requirement of the applications.

Behavioural biometric traits, including signature, voice, gait, ECG, Photoplethysmographic (PPG),

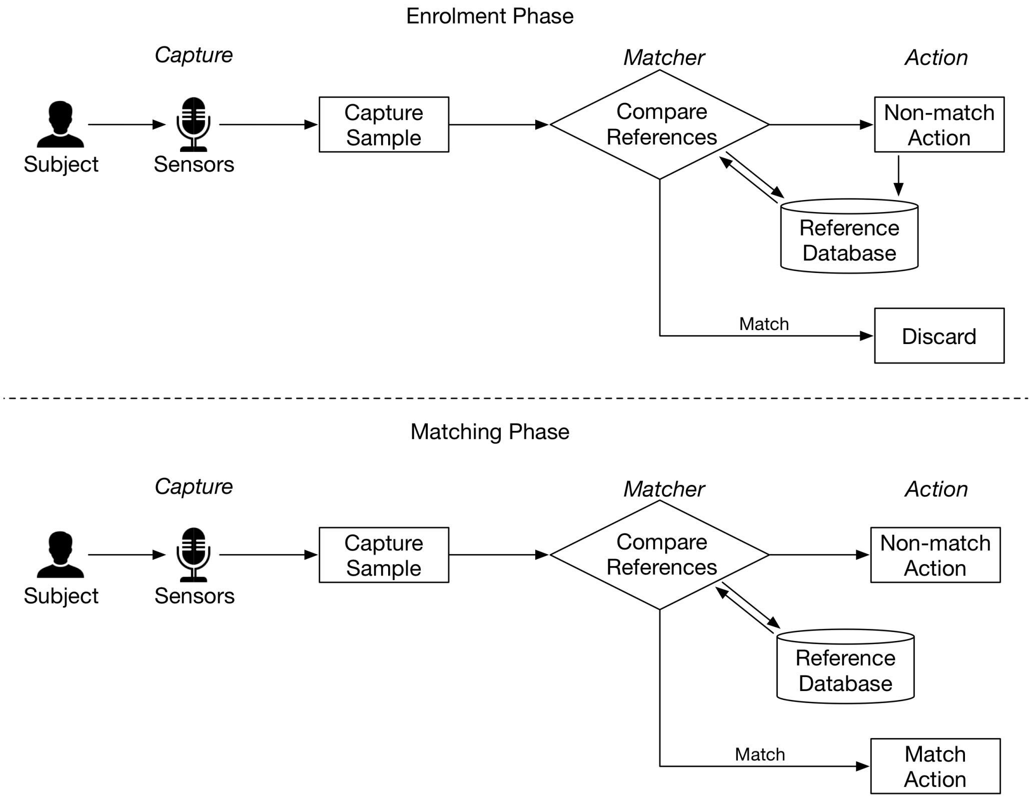
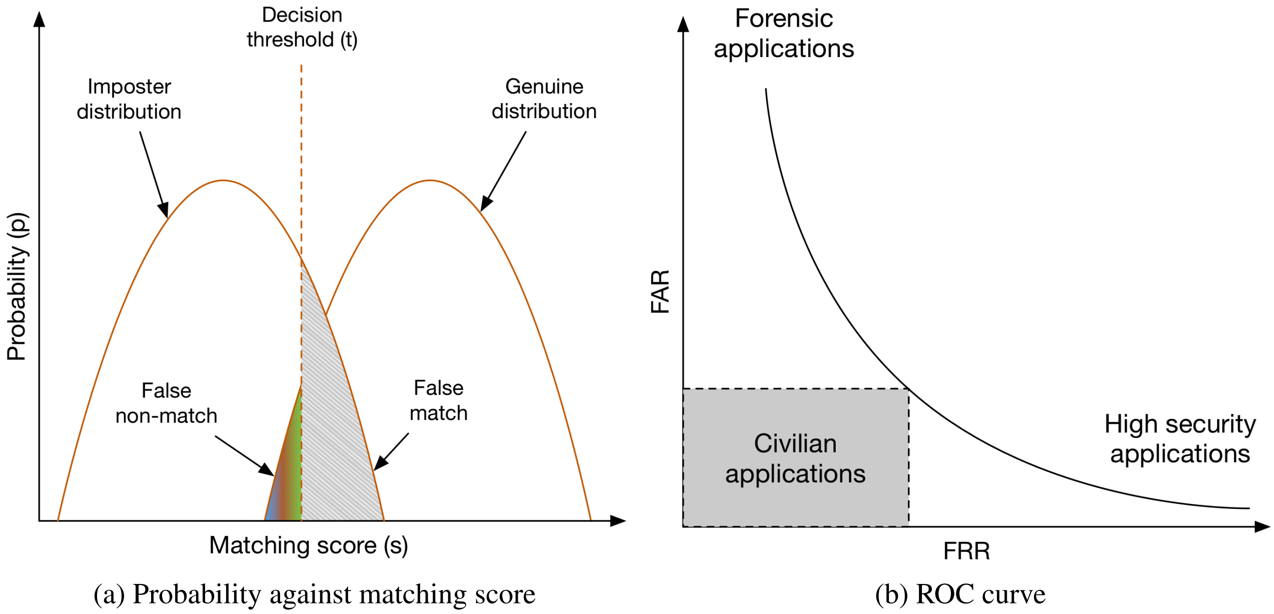


Figure 2.2: Block diagram of general biometric authentication systems (Dharavath, Talukdar, and Laskar, 2013)



(a) Probability against matching score

(b) ROC curve

Figure 2.3: Trade-off between FRR and FAR (Prabhakar, Pankanti, and Jain, 2003)

Table 2.3: Common performance metrics in biometric authentication systems (Thakkar, 2017)

| Performance Metrics | Acronym | Explanations |
|---|---|---|
| Failure-to-Enrol Rate | FTE | It is the percentage of the subjects who were not able to register their biometrics after several attempts |
| Failure-To-Acquire Rate | FTA | It is the probability where the system is not able to acquire data or extract template of subjects |
| False Acceptance Rate | FAR | It is the probability where the system matches the testing sample to non-matching templates |
| False Rejection Rate | FRR | It is the probability where the system fails to match the testing sample to the matching templates |
| Equal Error Rate | EER | It is the probability where both FFR and FAR are equal in the ROC curve |
| Graphical Plot | | |
| Receiver Operating Characteristic | ROC | FAR against FRR |

and keystrokes, can be used in both authentication applications. The strengths and weaknesses of those behavioural biometric traits are summarised in Table. 2.4 (Yampolskiy and Govindaraju, 2008). Behavioural biometric traits can often be captured with low-cost hardware, requiring only algorithms for feature extraction, which makes behavioural biometric based security systems simpler and less costly. Signature and keystroke dynamics are not applicable to BSN sensors, due to the size of the sampling hardware, such as keypad and electronic signature pad. However, they can be used on mobile phones, which are often the coordinators of BSNs.

On the other hand, a large number of physical biometric traits of humans can be used for a variety of biometric authentication applications. In the recent years, the majority of physical biometric traits have been exploited in biometric security systems, including fingerprint (Maltoni et al., 2009), palm print (Han et al., 2003), face (Zhao, Chellappa, et al., 2003), retina/iris (Wildes, 1997), hand geometry (Ross, Jain, and Pankati, 1999), ear shape (Yan and Bowyer, 2007), body odour (Shu, Liu, and Fang, 2014), vein pattern (Watanabe et al., 2005), and DNA (Zayaraz, Vijayalakshmi, and Jagadiswary, 2009), as summarised in Table. 2.5. Every physical biometric trait has its own application scenarios regarding to security requirement and hardware availability. Therefore, no individual biometric system can perform well in all scenarios. In order to achieve a higher level of security, multi-biometric fusion has drawn much attention. A few biometric traits have selected and discussed in details in the following sections.

Table 2.4: Common behavioural biometric traits (Yampolskiy and Govindaraju, 2008)

| Biometric traits | Strengths | Weaknesses |
|---|---|---|
| Signature | Can be captured by either a touch pad or a camera | Lack of long-term reliability and accuracy; signatures can be easily imitated |
| Voice | Only low-cost sensors, such as a microphone, are required | Changes, due to emotion, sick, or misspoken of pass phrase, in the voice degrade the performance of the voice-based biometric systems |
| Gait | Easily accessible; can be captured by either wearable sensors or cameras | Changes, due to injury, ageing, or on-purpose, in the gait degrade the performance of the gait-based biometric systems |
| ECG/PPG | Easily accessible by implanted or on-body sensors | Changes, due to cardiac diseases, activities, and emotion, in the ECG/PPG degrade the performance of the ECG/PPG-based biometric systems |
| Keystroke | Can be captured without user intervention | Require keystroke recorder in either mobile devices and computers; it depends on either a keyboard or a touch screen is used |

**Face** Human identifies others mainly by observing the visual features on their faces. Due to the complexity in quantifying facial features, face recognition has not been widely adopted for security applications until recently. Face recognition has been adopted by smartphones for user authentication. Bommagani, Valenti, and Ross (2014) proposed a face recognition system for mobile phone user identification with a cloud based framework. To improve the efficiency in face recognition, Osadchy et al. (2013) proposed a face identification system which divides a face image into a set of patches and identify the user by matching the patches with the patches of authorised users' face images. Face recognition has been extended for IoT applications, for instance, Hu, Ning, et al. (2017) proposed a face identification framework using fog computing for IoT applications.

**Fingerprint** Fingerprint is the most well-developed person identification technique. The concept of using fingerprint was first proposed by Faulds (1880), and then widely adopted in forensic system of the Scotland Yard and other police forces since 1901 (Wojciechowska, Choras, and Kozik, 2017). With the recent advances in cloud and mobile computing and services, fingerprints have been adopted for user authentication. Yang, Xiong, et al. (2011) proposed a fingerprint system for authenticating cloud service users. Rassan and Al Shaher (2013) proposed a method of using mobile images of fingerprints for authentication. In (Prakash and Venkatram, 2016), fingerprint recognition is chosen for authentication over voice or iris recognition as the technology is more reliable and can be implemented at a lower cost. A detector (Menotti et al., 2015) designed to identify fake iris, face, and fingerprint attacks provides further evidence to support the use of fingerprint recognition by showing that the current state-of-the-art is able to detect fingerprint spoofing more consistently than iris or face spoofing.

**Heart rhythm or Electrocardiogram (ECG)** Bao, Poon, et al. (2008) proposed an ECG-based BSN security scheme using grouped Inter-pulse Interval (IPI) of heartbeats as the source for key generation, which requires longer processing time comparing with only using individual IPIs. Bao, He, et al. (2013) further improved the scheme by using error correcting codes. Zheng, Fang, Shankaran, Orgun, Zhou, et al. (2017) uses multiple fiducial points of ECG signals instead of only one to improve key generation efficiency. The experiment results indicate that the generated keys process high randomness, but it does not show the performance of key matching amongst sensors. Karimian et al. (2017) proposed Interval Optimised Mapping Bit Allocation (IOMBA), which is a framework that takes consideration of statistical information of the population, the individual users, and trade off parameters in terms of binary key reliability and entropy. Chizari and Lupu (2019) proposed a new randomness extraction method, Martingale Randomness Extraction IPI of ECG signals, which largely increased randomness of the extracted binary sequences but it requires longer time for the extraction.

**Iris and retina** It is well established that everyone has a different vascular pattern in our retina, and retina recognition is found to be very accurate and difficult to forge, but due to the intrusive method of data acquisition, retina recognition has not been widely adopted (Borgen, Bours, and Wolthusen, 2008). To capture the vascular pattern in our retina, a retina scanner has to illuminate the retina through the pupil, and the user's head has to be fixed on a chin rest or something similar to minimise motion artefacts. Instead of retina recognition, recent research has proposed the use of iris pattern recognition. Comparing to retinal pattern, iris images can be easily acquired and which enable large scale user authentication and deployment. Kumar and Passi (2010) proposed the use of iris images for user identification. Barra et al. (2015) proposed the use of mobile devices for iris recognition based on spatial histograms from the iris images.

**Motion and Gait** Compare to iris and fingerprint, gait is a relatively new biometric measurement. Due to the difference in bio-mechanical structure and phenotypes, everyone walks differently, and by capturing the gait parameters, individual can be identified (Gafurov, Helkala, and Sondrol, 2006). Apart from user authentication, device-to-device authentication can also be achieved by using gait parameters, as wearable or implantable inertial sensors can capture the same gait parameters when the user walks. A study carried out by Muaaz and Mayrhofer (2017) demonstrates that a person's gait inertial signals are very difficult to imitate, because impersonators often lose their own regularity between steps when mimicking legitimate users. Zhang, Pan, et al. (2015) presented an inertial sensor based gait recognition study on a large gait dataset of 175 subjects, showing the feasibility of gait biometrics to be used on a large population. A fuzzy commitment based gait authentication was proposed by Hoang, Choi, and Nguyen (2015) for encrypting gait templates in the dataset for privacy preservation against potential data breach. Despite open problems such as gait changes due to ageing and low performance on false agreement rate compared to fingerprint and iris, gait biometric holds great potential in cryptographic applications due to its uniqueness, freshness, and availability.

**Voice** Instead of using pin numbers, banks have started to use voice recognition for user authentication in their telephone banking services (HSBC, 2017). Due to the structural difference in vocal chords, trachea, nose, teeth and accentuates sounds, one's voice can be as distinctive as his/her fingerprint (Khitrov, 2013). Unlike other biometric, voice print does not require physical contact with the scanner/reader and can be taken remotely. Voice authentication methods have been extended for IoT systems. For instance, Gong et al. (2017) proposed a proximity-based user authentication method for access control of IoT devices. Voice identification has also been integrated with other biometric measurement devices to provide secured authentication. For example, Spanakis et al. (2016) proposed the SpeechXRays system which uses voice acoustics analysis and audio-visual identity to authenticate the users.

**EEG** Many wearable EEG sensors have been developed over the years, and EEG biometrics has been studied over the last few decades (Jayarathne, Cohen, and Amarakeerthi, 2017). EEG biometrics is very rich in discriminative information or features in both time and frequency domains. Moreover,

Table 2.5: Common physical biometric traits

| Biometric traits | Strengths | Weaknesses |
|---|---|---|
| Fingerprint (Maltoni et al., 2009) | Easily accessible | Wet and wrinkled fingers degrade the performance of fingerprint-based biometric systems |
| Palm print (Han et al., 2003) | Easily accessible | Wet and wrinkled palms degrade the performance of fingerprint-based biometric systems; the size of a palm print template is much larger than a fingerprint template, requiring larger databases; larger size optical readers are required, which is not feasible to be used in mobile phones or IoT devices |
| Face (Zhao, Chellappa, et al., 2003) | Easily accessible | Require high quality cameras; variation in lights and facial expressions can affect the performance of face-based biometric systems; accessories and masks can also affect the performance |
| Retina/iris (Wildes, 1997) | Easily accessible, blood vessel pattern within a retina provides a large set of feature vectors | Require high precision retinal scanners; sunglasses and lens can degrade the performance of retina-based biometric systems; not applicable to WBANs/BSNs |
| Hand geometry (Ross, Jain, and Pankati, 1999) | Easily accessible, an adequate amount of features available | Require specific hardware and software, which has not been widely commercialised yet; not applicable to WBANs/BSNs |
| Ear shape (Yan and Bowyer, 2007) | Easily accessible | Ear can be easily covered by hair, hats, and glasses, affecting the performance of ear-based biometric systems |
| Body odour (Shu, Liu, and Fang, 2014) | Easily accessible; can be easily captured by on-body sensor nodes in BSNs | Deodorants can alter natural body odour, affecting the performance; only a small amount of studies on body odour recognition available |
| Vein pattern (Watanabe et al., 2005) | Provide a large amount of features, thus, high level of security | Require infrared light based special cameras; not very reliable due to the complexity in vein patterns |
| DNA (Zayaraz, Vijayalakshmi, and Jagadiswary, 2009) | Provide a high recognition rate; can be easily obtained via saliva, hair, or blood | Sample processing is complex and not automatic; not applicable to WBANs/BSNs |

EEG biometrics has both unique/time-varying patterns, which may occur when subject is watching an unique picture (visual stimuli), as well as permanent patterns. Traditionally, researchers exploited feature extraction techniques, including Power Spectrum Density (PSD) (Marcel and Millan, 2007), Auto Regressive (AR) coefficients (Paranjape et al., 2001), and Wavelet Transform (Yang and Deravi, 2013), and manually designed features for subject recognition. Recently, deep learning approaches have also been applied to EEG biometrics for subject recognition, identification, and authentication (Arnau-Gonzalez et al., 2017; Mao, Yao, and Huang, 2017; Schons et al., 2017). As stated in (Gui et al., 2015), a person's EEG signals varies from that of another person due to different brain structures, memory, mood, stress, and mental state, mimicking an individual's EEG signals is very difficult to achieve with current technologies (Marcel and Millan, 2007).

Biometrics has yet to be widely adopted for user authentication in medical and healthcare devices. Given the fact that most medical devices capture physiological measurements of the user, the unique and individual characteristics of users' physiology can be used as biometric to enable authentication and secure communication. For example, a real-time biometric key authentication can be carried out by comparing physiological measurements of the patient captured by wearable devices with the signals obtained by implanted sensors.

In theory, this authentication is only available with physical access and contact to the patient. One example of this is authentication via comparison of ECG signals obtained by electrodes attached to a pacemaker programmer with the ECG signal measured by the pacemaker (Rostami, Juels, and Koushanfar, 2013). The programmer attempts to authenticate itself by transmitting the externally measured ECG data to the implant. The implant subsequently compares the received ECG signal with its own recordings to authenticate the programmer.

#### 2.2.3.2 Cryptography

**Encryption/Decryption** There are generally two types of encryption: symmetric, such as AES (Rouse, 2017), Blowfish DES (Nie and Zhang, 2009), and asymmetric where an identical key is used in symmetric encryption and a pair of public and private keys are used in asymmetric ciphers (Russell and Van Duren, 2016). Due to the limited computational resources, symmetric key cipher is commonly used in IoT devices. Advanced Encryption Standard (AES) (Rouse, 2017) is the most popular symmetric key cipher and it has been widely adopted in IoT and Wireless Sensor Network (WSN) (Zhang, Heys, and Li, 2010). Many IoT wireless network chipset has already hardware AES encryption built-in, such as the Nordic BLE nRF52 series (Nordic, 2019), and, TI Zigbee wireless micro-controller series (TI, 2017), which all have built-in 128-bit or 256-bit AES.

Compared to symmetric encryption, asymmetric ciphers provide better security but require significantly more computational power. Wander et al. (2005) have shown that it is viable to implement public-key cryptography on an 8-bit low power Atmel ATmega128L platform, and Doukas et al. (2012) proposed the use of IoT gateways for public key encryption. However, most IoT devices have yet to adopt the use of asymmetric ciphers. Medical and healthcare device development are mainly following the IoT development and adopting the established encryption and decryption schemes into their devices.

Due to the limited computational capabilities of medical and healthcare devices, any data encryption and decryption solutions proposed for securing such devices should be light-weighted with minimal overhead to the communication channels. A popular approach is to modify existing light-weight protocols, such as 6LoWPAN, NFC, and RFID, to support secure communication for medical and healthcare devices. For example, an IoT architecture for securing medical devices is proposed in (Valera, Zamora, and Skarmeta, 2010), where the communication to and from medical devices is secured by security techniques, such as symmetric ciphers, and cryptographic SIM cards. Another example of existing network protocol modification is Lithe (Raza, Shafagh, et al., 2013), an integration of DTLS and CoAP for IoT applications. Lithe has been proven to be able to significantly reduce the power consumption, packet size, and transmission and response time of the IoT networks.

**Random Number Generator** One of the fundamental requirement for cryptography is to have a True Random Number Generator (TRNG) for data encryption (Knight, 2012). Random numbers are often generated by a Pseudo-Random Number Generator (PRNG) with a random seed in modern computers (Hoffman, 2019). PRNGs are deterministic approaches implemented in software. The PRNGs with the same seed will always generate the same sequence of random numbers. If the seed is not generated from a true random source, the PRNGs can be deduced by potential attackers.

For instance, Goldberg and Wagner (1996) found that Netscape's random number generator seed was derived from the process and its parent process IDs and the time of day, which could be computed easily by an attacker. Physical processes or phenomena are often adopted as the random sources. Thermal, atmospheric noise or bit error rate have been proposed as the source of random data. Such TRNG can be formatted as follows (Lo Re, Milazzo, and Ortolani, 2015a):

$$r_t = f(m_{t-w}, m_{t-w+1}, ..., m_t)$$

where $m_t$ is the physical phenomenon (temperature, noise, etc.) at time $t$, $w$ is the window size, and $r_t$ is the random number generated. For instance, Intel's RNG is based on sampling the thermal noise in undriven resistors and noise is expected to be coupled with other environmental noise, such as power supply fluctuations (Jun and Kocher, 1999), etc. Fukushima et al. (2014) proposed a TRNG based on spintronics where binary random bits are generated by using the stochastic nature of spin-transfer-torque switching in magnetic tunnel junctions. Such TRNG requires post processing to ensure that the random numbers are widely distributed, but due to the deterministic design of conventional hardware, the implementation of TRNG is often slow.

Recent advances in quantum mechanics have led to the introduction of new Quantum Random Number Generator (QRNG) (Jennewein et al., 2000). QRNG exploits the randomness of quantum measurements. Most of the QRNG are developed as photonic system using high quality optical components, such as the single photon systems proposed in (Ma, Xie, and Wu, 2005; Nie, Zhang, et al., 2014), where RNG is generated based on the arrival time between single photons, the homodyne measurement approach proposed by Gabriel et al. (2010), where random numbers are generated based on the purity of a continuous-variable quantum vacuum state, and the amplified spontaneous emission technique proposed by Abellan et al. (2014), where random numbers are generated by the interferometric detection of phase diffusion in a pulsed laser diode. On the other hand, instead of using expensive physics instruments, Sanguinetti et al. (2014) proposed the use of conventional mobile phone camera to generate QRNG with a standard LED as the light source. Based on the quantum uncertainty of the light emitted, true random numbers can be generated using a low cost mobile phone camera. Although some of the QRNG approaches can potentially be implemented in the size of a chip (Ma, Yuan, et al., 2016), QRNG is still yet to be implemented in any chipset. Given that QRNG can generate true random numbers at very high speed and potentially very low power, it will be a very attractive hardware option for TRNG designs.

Due to the size and power constraint of IoT Health devices, many true random number generators are not suitable for the miniaturised sensors. Different approaches have been proposed for the implementation of random number generators with low power devices. For instance, Seetharam and Rhee (2004) proposed an efficient PRNG based on a free running timer for low power sensor networks. Francillon and Castelluccia (2007) proposed the TinyRNG, a random number generator based on the received bit error as the source of randomness for wireless sensor nodes. Lo Re, Milazzo, and Ortolani (2015b) proposed a decentralised approach, called ScatterRNG, where the source data for generating the random number is captured by multiple nodes with an authenticated reading collection protocol (Gaglio et al., 2010; Jun and Kocher, 1999).

As such, to break the TRNG, the attacker will need to acquire a large number of sensor nodes. However, the reliance of multiple sensor nodes could expose the network to other attacks. Instead of using analogue circuitry, Xu and Potkonjak (2013) proposed a Field Programmable Gate Array (FPGA) based random number generators with look up tables and hot carrier injection. It is based on the phenomenon that each static random access memory cell will randomly alter its bit if the circuit is powered up for an excessively long period of time (125s). The power consumption of hot carrier injection and FPGA could hinder its application for IoT platforms.

Another approach to generate true random numbers is the use of inertial sensors on mobile devices. Voris, Saxena, and Halevi (2011) proposed the use of an accelerometer as the random source for generating random numbers on a RFID tag. Suciu, Lebu, and Marton (2011) proposed a TRNG design using GPS and inertial sensors. Another inertial sensors based RNG design is proposed in (Loutfi et al., 2014), where raw data streams from inertial sensors are whiten by the Secure Hash Algorithms (SHA). Gait signals collected by inertial sensors can also be used as random sources for TRNGs (Sun and Lo, 2018c). Wallace et al. (2016) proposed SensoRNG, a TRNG design based on multiple internal sensors on mobile phones, including microphones, inertial sensors, and radio.

Inertial sensors based TRNGs have the potential to be used in medical and healthcare devices for data encryption, but issues such as low entropy when idling and high power consumption for implantable devices need to be addressed first.

#### 2.2.3.3 Security Schemes for Implantable Medical Devices

Implantable devices typically require surgery to be implanted into the patients. Therefore, security schemes for implantable devices have strict requirements on power consumption, communication overhead, attack resilience, and support for emergency situations (Ellouze, Allouche, Ahmed, et al., 2014). In addition to the aforementioned challenges, security schemes for implantable devices must comply with strict regulations (Zheng, Shankaran, et al., 2017).

**Proxy based protection** The concept of proxy based implant security is based on a secondary device acting as a “proxy” between communications of the implant and external devices. The advantage of this scheme is that it aims to enhance security of existing implanted devices with the secondary device. An example of this is the “IMD-Shield” (Gollakota et al., 2011). “Shielding” is carried out by introducing noise to intercept communication between the implant and any device that attempts to communicate with it. The decoding of implant signal at the proxy is made possible with the knowledge of the generated noise. A security scheme is implemented such that only authenticated communication is relayed to/from the implant. Another proxy based Implantable Medical Device (IMD) protection is the “IMDGuard” (Xu, Qin, et al., 2011), which is able to share keys between the IMD and the guardian using the owner’s ECG signals.

**Distance bounding** Distance bounding, or proximity based access control, limits attack possibilities by restricting the wireless communication distance between an implant and an external device (Kilinc and Vaudenay, 2017). One example of this is inductive coupling, which often limits effective wireless transmission range to only a few centimetres. While inductive links inherently operate at shorter distances and are suitable for use with device charging and programming, for data communication it lacks the bandwidth required for modern devices. Implant manufacturers have adopted the higher bandwidth MICS (Medical Implant Communication System) which runs in the spectral range of 402-405MHz and signals from the implant are limited to a maximum of 2m. Practically bed-side systems streaming implant data operate at $<$ 1m. Another example of distance bounding authentication through physical layer is (Ankaral et al., 2015), which distinguishes legitimate external device and adversary based on the received signal power. Distance bounded communication schemes alternative to RF/inductive such as skin electrodes and ultrasound (Charthad et al., 2015) have also been proposed.

**ECG based encryption** Theoretically, ECG signals can be captured by IMDs, therefore, ECG based data encryption schemes have the potential to be applied for implantable devices. The advantage of using ECG signals as entropy sources for data encryption is that patients are not required to remember passwords, which remove the risk of being stolen. For example, a one-time-pad encryption scheme proposed in (Zheng, Fang, Shankaran, and Orgun, 2015), which uses the Inter-pulse Intervals of the ECG signals to encrypt messages between the IMD and the external device. The disadvantages of using ECG signals as entropy sources are as follows: firstly, ECG based security schemes typically require signal collection time, which is not feasible in emergency situations; secondly, distortion and attenuation can be easily introduced to ECG signals due to patients' movement or poor contact between skin and the electrodes of ECG sensors; thirdly, although error collection coding is often used to reduce bit errors, it is not sufficient to eliminate false rejection rate. Although ECG signals can be measured very accurately by an external device, the ECG signals captured by the external device are still different than the ECG signals captured by the IMD at a different location.

**IMU based encryption** A Inertial Measurement Unit (IMU) sensor typically consist of an accelerometer, a gyroscope, and a magnetometer, and it is used together by micro-controllers to process collected measurements for on-node human motion tracking and analysis (Tong, 2018). IMU sensors nowadays have been embedded in the majority of mobile phones and wearable sensors, and IMDs are likely to equip with inertial sensors in the near future. Therefore, IMU based encryption and authentication schemes have the potential to be used for securing IMDs. For example, an on-body authentication scheme BANDANA is proposed in (Schurmann et al., 2017), where binary keys are extracted from instantaneous energy variations in motion signals. Similarly, an IPI-based encryption scheme is proposed in (Sun, Wong, et al., 2017) for securing wireless channels in BSNs. Another gait-based security scheme was proposed in (Oberoi et al., 2016), in which secret keys are derived using Hamming window enhanced FFT algorithms. Xu, Javali, et al. (2017) proposed a gait-based automatic key generation protocol, in which Independent Source Analysis (ICA) is applied to separate gait signals and arm swing acceleration signals to improve group key similarity. Based on the same principle, Revadigar, Javali, Xu, Vasilakos, et al. (2017) proposed a fuzzy vault-based group key generation protocol. The aforementioned IMU based security schemes can also be used to protect proxy or gateway of the medical and healthcare IoT systems.

**Analogue shielding** Researchers have shown that implants without adequately robust sensor architectures are susceptible to "analogue attacks" (Kune et al., 2013). Typically, sensors play a pivotal role in a closed loop system such as implanted drug pumps. The sensor signal is inherently analogue in nature and can be interfered, resulting in incorrect sensor readings and erroneous implant operation (Rushanan et al., 2014). The disturbance of analogue signals, often of small amplitude, from intentional noise injection can be mitigated by following good design practices. These include using differential signalling (Pinkle, 2016), shielding in the form of co-axial and tri-axial wirings (Cassiolato, 2011), and keeping physical signal path as short as possible.

**Zero power communication** This security measure is devised to counter "power drawing" attacks where deliberate continuous requests to communicate with the implant are used with the intention to deplete the implant battery. Zero power communication requires all communication from the implant to be initialised by non-battery sources such as piezoelectric RF harvesters (Halperin et al., 2008), also improving patient security awareness by signalling during communication initialisation. Zero power communication can also be achieved by radio frequency energy harvesting. For example, a powerless mutual authentication protocol proposed in (Ellouze, Allouche, Ben Ahmed, et al., 2013), which utilises ultra-high frequency energy harvester and dynamic encryption keys extracted from ECG signals for securing IMDs. In addition, inductive (Kim, Yu, and Kim, 2012) or ultrasound (Charthad et al., 2015) powered schemes mentioned above have also been proposed as zero power communication defence against battery-draining attacks.

**Anomaly Detection** Resource depletion attacks, which could sufficiently reduce the battery power of an IMD, can be detected by anomaly detection, by investigating the patterns of communications between a IMD and legitimate external devices. A Support Vector Machine (SVM) based scheme proposed in (Hei et al., 2010) detects abnormal access attempts to the IMD based on command types, GPS locations, and time. The computation of SVMs is performed on patients' mobile phones, which reduces computational overheads on the IMDs but it will not work without mobile phones. Another example of anomaly detection is MedMon (Zhang, Raghunathan, and Jha, 2013), in which a smart phone examining physical layer characteristics, such as Received Signal Strength Indication (RSSI), as well as behavioural characteristics, such as value range and frequency, of the signals to and from IMDs to identify potential malicious communications. A limitation of MedMon is that it only provides IMD integrity protection, therefore, additional security schemes should be used to protect the confidentiality and availability of the implantable devices.

### 2.2.4 Summary

To enable decision support and personalised care, majority of these new generation of healthcare devices have wireless and network capabilities, and they can be seamlessly connected to smartphone and tablets to capture user feedback and enable personalised configuration. Although the network connectivity greatly eases the control and monitoring functions of the devices, it causes vulnerabilities of the devices. Similar to other IoT devices and systems, IoT medical devices could suffer from similar security threats and attacks. Given the fact that the medical devices handle highly personal health data and some of the devices have life supporting actuation functions, security attacks on connected health devices could have direct and life-threatening impacts on the users.

In the last few years, the number of IoT devices deployed in healthcare systems have grown and expanded rapidly, as a myriad of new wearable and implantable medical devices have been introduced in recent years for healthcare applications, ranging from glucose sensors, insulin pumps, to ingestible core body temperature sensors and drug-eluting stents. These smart devices have facilitated the transformation of healthcare services, enabling personalised and preventative patient care.

Many security schemes developed for IoT devices could potentially be applied for protecting medical devices; however, due to the size and power constraints, wearable and implantable devices are often built with very limited resources and they may not have sufficient resources to implement those schemes. Ensuring the safety and security of such devices requires new solutions that span across the design space of human, cyber and physical elements. Apart from increasing research efforts in the security and privacy of IoT devices, close collaboration is needed between the academic, industries and standard agencies to develop new methods, regulations, and standards to ensure the security of this new generation of medical technologies.

## 2.3 Gait Analysis using Body Sensor Network

The reasons that a brief literature review on gait analysis using BSNs is included in the thesis are twofold. First, gait analysis is often an important part in BSN applications, therefore, an overview of requirements for potential security implementations can be obtained, by studying the requirements of different gait analysis systems. Secondly, a review on gait analysis methods can provide insight on the designs of gait-based biometric systems, which are presented in the following chapters.

### 2.3.1 Gait Events, Temporal, and Spatial Parameters

A gait cycle means the time interval between the occurrence of a repetitive event of walking and the occurrence of the next successive repetitive event. There are seven key events in a normal gait cycle, which divide a gait cycle into seven phases as illustrated in Fig. 2.4:

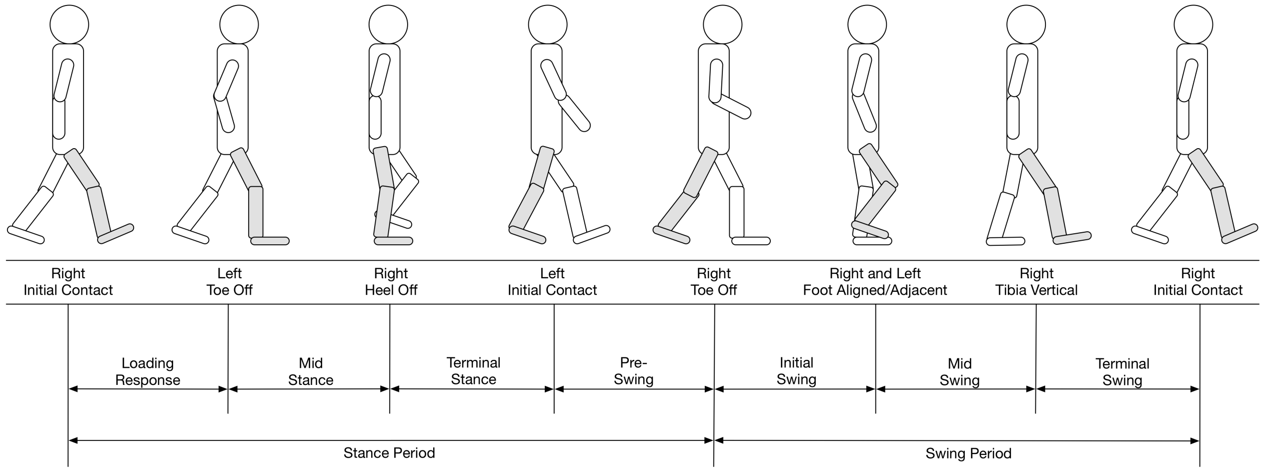


Figure 2.4: Key events and phases of a normal gait cycle (Whittle, Levine, and Richards, 2012a)

1. Initial contact: often called heel strike or heel contact, it indicates the start of the loading response phase (0-10%), which is the first phase of the gait cycle
2. Opposite toe off: it means the beginning of the mid-stance phase (10-30%)
3. Heel rise: often called heel-off, which is beginning of the terminal stance phase (30-50%)
4. Opposite initial contact: it occurs in the middle of a symmetrical gait cycle, and it is the beginning of pre-swing phase (50-60%)

5. Toe off: often called foot-off/terminal contact, which indicates the beginning of the initial swing phase (60-73%)

6. Feet adjacent: it is the instant when the swinging leg passes the stance phase leg, and it starts the mid-swing phase (73-87%)

7. Tibia vertical: it occurs when the stance phase leg's tibia gets vertical, and it indicates the terminal swing phase (87-100%)

The most commonly measured temporal and spatial gait parameters are cadence, speed and stride length. Cadence is the average number of steps per minute, which gives a more general description on the pace of gait. Speed is calculated using cadence with the equation:

$$speed(m/s) = \frac{stride\_length(m) \times cadence(step/min)}{2 \times 60}$$

where stride length is determined by the total travel distance of the walk and the cadence of the person. In addition, stride time is also called cycle time, which is defined as the average time completing one gait cycle, which contains two steps. It can be calculated using the equation:

$$stride\_time(s) = \frac{2 \times total\_time}{total\_step} = \frac{stride\_length}{speed}$$

The total_time is multiplied by 2 because there are two steps in each stride (Kirtley, 2006). Velocity can also be used to describe the speed of gait, if the walking direction is also provided. Stride length is defined as the average distance covered by the swing foot per stride. If both the speed and cadence have been calculated, the stride length can be calculated using the equation:

$$stride\_length(m) = \frac{2 \times 60 \times speed}{cadence}$$

Gait parameters listed in Table 2.6 are often extracted for assessing patients' health, evaluating athletes' performance, and human identification.

Table 2.6: Gait parameters and applications (Chen, Lach, et al., 2016; Muro-de-la-Herran, Zapirain, and Zorrilla, 2014)

| Gait parameters | Definitions | Applications | |
|---|---|---|---|
| | | Clinical | Sports |
| Gait velocity | The rate and direction of position changing during gait | X | X |
| Gait speed | Average gait velocity without direction | X | X |
| Step length | Distance between two successive foot placements | X | X |
| Stride length | Distance of the placements of one foot | X | X |
| Cadence | The average number of steps per minute | X | X |
| Step width | The side-to-side distance between the line of the two feet | X | X |
| Step angle | The angle between the foot and the line of the foot | X | X |
| Stride time | The time completing one gait cycle | X | X |
| Swing time | The time completing the swing period of one gait cycle | X | |
| Stance time | The time completing the stance period of one gait cycle | X | |
| Traversed distance | Distance travelled during gait | X | X |
| Gait autonomy | The maximum time a person can walk | X | |
| Tremors | Existence of tremors during gait | X | |
| Gait phases | The seven phases of one gait cycle | X | X |
| Ground reaction forces | The force exerted by the ground | X | |
| Joint angles | The angles of different joints, such as ankle, knee, and hip | X | X |
| Muscle force | Muscle electrical activity from Electromyography(EMG) | X | X |
| Moment | Moment of forces involved in gait | X | X |

### 2.3.2 Gait Analysis Systems

Gait analysis systems reviewed in this chapter can be categorised into vision-based kinematics analysis systems, goniometer systems, force plate, accelerometers and gyroscopes, and combinations.

#### 2.3.2.1 Vision Based Systems

Vision-based systems are often used to measure and quantify the kinematic parameters of gait, which describes the motion of joints, such as knees, ankles, and toes, in terms of displacements, velocities and accelerations. The simplest vision-based gait analysis approach is by observation, but it has a few limitations, such as, no permanent records, no forces and muscle activity, and results are subjective (Whittle, Levine, and Richards, 2012a). Therefore, camera-based systems have been used in the clinics for gait assessment to provide quantitative measures, such Vicon® Nexus Plug-in-Gait (Anang et al., 2016) and optical marker motion capture system (Perry and Burnfield, 2010). In fact, numerous novel vision-based gait analysis approaches have been proposed in recent years, and the intentions of these approaches are to replace the intrusive, cumbersome, and expensive optical marker motion capture systems. Soda et al. (2009) proposed a Kalman filter based system that provides the kinematic information of gait, by tracking motion marker landmarks on subject's leg in a video stream. Similarly, Kusakunniran (2016) proposed a new marker-less method to extract gait figures in a 2D video, using statistical techniques including linear regression, parabolic regression and polynomial interpolation to extract joint positions in each figure. Furthermore, systems that extract lower joint positions from subject's silhouette have been proposed in (Derbel et al., 2014; Prakash, Mittal, et al., 2015; Shaikh, Saeed, and Chaki, 2014; Wang, Makihara, and Yagi, 2008).

Microsoft Kinect for Windows was released in 2012, which provides image and depth sensors allowing human skeleton and silhouette information to be extracted in real time. Some of the major Kinect-based gait analysis research were selected and summarised in Table. 2.7. The extracted gait features and applications are listed in the second and fourth columns respectively, and the third column shows the testing participants in each research. There are 9 papers researched using Kinect to study Parkinson's Disease (PD), which has the most distribution of research efforts among all gait pathologies (Chen, Lach, et al., 2016).

#### 2.3.2.2 Wearable Sensors

Wearable sensors, such as accelerometers, gyroscopes, and magnetometers, are relatively small, low cost, low power consumption, and with wireless connectivity, so that they are very suitable for ambient and pervasive gait analysis in both clinical and free-living settings. In this section, wearable sensors are categorised by their mounting or worn locations on the subject's body. The studies where multiple sensors were used on different positions (Atallah, Lo, King, et al., 2011; Chen, Cunningham, et al., 2011; Hsu et al., 2014; Yeoh et al., 2008) are categorised by the most important sensor position in their studies.

**Head** Head acceleration caused by gait events can be measured by a single 3D accelerometer fixed onto a subject's head. Heel strike and toe off events are detected in real time using a low pass filter, a threshold, and a peak detection algorithm in (Hwang et al., 2016). In this study, foot-ground contact time and step length were also derived from the detected gait events, then the results were compared

Table 2.7: Recent Research on Gait Analysis Using Microsoft Kinects

| Reference | Gait Features Extracted | Applications |
|---|---|---|
| Gholami et al., 2016 | Joint positions and angles | Quantify gait abnormalities in MS patients |
| Bigy et al., 2015 | Standing to sitting, sitting to standing, falling, and tremor in FOG detections | Recognition of FOG of PD patients |
| Cunha et al., 2016 | Gait cycles, left and right heel strikes, velocity, distance between joints, and joint angles | Motion analysis in neurological diseases |
| Rocha et al., 2015 | Gait cycle, duration, length, velocity, and cadence | PD assessment in a clinical environment |
| Kargar et al., 2014 | Number of steps, step duration, and turning duration | Automatic analysis and classification of human gait in the Get-Up-and-Go Test |
| Cancela, Arredondo, and Hurtado, 2014 | Step length, left and right stride length, and cadence | Walking movement tracking for gait rehabilitation for PD patients |
| Arango Paredes et al., 2015 | Cadence, stride length, and gait velocity | Motor and spatiotemporal parameters calculation of PD patients |
| Staranowicz, Ray, and Mariottini, 2015 | Stride width, and stride length | Multiple-view calibration algorithm for gait monitoring |
| Kastaniotis et al., 2014 | Skeleton data, gait sequences represented in high dimension Euler space | Classification between MS patients and health control subjects |
| Stone and Skubic, 2012; Stone, Skubic, and Back, 2014 | Walking speed, stride time, and stride length | In home gait measurement systems in a senior living facility |
| Staranowicz, Brown, and Mariottini, 2013 | Stride length, duration, left and right foot joint angles | Monitoring human gait during normal daily-life activities and falling prediction |
| Clark et al., 2015 | Step length and foot swing velocity | Evaluation of the dynamic balance capacity of people living with stroke |
| Geerse, Coolen, and Roerdink, 2015 | Gait velocity, direction, and displacement; step time and step length | Multi-Kinect v2 system for quantitative gait assessments |
| Tupa et al., 2015 | Stride length and gait velocity | PD assessment in a clinical environment |
| Motiian et al., 2015 | Step, stride, swing, heel strike, and toe-off time, and stride and step lengths | Gait assessment in both clinical environment and in-home environment |
| Bonnet et al., 2015 | Lower limb joint angles and stride length | Mobile stride length and FOG detection systems |

with the ones obtained from foot acceleration signals, showing the high reliability of gait event detection from a single head-worn accelerometer. A series of studies using ear-worn inertial sensor (Atallah, Wiik, et al., 2014; Atallah, Jones, et al., 2011; Atallah, Lo, Yang, et al., 2009; Aziz et al., 2006; Jarchi, Lo, Wong, et al., 2016; Jarchi, Wong, et al., 2014; King et al., 2010; Li, Atallah, et al., 2014; Wong et al., 2012) have been conducted. The ear-worn sensor was first used for monitoring the recovery of a group of post-abdominal surgery patients (Aziz et al., 2006), presenting potential of using ear-worn sensor in both clinical and free-living settings. Next, discrete wavelet transform and margin based feature selection were applied to the source separated head acceleration time series data in (Atallah, Lo, Yang, et al., 2009), in order to distinguish walking gait impairment from healthy gait patterns. The results showed the ear-worn sensor could be used to observe the progress of some diseases that might influence gait. Then, the following studies (Atallah, Wiik, et al., 2014; King et al., 2010) applied the proposed method to elderly gait asymmetry and fall risk assessment, and Atallah, Jones, et al. (2011) observed recovery from knee-replacement surgery patients using the ear-worn sensors, where the changes in patients' gait could be visualised and represented to clinicians remotely when the patients are at home. Wong et al. (2012) proposed a new method, combining the ear-worn sensor with a depth camera equipped mobile robot, to provide more accurate classification of abnormal gait. Furthermore, feature extraction techniques, such as signal decomposition and reconstruction, singular spectrum analysis, and longest common subsequence, were studied with the head acceleration data collected by the ear-worn sensor in (Li, Atallah, et al., 2014) and (Jarchi, Wong, et al., 2014); and the proposed algorithm was first validated using parotec foot insoles in post-operative recovery monitoring on orthopaedic patients gait assessment datasets, and further analysed and discussed in (Jarchi, Lo, Wong, et al., 2016).

**Waist** A method has been proposed in (Kose, Cereatti, and Croce, 2011) for estimating stride length for one side and the displacement using a single waist-mounted accelerometer; then further work (Kose, Cereatti, Laudani, et al., 2011) and Kose, Cereatti, and Della Croce (2012) extracted spatiotemporal parameters for both left and right sides, where the error rate of step length estimation was less than 3% and that of traversed distance was less than 2%. Hu, Sun, and Cheng (2013) proposed a better kinematic model for estimating gait speed using waist accelerations, with a 0.58% absolute error mean and 0.72% error deviation. Moreover, Soaz and Diepold (2016) proposed a novel method step detection using a single waist-mounted accelerometer, and healthy and frail walking gait patterns were classified using K-means clustering with average error less than 0.02s. Abhayasinghe and Murray (2014) investigated the feasibility of identifying major gait events (initial contact, loading response, mid-stance, terminal stance, pre-swing and swing period), using a single IMU placed in the subject's pocket.

**Leg** Li, Young, et al. (2009) proposed a method to estimate stride length, walking speed, and slope in each gait cycle in real time, based on acceleration and angular velocity measured by a shank-mounted accelerometer. However, the accuracy of estimated slope of this method was low. Trkov et al. (2015) presented a real time slip detection and prediction system with four IMUs attached to one leg. The system is able to predict slipping distance with accuracy within a range of a few centimetres.

**Foot** GaitShoe, a wireless shoe-integrated gait analysis system, with three orthogonal accelerometers, three orthogonal gyroscopes, four force sensors, two bidirectional bend sensors, two dynamic pressure sensors, as well as electric field height sensors was presented by Bamberg et al. (2008). It is able to detect heel-strike and toe-off with high accuracy and estimate foot orientation and position. Systems with only foot-mounted IMUs are also feasible for gait analysis; for example, Patterson and Caulfield (2011) proposed a system where slow, normal, and fast walking can be distinguished as well as initial contact and mid-swing gait events, then, normal and stiff ankle walking patterns were classified (Patterson and Caulfield, 2013). Furthermore, Boutaayamou et al. (2015) proposed a method identifying durations of gait phases in gait cycles. This method was applied in PD gait assessment to quantify subtle gait disturbances in PD patients.

#### 2.3.2.3 Goniometers

Electrogoniometer and goniometer can convert angle to a voltage, therefore, they are often used for joint angle measurements during gait; those measurements are much more accurate and consistent than the joint angle calculations provided in many marker-less vision-based systems, such as Kinect systems, at the cost of increasing intrusiveness of the systems. Reeder (1998) proposed a gait analysis system that mounts two goniometric sensors onto the thigh and calf of the subject. This system is capable of providing hyper-extension information about the stance phases of gait cycles and feedbacks during the gait therapy. Knee movement was also investigated (Micera et al., 2004), where a wearable bio-mechatronic system, called MEKA, was proposed. MEKA is capable of analysing knee movements in two degrees of freedom, moreover, it was used to analyse the modifications of motor performance of elderly and young people during gait using a "dual-task" approach. The results showed a greater variability of the response in the elderly subjects than in the young subjects. Song et al. (2006) took a similar approach analysing leg movement, but it also provided an impedance measurement system. Maranesi et al. (2014) also proposed a method to assess spatiotemporal gait parameters using only 1-degree-of-freedom goniometers mounted on the hip and knee joints of the subject.

#### 2.3.2.4 Mobile Force Plates

Large force plate systems have high accuracy but can only be placed in a gait lab for indoor gait analysis only. Therefore, a mobile force plate system for gait analysis was proposed by Liu, Inoue, Shibata, Hirota, et al. (2010). It was first used in quantitative evaluation of normal and pathological gait for measuring the ground reaction forces with an error rate of less than 6.4%; then a stick-chain model was developed using this system to visualise 3D human gait and joint trajectories (Liu, Inoue, Shibata, and Shiojima, 2011); finally, it was validated by using a stationary force plate, a high-speed cameras-based motion capture system and a XSENS motion track system (Liu, Inoue, Shibata, and Shiojima, 2012). The system is integrated into the bottom of the instrumented shoe, which means it can only be used in specific types of shoes.

In addition, the pressure produced by the arch of the foot cannot be measured, which may affect gait abnormality detection, such as gait asymmetry. Park et al. (2016) also proposed a mobile ground reaction force measurement system, but instead of using force sensitivity resistors, it used optoelectronic force sensors. The overall size of this system is smaller than that of (Liu, Inoue, Shibata, Hirota, et al., 2010), but it has an additional micro-controller unit mounted on the calf of the subject.

## 2.3.3 Methodology

### 2.3.3.1 Skeleton and silhouette

Skeleton and silhouette can only be extracted from vision-based gait analysis systems. For instance, Microsoft Kinect can track skeleton and silhouette data over time, therefore, many vision-based gait analysis systems use Kinects to track the movement and extract gait parameters. Rocha et al. (2015) proposed a Time-of-Flight-based gait parameter extraction method to calculate velocity, acceleration, distance, and angle of all the body joints shown in Fig. 2.5, where left body presents the body joints tracked by Kinect v1, and right body presents the body joints tracked by Kinect v2, which was released on July 15, 2014 alongside the Kinect for Windows software development kit 2.0.

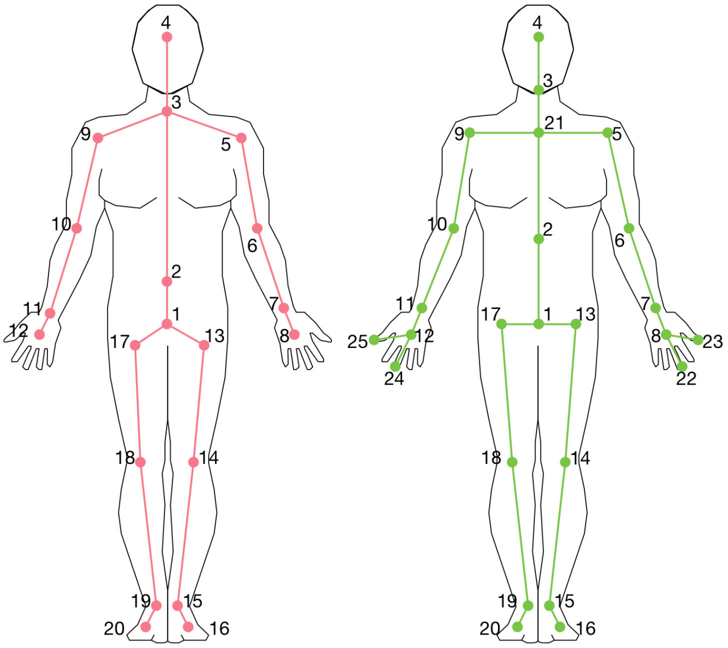


Figure 2.5: Body joints tracked by Microsoft Kinects v1 (left) and v2 (right) (Rocha et al., 2015)

The velocity and acceleration are calculated using Eq. 2.1 and Eq. 2.2, where $v$ is the velocity, and $a$ is the acceleration; $\Delta x$, $\Delta y$, and $\Delta z$ are the difference among x, y, and z axis respectively between two successive frames; $\Delta t$) is the time interval between the two successive frames. The distances between two symmetrical joints in the same frame are calculated using Eq. 2.3, where $P_{left}$ is the joint on the left side of the body and vice versa. Eq. 2.4 is used to calculate the angle of a joint $P_1$, and $P_2$ and $P_3$ correspond to the adjacent joints.

$$v = \sqrt{v_x^2 + v_y^2 + v_z^2} \approx \sqrt{\frac{\Delta x^2 + \Delta y^2 + \Delta z^2}{\Delta t^2}} \tag{2.1}$$

$$a = \sqrt{a_x^2 + a_y^2 + a_z^2} \approx \sqrt{\frac{\Delta v_x^2 + \Delta v_y^2 + \Delta v_z^2}{\Delta t^2}} \tag{2.2}$$

$$distance = \left\| \overrightarrow{P_{left}P_{right}} \right\| \tag{2.3}$$

$$angle = \mathbf{arccos}(\frac{\overrightarrow{P_2P_1} \cdot \overrightarrow{P_2P_3}}{\left\| \overrightarrow{P_2P_1} \right\| \times \left\| \overrightarrow{P_2P_3} \right\|}) \tag{2.4}$$

#### 2.3.3.2 Inverted Pendulum Model

Inverted Pendulum Model (IPM) has been investigated in (Arevalo et al., 2012; Cerny, Noury, and Deplorte, 2015; Esser et al., 2011; Hu, Sun, and Cheng, 2013; Shin, Ikemoto, and Hosoda, 2014; Strozzi, Parisi, and Ferrari, 2016; Tang, Er, and Chien, 2008; Zijlstra and Hof, 2003). Tang, Er, and Chien (2008) suggested that the model should be divided into four phases: frontal single support phase, frontal double support phase, sagittal single support phase, and double support phase. Shin, Ikemoto, and Hosoda (2014) proposed a new human walking model, which improves the IPM with fixed support leg length. In (Hu, Sun, and Cheng, 2013), gait speed was estimated from acceleration signals at the centre of the waist, using kinematic equations combined with the IPM and the rolling-foot behaviour. IPM was also used in (Cerny, Noury, and Deplorte, 2015), estimating stride length combined with the extremes of vertical centre of mass.

#### 2.3.3.3 Machine learning

Machine learning is essentially the means of using an algorithm or method to extract patterns out of noisy data (Kirk, 2015), therefore, often applied to classify the normal and abnormal gait patterns from data obtained in gait assessments. It involves mainly three steps: pre-processing, feature selection, and classification. Fourier Transform (FT) and Wavelet Transform (WT) are mostly used in pre-processing phase, in order to extract primary information, reduce data dimension, eliminate noises, and convert time-domain data into frequency-domain (Khillar, 2018). They both have discrete forms, namely Discrete-FT and Discrete-WT, which are capable of handling discretely sampled input data. For examples, Tallapragada and Srinivas (2011) proposed a new method for viewpoint independent marker-less gait analysis using Discrete-FT; and Atallah, Jones, et al. (2011) applied Discrete-WT to observe variations in both time and frequency domain, in order to quantify patients' gait impairment level during the recovery of the knee-replacement surgeries. Statistical methods such as principal component analysis, independent component analysis, and local discriminant analysis, are often applied to map high-dimensional feature space into relative lower dimensions, thus reducing features, which are used as inputs for the classification and pattern recognition algorithms in Table 2.8.

**K-Nearest Neighbour** It is designed for measuring distance-based approximations, because it classifies new data based on the closest training examples in the feature space. Derlatka and Bogdan (2015) applied ensemble K-Nearest Neighbour (KNN) classifier on a few sub phases of ground reaction force feature sets, which represent the different support phases of the gait cycle, for human gait recognition; and the successful recognition rate was more than 97.37%, based on the measurements of more than 3500 gait cycles from 200 people. Shelke and Deshmukh (2015) also applied KNN classifier to identify the gender, in order to improve the performance of gait based human identification system. KNN is often employed in healthy and pathological gait pattern classification, such as (Dolatabadi, Taati, and Mihailidis, 2016), which proposed a method to distinguish between healthy and pathological gait after stroke, using KNN combined with dynamic time warping.

**Naive Bayesian** It is a simple probabilistic based algorithm, particularly useful when inputs are conditional independent. Nandy and Chakraborty (2015) used both KNN and Naive Bayesian (NB) classifiers on human skeleton dataset captured by Kinect for human identification. Manap, Tahir, and Abdullah (2012) investigated NB classifier for abnormal gait pattern classification in Parkinson's disease, and similarly, Bilgin and Gzeler (2015) applied NB classifier to distinguish three types of neurodegenerative diseases: amyotrophic lateral sclerosis, Parkinson's disease, and Huntington's disease.

**Hidden Markov Model** Hidden Markov Model (HMM) is widely used in gait (Aqmar, Shinoda, and Furui, 2012) and activity (Panahandeh et al., 2013) recognition. Zhang, Wang, and Bhanu (2010) proposed a new framework for age classification based on human gait using HMMs, and the correct classification rate of distinguishing the young and the elderly was over 80% when using appropriate contour features.

#### 2.3.3.4 Support Vector Machine

SVM performs classification by identifying decision boundaries between different classes. Nakano et al. (2016) applied 4 different types of SVM to identify the rehabilitation patients from the gait data and achieved the correct classification rate of 98%. Gupta et al. (2015) proposed a SVM and Bayesian Network combined method to identify people from a distance by gait recognition. Similarly, Das (2015) combined SVMs with HMMs for human gait identification, which outperformed individual classifiers.

**Artificial Neural Networks** ANN provides the means of mapping previous observations through a functional model in the way human brain works. An ANN-based activity classification method was proposed in (Parkka et al., 2006), which is capable of classifying daily activities, such as walking, running, and cycling, which a correct classification rate of 82%. Geman (2013) applied three types of ANNs, namely radial basis function, multilayer perceptrons, and adaptive neuro-fuzzy classifier with linguistic hedges, to discriminate between healthy people and PD patients, with the correct classification rates of 93.44%, 93.34% and 97.67%.

**K-Means Clustering** Soaz and Diepold (2016) proposed a single 3D accelerometer-based system using K-means clustering to obtain normal and frail walking step patterns. Ball et al. (2012) applied

K-means clustering on skeleton data obtained from Kinect for human gait recognition, with a correct classification rate of 43.6% when clustering gait samples from four subjects. To improve the accuracy of this work, Kinect V2 should be employed for obtaining more accurate skeleton tracking data.

### 2.3.4 Summary

Both vision-based and IMU-based gait analysis techniques have been widely adopted in clinical applications, such as chronic disease diagnosis. With the rise of artificial intelligence, the amount of applications involves vision-based gait analysis has been grown rapidly in recent years. For instance, tracking people on the pedestrian, and identifying criminals from the crowd. The techniques used for gait analysis will be advanced much further by the deep learning technologies and massive data collected with the cameras all over the world.

Table 2.8: Commonly Used Machine Learning Methods and Related Applications

| Algorithms | Ref. | Applications |
|---|---|---|
| K-Nearest Neighbour | Derlatka and Bogdan, 2015 | Gait recognition based on ground reaction forces |
| | Shelke and Deshmukh, 2015 | Gait based gender identification |
| | Dolatabadi, Taati, and Mihailidis, 2016 | Automated classification of pathological gait after stroke |
| Naive Bayesian | Nandy and Chakraborty, 2015 | Human gait analysis with Microsoft Kinect |
| | Manap, Tahir, and Abdullah, 2012 | Detection of abnormal gait pattern in PD. |
| | Bilgin and Gzeler, 2015 | Classification of neurodegenerative disease |
| Hidden Markov Models | Zhang, Wang, and Bhanu, 2010 | Age classification |
| | Aqmar, Shinoda, and Furui, 2012 | Human identification |
| | Panahandeh et al., 2013 | Pedestrian activity classification |
| | Yang, Wang, et al., 2014 | Automated gait pattern discrimination |
| Support Vector Machines | Nakano et al., 2016 | Rehabilitation patient classification |
| | Gupta et al., 2015 | Human identification |
| | Das, 2015 | Human identification |
| Artificial Neural Networks | Parkka et al., 2006 | Activity classification |
| | Geman, 2013 | Automatic assessment of tremor severity |
| K-Means Clustering | Soaz and Diepold, 2016 | Step Detection |
| | Ball et al., 2012 | Human identification |

# Chapter 3

# User Identification using EEG Biometrics

This chapter explores the use of EEG biometrics and its potential on user identification applications. The work presented in this chapter has been published in the journal article (Sun, Lo, and Lo, 2019a). Although EEG has less availability than gait biometrics, a person's EEG signal is unique and nearly impossible to mimic. The reason EEG has not been widely adopted for security systems is due to the cumbersomeness of the EEG devices. However, the new generation EEG headsets are becoming smaller and smaller, which makes EEG become more promising to be used in biometric systems.

User identification system is an essential component in all systems, such as IoT/BSN-based healthcare systems, to verify a user's identity and to protect privileged data from unauthorised accesses. The verification process is often between human and machine consists of verifying the credentials of the user to confirm the user's identity. Traditionally, passwords or smart cards are used for user identification (Allison, 2016), but they suffer from many issues, such as the user may have forgotten the password or the password got stolen.

In recent years, password-based security has gradually been replaced by biometrics. Biometric identification systems are designed to identify users based on their biometric traits. A biometric system is often designed to extract features by applying signal processing, machine learning and pattern recognition techniques on the user's physiological signals, and compare the features with the users' profiles/templates stored in the database. Physiological and behavioural biometric traits, such as fingerprint (Isenor and Zaky, 1986), face (Samaria and Harter, 1994), gait (Sun and Lo, 2018a), and

ECG (Zhao, Yang, et al., 2013) have been widely accepted and applied in user identification systems. Despite the popularity of such biometric systems, there are weaknesses in using fingerprint, iris or voice for user identification. For instance, features of the fingerprints, irises and voice can be extracted from high quality photos, videos or audio recordings. In addition, fingerprints can be easily left on surfaces and obtained by malicious attackers.

Recently, EEG, which captures the neural activities or signals in the brain, has been proposed as a biometric measurement for user identification applications. EEG biometrics have several advantages over other traditional biometrics, such as fingerprints. EEG signals highly depend on the person's brain structure (Gui et al., 2015) and association with the person's memory, mood, stress and mental state (Marcel and Millan, 2007). To capture a user's EEG signals, a EEG capturing device has to be attached or worn on the user's head and the user has to be conscious which greatly hinders the chances of malicious attacks.

Despite the increasing popularity of EEG-based biometrics, the state-of-the-art EEG identification approaches still mainly rely on manually designed features and are processed using conventional classification techniques, such as KNN and Eigenvector (Fraschini et al., 2015). Deep learning approaches used for EEG-based identification have not been widely studied. Convolutional Neural Network (CNN) has shown the ability to extract reliable features from images and videos for image recognition applications, such as (Karpathy et al., 2014; Krizhevsky, Sutskever, and Hinton, 2012); however, one of issues with CNNs is that they work well with stationary data (such as an image frame or signal segment), but cannot take into the account for temporal or prior information in the time-series signals.

To consider both spatial and temporal information in time series classification, researchers have proposed the use of Recurrent Neural Network (RNN) to capture and process the temporal variations for speech recognition, such as (Graves, Mohamed, and Hinton, 2013; Mikolov et al., 2010). The order of inputs in RNN can effectively affect the training of the network weights, and thus capture the information from previous time steps. LSTM is one of the RNN architectures, which has showed outstanding performance in medical and healthcare applications. For example, Chauhan and Vig (2015) utilised LSTM to detect arrhythmia in ECG signals, which no prior information about abnormal sig-

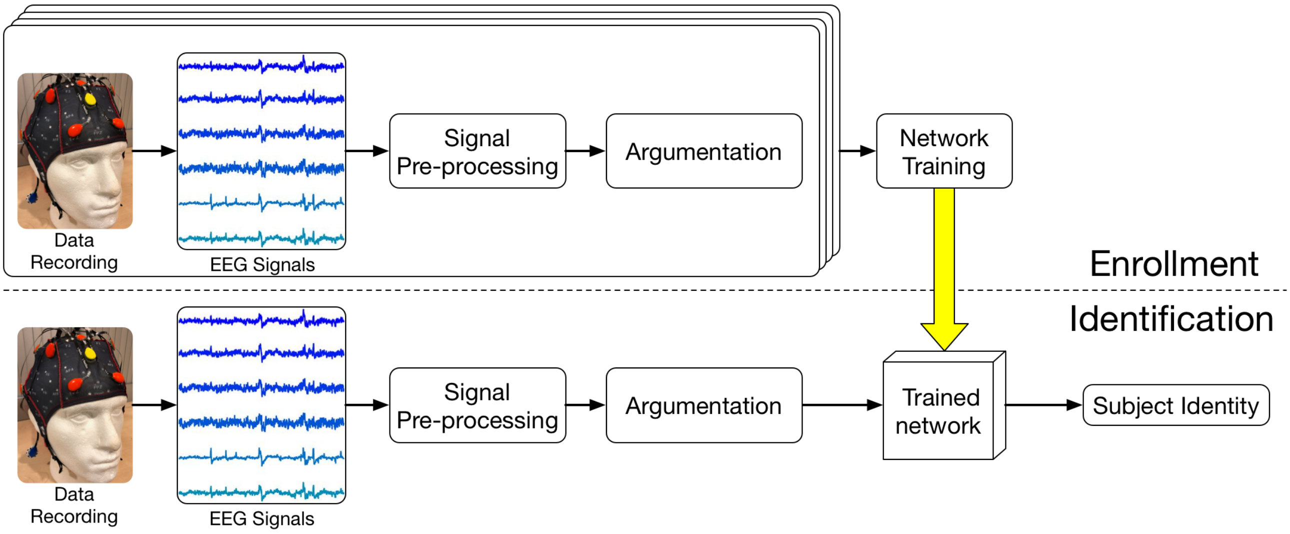


Figure 3.1: Overview of the proposed EEG-based biometric identification system

nals is required. Lo, Li, et al. (2017) proposed using ECG and PPG signals to estimate systolic and diastolic blood pressure based on LSTM neural network. Similarly, Tan et al. (2018) proposed the use of both LSTM and CNN for classifying normal and coronary artery disease ECG signals. LSTM has unique capability of memorising spatial and temporal signal characteristics of physiological signal; therefore, it is hypothesised that such capability could also be applied and improve EEG-based user identification as the spatial and temporal signal characteristics are represented in the architecture

In this chapter, a novel 1D-Convolutional LSTM approach is proposed for EEG-based subject identification. The proposed approach is able to extract both spatial and temporal features from EEG signals, resulting in higher accuracy than CNN or LSTM only identification approaches. The databases used by the previous studies contained a relatively small number of subjects and often the data was recorded when the user was asked to perform a specific task which hinder the generalisation of the approaches and also insufficient to demonstrate the robustness of the EEG-based identification systems. In our experiments, the database contains EEG data collected from 109 subjects, and the proposed approach works on many imaginary and physical activities, instead of only one imaginary or one physical activity.

## 3.1 Related Work

### 3.1.1 Manually Designed Feature Extraction

Paranjape et al. (2001) proposed the use of auto regression coefficients as features and inputs to a Discriminant Function Analysis method for subject identification. The algorithm has been tested on a database with EEG signals of 40 subjects at their resting state and the proposed algorithm has achieved the recognition accuracy of 85%. Campisi et al. (2011) improved the accuracy to 96.08% when subjects are in the resting conditions where their eyes are closed. The method was validated using a database with 48 subjects. Palaniappan and Raveendran (2001) first demonstrated the efficacy of using Visually Evoked Potential (VEP) based EEG signals, which refers to the EEG signal generated in response to a specific visual stimulus (different patterns or objects), for subject identification.

The methodology has been further researched by Palaniappan and Mandic (2007), using multiple signal classification to extract signal features since they assumed that there was only one major sinusoid in each electrode (61 electrodes in total) on the gamma band of EEG signals elicited by visual stimulus and the VEP spectrum was then be used as the dominant features. The algorithm was tested on a large public database with EEG signals of 102 subjects. The accuracy of the proposed methods have achieved an average of 95.85% using KNN. This proposed technique has become the-state-of-art and outperformed other methodologies which have been tested on a similar size database with non-VEP based EEG signal. In addition, wavelet transforms have also been proposed by Yang and Deravi (2013) for feature extraction. Different features including peak amplitude, variance, power spectrum density, mean, eigenvector centrality, zero crossing and other statistical, temporal, and spectral features have also been used in previous studies. Many of the manually designed feature extraction approaches require subjects to perform certain activities, i.e. eye close, or visual stimulus to induce brain activities, from which designed features can be extracted. The advantage of such approach is that when new users are enrolled, their features can be easily stored as profiles/templates in the database. However, such approaches could lead to risks of biometrics being stolen or system being reverse engineered to obtain the feature extraction methods by attackers.

### 3.1.2 Deep Learning for User Identification

Deep learning has gained much attention due to the its outstanding performance in different artificial intelligence applications; however, deep learning approach for EEG-based user identification has only been considered in very few works. Since neural activities are highly dynamic and the EEG pattern varies largely across different users, standard manually designed feature extraction techniques often cannot sufficiently abstract or represent the characteristics of the signals.

Mao, Yao, and Huang (2017) have recently demonstrated the potential for deep learning to perform subject identification, offering a easier training procedure without the need for identifying or designing the EEG features manually. Their group has proposed a biometric identification method based on a convolution neural network, described in (Cecotti and Graser, 2011), trained and validated using raw EEG data collected from a brain-computer interface task designed for measuring driving fatigue. The system achieved 97% accuracy in identifying different individuals under a specific recording paradigm (sampled from a 5 second time window) but only 90% accuracy from randomly sampled EEG signals in an hour session. This is due to other brain activities and physical activities in the whole session that introduce noises and annotation to the EEG signals.

Schons et al. (2017) have also proposed the use of CNNs for EEG-based biometric systems using eyes open EEG signals for training and 5 eyes close 12s-EEG segments for testing. The proposed CNN architecture achieved 0.19% EER, however, in practice, collecting 12s EEG signals could be considered as taking too long for identification purposes. Arnau-Gonzalez et al. (2017) have also proposed a network architecture named EEG-based Subject Identification (ES1D). This network is a structural modification of the conventional CNN by implementing a series of CNN layers and an inception layer. ES1D uses Welch's power spectral density estimation of EEG signal collected from a public database DREAMER (Katsigiannis and Ramzan, 2018) with 23 individuals' EEG data, and achieved an accuracy of 94% which outperforms previous approaches using manually designed features.

However, the number of subjects participated in the experiments was insufficient to demonstrate the scalability of the system, and the proposed deep neural networks for subject identification were constructed with a relatively simple feed-forward layout, without fully utilised the temporal and spatial properties of EEG signal. Our work presents a comprehensive research in examining the performance of deep neural network methods by implementing a hybrid convolutional and recurrent deep neural network, and validated using a public database with EEG data of 109 subjects. The literature has yet to fully exploit the spatiotemporal information in the EEG channels, therefore, a 1D-convolutional LSTM EEG identification approach is proposed for extracting both spatial and temporal features of EEG signals, enhancing the performance of the current state-of-the-art deep learning EEG-based identification approaches, such as CNNs.

## 3.2 Methodology

### 3.2.1 System Overview

Fig. 3.1 shows the overview of the proposed EEG-based biometric identification system, which consists of two phases: enrolment phase and identification phase. In this system, all users' EEG biometrics are learned and stored in a 1D-Convolutional LSTM neural network, trained in the enrolment phase. The recorded EEG signals, either in enrolment phase or in identification phase, will be pre-processed including batch normalisation, and segmented into 1-second normalised signal recordings before being fed into the 1D-convolutional LSTM. The identify of the 1-second EEG signal recording will be the output of the trained 1D-convolutional LSTM in the identification phase. In the rest of the methodology section, EEG signal pre-processing, network architecture, EEG dataset, training, and k-fold cross-validation will be explained in detail.

### 3.2.2 Signal Pre-processing

The EEG signals with $N_{chan}$ channels, where $N_{chan}$ refers to the number of channels, have been used as the input for training the proposed neural network. The sampling frequency is 160Hz, and the signals have been pre-processed before entering the convolutional layer. First, EEG signals have been normalised over time for each channel as follows:

$$I_{i,j} = (Input_{i,j} - \sum_{j=1}^{N_{len}} Input_{i,j}/N_{len})/\sigma_i \tag{3.1}$$

where $i$, $j$, $N_{len}$ and $\sigma_i$ refer to the the channel, the position in the signal, number of sample sequence that fed into the input in one batch and the standard deviation of the channel $i$. Then normalised signals ($I_{i,j}$) are then divided into batches. After pre-processing, the signals will be fed directly to the convolutional layer. The input to the convolutional layer can be written as a form of matrix $N_{chan} \times N_{len}$. In our work, $N_{chan}$ and $N_{len}$ have been set to 64 and 160 respectively which represents 1 second.

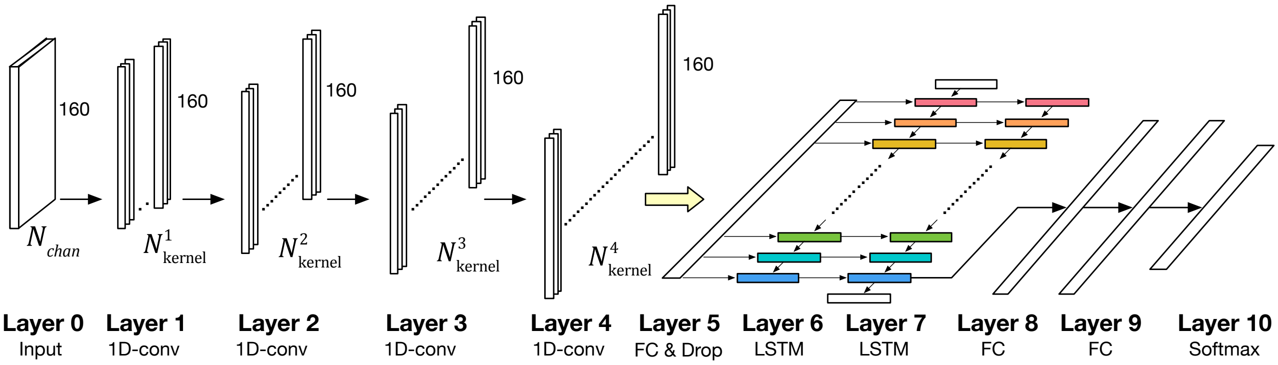


Figure 3.2: Architecture of the proposed 1D-Convolutional LSTM identification system

### 3.2.3 1D-Convolutional LSTM Network Architecture

The network composes of 10 layers with several convolutional layers, LSTM layers and fully connected layers which are combined to form a unified neural network. First, the signals are passed into the first convolutional layer. In our proposed 1D-Convolutional LSTM network, the kernel used in the first layer is in the shape of 2 × 64 having kernel size equals to 2. As previously mentioned, the input fed into the first layer is in a matrix form of 160 × 64. After the convolution, the feature map is shown as a 160 × 1 (1D) array if the stride is set to 1. Since 128 kernels have been used in total for the first layer, the output is shown as 160 × 128. The feature maps are then fed into the Rectified Linear

Unit (ReLU) for non-linear activation. For Layer 1 ($L_1$), the mathematical expression is as follows:

$$\sigma_m^1(j) = b^1(j) + \sum_{i=1}^{i \leq 64} (I_{i,j} w_1(1,m,i) + I_{i,j+1} w_2(1,m,i)) \tag{3.2}$$

where $\sigma_m^l(j)$ refers to the neuron $j$ in the layer $l$ and map $m$. It also denotes the scalar product between the input neurons and the weighted values. $w_k(l,m,i)$ is the filter used in the neural network. $l$, $m$, $i$ and $k$ represent the layer, the map, the channel/kernel and the position in the kernel respectively. $b^l(j)$ refer to the bias in the $l$ layer for the neuron $j$.

Layer 2 ($L_2$) takes an input of matrix with size 160 × 128. The kernel used in the second convolutional layer is in the shape of 2 × 128 having kernel size equals to 2. Again, the feature map is shown as a 160 × 1 (1D) array after the convolution. Since 256 kernels have been used in total for the first layer, the output is shown as 160 × 256. The main function of this layer is to select the best combinations of abstracted features in the feature map which facilitate the classification. Layer 3 and 4 are both convolutional layers. Their structures and properties are similar to the previous layer but with 512 and 1024 feature maps respectively. For $L_2$, $L_3$ and $L_4$, the feed-forward processing is formulated as follows:

$$\sigma_m^l(j) = b^l(j) + \sum_{i=1}^{i \leq N_{kernel}^l} (M_{i,j}^{l-1} w_1(l,m,i) + M_{i,j+1}^{l-1} w_2(l,m,i)) \tag{3.3}$$

where $N_{kernel}^l$ is the number of kernel being used in layer $l$. $M_{i,j}^l$ refers to the element $i, j$ (neuron $j$ in kernel $i$) of the feature maps generated after convolution from the previous layers. The mathematical expression of the feature maps can be expressed as:

$$M^l = \left[\sigma_1^l(j), \sigma_2^l(j), \sigma_3^l(j), \cdots, \sigma_m^l(j)\right]^T \tag{3.4}$$

Layer 5 is a fully connected and dropout layer which consists of 192 neurons. The main purpose of this layer is to reduce the number of feature dimensions before passing to the LSTM layer so that the outputs of Layer 4 can match Layer 5. Dropout is also applied to reduce over-fitting. The feed forward process of this layer is formulated as follows:

$$\sigma^5(j) = b^5(j) + \sum_{i=0}^{i<1024} \sum_{k=0}^{k<160} M^4_{i,k} w(5,i,k,j)) \tag{3.5}$$

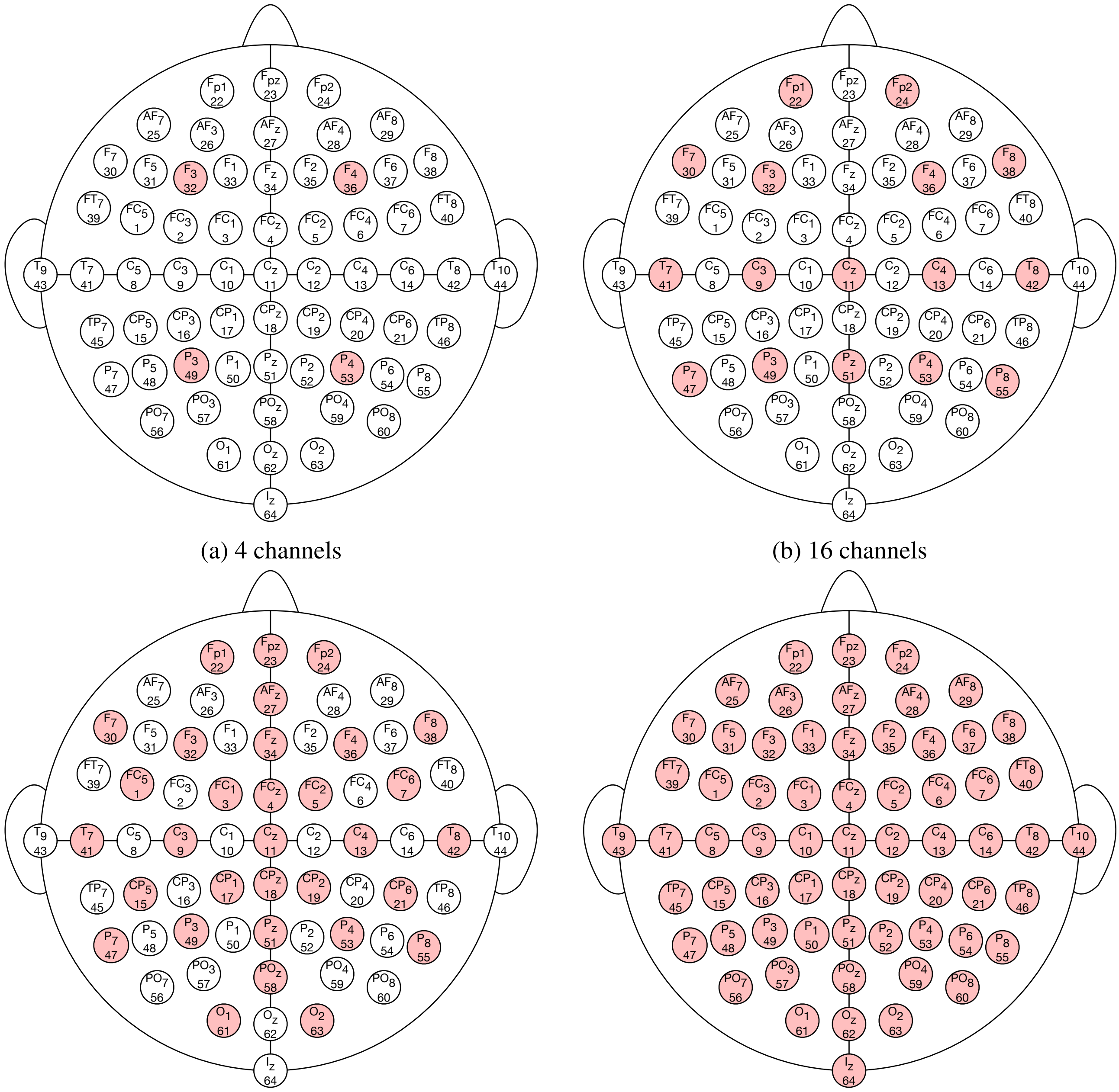
In a LSTM cell, it includes several gates which determine whether the cell forgets, stores or outputs its state. In this way, the LSTM neural networks are able to remember previous information and preserve temporal dependencies. Layer 6 and 7 are the LSTM layers with 192 neurons each. The data fed into the first LSTM layer is in the form of a $192 \times 1$ vector. By iterating the following equations from $t = 1$ to $T$, the output vector $y_t$ can be computed as

$$\begin{aligned} h_t &= \mathfrak{F}(x_t, c_{t-1}, h_{t-1}) \\ y_t &= \sigma W_y h_t + b_y \end{aligned} \tag{3.6}$$

where $x_t$ and $y_t$ refer to the input and output in the state $t$ respectively, $c_t$ represents the cell vector and $h_t$ refers to the hidden vector. $\sigma$ is the logistic sigmoid function, $W$ terms denote weight matrices, the $b$ terms denote bias vectors, $\mathfrak{F}$ is the operator of the hidden layer. The equations of the LSTM memory cell $\mathfrak{F}$ can be generalised as follows

$$\begin{aligned} i_t &= \sigma(W_i \cdot [x_t, h_{t-1}] + b_i) \\ f_t &= \sigma(W_f \cdot [x_t, h_{t-1}] + b_f) \\ o_t &= \sigma(W_o \cdot [x_t, h_{t-1}] + b_o) \\ \widetilde{c_t} &= \ tanh(W_c \cdot [x_t, h_{t-1}] + b_c) \\ c_t &= \widetilde{c_t} * i_t + c_{t-1} * f_t \\ h_t &= \mathrm{tanh}(c_t) * o_t \end{aligned} \tag{3.7}$$

where $i_t$ denotes the input gate equation that determines how much input information should be kept, $f_t$ refers to the forget gate equation that determine how much previous information should be removed, and $o_t$ represents the output gate equation which indicates how much information should be output to the next state. After passing through the LSTM layers, the data is then fed into 2 fully connected (FC) layers for further classification. A softmax layer has been used at the end for subject identification.



(a) 4 channels

(b) 16 channels

(c) 32 channels

(d) 64 channels

Figure 3.3: Electrode positions on scalp and their corresponding channels (red represents empirically selected channels, and white represents unused channels)

### 3.2.4 EEG Dataset

The publicly available Physionet EEG Motor Movement/Imagery Dataset (Goldberger et al., 2000) was used in our experiments to validate the proposed identification system. The dataset consists of EEG data of 109 subjects performing different motor/imagery tasks while being recorded with the BCI2000 system (http://www.bci2000.org) described in (Schalk et al., 2004). In the dataset, 14 experimental runs were conducted per subject with 1-min eye open, 1-min eye close, and three sets of four tasks, including opening and closing fists and feet both physically and imaginarily. BCI2000 consists of 64 channels and the sampling frequencies were set to 160Hz for all channels. As 1-second EEG signal segments are used in the experiment, each signal segment has $160 \times 64$ samples. To evaluate the spatial information resides in the EEG channels, a series of experiments were carried out with 4, 16, 32, and 64 respectively. The selected channels for these experiments are shown in Fig. 3.3 highlighted in red.

### 3.2.5 Training

To examine whether the proposed identification system can be used without the need of asking the user to perform specific mind tasks, all 14 experimental runs of EEG recordings of each subject were used in all the experiments regardless whether the subjects were performing tasks or not.

There were two experiments: 1) the first experiment is to examine and compare the performance of the proposed identification approach with CNN, LSTM, and the state-of-the-art deep learning based identification and classification methods. In the training phase, first 90% of EEG signals in each experimental run were fed into the network for training/validation, and the rest 10% of data were reserved for testing in the identification phase. The training and validation data were randomly selected by a 3:1 ratio. The training dataset was normalised, shuffled, and randomly selected into batches for each iteration of training of all the networks in the experiments. Each batch contains 80 sets of $160 \times N_{chan}$ EEG samples, depending on the number of the active channels.

The training of a network were stopped when it has reached 1000 epochs or the training and validation loss were no longer reduced; 2) the second experiment is to examine the effectiveness of the proposed approach. In the experiments, a k-fold ($k = 3$) cross-validation was conducted on 64-channel CNN, LSTM, and 1D-convolutional LSTM identification systems. In each validation, 4 out of 14 EEG recordings per subject were reserved for testing, and the training of the networks were stopped when reaching 200 epochs. For both experiments, weights and biases of filters were initialised randomly and Adam algorithm (Kingma and Ba, 2015) was used for optimisation.

The dropout rate in the dense layer (layer 6 in Fig. 3.2) and the learning rate $L$ for all the networks were set to 0.5 and 0.0001 respectively. The performance of the trained networks were evaluated using Rank-1 accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). Rank-1 accuracy is used to evaluate the performance in identification scenarios, where the input is 1-second EEG signals from a user whose identity is not revealed. FAR, FRR, and EER are used to evaluate the performance of the systems in identification scenarios, where the systems determines whether a user is who he or she claims to be.

## 3.3 Experimental results

The performance of the CNN, LSTM, and the proposed 1D-Convolutional LSTM based identification systems, with different numbers of EEG channels, are listed in Table 3.1. The Rank-1 accuracies in Table 3.1 are testing accuracies, which are calculated from the EEG recordings that were not fed into the neural networks for training. As the 1D-Convolutional LSTM network exploits both spatial and temporal information within the EEG recordings, the methods are tested with EEG recordings with different number of channels. The symmetrically selected electrode positions on scalp for active channels in four sets of experiments are depicted in Fig. 3.3.

When evaluating the correlations between the number of channels and the identification performance of a specific network architecture, it is clear that higher number of channels will lead to better performance in user identification. By using CNN for identification, the performance of the approach improves as the number of channels increases in the systems, as 16, 32, and 64-channel CNN systems have Rank-1 accuracies of 98.07%, 98.50%, and 98.87% respectively. LSTM identification systems, on the other hand, reduce the identification performance from 96.71% to 96.39% when increasing the

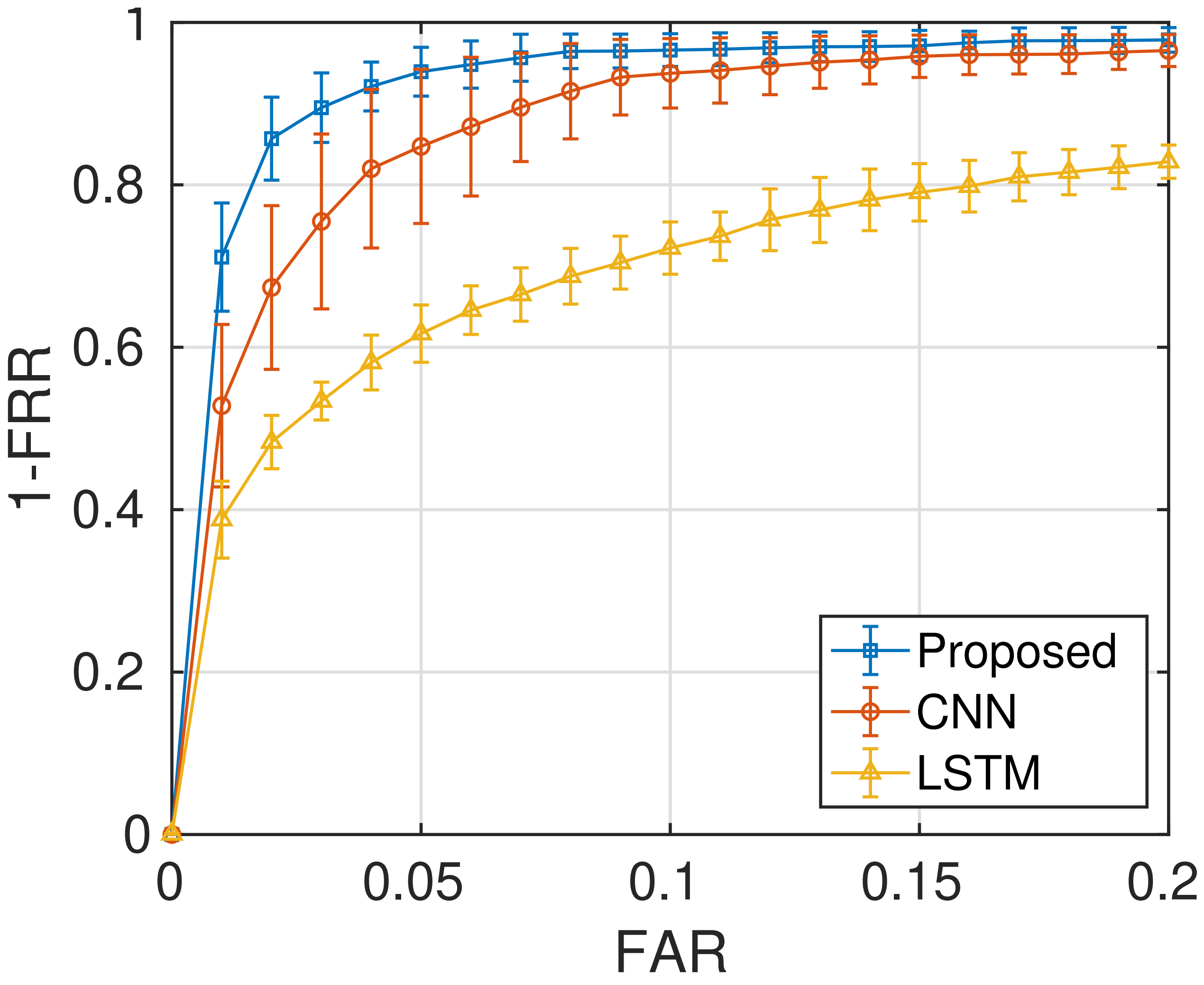


Figure 3.4: ROC curves of k-fold cross-validations on 64-channel CNN, LSTM, and the proposed 1D-convolutional LSTM identification systems (Exp. 2)

Table 3.1: Comparison of the performance of CNN, LSTM, and the proposed 1D-Convolutional LSTM identification systems with 4, 16, 32, and 64 channels EEG signals (positions of the electrodes are shown in Fig. 3.3) for Exp. 1

| | Channel | Rank-1 | FAR | FRR | EER |
|---|---|---|---|---|---|
| CNN | 4 | 0.9434 | 0.0554 | 0.0565 | 0.0559 |
| | 16 | 0.9807 | 0.0190 | 0.0192 | 0.0191 |
| | 32 | 0.9850 | 0.0147 | 0.0150 | 0.0149 |
| | 64 | 0.9887 | 0.0112 | 0.0113 | 0.0112 |
| LSTM | 4 | 0.9036 | 0.0934 | 0.0963 | 0.0948 |
| | 16 | 0.9594 | 0.0395 | 0.0405 | 0.0400 |
| | 32 | 0.9671 | 0.0321 | 0.0328 | 0.0325 |
| | 64 | 0.9639 | 0.0356 | 0.0361 | 0.0359 |
| Proposed | 4 | 0.9428 | 0.0548 | 0.0571 | 0.0560 |
| | 16 | 0.9958 | 0.0041 | 0.0041 | 0.0041 |
| | 32 | 0.9950 | 0.0049 | 0.0050 | 0.0049 |
| | 64 | 0.9958 | 0.0041 | 0.0042 | 0.0041 |

number of channels from 32 to 64. There is a 0.32% decrease in the identification performance, which could be caused by the larger amount of iterations required for the 64-channel LSTM identification system to fully converge.

For a fair comparison, the training of all neural networks stop at 1000 epochs, regardless of whether the training loss has reached its minimum. Additionally, the LSTM systems only exploit the spatial information in the EEG channels. Without feature extraction from CNNs, the spatial information resides in 64 EEG channels is too complex for LSTMs to learn within 1000 epochs of training. The proposed 1D-Convolutional LSTM identification systems does not benefit from increasing the number of channels in the systems either, having Rank-1 accuracies of 99.58%, 99.50%, and 99.58% for 16, 32, and 64 channels respectively.

The accuracy of 32-channel 1D-Convolutional LSTM network is 0.08% lower than that of 16-channel and 64-channel 1D-Convolutional LSTMs, which could be caused by insufficient training iterations and randomly initialised parameters. However, it is clear that increasing the number of channels ($N_{chan} \geq 16$) does no effect on the identification performance of the proposed 1D-Convolutional LSTM systems. Moreover, when increasing the number of channels from 4 to 16, all three types of networks perform significantly better, with the increments in Rank-1 accuracy of 3.73%, 5.58%, and 5.30% for CNN, LSTM, and 1D-Convolutional LSTM respectively.

Both LSTM and 1D-Convolutional LSTM systems have more significant improvement than the CNN system, as the CNNs in the experiments do not exploit the spatial information resides in the EEG channels.

Table 3.2: Comparison of the performance of k-fold (k=3) cross-validations on 64-channel CNN, LSTM, and the proposed 1D-convolutional LSTM identification systems

| | Rank-1 | FAR | FRR | EER |
|---|---|---|---|---|
| CNN | 0.94±0.05 | 0.07±0.03 | 0.07±0.03 | 0.07±0.03 |
| LSTM | 0.79±0.02 | 0.19±0.01 | 0.21±0.02 | 0.20±0.02 |
| Proposed | 0.97±0.01 | 0.03±0.01 | 0.03±0.01 | 0.03±0.01 |

Table 3.3: Tensorflow model loading time ($T_{graph}$) and averaged execution time for batch testing ($T_{batch}$) for CNN, LSTM, and the proposed 1D-Convolutional LSTM identification systems (Time Unit: second)

| | CNN | | LSTM | | Proposed | |
|---|---|---|---|---|---|---|
| Channel | $T_{model}$ | $T_{batch}$ | $T_{model}$ | $T_{batch}$ | $T_{model}$ | $T_{batch}$ |
| 4 | 1.400 | 0.027 | 17.866 | 0.040 | 18.895 | 0.065 |
| 16 | 1.400 | 0.027 | 16.831 | 0.040 | 17.852 | 0.065 |
| 32 | 1.390 | 0.027 | 17.547 | 0.042 | 17.965 | 0.065 |
| 64 | 1.965 | 0.026 | 18.115 | 0.047 | 18.477 | 0.071 |

When the number of active EEG channels ($N_{chan}$) is reduced to 4, the Rank-1 accuracies of CNN, LSTM, and 1D-Convolutional LSTM identification systems are 94.34%, 90.36%, and 94.28% respectively. The accuracy of CNN system is 0.06% higher than that of 1D-Convolutional LSTM and is 3.98% higher than that of LSTM, because the spatial information reside in the selected four channels is not sufficient for the proposed 1D-Convolutional LSTM systems to outperform CNNs.

However, when there are 16 channels, the accuracies of CNN, LSTM, and 1D-Convolutional LSTM systems are 98.07%, 95.94%, and 99.58% respectively. The proposed 1D-Convolutional LSTM system achieved 1.51% higher accuracy, which is a significant improvement considering the accuracy of CNN system has already achieved more than 98%. This can potentially lead to significant impact in biometric application when deploying EEG-based identification systems for a large number of users, providing more unique features to distinguish different subjects.

It worth mention that, comparing with CNN and 1D-Convolutional LSTM systems, the lower accuracy of the LSTM system shows that the feature extraction provided by CNNs could accelerate the learning speed for LSTM when exploiting spatial information from EEG channels. In addition, the 16-channel 1D-Convolutional LSTM system provides 0.71% higher accuracy than that of the 64-channel CNN system, which also proves that EEG channel spatial information for each individual in the dataset is unique and can be used to reduce the number of electrodes in the current EEG-based identification systems.

The differences between FAR and FRR for 4-channel CNN, LSTM, and 1D-Convolutional LSTM identification systems are -0.21%, -0.29%, and -0.23% respectively, with the LSTM system having the worst balance between FAR and FRR. The FAR and FRR difference for 16-channel CNN, LSTM, and 1D-Convolutional LSTM systems are -0.02%, -0.10%, and 0 respectively, with the 1D-Convolutional LSTM system having the best balance between FAR and FRR. For Exp. 2, the results of k-fold cross-validation of 64-channel CNN, LSTM, and the proposed approach are listed in Table. 3.2. The average Rank-1 accuracy of the proposed 1D-convolutional LSTM is 97%, which is 3% and 18% higher than CNN and LSTM respectively. The standard deviation of the accuracies among 3 runs for 1D-convolutional LSTM is 1%, which indicates that the proposed approach is effective and robust.

Moreover, the 1D-convolutional LSTM performs better than CNN and LSTM in terms of FAR, FRR, and EER, which is the same as the results from Exp. 1. ROC curves shown in Fig. 3.4 are the averaged results (mean and standard deviation) from class to class ROC of the k-fold cross-validation. The proposed 1D-convolutional LSTM outperforms the CNN and LSTM identification systems.

## 3.4 Discussion

### 3.4.1 Trade-off among performance, cost, and efficiency

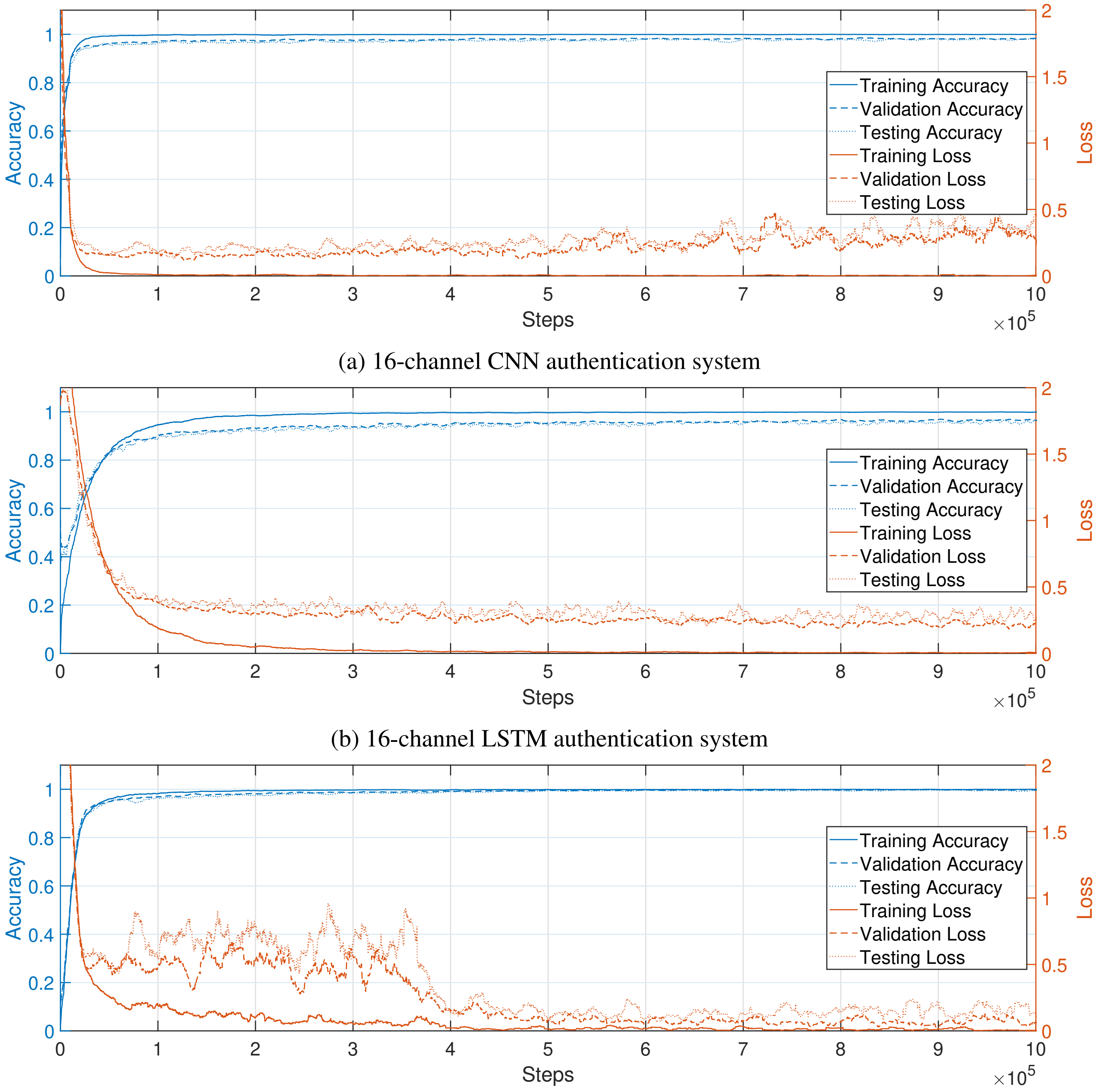
As the performance of the proposed 1D-Convolutional LSTM authentication systems is heavily depended on the types and parameters of the networks, the number of channels of the EEG signals, and the total training time etc., trade-offs can be made to balance and optimise the performance, the cost, and the efficiency of the system. The three graphs in Fig. 3.5 are the first $10^6$ steps of training, validation, and testing accuracy and loss of 16-channel CNN, LSTM, and 1D-Convolutional LSTM authentication systems. Among the three types of neural networks, the CNN system has the fastest convergence speed, whereas the LSTM system has the slowest convergence speed.

Although all the systems have reached training accuracy of 100% after $2 \times 10^5$ steps, the proposed system has the lowest difference between the training accuracy and testing accuracy as shown in Fig. 3.5c, which means 1D-Convolutional LSTM can provide more unique features to identify users. This is also proved by the losses against steps as indicated as the red lines on the right y-axis of each graph. Training losses for all the systems dropped to zero after $5 \times 10^5$ steps, but the testing loss of the 1D-Convolutional LSTM system can reach about 0.1 lower than that of CNN and LSTM systems.

In addition, as shown in Fig. 3.5c, the training and validation losses of the 1D-Convolutional LSTM systems decrease with much less speed than those of CNN and LSTM systems, therefore requiring longer training time than CNN and LSTM systems, which is one of the disadvantages of the proposed approach. However, it is not necessary to train these networks extensively if the application does not require the networks to be fully optimised, and less training can also help to retain the network's generation capability. Trade-offs can also be made on increasing the efficiency and the performance of the identification systems by increasing the number of channels in the EEG signals, or reducing the cost of the systems by using less number of electrodes of the EEG signal recording devices. In addition, there is another trade-off can be made to improve the efficiency of the systems by reducing the limit on the maximum number of steps for training, or increasing the performance of the systems by increasing the amount of training time.

It is also crucial to evaluate the influences of the network types and the number of channels on the time needed for establishing and loading a Tensorflow model and the time needed for identifying a user in practice. Table 3.3 lists all Tensorflow models loading time ($t_{model}$) and the averaged execution time of batch testing $T_{batch}$ for different identification systems. All the time listed in Table 3.3 were recorded on the same PC, which is equipped with an Intel i7-6850K CPU, a TITAN Xp graphic card and a TITAN X graphic card. $T_{model}$ was 1.4 seconds for 4, 16, and 32-channel for CNN identification systems, and it was under 2 seconds for 64 channels.

On the other hand, LSTM and 1D-Convolutional LSTM systems require much longer time for loading Tensorflow model, both under 20 seconds. $T_{batch}$ for 4-channel CNN, LSTM, and 1D-Convolutional LSTM systems was 0.027 second, 0.040 second, and 0.065 second respectively. The batch size was



(a) 16-channel CNN authentication system

(b) 16-channel LSTM authentication system

(c) 16-channel 1D-Convolutional LSTM authentication system

Figure 3.5: Training, validation, and testing accuracy (left y-axis) and loss (right y-axis) against steps for 16-channel CNN (a), LSTM (b), and 1D-Convolutional LSTM (c) authentication systems (only the first $10 \times 10^5$ steps are shown for each system))

Table 3.4: Comparison with some state-of-the-art EEG-based identification systems

| | Features | Dataset | Sampling Rate | Channels | Subjects | Length | Rank-1 | EER |
|---|---|---|---|---|---|---|---|---|
| Fraschini et al., 2015 | Eigenvector | Physionet | 160Hz | 64 | 109 | 12s | 92.60% | 4.40% |
| Arnau-Gonzalez et al., 2017 | CNN | DREAMER | 128Hz | 14 | 23 | 1s | 94.01% | - |
| Schons et al., 2017 | CNN | Physionet | 160Hz | 64 | 109 | 12s | - | 0.19% |
| Mao, Yao, and Huang, 2017 | CNN | BCIT | 64Hz | 64 | 100 | 1s | 97.00% | - |
| Proposed work | Proposed | Physionet | 160Hz | 16 | 109 | 1s | 99.58% | 0.41% |

set to 8 in these experiments, therefore, the execution time for identifying one EEG recording should be one eighth of $T_{batch}$. The CNN system on average was 0.002 second and 0.005 second faster than LSTM and 1D-Convolutional LSTM systems respectively. Although it takes approximately 18 seconds to load the parameters of the models for the proposed approach, once it is loaded, the system is able to perform identifications instantaneously. Therefore, it would not affect the efficiency of the system.

### 3.4.2 Comparison with related works

The results of the proposed 1D-Convolutional LSTM-based identification system are compared with some of the state-of-the-art EEG-based identification systems in Table 3.4. Fraschini et al. (2015) proposed the use of eigenvector centrality of EEG signals as features to distinguish different subjects, and the authors also adopted the Physionet EEG motor Movement/Imagery dataset for evaluating the performance of the proposed biometric system.

The system achieved rank-1 accuracy of 92.60% and EER of 4.40%, however, it requires 12-second EEG signals for feature extraction, which would be too long for practical applications in real-time identification. Similarly, Schons et al. (2017) proposed the use of CNN on 12-second EEG signals and the system was evaluated using the same EEG dataset (resting brain state only). Although the system achieved the EER of 0.19%, it could be impractical for users to wait 12 seconds for collecting EEG signals. In addition, Arnau-Gonzalez et al. (2017) and Mao, Yao, and Huang (2017) also proposed the use of CNN for user identification, achieved Rank-1 accuracies of 94.01% and 97.00% using DREAMER and BCIT Experiment Baseline Driving (Lin et al., 2005) EEG datasets respectively.

In our experiment, we applied CNN identification systems to Physionet EEG dataset and the Rank-1 accuracy for 64-channel EEG signals was 98.87% on 109 subjects as listed in Table 3.1. As discussed previously in the results section, the proposed 1D-Convolutional LSTM identification system can exploit spatiotemporal information in the EEG channels, improving the performance and reducing the number of channels required at the same time. As stated in Table 3.4, the proposed 1D-Convolutional LSTM identification system outperforms other previous approaches (Mao, Yao, and Huang, 2017) by 2.58% and required only 16 EEG channels. In addition, k-fold cross-validation was performed in our experiments and results show that our proposed approach is effective and robust.

However, introducing LSTM into the network architecture will inevitably increase the computational complexity, thus increases the training time required for high identification performance as indicated in Table 3.3. In addition, the use of deep learning would increase the initial cost of the user identification systems as for the moment deep learning requires graphics processing units (GPU) for faster calculation of complex equations used in the neural networks.

## 3.5 Conclusions

In this chapter, a novel EEG-based identification system is proposed using 1D-convolutional LSTM neural network. A comparative experiment was carried out to assess the performance of the proposed 1D-Convolutional LSTM against CNN, and LSTM identification systems, using a public database with EEG data of 109 subjects. The Rank-1 accuracy and EER of the 16-channel 1D-Convolutional LSTM identification system is 99.58% and 0.41% respectively, which shows that the proposed approach outperforms the state-of-the-art EEG-based identification approaches in the literature.

In addition, a k-fold cross-validation was performed, and results illustrate the efficacy and the robustness of the proposed approach. The results from both experiments show that the 1D-Convolutional LSTM can exploit spatial information resides in the EEG channels, providing additional features for distinguishing different subjects. In addition, with 1D-Convolutional LSTM, less number of electrodes can be used to achieve similar performance which could significantly reduce the cost of EEG-based biometric identification systems.

The future work of the proposed 1D-convolutional LSTM network would be to further testing its scalability by retraining the networks with EEG data from other databases. In addition, studies will be extended to determine which EEG channels are the most effective ones for distinguishing different users, and to develop automatic channel selection algorithms instead of manual channel selection used in the current experiments.

As for the future work of EEG-based user identification systems, the effect of ageing on the EEG signals, which could potentially hinder the performance of the systems, has yet to be investigated. As training a new deep learning network is time consuming, transfer learning technique should be introduced to reduce time consumption for adding new users in the fully trained deep learning networks. In addition, the fusion of EEG with other biometric traits is an interesting topic, as it would potentially be used to design more secured identification systems.

# Chapter 4

# Body Sensor Network Security Using Gait

Although EEG-based security systems proposed in the previous chapter perform exceptionally well, EEG headsets are still very expensive and cumbersome in size. An alternative biometric trait, gait, is studied in the following chapters. The work presented in this chapter has been published in two conference papers (Sun, Wong, et al., 2017; Sun, Lo, and Lo, 2019b).

## 4.1 Secure Key Generation Using Temporal Gait

With the aim of providing pervasive health monitoring, Body Sensor Networks capture and process sensitive personal information, such as physiological data, life style preferences, etc. Such information could be targeted by hackers to cause harm to the users (Lo, Ip, and Yang, 2016). With no user interface and limited computational power in the sensor node, security solutions for BSN have to be light weight, energy efficient and autonomous. A widely researched security solution for BSNs is Biometric Cryptosystem (BCS), which utilises biometrics, such as ECG, PPG, and fingerprints, to secure the body sensing signals (Guo et al., 2016). The primary advantages of employing biometrics are twofold. First, biometrics can be easily collected by body worn sensor nodes, which means that no key pre-deployment is required; second, biometrics are unique and permanent (Campisi, 2013), which makes it especially suitable for user authentication.

The state-of-the-art BCSs employ Fast Fourier Transform (FFT) (Miao et al., 2009b; Ramli, Ahmad, and Abdollah, 2013) and Discrete-WT (Garcia-Baleon, Alarcon-Aquino, and Starostenko, 2009) to extract frequency and spatial coefficients from ECG signals captured by BSN sensor nodes, which are then used to generate binary sequences to form a common secret key for the secure network communication. However, as frequency domain analysis is computationally demanding, the proposed schemes are often too complex for real time processing in miniaturised BSN sensor nodes. Another approach is to use the variations of IPIs of consecutive ECG pulses; this particular approach has been investigated in (Bao, Poon, et al., 2008; Zhang, Poon, and Zhang, 2012; Zheng, Fang, Shankaran, Orgun, and Dutkiewicz, 2014). IPI-based BCS approaches are relatively light weight in comparison to FFT and Discrete-WT key generation schemes. Although ECG and PPG signals are available to many wearable devices and mobile phones, the majority of wearable devices are often unable to obtain correct ECG or PPG measurement without user intervention. The ECG and PPG signals are also easily affected by motion artifacts. With the aim of developing a security scheme for BSN, we propose the use of gait biometrics for key generation for BSN. The scheme is based on gait acceleration signals measured by accelerometers, which are readily available in most wearable devices and mobile phones. The scheme is capable of generating and distributing secret keys amongst sensor nodes without complex frequency domain analysis.

Gait signals as a biometric behavioural trait has been proposed for authentication (Cola et al., 2015) and recognition (Meharia and Agrawal, 2015; Zhang, Pan, et al., 2015); however, the feasibility of adopting gait in BCSs requires further investigation. An automatic key generation scheme based on gait was proposed in (Revadigar, Javali, Xu, Hu, et al., 2016; Xu, Revadigar, et al., 2016), in which Independent Component Analysis is applied to separate accelerations produced from leg motions and arm swing motions. As previously mentioned, complex frequency domain analysis introduces high computation overheads to the security system; therefore, the scheme may not be suitable for typical BSN sensors.

In addition to the design complexity, the key generation scheme in (Xu, Revadigar, et al., 2016) requires a number of message exchanges during key establishment, which results in more overheads in the channel. Another device-to-device authentication scheme based on gait was recently proposed in (Schurmann et al., 2017), where gait fingerprint bits are extracted from energy level difference between each gait cycle and the average gait cycle. In a similar work by Hoang and Choi (2014), the secret key is generated from a set of extracted features in both time and frequency domains from gait signals. In addition to the high computation overheads of FFT and discrete cosine transform analysis in this scheme, the error rate of the generated key will rapidly increase if the key size is greater than 40 bits, as the similarity between collected signals and templates is not sufficient enough to extract too many bits.

To secure wireless communications among BSN sensors, a novel light-weight symmetric key generation scheme is proposed in the first part of this chapter, which is based on gait events timing (temporal gait) from acceleration signals.

## 4.1.1 Methodology

### 4.1.1.1 System Modelling and Experimental Set-up

As shown in Fig. 4.1, a typical BSN employs the star topology, where sensor nodes only communicate directly with the network coordinator, which is often a mobile phone. Sensor information is then aggregated by the coordinator before being forwarded to the server via Wi-Fi or a mobile network.

Our key generation and distribution scheme is focused on securing wireless communication amongst a network of sensors worn by a user, where gait acceleration signals can be obtained directly from the sensor node with its embedded accelerometer. Fig. 4.2 illustrates the acceleration signal of an entire gait cycle on a sensor worn on the back, which consists of a right step and a consecutive left step, along the superior-inferior axis. There are seven key gait events: right heel contact, left toe off, heel off, left heel contact, right toe off, feet adjacent, and tibia vertical. The timing of each gait event varies from cycle to cycle, which is used in the proposed scheme for generating the biometric key. For the ease of explanation, ECG pulse naming convention is applied to label one gait cycle as indicated in Fig. 4.2: right or left heel contact in a gait cycle is denoted as P wave; right or left foot flat pulse is named QRSTU complex, while valley S represents the toe-off event, the pulse in the mid-stance phase between toe-off and heel off is labelled as T, and finally heel off event is named as U. Gait events often have a slight variation between each gait cycle, so that they can all be used to generate

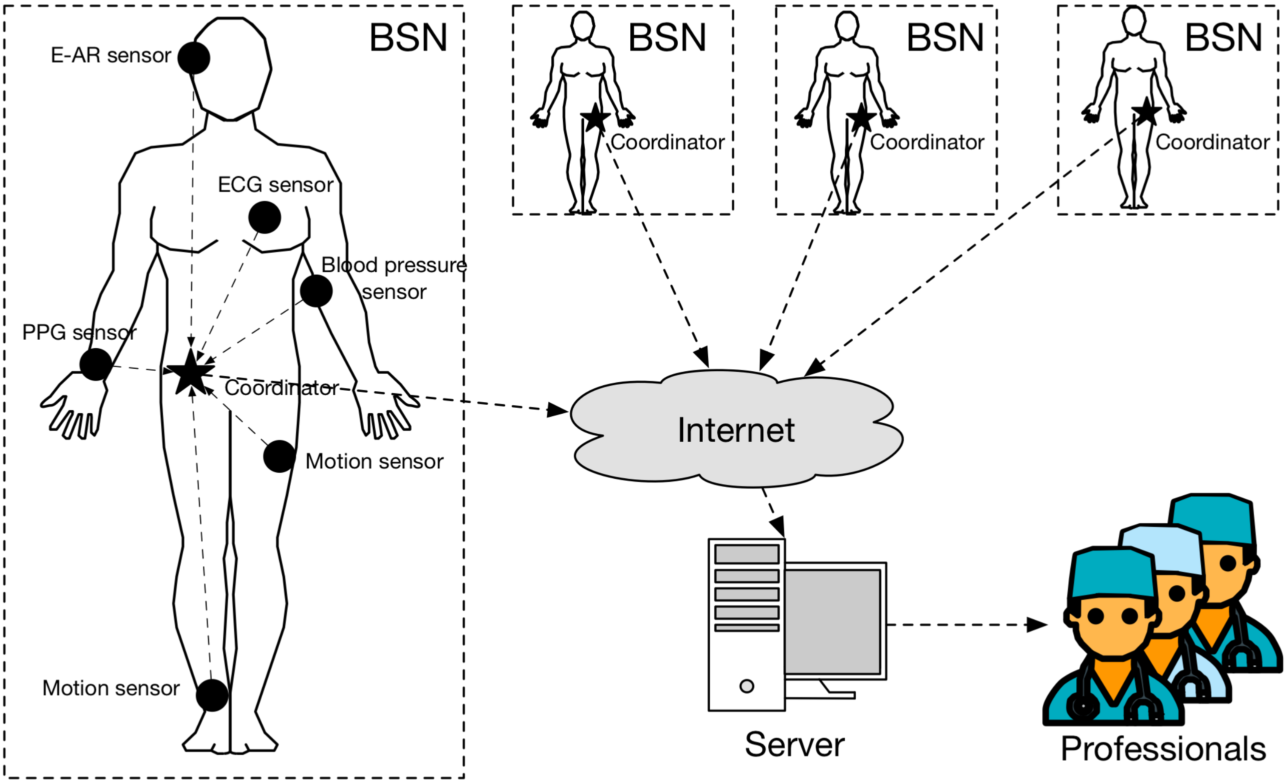


Figure 4.1: Design of a typical BSN system

random binary sequences. Although any of the gait events can be used in the proposed scheme, only R peaks are used for the explanation in the rest of the chapter.

For data collection, we used two iPhones and an e-AR sensor in our experiments, while acceleration data was captured and recorded in each device separately. The e-AR sensor is an ear-worn activity recognition sensor, designed for gait analysis (Jarchi, Lo, Ieong, et al., 2014). The data was then downloaded onto a computer for processing. The proposed key generation and distribution scheme was implemented, simulated and evaluated using Matlab R2016b. To evaluate the performance of the scheme, we have first conducted an experiment with one iPhone placed on the lower back and another placed on the front of the waist of each subject, and about 300 steps were collected from 5 test subjects. A second experiment was conducted with one iPhone placed on the lower back and the other iPhone placed on the right upper arm of each subject. Finally, a third experiment was carried out by placing one iPhone on the lower back and the e-AR sensor on right ear of the test subjects.

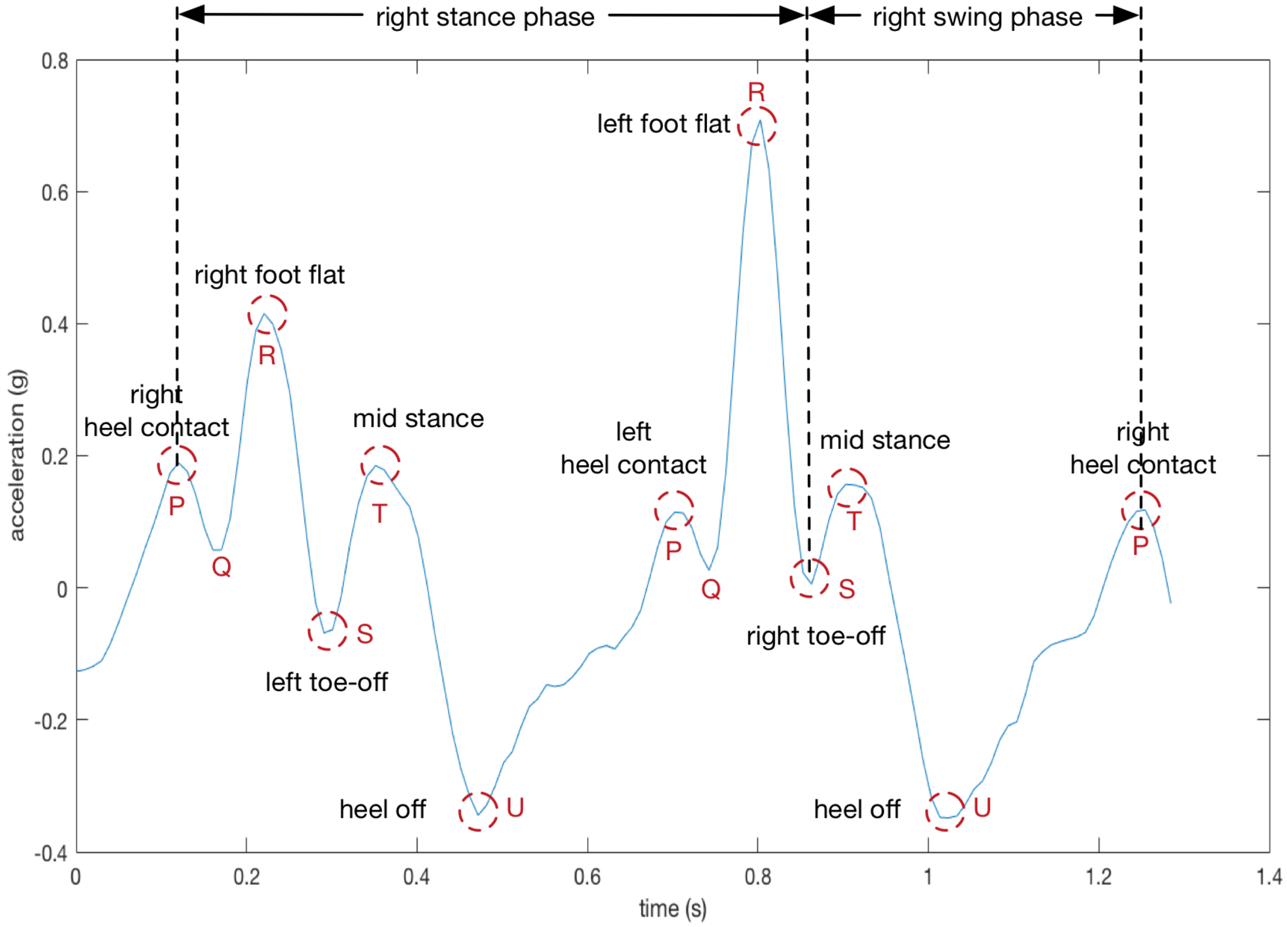
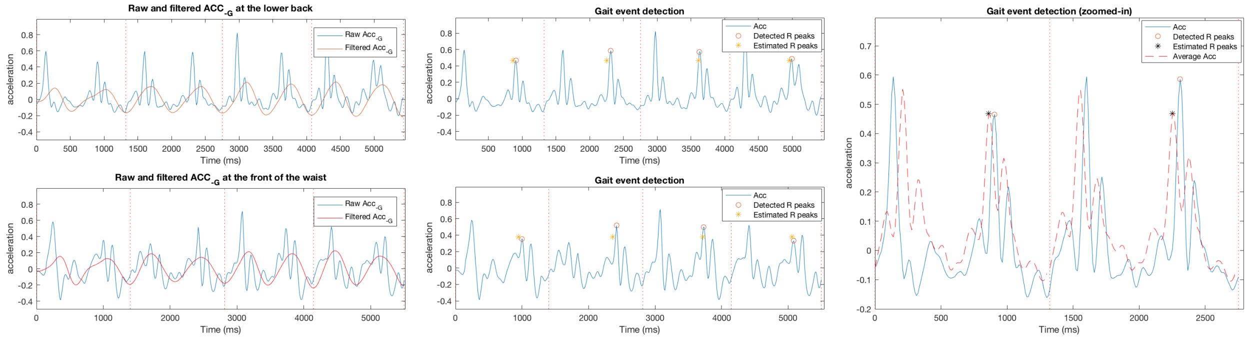


Figure 4.2: Gait acceleration data in the inverted gravity direction



(a) Filtered signals

(b) R-peak detection

(c) Zoom-in

Figure 4.3: Gait cycle and gait event detection

#### 4.1.1.2 Signal Pre-processing

Acceleration signals collected by a sensor node are captured in respect of its own orientation and coordinate system; therefore, to extract accurate gait features from body worn sensors, the acceleration signals have to be projected onto the same coordinate system (Xu, Revadigar, et al., 2016). In the proposed scheme, rotation matrix $\mathbb{R}^{3\times3}$ is multiplied to the 3-axis acceleration signals, denoted as $Acc_x$, $Acc_y$, $Acc_z$, to project the acceleration signals onto the common world coordinate system:

$$\begin{bmatrix} Acc_N \\ Acc_E \\ Acc_{-G} \end{bmatrix} = \mathbb{R} \begin{bmatrix} Acc_x \\ Acc_y \\ Acc_z \end{bmatrix} \tag{4.1}$$

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

$$\mathbb{R} = \begin{bmatrix} 1-2(y^2+z^2) & 2(xy-wz) & 2(xz+wy) \\ 2(xy+wz) & 1-2(x^2+z^2) & 2(yz-wx) \\ 2(xz-wy) & 2(yz+wx) & 1-2(x^2+y^2) \end{bmatrix} \tag{4.2}$$

The quaternion vector $\mathbf{q}$ can be calculated from raw gyroscope data as followings: (Mohssen et al., 2014)

$$\mathbf{q} = \begin{bmatrix} w \\ x \\ y \\ z \end{bmatrix} = \begin{bmatrix} cos(\frac{\alpha}{2})cos(\frac{\beta}{2})cos(\frac{\gamma}{2}) + sin(\frac{\alpha}{2})sin(\frac{\beta}{2})sin(\frac{\gamma}{2}) \\ cos(\frac{\alpha}{2})sin(\frac{\beta}{2})cos(\frac{\gamma}{2}) - sin(\frac{\alpha}{2})cos(\frac{\beta}{2})sin(\frac{\gamma}{2}) \\ sin(\frac{\alpha}{2})cos(\frac{\beta}{2})cos(\frac{\gamma}{2}) + cos(\frac{\alpha}{2})sin(\frac{\beta}{2})sin(\frac{\gamma}{2}) \\ cos(\frac{\alpha}{2})cos(\frac{\beta}{2})sin(\frac{\gamma}{2}) - sin(\frac{\alpha}{2})sin(\frac{\beta}{2})cos(\frac{\gamma}{2}) \end{bmatrix} \tag{4.3}$$

where $\alpha$, $\beta$, and $\gamma$ are the raw 3-axis gyroscope signals recorded alongside with acceleration signals. By projecting the sensor signals onto the same coordinate system, the accuracy of the gait event detection can be improved significantly, even though, the proposed key generation scheme can work without projection, as it mainly relies on the timing information.

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

#### 4.1.1.3 Gait Cycle and Gait Event Detection

A low pass filter with a cut-off frequency of 10Hz is applied to $Acc_{-G}$, as indicated in Fig. 5.20a, to identify and split repetitive gait cycles in $Acc_{-G}$. 10Hz is chosen as the cut-off frequency because human motion has no significant effects on frequencies above 10Hz (Schurmann et al., 2017). Assuming N gait cycles are found, the detected gait cycles

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

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

$$\widetilde{t_i} = \frac{T_i}{\overline{T}}\bar{t}$$

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

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

On the other hand, $\bar{y}$ can be used directly as the estimated magnitude of the R peaks, $\widetilde{y_i} = \bar{y}$ because human gait is highly repetitive and gait events are likely to occur at the same positions in every gait cycle as indicated in Fig. 4.3. To simplify the representation of the estimated R peaks, it is represented as

$$\widetilde{p_i} = (\widetilde{t_i}, \widetilde{y_i})$$

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

**Algorithm 1** Pseudo code for binary sequence generation

```
Require: $ACC \leftarrow$ Acceleration sample
    $n \leftarrow$ Codeword length
    $f \leftarrow$ Sampling frequency
    $q \leftarrow$ Bits generated per gait cycle
function GENBS(ACC,n,f,q)
    $accT \leftarrow \text{PEAK\_DETECTION}(ACC)$
    for i=1 to $length(accT)$-1 do
        $IPI(i) \leftarrow accT(i+1) - accT(i)$
    end for
    $IPI \leftarrow mod(round(IPI/(m \times 1000/f)), 2^q)$
    $grayIPI \leftarrow bin2gray(IPI,'qam', 2^q)$
    $R \leftarrow de2bi(grayIPI,'\text{left-msb}')$
    $[rr, cc] \leftarrow size(R)$
    $reshapeR \leftarrow reshape(R^T, [1\ rr \times cc])^T$
    $S \leftarrow S(1:n)$
    return S
end function
```

R peaks. The selected R peak corresponds to each interval $T_i$ is represented as:

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

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

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

where $\hat{p}_i$ is the final selected peak in the $i^{th}$ gait cycle. During data collection, subjects were instructed to walk at a normal constant speed. However, even at normal speed, temporal variations still exist between each gait cycle, which is the source of the randomness in the generated binary sequences. $\hat{p}_i$ will likely drift from the estimated time $\tilde{t}$ and magnitude $\tilde{y}$ as shown in Fig. 5.20b and 4.3c, which are the two example results of the R peak detection algorithms.

#### 4.1.1.4 Key Generation

Upon receiving the synchronisation signal from the coordinator, all the sensor nodes and the coordinator in the same BSN will start recording 3-axis gait acceleration signals, and the signals will be projected onto the world coordinate system using Eq. 4.1. Then, the R peak detection algorithm will be applied to the acceleration signal $Acc_{-G}$ to find the timing of R peaks $accT$, and the inter-pulse interval $IPI$ is calculated. Next, as $accT$ is in milliseconds, $IPI$ is divided by $m \times \frac{1000}{f_s}$ and a round operation is applied afterwards. Round and modulo operations are also applied to $IPI$ to quantise it into $2^q$ levels. To improve the bit agreement rate, $IPI$ is mapped onto gray coded $grayIPI$ using the Matlab function $bin2gray$, and an integer to binary Matlab function $de2bi$ is applied to $grayIPI$, producing a binary matrix $R^{q \times N}$. Finally, $R^{q \times N}$ is reshaped into $reshapeR^{1 \times q \cdot N}$ using Matlab function $reshape$, and the first $n$ bits are used for generating binary sequence $S$. $n$ is the codeword length used in the BCH scheme. The procedures are summarised in Algorithm 1.

**Algorithm 2** Pseudo code for the network simulation

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

#### 4.1.1.5 Key Distribution And Network Simulation

The fuzzy commitment (Juels and Wattenberg, 1999) was widely adopted in BCSs (Hoang and Choi, 2014; Zheng, Fang, Shankaran, Orgun, and Dutkiewicz, 2014); in comparison to the fuzzy vault scheme, it is less complex and computationally demanding in terms of key concealing and revealing while yielding a superior FAR performance (Zheng, Fang, Orgun, et al., 2015). Therefore, the fuzzy commitment scheme with Bose-Chaudhuri-Hocquenghem (BCH) codes is adopted in the proposed scheme. The network simulation is described in Algorithm 2, illustrating how the key is encoded and decoded by the transmitter and the receiver, respectively. On the transmitter, the secret $K^{5\times k}$ is a randomly generated binary matrix, and it is encoded by BCH codes with the parameters of $(n,k,t)$, where $n$ is the codeword length, $k$ is the length of $K$, and $t$ is the maximum error correction capability of a valid BCH pair $[n,k]$. A codeword length long binary sequence $S$ is generated by the proposed key generation scheme, and an XOR operation is performed between each row of $K_{ecc}$ and $S$ to encrypt the secret $K$ into cipher-text $K_{en}$. On the receiver, an XOR operation is applied to each row of $K_{en}$ and $S'$ to obtain $K'_{ecc}$, which is then decoded by the BCH decoder, producing $K'$. Finally, the bit difference $e$ is calculated by comparing $K'$ and $K$.

Table 4.1: Theoretical maximum security of the generated binary sequences in different sampling frequencies and settings

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

### 4.1.2 Results

Table. 4.1 presents the summary of the settings for achieving theoretical maximum security of the generated binary sequences in different sampling frequencies. The theoretical maximum secure bits generated per gait cycle is calculated as

$$maximum\ secure\ bits = \left\lfloor \frac{\lfloor \overline{\sigma} \rfloor}{m \times \frac{1000}{f_s}} \right\rfloor \tag{4.4}$$

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

Table 4.2: Bit Agreement Rate (BAR) of the generated binary sequences in terms of different m and q settings

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

The results from three experiments are summarised in Table. 4.2. In Experiment I, one iPhone was placed on the lower back while the other one on the front of the waist of 5 test subjects walking in normal speed, and the sampling frequency was 100Hz. In Experiment II, one iPhone was placed on the lower back while the other one was attached to the right upper arm of the subjects with the same settings in Exp. I. In Experiment 3, only one iPhone was placed on the lower back while the e-AR sensor was placed on the right ear of the subjects, and the sampling frequency of 100Hz was used on both devices. The experimental results suggest that scheme with $m$=3 and $q$=4 is the best configuration for the proposed scheme. The bit agreement rates in Exp. III are lower than Exp. I and Exp. II, which is mainly due to the measurement errors introduced by Bluetooth wireless transmission delays, unstable sampling rates, and noise due to head movements. When $m$=10, the system is not able distinguish intra-class keys and inter-class keys.

### 4.1.3 Conclusions

In the first part of this chapter, a novel light-weight symmetric key generation scheme based on the timing information of gait is proposed. The proposed scheme was designed and simulated using Matlab R2016b and analysed the average bit agreement rates between the keys generated during the experiments. With the setting of $m$=3 and $q$=4, the BAR is about 79% (except for Exp. III), which means the encrypted secret $K$ can be corrected by BCH codes ($n$=127, $k$=15, $t$=27). Although the BAR between intra-class keys is high enough for BCH codes to correct, the randomness of the generated keys were not considered in this chapter. When m is set to equal to or greater than 5, the keys generated by the proposed schemes are not sufficiently random to be used for cryptographic operations. In the next chapter, a new scheme is proposed which takes randomness of the keys into full consideration. The future work for the proposed scheme in this chapter can be to expand the database, increase the number of sensor nodes on the subjects, conduct a detailed security analysis, test randomness of the generated keys, and investigate other binary sequence extraction techniques that could utilise all 3-axis acceleration signals.

## 4.2 Gender and Age Recognition using gait signals

Physical biometric traits, such as fingerprint and iris, will not change due to ageing (Villazon, 2018), whereas behavioural biometric traits can often change throughout a person's life (Basaraba, 2019). For instance, a person's voice is often matured and its tune is changed during adolescence. The second part of this chapter explores the effect of gender and ageing on inertial sensor-based gait biometrics. It is not feasible to collect one person's gait biometrics started from young age to old age, therefore, a whole-generation inertial gait database, which consists of more than 700 subjects, is adopted for this study.

In recent years, biometrics has been widely adopted in security applications such as mobile phone authentication. These applications are often focused on the uniqueness of hard biometrics - typical physiological traits, such as face and fingerprint, and behavioural traits, such as gait and voice (Mahfouz, Mahmoud, and Eldin, 2017). Although hard biometrics are the core metrics for biometric systems, much research has shown that soft biometrics, such as age, skin colour, and gender, can also improve the performance of biometric systems (Abreu and Fairhurst, 2011; Dantcheva et al., 2011; Zewail et al., 2004). Soft biometrics, especially gender and age, can also provide personal specific information which could benefit in business, healthcare, robotic, and gaming applications. The state-of-the-art human gender and age recognition methods are often based on the static facial features (Eidinger, Enbar, and Hassner, 2014) or whole body images (Perlin and Lopes, 2015), and dynamic features from voice (Sedaaghi, 2009) and gait (Hediyeh, Sayed, and Zaki, 2013). Gait, the walking pattern of a person, can be captured by a camera from a distance, or captured by inertial sensors attached to the person (Sun, Wong, et al., 2017). Similar to face and iris, a gait pattern of a person is unique because bones, joints and muscles used for walking are very different from person to person.

Gender and age recognition using gait sequences captured by a camera has gained more popularity in the past few years. For example, Li, Maybank, et al. (2008) proposed a vision-based gender recognition method using different components of human walking silhouettes, and Makihara et al. (2011) proposed a vision-based age estimation method also using human walking silhouettes. Vision-based gender and age recognition is robust and effective in a controlled environment, such as a situation where a person walking in front of a camera at a fixed location. It is difficult to extract gait silhouettes

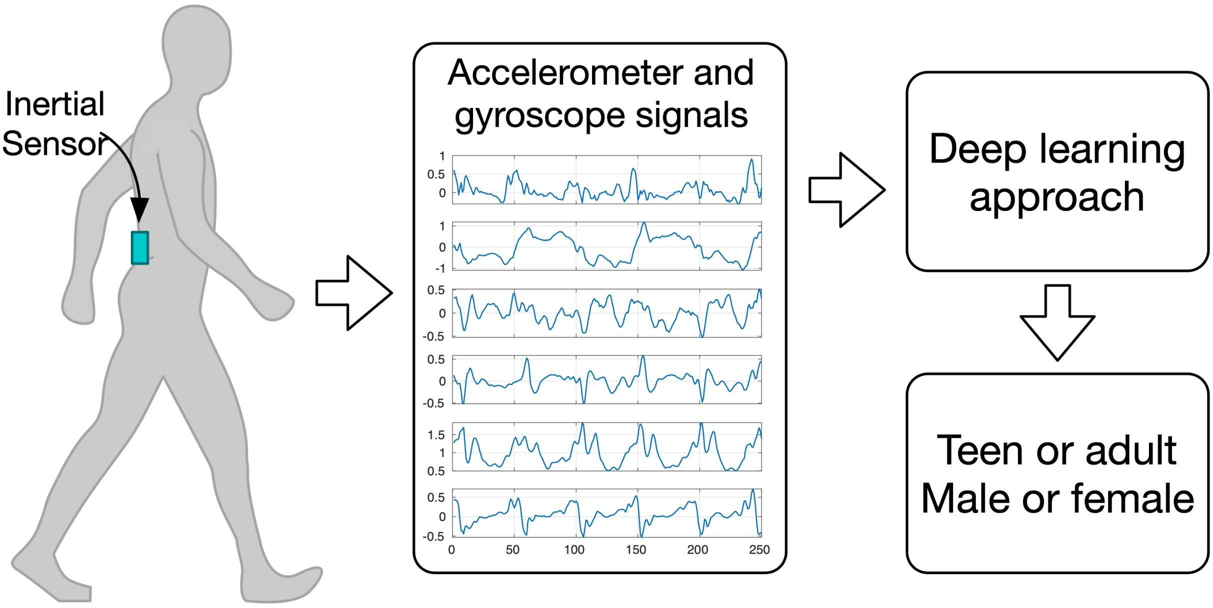


Figure 4.4: Illustration of the proposed inertial sensor-based gender and age recognition approach

if the target subject is occluded by another person or objects. These problems can be solved by using inertial sensors to capture gait biometrics. Although inertial sensors have to be attached to or carried by the person, they can be used in uncontrolled environments, such as a group of people walking closely together in a pedestrian area, a situation where vision-based approaches could not be applied.

Although inertial sensor-based gait biometrics is widely used for authentication, it has not been fully exploited for gender and age recognition. Riaz et al. (2015) studied the estimation of gender, age and height using a trained random forest classifiers with hand-crafted features of single-step inertial signal recordings. The dataset collected by the authors consisted of only 26 subjects with a balanced gender ratio and an averaged age of 48.1±12.7 years. The authors have demonstrated the feasibility of gender and age recognition using inertial sensors on a small population using 10-fold cross validation. But the hand-crafted feature extraction technique used by the authors suffered significant performance drop (from over 85% to around 65%) when using inter-subject cross validation for age estimation, failing to show the robustness of the proposed approach.

Furthermore, Jain and Kanhangad (2018) studied gender classification using a built-in inertial sensors of smartphones when users are walking at different speeds. The authors also used hand-crafted features in the proposed approach, and tested it on two datasets containing 46 and 63 subjects separately. The subjects in these datasets are mostly adults and age from 19 to 36 years, and people younger than

19 years or older than 36 years were not considered in the experiments. Another related work carried out by Bales et al. (2016) also based on inertial sensors, however, the sensors were installed beneath the floor of a building instead of attaching to the body. The authors proposed a machine learning based gender classification approach using data collected from only fifteen subjects.

In the second part of the chapter, a deep learning approach is proposed for gender and age recognition using a single inertial sensor attached to the lower back of the subjects. Deep learning approaches are widely exploited in vision-based gender recognition, but to the best of our knowledge, it has not been used for inertial sensor-based gender and age recognition. The proposed approach was evaluated on the largest inertial sensor-based gait database available (Ngo et al., 2014), which has inertial data collected from 744 subjects. 640 out of 744 subjects (whose gender information is provided) with a gender ratio of 1:1 and age range from 2 to 79 years, were used in the experiments. 10 trials of inter-subject Monte-Carlo cross validation were carried out for all the experiments to demonstrate the robustness and effectiveness of the proposed approach.

### 4.2.1 Methodology

As shown in Fig. 4.4, the proposed deep learning-based age and gender recognition approach requires only a single inertial sensor attached to the lower back of the subject. The deep learning approach consists of three blocks as shown in Fig. 4.5: a signal pre-processing block, a convolutional feature extraction block, and a fully connected classifier. In the signal pre-processing block, a sliding window is applied to the accelerometer and gyroscope signals collected from the inertial sensor. Then, the partitioned signal data is fed into the convolutional feature extraction block to extract features inside each sliding window. At last, a 2-class fully connected classifier will then classify either teen or adult, or male or female.

#### 4.2.1.1 Convolutional Feature Extraction

The partitioned signal data fed into the first layer is in a 3D matrix form of $(B \times W \times N)$, in which batch size $B = 10$, sliding window size $W = 100$ (which is 1 second), and the number of channels

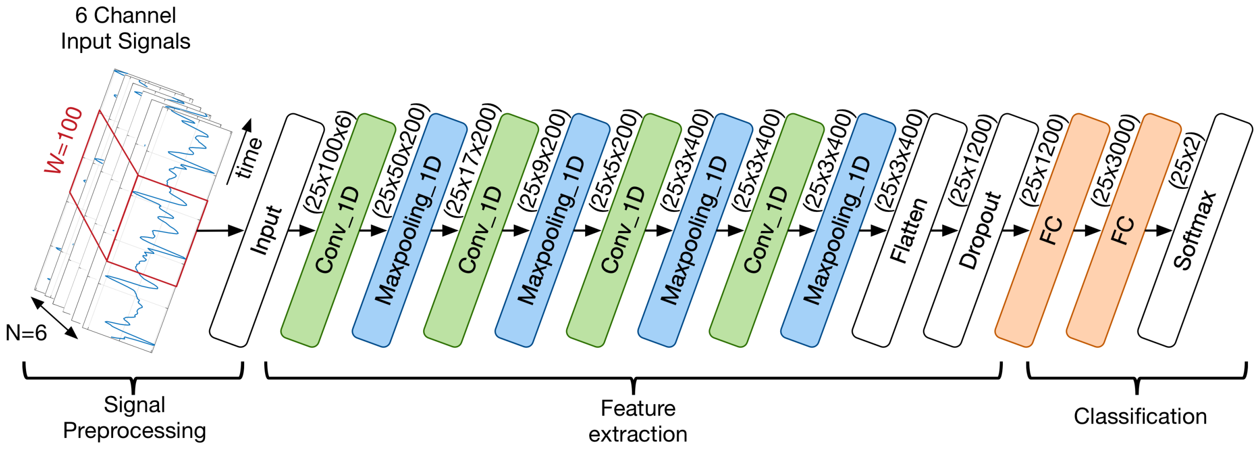


Figure 4.5: Network architecture of the proposed deep learning approach

$N = 6$ (i.e. 3-axis accelerometer and 3-axis gyroscope data). In the first 1D convolutional layer, there are 200 filters/kernels with kernel size set to 5 and stride set to 2. The output feature map of the first convolutional layer has a shape of $25 \times 50 \times 200$, and it is fed into a max pooling layer whose pool size is set to 2 and stride is set to 3. The dimension of feature map is reduced based on the maximum value of each pool, and its shape is reduced to $(25 \times 17 \times 200)$. The same feature extraction procedure is repeated 3 more times as indicated in Fig. 4.5. The mathematical expression of the output feature maps of $l^{th}$ $(l = [1,2,3,4])$ 1D convolutional layer is

$$\theta^l = \left[\gamma_1^l(j), \gamma_2^l(j), \gamma_3^l(j), \cdots, \gamma_m^l(j)\right] \tag{4.5}$$

and feed forwarding process for each neuron is

$$\gamma_m^l(j) = \beta^l(j) + \sum_{i=1}^{i \leq K^l} (\theta_{i,j}^{l-1} w_1(l,m,i) + \theta_{i,j+1}^{l-1} w_2(l,m,i)) \tag{4.6}$$

where $\gamma_m^l(j)$ is the $j^{th}$ neuron in the $m^{th}$ kernel of the $l^{th}$ 1D convolutional layer, and $w_k(l,m,i)$ refers to the weights of the $l,m,i^{th}$ filter used in the neural network. $\beta^l(j)$ is the bias of the $j^{th}$ neuron in the $l^{th}$ 1D convolutional layer. $K^l$ is the number of kernel being used in the $l^{th}$ 1D convolutional layer, and $\theta_{i,j}^l$ is the $i,j^{th}$ element of the output feature maps from the max pooling layer following the $(l-1)^{th}$ 1D convolutional layer. The output of the final max pooling layer is flatten to a shape of $(25 \times 1200)$, and it passes through a dropout layer with a keep probability of 0.95 to prevent overfitting. Then, the

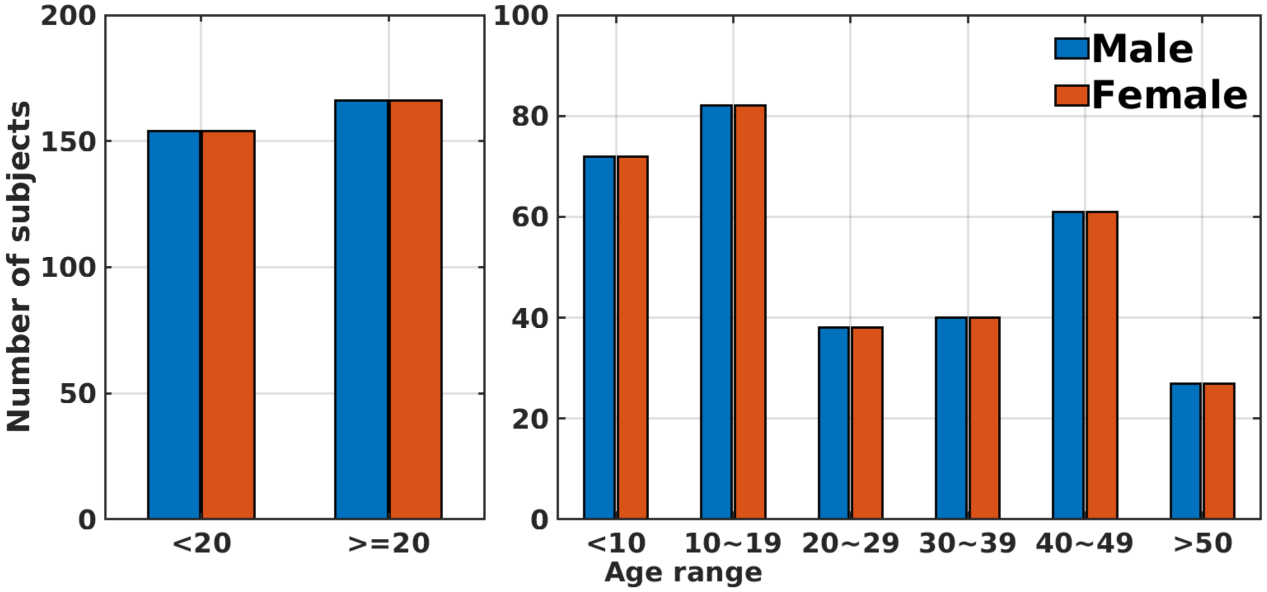


Figure 4.6: Distributions of gender and age of the selected subjects from the OU-ISIR gait database

final feature map is fed into a classifier with two fully connected layers to produce the final output, which is the probabilities of the two classes (teen/adult or male/female). The softmax layer at the end calculates the loss, which is used for optimising the neurons of the network in the training phase.

#### 4.2.1.2 Database

To evaluate the proposed gender and age recognition approach on the whole generation, the largest available inertial sensor-based OU-ISIR gait database (Ngo et al., 2014) was used in the experiments. To ensure a balanced gender ratio in all age groups, we followed protocol 5.6, in which 640 subjects are selected. The distributions of gender and age of the selected subjects as shown in Fig. 4.6. The subplot on the left side shows the number of subjects of teens and adults respectively, and the subplot on the right side shows the number of subjects for 6 age groups. Each subject has two sequences of level walking inertial sensor recordings, which contains about 7 to 12 steps.

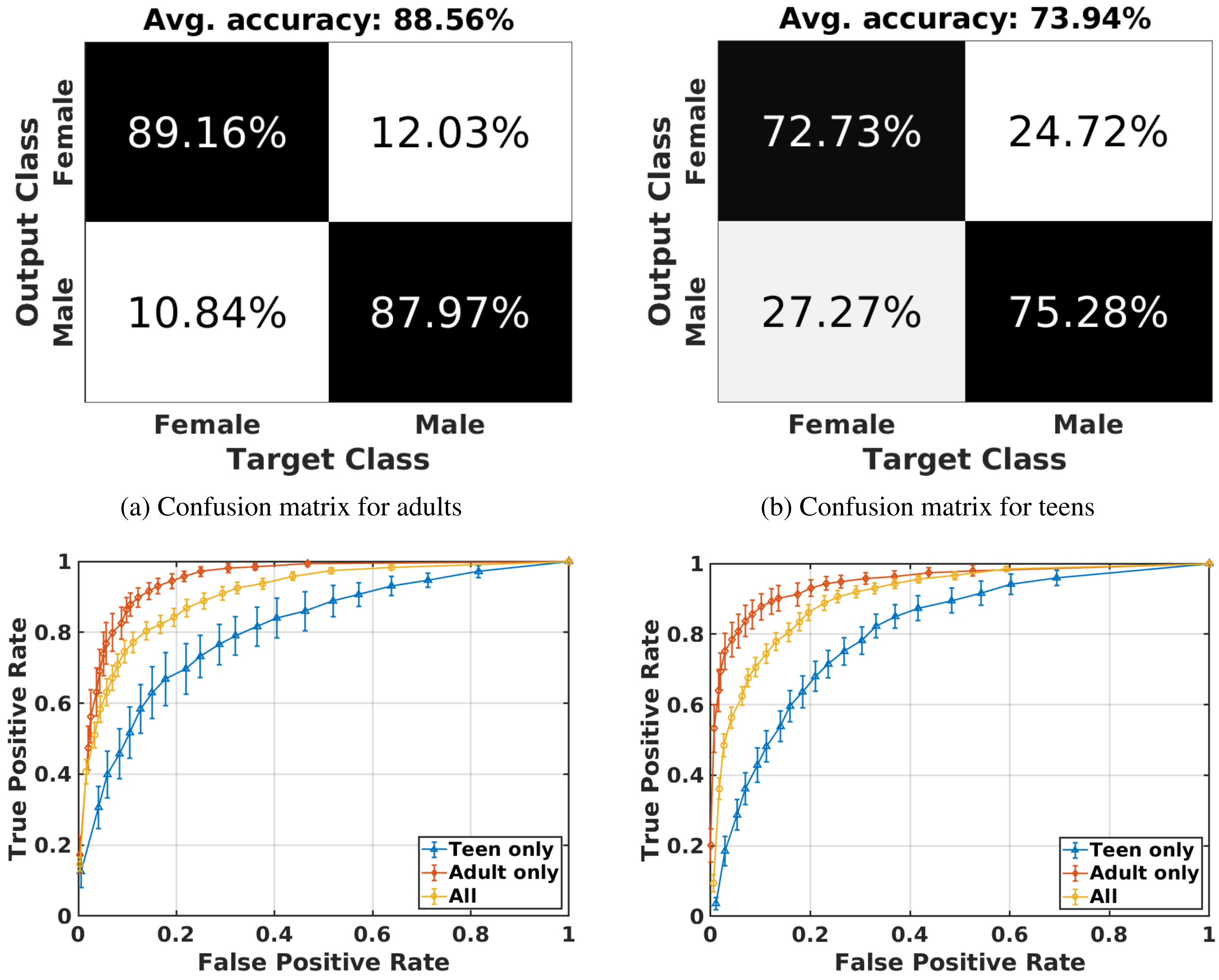
#### 4.2.1.3 Training and Testing

To demonstrate the robustness and effectiveness of the proposed approach, inter-subject Monte-Carlo cross validation was carried out 10 times, and the means and standard deviations of the results across 10 trials are presented in the experimental results section for both gender and age recognition. For age recognition, there were two classes: teen (age<20) and adult (age≥20). In each trial, 70% of the subjects in each class were randomly selected for training, and the rest was reserved for testing. For gender recognition, two experiments were carried out: 1) in the first experiment, all the subjects, either teens or adults, were trained in the same network; 2) in the second experiment, gender recognition for teens and adults was carried out using two separate networks (i.e. a subject who is below 20 will not be considered at all in the network for recognising gender for adults).

In addition, the data of the selected testing subjects were not used for training the network, which eliminates the possibilities of over-fitting the network for better testing results. It can be also proven that the proposed approach is capable of recognising gender and age of subjects from other dataset with high accuracy. As shown in Fig. 4.5, a sliding window is applied to partition the sequences of inertial sensor recordings into slices of data with shape 100×6. Then, a batch of 25 slices is fed into the network together in each iteration. The initial learning rate of the network is set to 0.001, and it decays by 4% after every 10 thousand iterations. The weights and biases in the convolutional and fully connected layers are randomly initialised and optimised using ADAM optimisation algorithm (Kingma and Ba, 2014), and the training process is stopped when reaching 5 epochs.

### 4.2.2 Experimental Results

In this section, the performance of the proposed approach is presented, using evaluation matrices for typical biometric systems, including confusion matrices and ROC curves. The recognition performance per sliding window and per recording was reported using accuracy, sensitivity, specificity, and F1-score, which are averaged across 10 trials. In addition, the proposed approach was also compared with conditional machine learning approaches using hand-crafted features, which are listed in Table 4.7. Five classic machine learning classifiers were selected for comparative studies: Fine Tree, Linear SVM, Quadratic SVM, Fine KNN, and Boosted Tree.



(a) Confusion matrix for adults

(b) Confusion matrix for teens

(c) ROC curves for female

(d) ROC curves for male

Figure 4.7: Experimental results for gender recognition: (a) and (b) show confusion matrices (sum up for 10 trials) for adult-only and teen-only respectively. (c) and (d) show ROC curves for female class and male class separately, with point-wise confidence bounds calculated for 10 trials

Table 4.3: Gender recognition results (averaged for 10 trials)

| | | Accuracy | Sensitivity | Specificity | F1-score |
|---|---|---|---|---|---|
| per recording | Teen | 0.739±0.028 | 0.766±0.092 | 0.713±0.066 | 0.744±0.043 |
| | Adult | **0.886±0.025** | **0.878±0.053** | **0.893±0.058** | **0.885±0.026** |
| | All | 0.828±0.028 | 0.822±0.040 | 0.833±0.042 | 0.827±0.029 |
| per sliding window | Teen | 0.702±0.017 | 0.728±0.074 | 0.676±0.058 | 0.706±0.033 |
| | Adult | 0.836±0.016 | 0.821±0.055 | 0.853±0.052 | 0.837±0.019 |
| | All | 0.787±0.015 | 0.788±0.036 | 0.787±0.028 | 0.790±0.019 |

#### 4.2.2.1 Gender Recognition

As aforementioned, there are two experiments conducted for gender recognition using the proposed approach: the first one using the entire dataset and the second one splits the dataset into teen group and adult group for separate training. This is to investigate how the age of the subject affects the performance of the proposed approach on gender recognition. Fig. 4.7(a) and (b) show confusion matrices for gender recognition using adult-only dataset and teen-only dataset respectively. The proposed approach can distinguish gender for adults (age≥20) with an averaged accuracy of 88.56% across 10 trials, whereas it performs poorly, with only an averaged accuracy of 73.94% for teens. This is expected because the muscle and bones of teens are still growing, which makes their gait less predictive.

In addition, female is more recognisable then male for adults, and male is more recognisable than female for teens. Fig. 4.7(c) and (d) show the ROC curves for the proposed approach for gender recognition, and they also indicate that gender is more distinctive for adults than teens. More details for the gender recognition performance are listed in Table 4.3, where accuracy, sensitivity, specificity, and F1-score for teen-only, adult-only, and all age group across 10 trials are presented. The results for each inertial data recording, which contains about 5 to 10 steps, are aggregated from the recognition results from each sliding window. Therefore, accuracy per recording is better than that of per sliding window.

Table 4.4: Age recognition results (averaged for 10 trials)

| | | Accuracy | Sensitivity | Specificity | F1-score |
|---|---|---|---|---|---|
| per recording | Female | 0.843±0.028 | 0.785±0.033 | 0.896±0.054 | 0.827±0.028 |
| | Male | **0.887±0.026** | **0.913±0.029** | **0.864±0.037** | **0.885±0.026** |
| | All | 0.866±0.024 | 0.849±0.025 | 0.880±0.042 | 0.857±0.023 |
| per sliding window | Female | 0.775±0.025 | 0.728±0.050 | 0.814±0.052 | 0.743±0.027 |
| | Male | 0.830±0.019 | 0.867±0.026 | 0.798±0.033 | 0.827±0.019 |
| | All | 0.802±0.019 | 0.798±0.031 | 0.806±0.040 | 0.787±0.018 |

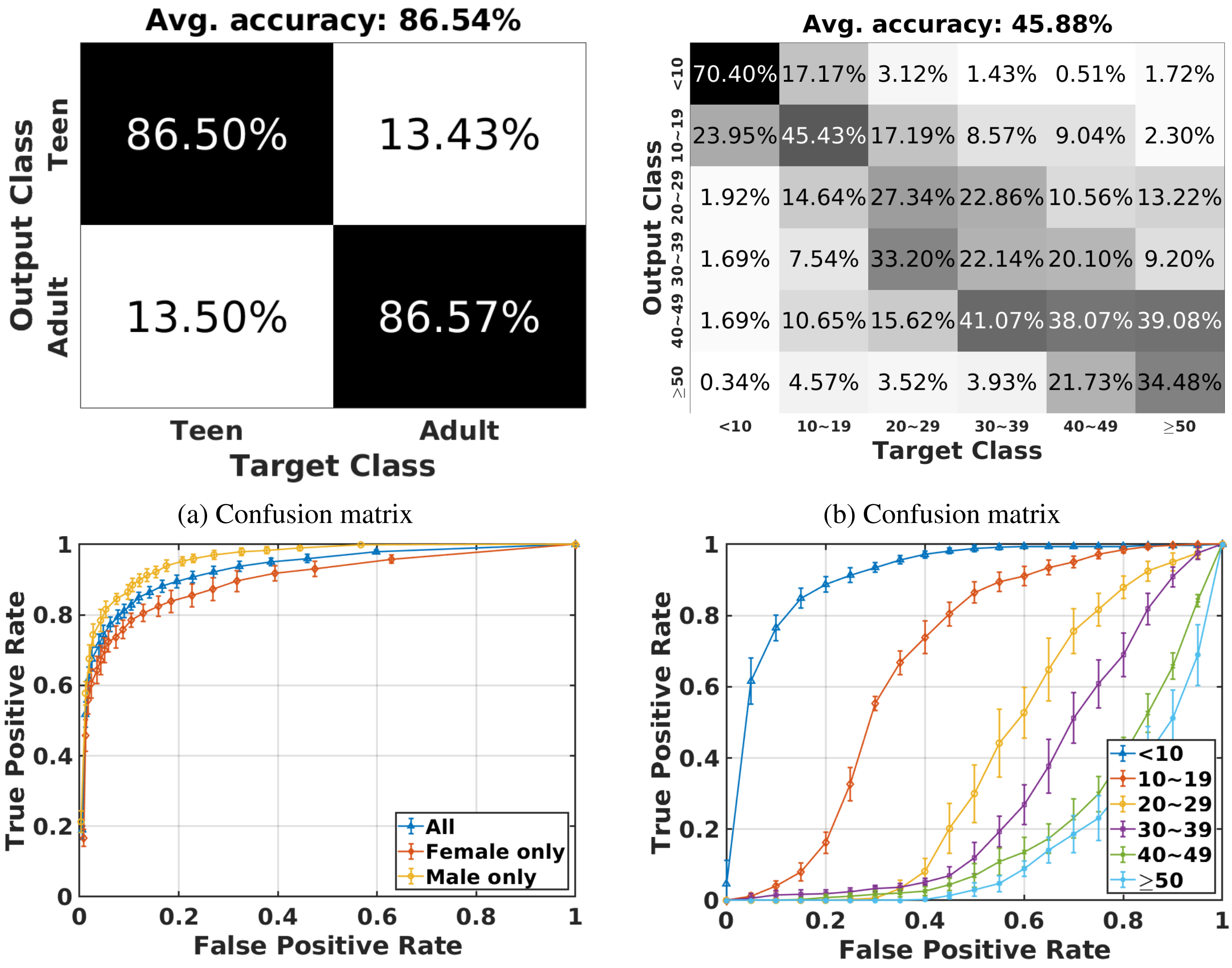
#### 4.2.2.2 Age Recognition

The proposed approach is capable of distinguishing two age groups: teen and adult. The confusion matrix in Fig. 4.8(a) show that the average accuracies for teens and adults are 85.50% and 86.57% respectively. It indicates that proposed approach has no bias towards either age group. Fig. 4.8(c) shows the ROC curves of the age recognition for all the subjects, female subjects, and male subjects. The proposed approach performs better for age recognition on male subjects than female subjects. This is also shown in Table 4.4, where the age recognition accuracy of male subjects per recording is 88.7%, 4.4% higher than that of female subjects. Moreover, age recognition using the proposed approach for male subjects has higher sensitivity but less specificity than female subjects.

Another experiment was conducted on age recognition using proposed approach with 6 classes: $<10$, 10 to 19, 20 to 29, 30 to 39, 40 to 49, and $\geq 50$. The confusion matrix is shown in Fig. 4.8(b), where the averaged accuracy for all classes is 45.88%. The misclassification mostly happens between the two teen classes, and among four adult classes. A possible explanation is that once a person has reached adulthood, his or her gait remains mostly unchanged if healthy. But there are changes in gait with age as the proposed approach can distinguish gaits with higher accuracy when the age gap between two groups is larger. Fig. 4.8(d) shows the ROC curves for different classes. It can be seen that the two teen classes have much better performance than the other four adult classes.

#### 4.2.2.3 Comparative Study

To test the effectiveness of the proposed approach, comparative studies against traditional machine learning approaches were conducted, and the hand-crafted features selected for the comparison are



Avg. accuracy: 86.54%

| Output Class \ Target Class | Teen | Adult |
|---|---|---|
| Teen | 86.50% | 13.43% |
| Adult | 13.50% | 86.57% |

(a) Confusion matrix

Avg. accuracy: 45.88%

| Output Class \ Target Class | <10 | 10~19 | 20~29 | 30~39 | 40~49 | ≥50 |
|---|---|---|---|---|---|---|
| <10 | 70.40% | 17.17% | 3.12% | 1.43% | 0.51% | 1.72% |
| 10~19 | 23.95% | 45.43% | 17.19% | 8.57% | 9.04% | 2.30% |
| 20~29 | 1.92% | 14.64% | 27.34% | 22.86% | 10.56% | 13.22% |
| 30~39 | 1.69% | 7.54% | 33.20% | 22.14% | 20.10% | 9.20% |
| 40~49 | 1.69% | 10.65% | 15.62% | 41.07% | 38.07% | 39.08% |
| ≥50 | 0.34% | 4.57% | 3.52% | 3.93% | 21.73% | 34.48% |

(b) Confusion matrix

(c) ROC curves

(d) ROC curves

Figure 4.8: (a) and (b) show the confusion matrices of 10 trials for 2-class and 6-class age recognition. (c) shows the ROC curves for all, female-only and male-only respectively for 2-class age recognition, whereas (d) shows the ROC curves for 6-class age recognition (all subjects) results, with point-wise confidence bounds calculated across 10 trials

Table 4.5: Comparative studies on gender recognition per sliding window on subjects of all age using the proposed approach and five machine learning classifiers with hand-crafted features listed in Table 4.7.

| | Accuracy | Sensitivity | Specificity | F1-score |
|---|---|---|---|---|
| Fine Tree | 0.570±0.018 | 0.658±0.040 | 0.478±0.041 | 0.607±0.022 |
| Linear SVM | 0.652±0.012 | 0.659±0.008 | 0.646±0.020 | 0.658±0.011 |
| Quadratic SVM | 0.627±0.012 | 0.640±0.017 | 0.614±0.013 | 0.635±0.014 |
| Fine kNN | 0.544±0.009 | 0.567±0.013 | 0.512±0.011 | 0.557±0.011 |
| Boosted Tree | 0.614±0.016 | 0.649±0.022 | 0.579±0.024 | 0.630±0.016 |
| **Proposed** | **0.787±0.015** | **0.788±0.036** | **0.787±0.028** | **0.790±0.019** |

Table 4.6: Comparative studies on age recognition (two classes: teen and adult) per sliding window on all the subjects using the proposed approach and five machine learning classifiers with hand-crafted features.

| | Accuracy | Sensitivity | Specificity | F1-score |
|---|---|---|---|---|
| Fine Tree | 0.653±0.019 | 0.605±0.061 | 0.694±0.058 | 0.614±0.028 |
| Linear SVM | 0.714±0.023 | 0.631±0.038 | 0.785±0.041 | 0.669±0.025 |
| Quadratic SVM | 0.717±0.016 | 0.688±0.029 | 0.743±0.033 | 0.690±0.017 |
| Fine kNN | 0.635±0.011 | 0.626±0.025 | 0.642±0.027 | 0.611±0.013 |
| Boosted Tree | 0.693±0.022 | 0.619±0.047 | 0.755±0.043 | 0.648±0.027 |
| **Proposed** | **0.802±0.019** | **0.798±0.031** | **0.806±0.040** | **0.787±0.018** |

listed in Table 4.7. These features were also used in (Riaz et al., 2015), in which hand-crafted features were extracted per step. In the proposed approach, gait cycle detection is not required, therefore, the feature extraction process was applied per sliding window with a window size of $W = 100$ and a stride of $S = 5$. For example, as inertial signals in a sliding window has a shape of (100×6), the calculations of features will be applied to each of the 6 channels individually, results in a total of 7×6 features per sliding window.

Table 4.5 presents the accuracy, sensitivity, specificity, and F1-score of the five classic machine learning classifiers and the proposed deep learning approach on gender recognition for subjects of all age. Linear SVM has the best performance out of five classifiers, having a averaged accuracy of 65.2%±1.2%, which is 13.6% lower than that of the proposed approach. Table 4.6 presents the age recognition results for distinguishing teens and adults, and Quadratic SVM has the best accuracy at 71.7%±1.6% out of the five classifiers, whereas the proposed approach has 8.5% higher accuracy. Both comparative studies on gender and age recognition show that the proposed deep learning approach performs much better than classic machine learning approaches with hand-crafted features.

Table 4.7: Hand-crafted features for each of the 3 axes of the acceleration signal and 3 axes of the gyroscope signal for each sliding window

| Feature Name | Mathematical Equation | Total |
|---|---|---|
| Mean | $\bar{x} = \frac{1}{N}(\sum_{i=1}^{N} x_i)$ | 6 |
| Standard Deviation | $s = \sqrt{\frac{\sum_{i=1}^{N}(x_i-\bar{x})^2}{N-1}}$ | 6 |
| Minimum | $min(x_i)$ | 6 |
| Maximum | $max(x_i)$ | 6 |
| Root Mean Square | $x_{rms} = \sqrt{\frac{1}{N}(\sum_{i=1}^{N} x_i^2)}$ | 6 |
| Shannon Entropy | $E = -\sum_{i=1}^{N} x_i^2 log(x_i^2)$ | 6 |
| Signal Energy | $\delta = \sum_{i=1}^{N} x_i^2$ | 6 |

### 4.2.3 Conclusion

The proposed deep learning approach on gender and age recognition using a single inertial sensor demonstrated that a person's gait is unlikely to change once becoming an adult. Also, gender information can be very useful to the biometric security systems for better recognition performance. The results from 10 trials of inter-subject Monte-Carlo cross validation show that the proposed approach is robust and effective. The proposed approach is capable of recognising either teen or adult with an averaged accuracy of 86.6%±2.4%, and recognising gender with averaged accuracies of 88.6%±2.5% and 73.9%±2.8% for adults and teens separately.

## 4.3 Summary

In this chapter, gait biometrics has been studied in two ways: to generate secret keys for data encryption, and to extract gender and age information of users for user authentication. The symmetric key generation scheme presented in the first part of this chapter is a light weighted approach, which can be used on low-power sensor nodes. Whereas the deep learning based gender and age recognition approach proposed in the second part of this chapter cannot be used directly on the sensor nodes. It is designed to be used on smart phones or cloud servers for user authentication purposes.

# Chapter 5

# Improved Body Sensor Network Security using Gait and ANN Frameworks

The gait timing based light-weight symmetric cryptosystem proposed in previous chapter still suffers issues like low intra-class key matching rates and long key generation time. To improve the proposed gait-based symmetric cryptosystem, this chapter focus on developing an ANN framework to increase the correlations among gait signals from different body positions. The proposed ANN framework is first designed and developed to estimate lower limb motion using foot mounted inertial sensor signals in the first part of this chapter, and then the ANN framework is added in the proposed gait-based cryptosystem as a signal processing block to improve the performance of the system. The work presented in this chapter has been published in (Sun and Lo, 2018b; Sun, Yang, and Lo, 2018).

## 5.1 Gait Signal Estimation using Minimal Inertial Sensors

To tackle the challenge of insufficient correlation among gait signals from different body positions, this chapter is focused on solutions based on artificial intelligence. First of all, a method of estimating on-body sensor signals (motion signals) at one body position from another sensor at different body position is required to improve the correlation of signals captured by sensors on different locations. With this objective, the first part of this chapter explores sensor reduction technique for lower limb motion signal estimations.

Lower limb kinematics play an important role in gait analysis. Conventionally, lower limb motion tracking has been carried out by marker-based optical motion capture systems, such as Vicon (Vicon, 2017), where subjects are required to wear reflective markers which can be detected and tracked by infrared cameras. Alternatively, markerless motion capture systems, such as Microsoft Kinects (Patrizi, Pennestri, and Valentini, 2016), provide a low-cost and less cumbersome solution but with more noise and less accurate. Although both marker-based and markerless systems can track lower limb motion in real-time, they can only be performed in an indoor controlled environment (i.e. no infrared reflective materials) and the subjects have to stay within the range of the cameras.

With the continuous development of micro-electro-mechanical systems, Inertial Measurement Units have been miniaturised and are able to be worn by the users to measure acceleration and angular velocity signals directly (Li, Liu, et al., 2014; Tadano, Takeda, and Miyagawa, 2013; Wang and Ji, 2015).

With such miniaturised wearable IMUs, lower limb motion tracking and gait analysis can be performed in free living environments. Much research has proposed the use of IMU-based motion tracking systems for lower limb motion capture and gait analysis. For example, Tadano, Takeda, and Miyagawa (2013) proposed a low-cost IMU-based system that requires 7 IMUs to be attached to subjects' shins, thighs, feet, and waist, to obtain the entire lower limb kinematics. Similarly, a magnetic and inertial sensor based system was proposed in (Agostini et al., 2015), where ankle, knee and hip kinematic parameters can be measured using 7 IMUs on the predefined positions. Furthermore, Ahmadi et al. (2016) proposed a 3D gait reconstruction method using 7 wireless IMUs with kinematic model adjustment. It was further indicated that, with customised kinematic models, the entire body motion can be reconstructed using only IMU-based systems.

However, the aforementioned IMU-based systems are still cumbersome due to the required number of wearable IMUs. Typically, at least one IMU is attached to each body segment for calculating the relative position and orientation of two adjacent body segments (Seel, Schauer, and Raisch, 2012). Many studies have shown the feasibility of reducing the number of IMUs required for obtaining lower limb kinematics. For instance, Hu and Soh (2014) proposed a 2D gait model with inverse kinematics to estimate planar gait kinematics using only four IMUs attached to the pelvis and heels. In this model, knee joint gait parameters, which are not directly measured, can be estimated using acceleration and angular velocity signals measured by the IMUs at the pelvis and heels.

In the first part of this chapter, a novel sensor reduction method is proposed for estimating lower limb motion signals and real-time gait analysis with an artificial neural network (ANN) framework. After training the ANNs, the method can estimate the shin, thigh, and waist motion signals from only two IMUs attached to the feet or ankles, thus reducing the number of IMUs required for the estimation of lower limb motion signals for gait analysis applications.

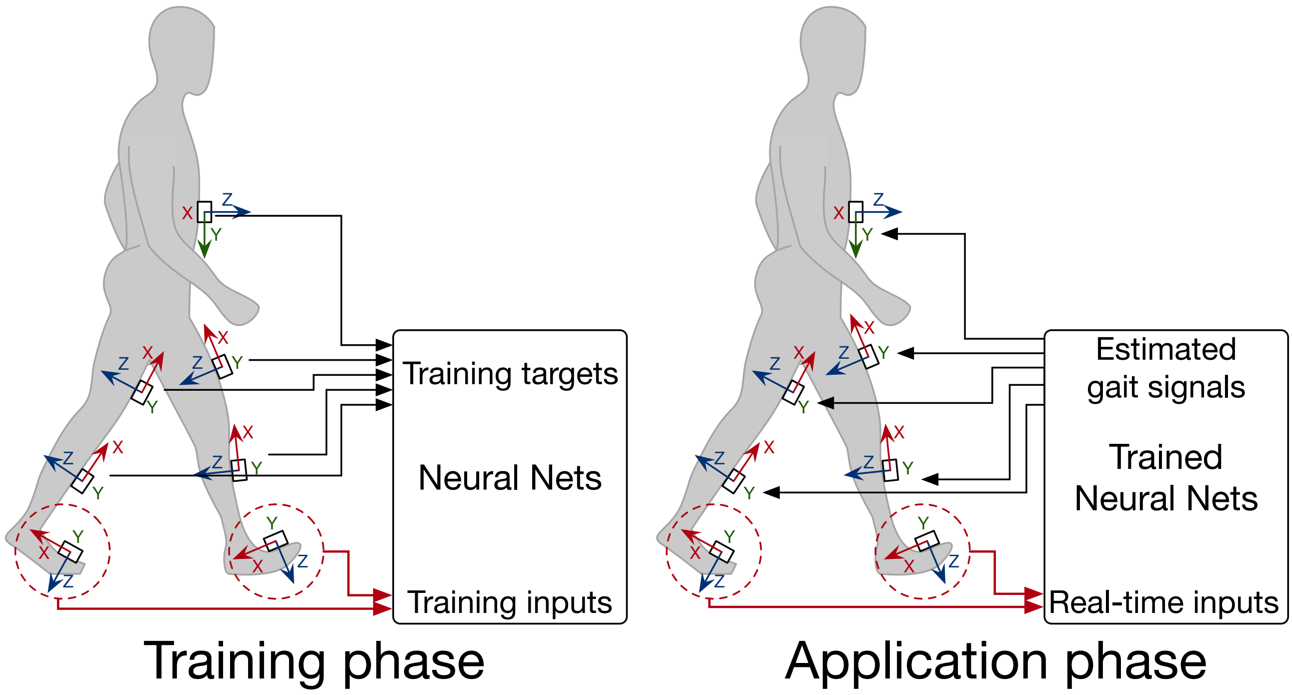


Figure 5.1: Training and application phases

### 5.1.1 Methodology

In this section, the experimental setup, ANN-based gait signal estimation, and gait parameter estimation are presented in detail. As illustrated in Fig. 5.1, there are two phases, namely a training phase and an application phase, in the proposed method. In the training phase, the ANNs are trained using the gait signals recorded by the IMUs attached to the shoes to estimate gait signals of sensors positioned at other locations, including left and right shin, thigh, and the centre of the waist. In the

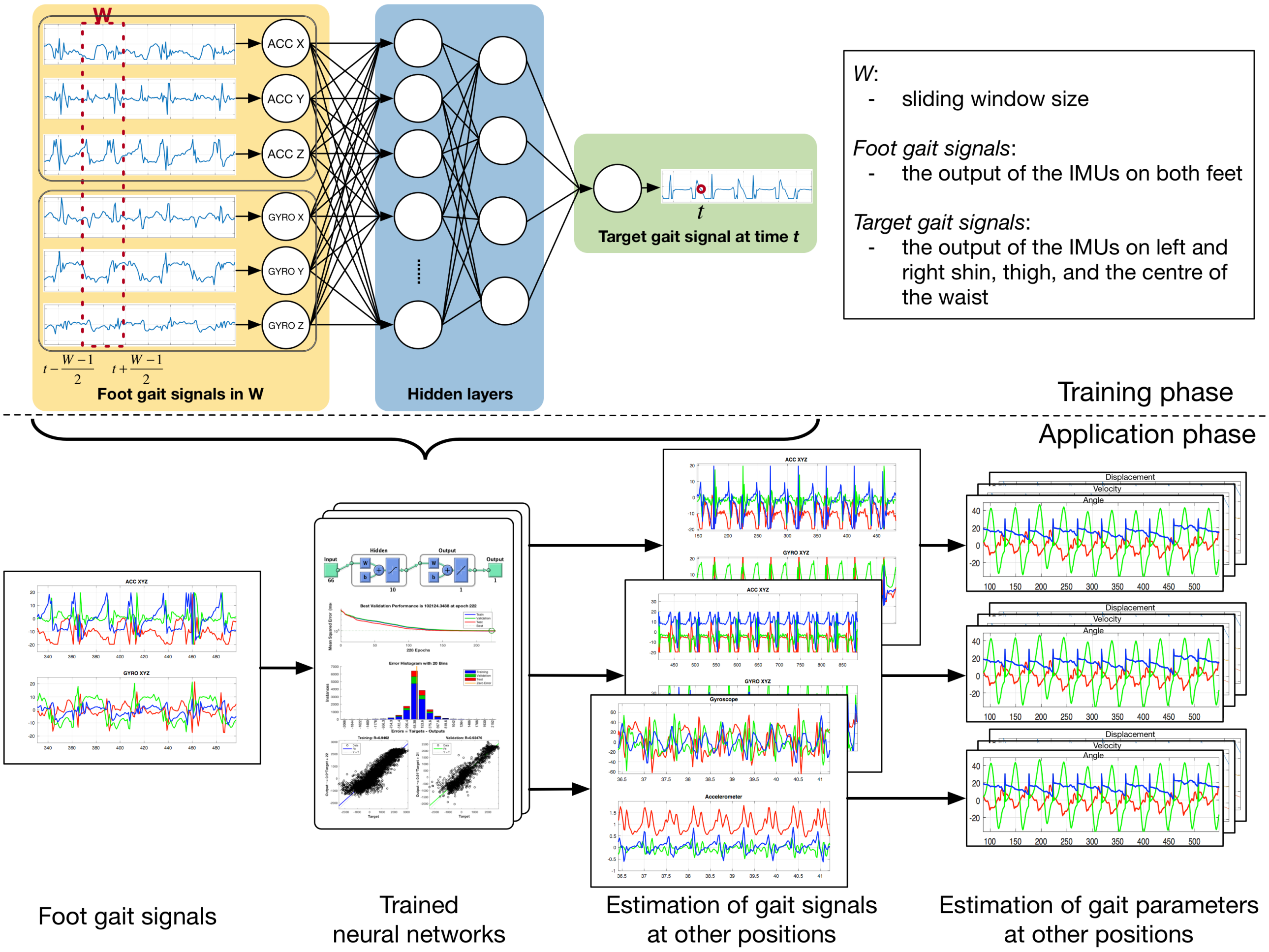


Figure 5.2: Illustration of estimating shin, thigh, and waist gait signals from foot gait signals using the ANN framework

application phase, the proposed method uses the trained ANNs to estimate gait signals of the lower limbs using only the IMU signals on both feet in real-time.

#### 5.1.1.1 ANN-Based Gait Signal Estimation

In the experiment, 1 multiple outputs or 6 single output feed-forward ANNs with 10 hidden nodes were used for each target position, as depicted in Fig. 5.2, to demonstrate the feasibility of the proposed method. Training data are obtained from the output of the N Degree-of-Freedom (DoF) IMUs attached onto the feet, which can be represented as $m_i, \forall i \in \{1, 2, ..., N\}$. For instance, if a 6DoF IMU is applied, where $N = 6$, $m_1$, $m_2$, and $m_3$ will represent accelerometer output on X, Y, and Z axes, and $m_4$, $m_5$, and $m_6$ will represent gyroscope output on X, Y, and Z axes. In terms of the format of the training inputs and training target, for each time instant $t$, a sliding window, which is denoted as $w(t)$, is applied to each IMU output $m_i$ at the foot positions, and the size of the sliding window is $W$. On the other hand, training target can be either single target IMU output, $y(t)$, or multiple target IMU outputs, $y_u(t), u = 1,2,...,N$, at the time instant $t$. The single-output-neural-net (SONN) and multiple-output-neural-net (MONN) are both implemented and compared in the results section. Target IMUs refer to the IMUs placed at other positions, including left and right shin, thigh, and the centre of the waist. In Fig. 5.2, the red dash-line rectangle indicates the sliding window $w(t)$ at the time instant $t$, given by

$$m_i(w(t)), w(t) \in [t - \frac{W-1}{2}, t + \frac{W-1}{2}] \tag{5.1}$$

where $i = 1,2,...,N$, and the red circle indicates the target IMU reading at the instant $t$ in single target IMU output setting. Then, the training input, denoted as $x(t)$, at the time instant $t$ is the concatenation of all the $m_i(w(t))$

$$x(t) = [m_1(w(t)), m_2(w(t)), ..., m_N(w(t))]^T \tag{5.2}$$

where $t = 1,2,...,M$ and M is the number of time instant in the recording. The entire training input set can be expressed as

$$\mathbb{X} = [x(1), x(2), ..., x(M)] \tag{5.3}$$

whereas the training target set is

$$Y = [y(1), y(2), ..., y(M)] \tag{5.4}$$

#### 5.1.1.2 Experimental Setup

The proposed method was implemented and evaluated in Matlab R2017b on a PC, and the data for training and testing the method was from two publicly available gait databases: HuGaDB (Chereshnev and Kertesz-Farkas, 2017) and MAREA (Khandelwal and Wickstrom, 2017). HuGaDB gait database, collected by Chereshnev and Kertesz-Farkas (2017), consists of many human activity recordings. In our experiment, only the walking dataset, which has 192 minutes gait signals collected from 18 subjects with 6 IMUs (placed on the right and left thighs, shins, and feet) during walking on a flat surface, was used. As each subject has multiple recording sessions, we used the first session of each subject for training of the ANNs and used the remaining sessions of each subject for evaluation.

MAREA gait database comprises of gait signal recordings from 20 subjects with 4 IMUs (placed on the right and left ankles, waist, and wrist) in various activities, including treadmill, indoor flat space, and outdoor streets. There is only one section for each subject, thus, the three quarters of the section was used for training and the rest of the section was used for evaluation. The reason why we used MAREA gait database is to evaluate the proposed method in estimating gait signals on the waist (centre of mass) position from the gait signals on the ankle positions.

#### 5.1.1.3 Gait Parameter Estimation

In this section, the algorithms for calculating gait parameters, namely angle, velocity, and displacement, are presented. For the ease of explanation, the notations of the gait signals and gait parameters are listed in Table. 5.1. To reduce the drift effect, acceleration and angular velocity is reset to zero at the beginning of each gait cycle for all IMUs.

Table 5.1: Notation

| Gait signal | Notation | Gait parameter | Notation |
|---|---|---|---|
| Acceleration | $a$ | Angle | $\theta$ |
| Angular velocity | $\omega$ | Velocity | $v$ |
| Magnetic field | $B$ | Displacement | $d$ |

**Gait Cycle Detection** The gait cycle detection algorithm is adopted from (Sun, Wong, et al., 2017), where a low pass filter is applied to the gait signals as shown in Fig. 5.3. The blue signal is the z-axis gyroscope signal $\omega_z$ at the left foot position, the black dash signal is the filtered $\omega_z$, and the red vertical lines are the boundaries between gait cycles.

**Angle, Velocity, and Displacement Estimation** The estimated angle $\hat{\theta}(t)$ is the integral of the estimated angular velocity $\hat{\omega}(t)$ of an IMU, given by

$$\hat{\theta}(t) = \int_0^t \hat{\omega}(\tau) d\tau + \hat{\omega}(0) \tag{5.5}$$

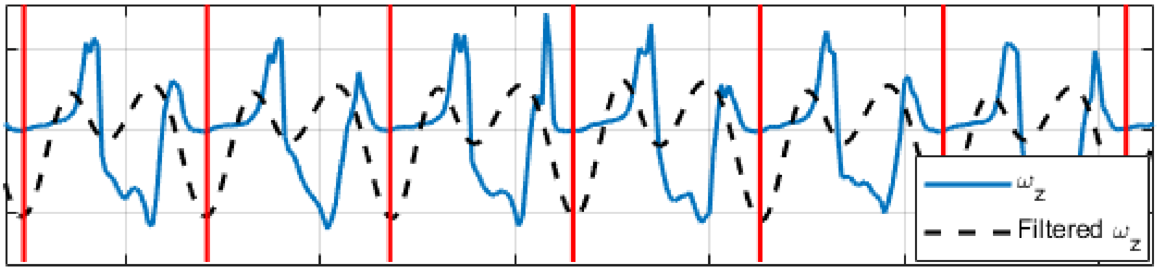


Figure 5.3: Gait cycle detection

Table 5.2: CC for the estimated gait signals and gait parameters using SONN and $W$=19, averaged over 10 iterations (sl: left shin, sr: right shin, tl: left thigh, tr: right thigh, w: waist with a 12Hz low-pass filter)

| | $\hat{a}$ | $\hat{\omega}$ | $\hat{\theta}$ | $\hat{v}$ | $\hat{d}$ |
|---|---|---|---|---|---|
| $\text{CC}_{\text{sl}}$ | 0.91±0.07 | 0.95±0.06 | 0.97±0.05 | 0.97±0.05 | 0.98±0.03 |
| $\text{CC}_{\text{sr}}$ | 0.89±0.08 | 0.94±0.07 | 0.97±0.05 | 0.95±0.08 | 0.98±0.04 |
| $\text{CC}_{\text{tl}}$ | 0.89±0.07 | 0.91±0.06 | 0.95±0.03 | 0.94±0.06 | 0.97±0.03 |
| $\text{CC}_{\text{tr}}$ | 0.88±0.07 | 0.90±0.06 | 0.94±0.03 | 0.94±0.08 | 0.96±0.05 |
| $\text{CC}_{\text{w}}$ | 0.67+0.13 | - | - | 0.93±0.08 | 0.97±0.03 |

where $\hat{\omega}(0)$ is an offset determined by the value of local minima of $\int_0^T \hat{\omega}(\tau)d\tau$ over a gait cycle period $T$. Similarly the estimated velocity $\hat{v}(t)$ is the integral of the estimated acceleration $\hat{a}(t)$ of an IMU, given by

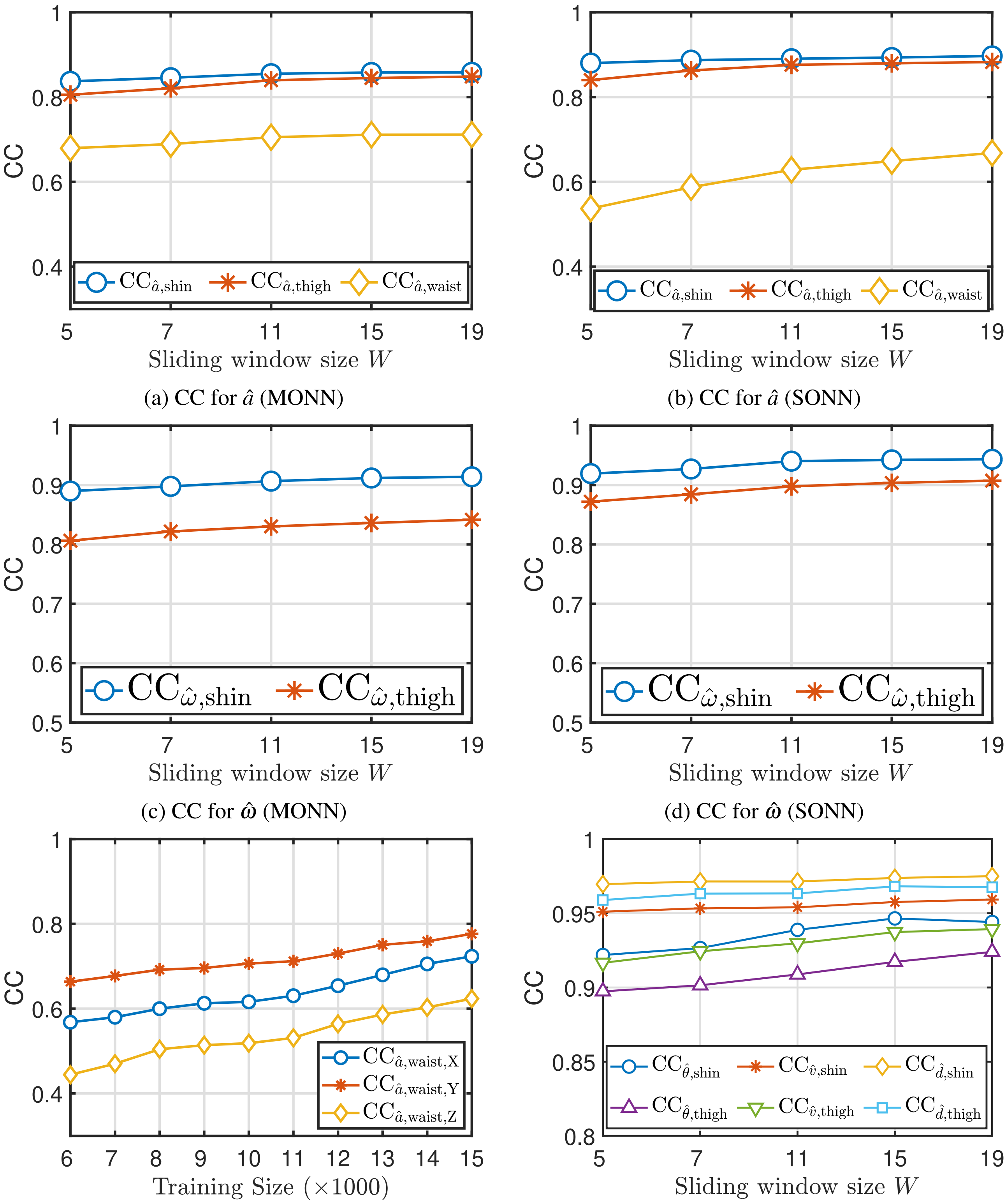
$$\hat{v}(t) = \int_0^t \hat{a}(\tau)d\tau + \hat{a}(0) \tag{5.6}$$

where $\hat{a}(0)$ is an offset determined by the value of local minima of $\int_0^T \hat{a}(\tau)d\tau$ over a gait cycle period $T$. Then the estimated displacement $\hat{d}(t)$ is the integral of the estimated velocity $\hat{v}(t)$, given by

$$\hat{d}(t) = \int_0^t \hat{v}(\tau)d\tau \tag{5.7}$$

### 5.1.2 Results

In this section, the performance of the proposed method is evaluated using Pearson Correlation Coefficient (CC). CC is often used as a measure of the difference between an estimator and its ground truth value. As aforementioned, the ANNs can have either single output, SONN or multiple outputs, MONN. In general, one MONN or $N$ SONNs are required for the estimation of a complete set of gait signals, including a 3-axis accelerometer ($N = 3$), a 3-axis gyroscope ($N = 6$), and potentially a 3-axis



(a) CC for $\hat{a}$ (MONN)

(b) CC for $\hat{a}$ (SONN)

(c) CC for $\hat{\boldsymbol{\omega}}$ (MONN)

(d) CC for $\hat{\boldsymbol{\omega}}$ (SONN)

(e) CC for $\hat{a_X}$, $\hat{a_Y}$, and $\hat{a_Z}$ against training size at the waist position (MONN)

(f) CC for gait parameter estimation at the shin and thigh positions (SONN)

Figure 5.4: Experimental results

magnetometer ($N = 9$), of an IMU. In the experiment, the sliding window size $W$ was set from 5 to 19 for both SONN and MONN, and all experiments were repeated 10 times and averaged to reduce the randomness of the results. In addition, the results in Fig. 5.4 and Table 5.2 were averaged over X, Y, and Z axis of any gait signals or gait parameters, except those in Fig. 5.4e.

Fig. 5.4a and Fig. 5.4b are the averaged CC against sliding window size $W$ for the estimated acceleration $\hat{a}$ at shin, thigh, and waist positions, using MONN and SONN respectively. Fig. 5.4c and Fig. 5.4d are the averaged CC against $W$ for the estimated angular velocity $\hat{\omega}$ at only shin and thigh positions, as the MAREA dataset does not provide gyroscope recordings. As shown in Table 5.2 and Fig. 5.4, the accuracy of $\hat{a}$ and $\hat{\omega}$ at the shin and thigh, when $W$=19, are higher than 88%, which demonstrated the feasibility and accuracy of the proposed method in estimating the lower limb sensor signals. Also, it can be observed that the performance of SONN is better than that of MONN. However, the CC for the estimation of $\hat{a}$ at the waist position is only around 67%, which is much lower than the ones for the shin and thigh. It maybe caused by the insufficient training sample data and less correlation between the target and input gait signals. As shown in Fig. 5.4e, a larger training size for the ANNs produces better CC results on all 3 axes of the accelerometer at the waist position, where $W$ was fixed to 19 (samples). $W$ also influences the performance of the proposed method, but it saturates at around 15 in most cases. Furthermore, Fig. 5.4f shows the averaged CC for gait parameters, $\hat{\theta}$, $\hat{v}$, and $\hat{d}$, of the IMUs at the shin and thigh positions, against $W$. The high CC results prove that the proposed method can be used for lower limb motion tracking and real-time gait analysis.

### 5.1.3 Conclusions

The results show that the proposed ANN-based method can accurately (with average accuracy higher that 88%) estimate gait signals at the shin and thigh positions by using only the inertial sensors on the feet. However, when estimating gait signals at the waist position, the performance of the proposed method was not as accurate as expected (with the averaged CC of 67%), which may due to insufficient training sample size in the artificial neural network training phase. There are a few future works for this project. First, we will investigate the use of other types of ANNs, such as recurrent neural network, to further improve the performance of the proposed method. Second, the estimation of the joint angles, such as the ankle angle and knee angle, will be investigated in the future. Third, we will evaluate the impact of the hardware synchronisation and stochastic noise on the proposed method. Finally, the proposed method can be further extended to estimate the upper limb motion signals, including torso movement, arm swing, and head movement.

## 5.2 An Improved ANN Framework for Gait Biometrics

The second part of this chapter presents the investigation on the use of the ANN framework proposed in the first part of this chapter for gait biometrics. As correlations among different gait signals at different body positions can be increased, the projected gait signals are now highly correlated and can be used as the common entropy source for improving the symmetric cryptosystem proposed in the previous chapter.

Recent wireless communication technology advancements have facilitated the development of light-weight, low-energy, miniaturised 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), and associated wireless networking technology which is known as the Wireless Body Area Network defined by the IEEE standard 802.15.6 (IEEE, 2012). Operating mainly in ISM (Industrial, Scientific and Medical) bands, wireless channels in WBANs are opened to anyone with matched radio interface configurations, and thus attackers can eavesdrop or even participate within the wireless communication amongst WBAN sensor nodes (Mainanwal, Gupta, and Upadhayay, 2015). As a result, a high level data protection is a necessity for BSNs, whereby the protection of patients' data from unauthorised 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 ECG, PPG, and behavioural characteristics, such as voice (Khitrov, 2013), and gait (Derawi et al., 2010), can be captured by BSN sensors, thus, providing opportunities for Biometric Cryptosystems 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 (Bao, Poon, et al., 2008; Chan et al., 2008) 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 centimetres 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 (Hoang, Choi, and Nguyen, 2015; Nickel, Wirtl, and Busch, 2012; Zhang, Pan, et al., 2015). 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 and Kotz (2012), 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 (Schurmann et al., 2017) can only extract 4 bits per gait cycle from the IMU signals. Another gait-based authentication scheme (Oberoi et al., 2016) using 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, as presented in the first part of this chapter, the ANN framework is used 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 (Kerimbaev, 2016) or Android (Matney, 2017) based wearable devices. Xu, Javali, et al. (2017) have also proposed a gait-based automatic key generation protocol, in which an Independent Component Analysis 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 practice, 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 (Hoang, Choi, and Nguyen, 2015; Nickel, Wirtl, and Busch, 2012; Revadigar, Javali, Xu, Vasilakos, et al., 2017; Xu, Javali, et al., 2017; Zhang, Pan, et al., 2015), whereas the proposed security scheme can be applied on the wearable devices located at any body positions. 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.

## 5.2.1 Methodology

### 5.2.1.1 System Modelling

Fig. 5.5 illustrates a typical 3-tier BSN-based healthcare system (Miao et al., 2009c), 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, such as 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. However, there is very limited protection for the wireless communications among the sensors and the personal

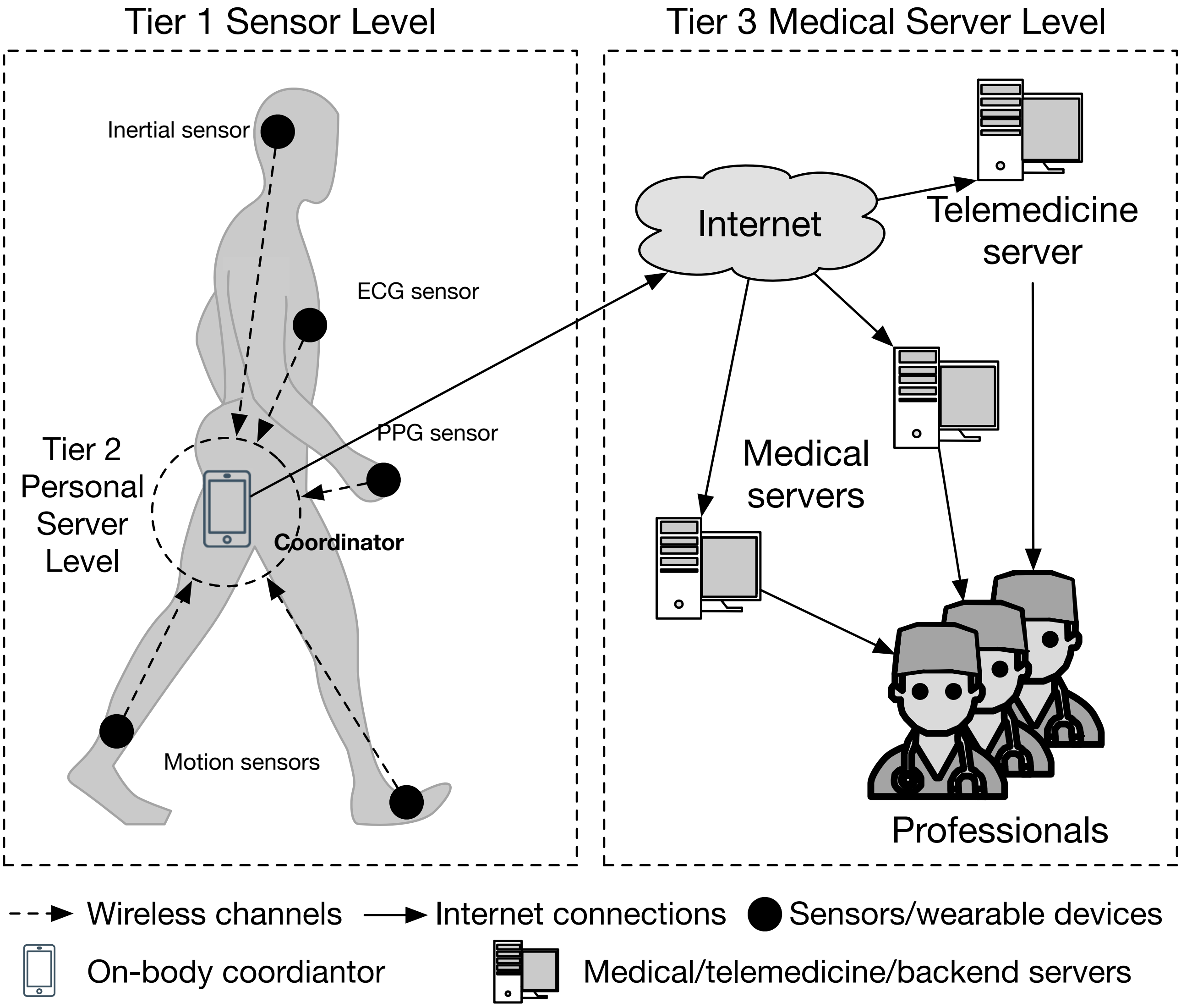
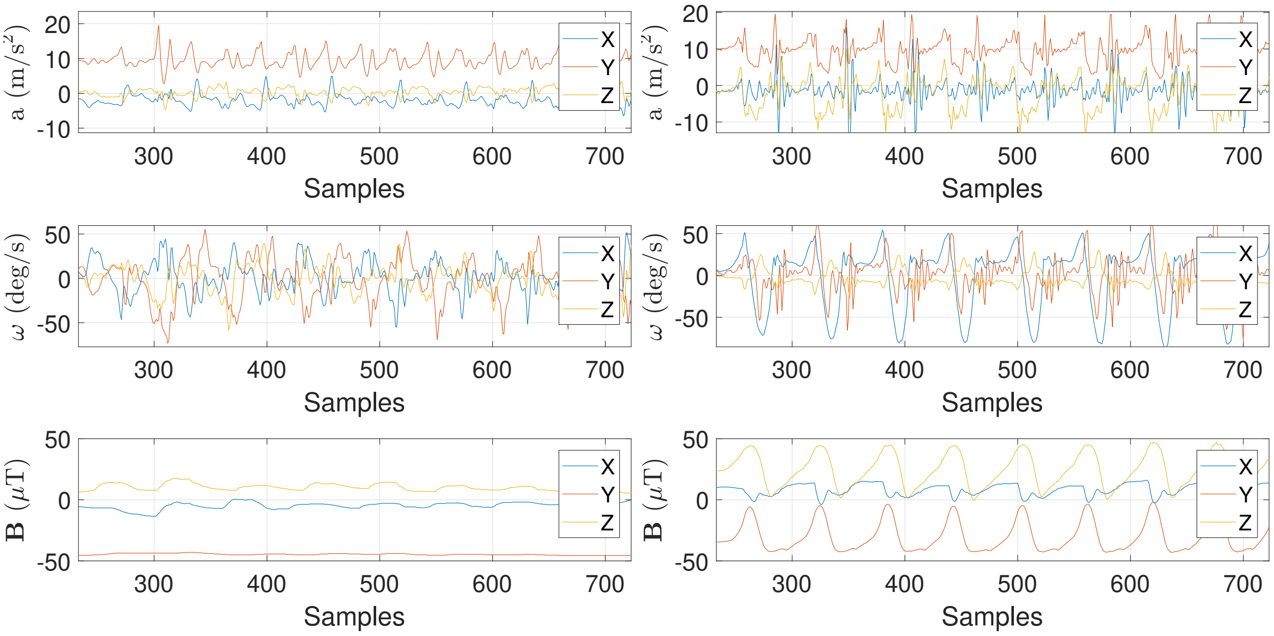


Figure 5.5: A typical 3-tier BSN-based healthcare system

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 chapter refer to the acceleration and angular velocity captured by the IMU sensors during the walking motion. Gait signals can also be recognised as a behaviour 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 behavioural 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 by the sensors positioned at different locations on the body will have different patterns as shown in Fig. 5.6. The discrepancies between the sensor signals are often introduced by body movements such as arm and leg swings. As stated in (Xu, Javali, et al., 2017), 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 (Sun, Yang, and Lo, 2018) to project the gait signals acquired from body worn sensors onto the chest, to minimise 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. 5.7, where an overview of the proposed security scheme is presented.

As presented in the bottom of Fig. 5.7, 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 and the trained model can then be transferred onto the sensors for on-node processing, therefore, the power consumption can be minimised 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



(a) IMU outputs at the chest

(b) IMU outputs at the shin

Figure 5.6: IMU outputs at the chest and shin positions, a=acceleration, $\omega$=angular velocity, and **B**=magnetic field

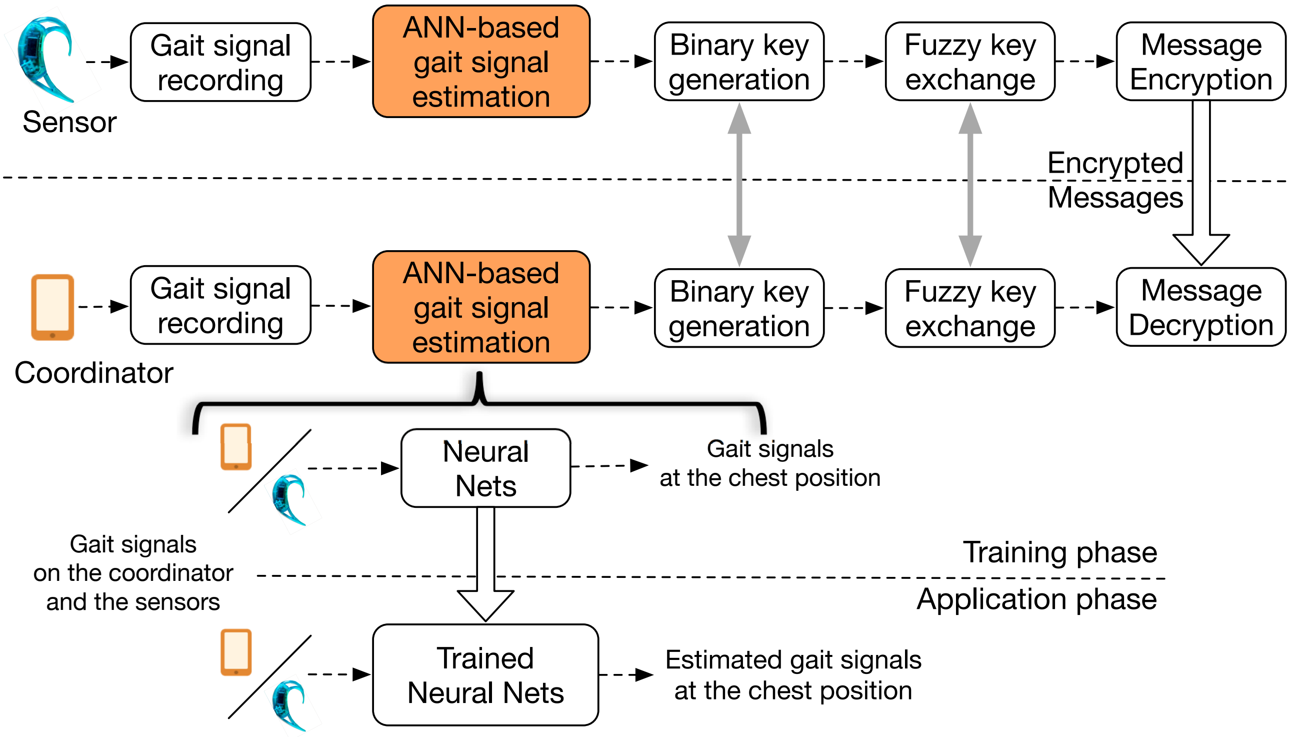


Figure 5.7: Overview of the proposed security scheme

indicated using the gray double-headed arrows in Fig. 5.7.

#### 5.2.1.2 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, $a_{-G,\text{chest}}$, 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 chapter. The gait signals, $a_{-G,\text{input}}$, 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. 5.8. 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

$$x(n) = [a_{-G,\text{input}}(w(n))]^T \tag{5.8}$$

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

$$\mathbb{X} = [x(1), x(2), ..., x(n), ..., x(N)] \tag{5.9}$$

whereas the training target set is

$$Y = [y(1), y(2), ..., y(n), ..., y(N)] \tag{5.10}$$

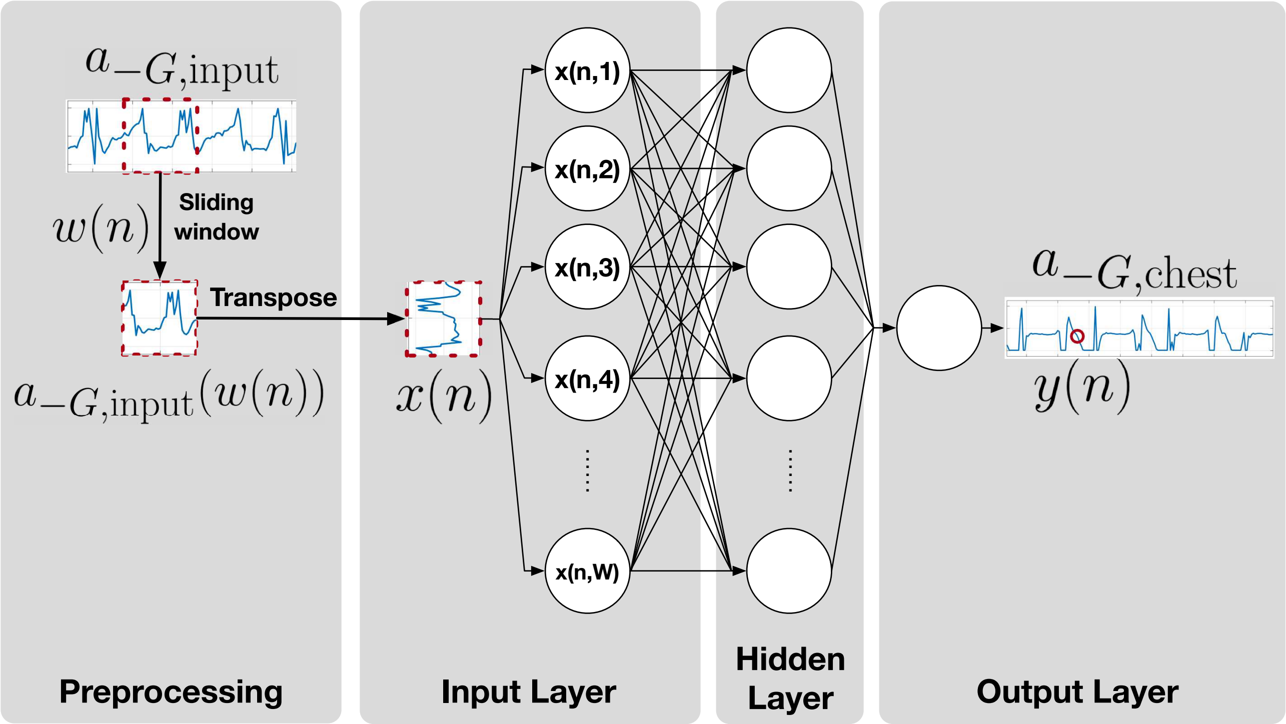


Figure 5.8: ANN-based gait signal estimation

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 $\hat{a}_{-G,\text{chest}}$. 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. 5.14, from which binary keys with high similarity can be generated using the algorithms presented previously.

### 5.2.1.3 Binary Key Generation

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

**Gait cycle detection** the gait cycle detection module is adopted from (Sun, Wong, et al., 2017), 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 (Revadigar, Javali, Xu, Vasilakos, et al., 2017). Every two consecutive valley is considered as the boundary between two adjacent gait cycles, as indicated with the red vertical lines in Fig. 5.9b, 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. 5.9c, 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 normalised gait cycles are denoted as

$$\mathbf{c} = [c_1, c_2, ..., c_j, ..., c_J] \tag{5.11}$$

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

**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

$$\mathbf{C} = [C_1, C_2, ..., C_\mu, ..., C_U] \tag{5.12}$$

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

$$\alpha = [\alpha_1, \alpha_2, ..., \alpha_\mu, ..., \alpha_U] \tag{5.13}$$

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

$$\delta_{\mu l} = c_{\mu+l} - \alpha_\mu \tag{5.14}$$

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

$$b_{\mu lt} = \begin{cases} 1, & \delta_{\mu lt} \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{5.15}$$

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. 5.9c, 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 randomised 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.

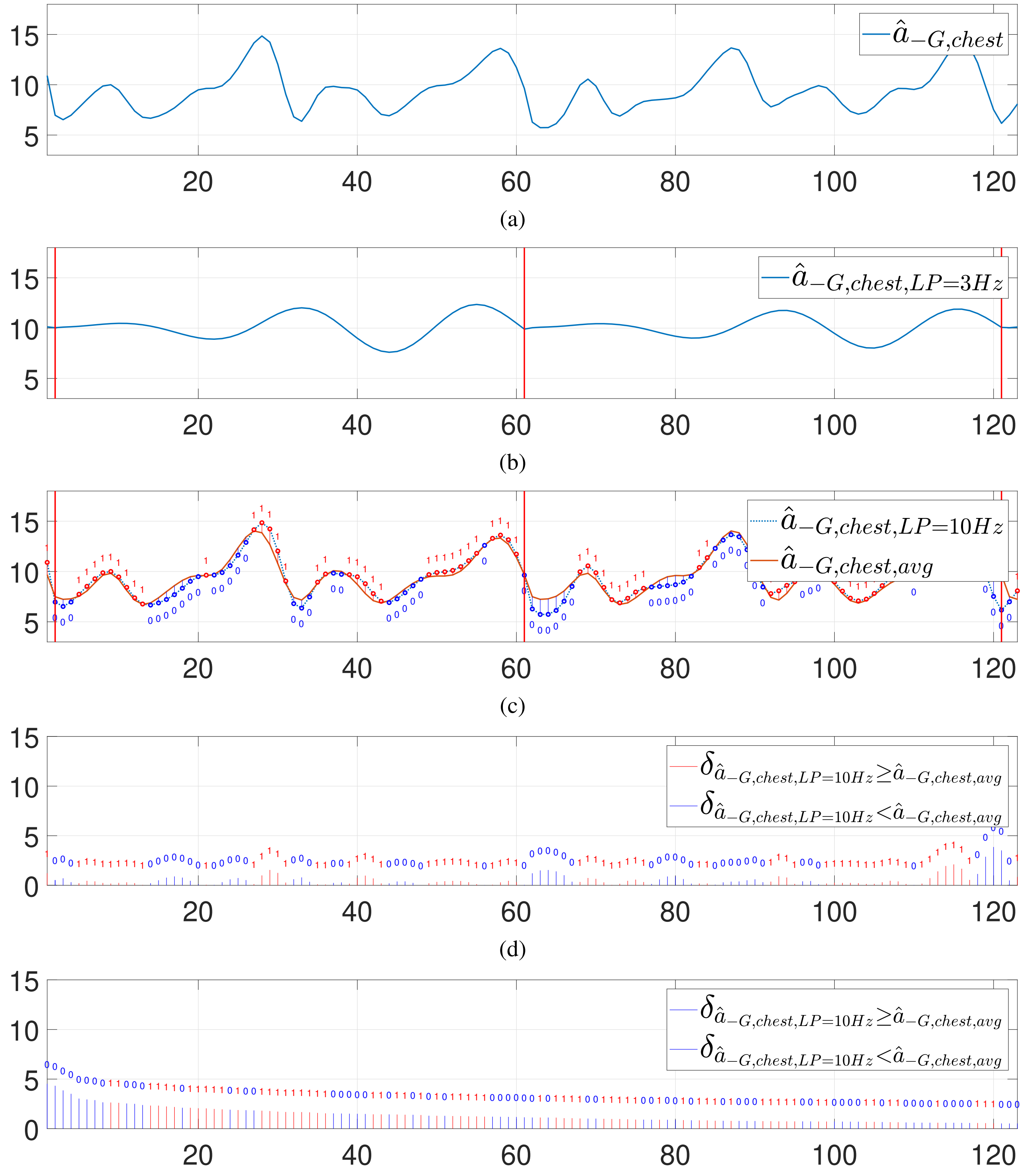
**Reliable Bit Extraction** The calculation of the reliability is adopted from (Schurmann et al., 2017), where a reliability vector is defined as the descending index vector of the absolute values of the signal energy differences. The absolute values of the signal energy difference for the $\mu^{th}$ gait cycle group $C_{\mu}$ can be represented as

$$\Delta_{\mu} = [|\delta_{\mu 1}|, |\delta_{\mu 2}|, ..., |\delta_{\mu \eta}|, ..., |\delta_{\mu (L \cdot T)}|] \tag{5.16}$$

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

$$\mathbf{r}_{\mu} = [r_{\mu 1}, r_{\mu 2}, ..., r_{\mu \eta}, ..., r_{\mu (L \cdot T)}] \tag{5.17}$$

where $r_{\mu \eta} \geq r_{\mu \eta + 1}$. The generated binary keys are re-indexed using the reliability vectors as illustrated in Fig. 5.9d and Fig. 5.9e. 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 (ibid.). 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.



(a)

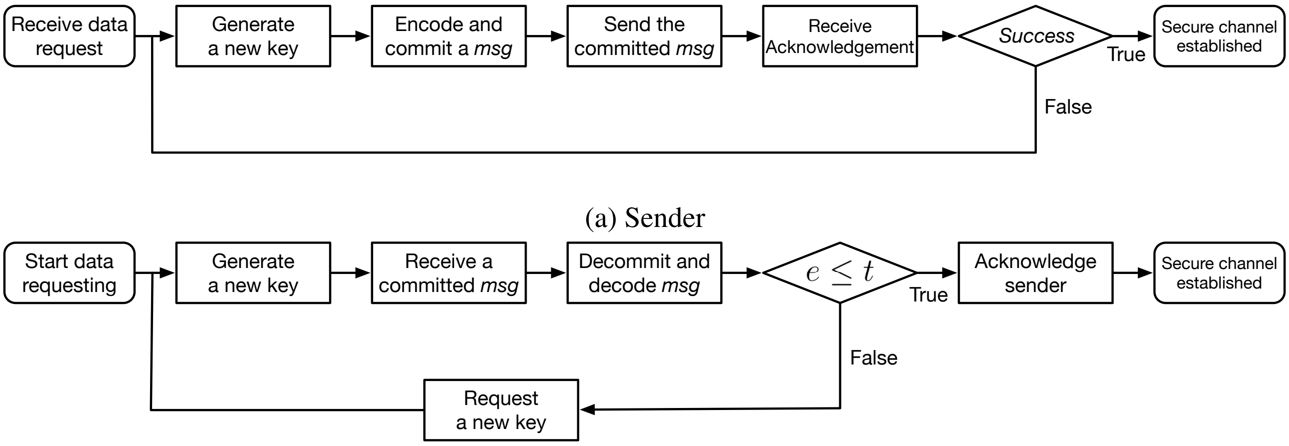
(b)

(c)

(d)

(e)

Figure 5.9: 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.



(a) Sender

(b) Requester

Figure 5.10: Flowcharts of the fuzzy key exchange block

#### 5.2.1.4 Fuzzy Key Exchange

In the fuzzy key exchange block, we adopt the fuzzy commitment scheme (Juels and Wattenberg, 1999), which has been used in biometric-based security systems (Hoang, Choi, and Nguyen, 2015). To correct the bit errors introduced by the dissimilarity of the intra-class keys, BCH error correction codes (Peterson and Weldon, 1972) 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

$$n = 2^m - 1 \text{ and } d_{min} \geq 2t + 1 \tag{5.18}$$

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

$$n - k \leq mt \tag{5.19}$$

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. 5.10.

### 5.2.2 Experiments and Results

#### 5.2.2.1 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±12.4, height 173.1±6.9cm, weight 74.1±13.8kg, 8 males and 7 females) from the Real World Human Activity Recognition (HAR) dataset (Sztyler, Stuckenschmidt, and Wolfgang, 2017). 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. 5.11. As there is only one recording at one sensor position 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.

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 synchronised and have different lengths of samples. To solve this issue, we re-sampled the 7 gait recordings to the same

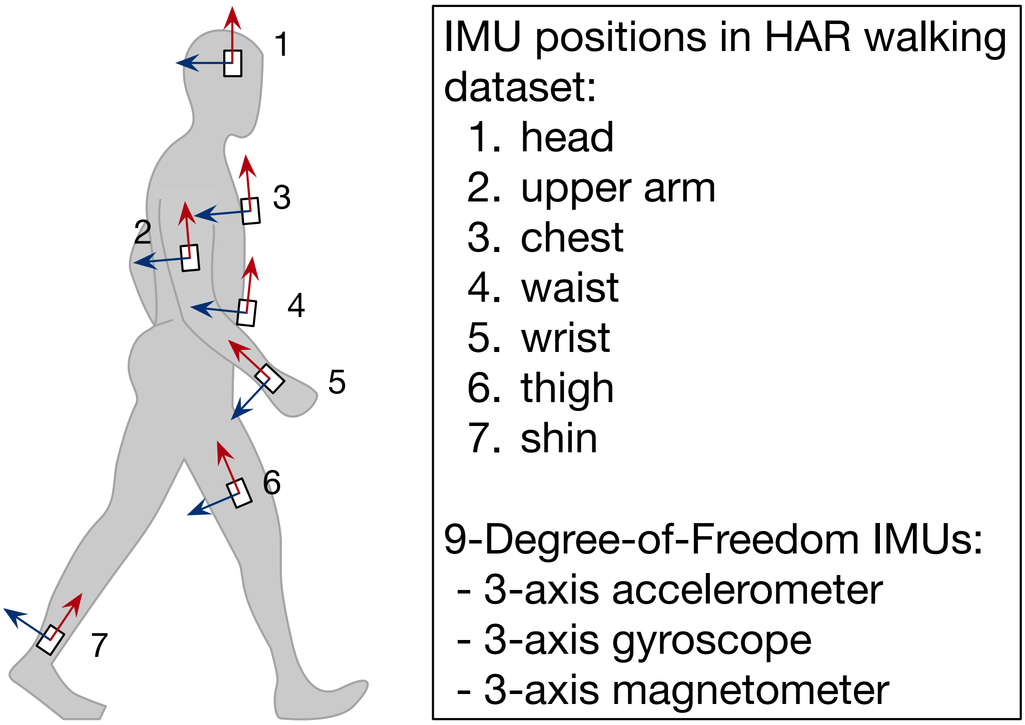


Figure 5.11: HAR walking dataset

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, only the acceleration in the inverted gravity direction was used as the gait signals in our experiments.

#### 5.2.2.2 Group Similarity Evaluation

**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. 5.12. 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.

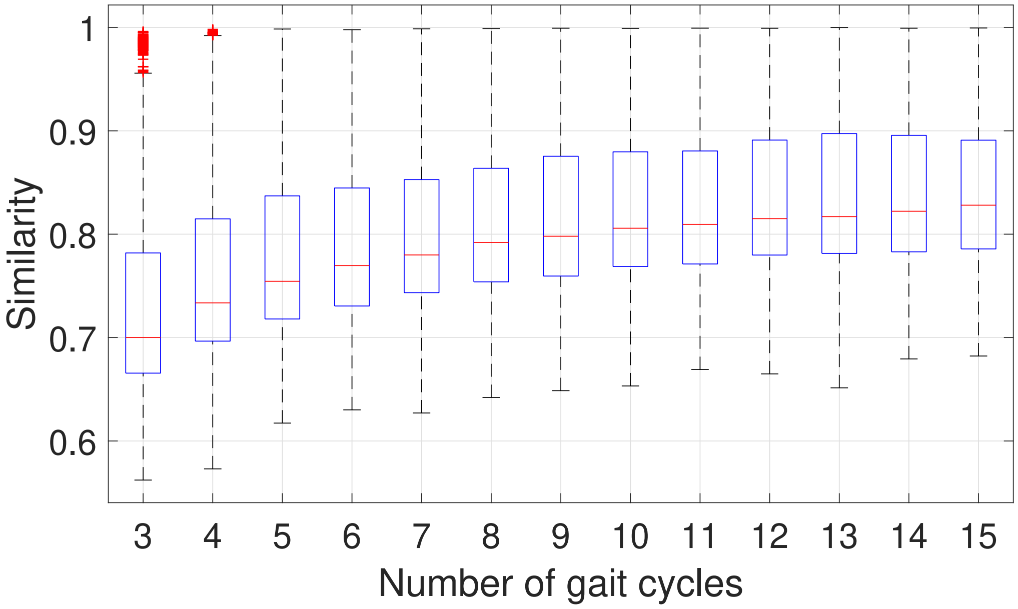


Figure 5.12: Averaged similarity between 128-bit binary keys generated simultaneously from two sensors on different sensor positions of the same subject (intra-class group)

**Key Length** the similarity of the intra-class keys decreases with the increase of the key length, as shown in Fig. 5.13, 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.

**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. 5.6 and Fig. 5.14a. 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. 5.14b. The results of using the ANN-based gait signal estimation block is illustrated in Fig. 5.15, where correlation coefficients 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 assess-

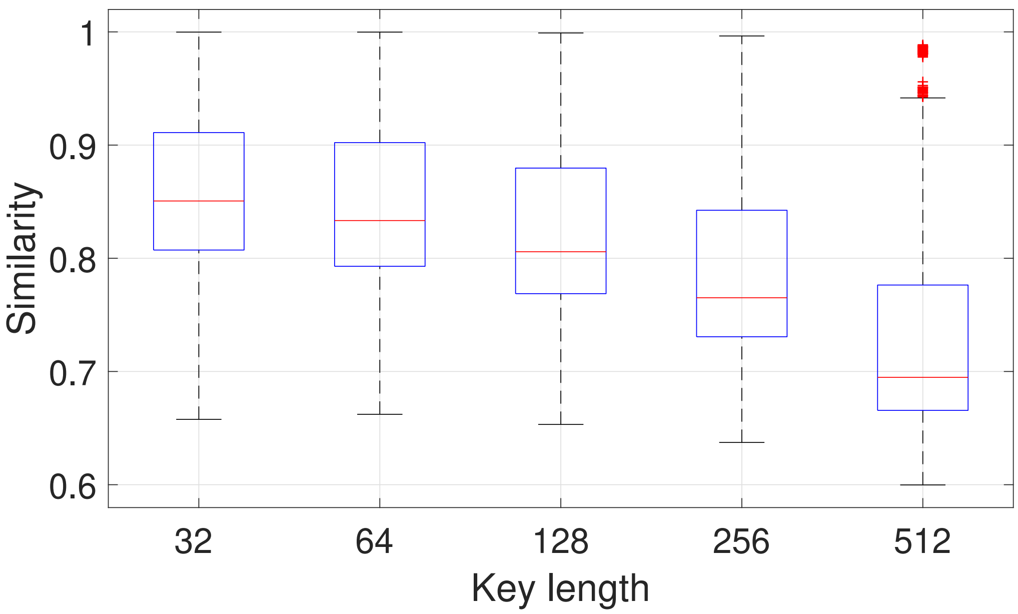
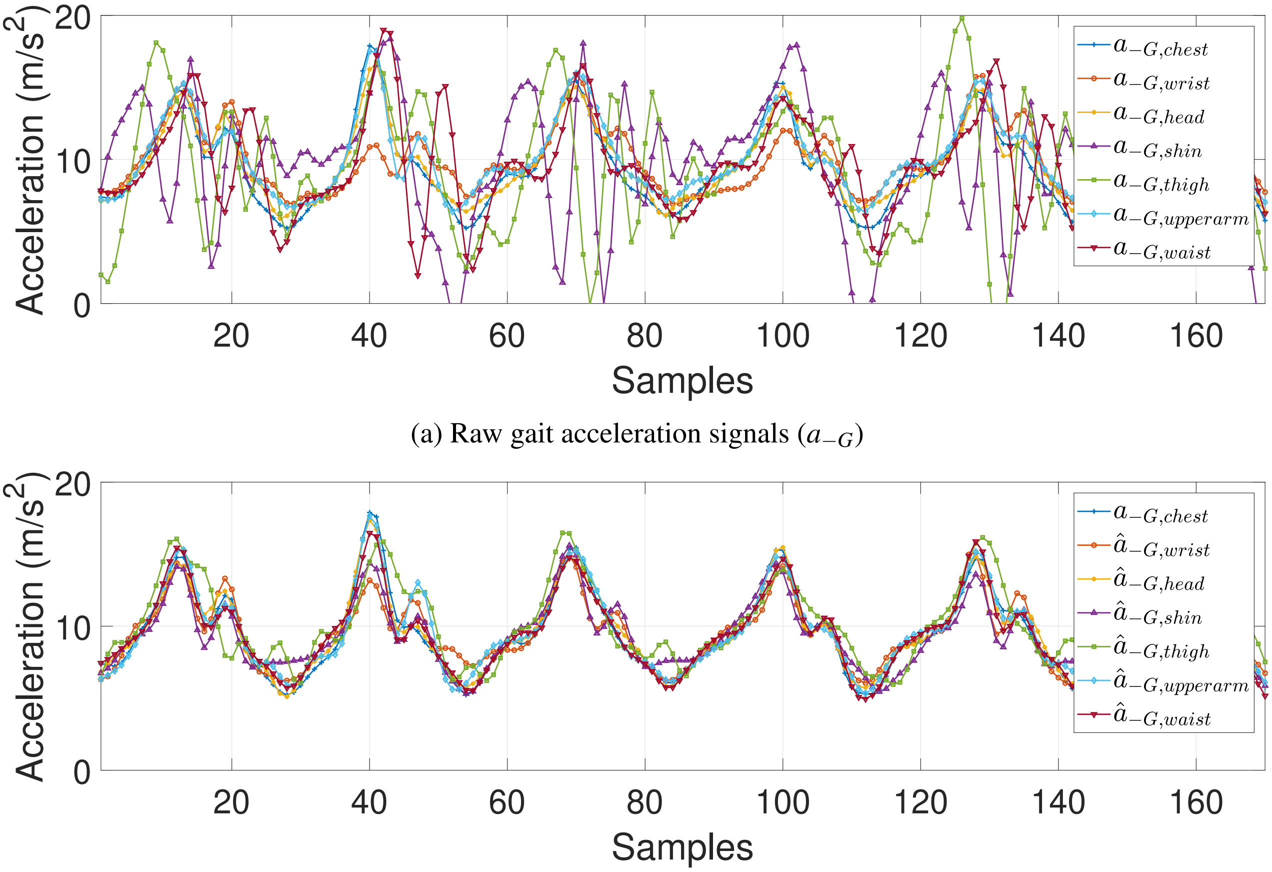


Figure 5.13: Averaged similarity between intra-class keys at different key lengths. The keys were generated by reordering binary sequences using reliability vectors and cutting off at the key lengths

ing linear relationship between two continuous variables (Altman, 1990), 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 (Tadano, Takeda, and Miyagawa, 2013). According to Hinkle, Wiersma, and Jurs (2002), 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. 5.15, 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. 5.16, 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. 5.16, espe-



(a) Raw gait acceleration signals ($a_{-G}$)

(b) Estimated gait acceleration signals ($\hat{a}_{-G}$)

Figure 5.14: Illustration of the ANN-based signal estimation

cially 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 (Peterson and Weldon, 1972). 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 5.3. Therefore, the minimum similarity between the encryption key and the decryption key required by BCH 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 5.4. 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.

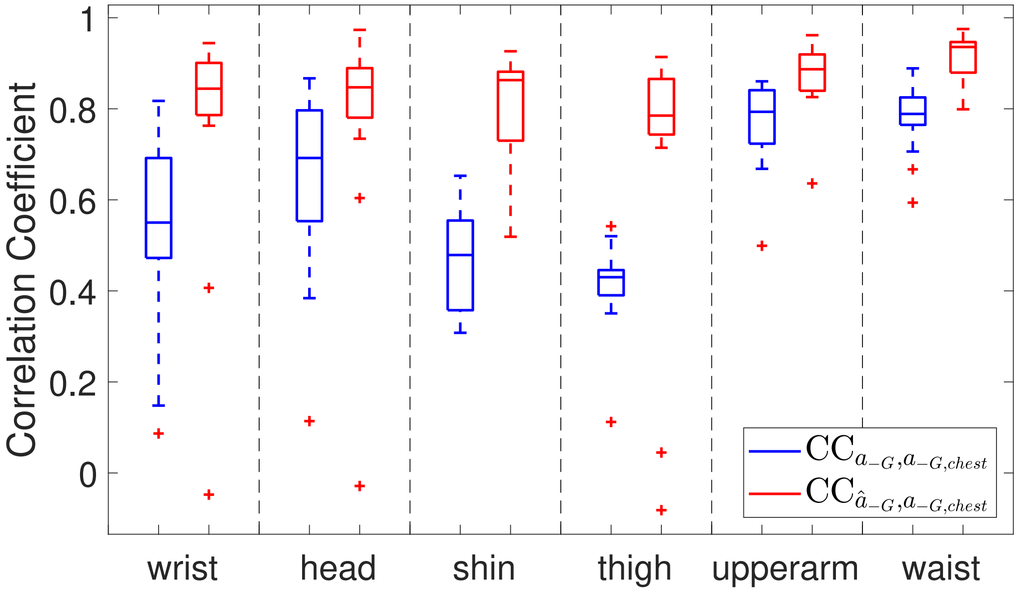


Figure 5.15: CCs between the raw gait signals at other positions and chest gait signals (blue boxes), and CCs between estimated gait signals, using trained ANNs, at other positions and the chest gait signals (red boxes)

Table 5.3: 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% |

Assuming a successful fuzzy key exchange in a series of attempts is an independent event, the probability of a successful fuzzy key exchange after the $n^{th}$ attempt is calculated as

$$P_n = \sum_{i=1}^{n} P_{success} \times (1 - P_{success})^{n-1} \tag{5.20}$$

where $P_{success}$ is the probability of a successful fuzzy key exchange for an individual attempt. Using Eq. 5.20, the probabilities of success against the number of attempts for the BCH pair (127,8,31) are calculated and shown in Fig. 5.17. At all 7 positions, a successful fuzzy key change occur 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. However, multiple attempts of key exchanges can only be supported if a secured communication channel has already

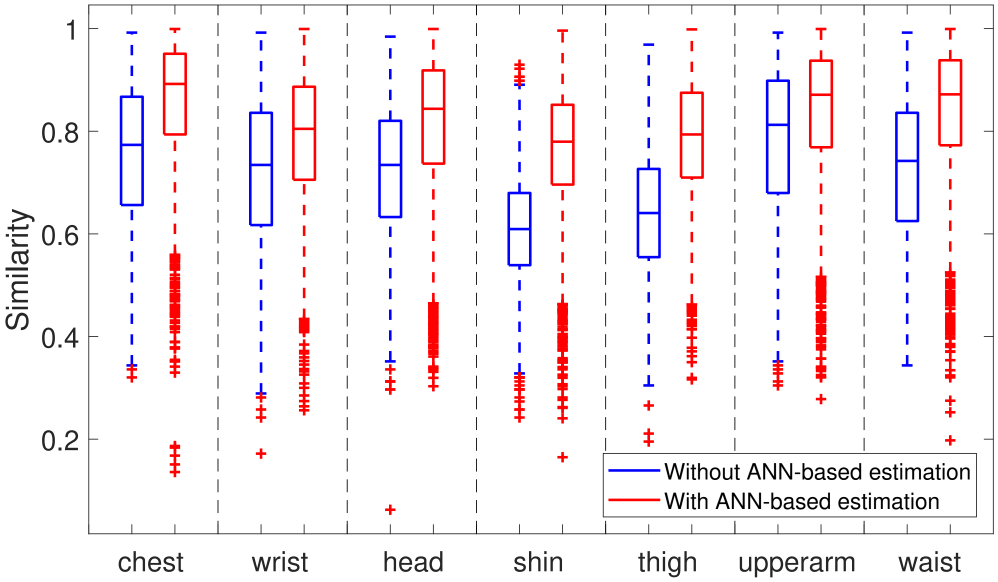


Figure 5.16: Similarity of the keys generated at various positions against the keys generated at the rest of the positions

Table 5.4: 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 |

been established and new keys are required to replace the old ones.

A detailed comparison amongst position-to-position intra-class similarity, averaged for all the subjects in the HAR walking dataset, is presented in Table 5.5. 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. 5.16. It is due to the fact that shin and thigh gait signals are less correlated with chest gait signals, as shown in Fig. 5.15.

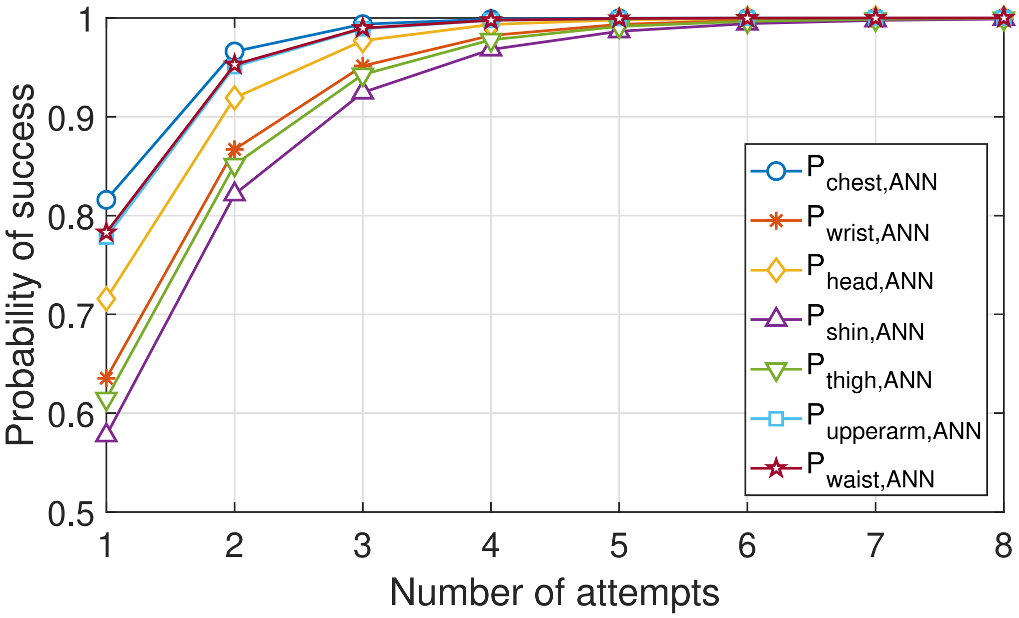


Figure 5.17: Probability of successful fuzzy key exchanges on various positions to the rest of positions in different number of attempts

Table 5.5: 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 |

**Reliability** the impact of reordering keys using associated reliability vectors has also been investigated and the results are shown in Fig. 5.18, 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. 5.13. 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.

#### 5.2.2.3 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 analysing the distribution of the Hamming Distance (HD) for the inter-class keys and vitalising 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 (Encyclopedia, 2017). HD=0 means two binary keys are identical, while HD=1 means two binary keys are completely different from one another (Altop, Levi, and Tuzcu, 2015). For sufficiently long binary keys, the distribution of HD should be a normal distribution with a mean close to 50% (Zheng, Fang, Shankaran, Orgun, Zhou, et al., 2017). As shown in Fig. 5.20, 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 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.

#### 5.2.2.4 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.

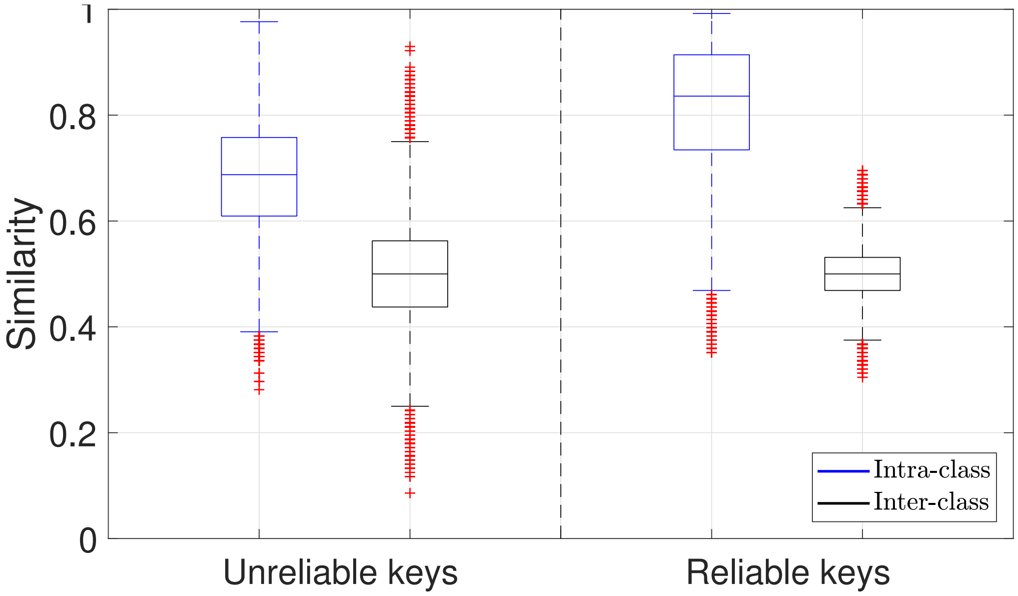


Figure 5.18: Similarity of intra-class group and inter-class group. Unreliable keys are the 128-bit keys generated without reordering by their reliability vectors, while reliable keys are the reordered unreliable keys using their associate reliability vectors

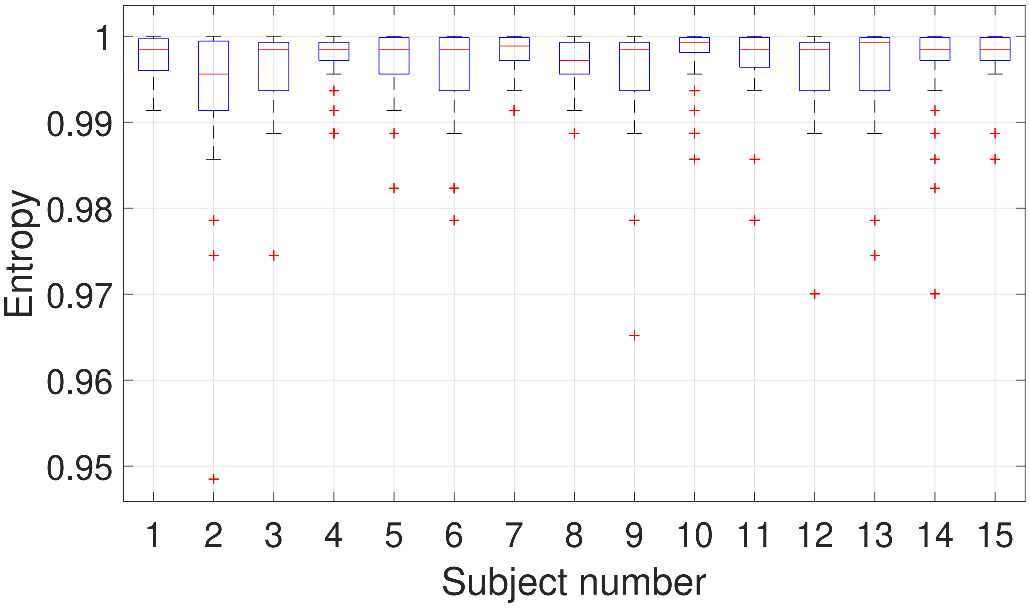
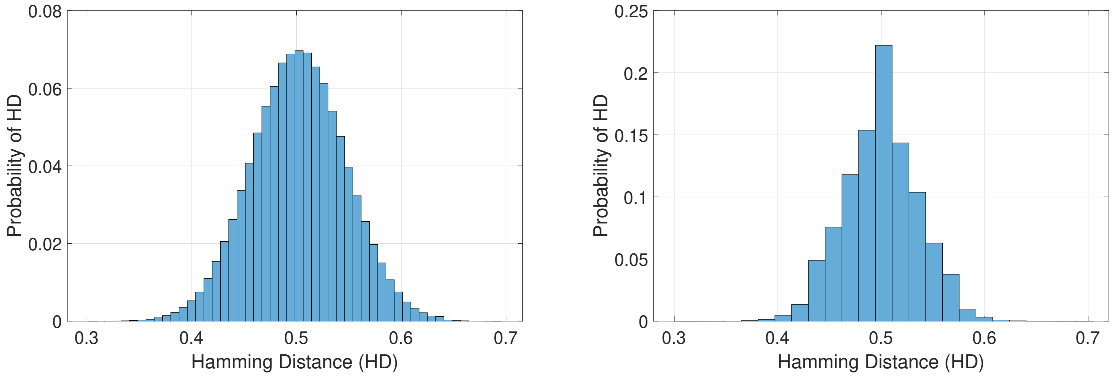


Figure 5.19: Shannon entropy of 128-bit keys for 15 subjects in the HAR walking dataset ($N_{gc} = 10$)



(a) (b)

Figure 5.20: Probability distribution of hamming distance of (a) any two inter-class 128-bit keys generated from all 15 subjects, with the mean distance of 49.96%, and (b) random numbers generated by Matlab built-in function *randi*()

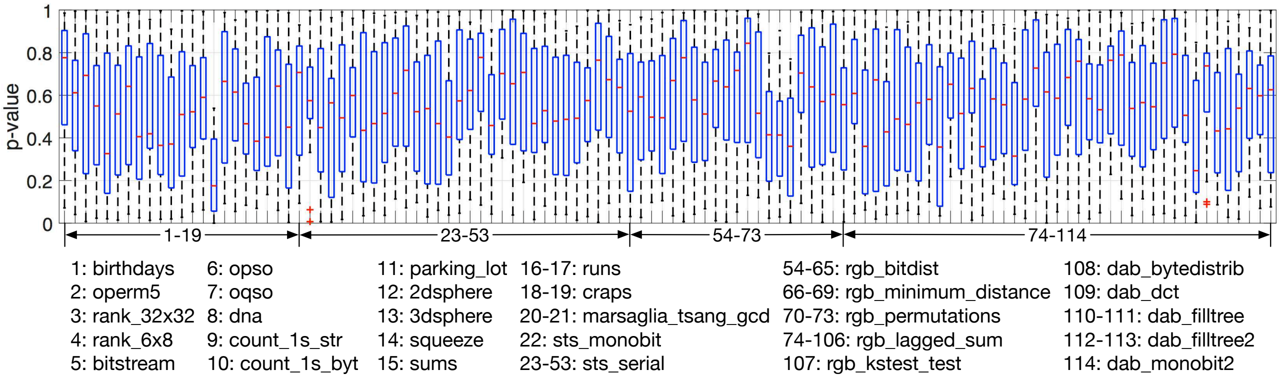


Figure 5.21: Distribution of p-values in the Dieharder statistical test results

**Entropy Analysis** the generated keys in the experiments were tested with the entropy analysis. Shannon entropy is a measure of uncertainty of binary sequences (Moosavi et al., 2017). 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 (Shannon, 1948)

$$H(\{0,1\}) = -P(0)\log_2 P(0) - P(1)\log_2 P(1) \tag{5.21}$$

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. 5.19. 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.

Table 5.6: NIST Statistical Test Results

| Statistical test | P-value | Proportion | Pass/Fail |
|---|---|---|---|
| Frequency | 0.595549 | 99% | Pass |
| Block Frequency | 0.739918 | 98% | Pass |
| Cumulative Sums$^{+}$ (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$^{+}$ (148) | 0.136742 | 97% | Pass |
| Serial$^{+}$ (2) | 0.457748 | 99% | Pass |
| Linear Complexity | 0.137282 | 96% | Pass |

**NIST Randomness Test** the National Institute of Standards and Technology (NIST) randomness test suite has also been used widely by researchers (Xu, Javali, et al., 2017; Yin et al., 2017; Zheng, Fang, Shankaran, Orgun, Zhou, et al., 2017) to detect deviations of a binary sequence from randomness (Rukhin et al., 2010). We tested all the 600-bit (60×10) 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 5.6. The minimum pass rate for each statistical test is approximately 96%, therefore, all tests have passed the tests. The P-values in Table 5.6 are from the uniformity tests for these statistical tests, and P>0.0001 indicates the p-values from the corresponding statistical test are uniformly distributed on the interval [0,1) (Sys et al., 2015).

**Dieharder Test** all the keys generated in the experiments were also run through a series of Dieharder statistical tests (Brown, 2004), and the p-value distributions of 21 runs of the Dieharder tests are shown in Fig. 5.21. 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. 5.21 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.

### 5.2.3 Discussion

#### 5.2.3.1 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.

#### 5.2.3.2 Dictionary Attacks

Besides brute force attacks, dictionary attacks are also very popular methods used by among hackers in recent years (Millman, 2018). 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.

#### 5.2.3.3 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.

#### 5.2.3.4 Impersonation Attacks

Impersonation attacks in gait biometrics have been studied extensively in the literature (Gafurov, Snekkenes, and Bours, 2007; Hadid et al., 2012; Muaaz and Mayrhofer, 2017). Muaaz and Mayrhofer (2017) 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. 5.22 shows that when using victims' neural networks, the zero-effort impersonation does not increase the CC results nor improve chances of the impersonation.

#### 5.2.3.5 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 (Rathgeb and Uhl, 2012; Tams, 2014) have demonstrated that fuzzy commitment or fuzzy vault schemes are vulnerable against many attacks (i.e. Decodability (Tams, 2014), record multiplicity, surreptitious key-inversion, and novel blended substitution (Scheirer and Boult, 2007)). 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 (X. Zhou et al., 2011). 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 1s and 0s. In our proposed scheme, temporal gait features are used for generating encryption keys with a high level of freshness. Because temporal features are time-variant, producing distinctive keys even in a short period of time. As shown in Fig. 5.18 and 5.20, 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.

#### 5.2.3.6 Efficiency

The number of the gait cycles required for generating one 128-bit key is sufficiently reduced compared with our previous work (Sun, Wong, et al., 2017), 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 50Hz in the HAR walking dataset is 60, thus, the averaged time for one gait cycle is $60 \times \frac{1}{50} = 1.2s$. When $N_{gc} = 10$, the averaged time required for generating one 128-bit key is 12s, and the averaged output rate of the binary key generation block is $128 \times \frac{1}{12}$=10.7bps. 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.

#### 5.2.3.7 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. 5.23a and Fig. 5.23b present the performance of such authentication usage using FAR, FRR, and ROC curves. 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.

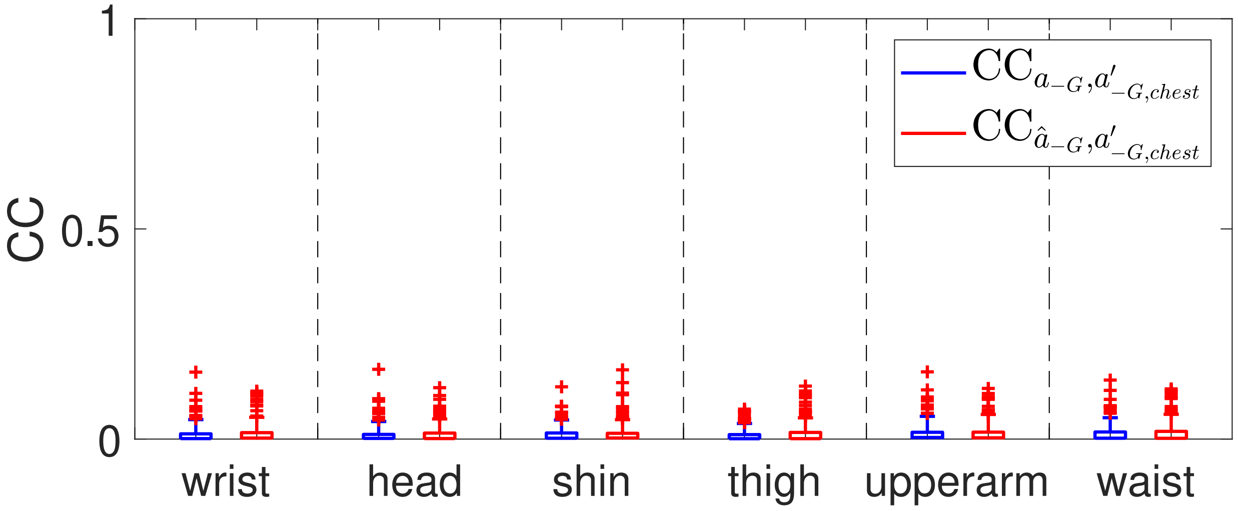
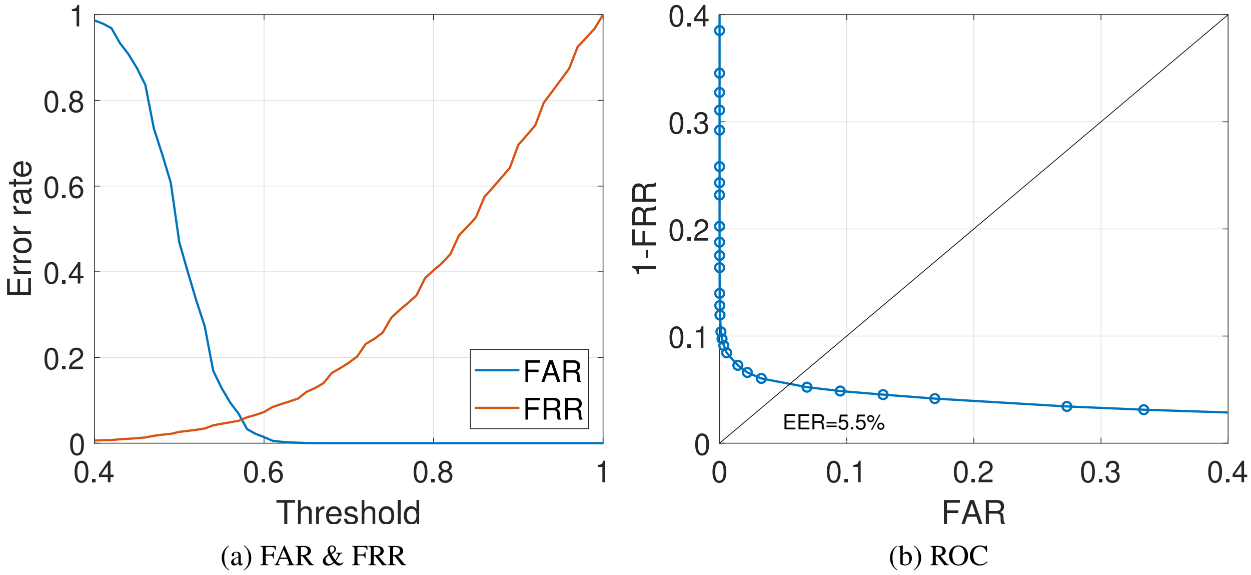


Figure 5.22: CCs between impersonators and victims (blue boxes), and CCs between impersonators and victims when using victims' trained neural networks (red boxes)



(a) FAR & FRR

(b) ROC

Figure 5.23: Use the proposed security scheme as biometric device-to-device authentication

### 5.2.4 Conclusion

An improved gait-based security scheme with ANNs is proposed 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.

## 5.3 Summary

In this chapter, an ANN framework based method is proposed to estimate on-body sensor signals (motion signals) at one body position from another sensor at different body position. In the first part of this chapter, the proposed ANN framework is applied to estimate lower limb motion using foot mounted inertial sensor signals. Next, the ANN framework is added in the previously proposed gait-based cryptosystem as a signal processing block. The performance of the security scheme has been improved in terms of binary key output rates and intra-class key matching rates.

# Chapter 6

# Random Number Generation Using Gait

Random numbers are fundamental to almost all the cryptographic algorithms and secure computer systems (Graham, 2013). The research on the use of gait biometrics for securing BSNs in the previous chapters also reveals that the freshness of gait signals can be used to generate random numbers by removing the low frequency periodical components in the signals. Therefore, in this chapter, the use of gait signals for generating random numbers is investigated, and the work presented in this chapter has been published in (Sun and Lo, 2018c).

On potential low-cost solution to address the inadequate resources of the current healthcare systems is the Internet of Things, which brings seamless connections for on-body BSN sensors. This enables sensors and coordinators, such as mobile phones, to send real-time data to the server, creating new possibilities for long-term patient monitoring, disease diagnosis, and emergency responses. This chapter presents the research on the potential use of gait biometrics in securing those on-body IoT devices. The Internet of Things can be described as a network of uniquely identifiable devices, usually are embedded computing devices with a variety of sensors, connected to the internet. By 2020, approximately 26 billion devices will be connected to the internet, and a large number of them will be wearable and implantable devices (Arias et al., 2015; Middleton, Kjeldsen, and Tully, 2013). Wearable and implantable sensing for health is considered as one of the most vital IoT applications, because its potentials in transforming the way we live (Meola, 2016). CCS Insight predicted that the wearable technology market will reach 411 million units, which would potentially worth 34 billion dollars, in 2020 (Lamkin, 2016).

As the purpose of wearable and implantable IoT devices is to capture and monitor user's physiological state, strong security and privacy is essential in such applications (Cai et al., 2017). The lack of security protection in IoT systems will not only endanger user's privacy, but it could also threaten the user's life; for example, a pacemaker without any security protection can be hijacked. For example, former vice present of United State Dick Cheney asked his doctors to disable the wireless capabilities of his pacemaker to prevent against possible assassination attempts on his life (Kloeffler and Shaw, 2013).

To provide a strong security for wearable and implantable IoT applications, a good random number generator is essential. RNG is a critical component in any cryptographic systems, producing random numbers to be used for both asymmetric and symmetric key generation (Sun, Wong, et al., 2017), block cipher initialisation vectors (Kumar, Lee, and Lee, 2010), one-time padding (Tobin et al., 2017), digital signatures (Buchmann, Dahmen, and Szydlo, 2009), and password storage.

There are two basic types of RNGs: true random number generators, which generate unpredictable random numbers from physical processes; and pseudo random number generators, which are often based on deterministic algorithms that generate reproducible pseudo-random numbers. As PRNGs can easily generate not truly random numbers at high speeds, they are widely used in cryptographic systems. However, as PRNGs only expand short seeds into longer deterministic pseudo-random numbers (Goldreich, 2007), PRNGs are vulnerable to brute-force attacks if the seed selection is faulty. For instance, using timestamps as the seeds for PRNG, which is a common practice for many websites including Hackernews (Dfranke, 2009), can produce weak random numbers to be guessed by external attackers. Therefore, to reduce the vulnerability introduced by PRNGs, TRNGs or PRNGs with seeds generated from TRNGs are used in state-of-the-art cryptographic systems for IoT applications to produce truly random numbers with high entropy.

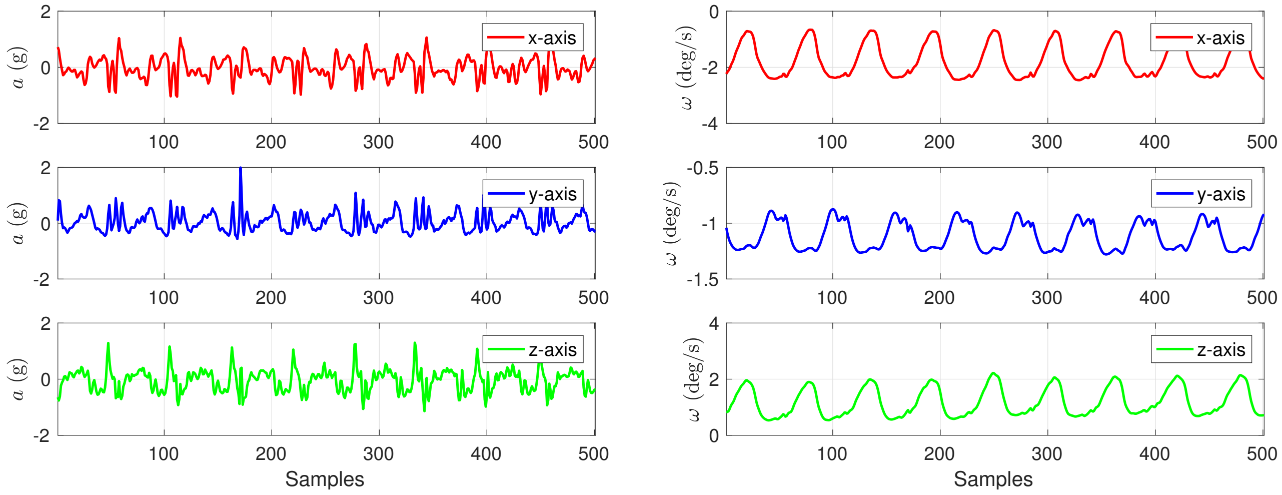
Many hardware-based TRNGs have been proposed for securing wearable and implantable IoT devices (Bucci et al., 2003; Mathew et al., 2016; Yang, Lin, Fu, et al., 2017), however, they required special integrated circuits to be embedded onto the devices. Alternatively, sensors on the wearable and implantable devices can measure physical phenomena of the users, including acceleration, angular velocity, and magnetic field, and such entropy can be harvested to generate truly random numbers (Loutfi et al., 2014). Other researchers have studied the use of sensor-based TRNGs to generate random numbers for mobile, wearable and implantable devices (Hong and Liu, 2015; Marghescu, Teseleanu, and Svasta, 2014; Sathya, Premalatha, and Rajasekar, 2015; Suciu, Lebu, and Marton, 2011; Wallace et al., 2016).

However, there are a few issues that have not been fully addressed. First, the raw sensor data collected during daily activities, such as walking (Dinca and Hancke, 2017), is periodic and predictable, thus, the random numbers generated from the raw sensor data are not truly random. Second, studies in (Hennebert, Hossayni, and Lauradoux, 2013; Hong and Liu, 2015; Sathya, Premalatha, and Rajasekar, 2015) show entropy of a single sensor data is too low to be used as an entropy source for random number generation. Third, most of the studies only include one randomness test, NIST statistical test. It has certain risks to assume a random number sequence is truly random based on only one statistical test suite, as it may be weak to detect certain biases. These issues can be tackled using correct post-processing, conditioning, or whitening methods, such as in (Wallace et al., 2016), where data from multiple sensors are mixed by aggregation, folding, and reduction.

In this chapter, a light-weight mean-removal stochastic energy variation based random number generation method is proposed, which uses accelerometer and gyroscope signals captured during walking for mobile, wearable, and implantable IoT devices.

## 6.1 IMU-Based Random Number Generation

An IMU consists of an accelerometer, a gyroscope, and possibly a magnetometer. As the proposed method is designed for on-body IoT devices and since some wearable and implantable devices may not have magnetometers, the magnetometer data is excluded from this method. Fig. 6.1 shows an example 6-axis IMU signals (i.e 3-axis accelerometer and 3-axis gyroscope signals) captured during normal walking, where clear patterns can be observed. The proposed method generate truly random numbers during walking motion, by executing the following post-processing modules: IMU signal recording, gait cycle detection, mean-removal, bit sequence re-indexing and mixing, and a XOR operation, as shown in both Fig. 6.2 and 6.3. The purpose of these post-processing modules is to remove the periodic and predictable components of the IMU signals during walking, and to use only the stochastic signal energy variations to generate truly random numbers.



(a) 3-axis acceleration ($a$) from Accelerometer (b) 3-axis angular velocity ($\omega$) from Gyroscope

Figure 6.1: Example of 6-axis IMU signals

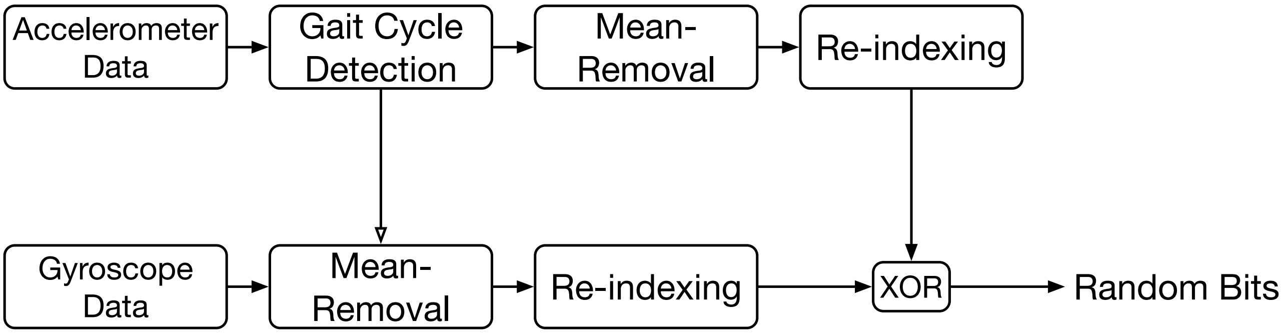


Figure 6.2: Simplified structure of the IMU-based random number generation algorithm

### 6.1.1 Gait Cycle Detection

A gait cycle, as defined in (Whittle, Levine, and Richards, 2012b), is the interval of the time between the occurrence of a repetitive event of walking and the occurrence of the next successive repetitive event, such as heel-strike or toe-off events. In this paper, we use the IMU signals in the time interval of a gait cycle from heel-strike to heel-strike. The algorithm in the gait cycle detection module is modified from (Sun, Wong, et al., 2017), where a low-pass filter is applied to one axis of the IMU signals. The filter's cut-off frequency is 3 Hz, as the average human walking frequency is between

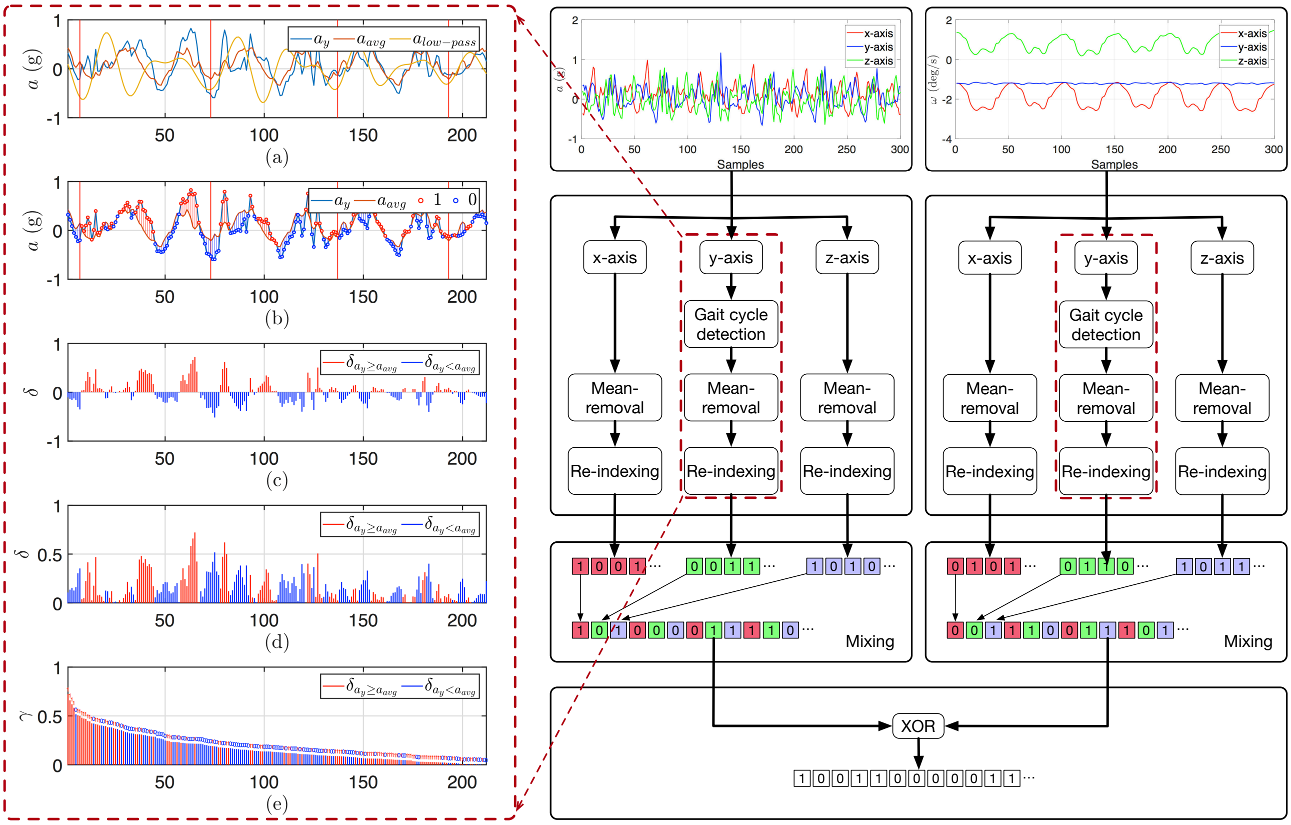


Figure 6.3: Illustration of the IMU-based random number generation algorithm. (a) Gait cycle detection using the 3Hz low-pass filter. (b) Stochastic signal energy variation extraction and bit generation. (c) Raw values of the signal energy differences $\delta$. (d) Absolute values of the signal energy differences $|\delta|$. (e) Re-indexing the generated bits using the descending order $\gamma$ of the absolute values of the signal energy differences $|\delta|$

1.7 and 2.7 Hz (Revadigar, Javali, Xu, Vasilakos, et al., 2017). This is shown in Fig. 6.3 (a), where every two adjacent hill-shape patterns on the filtered signal $a_{low-pass}$ are considered as a gait cycle, and the boundaries between adjacent gait cycles are indicated using red vertical lines.

The purpose of the gait cycle detection is to obtain the time intervals of the gait cycles for calculating the averaged gait cycle (mean) as $a_avg$ in Fig. 6.3 (a). $a_avg$ will be the same for all the gait cycles in the same gait cycle group. As only rough time intervals of the gait cycles are required in the proposed method, we use only the y-axis of the accelerometer signals, where the gravity resides, for the gait cycle detection, and apply the detected gait cycle information to the other axes of the IMU signals afterwards. As the x,y and z of the IMU may not be directly aligned with the anatomical axes and the orientation of the IMU may vary; therefore, the y-axis of the accelerometer is selected by choosing the axis which has the largest mean value among the three axes.

### 6.1.2 Mean-Removal

The purpose of the mean-removal module is to subtract the averaged gait cycle from each gait cycle individually to obtain the stochastic signal energy variations, and it is illustrated in Fig. 6.3 (b) and (c). Assuming a total number of $M$ gait cycles are found in the gait cycle detection module for a IMU signal recording, all the gait cycles are then normalised to the same length, $L = 60$, which is the averaged number of samples in one gait cycle. The normalised gait cycles can be represented as

$$\mathbf{g} = [g_1, g_2, ..., g_m, ..., g_M] \tag{6.1}$$

where $g_m = [f_{m1}, f_{m2}, ..., f_{ml}, ..., f_{mL}]^T$ and $f_{ml}$ represents the $l$-th sample in the $m$-th gait cycle. To calculate the averaged gait cycle (mean), $\mathbf{g}$ is divided into $N$ groups, each of which contains $C$ gait cycles. The grouped gait cycles, $\mathbf{G}$ can be expressed as

$$\mathbf{G} = [G_1, G_2, ..., G_n, ..., G_N] \tag{6.2}$$

where $G_n = [g_n, g_{n+1}, ..., g_{n+c}, ..., g_{n+C}]$ and $N \times C \leq M$. The remained gait cycles that are not enough to form a gait cycle group are discarded. Then, the averaged gait cycle (mean) for the $n$-th group is

$$\alpha_n = \frac{1}{C} \sum_{c=1}^{C} g_{n+c} \tag{6.3}$$

The stochastic signal energy variation for the $m$-th gait cycle, $\delta_m$, is the signal difference between $g_m$ and $\alpha_n$, where $g_m$ belongs to the $n$-th gait cycle group, and it can be expressed using

$$\delta_m = g_m - \alpha_n \text{ and } g_m \in G_n \tag{6.4}$$

A $(C \times L)$-bit binary sequence will be generated from $\delta_m$. In other words, the stochastic signal energy variation for the $l$-th individual sample in the $c$-th gait cycle of the $n$-th group is $\delta_{ncl}$, from which the

$l$-th bit in the $m$-th binary sequence, $b_{ncl} \in \{0,1\}$, is generated using

$$b_{ncl} = \begin{cases} 1, & \delta_{ncl} \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{6.5}$$

Finally, there are $(C \times L \times N)$ bits generated from $M$ gait cycles for each axis of the IMU signals. This process is illustrated in Fig. 6.3 (b), where 1s, indicated as red circles, are generated from the samples who have values higher or equal to the values of the averaged gait cycle (mean), and 0s, indicated as blue circles, otherwise. Fig. 6.3 (c) shows the raw values of the signal energy differences. 1s are generated from the red and positive ones, and 0s are generated from the blue and negative ones.

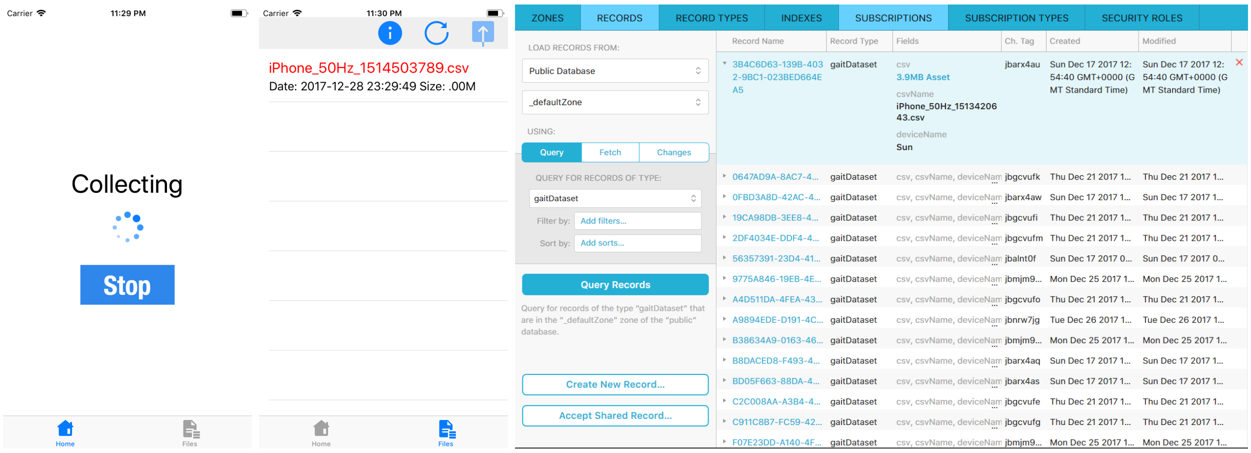
### 6.1.3 Re-Indexing and Mixing

To purpose of the re-indexing module is to further randomise the generated binary sequences using naturally random features (Veen et al., 2006), which are the orders of the absolute values of the energy energy differences in a gait cycle group, as shown in Fig. 6.3 (d). The $n$-th binary sequences are re-indexed using the descending indexes $\gamma_n$ of the energy variations in $G_n$ as

$$\gamma_n = [r_{n1}, r_{n2}, ..., r_{n\mu}, ..., r_{n(C \times L)}] \tag{6.6}$$

where $r_{n\mu} \geq r_{n\mu+1}$, and $r_{n\mu}$ represents the $\mu$-th index of the $n$-th binary sequence in descending order. The re-indexing module, which is illustrated in Fig. 6.3 (e), is applied to every axis of the IMU signals, thus, producing 6 binary sequences. The illustration of the mixing modules in Fig. 6.3 is inspired by (Revadigar, Javali, Xu, Vasilakos, et al., 2017). Then, a mixing process is applied to the binary sequences generated from accelerometer signals and gyroscope signals separately as indicated in Fig. 6.3. The binary sequences generated from the X, Y, and Z axes of the accelerometer signals are sequentially placed in one row following the rule

$$[X_1, Y_1, Z_1, X_2, Y_2, Z_2, ..., X_\mu, Y_\mu, Z_\mu, ..., X_{C \times L}, Y_{C \times L}, Z_{C \times L}] \tag{6.7}$$



iPhone_50Hz_1514503789.csv
Date: 2017-12-28 23:29:49 Size: .00M

LOAD RECORDS FROM: Public Database

_defaultZone

USING: Query

QUERY FOR RECORDS OF TYPE: gaitDataset

Filter by: Add filters...

Sort by: Add sorts...

Query for records of the type "gaitDataset" that are in the "_defaultZone" zone of the "public" database.

| Record Name | Record Type | Fields | Ch. Tag | Created | Modified |
|---|---|---|---|---|---|
| 3B4C6D63-139B-4032-9BC1-023BED664EA5 | gaitDataset | csv<br>3.9MB Asset<br>csvName<br>iPhone_50Hz_1513420643.csv<br>deviceName<br>Sun | jbarx4au | Sun Dec 17 2017 12:54:40 GMT+0000 (GMT Standard Time) | Sun Dec 17 2017 12:54:40 GMT+0000 (GMT Standard Time) |
| 0647AD9A-8AC7-4... | gaitDataset | csv, csvName, deviceNam... | jbgcvufk | Thu Dec 21 2017 1... | Thu Dec 21 2017 1... |
| 0FBD3A8D-42AC-4... | gaitDataset | csv, csvName, deviceNam... | jbarx4aw | Sun Dec 17 2017 1... | Sun Dec 17 2017 1... |
| 19CA98DB-3EE8-4... | gaitDataset | csv, csvName, deviceNam... | jbgcvufi | Thu Dec 21 2017 1... | Thu Dec 21 2017 1... |
| 2DF4034E-DDF4-4... | gaitDataset | csv, csvName, deviceNam... | jbgcvufm | Thu Dec 21 2017 1... | Thu Dec 21 2017 1... |
| 56357391-23D4-41... | gaitDataset | csv, csvName, deviceNam... | jbalnt0f | Sun Dec 17 2017 0... | Sun Dec 17 2017 0... |
| 9775A846-19EB-4E... | gaitDataset | csv, csvName, deviceNam... | jbmjm9... | Mon Dec 25 2017 1... | Mon Dec 25 2017 1... |
| A4D511DA-4FEA-43... | gaitDataset | csv, csvName, deviceNam... | jbgcvufo | Thu Dec 21 2017 1... | Thu Dec 21 2017 1... |
| A9894EDE-D191-4C... | gaitDataset | csv, csvName, deviceNam... | jbnrw7jg | Tue Dec 26 2017 1... | Tue Dec 26 2017 1... |
| B38634A9-0163-46... | gaitDataset | csv, csvName, deviceNam... | jbmjm9... | Mon Dec 25 2017 1... | Mon Dec 25 2017 1... |
| B8DACED8-F493-4... | gaitDataset | csv, csvName, deviceNam... | jbarx4aq | Sun Dec 17 2017 1... | Sun Dec 17 2017 1... |
| BD05F663-88DA-4... | gaitDataset | csv, csvName, deviceNam... | jbarx4as | Sun Dec 17 2017 1... | Sun Dec 17 2017 1... |
| C2C008AA-A3B4-4... | gaitDataset | csv, csvName, deviceNam... | jbgcvufe | Thu Dec 21 2017 1... | Thu Dec 21 2017 1... |
| C911C8B7-FC59-42... | gaitDataset | csv, csvName, deviceNam... | jbgcvufg | Thu Dec 21 2017 1... | Thu Dec 21 2017 1... |
| F07E23DD-A140-4F... | gaitDataset | csv, csvName, deviceNam... | jbmjm9... | Mon Dec 25 2017 1... | Mon Dec 25 2017 1... |

(a) (b) (c)

Figure 6.4: (a) Screenshot of data collecting user interface. (b) Screenshot of the local file management user interface. (c) Screenshot of the cloudkit-based online database

The same rule is also applied to gyroscope signals, resulting two mixed binary sequences for each gait cycle group. Finally, the two binary sequences are bitwise-XOR operated, as combining two entropy sources can improve randomness (Dinca and Hancke, 2017), to produce the final $(3 \times C \times L)$-bit random binary sequence, which can be used as it is or be converted into decimals (random numbers) depending on the requirements of the applications.

## 6.2 Experimental Set-up

The proposed method was evaluated by conducting a series of experiments, using a Real World Human Activity Recognition (HAR) dataset from (Sztyler, Stuckenschmidt, and Wolfgang, 2017), which contains averaged 10 to 12 minutes IMU recordings from 15 subjects and our walking dataset which contains averaged 3.17 hours IMU recordings from 6 subjects. There are 7 sensors placed on each subject in the HAR dataset, and we selected the IMU recordings from right thigh positions to be tested in the experiments. When collecting the data in our walking dataset, subjects were instructed to place the mobile phone in the right trouser pockets, and walk freely in the streets or parks.

To assure the real-world scenario, the use of mobile phones, such as making phone calls, were allowed. An iOS application, as shown in Fig. 6.4 (a) and (b), was created for the purpose of collecting and uploading IMU data to a cloudkit-based database, as shown in Fig. 6.4 (c). The sensor data files were then downloaded to a computer running 64-bit Windows 10 Enterprise version 1703, and the proposed method was implemented in Matlab R2017a.

All the generated random numbers were stored in an ASCII file for NIST and Dieharder tests, and a binary file for ENT and RaBiGeTe tests. All the tests were performed on the same computer but in virtual machines. In detail, NIST STS-2.1.2, Dieharder 2.24.1, and ENT (28/01/2008) were installed and used in Ubuntu 16.04 virtual environment, and RaBiGeTe 32-bit version 2.0.0 with graphical user interfaces was installed and used in 32-bit Windows 7 Home basic N SP1 build 7601 virtual environment.

## 6.3 Randomness Tests

We tested the random numbers generated from both our dataset and the HAR walking dataset using four randomness tests, which are explained in this section. All the test results will be presented and evaluated in the results section.

NIST-STS has been adopted by most researchers for testing the randomness of binary sequences. Our experiments were carried out by following the instructions provided by the official documentation NIST SP 800-22 (Rukhin et al., 2010) and an explanatory journal article on the interpretation of the NIST-STS results (Sys et al., 2015). The latest NIST-STS version 2.1.2 includes 15 tests, each of which is designed to test a pre-defined null hypothesis (the tested sequence is random, notated as $H_0$) and also produces a probability value (p-value) in the range of the interval [0,1). When evaluating the results from a test, the p-value produced by the test is compared with a constant $\alpha$, which is the significance level that can be set by the user. If the p-value is larger than $\alpha$, its $H_0$ is accepted, otherwise rejected. Moreover, two types of errors , Type I, where $H_0$ is rejected but the tested sequence is actually from a good RNG and Type II, where $H_0$ is accepted but the sequence is not random, are defined. The probability of Type II error occurring is denoted as $\beta$, which is related to $\alpha$ and in practice calculated by the NIST-STS.

ENT is a pseudo-random number sequence test program, which evaluates PRNGs for applications such as encryption and compression (Walker, 2008). The ENT consists of the following tests:

1. Entropy: it is the information density of the test random number sequences, expressed as a number of bits per byte. The percentage of the sequence, which can be reduced by optimum compression, is also calculated
2. Chi-square Distribution: it indicates how often a value, which is calculated based on the stream of bytes, is exceeded
3. Arithmetic Mean: it is the sum of all the bytes in the test sequence, dividing by the sequence length
4. Monte Carlo Value for $\pi$: every six bytes of the test sequence are converted into rectangular coordinates within a square, and a hit is made if a random point is less than the radius of a circle inscribed within the square. The percentage of hits is the Monte Carlo Value for $\pi$, which should be close to the value of $\pi$ for random sequences
5. Serial Correlation Coefficient: it measures the correlations between every successive bytes in the test sequences, which should be close to 0 for random sequences

Dieharder consists of tests from Diehard and many improved tests from NIST-STS. Some of the unique tests that Dieharder provides are listed as followings (Brown, 2004):

1. Birthday: to test whether the spacings of random intervals from the test sequences follows a Poisson distribution
2. Bitstream: to test the sequences by considering them as streams of bits or overlapping ‘words’
3. OPSO: Overlapping Pairs Sparse Occupancy test converts the test sequences into 2-letter words and determines whether the number of missing words follows a normal distribution
4. OQSO: Overlapping Quadruples Sparse Occupancy test uses 4-letter words instead of 2-letter words
5. DNA: to test whether the number of missing 10-letter words, which consists of 4 letters, C, G, A, and T, follows a normal distribution
6. Parking Lot: to test whether the number of successful attempts to randomly park a $1^2$ car on a $100^2$ parking lot follows a normal distribution

7. Craps: to test whether the number of wins when plays 200,000 games of craps using the test sequences follows the excepted normal distribution
8. Marsaglia and Tsang GCD: to test whether the test sequences can pass the greatest common divisor test developed by (Marsaglia, Tsang, et al., 2002)
9. RGB Kolmogorov-Smirnov: to test the uniformity by applying an Anderson-Darling or Kuiper KS test to a vector of uniform deviates from the test sequences (Brown, 2004)

RaBiGeTe is a multi-threaded highly configurable windows-based RNG tester (Cristiano, 2011) that includes some of the tests in the NIST-STS and Dieharder. Therefore, only the tests that are unique in RaBiGeTe are listed as followings:

1. AMLS: it is based on the bits generated using Mitzenmacher's advanced multi-level strategy (Mitzenmacher, 2008), where Von Neumann's rule are applied to the test sequences in predefined orders
2. Coupon Collector's test: to test whether the distribution of the lengths of successive 'full sets' of digits from 0 to $d-1$, of the test sequences, are as expected (Greenwood, 1955)
3. Maurer: to test any major deviations of the statistics of the test sequences from the statistics of a truly random binary source, proposed by Maurer (1992)
4. Permutation: to obtain the permutation distribution of the test sequences under the null hypothesis by re-sampling the test sequences (Rice and Lumley, 2008)
5. Windowed Autocorrelation: to test the correlations between the bits in the test sequences

## 6.4 Results

### 6.4.1 NIST

The NIST results for the random numbers generated from our dataset and the HAR walking dataset are listed in Table 6.1. The lengths of the test sequences for our datasets, the HAR walking dataset, and

Blum-Blum-Shub (BBS) referencing PRNG provided by the NIST-STS program were set to 100,000, except the ones for the Universal test, which were set to 1,000,000. However, the HAR dataset was not tested using the Universal test, as it requires at least 1,000,000 samples in each test sequence. The p-values listed in Table 6.1 are from the uniformity test, which indicates how uniform the p-values (of individual statistical tests) are distributed in the interval [0,1), which should be larger than 0.0001 for good RNGs. The minimum pass rate (with the exception of the Random Excursion, Random Excursion Variant, and Universal tests) for our dataset and BBS is approximately 96% (96/100), and the minimum pass rates for the Random Excursion (Variant) tests and the Universal test are 88.8% (8/9) and 80% (8/10) respectively. On the other hand, the minimum pass rate (with the exception of the Random Excursion (Variant) tests) for the HAR dataset is approximately 85.7% (12/14). As there are multiple Non-Overlapping Template, Random Excursions, and Random Excursions Variant tests, the p-values from each group of the same tests are averaged (as indicated using $^{*}$), and the proportions that have passed the tests are accumulated (as indicated using $^{+}$). The individual proportions for these tests, which are all greater than the corresponding minimum pass rates, are not shown in Table 6.1. To summarise, the random numbers generated from both datasets passed all the NIST tests with very high efficiency.

Table 6.1: NIST-STS results for the random numbers generated from our dataset, HAR dataset, and BLum-Blum-Shub referencing PRNG provided in the NIST-STS program ($^{*}$: averaged value; $^{+}$: accumulated value)

| | Our dataset | | HAR dataset | | Blum-Blum-Shub | |
|---|---|---|---|---|---|---|
| Statistical tests | p-value | Proportion | p-value | Proportion | p-value | Proportion |
| Frequency | 0.017912 | 96/100 | 0.035174 | 14/14 | 0.816537 | 98/100 |
| Block Frequency | 0.304126 | 96/100 | 0.350485 | 14/14 | 0.366918 | 100/100 |
| Cumulative Sums (Forward) | 0.883171 | 97/100 | 0.122325 | 14/14 | 0.955835 | 98/100 |
| Cumulative Sums (Reverse) | 0.657933 | 97/100 | 0.534146 | 14/14 | 0.401199 | 99/100 |
| Runs | 0.202268 | 100/100 | 0.213309 | 14/14 | 0.090936 | 99/100 |
| Longest Run | 0.779188 | 97/100 | 0.066882 | 14/14 | 0.202268 | 99/100 |
| Rank | 0.883171 | 100/100 | 0.008879 | 14/14 | 0.202268 | 98/100 |
| FFT | 0.115387 | 96/100 | 0.739918 | 14/14 | 0.275709 | 100/100 |
| Non Overlapping Template (148) | $0.535721^{*}$ | $14638/14800^{+}$ | $0.228108^{*}$ | $2042/2072^{+}$ | $0.518429^{*}$ | $14655/14800^{+}$ |
| Overlapping Template | 0.851383 | 100/100 | 0.213309 | 14/14 | 0.455937 | 99/100 |
| Universal | 0.739918 | 10/10 | - | - | 0.017912 | 10/10 |
| Approximate Entropy | 0.419021 | 99/100 | 0.008879 | 13/14 | 0.971699 | 99/100 |
| Random Excursions (8) | - | $72/72^{+}$ | - | $8/8^{+}$ | $0.571206^{*}$ | $80/80^{+}$ |
| Random Excursions Variant (18) | - | $156/162^{+}$ | - | $18/18^{+}$ | $0.548565^{*}$ | $180/180^{+}$ |
| Serial (Forward) | 0.455937 | 99/100 | 0.213309 | 14/14 | 0.739918 | 99/100 |
| Serial (Reverse) | 0.897763 | 98/100 | 0.122325 | 14/14 | 0.037566 | 98/100 |
| Linear Complexity | 0.383827 | 100/100 | 0.350485 | 14/14 | 0.145326 | 100/100 |

Table 6.2: ENT results for the random numbers generated from our dataset and HAR dataset

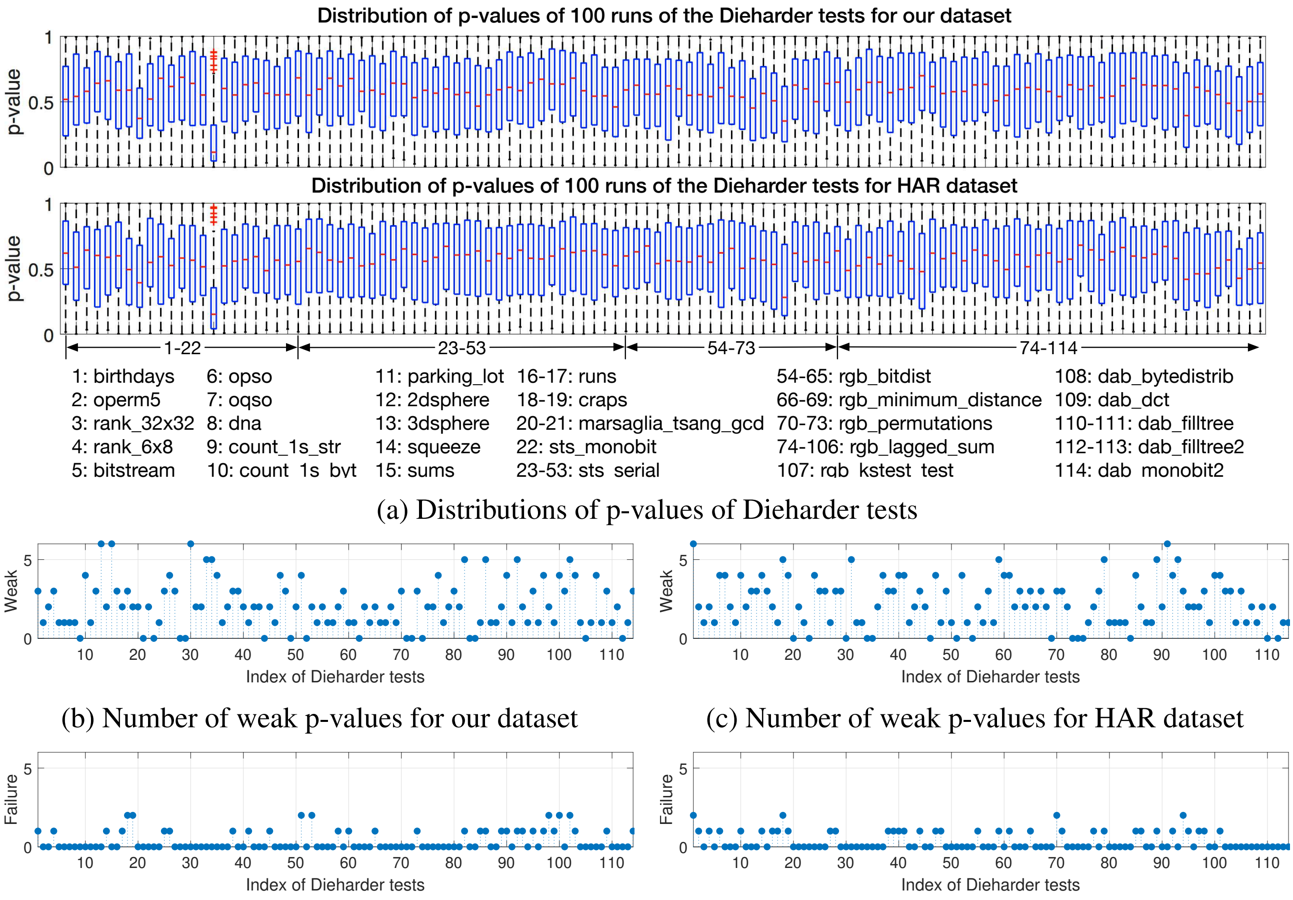
| | Our dataset | HAR | Completely random |
|---|---|---|---|
| Entropy | 7.999848 bits/byte | 7.998900 bits/byte | 8 bits/byte |
| Optimum compression | 0% | 0% | 0% |
| Chi square distribution | 282.32 (p=11.54%) | 282.80 (p=11.15%) | 1% <p <99% |
| Arithmetic mean | 127.5753 | 127.7763 | 127.5 |
| Monte Carlo value | 3.140367341 (e=0.04%) | 3.130744557 (e=0.35%) | 3.141592654 (e=0.00%) |
| Serial correlation coefficient | 0.001383 | -0.003812 | 0 |

### 6.4.2 ENT

The ENT test results for our dataset and the HAR walking dataset are listed in Table 6.2. The last column in Table 6.2 lists the expected values for completely random sequences. All the ENT results indicate good randomness for the random numbers generated from both our dataset and the HAR dataset. Additionally, the random numbers generated from our dataset perform slightly better (closer to the expected values) than the ones from the HAR dataset, which is possibly due to the larger size of our dataset.

### 6.4.3 Dieharder

The p-value distributions, the number of weak p-values, and the number of failure p-values of the Dieharder tests for the random numbers generated from both our dataset and the HAR walking dataset are presented in Fig. 6.5. It is important to note that the null hypothesis in Dieharder test differs from the ones used in the NIST-STS tests. Weak p-values (p<0.5% or p>99.5%) is expected 5% on average from any Dieharder tests for a good RNG, meanwhile failure p-values (p<0.05% or p>99.95%) should rarely occur. Furthermore, the distribution of p-values for a Dieharder test should in turn be uniformly distributed between the interval [0,1) (Brown, 2004; SysTutorials, n.d.). The distributions for 100 runs of the Dieharder tests for both datasets are evenly distributed in [0,1), except for the sums tests (No. 15), where a bias towards 0 can be observed. Although it is not uniformly distributed, the weak p-values of sums tests are less than 5%, thus it is not too weak for attackers to exploit. Additionally, the number of weak p-values for all the Dieharder tests are equal or less than 6%, and the number of failure p-values for all the tests are equal or less than 3%. It is safe to conclude that the random numbers generated from both datasets passed the Dieharder tests.



(a) Distributions of p-values of Dieharder tests

(b) Number of weak p-values for our dataset

(c) Number of weak p-values for HAR dataset

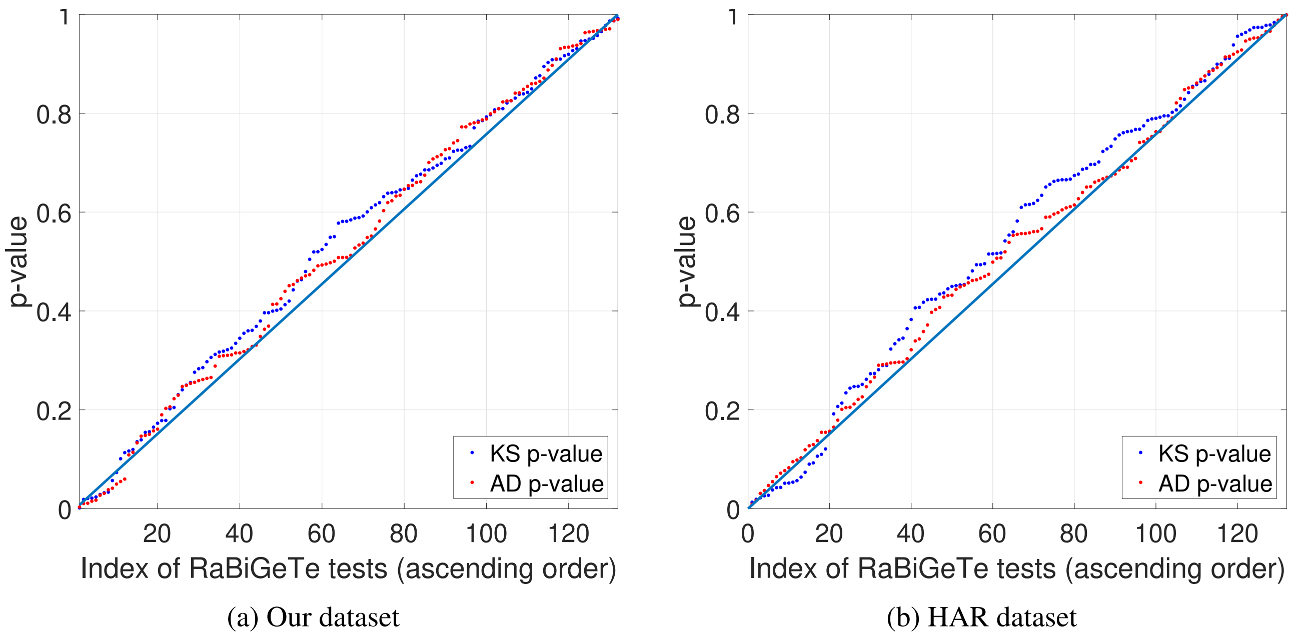
(d) Number of failure p-values for our dataset

(e) Number of failure p-values for HAR dataset

Figure 6.5: Dieharder test results

### 6.4.4 RaBiGeTe

Table 6.3 lists the overall Kolmogorov-Smirnov (KS) p-values and Anderson-Darling (AD) p-values for some statistical tests applied in RaBiGeTe. KS and AD p-values indicate whether the tested random numbers are randomly distributed, and any p-values less than 0.00001 or greater than 0.99999 is considered a failure to the corresponding statistical test. As listed in Table 6.3, no KS or AD p-value exceeds the range of 0.00001 to 0.99999, thus both our dataset and the HAR walking dataset passed all the RaBiGeTe tests. Furthermore, Fig. 6.6a and Fig. 6.6b are the Straight Line (SL) test results, where the distributions of the ascending ordered KS and AD p-values obtained from 132 sub-tests in RaBiGeTe default settings for both datasets. The blue straight line is the ideal positions of the p-values. The closer the p-values are to the line, the more uniformly distributed they are. As shown in Fig. 6.6, both datasets passed the SL tests.



(a) Our dataset

(b) HAR dataset

Figure 6.6: RaBiGeTe Straight Line (SL) test results

## 6.5 Discussion

The use of inertial sensors for generating random numbers has been proposed by other previous research. For instance, Voris, Saxena, and Halevi (2011) discussed the feasibility of using an accelerometer as the entropy source for RNGs on ubiquitous devices, and implemented an accelerometer-based RNG on a RFID tag. The authors demonstrated the resilience of accelerometer-based RNGs against adversaries and environmental variations via comparative analysis with adversarial modelling. However, Hennebert, Hossayni, and Lauradoux (2013) observed far less entropy than expected in their experiments on entropy harvesting from physical sensors, and argued that the amount of min-entropy reported in (Voris, Saxena, and Halevi, 2011) was overestimated.

Moreover, Dinca and Hancke (2017) studied using smart-phone sensors as entropy sources for random number generation during human gait, and concluded that the raw data collected from smart-phone sensors on the subjects during randomly walking on the city streets is highly predictable. The authors also argued that using data from any combination of two sensors can only slightly improve randomness. To ensure the randomness of the numbers generated, in our proposed method, a mean-removal algorithm is proposed to remove regular patterns of the IMU signals during walking and use only the stochastic signal energy variation for random number generation.

Table 6.3: RaBiGeTe statistical test results (KS: Kolmogorov-Smirnov, AD: Anderson-Darling, SL: straight line, CM: Cramer-von Mises, SW: Shapiro-Wilk, CC: Pearson's correlation coefficient, AV: absolute value correlation coefficient)

| | Our dataset | | HAR dataset | |
|---|---|---|---|---|
| | KS | AD | KS | AD |
| KS | 0.36137 | 0.83739 | 0.07815 | 0.47745 |
| AD | 0.75118 | 0.87342 | 0.06660 | 0.58350 |
| SL | 0.67879 | 0.90847 | 0.08402 | 0.59756 |
| CM | 0.60727 | 0.89412 | 0.06246 | 0.49069 |
| SW | 0.38089 | 0.28437 | 0.30779 | 0.71776 |
| CC | 0.44210 | 0.92092 | 0.05401 | 0.71767 |
| AV | 0.43196 | 0.92605 | 0.05629 | 0.62781 |

Many methods have been proposed on how to increase the randomness of the bits generated directly from raw sensor data in a post-processing manner. Suciu, Lebu, and Marton (2011) proposed a mobile sensors based RNG, where $z$, based on the user's selection, least significant bits of a GPS, an accelerometer, a magnetometer, and an orientation sensor are combined and concatenated. Similarly, A. Marghescu and G. Teseleanu proposed a sensor-based RNG using four types of Von Neumann randomness extractors to increase the quality and the throughput of the RNG. Loutfi et al. (2014) presented a smart-phone sensor based RNG design, where the NIST Secure Hash Algorithms (SHA) hashing family is used to whiten the bit sequences generated from raw 32-bit sensor data streams.

Hong and Liu (2015) and Sathya, Premalatha, and Rajasekar (2015) both applied Wash-Rinse-Spin method on raw sensor data to increase randomness. Wash is designed to remove drifting patterns, Rinse is implemented to remove data points that process less entropy, and Spin is developed to use sensor data as PRNG seeds to produce larger and longer sequences of pseudo-random numbers (Hong and Liu, 2015). However, these methods only whitens the raw sensor data or uses the raw sensor data as PRNG seeds, which, as aforementioned, are vulnerable to brute-force attacks if the randomness of the seed selection is week.

In a similar work, Wallace et al. (2016) proposed an experimental framework called SensoRNG, where only the bits, from various smart-phone sensors, with sufficient randomness are selected, aggregated, and mixed to produce random numbers. When testing against NIST-STS, SensoRNG has weak p-values in the runs test and rank test, and no Non Overlapping Template, Overlapping Template, Universal, Random Excursions, and Random Excursions Variant test results are reported in the paper. Whereas our proposed method passed all NIST-STS tests with high efficiency.

## 6.6 Conclusions

In this chapter, a random number generation method using IMU signals and stochastic signal energy variation is proposed for securing on-body IoT devices. The use of a mean-removal algorithm has been proposed to reduce patterns and to enhance randomness. The proposed method was tested with our dataset and the HAR walking dataset, and the generated random numbers passed all the tests in four randomness test suites, namely NIST-STS, ENT, Dieharder, and RaBiGeTe. Therefore, we demonstrated the feasibility and the robustness of our proposed IMU-based random number generation method for on-body IoT devices.

The designs and test results for proposed gait-based RNG are still preliminary, but they present great potentials of gait-based RNGs for IoT healthcare systems in many ways, such as for generating temporary identities for newly registered devices. Moreover, the random numbers generated from proposed gait-based RNG can also be used as seeds for traditional PRNGs to generate pseudo random numbers. This will increase the output bit rate of the generator while maintaining randomness. As inertial measurement units are very small and not power hungry, the proposed gait-based RNG can be implemented in a system-on-a-chip fashion, which can be used in cryptographic devices and applications, such as key cards.

# Chapter 7

# Conclusion

This thesis presents novel methods regarding EEG and gait biometrics for securing wireless communications among BSN sensors and coordinators, as well as BSN/IoT-based healthcare systems. In the following sections, a summary of the achievements and contributions of the thesis is presented. Then a discussion of future research directions and works of the EEG and gait biometrics for securing healthcare applications is presented in the final section of this thesis.

Chapters on gait biometrics indicate that the correlations of gait signals from different body positions are sufficient to be used for on-body device authentication and data encryption. However, one of the limitations of using IMU-based gait biometrics is that it can only be used for on-body wireless communications, such as wearable device pairing; or for mobile device authentication, where the position of the mobile device has to be fixed to maintain authentication performance. The trend of gait biometric research is on camera-based gait recognition in the wild, which can be used for identifying criminals and detecting pedestrians. In addition, the fusion of IMU-based gait biometrics with other wearable sensors, such as multiple IMU sensors at different body positions, Electromyography (EMG) sensors, and on-body cameras, is also a promising future research direction.

## 7.1 Summary of Thesis Achievements

The main technical achievements of the work presented in this thesis include:

- Introduced a light-weight symmetric key generation scheme based on gait event timing (temporal gait) from inertial signals;
- Proposed a deep learning approach for gender and age recognition using a single inertial sensor;
- Designed and developed an Artificial Neural Network framework for lower limb motion signal estimation;
- Presented an improved key generation scheme based on ANN-based gait signal estimation and fuzzy key exchange;
- Developed of a random number generation method using gait signals and stochastic signal energy variation for on-body IoT devices;
- Derived a 1D-convolutional LSTM approach for EEG-based user identification for securing IoT-based healthcare systems.

The thesis started with an introduction of the challenges and issues of the security measures of the current healthcare systems in the first two chapters. By reviewing state-of-the-art methodologies, many new perspectives on how to tackle the challenges of applying EEG and gait biometrics in BSN security were found and presented.

A novel EEG-based user identification system was proposed in Chapter 3, where 1D-convolutional LSTM approach was presented in detail. The system extracts spatiotemporal features resided in the EEG signals with better performance than state-of-the-art deep learning approaches, and it can be used to reduce the number of EEG channels required by the systems, subsequently reducing the costs of the systems.

As EEG headsets are still cumbersome in size and not suitable for low-power BSN sensors. In Chapter 4, a novel light-weight symmetric key generation scheme was presented, where gait event timing as the common entropy source for cryptography. Moreover, the influence of gender and age for gait biometrics was also investigated in the second part of the chapter. Through assessing the gender and age recognition using only inertial sensors, it can be concluded that a person's gait is unlikely to change once he/she reaches adulthood.

To improve intra-class key matching rates of the gait-based symmetric cryptosystem, Chapter 5 focused on improving the symmetric key generation scheme by applying Artificial Neural Network to increase the correlations among gait signals from sensors located at different body positions. The first part of the chapter presented a novel lower limb motion estimation method using two inertial sensors attached to the ankles, and the second part extended the proposed method to generate higher correlations among gait signals collected from different positions, which can be used as the common entropy source for cryptography.

To explore the possibility of using gait signals to generate random numbers, Chapter 6 presented a novel random number generation method for securing on-body IoT devices based on temporal signal variations of gait signals. The method was rigorously tested and passed using four widely adopted randomness test suites.

## 7.2 Future Research Directions

The work presented in this thesis can be categorised into three directions: using EEG signals for user identification applications, using inertial gait signals for secure key generation, and using inertial gait signals for random number generation.

First of all, the future research directions of the proposed schemes in Chapter 3 would be to further testing its scalability by retraining the networks with EEG data from other databases. Further investigation on which EEG channels are the most effective ones for distinguishing different users are useful for reducing costs of the security systems. In addition, development of an automatic channel selection algorithms instead of manual channel selection is also an interesting future research direction. with respect of deep learning on EEG biometrics, as training a new deep learning network is time consuming, transfer learning technique should be introduced to reduce time consumption for adding new users in the fully trained deep learning networks. In addition, the fusion of EEG with other biometric traits is an interesting topic as it would potentially be used to design more secured identification systems.

Next, for using inertial gait signals for secure key generation of symmetric cryptosystems, the future research directions are follows: first, investigate other fuzzy systems for binary sequence correcting, such as fuzzy vault. The fuzzy commitment scheme used in the proposed key generation scheme is light-weight but can only recover keys that have sufficient identical bits to the original keys, whereas fuzzy vault can distinguish keys that have even less identical bits but with higher computational complexity. With recent advancement in the miniaturised on-body devices in terms of on-node resource and power consumption, such intense computations can be achieved without compromising the performance of other parts of the systems.

Then, for the proposed method in Chapter 5 uses an ANN framework for estimating gait signals at other body positions. The future work can be exploring more advanced machine learning techniques, such as deep learning. In addition, other periodical sensor signals captured by BSN sensors can also be estimated or predicted. Such approach can significantly reduce the number of the sensors needed for healthcare applications that does not require high accuracy sensor data. The predicted sensor data can also be used for validating of real sensor data, preventing malicious man-in-the-middle attacks.

Finally, for using inertial gait signals for random number generation for securing on-body IoT devices, the future research directions are as follows. First, the proposed gait-based RNG could be extended for many applications, such as for generating temporary identities for newly registered devices. Second, the random numbers generated from proposed gait-based RNG can also be used as seeds for traditional PRNGs to generate pseudo random numbers. This will increase the output bit rate of the generator while maintaining randomness. Third, as inertial measurement units are very small and low power, the proposed gait-based RNG can be implemented in a system-on-a-chip approach, which can be used in cryptographic devices and applications, such as key cards. These applications are practical therefore can be further developed into patients or commercialised services.

# Abbreviations

**6LoWPAN** IPv6 over Low-Power Wireless Personal Area Networks. 18

**ABE** Attribute-Based Encryption. 22

**AES** Advanced Encryption Standard. 35

**ANN** Artificial Neural Network. 7

**BAR** Bit Agreement Rate. xvi, 88

**BCH** Bose-Chaudhuri-Hocquenghem. 87

**BCS** Biometric Cryptosystem. 78

**BEL** Base Encryption Layer. 22

**BLE** Bluetooth Low Energy. 12

**BSNs** Body Sensor Networks. 1

**CC** Correlation Coefficient. 108

**CIA** Confidentiality-Integrity-Availability. 18

**CNN** Convolutional Neural Network. 58

**CoAP** Constrained Application Protocol. 18

**DoF** Degree-of-Freedom. 105

**DoS** Denial of Service. 23

**DSA** Digital Signature Algorithm. 11

**DTLS** Datagram Transport Layer Security. 18

**ECC** Elliptic Curve Cryptography. 23

**ECG** Electrocardiogram. 16

**EEG** Electroencephalographic. 3

**EER** Equal Error Rate. 29

**EHR** Electronic Health Record. 21

**EMR** Electronic Medical Record. 21

**FAR** False Acceptance Rate. 27

**FDA** Food and Drug Administration. 25

**FFT** Fast Fourier Transform. 79

**FPGA** Field Programmable Gate Array. 37

**FRR** False Rejection Rate. 27

**FT** Fourier Transform. 53

**FTA** Failure-to-Acquire Rate. 29

**FTE** Failure-to-Enrol Rate. 29

**GDPR** General Data Protection Regulation. 12

**HAR** Human Activity Recognition. 123

**HD** Hamming Distance. 131

**HMM** Hidden Markov Model. 54

**ICO** Information Commissioner's Office. 12

**IMD** Implantable Medical Device. 38

**IMUs** Inertial Measurement Units. 3

**IoT** Internet of Things. 7, 10

**IPI** Inter-pulse Interval. 31

**IPM** Inverted Pendulum Model. 52

**IPsec** Internet Protocol Security Framework. 18

**KNN** K-Nearest Neighbour. 53

**LoT** Location of Things. 19

**LSTM** Long Short-Term Memory. 6

**MONN** multiple-output-neural-net. 106

**NB** Naive Bayesian. 53

**NFC** Near-Field Communication. 12

**NIST** National Institute of Standards and Technology. 134

**OTA** Over-the-air. 20

**PD** Parkinson's Disease. 46

**PPG** Photoplethysmographic. 27

**PRE** Proxy Re-Encryption. 22

**PRNG** Pseudo-Random Number Generator. 35

**QoS** Quality of Service. 16

**QRNG** Quantum Random Number Generator. 36

**RFID** Radio-Frequency IDentification. 12

**RNN** Recurrent Neural Network. 58

**ROC** Receiver Operating Characteristic. 29

**RSA** Rivest-Shamir-Adleman. 11

**RSSI** Received Signal Strength Indication. 41

**SEL** Surface Encryption Layer. 22

**SONN** single-output-neural-net. 106

**SVM** Support Vector Machine. 41

**TRNG** True Random Number Generator. 35

**VEP** Visually Evoked Potential. 60

**WBAN** Wireless Body Area Network. 12

**WSN** Wireless Sensor Network. 35

**WT** Wavelet Transform. 53

# Bibliography

Abellan, C et al. (2014). “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode”. In: *Optics express* 22.2, pp. 1645–1654 (cit. on p. 36).

Abhayasinghe, N and I Murray (2014). “Human gait phase recognition based on thigh movement computed using IMUs”. In: *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 1–4 (cit. on p. 49).

Abreu, M. and M. Fairhurst (Sept. 2011). “Enhancing Identity Prediction Using a Novel Approach to Combining Hard- and Soft-Biometric Information”. In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 41.5, pp. 599–607 (cit. on p. 90).

Agostini, V et al. (2015). “Wearable sensors for gait analysis”. In: *2015 IEEE International Symposium on Medical Measurements and Applications (MeMeA) Proceedings*, pp. 146–150 (cit. on p. 103).

Ahmadi, A et al. (2016). “3D Human Gait Reconstruction and Monitoring Using Body-Worn Inertial Sensors and Kinematic Modeling”. In: *IEEE Sensors Journal* 16.24, pp. 8823–8831 (cit. on p. 103).

Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak (2012). “Security and privacy issues in wireless sensor networks for healthcare applications”. In: *Journal of medical systems* 36.1, pp. 93–101 (cit. on pp. 18, 24).

Allison, Peter R. (2016). *The problem of passwords and how to deal with it*. URL: `https://www.computerweekly.com/feature/The-problem-of-passwords-and-how-to-deal-with-it` (cit. on p. 57).

Almeida, Fernando Mendonca de, Admilson de Ribamar Lima Ribeiro, and Edward David Moreno (2015). "An architecture for self-healing in Internet of Things". In: *UBICOMM 2015*, p. 89 (cit. on p. 19).

AlTawy, Riham and Amr M Youssef (2016). "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices". In: *IEEE Access* 4, pp. 959–979.

Altman, D. G. (1990). *Practical Statistics for Medical Research*. 1st ed. Chapman and Hall/CRC (cit. on p. 126).

Altop, D K, A Levi, and V Tuzcu (May 2015). "Towards using physiological signals as cryptographic keys in Body Area Networks". In: *2015 9th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth)*, pp. 92–99 (cit. on p. 131).

Anang, Nurhazwani et al. (2016). "Analysis of kinematic gait parameters in chronic stroke survivors". In: *2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pp. 57–62 (cit. on p. 45).

Andrea, I, C Chrysostomou, and G Hadjichristofi (2015). "Internet of Things: Security vulnerabilities and challenges". In: *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180–187 (cit. on p. 25).

Ankaral, Z Esat et al. (2015). "Physical layer security for wireless implantable medical devices". In: *Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015 IEEE 20th International Workshop on*. IEEE, pp. 144–147 (cit. on p. 39).

Aqmar, M R, K Shinoda, and S Furui (2012). "Efficient model training for HMM-based person identification by gait". In: *Signal & Information Processing Association Annual Summit and Conference (APSIPA ASC), 2012 Asia-Pacific*, pp. 1–4 (cit. on pp. 54, 56).

Arango Paredes, Juan David et al. (2015). "A reliability assessment software using Kinect to complement the clinical evaluation of Parkinsons disease". In: *International Conference of the Ieee Engineering in Medicine and Biology Society (Embc)*, pp. 6860–6863 (cit. on p. 47).

Arevalo, J C et al. (2012). "Parameterized inverted and double pendulum model for controlling lower-limb active orthosis". In: *Robotics and Biomimetics (ROBIO), 2012 IEEE International Conference on*, pp. 1899–1905 (cit. on p. 52).

Arias, O et al. (2015). "Privacy and Security in Internet of Things and Wearable Devices". In: *IEEE Transactions on Multi-Scale Computing Systems* 1.2, pp. 99–109 (cit. on p. 140).

Arnau-Gonzalez, P et al. (Oct. 2017). "ES1D: A Deep Network for EEG-Based Subject Identification". In: *2017 IEEE 17th International Conference on Bioinformatics and Bioengineering (BIBE)*, pp. 81–85 (cit. on pp. 34, 61, 75).

Aronson, Ronnie et al. (2018). *Fully Implantable, Continuous Glucose Monitoring Sensor Provided Accuracy for Six Months in Adolescents and Adults with Type 1 Diabetes*. URL: http://www.diabetes.org/newsroom/press-releases/2018/implantable-cgm-sensor-provided-accuracy-for-six-months.html.

Atallah, L, A Wiik, et al. (2014). "Gait asymmetry detection in older adults using a light ear-worn sensor." In: *Physiological measurement* 35.5, pp. 29–40 (cit. on p. 48).

Atallah, Louis, Gareth G. Jones, et al. (2011). "Observing recovery from knee-replacement surgery by using wearable sensors". In: *Proceedings - 2011 International Conference on Body Sensor Networks, BSN 2011*, pp. 29–34 (cit. on pp. 48, 53).

Atallah, Louis, Benny Lo, Rachel King, et al. (2011). "Sensor positioning for activity recognition using wearable accelerometers". In: *IEEE Transactions on Biomedical Circuits and Systems* 5.4, pp. 320–329 (cit. on p. 46).

Atallah, Louis, Benny Lo, Guang Zhong Yang, et al. (2009). "Detecting walking gait impairment with an ear-worn sensor". In: *Proceedings - 2009 6th International Workshop on Wearable and Implantable Body Sensor Networks, BSN 2009*, pp. 175–180 (cit. on p. 48).

Azeez, Nureni Ayofe and Charles Van der Vyver (2018). "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis". In: *Egyptian Informatics Journal* (cit. on p. 21).

Aziz, Omer et al. (2006). "Pervasive Body Sensor Network : An Approach to Monitoring the Post-Operative Surgical Patient." In: *Networks*, pp. 18–21 (cit. on p. 48).

Bales, Dustin et al. (2016). "Gender classification of walkers via underfloor accelerometer measurements". In: *IEEE Internet of Things Journal* 3.6, pp. 1259–1266 (cit. on p. 92).

Ball, A et al. (2012). “Unsupervised clustering of people from skeleton data”. In: *Human-Robot Interaction (HRI), 2012 7th ACM/IEEE International Conference on*, pp. 225–226 (cit. on pp. 54, 56).

Bamberg, Stacy J Morris et al. (2008). “Gait analysis using a shoe-integrated wireless sensor system”. In: *IEEE Transactions on Information Technology in Biomedicine* 12.4, pp. 413–423 (cit. on p. 49).

Bao, S D, Z K He, et al. (2013). “A compensation method to improve the performance of IPI-based entity recognition system in body sensor networks”. In: *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 1250–1253 (cit. on pp. 18, 31).

Bao, S D, C C Y Poon, et al. (2008). “Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network”. In: *IEEE Transactions on Information Technology in Biomedicine* 12.6, pp. 772–779 (cit. on pp. 31, 79, 112).

Barra, Silvio et al. (2015). “Ubiquitous iris recognition by means of mobile devices”. In: *Pattern Recognition Letters* 57, pp. 66–73 (cit. on p. 31).

Barrett, Paul (1986). “Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor”. In: *Conference on the Theory and Application of Cryptographic Techniques*. Springer, pp. 311–323 (cit. on p. 11).

Basaraba, Sharon (2019). *5 Ways Our Voices Change as We Age*. URL: https://www.verywellhealth.com/ways-voices-change-as-we-age-2223342 (cit. on p. 90).

Bichell, Rae E. (2015). *A Tiny Pill Monitors Vital Signs From Deep Inside The Body*. URL: https://www.npr.org/sections/health-shots/2015/11/18/455953304/a-tiny-pill-monitors-vital-signs-from-deep-inside-the-body?t=1563279721897.

Bienkowski, Tom (2018). *GDPR is Explicit About Protecting Availability*. URL: https://www.netscout.com/blog/gdpr-availability-protection (cit. on p. 18).

Bigy, A. et al. (2015). “Recognition of Postures and Freezing of Gait in Parkinson Disease Patients Using Microsoft Kinect Sensor”. In: *7th Annual International IEEE EMBS Conference on Neural Engineering*, pp. 731–734 (cit. on p. 47).

Bilgin, S and A C Gzeler (2015). “Naive Bayes classification of neurodegenerative diseases by using discrete wavelet transform”. In: *Biomedical Engineering Meeting (BIYOMUT), 2015 19th National*, pp. 1–4 (cit. on pp. 54, 56).

Blaze, Matt, Gerrit Bleumer, and Martin Strauss (1998). “Divertible protocols and atomic proxy cryptography”. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, pp. 127–144 (cit. on p. 22).

Bohan, Zeng et al. (2013). “Encryption node design in Internet of Things based on fingerprint features and cc2530”. In: *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*. IEEE, pp. 1454–1457 (cit. on p. 26).

Bommagani, Aruna Sri, Matthew C Valenti, and Arun Ross (2014). “A framework for secure cloud-empowered mobile biometrics”. In: *Military Communications Conference (MILCOM)*. IEEE, pp. 255–261 (cit. on p. 30).

Bonnet, V et al. (Apr. 2015). “Towards an affordable mobile analysis platform for pathological walking assessment”. In: *Robotics and Autonomous Systems* 66, pp. 116–128 (cit. on p. 47).

Borgen, Halvor, Patrick Bours, and Stephen D Wolthusen (2008). “Visible-spectrum biometric retina recognition”. In: *Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP’08 International Conference on*. IEEE, pp. 1056–1062 (cit. on p. 31).

Boukerche, A and Yonglin Ren (2009). “A secure mobile healthcare system using trust-based multicast scheme”. In: *IEEE Journal on Selected Areas in Communications* 27.4, pp. 387–399 (cit. on p. 23).

Boutaayamou, M et al. (2015). “Segmentation of gait cycles using foot-mounted 3D accelerometers”. In: *3D Imaging (IC3D), 2015 International Conference on*, pp. 1–7 (cit. on p. 49).

Bromwich, Matthew and Rebecca Bromwich (2016). “Privacy risks when using mobile devices in health care”. In: *CMAJ: Canadian Medical Association Journal* 188.12, p. 855 (cit. on p. 20).

Brooks, Steve (2019). *Can you trust Healthcare organisations with your digital wellbeing?* URL: https://www.enterprisetimes.co.uk/2019/06/27/can-you-trust-healthcare-organisations-with-your-digital-wellbeing/ (cit. on p. 12).

Brown, Robert G. (2004). *Dieharder: A Random Number Test Suite*. URL: https://webhome.phy.duke.edu/~rgb/General/dieharder.php (cit. on pp. 134, 149, 150, 152).

Bucci, M et al. (Apr. 2003). “A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC”. In: *IEEE Transactions on Computers* 52.4, pp. 403–409 (cit. on p. 141).

Buchmann, Johannes, Erik Dahmen, and Michael Szydlo (2009). “Hash-based Digital Signature Schemes”. In: *Post-Quantum Cryptography*. Ed. by Daniel J Bernstein, Johannes Buchmann, and Erik Dahmen. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 35–93 (cit. on p. 141).

Cai, H et al. (June 2017). “Deploying Data-Driven Security Solutions on Resource-Constrained Wearable IoT Systems”. In: *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 199–204 (cit. on p. 141).

Califano, Jessica (2018). *How to Approach OTA Updates for IoT*. URL: https://dzone.com/articles/how-to-approach-ota-updates-for-iot (cit. on p. 20).

Camara, Carmen, Pedro Peris-Lopez, and Juan E Tapiador (2015). “Security and privacy issues in implantable medical devices: A comprehensive survey”. In: *Journal of biomedical informatics* 55, pp. 272–289.

Campisi, Patrizio (2013). “Security and Privacy in Biometrics: Towards a Holistic Approach”. In: *Security and Privacy in Biometrics*. Springer. Chap. 1, pp. 1–23 (cit. on p. 78).

Campisi, P et al. (Nov. 2011). “Brain waves based user recognition using the eyes closed resting conditions protocol”. In: *2011 IEEE International Workshop on Information Forensics and Security*, pp. 1–6 (cit. on p. 60).

Cancela, Jorge, Maria T. Arredondo, and Olivia Hurtado (2014). “Proposal of a Kinect(TM)-based system for gait assessment and rehabilitation in Parkinsons disease”. In: *International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 4519–4522 (cit. on p. 47).

Cassiolato, Cesar (2011). *How shielding can help minimize noises*. URL: http://www.smar.com/en/technical-article/how-shielding-can-help-minimize-noises (cit. on p. 40).

Cecotti, H and A Graser (Mar. 2011). “Convolutional Neural Networks for P300 Detection with Application to Brain-Computer Interfaces”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 33.3, pp. 433–445 (cit. on p. 61).

Cerny, M, N Noury, and L Deplorte (2015). “Validation of Inverted Pendulum model for gait length calculation”. In: *Applied Machine Intelligence and Informatics (SAMI), 2015 IEEE 13th International Symposium on*, pp. 129–132 (cit. on p. 52).

Chakrabarti, Dibyendu, Subhamoy Maitra, and Bimal Roy (2006). “A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design”. In: *International Journal of Information Security* 5.2, pp. 105–114 (cit. on p. 23).

Chakravorty, Rajiv (2006). “A programmable service architecture for mobile medical care”. In: *Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on*. IEEE, 5–pp (cit. on p. 14).

Chan, A D C et al. (2008). “Wavelet Distance Measure for Person Identification Using Electrocardiograms”. In: *IEEE Transactions on Instrumentation and Measurement* 57.2, pp. 248–253 (cit. on p. 112).

Charthad, J et al. (2015). “A mm-Sized Implantable Medical Device (IMD) With Ultrasonic Power Transfer and a Hybrid Bi-Directional Data Link”. In: *IEEE Journal of Solid-State Circuits* 50.8, pp. 1741–1753 (cit. on pp. 39, 40).

Chauhan, Sucheta and Lovekesh Vig (2015). “Anomaly detection in ECG time signals via deep long short-term memory networks”. In: *Data Science and Advanced Analytics (DSAA), 2015. 36678 2015. IEEE International Conference on*. IEEE, pp. 1–7 (cit. on p. 58).

Chen, Hongyang, Pei Huang, et al. (2008). “Novel centroid localization algorithm for three dimensional wireless sensor networks”. In: *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM’08. 4th International Conference on*. IEEE, pp. 1–4 (cit. on p. 19).

Chen, Shanshan, Christopher L Cunningham, et al. (2011). “Enabling Longitudinal Assessment of Ankle-foot Orthosis Efficacy for Children with Cerebral Palsy”. In: *Proceedings of the 2Nd Conference on Wireless Health*. WH ’11. New York, NY, USA: ACM, pp. 1–10 (cit. on p. 46).

Chen, Shanshan, John Lach, et al. (2016). “Towards Pervasive Gait Analysis for Medicine with Wearable Sensors: A Systematic Review for Clinicians and Medical Researchers”. In: *IEEE Journal of Biomedical and Health Informatics* 14.8, pp. 1–1 (cit. on pp. 45, 46).

Chereshnev, Roman and Attila Kertesz-Farkas (2017). “HuGaDB: Human Gait Database for Activity Recognition from Wearable Inertial Sensor Networks”. In: *The 6th International Conference on Analysis of Images, Social networks and Texts* (cit. on p. 106).

Chizari, Hassan and Emil C Lupu (2019). “Extracting Randomness From The Trend of IPI for Cryptographic Operators in Implantable Medical Devices”. In: *IEEE Transactions on Dependable and Secure Computing* (cit. on p. 31).

Choudhury, Amlan Jyoti et al. (2011). “A strong user authentication framework for cloud computing”. In: *2011 IEEE Asia-Pacific Services Computing Conference*. IEEE, pp. 110–115 (cit. on p. 26).

Clark, Ross A et al. (Feb. 2015). “Instrumenting gait assessment using the Kinect in people living with stroke: reliability and association with balance tests”. In: *Journal of NeuroEngineering and Rehabilitation* 12, p. 15 (cit. on p. 47).

Cola, G et al. (2015). “An unsupervised approach for gait-based authentication”. In: *International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 1–6 (cit. on p. 79).

Cole, P. Alexander, M. Carlton, and Quoc-Dien Trinh (2017). *We must improve the security of networked medical devices*. URL: https://www.statnews.com/2017/11/02/medical-devices-security-hospitals/ (cit. on p. 25).

Cornelius, Cory T and David F Kotz (2012). “Recognizing whether sensors are on the same body”. In: *Pervasive and Mobile Computing* 8.6, pp. 822–836 (cit. on p. 112).

Crilly, Patrick and Vallipuram Muthukkumarasamy (2010). “Using smart phones and body sensors to deliver pervasive mobile personal healthcare”. In: *2010 Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*. IEEE, pp. 291–296 (cit. on p. 20).

Cristiano (2011). *RaBiGeTe Random Bit Generators Tester*. URL: http://cristianopi.altervista%5C%5C.org/RaBiGeTe/ (cit. on p. 150).

Cunha, Joao Paulo Silva et al. (2016). “A novel portable, low-cost kinect-based system for motion analysis in neurological diseases”. In: *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 2339–2342 (cit. on p. 47).

Dantcheva, Antitza et al. (Jan. 2011). “Bag of soft biometrics for person identification”. In: *Multimedia Tools and Applications* 51.2, pp. 739–777 (cit. on p. 90).

Das, D (2015). “Human gait classification using combined HMM &amp; SVM hybrid classifier”. In: *Electronic Design, Computer Networks & Automated Verification (EDCAV), 2015 International Conference on*, pp. 169–174 (cit. on pp. 54, 56).

Davis, Jessica (2018). *User Authentication Most Common Cyber Risk for Hospitals, Health Systems*. URL: https://healthitsecurity.com/news/user-authentication-most-common-cyber-risk-for-hospitals-health-systems (cit. on p. 21).

— (2019). *IoT Devices, Ultrasound Machines Pose Risk to Health IT Network*. URL: https://healthitsecurity.com/news/iot-devices-cloud-mobile-are-weakest-links-in-health-it-network (cit. on p. 11).

Derawi, M O et al. (2010). “Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition”. In: *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 306–311 (cit. on p. 111).

Derbel, Ahmed et al. (2014). “Interest lower body point’s detection for markerless gait analysis”. In: *2014 4th International Conference on Image Processing Theory, Tools and Applications (IPTA)*, pp. 1–6 (cit. on p. 46).

Derlatka, M and M Bogdan (2015). “Ensemble kNN classifiers for human gait recognition based on ground reaction forces”. In: *2015 8th International Conference on Human System Interaction (HSI)*, pp. 88–93 (cit. on pp. 53, 56).

Dfranke (2009). *How I Hacked Hacker News (with arc security advisory)*. URL: https://news.ycombinator.com/item?id=639976 (cit. on p. 141).

Dharavath, K, F A Talukdar, and R H Laskar (2013). “Study on biometric authentication systems, challenges and future trends: A review”. In: *2013 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1–7 (cit. on pp. 27, 28).

DHS (2014). *National Cybersecurity and Communications Integration Center: DDoS Quick Guide*. URL: https://www.us-cert.gov/sites/default/files/publications/DDoS%5C%20Quick%5C%20Guide.pdf (cit. on p. 23).

Di Vimercati, Sabrina De Capitani et al. (2007). “Over-encryption: management of access control evolution on outsourced data”. In: *Proceedings of the 33rd international conference on Very large data bases*. VLDB endowment, pp. 123–134 (cit. on p. 22).

Dinca, L M and G Hancke (June 2017). “Behavioural sensor data as randomness source for IoT devices”. In: *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, pp. 2038–2043 (cit. on pp. 142, 147, 154).

Dolatabadi, E, B Taati, and A Mihailidis (2016). “Automated classification of pathological gait after stroke using ubiquitous sensing technology”. In: *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 6150–6153 (cit. on pp. 53, 56).

Dolmatov, Vasyl (2019). *Cyberattacks are putting lives at risk*. URL: https://www.openaccessgovernment.org/cyberattacks-are-putting/62469/ (cit. on p. 11).

Doukas, C et al. (2012). “Enabling data protection through PKI encryption in IoT m-Health devices”. In: *2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE)*, pp. 25–29 (cit. on p. 35).

Du, Wenliang et al. (2005). “A pairwise key predistribution scheme for wireless sensor networks”. In: *ACM Transactions on Information and System Security (TISSEC)* 8.2, pp. 228–258 (cit. on p. 23).

Eidinger, E., R. Enbar, and T. Hassner (Dec. 2014). “Age and Gender Estimation of Unfiltered Faces”. In: *IEEE Transactions on Information Forensics and Security* 9.12, pp. 2170–2179 (cit. on p. 90).

Ellouze, Nourhene, Mohamed Allouche, Habib Ben Ahmed, et al. (2014). “Security of implantable medical devices: limits, requirements, and proposals”. In: *Security and Communication Networks* 7.12, pp. 2475–2491 (cit. on p. 38).

Ellouze, Nourhene, Mohamed Allouche, Habib Ben Ahmed, et al. (2013). “Securing implantable cardiac medical devices: Use of radio frequency energy harvesting”. In: *Proceedings of the 3rd international workshop on Trustworthy embedded devices*. ACM, pp. 35–42 (cit. on p. 40).

Encyclopedia (2017). *Hamming distance*. URL: http://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/hamming-distance (cit. on p. 131).

Esser, Patrick et al. (2011). “Assessment of spatio-temporal gait parameters using inertial measurement units in neurological populations”. In: *Gait & Posture* 34.4, pp. 558–560 (cit. on p. 52).

Evans, Jae A (1999). *Electronic medical records system*. US Patent 5,924,074 (cit. on p. 11).

Faulds, Henry (1880). “On the skin-furrows of the hand”. In: *Nature* 22.574, p. 605 (cit. on p. 30).

Fazzini, Kate (2019). *Here's how criminals use stolen passport information*. URL: https://uk.finance.yahoo.com/news/apos-criminals-stolen-passport-information-195422565.html (cit. on p. 12).

Francillon, Aurelien and Claude Castelluccia (2007). "TinyRNG: A cryptographic random number generator for wireless sensors network nodes". In: *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops, 2007. WiOpt 2007. 5th International Symposium on*. IEEE, pp. 1–7 (cit. on p. 37).

Fraschini, M et al. (2015). "An EEG-Based Biometric System Using Eigenvector Centrality in Resting State Brain Networks". In: *IEEE Signal Processing Letters* 22.6, pp. 666–670 (cit. on pp. 58, 75).

Fukushima, Akio et al. (2014). "Spin dice: A scalable truly random number generator based on spintronics". In: *Applied Physics Express* 7.8, p. 83001 (cit. on p. 36).

Gabriel, Christian et al. (2010). "A generator for unique quantum random numbers based on vacuum states". In: *Nature Photonics* 4.10, p. 711 (cit. on p. 36).

Gafurov, Davrondzhon, Kirsi Helkala, and Torkjel Sondrol (2006). "Biometric Gait Authentication Using Accelerometer Sensor." In: *JCP* 1.7, pp. 51–59 (cit. on p. 32).

Gafurov, Davrondzhon, Einar Snekkenes, and Patrick Bours (2007). "Spoof Attacks on Gait Authentication System". In: *IEEE Transactions on Information Forensics and Security* 2.3, pp. 491–502 (cit. on p. 136).

Gaglio, Vincenzo et al. (2010). "A TRNG exploiting multi-source physical data". In: *Proceedings of the 6th ACM workshop on QoS and security for wireless and mobile networks*. ACM, pp. 82–89 (cit. on p. 37).

Garcia-Baleon, H A, V Alarcon-Aquino, and O Starostenko (2009). "A wavelet-based 128-bit key generator using electrocardiogram signals". In: *IEEE International Midwest Symposium on Circuits and Systems*, pp. 644–647 (cit. on p. 79).

Garun, Natt (2017). *Yahoo says all 3 billion user accounts were impacted by 2013 security breach*. URL: https://www.theverge.com/2017/10/3/16414306/yahoo-security-data-breach-3-billion-verizon (cit. on p. 11).

Geerse, Daphne J, Bert H Coolen, and Melvyn Roerdink (Oct. 2015). “Kinematic Validation of a Multi-Kinect v2 Instrumented 10-Meter Walkway for Quantitative Gait Assessments”. In: *PLoS ONE* 10.10. Ed. by Alfonso Fasano (cit. on p. 47).

Geman, O (2013). “Nonlinear dynamics, artificial neural networks and neuro-fuzzy classifier for automatic assessing of tremor severity”. In: *E-Health and Bioengineering Conference (EHB), 2013*, pp. 1–4 (cit. on pp. 54, 56).

Gholami, Farnood et al. (2016). “A Microsoft Kinect-Based Point-of-Care Gait Assessment Framework for Multiple Sclerosis Patients”. In: *IEEE Journal of Biomedical and Health Informatics*, pp. 2168–2194 (cit. on p. 47).

Goldberg, Ian and David Wagner (1996). “Randomness and the Netscape browser”. In: *Dr Dobb’s Journal-Software Tools for the Professional Programmer* 21.1, pp. 66–71 (cit. on p. 36).

Goldberger, A. et al. (2000). “PhysioBank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals”. In: *Circulation* 101.23, e215–e220 (cit. on p. 67).

Goldreich, Oded (2007). *Foundations of Cryptography Volume I Basic Tools*. Cambridge University Press, pp. 101–103 (cit. on p. 141).

Goldwasser, Shafi, Yael Tauman Kalai, and Guy N Rothblum (2008). “One-Time Programs”. In: *Proceedings of the 28th Annual Conference on Cryptology: Advances in Cryptology*. CRYPTO 2008. Berlin, Heidelberg: Springer-Verlag, pp. 39–56. URL: http://dx.doi.org/10.1007/978-3-540-85174-5_3 (cit. on p. 20).

Gollakota, Shyamnath et al. (2011). “They can hear your heartbeats: non-invasive security for implantable medical devices”. In: *ACM SIGCOMM Computer Communication Review*. Vol. 41. ACM, pp. 2–13. ISBN: 1450307973 (cit. on p. 38).

Gong, Zhenqiang et al. (2017). “PIANO: Proximity-based User Authentication on Voice-Powered Internet-of-Things Devices”. In: *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, pp. 2212–2219 (cit. on p. 32).

Goode, Alan (2018). *Biometric Identification or Biometric Authentication?* URL: https://www.veridiumid.com/blog/biometric-identification-and-biometric-authentication/ (cit. on p. 26).

Gope, Prosanta and Tzonelih Hwang (2016). “BSN-Care: A secure IoT-based modern healthcare system using body sensor network”. In: *IEEE Sensors Journal* 16.5, pp. 1368–1376 (cit. on p. 14).

Goyal, Vipul et al. (2006). “Attribute-based encryption for fine-grained access control of encrypted data”. In: *Proceedings of the 13th ACM conference on Computer and communications security*. Acm, pp. 89–98 (cit. on p. 22).

Graham, John (2013). *Why secure systems require random numbers*. URL: https://blog.cloudflare.com/why-randomness-matters/ (cit. on p. 140).

Graves, Alex, Abdel-rahman Mohamed, and Geoffrey Hinton (2013). “Speech recognition with deep recurrent neural networks”. In: *2013 IEEE international conference on acoustics, speech and signal processing*. IEEE, pp. 6645–6649 (cit. on p. 58).

Gravina, Raffaele et al. (2010). “Enabling multiple BSN applications using the SPINE framework”. In: *2010 International Conference on Body Sensor Networks*. IEEE, pp. 228–233 (cit. on p. 16).

Greenwood, Robert E (1955). “Coupon collector’s test for random digits”. In: *Mathematical Tables and Other Aids to Computation*, pp. 1–5 (cit. on p. 150).

Guennouni, Souhail, Anass Mansouri, and Ali Ahaitouf (2019). *Biometric Systems and Their Applications*. URL: https://www.intechopen.com/online-first/biometric-systems-and-their-applications (cit. on p. 27).

Gui, Q et al. (Dec. 2015). “Multichannel EEG-based biometric using improved RBF neural networks”. In: *2015 IEEE Signal Processing in Medicine and Biology Symposium (SPMB)*, pp. 1–6 (cit. on pp. 34, 58).

Gulen, Utku, Abdelrahman Alkhodary, and Selcuk Baktir (2019). “Implementing RSA for Wireless Sensor Nodes”. In: *Sensors* 19.13, p. 2864 (cit. on p. 23).

Guo, Z et al. (2016). “Hardware security meets biometrics for the age of IoT”. In: *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1318–1321 (cit. on p. 78).

Gupta, A et al. (2015). “Hybrid method for Gait recognition using SVM and Baysian Network”. In: *2015 IEEE 8th International Workshop on Computational Intelligence and Applications (IWCIA)*, pp. 89–94 (cit. on pp. 54, 56).

Hadid, Abdenour et al. (2012). “Can gait biometrics be Spoofed?” In: *2012 21st International Conference on Pattern Recognition (ICPR)* (cit. on p. 136).

Halperin, Daniel et al. (2008). “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses”. In: *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. IEEE, pp. 129–142 (cit. on p. 40).

Hamza, Taieb et al. (2016). “A survey on intelligent MAC layer jamming attacks and countermeasures in WSNs”. In: *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. IEEE, pp. 1–5 (cit. on p. 24).

Han, Chin-Chuan et al. (2003). “Personal authentication using palm-print features”. In: *Pattern recognition* 36.2, pp. 371–381 (cit. on pp. 29, 33).

He, Debiao and Sherali Zeadally (2015). “An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography”. In: *IEEE internet of things journal* 2.1, pp. 72–83 (cit. on p. 26).

Hediyeh, Houman, Tarek Sayed, and Mohamed H. Zaki (2013). “Use of Spatiotemporal Parameters of Gait for Automated Classification of Pedestrian Gender and Age”. In: *Transportation Research Record* 2393.1, pp. 31–40 (cit. on p. 90).

Hei, Xiali et al. (2010). “Defending resource depletion attacks on implantable medical devices”. In: *Global telecommunications conference (GLOBECOM 2010), 2010 IEEE*. IEEE, pp. 1–5 (cit. on p. 41).

Hennebert, Christine, Hicham Hossayni, and Cedric Lauradoux (2013). “Entropy Harvesting from Physical Sensors”. In: *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*. New York, NY, USA: ACM, pp. 149–154 (cit. on pp. 142, 154).

Hinkle, D. E., W. Wiersma, and S. G. Jurs (2002). *Applied Statistics for the Behavioral Sciences*. 5th ed. Houghton Mifflin (cit. on p. 126).

Hoang, Thang and Deokjai Choi (May 2014). “Secure and Privacy Enhanced Gait Authentication on Smart Phone”. In: *The Scientific World Journal* (cit. on pp. 80, 87).

Hoang, Thang, Deokjai Choi, and Thuc Nguyen (2015). “Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme”. In: *International Journal of Information Security* 14.6, pp. 549–560 (cit. on pp. 32, 112, 113, 122).

Hoffman, Chris (2019). *How Computers Generate Random Numbers*. URL: https://www.howtogeek.com/183051/htg-explains-how-computers-generate-random-numbers/ (cit. on p. 35).

Hoffman, Ted L (2003). *Over-the-air programming of wireless terminal features*. US Patent 6,622,017 (cit. on p. 20).

Hong, S L and C Liu (2015). "Sensor-Based Random Number Generator Seeding". In: *IEEE Access* 3, pp. 562–568 (cit. on pp. 142, 155).

HSBC (2017). *HSBC Voice ID making telephone banking safer than ever*. URL: https://www.hsbc.co.uk/1/2/voice-id (cit. on p. 32).

Hsu, Yu-Liang et al. (2014). "Gait and balance analysis for patients with Alzheimer's disease using an inertial-sensor-based wearable instrument". In: vol. 18. 6. IEEE, pp. 1822–1830 (cit. on p. 46).

Hu, Jwu-Sheng, Kuan-Chun Sun, and Chi-Yuan Cheng (2013). "A kinematic human-walking model for the normal-gait-speed estimation using tri-axial acceleration signals at waist location". In: vol. 60. 8. IEEE, pp. 2271–2279 (cit. on pp. 48, 52).

Hu, Pengfei, Huansheng Ning, et al. (2017). "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things". In: *IEEE Internet of Things Journal* 4.5, pp. 1143–1155 (cit. on p. 30).

Hu, X and G S Soh (2014). "A study on estimation of planar gait kinematics using minimal inertial measurement units and inverse kinematics". In: *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 6911–6914 (cit. on p. 103).

Huang, Haiping, Linkang Hu, et al. (2019). "An EEG-Based Identity Authentication System with Audiovisual Paradigm in IoT". In: *Sensors* 19.7, p. 1664 (cit. on p. 26).

Huang, Haojun, Jianguo Zhou, et al. (2016). "Wearable indoor localisation approach in Internet of Things". In: *IET Networks* 5.5, pp. 122–126 (cit. on p. 17).

Hutchinson, Bill (2018). *87 million Facebook users to find out if their personal data was breached*. URL: https://abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187 (cit. on p. 11).

Hwang, Tong-Hun et al. (2016). “Real-time gait event detection using a single head-worn inertial measurement unit”. In: *2016 IEEE 6th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, pp. 28–32 (cit. on p. 46).

ICO (2019). *Health and social care*. URL: https://ico.org.uk/for-organisations/in-your-sector/health/ (cit. on p. 12).

IEEE (2012). “IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks”. In: *IEEE Std 802.15.6-2012*, pp. 1–271 (cit. on p. 111).

Isenor, DK and Safwat G Zaky (1986). “Fingerprint identification using graph matching”. In: *Pattern Recognition* 19.2, pp. 113–122 (cit. on p. 57).

Ismail, Nick (2018). *The financial impact of data breaches is just the beginning*. URL: https://www.information-age.com/data-breaches-financial-impact-123470254/ (cit. on p. 17).

Jain, Ankita and Vivek Kanhangad (2018). “Gender classification in smartphones using gait information”. In: *Expert Systems with Applications* 93, pp. 257–266 (cit. on p. 91).

Jarchi, Delaram, Benny Lo, Edmund Ieong, et al. (2014). “Validation of the e-AR sensor for gait event detection using the parotec foot insole with application to post-operative recovery monitoring”. In: *International Conference on Wearable and Implantable Body Sensor Networks*, pp. 127–131 (cit. on p. 81).

Jarchi, Delaram, Benny Lo, Charence Wong, et al. (2016). “Gait Analysis from a Single Ear-Worn Sensor: Reliability and Clinical Evaluation for Orthopaedic Patients”. In: *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 24.8, pp. 882–892 (cit. on p. 48).

Jarchi, Delaram, Charence Wong, et al. (2014). “Gait parameter estimation from a miniaturized ear-worn sensor using singular spectrum analysis and longest common subsequence”. In: *IEEE Transactions on Biomedical Engineering* 61.4, pp. 1261–1273 (cit. on p. 48).

Jayarathne, Isuru, Michael Cohen, and Senaka Amarakeerthi (2017). “Survey of EEG-based biometric authentication”. In: *2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST)*. IEEE, pp. 324–329 (cit. on p. 32).

Jennewein, Thomas et al. (2000). “A fast and compact quantum random number generator”. In: *Review of Scientific Instruments* 71.4, pp. 1675–1680 (cit. on p. 36).

Jonsson, Fredrik and Martin Tornkvist (2017). *RSA authentication in Internet of Things : Technical limitations and industry expectations* (cit. on p. 11).

Jonsson, J. and B. Kaliski (2003). *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*. URL: https://tools.ietf.org/html/rfc3447 (cit. on p. 23).

Juels, A and M Wattenberg (1999). "A fuzzy commitment scheme". In: *ACM Conference on Computer and Communications Security*, pp. 28–36 (cit. on pp. 87, 122).

Jun, Benjamin and Paul Kocher (1999). "The Intel random number generator". In: *Cryptography Research Inc. white paper* (cit. on pp. 36, 37).

Kantoch, Eliasz (2013). "Technical verification of integrating wearable sensors into bsn-based telemedical monitoring system". In: *2013 12th International Conference on Machine Learning and Applications*. Vol. 2. IEEE, pp. 432–435 (cit. on p. 12).

Kaplan, Dan (2011). *Black Hat: Insulin pumps can be hacked*. URL: https://www.scmagazine.com/black-hat-insulin-pumps-can-be-hacked/article/559187/ (cit. on p. 25).

Kargar, B. Amir H et al. (2014). "Automatic measurement of physical mobility in Get-Up-and-Go Test using Kinect sensor". In: *International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 3492–3495 (cit. on p. 47).

Karimian, N et al. (2017). "Highly Reliable Key Generation From Electrocardiogram (ECG)". In: *IEEE Transactions on Biomedical Engineering* 64.6, pp. 1400–1411 (cit. on p. 31).

Karpathy, Andrej et al. (2014). "Large-scale video classification with convolutional neural networks". In: *Proceedings of the IEEE conference on Computer Vision and Pattern Recognition*, pp. 1725–1732 (cit. on p. 58).

Kastaniotis, Dimitris et al. (2014). *Using kinect for assesing the state of Multiple Sclerosis patients* (cit. on p. 47).

Katsigiannis, S and N Ramzan (2018). "DREAMER: A Database for Emotion Recognition Through EEG and ECG Signals From Wireless Low-cost Off-the-Shelf Devices". In: *IEEE Journal of Biomedical and Health Informatics* 22.1, pp. 98–107 (cit. on p. 61).

Kephart, J O and D M Chess (2003). "The vision of autonomic computing". In: *Computer* 36.1, pp. 41–50 (cit. on p. 19).

Kerimbaev, Bolot (2016). *Big Nerd Ranch: Neural Networks in iOS 10 and macOS*. URL: http://www.bignerdranch.com/blog/neural-networks-in-ios-10-and-macos/ (cit. on p. 113).

Khandelwal, Siddhartha and Nicholas Wickstrom (Jan. 2017). “Evaluation of the performance of accelero-meter-based gait event detection algorithms in different real-world scenarios using the MAREA gait database”. In: *Gait and Posture* 51, pp. 84–90 (cit. on p. 106).

Khillar, Sagar (2018). *Difference Between FFT and DFT*. URL: http://www.differencebetween.net/technology/difference-between-fft-and-dft/ (cit. on p. 53).

Khitrov, Mikhail (2013). “Talking passwords: voice biometrics for data access and security”. In: *Biometric Technology Today* 2013.2, pp. 9–11 (cit. on pp. 32, 111).

Khoo, Benjamin (2011). “RFID as an Enabler of the Internet of Things: Issues of Security and Privacy”. In: *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, pp. 709–712 (cit. on p. 26).

Kilinc, Handan and Serge Vaudenay (2017). “Contactless access control based on distance bounding”. In: *International Conference on Information Security*. Springer, pp. 195–213 (cit. on p. 38).

Kim, Byungjo, Jiung Yu, and Hyogon Kim (2012). “In-vivo NFC: Remote monitoring of implanted medical devices with improved privacy”. In: *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*. ACM, pp. 327–328 (cit. on p. 40).

King, Rachel Christina et al. (2010). “Elderly risk assessment of falls with BSN”. In: *2010 International Conference on Body Sensor Networks, BSN 2010*, pp. 30–35 (cit. on p. 48).

Kingma, Diederik P. and Jimmy Ba (2015). “Adam: A Method for Stochastic Optimization”. In: *arXiv:1412.6980v9* (cit. on p. 68).

— (2014). “Adam: A method for stochastic optimization”. In: *arXiv preprint arXiv:1412.6980* (cit. on p. 95).

Kirk, Matthew (2015). *Thoughtful Machine Learning: A Test-Driven Approach*. 2nd. Sebastopol: O’Reilly Media. ISBN: 978-1-449-37406-8 (cit. on p. 52).

Kirtley, Christopher (2006). *Clinical gait analysis: theory and practice*. Elsevier Health Sciences (cit. on p. 44).

Kloeffler, Dan and Alexis Shaw (2013). *Dick Cheney Feared Assassination Via Medical Device Hacking: 'I Was Aware of the Danger'*. URL: https://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434 (cit. on p. 141).

Klonoff, David C (2015). "Cybersecurity for connected diabetes devices". In: *Journal of diabetes science and technology* 9.5, pp. 1143–1147 (cit. on p. 25).

Knight, Mark (2012). *Data Encryption: Random or pseudorandom?* URL: https://www.ncipher.com/blog/data-encryption-random-or-pseudorandom (cit. on p. 35).

Kogetsu, Atsushi, Soichi Ogishima, and Kazuto Kato (2018). "Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy, and Trustworthiness". In: *Frontiers in genetics* 9 (cit. on p. 21).

Kose, A, A Cereatti, and U D Croce (2011). "Estimation of traversed distance in level walking using a single inertial measurement unit attached to the waist". In: *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 1125–1128 (cit. on p. 48).

Kose, A, A Cereatti, Luca Laudani, et al. (2011). "Estimation of stride length in walking using a single inertial measurement unit attached to the waist". In: *Gait & Posture* 33, pp. 49–50 (cit. on p. 48).

Kose, Alper, Andrea Cereatti, and Ugo Della Croce (Feb. 2012). "Bilateral step length estimation using a single inertial measurement unit attached to the pelvis". In: *Journal of NeuroEngineering and Rehabilitation* 9, p. 9 (cit. on p. 48).

Koutsonikolas, Dimitrios, Saumitra M Das, and Y Charlie Hu (2007). "Path planning of mobile landmarks for localization in wireless sensor networks". In: *Computer Communications* 30.13, pp. 2577–2592 (cit. on p. 19).

Kravitz, David W (1993). *Digital signature algorithm*. US Patent 5,231,668 (cit. on p. 11).

Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E Hinton (2012). "Imagenet classification with deep convolutional neural networks". In: *Advances in neural information processing systems*, pp. 1097–1105 (cit. on p. 58).

Kumar, Ajay and Arun Passi (2010). "Comparison and combination of iris matchers for reliable personal authentication". In: *Pattern recognition* 43.3, pp. 1016–1026 (cit. on p. 31).

Kumar, Gulshan et al. (2014). "Understanding denial of service (DoS) attacks using OSI reference model". In: *International Journal of Education and Science Research* 1.5 (cit. on p. 23).

Kumar, Pardeep and Hoon-Jae Lee (2012). “Security issues in healthcare applications using wireless medical sensor networks: A survey”. In: *sensors* 12.1, pp. 55–91 (cit. on p. 23).

Kumar, Pardeep, Young-Dong Lee, and H Lee (Aug. 2010). “Secure health monitoring using medical wireless sensor networks”. In: *The 6th International Conference on Networked Computing and Advanced Information Management*, pp. 491–494 (cit. on p. 141).

Kumar, Ramesh and Rajeswari Mukesh (2013). “State Of The Art: Security In Wireless Body Area Networks”. In: *International Journal of Computer Science & Engineering Technology (IJCSET)* 4.5, pp. 622–630 (cit. on p. 22).

Kune, Denis Foo et al. (2013). “Ghost talk: Mitigating EMI signal injection attacks against analog sensors”. In: *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, pp. 145–159 (cit. on p. 40).

Kuryloski, Philip et al. (2009). “DexterNet: An open platform for heterogeneous body sensor networks and its applications”. In: *2009 Sixth International Workshop on Wearable and Implantable Body Sensor Networks*. IEEE, pp. 92–97 (cit. on p. 16).

Kusakunniran, Worapan (2016). “Extracting Gait Figures in a Video Based on Markerless Motion”. In: *Proceedings - 2015 IEEE International Conference on Knowledge and Systems Engineering, KSE 2015*, pp. 306–309 (cit. on p. 46).

Lamkin, Paul (2016). *Wearable Tech Market To Be Worth $34 Billion By 2020*. URL: https://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#16a010bd3cb5 (cit. on p. 141).

Lazzi, Gianluca (2005). “Thermal effects of bioimplants”. In: *IEEE Engineering in Medicine and Biology Magazine* 24.5, pp. 75–81.

Lee, Hsin-Fu, Lung-Sheng Wu, et al. (2016). “Dialysis patients with implanted drug-eluting stents have lower major cardiac events and mortality than those with implanted bare-metal stents: a Taiwanese Nationwide Cohort Study”. In: *PloS one* 11.1.

Lee, Phillip, Andrew Clark, et al. (2013). “A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems”. In: *CoRR* abs/1312.1. URL: http://arxiv.org/abs/1312.1397 (cit. on p. 25).

Li, Dan and Yu Hen Hu (2003). “Energy-based collaborative source localization using acoustic microsensor array”. In: *EURASIP Journal on Advances in Signal Processing* 2003.4, p. 985029 (cit. on p. 19).

Li, G, T Liu, et al. (2014). “Wearable gait analysis system for ambulatory measurement of kinematics and kinetics”. In: *IEEE SENSORS*, pp. 1316–1319 (cit. on p. 103).

Li, Ling, Louis Atallah, et al. (2014). “Feature extraction from ear-worn sensor data for gait analysis”. In: *2014 IEEE-EMBS International Conference on Biomedical and Health Informatics, BHI 2014*, pp. 560–563 (cit. on p. 48).

Li, Q, M Young, et al. (2009). “Walking speed and slope estimation using shank-mounted inertial measurement units”. In: *2009 IEEE International Conference on Rehabilitation Robotics*, pp. 839–844 (cit. on p. 49).

Li, X., S. J. Maybank, et al. (Mar. 2008). “Gait Components and Their Application to Gender Recognition”. In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 38.2, pp. 145–155 (cit. on p. 90).

Li, Yantao, Xin Qi, et al. (2011). “Energy modeling and optimization through joint packet size analysis of BSN and WiFi networks”. In: *30th IEEE International Performance Computing and Communications Conference*. IEEE, pp. 1–8 (cit. on p. 12).

Liang, Xuedong and Ilangko Balasingham (2007). “Performance analysis of the IEEE 802.15. 4 based ECG monitoring network”. In: *Proceedings of the 7th IASTED international conferences on wireless and optical communications*, pp. 99–104 (cit. on p. 16).

Lin, Chin-Teng et al. (2005). “Estimating Driving Performance Based on EEG Spectrum Analysis”. In: *EURASIP Journal on Advances in Signal Processing* 2005.19, pp. 3165–3174 (cit. on p. 75).

Liu, Guobin (2012). “Jamming attacks and countermeasures in wireless area networks”. In: (cit. on p. 23).

Liu, Kezhong, Shu Wang, et al. (2005). “Efficient localized localization algorithm for wireless sensor networks”. In: *Computer and Information Technology, 2005. CIT 2005. The Fifth International Conference on*. IEEE, pp. 517–523 (cit. on p. 19).

Liu, Ming, Wei Wei, and Zhihong Liu (2009). “A secure key pre-distribution scheme for wireless sensor networks”. In: *2009 4th IEEE Conference on Industrial Electronics and Applications*. IEEE, pp. 1762–1768 (cit. on p. 23).

Liu, T, Y Inoue, K Shibata, Y Hirota, et al. (2010). “A mobile force plate system and its application to quantitative evaluation of normal and pathological gait”. In: *2010 IEEE/ASME International Conference on Advanced Intelligent Mechatronics*, pp. 272–277 (cit. on p. 50).

Liu, T, Y Inoue, K Shibata, and K Shiojima (2011). “Three-dimensional gait analysis system with mobile force plates and motion sensors”. In: *2011 8th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, pp. 107–110 (cit. on p. 50).

Liu, Tao, Yoshino Inoue, Kyoko Shibata, and K Shiojima (2012). “A Mobile Force Plate and Three-Dimensional Motion Analysis System for Three-Dimensional Gait Assessment”. In: *IEEE Sensors Journal* 12.5, pp. 1461–1467 (cit. on p. 50).

Lo Re, Giuseppe, Fabrizio Milazzo, and Marco Ortolani (2015a). “Secure random number generation in wireless sensor networks”. In: *Concurrency and Computation: Practice and Experience* 27.15, pp. 3842–3862 (cit. on p. 36).

— (Oct. 2015b). “Secure random number generation in wireless sensor networks”. In: *Concurrency and Computation Practice and Experience* 27, pp. 3842–. DOI: 10.1002/cpe.3311 (cit. on p. 37).

Lo, B P L, H Ip, and G Z Yang (2016). “Transforming Health Care: Body Sensor Networks, Wearables, and the Internet of Things”. In: *IEEE Pulse* 7.1, pp. 4–8 (cit. on p. 78).

Lo, Benny, Athanasia Panousopoulou, et al. (2014a). “Autonomic Sensing”. In: *Body Sensor Networks*. Ed. by Guang-Zhong Yang. 2nd ed. Springger. Chap. 10, pp. 405–462 (cit. on p. 17).

— (2014b). “Autonomic Sensing”. In: *Body Sensor Networks*. Ed. by Guang-Zhong Yang. 2nd ed. Springger. Chap. 10, pp. 405–462 (cit. on p. 19).

Lo, F., C. Li, et al. (July 2017). “Continuous systolic and diastolic blood pressure estimation utilizing long short-term memory network”. In: *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 1853–1856. DOI: 10.1109/EMBC.2017.8037207 (cit. on p. 59).

Looper, Christian de (2019). *Apple patent hints at biometric authentication for the Apple Watch*. URL: https://www.digitaltrends.com/wearables/apple-watch-biometric-authentication-patent/ (cit. on p. 26).

Loutfi, J et al. (Nov. 2014). "Smartphone sensors as random bit generators". In: *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, pp. 773–780 (cit. on pp. 37, 142, 155).

Lu, Rongxing, Xiaodong Lin, and Xuemin Shen (2012). "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency". In: *IEEE transactions on parallel and distributed systems* 24.3, pp. 614–624 (cit. on p. 12).

Ma, Hai-Qiang, Yuejian Xie, and Ling-An Wu (2005). "Random number generation based on the time of arrival of single photons". In: *Applied optics* 44.36, pp. 7760–7763 (cit. on p. 36).

Ma, Xiongfeng, Xiao Yuan, et al. (2016). "Quantum random number generation". In: *npj Quantum Information* 2, p. 16021 (cit. on p. 37).

Maheswari, S U et al. (2016). "A novel robust routing protocol RAEED to avoid DoS attacks in WSN". In: *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1–5 (cit. on p. 25).

Mahfouz, Ahmed, Tarek M Mahmoud, and Ahmed Sharaf Eldin (2017). "A survey on behavioral biometric authentication on smartphones". In: *Journal of Information Security and Applications* 37, pp. 28–37 (cit. on p. 90).

Mahmoud, R et al. (2015). "Internet of things (IoT) security: Current status, challenges and prospective measures". In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336–341 (cit. on p. 25).

Mainanwal, V, M Gupta, and S K Upadhayay (2015). "A survey on wireless body area network: Security technology and its design methodology issue". In: *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1–5 (cit. on p. 111).

Makihara, Yasushi et al. (2011). "Gait-based age estimation using a whole-generation gait database". In: *2011 International Joint Conference on Biometrics*. IEEE, pp. 1–6 (cit. on p. 90).

Malan, David et al. (2004). “Codeblue: An ad hoc sensor network infrastructure for emergency medical care”. In: *International workshop on wearable and implantable body sensor networks*. Vol. 5. Boston, MA; pp. 12–14 (cit. on p. 14).

Maltoni, Davide et al. (2009). *Handbook of fingerprint recognition*. Springer Science and Business Media (cit. on pp. 29, 33).

Manap, H H, N M Tahir, and R Abdullah (2012). “Anomalous gait detection using Naive Bayes classifier”. In: *Industrial Electronics and Applications (ISIEA), 2012 IEEE Symposium on*, pp. 378–381 (cit. on pp. 53, 56).

Mao, Zijing, Wan Xiang Yao, and Yufei Huang (May 2017). “EEG-based biometric identification with deep learning”. In: *2017 8th International IEEE/EMBS Conference on Neural Engineering (NER)*, pp. 609–612 (cit. on pp. 34, 61, 75, 76).

Maranesi, E et al. (2014). “A goniometer-based method for the assessment of gait parameters”. In: *2014 IEEE/ASME 10th International Conference on Mechatronic and Embedded Systems and Applications (MESA)*, pp. 1–4 (cit. on p. 50).

Marcel, Sebastien and Jose del R Millan (Apr. 2007). “Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29.4, pp. 743–752 (cit. on pp. 34, 58).

Marghescu, A, G Teseleanu, and P Svasta (2014). “Cryptographic key generator candidates based on smartphone built-in sensors”. In: *2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, pp. 239–243 (cit. on p. 142).

Marsaglia, George, Wai Wan Tsang, et al. (2002). “Some difficult-to-pass tests of randomness”. In: *Journal of Statistical Software* 7.3, pp. 1–9 (cit. on p. 150).

Maskooki, A et al. (2011). “Opportunistic routing for body area network”. In: *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 237–241 (cit. on p. 14).

Masuda, Yuichi, Akihito Noda, and Hiroyuki Shinoda (2018). “Body Sensor Networks Powered by an NFC-Coupled Smartphone in the Pocket”. In: *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE, pp. 5394–5397 (cit. on p. 12).

Mathew, S K et al. (2016). “mu RNG: A 300 950 mV, 323 Gbps/W All-Digital Full-Entropy True Random Number Generator in 14 nm FinFET CMOS”. In: *IEEE Journal of Solid-State Circuits* 51.7, pp. 1695–1704 (cit. on p. 141).

Matney, Lucas (2017). *Google introduces Neural Networks API in developer preview of Android 8.1*. URL: https://techcrunch.com/2017/10/25/google-introduces-neural-networks-api-in-developer-preview-of-android-8-1/ (cit. on p. 113).

Maurer, Ueli (1992). “A Universal Statistical Test for Random Bit Generators”. In: *Journal of cryptology* 5, pp. 89–105 (cit. on p. 150).

Meharia, Pallavi and Dharma P Agrawal (2015). “The Able Amble: Gait Recognition Using Gaussian Mixture Model for Biometric Applications”. In: *ACM International Conference on Computing Frontiers*. New York, NY, USA, pp. 1–5 (cit. on p. 79).

Meng, Weizhi et al. (2018). “Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks”. In: *IEEE Transactions on Network and Service Management* 15.2, pp. 761–773 (cit. on p. 23).

Menotti, David et al. (2015). “Deep representations for iris, face, and fingerprint spoofing detection”. In: *IEEE Transactions on Information Forensics and Security* 10.4, pp. 864–879 (cit. on p. 31).

Meola, Andrew (2016). “Wearable technology and IoT wearable devices”. In: *Business Insider UK* (cit. on p. 140).

Miao, F et al. (2009a). “A Novel Biometrics Based Security Solution for Body Sensor Networks”. In: *International Conference on Biomedical Engineering and Informatics*, pp. 1–5 (cit. on p. 26).

— (2009b). “A Novel Biometrics Based Security Solution for Body Sensor Networks”. In: *International Conference on Biomedical Engineering and Informatics*, pp. 1–5 (cit. on p. 79).

— (2009c). “Biometrics based novel key distribution solution for body sensor networks”. In: *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2458–2461 (cit. on p. 113).

Micera, S et al. (2004). “On the analysis of knee biomechanics using a wearable biomechatronic device”. In: *2004 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (IEEE Cat. No.04CH37566)*. Vol. 2, pp. 1674–1679 (cit. on p. 50).

Middleton, P., P. Kjeldsen, and J. Tully (2013). “Forecast: The internet of things worldwide, 2013”. In: *Gartner* (cit. on p. 140).

Mikolov, Tomas et al. (2010). “Recurrent neural network based language model”. In: *Eleventh annual conference of the international speech communication association* (cit. on p. 58).

Millman, Rene (2018). *Brute force and dictionary attacks up 400 percent in 2017* (cit. on p. 135).

Mitzenmacher, Michael (2008). *Tossing a biased coin*. URL: http://www.eecs.harvard.edu/~michaelm/coinflipext.pdf (cit. on p. 150).

Mo, Yilin and Bruno Sinopoli (2009). “Secure control against replay attacks”. In: *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 911–918 (cit. on p. 24).

Mohssen, Nesma et al. (2014). “It’s the Human That Matters: Accurate User Orientation Estimation for Mobile Computing Applications”. In: *nternational Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 70–79 (cit. on p. 83).

Monrose, Fabian et al. (2000). “Cryptographic key generation from voice”. In: *Proceedings 2001 IEEE Symposium on Security and Privacy*. IEEE, pp. 202–213 (cit. on p. 26).

Moosavi, S R et al. (2017). “Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation”. In: *IEEE Access* 6.99, p. 1 (cit. on p. 133).

Morris, Thomas (2011). “Trusted platform module”. In: *Encyclopedia of cryptography and security*. Springer, pp. 1332–1335 (cit. on p. 18).

Motiian, Saeid et al. (2015). “Automated extraction and validation of childrens gait parameters with the Kinect”. In: *BioMedical Engineering OnLine* 14, p. 112 (cit. on p. 47).

Muaaz, Muhammad and Rene Mayrhofer (2017). “Smartphone-Based Gait Recognition: From Authentication to Imitation”. In: *IEEE Transactions on Mobile Computing* 16.11, pp. 3209–3221 (cit. on pp. 32, 136).

Muhammed, Thaha et al. (2018). “UbeHealth: a personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities”. In: *IEEE Access* 6, pp. 32258–32285 (cit. on p. 11).

Murgia, Madhumita (2017). *How smartphones are transforming healthcare*. URL: https://www.ft.com/content/1efb95ba-d852-11e6-944b-e7eb37a6aa8e (cit. on p. 20).

Muro-de-la-Herran, A, G B Zapirain, and M A Zorrilla (2014). “Gait analysis methods: an overview of wearable and non-wearable systems. Highlighting clinical applications”. In: *Sensors* 14.2, pp. 3362–3394 (cit. on p. 45).

Murugesan, San and Irena Bojanova (2016). *Encyclopedia of cloud computing*. John Wiley & Sons, pp. 208–219. ISBN: 1118821971 (cit. on p. 22).

Nakano, T et al. (2016). “Gaits classification of normal vs. patients by wireless gait sensor and Support Vector Machine (SVM) classifier”. In: *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, pp. 1–6 (cit. on pp. 54, 56).

Nandy, A and P Chakraborty (2015). “A new paradigm of human gait analysis with Kinect”. In: *Contemporary Computing (IC3), 2015 Eighth International Conference on*, pp. 443–448 (cit. on pp. 53, 56).

Newsome, James et al. (2004). “The sybil attack in sensor networks: analysis & defenses”. In: *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, pp. 259–268 (cit. on p. 25).

Ng, H S, M L Sim, and C M Tan (Apr. 2006). “Security Issues of Wireless Sensor Networks in Healthcare Applications”. In: *BT Technology Journal* 24.2, pp. 138–144 (cit. on p. 23).

Ng, Jason W P, Benny P L Lo, et al. (2004). “Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon)”. In: *International Conference on Ubiquitous Computing (Ubicomp)* (cit. on p. 14).

Ngo, Thanh Trung et al. (2014). “The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication”. In: *Pattern Recognition* 47.1, pp. 228–237 (cit. on pp. 92, 94).

Nickel, C, T Wirtl, and C Busch (July 2012). “Authentication of Smartphone Users Based on the Way They Walk Using k-NN Algorithm”. In: *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 16–20 (cit. on pp. 112, 113).

Nie, Tingyuan and Teng Zhang (2009). “A study of DES and Blowfish encryption algorithm”. In: *Tencon 2009-2009 IEEE Region 10 Conference*. IEEE, pp. 1–4 (cit. on p. 34).

Nie, You-Qi, Hong-Fei Zhang, et al. (2014). "Practical and fast quantum random number generation based on photon arrival time relative to external reference". In: *Applied Physics Letters* 104.5, p. 51110 (cit. on p. 36).

Nilges, Tobias (2015). "The Cryptographic Strength of Tamper-Proof Hardware." Karlsruhe Institute of Technology (cit. on p. 18).

Nordic (2019). *Bluetooth Low Energy The world's most popular connectivity choice*. URL: https://www.nordicsemi.com/Products/Low-power-short-range-wireless/Bluetooth-low-energy (cit. on p. 35).

Noubir, Guevara and Guolong Lin (2003). "Low-power DoS attacks in data wireless LANs and countermeasures". In: *ACM SIGMOBILE Mobile Computing and Communications Review* 7.3, pp. 29–30 (cit. on p. 24).

Oberoi, D et al. (2016). "Wearable security: Key derivation for Body Area sensor Networks based on host movement". In: *2016 IEEE 25th International Symposium on Industrial Electronics (ISIE)*, pp. 1116–1121 (cit. on pp. 40, 112).

OED (2019). *protocol, n.* URL: https://www.oed.com/view/Entry/153243?rskey=foWLmp%5C&result=1#eid (cit. on p. 14).

Olavsrud, Thor (2016). *Connected medical device makers need to step up security*. URL: https://www.cio.com/article/3102918/connected-medical-device-makers-need-to-step-up-security.html (cit. on p. 25).

Orme, David (2019). *The role of biometrics in healthcare*. URL: https://www.openaccessgovernment.org/biometrics-in-healthcare/59405/ (cit. on p. 21).

Osadchy, Margarita et al. (Sept. 2013). *System for secure face identification (SCIFI) and methods useful in conjunction therewith* (cit. on p. 30).

Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy (2011). "Cloud computing: security issues and research challenges". In: *International Journal of Computer Science and Information Technology & Security (IJCSITS)* 1.2, pp. 136–146 (cit. on p. 25).

Palaniappan, R and D P Mandic (Apr. 2007). "Biometrics from Brain Electrical Activity: A Machine Learning Approach". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29.4, pp. 738–742 (cit. on p. 60).

Palaniappan, R and P Raveendran (2001). “Single trial VEP extraction using digital filter”. In: *Proceedings of the 11th IEEE Signal Processing Workshop on Statistical Signal Processing*, pp. 249–252 (cit. on p. 60).

Panahandeh, G et al. (2013). “Continuous Hidden Markov Model for Pedestrian Activity Classification and Gait Analysis”. In: *IEEE Transactions on Instrumentation and Measurement* 62.5, pp. 1073–1083 (cit. on pp. 54, 56).

Paranjape, R B et al. (2001). “The electroencephalogram as a biometric”. In: *Canadian Conference on Electrical and Computer Engineering 2001*. Vol. 2, pp. 1363–1366 (cit. on pp. 34, 60).

Park, J et al. (2016). “Custom optoelectronic force sensor based ground reaction force (GRF) measurement system for providing absolute force”. In: *2016 13th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, pp. 75–77 (cit. on p. 50).

Parkka, J et al. (2006). “Activity classification using realistic data from wearable sensors”. In: *IEEE Transactions on Information Technology in Biomedicine* 10.1, pp. 119–128 (cit. on pp. 54, 56).

Patrizi, Alfredo, Ettore Pennestri, and Pier Paolo Valentini (2016). “Comparison between low-cost marker-less and high-end marker-based motion capture systems for the computer-aided assessment of working ergonomics”. eng. In: *Ergonomics* 59.1, pp. 155–162 (cit. on p. 103).

Patterson, Matthew R and Brian Caulfield (2011). “A novel approach for assessing gait using foot mounted accelerometers”. In: *2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops*, pp. 218–221 (cit. on p. 49).

— (2013). “Using a foot mounted accelerometer to detect changes in gait patterns”. In: *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 7471–7475 (cit. on p. 49).

Pearlman, Shana (2019). *What is Data Integrity and Why Is It Important?* URL: https://www.talend.com/resources/what-is-data-integrity/ (cit. on p. 17).

Perlin, Hugo Alberto and Heitor Silverio Lopes (2015). “Extracting human attributes using a convolutional neural network approach”. In: *Pattern Recognition Letters* 68, pp. 250–259 (cit. on p. 90).

Perry, Jacquelin and Judith M Burnfield (2010). *Gait Analysis: Normal and Pathological Function*. SLACK Incorporated. ISBN: 978-1-55642-766-4 (cit. on p. 45).

Peterson, W. and E. J. Weldon (1972). *Error-Correcting Codes*. 2nd ed. Cambridge, Massachusetts, and London: The M.I.T. Press, pp. 269–304 (cit. on pp. 122, 127).

Pinkle, Carsten (2016). *The Why and How of Differential Signaling*. URL: https://www.allaboutcircuits.com/technical-articles/the-why-and-how-of-differential-signaling/ (cit. on p. 40).

Prabhakar, S, S Pankanti, and A K Jain (2003). "Biometric recognition: security and privacy concerns". In: *IEEE Security & Privacy* 1.2, pp. 33–42 (cit. on p. 28).

Prakash, C, A Mittal, et al. (2015). "Identification of gait parameters from silhouette images". In: *Contemporary Computing (IC3), 2015 Eighth International Conference on*, pp. 190–195 (cit. on p. 46).

Prakash, Narayanam Sri and N Venkatram (2016). "Establishing efficient security scheme in home IOT devices through biometric finger print technique". In: *Indian Journal of Science and Technology* 9.17 (cit. on p. 30).

Pratley, Nils (2019). *British Airways fine shows GDPR has given watchdogs teeth*. URL: https://www.theguardian.com/business/nils-pratley-on-finance/2019/jul/08/british-airways-fine-shows-gdpr-has-given-watchdogs-teeth (cit. on pp. 12, 21).

Preidt, Robert (2018). *Medical E-Records Not Without Risks: Study*. URL: https://www.webmd.com/a-to-z-guides/news/20180328/medical-e-records-not-without-risks-study (cit. on p. 21).

Privacyrights (2018). *DATA BREACHES*. URL: https://www.privacyrights.org/data-breaches?title=&org_type%5B%5D=258 (cit. on p. 21).

Publico, Ricky (2017). *What is a Man-in-the-Middle Attack and How Can You Prevent It?* URL: https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack/ (cit. on p. 17).

Qin, Zhongyuan et al. (2014). "A Novel Key Pre-distribution Scheme in Wireless Sensor Networks". In: *Tenth International Conference on Computational Intelligence and Security*. IEEE, pp. 615–619 (cit. on p. 23).

Quinn, Ben (2016). *Google given access to healthcare data of up to 1.6 million patients*. URL: https://www.theguardian.com/technology/2016/may/04/google-deepmind-access-healthcare-data-patients (cit. on p. 22).

Quwaider, Muhannad and Subir Biswas (2009). "On-body packet routing algorithms for body sensor networks". In: *2009 first international conference on networks and communications*. IEEE, pp. 171–177 (cit. on p. 15).

Rahman, Lu (2018). *Why the hacking of medical devices is still big news*. URL: https://www.medicalplasticsnews.com/news/opinion/why-the-hacking-of-medical-devices-is-still-big-news/ (cit. on p. 25).

Ramli, S N, R Ahmad, and M F Abdollah (2013). "Electrocardiogram (ECG) signals as biometrics in securing Wireless Body Area Network". In: *International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pp. 536–541 (cit. on p. 79).

Raposo, Vera Lucia (2015). "Electronic health records: Is it a risk worth taking in healthcare delivery?" In: *GMS health technology assessment* 11 (cit. on p. 21).

Rassan, Iehab A L and Hanan Al Shaher (2013). "Securing mobile cloud using finger print authentication". In: *International Journal of Network Security & Its Applications* 5.6, p. 41 (cit. on p. 30).

Rathgeb, C. and A. Uhl (2012). "Statistical attack against fuzzy commitment scheme". In: *IET Biometrics* 1.2, pp. 94–104 (cit. on p. 136).

Rawlinson, Kristi (2015). *HP Study Reveals Smartwatches Vulnerable to Attack* (cit. on p. 10).

Raza, S., D. Trabalza, and T. Voigt (2012). "6LoWPAN compressed DTLS for CoAP". In: *Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on*. IEEE, pp. 287–289 (cit. on p. 18).

Raza, S, H Shafagh, et al. (2013). "Lithe: Lightweight Secure CoAP for the Internet of Things". In: *IEEE Sensors Journal* 13.10, pp. 3711–3720 (cit. on p. 35).

Raza, Shahid, Simon Duquennoy, et al. (2011). "Securing communication in 6LoWPAN with compressed IPsec". In: *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*. IEEE, pp. 1–8 (cit. on p. 18).

Raza, Shahid, Linus Wallgren, and Thiemo Voigt (2013). "SVELTE: Real-time intrusion detection in the Internet of Things". In: *Ad hoc networks* 11.8, pp. 2661–2674 (cit. on p. 19).

Reeder, R A (1998). “Detecting knee hyperextension using goniometric inclinometer sensing with vibrotactile feedback”. In: *IMTC/98 Conference Proceedings. IEEE Instrumentation and Measurement Technology Conference. Where Instrumentation is Going (Cat. No.98CH36222)*. Vol. 2, pp. 863–867 (cit. on p. 50).

Revadigar, G, C Javali, W Xu, W Hu, et al. (2016). “Secure key generation and distribution protocol for wearable devices”. In: *IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pp. 1–4 (cit. on p. 79).

Revadigar, G, C Javali, W Xu, A V Vasilakos, et al. (2017). “Accelerometer and Fuzzy Vault-Based Secure Group Key Generation and Sharing Protocol for Smart Wearables”. In: *IEEE Transactions on Information Forensics and Security* 12.10, pp. 2467–2482 (cit. on pp. 40, 113, 119, 144, 146).

Riaz, Qaiser et al. (2015). “One small step for a man: Estimation of gender, age and height from recordings of one step by a single inertial sensor”. In: *Sensors* 15.12, pp. 31999–32019 (cit. on pp. 91, 100).

Rice, Ken and Thomas Lumley (2008). *Permutation tests*. URL: http://faculty.washington.edu/kenrice/sisg/SISG-08-06.pdf (cit. on p. 150).

Rocha, Ana Patricia et al. (2015). “Kinect v2 based system for Parkinsons disease assessment”. In: *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*. Vol. 11, pp. 1279–1282 (cit. on pp. 47, 51).

Rosenblatt, Gideon (2011). *Trust and Networks*. URL: https://www.the-vital-edge.com/trust-and-networks/ (cit. on p. 23).

Ross, Arun, Anil Jain, and S Pankati (1999). “A prototype hand geometry-based verification system”. In: *Proceedings of 2nd conference on audio and video based biometric person authentication*, pp. 166–171 (cit. on pp. 29, 33).

Rostami, Masoud, Ari Juels, and Farinaz Koushanfar (2013). “Heart-to-heart (H2H): authentication for implanted medical devices”. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, pp. 1099–1112 (cit. on p. 34).

Rouse, Margaret (2017). *Advanced Encryption Standard (AES)*. URL: https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard (cit. on pp. 34, 35).

Roy, Sanjoy and Suparna Biswas (2019). "A Novel Trust Evaluation Model Based on Data Freshness in WBAN". In: *Proceedings of International Ethical Hacking Conference 2018*. Springer, pp. 223–232.

Rukhin, Andrew et al. (2010). *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 (cit. on pp. 134, 148).

Rushanan, Michael et al. (2014). "Sok: Security and privacy in implantable medical devices and body area networks". In: *2014 IEEE Symposium on Security and Privacy*. IEEE, pp. 524–539 (cit. on p. 40).

Russell, Brian and Drew Van Duren (2016). *Practical Internet of Things Security*. Packt Publishing Ltd (cit. on p. 34).

Saeedi, R et al. (2014). "Toward seamless wearable sensing: Automatic on-body sensor localization for physical activity monitoring". In: *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5385–5388. DOI: 10.1109/EMBC.2014.6944843 (cit. on p. 19).

Samaria, Ferdinando S and Andy C Harter (1994). "Parameterisation of a stochastic model for human face identification". In: *Applications of Computer Vision, 1994., Proceedings of the Second IEEE Workshop on*. IEEE, pp. 138–142 (cit. on p. 57).

Samonas, Spyridon and David Coss (2014). "THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY." In: *Journal of Information System Security* 10.3 (cit. on pp. 16, 18).

Sanguinetti, Bruno et al. (2014). "Quantum random number generation on a mobile phone". In: *Physical Review X* 4.3, p. 31056 (cit. on p. 36).

Sarkar, Manasi and Debdutta Barman Roy (2011). "Prevention of sleep deprivation attacks using clustering". In: *2011 3rd International Conference on Electronics Computer Technology*. Vol. 5, pp. 391–394 (cit. on p. 25).

Sathya, K, J Premalatha, and V Rajasekar (2015). "Random number generation based on sensor with decimation method". In: *2015 IEEE Workshop on Computational Intelligence: Theories, Applications and Future Directions (WCI)*, pp. 1–5 (cit. on pp. 142, 155).

Scammell, Robert (2019). *PCM data breach highlights risks of third-party cloud providers*. URL: https://www.verdict.co.uk/pcm-data-breach-cloud-providers/ (cit. on p. 11).

Schalk, G. et al. (2004). "BCI2000: A General-Purpose Brain-Computer Interface (BCI) System". In: *IEEE Transactions on Biomedical Engineering* 51.6, pp. 1034–1043 (cit. on p. 67).

Scheirer, W. J. and T. E. Boult (2007). "Cracking Fuzzy Vaults and Biometric Encryption". In: *Biometrics Symposium*, pp. 1–6 (cit. on p. 136).

Schons, Thiago et al. (2017). "Convolutional Network for EEG-Based Biometric". In: *Iberoamerican Congress on Pattern Recognition*, pp. 601–608 (cit. on pp. 34, 61, 75).

Schurmann, D et al. (2017). "BANDANA Body area network device-to-device authentication using natural gAit". In: *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 190–196 (cit. on pp. 18, 39, 79, 84, 112, 120).

Sedaaghi, M. H. (2009). "A comparative study of gender and age classification in speech signals". In: *Iranian Journal of Electrical and Electronic Engineering* 5.1, pp. 1–12 (cit. on p. 90).

Seel, T, T Schauer, and J Raisch (2012). "Joint axis and position estimation from inertial measurement data by exploiting kinematic constraints". In: *2012 IEEE International Conference on Control Applications*, pp. 45–49 (cit. on p. 103).

Seetharam, Deva and Sokwoo Rhee (2004). "An efficient pseudo random number generator for low-power sensor networks [wireless networks]". In: *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, pp. 560–562 (cit. on p. 37).

Shaikh, Soharab Hossain, Khalid Saeed, and Nabendu Chaki (2014). "Gait recognition using partial silhouette-based approach". In: *Signal Processing and Integrated Networks (SPIN), 2014 International Conference on*, pp. 101–106 (cit. on p. 46).

Shannon, C E (1948). "A mathematical theory of communication". In: *The Bell System Technical Journal* 27.3, pp. 379–423 (cit. on p. 133).

Shelke, P B and P R Deshmukh (2015). "Gait Based Gender Identification Approach". In: *2015 Fifth International Conference on Advanced Computing & Communication Technologies*, pp. 121–124 (cit. on pp. 53, 56).

Shin, Hirofumi, Shuhei Ikemoto, and Koh Hosoda (2014). "An extended inverted pendulum model giving minimal interpretation of vertical ground reaction force while a human walks". In: *Robotics and Biomimetics (ROBIO), 2014 IEEE International Conference on*, pp. 1487–1492 (cit. on p. 52).

Shin, Minchul and Inwhee Joe (2015). "An indoor localization system considering channel interference and the reliability of the RSSI measurement to enhance location accuracy". In: *2015 17th International Conference on Advanced Communication Technology (ICACT)*. IEEE, pp. 583–592 (cit. on p. 14).

Shit, Rathin Chandra et al. (2018). "Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure". In: *IEEE Communications Surveys & Tutorials* (cit. on p. 19).

Shu, Minglei, Yunxiang Liu, and Hua Fang (2014). "Identification authentication scheme using human body odour". In: *2014 IEEE International Conference on Control Science and Systems Engineering*. IEEE, pp. 171–174 (cit. on pp. 29, 33).

Singh, Ninoshka K and Darnell O Ricke (2016). "Towards an open data framework for body sensor networks supporting bluetooth low energy". In: *2016 IEEE 13th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. IEEE, pp. 396–401 (cit. on p. 12).

Soaz, Cristina and Klaus Diepold (2016). "Step Detection and Parameterization for Gait Assessment Using a Single Waist-Worn Accelerometer". In: *IEEE Transactions on Biomedical Engineering* 63.5, pp. 933–942 (cit. on pp. 49, 54, 56).

Soda, Paolo et al. (2009). "A low-cost video-based tool for clinical gait analysis". In: *Proceedings of the 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society: Engineering the Future of Biomedicine, EMBC 2009*, pp. 3979–3982 (cit. on p. 46).

Song, Chul Gyu et al. (2006). "A new approach for detection of leg movement using bio-impedance measurement". In: *2006 IEEE Biomedical Circuits and Systems Conference*, pp. 13–16 (cit. on p. 50).

Soni, Vinay, Pratik Modi, and Vishvash Chaudhri (2013). "Detecting Sinkhole attack in wireless sensor network". In: *International Journal of Application or Innovation in Engineering & Management* 2.2, pp. 29–32 (cit. on p. 25).

Spaan, Nienke A et al. (2014). "Implantable insulin pumps: an effective option with restricted dissemination". In: *The Lancet Diabetes and Endocrinology* 2.5, pp. 358–360.

Spacey, John (2016). *Backward Compatibility vs Forward Compatibility*. URL: https://simplicable.com/new/backward-compatibility-vs-forward-compatibility (cit. on p. 20).

Spanakis, Emmanouil G et al. (2016). "Secure access to patient's health records using SpeechXRays a mutli-channel biometrics platform for user authentication". In: *Engineering in Medicine and Biology Society (EMBC), 2016 IEEE 38th Annual International Conference of the*. IEEE, pp. 2541–2544 (cit. on p. 32).

Stankovic, J A (2014). "Research Directions for the Internet of Things". In: *IEEE Internet of Things Journal* 1.1, pp. 3–9 (cit. on p. 19).

Staranowicz, Aaron, Garrett R Brown, and Gian-Luca Mariottini (2013). "Evaluating the Accuracy of a Mobile Kinect-based Gait-monitoring System for Fall Prediction". In: *Proceedings of the 6th International Conference on PErvasive Technologies Related to Assistive Environments*. PETRA '13. New York, NY, USA: ACM, pp. 1–4 (cit. on p. 47).

Staranowicz, Aaron, Christopher Ray, and Luca Mariottini (2015). "Easy-to-use, general, and accurate multi-Kinect calibration and its application to gait monitoring for fall prediction". In: *International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, pp. 4994–4998 (cit. on p. 47).

Stone, E E and M Skubic (2012). *Capturing habitual, in-home gait parameter trends using an inexpensive depth camera* (cit. on p. 47).

Stone, Erik E., Marjorie Skubic, and Jessica Back (2014). "Automated health alerts from Kinect-based in-home gait measurements". In: *International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2961–2964 (cit. on p. 47).

Strozzi, Nicolo, Federico Parisi, and Gianluigi Ferrari (2016). "On single sensor-based inertial navigation". In: *BSN 2016 - 13th Annual Body Sensor Networks Conference*, pp. 300–305 (cit. on p. 52).

Subash, TD and C Divya (2011). "Novel key pre-distribution scheme in wireless sensor network". In: *2011 International Conference on Emerging Trends in Electrical and Computer Technology*. IEEE, pp. 959–963 (cit. on p. 23).

Suciu, A, D Lebu, and K Marton (2011). “Unpredictable random number generator based on mobile sensors”. In: *2011 IEEE 7th International Conference on Intelligent Computer Communication and Processing*, pp. 445–448 (cit. on pp. 37, 142, 155).

Sufyan, Nadeem, Nazar Abbass Saqib, and Muhammad Zia (2013). “Detection of jamming attacks in 802.11 b wireless networks”. In: *EURASIP Journal on Wireless Communications and Networking* 2013.1, p. 208 (cit. on p. 23).

Sun, Y. and B. Lo (Aug. 2018a). “An Artificial Neural Network Framework for Gait Based Biometrics”. In: *IEEE Journal of Biomedical and Health Informatics*. ISSN: 2168-2194. DOI: 10.1109/JBHI.2018.2860780 (cit. on p. 57).

Sun, Y, C Wong, et al. (2017). “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 (cit. on pp. 40, 78, 90, 107, 118, 137, 141, 143).

Sun, Yingnan and Benny Lo (2018b). “An Artificial Neural Network Framework for Gait-Based Biometrics”. In: *IEEE journal of biomedical and health informatics* 23.3, pp. 987–998 (cit. on pp. 13, 102).

— (2018c). “Random number generation using inertial measurement unit signals for on-body IoT devices”. In: *Living in the Internet of Things: Cybersecurity of the IoT-2018*. IET, pp. 1–9 (cit. on pp. 37, 140).

Sun, Yingnan, Frank P-W Lo, and Benny Lo (2019a). “EEG-based user identification system using 1D-convolutional long short-term memory neural networks”. In: *Expert Systems with Applications* 125, pp. 259–267 (cit. on p. 57).

Sun, Yingnan, Frank Lo, and Benny Lo (2019b). “A Deep Learning Approach on Gender and Age Recognition using a Single Inertial Sensor”. In: *IEEE Conference on Body Sensor Networks* (cit. on p. 78).

Sun, Yingnan, Guang-Zhong Yang, and Benny Lo (2018). “An Artificial Neural Network Framework for Lower Limb Motion Signal Estimation with Foot-Mounted Inertial Sensors”. In: *IEEE Conference on Body Sensor Networks* (cit. on pp. 102, 115).

Swain, Bijay (2009). *What are malware, viruses, Spyware, and cookies, and what differentiates them ?* URL: https://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them (cit. on p. 17).

Sys, Marek et al. (2015). "On the interpretation of results from the NIST statistical test suite". In: *ROMANIAN JOURNAL OF INFORMATIONSCIENCE AND TECHNOLOGY* 18.1, pp. 18–32 (cit. on pp. 134, 148).

SysTutorials (n.d.). *dieharder (1) - Linux Man Pages*. URL: https://www.systutorials.com/docs/linux/man/1-dieharder/#lbAG (cit. on p. 152).

Sztyler, T., H. Stuckenschmidt, and P. Wolfgang (2017). "Position-Aware Activity Recognition with Wearable Devices". In: *Pervasive and Mobile Computing* 38, Part 2, pp. 281–295 (cit. on pp. 123, 147).

Tadano, Shigeru, Ryo Takeda, and Hiroaki Miyagawa (2013). "Three Dimensional Gait Analysis Using Wearable Acceleration and Gyro Sensors Based on Quaternion Calculations". In: *Sensors* 13.7, pp. 9321–9343 (cit. on pp. 103, 126).

Tallapragada, Suma and L. V Chaitanya Srinivas (2011). "Marker less view independent gait analysis using DFT". In: *ICECT 2011 - 2011 3rd International Conference on Electronics Computer Technology*. Vol. 3, pp. 11–13 (cit. on p. 53).

Tams, Benjamin (2014). "Decodability Attack against the Fuzzy Commitment Scheme with Public Feature Transforms". In: *arXiv:1406.1154v3 [cs.CR]* (cit. on p. 136).

Tan, Jen Hong et al. (2018). "Application of stacked convolutional and long short-term memory network for accurate identification of CAD ECG signals". In: *Computers in Biology and Medicine* 94, pp. 19–26. ISSN: 0010-4825 (cit. on p. 59).

Tang, Qinghui, Naveen Tummala, et al. (2005a). "Communication scheduling to minimize thermal effects of implanted biosensor networks in homogeneous tissue". In: *IEEE Transactions on Biomedical Engineering* 52.7, pp. 1285–1294 (cit. on p. 15).

— (2005b). "TARA: Thermal-Aware Routing Algorithm for Implanted Sensor Networks". In: *Distributed Computing in Sensor Systems: First IEEE International Conference, DCOSS 2005, Marina del Rey, CA, USA, June 30 – July 1, 2005. Proceedings*. Ed. by Viktor K Prasanna et al. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 206–217 (cit. on p. 15).

Tang, Zhe, Meng Joo Er, and C J Chien (2008). “Analysis of human gait using an Inverted Pendulum Model”. In: *Fuzzy Systems, 2008. FUZZ-IEEE 2008. (IEEE World Congress on Computational Intelligence). IEEE International Conference on*, pp. 1174–1178 (cit. on p. 52).

Thakkar, Danny (2017). *Biometric Performance Metrics Can Help You Select the Right Biometric Solution*. URL: https://www.bayometric.com/biometric-performance-metrics-select-right-solution/ (cit. on pp. 27, 29).

TI (2017). *CC2630 Comparison*. URL: http://www.ti.com/product/CC2630/compare (cit. on p. 35).

Tobin, Paul et al. (2017). “On the Development of a One-Time Pad Generator for Personalising Cloud Security”. In: *Eighth International Conference on Cloud Computing, GRIDs, and Virtualization*, pp. 19–23 (cit. on p. 141).

Tong, Raymond (2018). *Wearable Technology in Medicine and Health Care*. Academic Press (cit. on p. 39).

Trkov, M et al. (2015). “Slip detection and prediction in human walking using only wearable inertial measurement units (IMUs)”. In: *2015 IEEE International Conference on Advanced Intelligent Mechatronics (AIM)*, pp. 854–859 (cit. on p. 49).

Tupa, Ondrej et al. (2015). “Motion tracking and gait feature estimation for recognising Parkinsons disease using MS Kinect”. In: *BioMedical Engineering OnLine* 14.1 (cit. on p. 47).

Turner, Dawn (2016). *Digital Authentication - the basics*. URL: https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics (cit. on p. 26).

Turner, John (2018). *Security for Connected Medical Devices*. URL: https://www.medtechintelligence.com/feature_article/security-for-connected-medical-devices/ (cit. on p. 11).

Uslan, Daniel Z et al. (2012). “Cardiovascular implantable electronic device replacement infections and prevention: results from the REPLACE Registry”. In: *Pacing and Clinical Electrophysiology* 35.1, pp. 81–87 (cit. on p. 15).

Valera, A J J, M A Zamora, and A F G Skarmeta (2010). “An Architecture Based on Internet of Things to Support Mobility and Security in Medical Environments”. In: *2010 7th IEEE Consumer Communications and Networking Conference*, pp. 1–5 (cit. on p. 35).

Veen, Michiel van der et al. (2006). "Face biometrics with renewable templates". In: *Proceedings of SPIE* (cit. on p. 146).

Vicon (2017). *Motion Capture for Life Science*. URL: https://www.vicon.com/motion-capture/life-sciences (cit. on p. 103).

Villazon, Luis (2018). *Can fingerprints change during a lifetime?* URL: https://www.sciencefocus.com/the-human-body/can-fingerprints-change-during-a-lifetime/ (cit. on p. 90).

Voris, Jonathan, Nitesh Saxena, and Tzipora Halevi (2011). "Accelerometers and Randomness: Perfect Together". In: *Proceedings of the Fourth ACM Conference on Wireless Network Security*. WiSec '11. New York, NY, USA: ACM, pp. 115–126 (cit. on pp. 37, 154).

Vu, Tri et al. (2018). "BiGRA: A preliminary bilateral hand grip coordination rehabilitation using home-based evaluation system for stroke patients". In: *2018 IEEE 15th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. IEEE, pp. 13–16 (cit. on p. 14).

Walker, John (2008). *ENT: A Pseudorandom Number Sequence Test Program*. URL: http://www.fourmilab.ch/random/ (cit. on p. 148).

Wallace, K et al. (2016). "Toward Sensor-Based Random Number Generation for Mobile and IoT Devices". In: *IEEE Internet of Things Journal* 3.6, pp. 1189–1201 (cit. on pp. 37, 142, 155).

Wander, Arvinderpal S et al. (2005). "Energy analysis of public-key cryptography for wireless sensor networks". In: *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*. IEEE, pp. 324–328 (cit. on p. 35).

Wang, Cong, Qian Wang, et al. (2010). "Privacy-preserving public auditing for data storage security in cloud computing". In: *2010 proceedings ieee infocom*. Ieee, pp. 1–9 (cit. on p. 26).

Wang, Junqiu, Yasushi Makihara, and Yasushi Yagi (2008). "Human tracking and segmentation supported by silhouette-based gait recognition". In: *Proceedings - IEEE International Conference on Robotics and Automation*, pp. 1698–1703 (cit. on p. 46).

Wang, Liang, Tao Gu, et al. (2016). "Toward a wearable RFID system for real-time activity recognition using radio patterns". In: *IEEE Transactions on Mobile Computing* 16.1, pp. 228–242 (cit. on p. 12).

Wang, Z and R Ji (2015). “Estimate spatial-temporal parameters of human gait using inertial sensors”. In: *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pp. 1883–1888 (cit. on p. 103).

Watanabe, Masaki et al. (2005). “Palm vein authentication technology and its applications”. In: *Proceedings of the biometric consortium conference*, pp. 19–21 (cit. on pp. 29, 33).

Welpton, Richard (2018). *Patient data saves lives. Here’s how we use and protect it.* URL: https://scienceblog.cancerresearchuk.org/2018/05/25/patient-data-saves-lives-heres-how-we-use-and-protect-it/ (cit. on p. 22).

Whittle, Michael W., David Levine, and Jim Richards (2012a). *Whittle’s Gait Analysis*. Churchill Livingstone/Elsevier. ISBN: 9780702042652 (cit. on pp. 43, 45).

— (2012b). *Whittle’s Gait Analysis*. Churchill Livingstone/Elsevier. ISBN: 9780702042652 (cit. on p. 143).

Wildes, Richard P (1997). “Iris recognition: an emerging biometric technology”. In: *Proceedings of the IEEE* 85.9, pp. 1348–1363 (cit. on pp. 29, 33).

WISeKey (2017). *IoT Security Solutions Connected Objects - Root of Trust*. URL: https://docs.wisekey.com/site/justdownload.html?id=61 (cit. on p. 11).

Wojciechowska, Agata, Michal Choras, and Rafal Kozik (2017). “The overview of trends and challenges in mobile biometrics”. In: *Journal of Applied Mathematics and Computational Mechanics* 16 (cit. on p. 30).

Wong, Charence et al. (2012). “Enhanced classification of abnormal gait using BSN and depth”. In: *Proceedings - BSN 2012: 9th International Workshop on Wearable and Implantable Body Sensor Networks*, pp. 166–171 (cit. on p. 48).

Wu, Taiyang et al. (2017). “An autonomous wireless body area network implementation towards IoT connected healthcare applications”. In: *Ieee Access* 5, pp. 11413–11422 (cit. on p. 12).

X. Zhou et al. (2011). “Quantifying privacy and security of biometric fuzzy commitment”. In: *2011 International Joint Conference on Biometrics (IJCB)*, pp. 1–8 (cit. on p. 137).

Xiao, Yang et al. (2007). “A survey of key management schemes in wireless sensor networks”. In: *Computer communications* 30.11-12, pp. 2314–2341 (cit. on p. 22).

Xu, Fengyuan, Zhengrui Qin, et al. (2011). “IMDGuard: Securing implantable medical devices with the external wearable guardian”. In: *INFOCOM, 2011 Proceedings IEEE*. IEEE, pp. 1862–1870 (cit. on p. 38).

Xu, Teng and Miodrag Potkonjak (2013). “Lightweight digital hardware random number generators”. In: *SENSORS, 2013 IEEE*. IEEE, pp. 1–4 (cit. on p. 37).

Xu, W, G Revadigar, et al. (2016). “Walkie-Talkie: Motion-Assisted Automatic Key Generation for Secure On-Body Device Communication”. In: *ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pp. 1–12 (cit. on pp. 18, 26, 79, 83).

Xu, Weitao, Chitra Javali, et al. (Jan. 2017). “Gait-Key: A Gait-Based Shared Secret Key Generation Protocol for Wearable Devices”. In: *ACM Trans. Sen. Netw.* 13.1, 6:1–6:27 (cit. on pp. 40, 113, 115, 134).

Xu, Wenyuan, Ke Ma, et al. (2006). “Jamming sensor networks: attack and defense strategies”. In: *IEEE network* 20.3, pp. 41–47 (cit. on p. 24).

Xu, Wenyuan, Timothy Wood, et al. (2004). “Channel surfing and spatial retreats: defenses against wireless denial of service”. In: *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, pp. 80–89 (cit. on p. 24).

Yampolskiy, Roman V and Venu Govindaraju (2008). “Behavioural biometrics: a survey and classification”. In: *International Journal of Biometrics* 1.1, pp. 81–113 (cit. on pp. 29, 30).

Yan, Ping and Kevin W Bowyer (2007). “Biometric recognition using 3D ear shape”. In: *IEEE Transactions on pattern analysis and machine intelligence* 29.8, pp. 1297–1308 (cit. on pp. 29, 33).

Yang, Bo, Kaijie Wu, and Ramesh Karri (2004). “Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard”. In: *2004 International Conferce on Test*, pp. 339–344 (cit. on p. 25).

Yang, J, Y Lin, Y Fu, et al. (May 2017). “A small area and low power true random number generator using write speed variation of oxidebased RRAM for IoT security application”. In: *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–4 (cit. on p. 141).

Yang, Jucheng, Naixue Xiong, et al. (2011). “A fingerprint recognition scheme based on assembling invariant moments for cloud computing communications”. In: *IEEE Systems Journal* 5.4, pp. 574–583 (cit. on p. 30).

Yang, Su and Farzin Deravi (Sept. 2013). “Wavelet-Based EEG Preprocessing for Biometric Applications”. In: *2013 Fourth International Conference on Emerging Security Technologies*, pp. 43–46 (cit. on pp. 34, 60).

Yang, Xinyu, Xiaofei He, et al. (Aug. 2015). “Towards a Low-Cost Remote Memory Attestation for the Smart Grid”. eng. In: *Sensors (Basel, Switzerland)* 15.8, pp. 20799–20824 (cit. on p. 24).

Yang, Xinyu, Jie Lin, Wei Yu, et al. (2015). “A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems”. In: *IEEE Transactions on Computers* 64.1, pp. 4–18 (cit. on p. 24).

Yang, Y, F Wang, et al. (2014). “Automated gait discrimination using Hidden Markov Model”. In: *2014 9th IEEE Conference on Industrial Electronics and Applications*, pp. 1067–1071 (cit. on p. 56).

Yao, Mariya (2017). *Your Electronic Medical Records Could Be Worth $1000 To Hackers*. URL: `https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#61a0d42850cf` (cit. on p. 11).

Yeh, Kuo-Hui (2016). “A secure IoT-based healthcare system with body sensor networks”. In: *IEEE Access* 4, pp. 10288–10299 (cit. on pp. 12, 14).

Yeoh, Wee-Soon et al. (2008). “Ambulatory monitoring of human posture and walking speed using wearable accelerometer sensors”. In: *2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5184–5187 (cit. on p. 46).

Yin, S et al. (July 2017). “Designing ECG-based physical unclonable function for security of wearable devices”. In: *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 3509–3512 (cit. on p. 134).

Zang, Weilin and Ye Li (2017). “Gait Cycle Driven Transmission Power Control Scheme for Wireless Body Area Network”. In: *IEEE Journal of Biomedical and Health Informatics* 99, p. 1 (cit. on pp. 14, 16).

Zayaraz, G, V Vijayalakshmi, and D Jagadiswary (2009). “Securing biometric authentication using DNA sequence and Naccache Stern Knapsack cryptosystem”. In: *2009 International Conference on Control, Automation, Communication and Energy Conservation*. IEEE, pp. 1–4 (cit. on pp. 29, 33).

Zewail, R. et al. (July 2004). "Soft and hard biometrics fusion for improved identity verification". In: *The 2004 47th Midwest Symposium on Circuits and Systems, 2004. MWSCAS '04.* Vol. 1, pp. I–225 (cit. on p. 90).

Zhang, D, Y Wang, and B Bhanu (2010). "Age Classification Base on Gait Using HMM". In: *Pattern Recognition (ICPR), 2010 20th International Conference on*, pp. 3834–3837 (cit. on pp. 54, 56).

Zhang, G H, C C Y Poon, and Y T Zhang (2012). "Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks". In: *IEEE Transactions on Information Technology in Biomedicine* 16.1, pp. 176–182 (cit. on p. 79).

Zhang, Jing, Dawu Gu, et al. (2010). "Differential power cryptanalysis attacks against PRESENT implementation". In: *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*. Vol. 6, pp. 61–65 (cit. on p. 25).

Zhang, Meng, Anand Raghunathan, and Niraj K Jha (2013). "MedMon: Securing medical devices through wireless monitoring and anomaly detection". In: *IEEE Transactions on Biomedical circuits and Systems* 7.6, pp. 871–881 (cit. on p. 41).

Zhang, Xueying, Howard M Heys, and Cheng Li (2010). "Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks". In: *Communications (QBSC), 2010 25th Biennial Symposium on*. IEEE, pp. 168–172 (cit. on p. 35).

Zhang, Y, G Pan, et al. (2015). "Accelerometer-Based Gait Recognition by Sparse Representation of Signature Points With Clusters". In: *IEEE Transactions on Cybernetics* 45.9, pp. 1864–1875 (cit. on pp. 32, 79, 112, 113).

Zhang, Yin, Meikang Qiu, et al. (2017). "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data". In: *IEEE Systems Journal* 11.1, pp. 88–95. ISSN: 1932-8184. DOI: `10.1109/JSYST.2015.2460747` (cit. on p. 11).

Zhao, Kai and Lina Ge (2013). "A Survey on the Internet of Things Security". In: *2013 Ninth International Conference on Computational Intelligence and Security*, pp. 663–667 (cit. on p. 24).

Zhao, Nan, Richard Yu, et al. (2016). "Anti-Eavesdropping Schemes for Interference Alignment (IA)-Based Wireless Networks". In: *IEEE Transactions on Wireless Communications* 15.8, pp. 5719–5732 (cit. on p. 25).

Zhao, Wenyi, Rama Chellappa, et al. (2003). “Face recognition: A literature survey”. In: *ACM computing surveys (CSUR)* 35.4, pp. 399–458 (cit. on pp. 29, 33).

Zhao, Zhidong, Lei Yang, et al. (2013). “A human ECG identification system based on ensemble empirical mode decomposition”. In: *Sensors* 13.5, pp. 6832–6864 (cit. on p. 58).

Zheng, G, G Fang, M A Orgun, et al. (2015). “A comparison of key distribution schemes using fuzzy commitment and fuzzy vault within wireless body area networks”. In: *IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 2120–2125 (cit. on p. 87).

Zheng, G, G Fang, R Shankaran, M A Orgun, and E Dutkiewicz (2014). “An ECG-based Secret Data Sharing scheme supporting emergency treatment of Implantable Medical Devices”. In: *International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pp. 624–628 (cit. on pp. 79, 87).

Zheng, Guanglou, Gengfa Fang, Rajan Shankaran, and Mehmet A Orgun (2015). “Encryption for implantable medical devices using modified one-time pads”. In: *IEEE Access* 3, pp. 825–836 (cit. on p. 39).

Zheng, Guanglou, Gengfa Fang, Rajan Shankaran, Mehmet A Orgun, Jie Zhou, et al. (2017). “Multiple ECG Fiducial Points-Based Random Binary Sequence Generation for Securing Wireless Body Area Networks”. In: *IEEE Journal of Biomedical and Health Informatics* 21.3, pp. 655–663 (cit. on pp. 31, 131, 134).

Zheng, Guanglou, Rajan Shankaran, et al. (2017). “Ideas and challenges for securing wireless implantable medical devices: A review”. In: *IEEE Sensors Journal* 17.3, pp. 562–576 (cit. on p. 38).

Zheng, Zhuoran, Xiangwei Zheng, et al. (2018). “A Transmission Power Control Algorithm for Wireless Body Area Networks”. In: *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*. IEEE, pp. 854–858 (cit. on p. 14).

Zhuang, Yan et al. (2015). “SleepSense: Non-invasive sleep event recognition using an electromagnetic probe”. In: *2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. IEEE, pp. 1–6 (cit. on p. 14).

Zijlstra, Wiebren and At L Hof (Oct. 2003). “Assessment of spatio-temporal gait parameters from trunk accelerations during human walking.” ENG. In: *Gait & posture* 18.2, pp. 1–10 (cit. on p. 52).