Using Ballistocardiography to Perform Key Distribution in Wearable IoT Networks

by

Alexander W. Witt

A Thesis

Submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfillment of the requirements for the

Degree of Master of Science

in

Computer Science

by

May 2017

APPROVED:

Professor Krishna K. Venkatasubramanian, Major Thesis Advisor

---

Professor Yanhua Li, Thesis Reader

Professor Craig E. Wills, Head of Department

Abstract

A WIoT is a wireless network of low-power sensing nodes placed on the human body. While operating, these networks routinely collect physiological signals to send to offsite medical professionals for review. In this manner, these networks support a concept known as pervasive healthcare in which patients can be continuously monitored and treated remotely. Given that these networks are used to guide medical treatment and depend on transmitting sensitive data, it is important to ensure that the communication channel remains secure. Symmetric pairwise cryptography is a traditional scheme that can be used to provide such security. The scheme functions by sharing a cryptographic key between a pair of sensors. Once shared, the key can then be used by both parties to encrypt and decrypt all future messages. To configure a WIoT to support the use of symmetric pairwise cryptography a key distribution protocol is required. Schemes for pre-deployment are often used to perform this distribution. These schemes usually require inserting key information into WIoT devices before they can be used in the network. Unfortunately, this need to manually configure WIoT devices can decrease their usability. In this thesis we propose and evaluate an alternative approach to key distribution that uses physiological signals derived from accelerometer and gyroscope sensors. The evaluation of our approach indicates that more study is required to determine techniques that will enable ballistocardiography-derived physiological signals to provide secure key distribution.

Acknowledgements

First, I would like to thank Professor Krishna K. Venkatasubramanian for advising this research during the 2016 - 2017 academic year, frequently allocating time to hold discussion, and offering useful advice. I would also like to express my gratitude to Professor Yanhua Li for volunteering to be the reader of this thesis work.

Next, I would like to thank Professor Venkatasubramanian's PhD student, Hang Cai, for allocating time to meet and discussing plans for both collecting, processing, and analyzing the sensor data that was used in this research.

Finally, I would like to thank all of the individuals who participated in this research study. Without their help and willingness to volunteer their time, it would not have been possible to acquire the necessary raw data and perform the resulting analysis.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A WIoT is a wireless network of health sensors positioned on a human body. In this network these sensors regularly collect and transmit vital signs. As such, WIoT networks support a concept known as **pervasive healthcare**. In pervasive healthcare a WIoT sends vital sign data to an offsite medical professional. In so doing, patient health can be continuously monitored. This affords individualized plans for medical treatment and timely diagnoses [3]. For WIoT to be used in this clinical manner, at least two criteria need to be satisfied. The first criterion is that the **integrity** of the vital sign data should not be compromised. This is essential because these vital signs are used to guide treatment. The second criterion is that the **confidentiality** of the vital sign data should not be violated. This is essential due to laws that govern the privacy of patient data. If these requirements are not met, adversaries can view patient data and adversely affect patient safety. For example, an adversary within range of a WIoT could connect to the network with a properly configured transceiver. This would allow for the collection of communicated vital signs and the injection of fake data. Therefore, it is important to secure the **wireless communications** transpiring within a WIoT. This problem must be solved before these networks can come into widespread use.

In the domain of network security, cryptography is often used to provide secure channels for communication. Cryptography works by encoding information so that only autho-

rized endpoints can decode that data. The guarantees afforded by cryptography typically include confidentiality, integrity, authentication, and non-repudiation. Generally speaking, there exist two different types of crypto systems. The first type are symmetric crypto systems and the second type are asymmetric crypto systems. Symmetric crypto systems work by providing the same secret information to all communicating parties. This secret information is known as a cryptographic key. During operation that key is used as a mechanism for encrypting and decrypting the data to send. On the other hand, asymmetric crypto systems work by using something called a public key infrastructure (PKI). In an asymmetric crypto system every device has two different cryptographic keys. The first key is a private key that is only known to the device. The second key is a public key shared to all through the PKI. To communicate data in this crypto system, the information is encrypted with the public key of the destination. Once received, the destination decrypts that information using its private key.

In the context of WIoT, symmetric cryptography is often used [3]. Advantages in using this technique include shorter key size and the lack of a need to configure and maintain a PKI. Both points are important when considering the resource-limited nature of WIoT sensors. Specifically, these sensors run on battery power and have limited memory and computational ability. The only device that is more capable within these networks is the aggregation device that also serves as a gateway between the WIoT and a wide area network (WAN). This device is termed as the sink. To enable the use of symmetric cryptography, **a protocol for key distribution is required**. Some known protocols include probabilistic key distribution [8], master key based distribution [7], and Bluetooth pairing [6]. Unfortunately, none of these techniques for key distribution provide **usable security**. Namely, the use of pre-deployment in [8] and [7] requires each WIoT device to be manually loaded with the appropriate key information prior to use. On the other hand, the use of a Bluetooth pairing approach in [6] decreases usability by requiring user involvement for additional security properties. To enhance the usability of WIoT, it would be best if the network could perform key distribution automatically without user

involvement.

Given that WIoT devices are in contact with the body, **we consider using vital signs to perform key distribution**. The general strategy for this approach is to use the similarity in the synchronously-recorded physiological signals to help transfer a dynamically generated key. This would eliminate both the need for pre-deployment as well as the need for any user involvement. An existing solution that uses this approach is a protocol called **physiological signal based key agreement [3]**. Within that scheme a cryptographic primitive, known as a fuzzy vault, is used to hide the key information during transfer to the other endpoint. The similarity in the signals then helps that endpoint to unlock the vault and recovery the key. While depending on this scheme as a foundation, our approach differs by **using accelerometer and gyroscope sensors to derive the physiological signals**. We do not leverage the special sensing hardware present within the WIoT sensors. We believe this approach to be an improvement because the sink, which does not have specialized hardware, can now be incorporated into the key distribution process. If successful, this approach would allow for the entire WIoT to be configured to use symmetric crypto systems like AES in a **plug-n-play** manner.

Due to our use of physiological signal based key agreement, our evaluation consists of assessing how well our derived vital signs could satisfy the design guidelines enumerated in [3]. This included assessing the properties of **distinctiveness** and **temporal variance**. Both properties determine the degree to which an adversary can circumvent the physiological signal based key agreement scheme. Having sufficient distinctiveness means that vital signs from other individuals cannot be used to predict key values. Similarly, having sufficient temporal variance means that future vital signs cannot be used to predict key values. To perform our evaluation, we first developed a testbed to collect accelerometer and gyroscope data from a set of participants. The next step was to filter this raw data into two different signal types, **blood volume pulse (BVP)** and **ballistocardiography (BCG)**. Next, the physiological signal based key agreement scheme was followed for each signal type and aggregate statistics were computed through the use of three different algo-

rithms. This statistical information was then analyzed to determine whether our approach would be successful according to the physiological signal based key agreement criteria.

There are two contributions made in this thesis. The first contribution is the idea of using vital signs derived from gyroscope and accelerometer sensors to perform key distribution. The second contribution is an evaluation of that scheme according to the physiological signal based key agreement criteria. The two types of derived signals that we evaluate in particular are BVP and BCG. Unfortunately, the results from the evaluation clearly indicate that while key distribution can be performed, the guidelines for physiological signal based key agreement are not satisfied. This means that our approach is able to be attacked by adversaries who either acquire data from other individuals or capture data from the same individual at some different point in time.

1.1 Outline

The remainder of this thesis is formatted as follows. Chapter 2 contains information on our system model, threat model, and problem statement. Chapter 3 describes related work on key distribution. Chapter 4 provides background information on physiological signal based key agreement and ballistocardiography. Chapter 5 details our approach to key distribution. Chapter 6 provides information on our evaluation and results. Chapter 7 provides a discussion on potential sources of error. Finally, Chapter 8 summarizes this work and concludes the thesis.

Chapter 2

Models and Problem Statement

In this chapter we focus on describing the capabilities and structure of the WIoT systems considered in this research. Next, we describe our adversaries and their respective capabilities. This includes a statement of our assumptions. Finally, we conclude with a statement of the problem our thesis seeks to address.

2.1 System Model

A WIoT consists of a collection of sensing nodes placed on the body of an individual [2] (Figure 2.1). While able to have their nodes wired together, WIoTs are usually wireless in nature. During their operation, the sensing nodes in a WIoT routinely collect data on physiological or environmental signals. When collected by the sensing nodes, this data is then forwarded to an aggregation device. This aggregation device, known as the sink, is the only other type of device existing within the WIoT. Similar to the sensing nodes, the sink is typically placed on the body. In general, there are a few differences between the sensing nodes and the sink. The first difference is functionality. Specifically, **sensing nodes** are designed to perform simple tasks due to their limited power, computational ability, and storage. Conversely, the **sink** is able to perform sophisticated processing while acting as a gateway between the WIoT and a wide area network (WAN).

Related to functionality, another difference between sensing nodes and the sink are

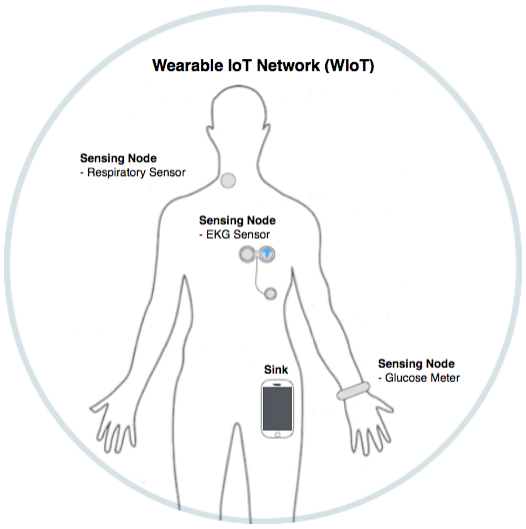

Figure 2.1: A WIoT network

the hardware components they contain. To perform its functionality, a typical sensing node consists of a battery, memory module, microprocessor, transceiver, sensing unit, and analog-to-digital converter (ADC) [2]. Similarly, the sink also contains a battery, transceiver, and ADC. However, the sink may not necessarily contain the same sensing unit as the sensing nodes. Link layer technologies used for communicating data between the sensing nodes and the sink include those existing within the industrial scientific and medical (ISM) band. Examples include, but are not limited to, Bluetooth, Zigbee, and WiFi [2]. To route communicated data across the WIoT, there exist at least three different topologies. The first is a single-hop topology in which every node is at most one-hop away from another node. The second is a multi-hop topology in which many nodes can be traversed. The third is a so-called star-topology in which the sink exists at the center of the network with every other node as a connected point.

Within the context of our work, we make a few assumptions about our WIoT. In particular, we assume that all of the devices are in contact with the body of the individual wearing the network. Another assumption that we make is that all devices contain the same sensing hardware. In our case, this means having an inertial measurement unit (IMU) containing an accelerometer and gyroscope. Finally, we also assumed all WIoT

communications to be wireless in nature. If this were not the case then the wired connection between nodes would already provide sufficient security.

2.2 Threat Model

Within our work we focus on developing a scheme for securing the wireless channel used for intra-WIoT communication. To understand what providing security would mean in this context, we first identify the capabilities of our potential adversaries. The insecure system, evaluated from a conceptual standpoint, was one in which information is openly exchanged between WIoT devices. This means that no cryptographic transformations are applied to the information in transit and that anyone using the same link-layer technology and a transceiver can have the potential to be disruptive. The two types of adversaries anticipated were active and passive. Active adversaries would focus on inserting or modifying information. **Passive adversaries** would focus on reading the wireless medium to acquire knowledge about the system or to record physiological data transmitted by the sensing nodes to the sink. The key concern associated with passive adversaries was the potential to violate the confidentiality of WIoT data. The concern for **active adversaries** was the potential to violate the integrity of WIoT data.

Specific attacks capable of being launched by active adversaries included the **injection** of new data, **spoofing**, the **modification** of data in transit, and the ability to **replay** old communications. The only attack capable of being launched by passive adversaries was **eavesdropping**. While these were the attacks forming the foundation for our threat model, it is important to identify threats we did not address. For instance, one critical aspect of WIoTs is that they can be used to continuously monitor patient health. This makes ensuring availability important. However, because we focus primarily on confidentiality and integrity, we do not address denial-of-service (DoS) or resource consumption attacks. Additionally, we do not consider the exploitation of the software or hardware in WIoT nodes. Consequently, physical attacks such as supply chain compromise or network infiltration at the sink were not a concern.

Further assumptions of ours include that we do not anticipate our adversaries to make use of side channels to indirectly acquire physiological data. Given our scheme for key distribution, adversaries might want to do this to enhance their chances of determining the shared key. Another assumption we make is that the wearer of the WIoT is not actively collaborating with the adversary. If this were the case, violating our scheme would be trivial. Finally, the last assumption is that no attacks will be directed between the sink and its connection to the WAN because that communication is protected by measures such as TLS.

2.3 Problem Statement

The task of this work is to **securely perform key distribution** for all devices participating within the confines of a WIoT. A secondary objective is to ensure that this process for distributing key information **does not require user interaction** and **can be completed automatically**. With WIoTs emerging as a technology to support pervasive healthcare, it is important that their data be kept confidential and unmodified. Basing plans for medical treatment on inaccurate information has the potential to adversely affect patient safety and well-being. Additionally, disclosing medical information without patient consent is illegal. In an attempt to provide WIoTs with a secure communication channel, we propose a scheme based on [3] that will use **derived physiological signals**. The benefit assumed here is that all devices will be able to be configured provided that they possess an accelerometer and gyroscope. To validate our approach, we evaluate two different design goals inherited from [3] called distinctiveness and temporal variance. Both design goals are meant to guarantee that an adversary cannot gain the ability to reliably guess keys based on additional information. This would include physiological data collected either from other individuals or from the same individual at some different point in time.

Chapter 3

Related Work

Existing schemes for key distribution in wireless sensor networks include the use of **pre-deployment** and the use of **Bluetooth pairing**. In work performed in [8] the authors describe a scheme for pre-deployment in which a ring of keys are inserted into each sensor prior to the use of the network. This ring, facilitates the use of pairwise symmetric cryptography if at least q of the keys in each ring for each sensor match. To reduce computational overhead the scheme reduces the number of these q keys that are used to produce a single shared key to some upper bound value of s. Because it is not always guaranteed that at least q keys match between pairs of sensors, this a probabilistic approach. In work performed in [7] the authors describe the setup of a body area network in which pre-deployment of a master key is used to ensure secure communication between all of the sensors. A survey conducted in [1] discusses the basic approach of manually inserting key information in sensor nodes. Additionally, [1] discusses distributing chains of keys from a random pool to sensors. This method is the predecessor to the scheme mentioned in [8]. Our proposed approach improves upon both schemes by dynamically generating keys and facilitating their distribution during network operation without any user involvement.

In work from [6] the authors discuss a scheme for using Bluetooth to pair groups of devices in a body area network. Additional security properties that the authors focus on developing include ensuring that the legitimacy of nodes in a formed group can be verified

through an out-of-band channel and allowing nodes to be added and removed from formed groups. The out-of-band channel used is a visual channel which requires devices in the network to blink LEDs to indicate their group membership. Upon this blinking the user can then know whether all nodes within a group are legitimate nodes belonging to that group. Our proposed approach does not focus on providing all of the security guarantees mentioned in that paper. Instead, our concerns are ensuring that key distribution is performed securely without any need for user involvement among pairs of devices. With respect to not requiring user involvement, our proposed approach is an improvement.

Chapter 4

Background Material

4.1 Physiological Signal Based Key Agreement

As mentioned previously, our proposed approach leverages a scheme for key distribution described in [3] called **physiological signal based key agreement**. Dissimilar to the schemes mentioned in [8] and [7], physiological signal based key agreement does not require any pre-deployment of key information. Instead, **keys can be dynamically generated** and the similarity in synchronously recorded physiological signals helps to perform the distribution. To distribute a pseudo-randomly generated key, physiological signal based key agreement operates in a total of seven phases. These include randomly generating a polynomial of a pre-determined order, synchronously collecting a physiological signal for a fixed duration, constructing an entity known as a vault, sending that vault over the wireless medium, reversing that vault to re-acquire the key information, confirming the correctness of the recovered key, and using the key in the context of a traditional crypto-system such as AES.

Since physiological signal based key agreement was developed to support pairwise symmetric key distribution, the setup occurs between two devices. The first device generates a key and securely distributes it to the second device. These two devices are respectively termed as the sender and the receiver. In the first phase, the sender uses a pseudo-random

number generator (PRNG) to produce each coefficient in a polynomial of a pre-determined order. When concatenated together as a binary string, the coefficients form an integer value representing the key to share. In the second phase, the sender and the receiver synchronously record the same type of physiological signal for the same duration at the same sampling rate. After these first two phases, a cryptographic primitive known as a **fuzzy vault** is then constructed by the sender. This construct is important in the physiological signal based key agreement scheme because it enables the secure exchange of the polynomial.

To construct the vault, the sender first examines the physiological signal that it had recorded. Specifically, the sender takes that signal and divides it into five equally-sized and consecutive windows having fifty percent overlap. Next, these windows of time-series data are then transformed into frequency-domain data by applying a fast-fourier-transform (FFT). Once in the frequency domain, the first 32 data points in each window are searched for local peaks using a local maxima detector. When finding these peaks, numerical values called **features** are formed. To construct each feature, the index and amplitude value of that peak are concatenated together into a single binary string consisting of 13 bits. The first 8 bits consist of the amplitude value of the observed peak. The next 5 bits consist of the index value at which the peak was observed. After generating these features, the next step is to transpose them onto the polynomial.

To transpose these features, each unique feature was provided as input to the polynomial. The result was a collection of two-dimensional **legitimate points**. The horizontal value of each point was the numerical value of the feature, while the vertical value was the evaluation of that feature when provided to the polynomial. After producing these legitimate points, the next step of vault production in physiological signal based key agreement is to pseudo-randomly generate a much larger set of distraction points. These points are termed **chaff** and are generated so that they do not overlap with any existing legitimate points or chaff points. Once produced, the chaff points are then permuted with the legitimate points to form a set known as the vault (Figure 4.1). This vault is then

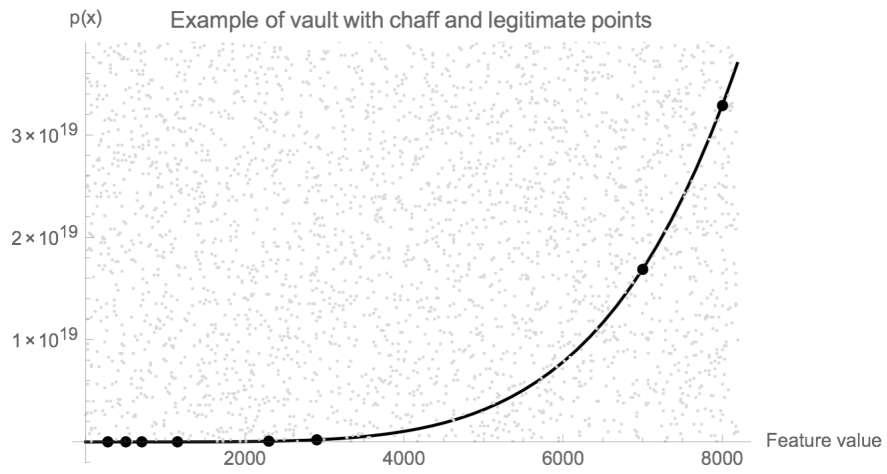

Figure 4.1: A vault according to the physiological signal based key agreement scheme

communicated from the sender to the receiver in the next phase of physiological signal based key agreement.

To send the vault and ensure the recovery of the key, the sender constructs a message. This message consists of the ID of the sender, the ID of the receiver, the vault, a nonce value, and a **message authentication code (MAC)** formed from the key and an OR operation on the vault, nonce, and sender ID. In this message the IDs are used for routing, the vault is used to support key recovery, the nonce is used to prevent replay, and the MAC is used to confirm key recovery. When sent to the receiver, the vault is then extracted and the process of unlocking the vault is initiated. The first step taken in the unlocking process is for the receiver to acquire the features from its recorded version of the physiological signal. Next, the intersection of these features and the horizontal component of the vault points is found. This forms a set of two-dimensional points believed to be legitimate points. Assuming that there is at least one more than the order of the polynomial such points the receiver can then start the recovery of the polynomial.

To recover the polynomial in the physiological signal based key agreement scheme, a technique known as **Lagrangian interpolation** is applied (Equation 4.1). This technique works by taking the order plus one points and using one of those points as a test point. A

polynomial of the appropriate order that is capable of linking these points is then formed. Once re-acquired, the second to last phase of physiological signal based key agreement is to confirm whether the recovered polynomial is the same as the original polynomial. To perform this check, the receiver recomputes the MAC that it had been sent. If the MAC that it computes matches the MAC that it had been sent, the receiver knows it has correctly recovered the key. If this is the case, the last step in physiological signal based key agreement is to confirm this recovery with the sender. To do this the receiver sends a message to the sender containing a different MAC. This MAC is formed from the recovered key and an OR operation on the nonce, sender ID, and receiver ID. If the sender can re-compute this MAC with its key then AES can begin to be used in the WIoT.

$$p(x) = \sum_{j=0}^{v} y_j d_j(x) \quad , \quad d_j(x) = \prod_{i \neq j, i=0}^{i=v} \frac{x - x_i}{x_j - x_i} \tag{4.1}$$

4.2 Ballistocardiography

Apart from physiological signal based key agreement, we also leverage two techniques for deriving ballistocardiography signals. Ballistocardiography signals are related to **subtle movements of the body caused by ejection of blood from the heart muscle as it beats**. When the human body is still, work in [5] and [6] has shown that gyroscope and accelerometer sensors can be used to detect these movements. By naturally detecting acceleration and rotation, accelerometers and gyroscopes capture this movement data in the form of meters/second^2 and radians/second, respectively. Upon removing noise from gyroscope and accelerometer data these body movements should appear.

Chapter 5

Approach

In this chapter we detail all of the steps involved in our proposed approach to performing key distribution in WIoTs. As mentioned earlier, the general idea for our approach is to use accelerometer and gyroscope data to derive physiological signals. Those signals are then used in the context of a scheme known as physiological signal based key agreement to perform key distribution. At the abstract level, these are the steps involved. More concretely, there are four steps. The first consists of collecting the raw sensor data. The second consists of deriving physiological signals from the raw data. The third consists of extracting features from the derived signals. The fourth consists of using the features in accordance with the physiological signal based key agreement protocol. Each of these steps is described further in the sections that follow.

5.1 Data Collection

Within our approach, the process of data collection is an activity performed synchronously between two devices in the WIoT. These devices form a pair wanting to communicate with one another (Figure 5.1). For both devices it is assumed that they have accelerometer and gyroscope sensors. Initiating data collection occurs when one of the devices in the pair sends a future timestamp to the other device. Afterward, both devices wait for that future timestamp to occur in real time as opposed to system time. Upon the future

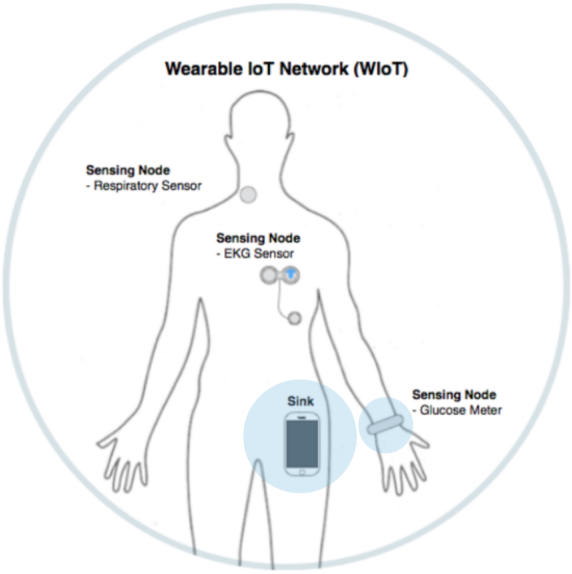

Figure 5.1: A pair of devices wanting to communicate in a WIoT

timestamp, both devices then begin to simultaneously collect triaxial accelerometer and triaxial gyroscope data from their own sensors at the same sampling rate for the same timespan. The sampling rate used was 100 Hz and the timespan was 7.68 seconds. The result of this collection are six streams of data per device. These components are for the X, Y, and Z axes of each of the two sensors. Measurement units for each of the sensors across both devices were assumed to be the same. Gyroscope values were recorded in radians/second while accelerometer values were recorded in meters/second^2. Finally, all sensors were assumed to be properly calibrated prior to the sampling of their readings. All data collection was performed ethically by having participants review and sign an approved consent form from the institutional review board.

5.2 BCG Generation

After collecting the raw accelerometer and gyroscope data, the next step was to use that data to derive a physiological signal for each device in the pair. In our approach, we evaluate two different filtering techniques to arrive at those signals. Specifically, we leverage

work from [5] and [4] to derive blood-volume-pulse (BVP) and ballistocardiography (BCG) signals. In both cases, these signals relate to subtle motion caused by the expansion and contraction of the heart muscle. Through sequences of signal processing techniques described in [5] and [4], the six axes of accelerometer and gyroscope data from each device are transformed into a single time-series signal. Applying the technique from [5] generates a BVP signal while applying the technique from [4] generates a BCG signal.

To derive a BCG signal from the six streams of data for each device (Figure 5.2), four steps were required according to [4]. In the first step of the BCG derivation, each of the six streams of data were normalized so that they would have zero mean and unit variance (Figure 5.3). This meant that each stream would first have its mean subtracted from all of its data values and would then have all of those values divided by its standard deviation. This was done to reduce the influence that different scales might have when filtering the data in later steps. Next, an averaging filter of 35 samples was subtracted from each normalized stream to remove the presence of slow motions due to other body signals [4] (Figure 5.4). Following this step, a Butterworth bandpass filter with cut off frequencies of 4 Hz and 11 Hz and order 4 was applied to each normalized and detrended stream of data (Figure 5.5). This was done to isolate the BCG waveform for each stream [4]. Finally, the stream with the highest amplitude response in the frequency domain was selected (Figure 5.6).

To derive a BVP signal for each device only the three streams of data from the gyroscope sensor were required (Figure 5.7). According to [5] the process involved four steps. The first step was to subtract an averaging filter of three samples from each of the three streams of data (Figure 5.8). The second step was to apply a bandpass Butterworth filter with cutoff frequencies of 10 Hz and 13 Hz and order 4 to each of the three streams of data (Figure 5.9). The third step was to combine the three data streams into one stream by taking the square root of the sum of the squared components from each stream (Figure 5.10). The last step was to apply a bandpass Butterworth filter to the single stream of data with cutoff frequencies of 0.75 Hz and 2.5 Hz and order 2 (Figure 5.11).

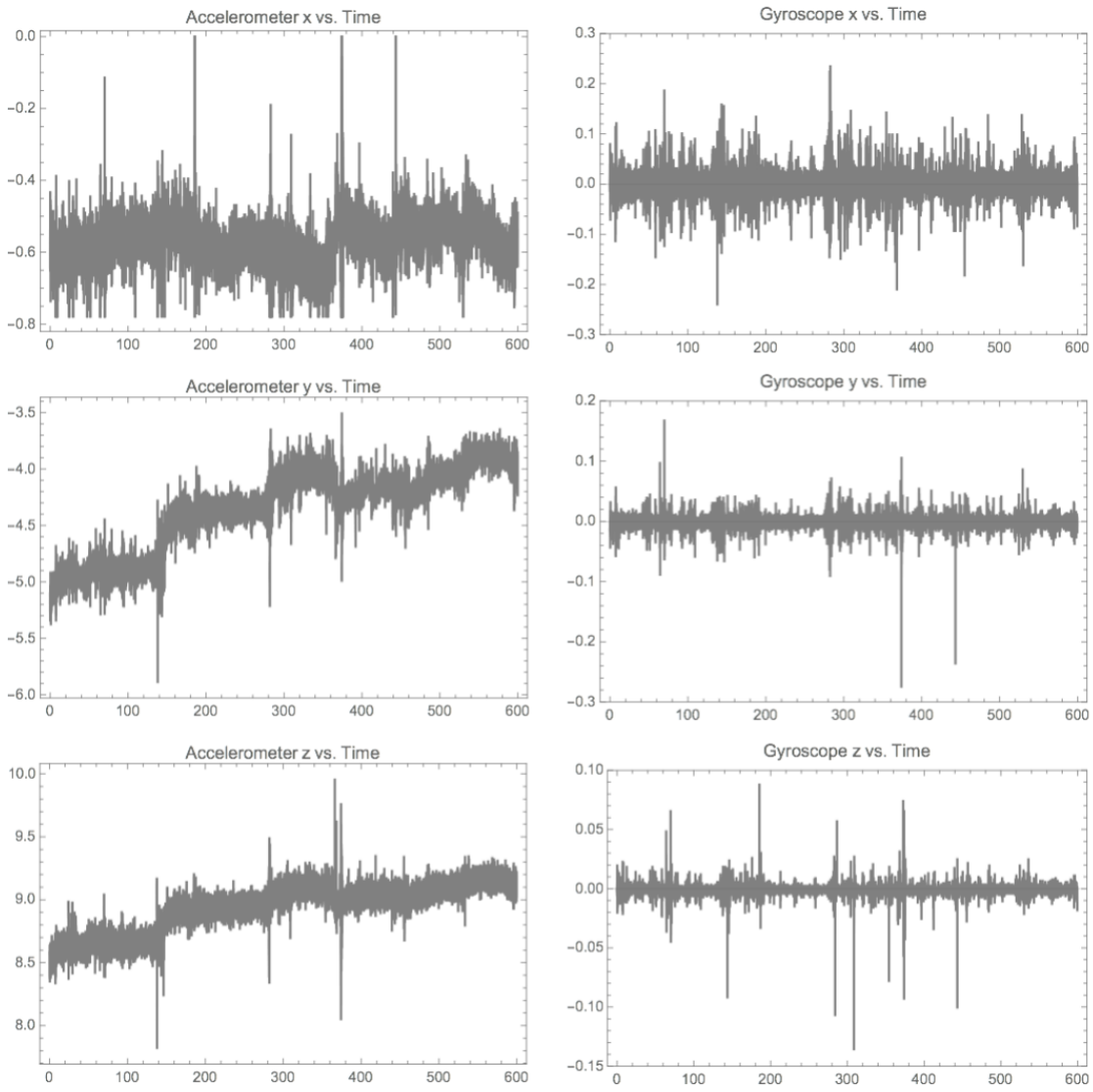

Figure 5.2: The six axes of raw accelerometer and gyroscope data from a WIoT device (BCG)

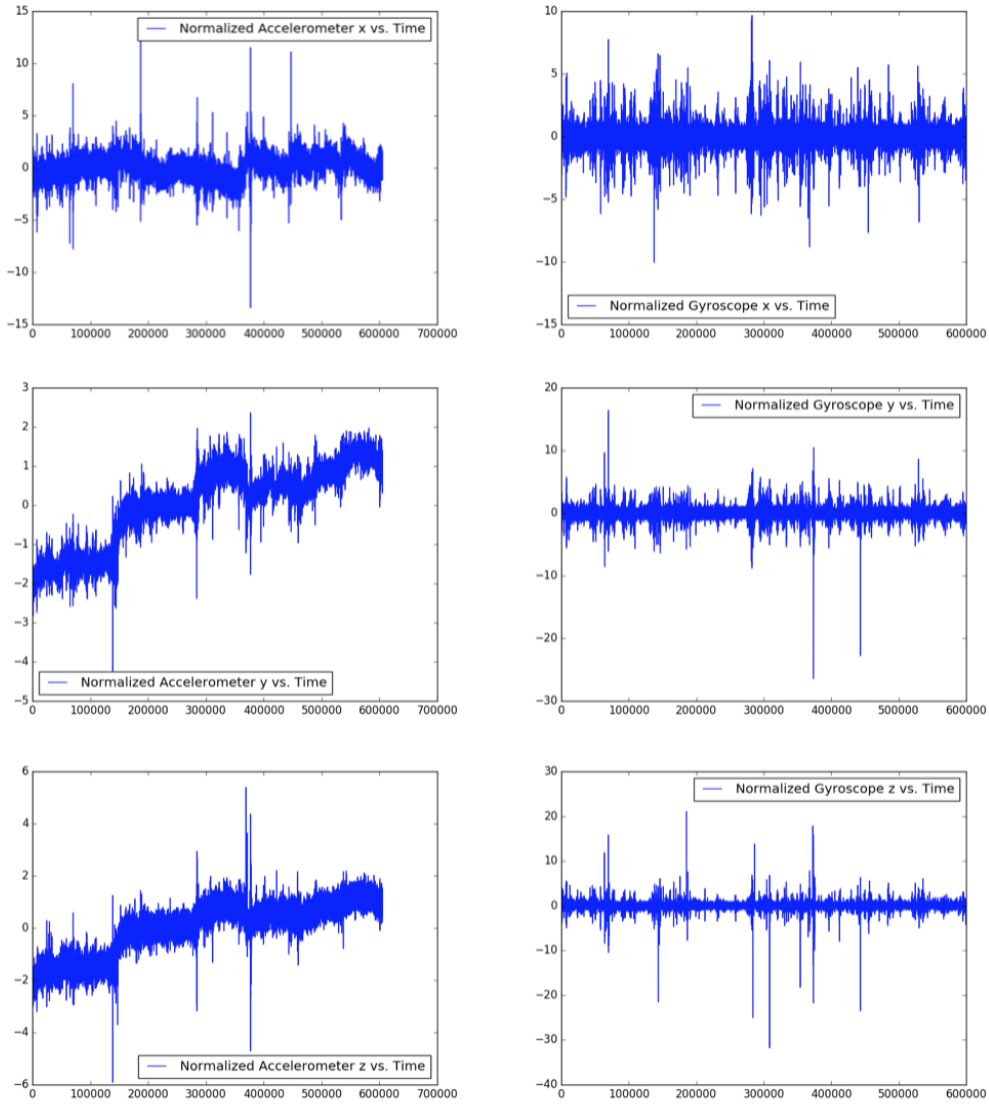

Figure 5.3: The six axes of normalized accelerometer and gyroscope data from a WIoT device (BCG)

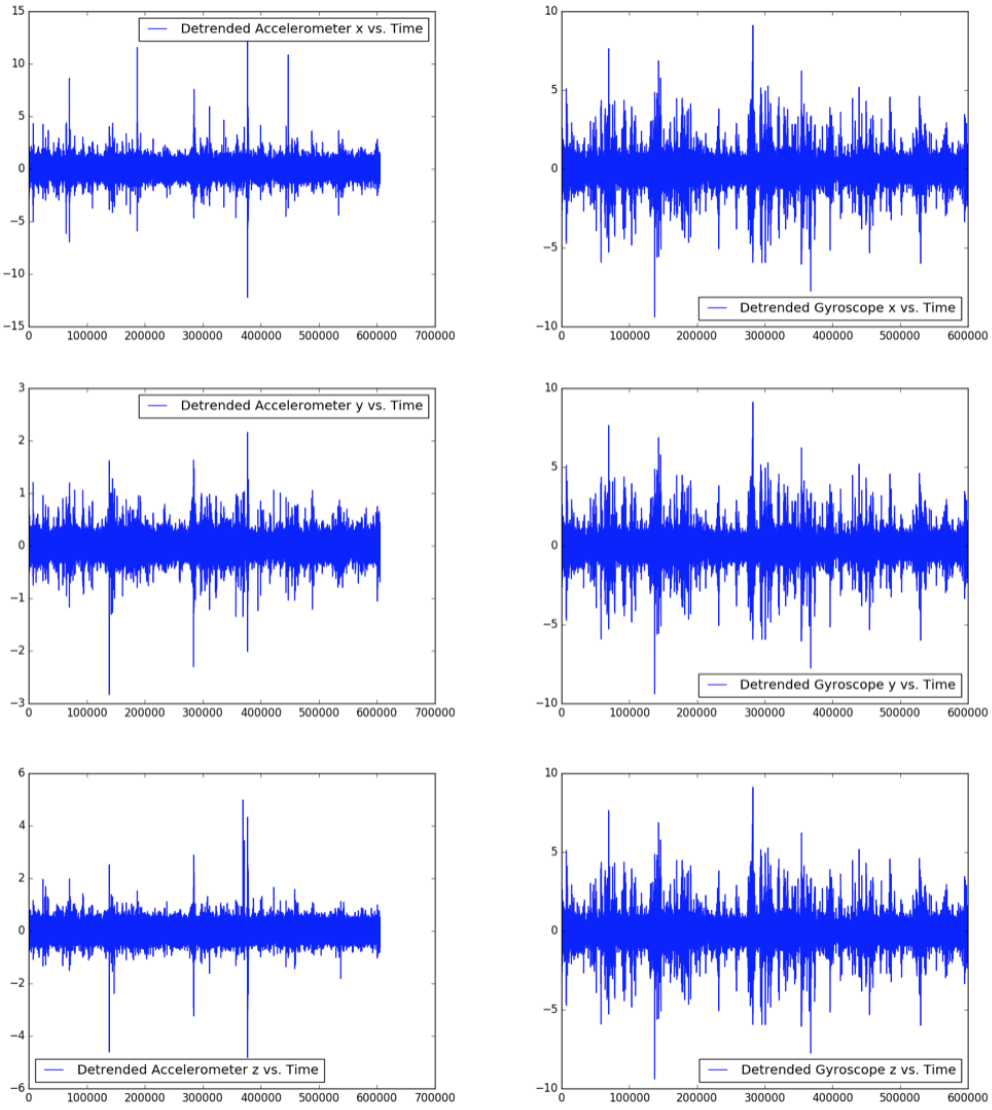

Figure 5.4: The six axes of detrended accelerometer and gyroscope data from a WIoT device (BCG)

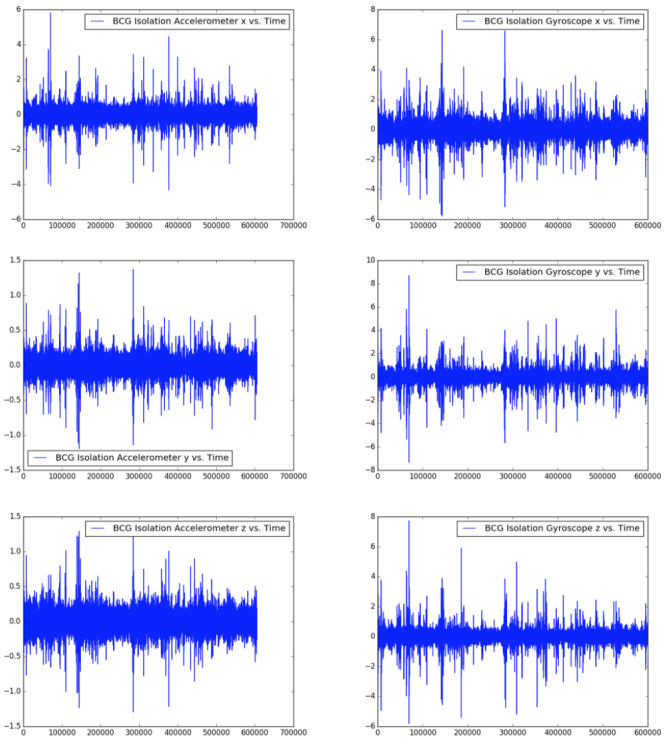

Figure 5.5: The six axes of BCG filtered accelerometer and gyroscope data from a WIoT device (BCG)

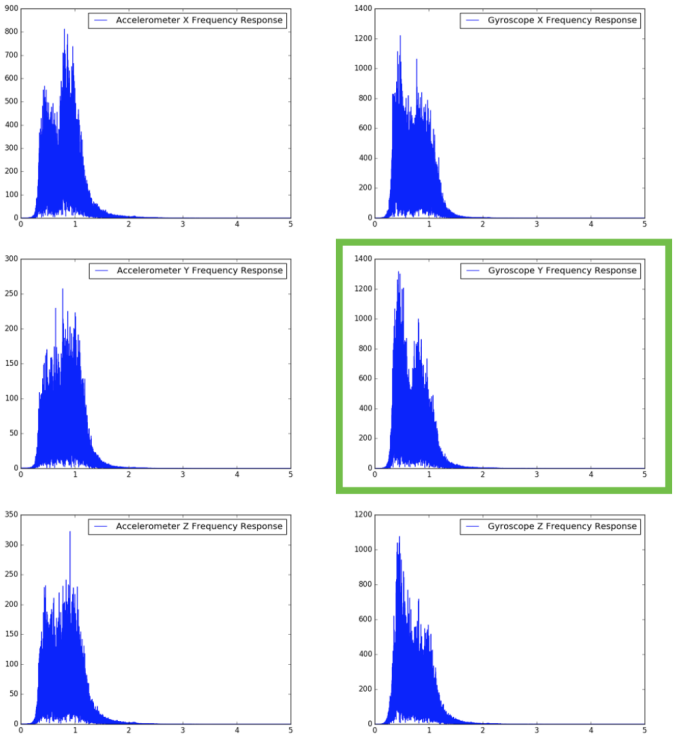

Figure 5.6: Selection of the signal with the best frequency response from a WIoT device (BCG)

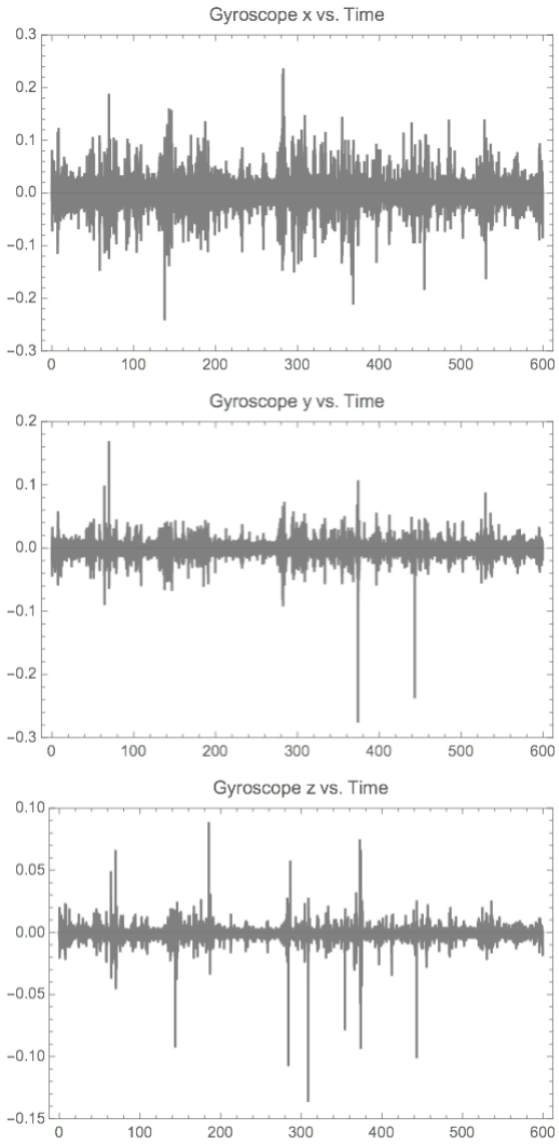

Figure 5.7: The three axes of raw gyroscope data from a WIoT device (BVP)

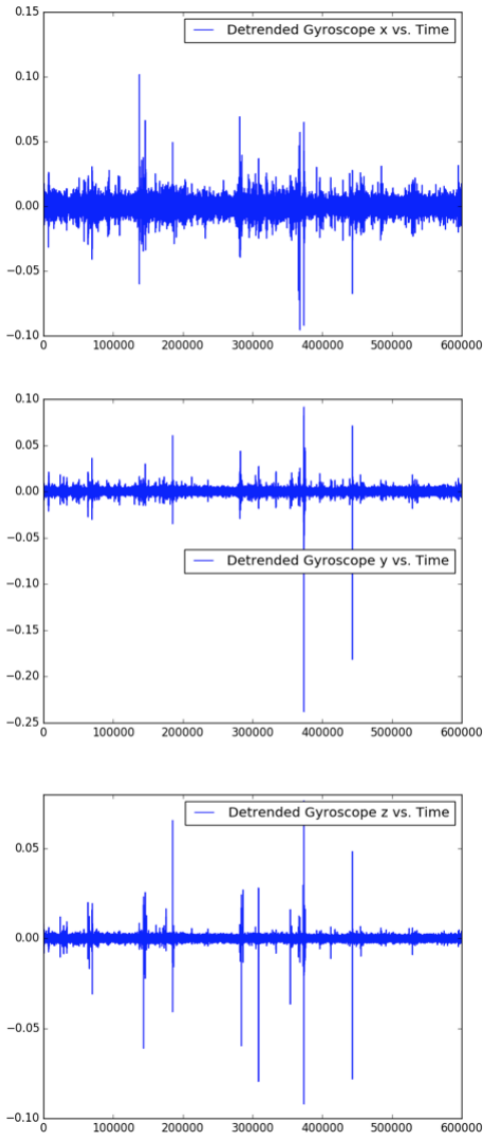

Figure 5.8: The three axes of detrended gyroscope data from a WIoT device (BVP)

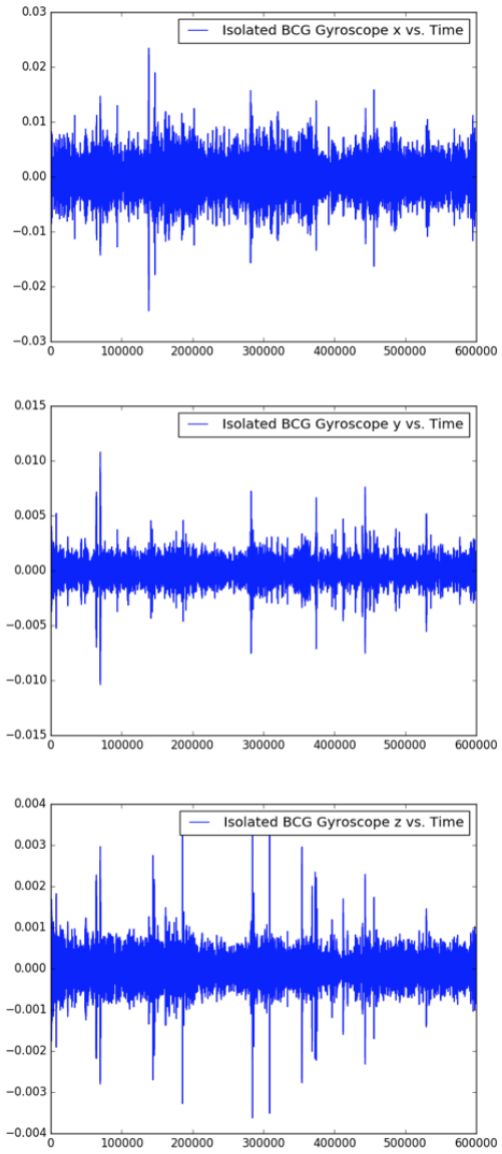

Figure 5.9: The three axes of BCG filtered gyroscope data from a WIoT device (BVP)

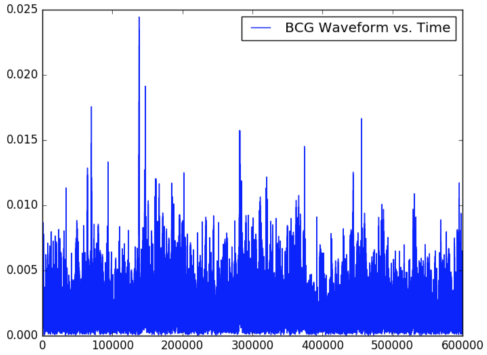

Figure 5.10: The L2 norm of the three axes of gyroscope data from a WIoT device (BVP)

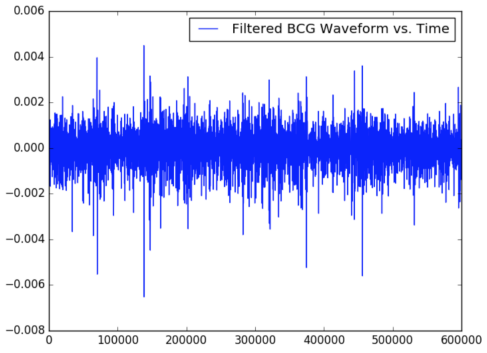

Figure 5.11: The BVP waveform from a WIoT device (BVP)

5.3 Feature Extraction

In the physiological signal based key agreement scheme described in [3] features are numerical values used for assessing the similarity of two physiological signals. Features are critical because without an ability to assess the similarity of two physiological signals, the physiological signal based key agreement scheme would not be able to perform secure key distribution. To mirror physiological signal based key agreement, we first divide our time-series physiological signals into 5 equally-sized and consecutive windows with 50 percent overlap. In the context of our signals, which consisted of 768 time-series data points, this meant producing windows on the following index-described intervals: [0, 256), [128, 384), [256, 512), [384, 640), [512, 768). After dividing our signals into these windows, we then perform FFT on each window. The result was a collection of 5 windows consisting of 128 frequency-domain data points. Specifically, these data points were amplitude values. Next, we examined each window for local peaks. This was done by sliding a window of size 32 to a horizontal offset within the window. This offset value was determined by a method that will be described later. Upon proper positioning at the offset, the sub-window of size 32 in each window was then searched by a local peak detector. The index (i.e., 0 - 31) and value for each local peak were then concatenated together in the form of a binary string. The result for each peak was a 13 bit integer value called a feature. The first 8 bits consisted of the amplitude value of the observed peak, and the next 5 bits consisted of the index value of the observed peak. To ensure that all binary strings used were integers and not floats, the amplitude values were scaled by a constant factor and truncated. In the case of our BCG signals, this factor was a factor of 1. In the case of our BVP signals this was a factor of 1000. To ensure that this result would fit within the designated 8 bits the remainder of division by 256 was taken.

To determine the offset at which to position the size 32 windows within our 5 size 128 windows, we evaluated all of the 96 possible placements within the size 128 windows. This evaluation consisted of assessing the number of instances in which the number feature matches for signals from the same users in our dataset was greater than the number of

feature matches between each user and all others in our dataset. For our BVP signals, this offset was determined to be 79 while for our BCG signals this offset was determined to be 41.

5.4 Physiological Signal Based Key Agreement

After extracting features from our physiological signals, we then use those features to assess how well the signals perform with respect to physiological signal based key agreement. This includes the evaluation of a property known as distinctiveness. This property was assessed by acquiring aggregate statistics on feature matches between the two signals obtained from the same users and by acquiring aggregate statistics on feature matches between signals from each user and all others. These aggregate statistics were then compared. If there were significantly less distinct feature matches between users than there were for the same user there was sufficient distinctiveness. Otherwise, there was not sufficient distinctiveness. The other property assessed was temporal variance. To assess this property multiple signals from the same user were recorded at different time offsets and feature matches between each offset signal were recorded. Aggregate statistics on the number of feature matches for each time offset for each user were recorded in order to construct a plot of feature matches over time. If the resulting curves did not quickly decrease to have 0 matching features then there was not sufficient temporal variance.

Chapter 6

Performance Results

This thesis recruited a total of 18 participants. To ensure that sufficient data was collected for analysis, 10 minutes of gyroscope and accelerometer data were recorded per trial. For each participant only one trial was performed. After collecting this triaxial accelerometer and gyroscope data from our participants, a filtering procedure was applied to each 10 minute sample. This filtering procedure was used to convert each sample into either a BCG or BVP signal. Next, these BVP or BCG signals were each divided into 74 segments consisting of 768 time-series data points. These segments were then further divided into 5 windows with 50 percent overlap. FFT was then applied to each window in each segment. Finally, algorithms were applied to the segments and their frequency domain windows to assess suitability of the BCG or BVP signals for key distribution. Overall, there were three algorithms for producing the aggregate statistics used in our analysis. These algorithms evaluated properties such as the degree to which the signals matched for each participant, the degree to which the signals were different between the participants, and the degree to which the signals varied over time.

6.1 Participants and Design

In order to acquire sufficient data for analysis, we collected 10 minutes of data per participant at a sampling rate of 100 Hz. In total, this amounted to 1332 segments. As previously

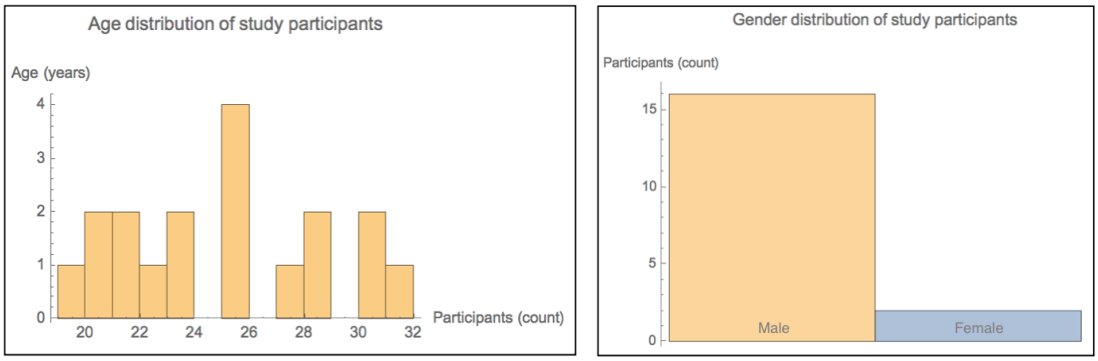

Figure 6.1: Histograms for sample population characteristics

mentioned, we recruited a total of 18 participants for the study. This population was randomly sampled from the larger population of undergraduate and graduate students in the computer science department at WPI. Recruitment in this context consisted largely of word-of-mouth advertisement and the willingness of individuals to participate when asked. With regard to the characteristics of the sample population, there were 16 males and 2 females. The ages of the sample population ranged from 19 to 31 with an average age of 24.6 and a standard deviation of 3.7 (Figure 6.1). Half of the sample population had their data collected in the student commons and the other half had their data collected in the B17 lab.

6.2 Apparatus and Materials

Participants whom we recruited were asked to wear two LG Urbane W150 smartwatches (one on each wrist) while accelerometer and gyroscope data were collected during a 10 minute trial. These smartwatches were used as analogue sensing nodes in a WIoT. Having limited battery power, limited processing capability, and limited memory along with the ability to communicate wirelessly through WiFi, these devices were regarded as suitable sensing nodes. During collection each smartwatch simultaneously collected accelerometer and gyroscope data from its physical sensors. According to information retrieved from use of the Android Sensors API, the gyroscope and accelerometer sensors are those

present within an InvenSense MPU6515 chip. The accelerometer and gyroscope were automatically calibrated by using the calibrated form of the sensor available through the Android Sensor API. The resolution of the gyroscope was 0.0010681152 radians/second with a range from -34.906586 radians/second to 34.906586 radians/second. The resolution of the accelerometer was 0.0005950928 meters/second^2 with a range from -19.613297 meters/second^2 to 19.613297 meters/second^2.

6.3 Reducing Noise

To reduce sources of noise, a few measures were take in the design of our study. First, it was ensured that none of the participants in our study had engaged in **physical exercise** prior to experimentation. This was done because an increased heart rate typically results in more frequent contractions and expansions of the heart. This increased frequency can result in differently shaped BCG and BVP signals. This is due to blood passing more frequently under the gyroscope and accelerometer sensors, resulting in more frequent subtle movement. Therefore, to make sure that our BCG and BVP signals were evaluated fairly when assessing their suitability for key distribution, they were collected from participants with a resting heart rate. Another measure taken was to ensure that participants did not make any **voluntary movement** while we collected their data. Finally, participants were also advised not to engage in **conversation** during data collection and to sit in a fixed chair with their arms resting on a sturdy desk. Preventing conversation was done to eliminate the influence of any vibrations resulting from speech. Maintaining the same **posture** across participants during data collection was done for consistency.

6.4 Procedure for Data Collection

The study procedure was performed in the following way: First the investigator prepared the testbed apparatus for data collection. This involved powering on both smartwatches, connecting both smartwatches to a wireless basestation, launching the Android applica-

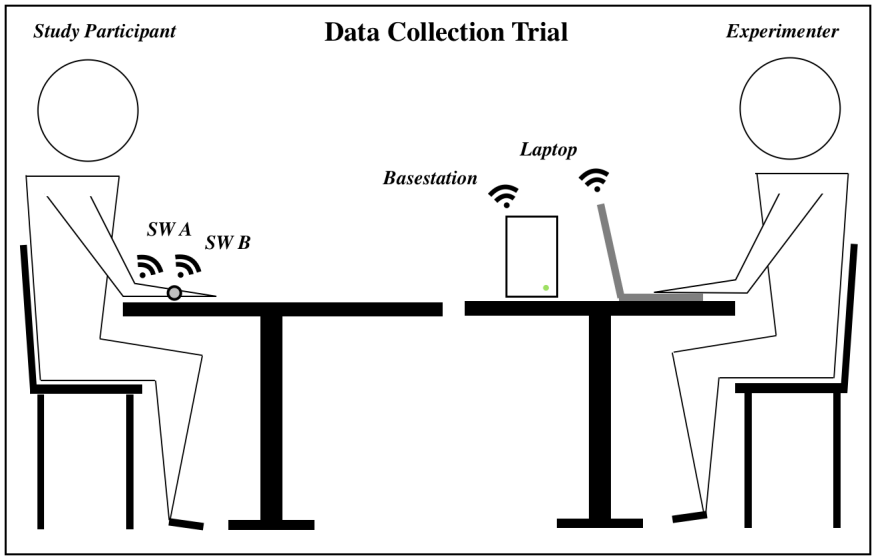

Figure 6.2: Testbed for data collection

tion for data collection on both smartwatches, and launching two data collection servers on a laptop computer connected to the same basestation. Following this setup phase, participants were then asked to read and sign the consent form that had been approved by the institutional review board. Next, participants securely fastened one of the two **smartwatches** to each of their wrists. If not securely fastened by adjustment of the strap, participants were asked to slide the smartwatches up their forearms until they were securely in contact with their skin. Once the participant was comfortable, he or she was asked to sit in a fixed chair with their forearms resting on a sturdy desk. Finally, the investigator initiated the data collection sequence by providing a start command to one of the servers running on the laptop. The participant then sat still for 10 minutes while their data was collected and streamed to the laptop for later use.

As per the description of the study outlined in the consent form, participants were allowed to opt-out of the study at any time if they felt uncomfortable. In this case, the data of that participant was removed since it would not provide a full 10 minutes of continuously collected data. The data collection apparatus can be seen in Figure 6.2.

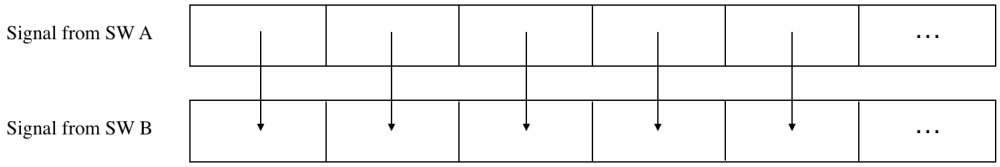

Figure 6.3: Algorithm for finding matches between two signals from the same participant

6.5 Analysis Algorithms

After applying the filtering techniques mentioned in section 6, the next step was to evaluate the derived BVP and BCG signals with respect to their ability to be used successfully in the physiological signal based key agreement scheme. To perform this evaluation three different algorithms were developed to return aggregate statistics capable of indicating whether the signals would have sufficient temporal variance and distinctiveness. Prior to executing these algorithms, each 10 minute signal was divided into 74 segments consisting of 768 data points. Next each of those segments was divided into five 50 percent overlapping windows and FFT was performed on each window. All of the frequency-domain data for each window of each segment for a signal from a participant was then written out in order to a CSV file. This allowed the segment data for either of a given participant's two signals to quickly be retrieved while the algorithms ran.

The first algorithm developed was one in which the two signals synchronously recorded from a participant were compared. In particular, the corresponding segments between a participant's two signals were each assessed for the number of features that they shared (Figure 6.3). After iterating through all 74 segments, the average number of feature matches for a user was then computed. Once this process of evaluation was completed, the average number of matching features for each user was then determined. In the context of the physiological signal based key agreement scheme, this information along with the average number of features shared between a given user and all other users helped to determine whether a suitable polynomial order existed.

The second algorithm developed was for finding the average number of feature matches

between the derived signals of a given participant and those of all other participants. The was done by comparing every segment from the two signals of a given participant to all other segments from all other participants. The average of the resulting sum of matches was then computed in each case. An illustration of the algorithm is shown below in Figure 6.3.

The third algorithm developed was for assessing temporal variance. This assessment was performed by computing the number of matches between the segments in a signal as the number of segments between them increased. After computing these offset matches for every segment in each of the two signals for a participant the average number of matches for each offset was able to be computed. The result was a collection of averages that could be drawn on a graph for each participant. In the graph, the number of separating segments was indicated along the horizontal axis and the number of matches was recorded along the vertical axis. By representing the results of the algorithm in this visual manner, the degree to which the number of feature matches would be affected by a given time offset could be observed. An illustration of this algorithm for temporal variance is shown in Figure 6.4.

6.6 Evaluation Metrics

This section describes the metrics used in our evaluation of our BVP and BCG signals for distinctiveness and temporal variance. Specifically, when evaluating distinctiveness we use the mean, mode, and maximum number of feature matches as our aggregate statistics. The mean is used to provide a measure of central tendency for the distributions of our feature matches across users. Namely, our two distributions consist of feature matches for the same users and between a given user and all others, respectively. The mode is used to provide an indication of what the most common number of feature matches tended to be within each distribution. The maximum was used to provide an upper bound on the number of feature matches within each distribution. These metrics were indicative of sufficient distinctiveness if all aggregate statistics for feature matches for the same users

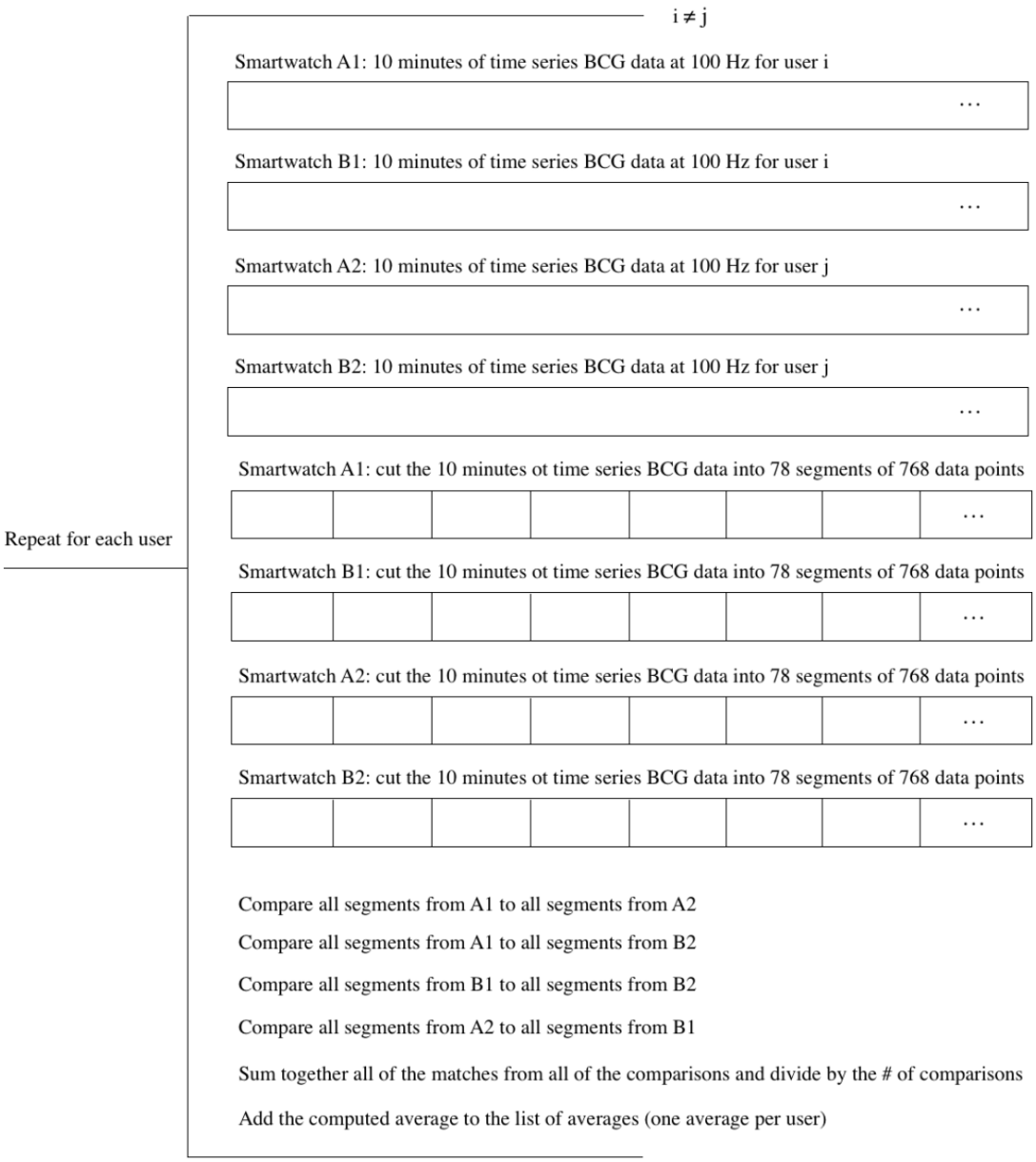

Figure 6.4: Algorithm for finding signal matches across participants

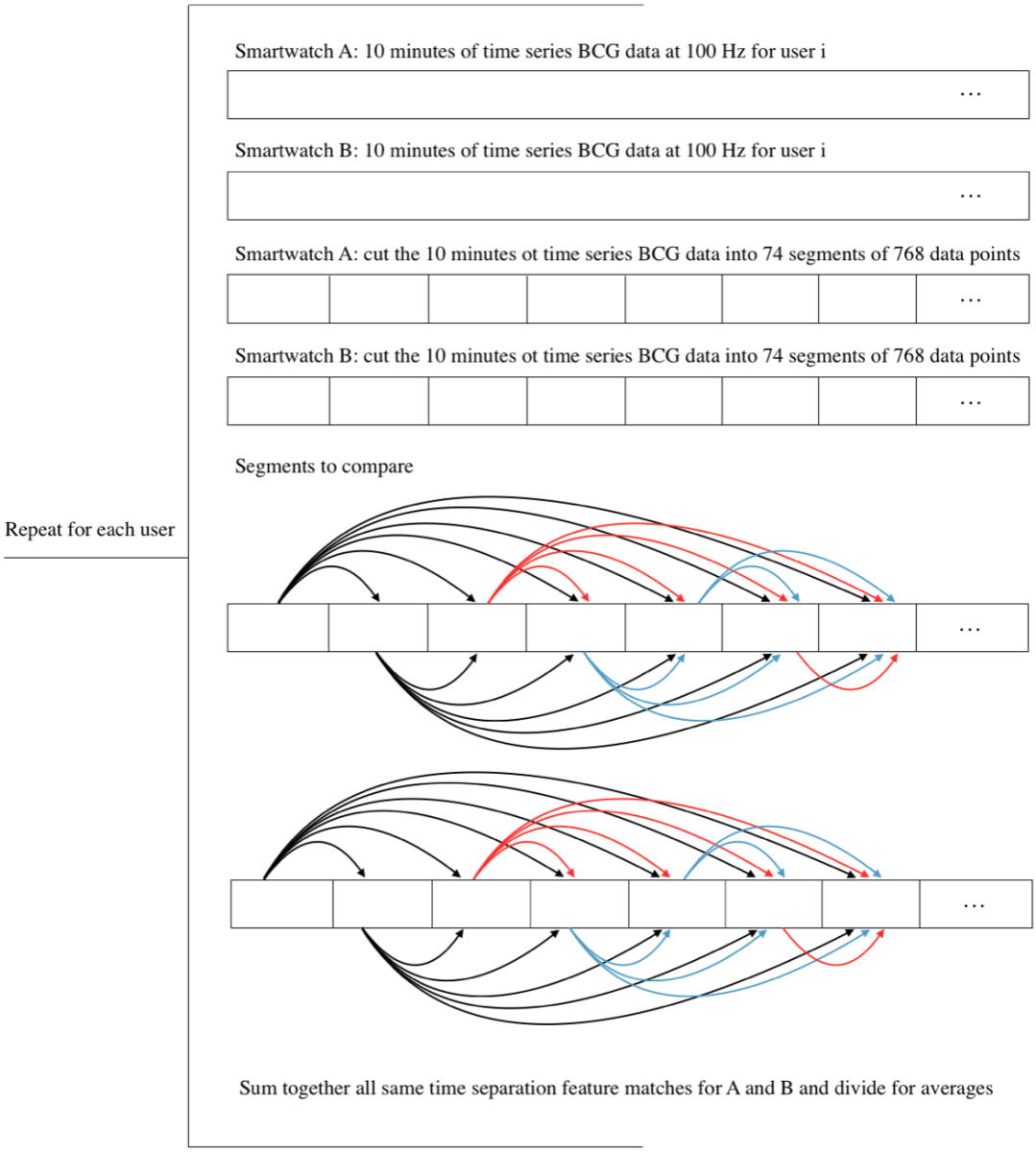

Figure 6.5: Algorithm for finding signal matches for the same participant over time

were greater than those for the number of feature matches between a given user and all others.

To evaluate temporal variance only the mean number of feature matches for each time offset for a given user was used. In the majority of cases the mean tended to accurately represent the center of the distribution of feature matches for each time offset. Since the curves for the mean number of feature matches over time were plotted for each user, visual inspection was used to assess whether sufficient temporal variance existed. This was done by observing how long it would take for a significant decline in the number of feature matches to occur. A significant decline would mean a drop to roughly 0 feature matches on average.

6.7 Evaluation

To perform an evaluation of our approach, we focus on assessing how well our derived BCG and BVP signals perform with respect to the design guidelines described in physiological signal based key agreement [3]. These guidelines were that the derived signals should have sufficient distinctiveness and temporal variance. Sufficient distinctiveness means that acquiring signal data from other individuals cannot help to predict the features of a given individual. Sufficient temporal variance means that acquiring signal data from the same individual at some different point in time cannot help to predict features for that individual. While we do evaluate each of our derived signals separately with respect to this criteria, we also perform a comparative analysis. Ultimately, the results indicate that while BVP performed slightly better than BCG for distinctiveness and temporal variance, both signals were inadequate for key distribution.

To evaluate distinctiveness for our derived BCG and BVP signals, we examined statistics computed over the sample population and over the two sub-populations within that population. The statistical measures that we used in each case were the mean, mode, and maximum number of feature matches between and for the same participants. As shown in the distributions of Figures 6.6 and 6.7 and as summarized in Table 6.1, the difference

Feature matches same (Mean, Mode, Max)	Feature matches different (Mean, Mode, Max)
18.6584, 19, 28	18.9826, 20, 43

Table 6.1: Evaluating the distinctiveness of derived BCG signals overall

between the mean number of features matches for the same participant and the mean number of features matches between participants for BCG signals was 0.3242 matches. Given that only an integer value can represent the order of a candidate polynomial in physiological signal based key agreement, this meant that no polynomial order could be formed from the mean. In Table 6.1, the mode for BCG did not perform any better. In fact, it performed worse because it indicated that more features tended to match between individuals than for the same individual. Specifically, the most common number of feature matches for the same individual was observed to be 19 while the most common number of feature matches between individuals was observed to be 20. Finally, the maximum in Table 6.1 indicated that the largest number of matching features between individuals was much greater than the largest number of matching features for the same individual. Specifically, the maximum number of BCG feature matches for the same individual was 28 while the maximum number of BCG feature matches between individuals was 43.

The numerical results for the distinctiveness of our derived BCG signals was not any better when considering the shape of the distributions shown in Figures 6.6 and 6.7. The shape of these distributions is very similar in the sense that both are left-skewed and have their shape positioned to cover roughly the same values. The number of occurrences can be ignored when comparing these distributions because that depended on the algorithms used for acquiring the aggregate statistics. Naturally, more comparisons are needed to find the average number of feature matches between individuals, resulting in more occurrences.

Analysis of the distinctiveness of derived BCG signals over each of the two sub-populations showed similar results. For the B17 lab sub-population, the mean and mode

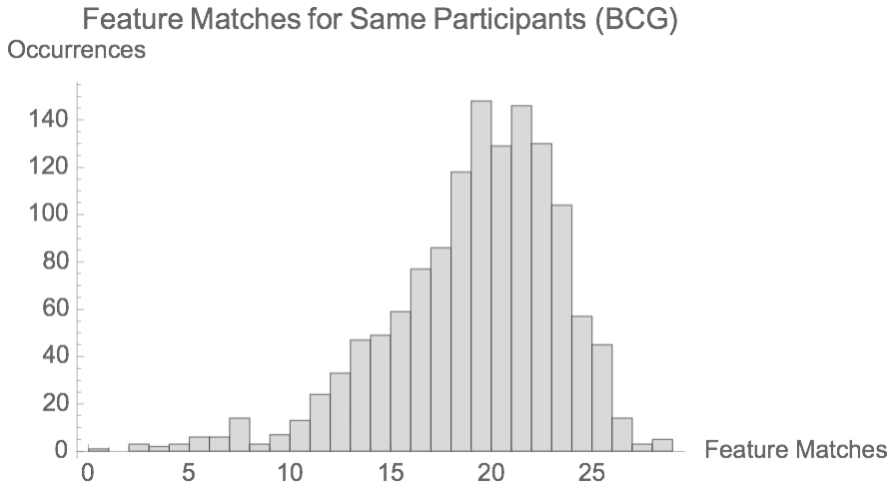

Figure 6.6: Histogram of BCG feature matches for same participant (sample population)

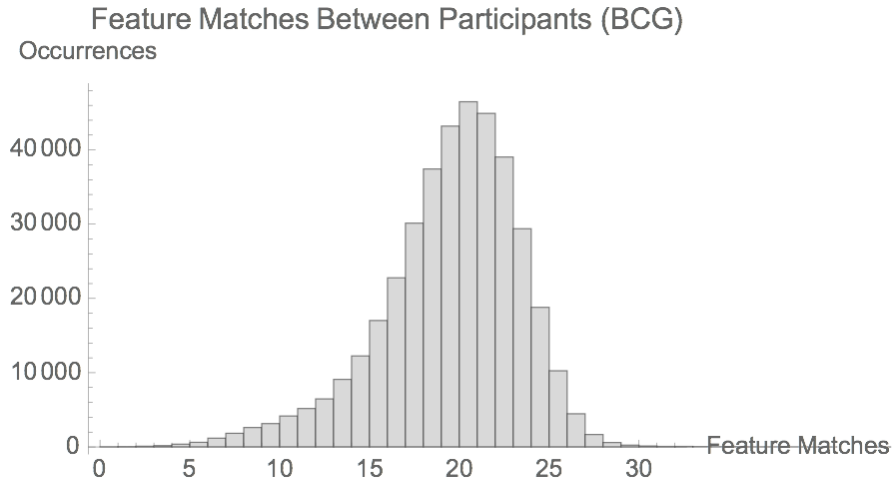

Figure 6.7: Histogram of BCG feature matches between participants (sample population)

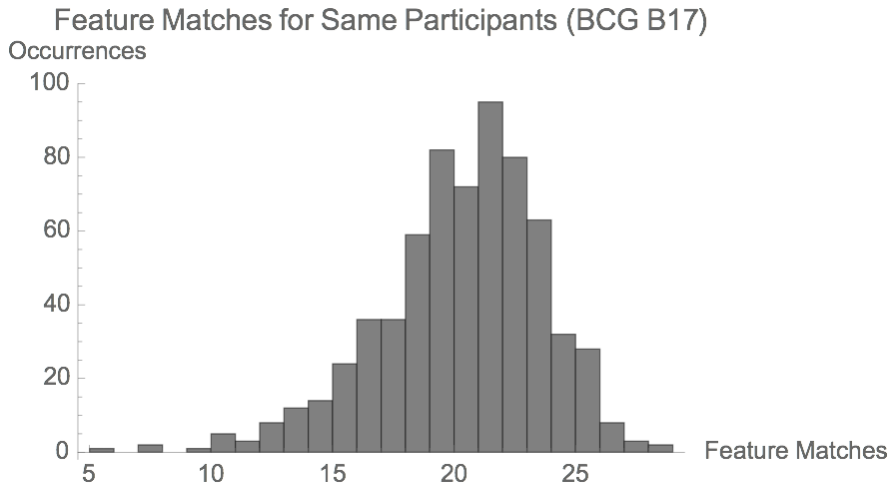

Figure 6.8: Histogram of BCG feature matches for same participant (B17 lab)

number of feature matches for the same individual was shown to be slightly higher than the mean and mode number of feature matches between individuals (Table 6.2). For the mean, this difference was a positive, but negligible, 0.7761 feature matches. A mean of 19.7958 features matched for the same individual, while a mean of 19.0197 features matched between individuals. For the mode, this difference was an additional feature match. A mode of 21 features matched for the same individual, while a mode of 20 features matched between individuals. The maximum number of feature matches remained considerably larger between individuals. A maximum of 28 features matched for the same individual, while a maximum of 43 features matched between individuals. The student commons sub-population performed worse than both the B17 sub-population and the sample population. Namely, both the mean and mode values for the same individual were less than the mean and mode values between individuals (Table 6.3). Additionally, the distributions for each sub-population remained left-skewed with roughly the sample population shape (Figures 6.8, 6.9, 6.10, and 6.11).

Next, we evaluated the distinctiveness of our derived BVP signals over the sample population. As observed in Table 6.3, the mean performed worse when compared to the use of the mean for BCG. For the same individual the mean number of feature matches

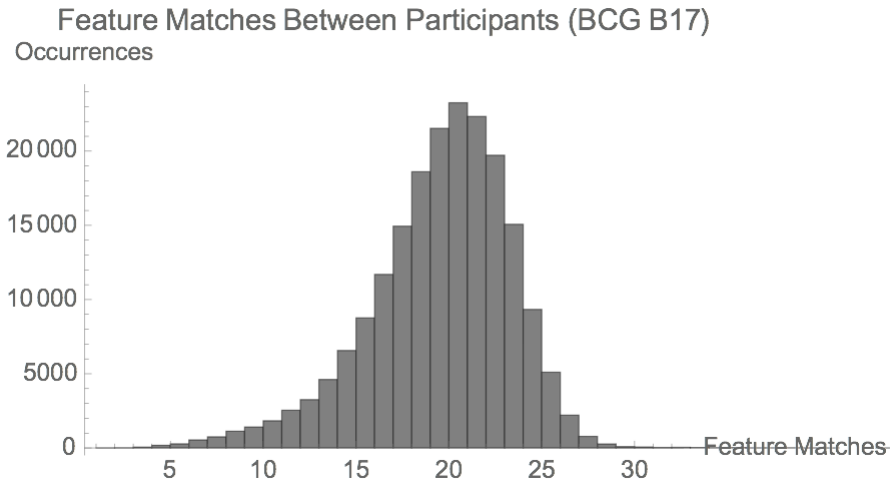

Figure 6.9: Histogram of BCG feature matches between participants (B17 lab)

Feature matches same (Mean, Mode, Max)	Feature matches different (Mean, Mode, Max)
19.7958, 21, 28	19.0197, 20, 43

Table 6.2: Evaluating the distinctiveness of derived BCG signals (B17 lab)

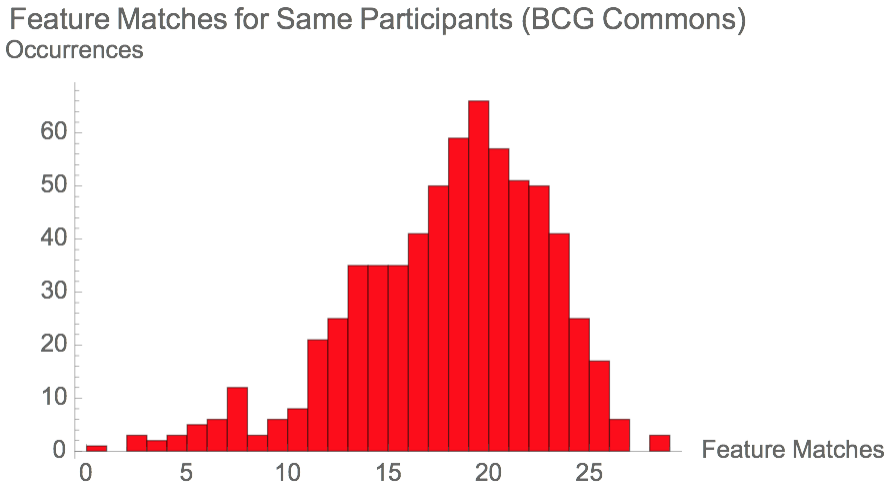

Figure 6.10: Histogram of BCG feature matches for same participant (Commons)

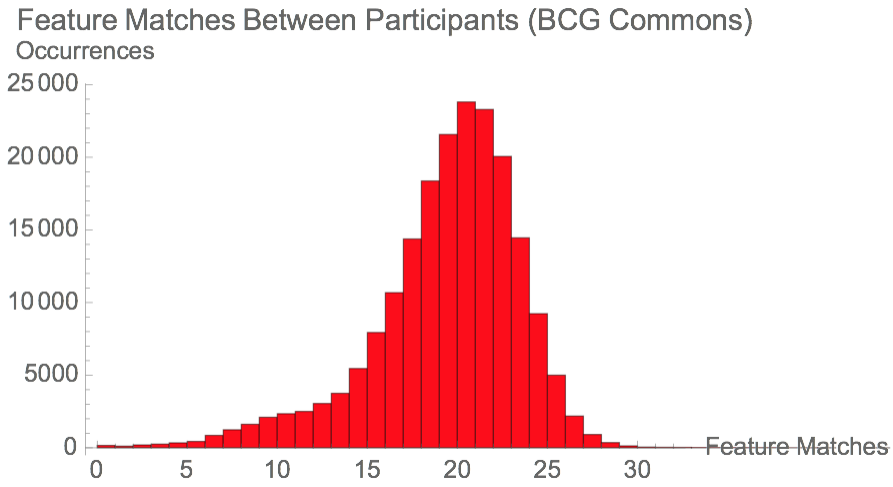

Figure 6.11: Histogram of BCG feature matches between participants (Commons)

Feature matches same (Mean, Mode, Max)	Feature matches different (Mean, Mode, Max)
17.521, 19, 28	18.9099, 20, 43

Table 6.3: Evaluating the distinctiveness of derived BCG signals (Commons)

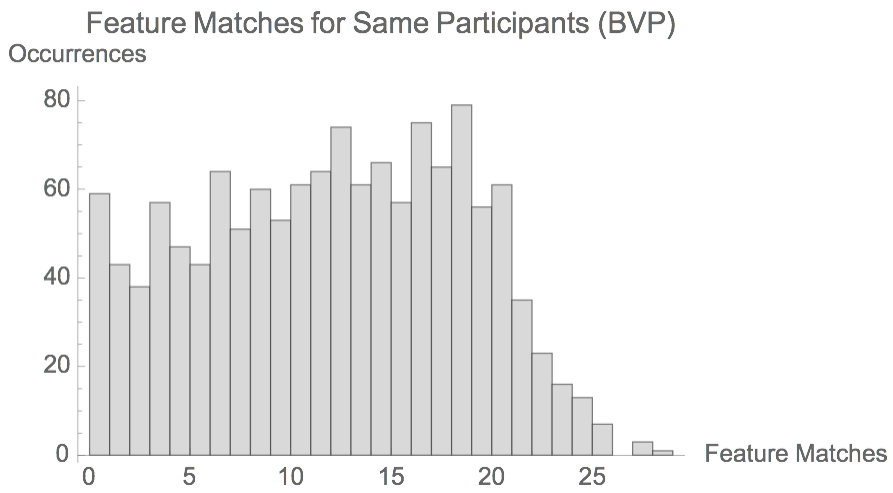

Figure 6.12: Histogram of BVP feature matches for same participant (sample population)

was 11.5473 while the mean number of feature matches between individuals was 12.167. Similar to BCG, this difference of -0.6197 was negligible. On the other hand, the mode number of features for the same individual was greater than the mode number of features between individuals. A mode of 18 features matched for the same individual while a mode of 15 features matched between individuals. Similar to BCG, the maximum number of feature matches for the same individual was considerably less than the maximum number of features between individuals. A maximum of 28 features matched for the same individual while a maximum of 55 features matched between individuals.

The numerical results for the distinctiveness of our derived BVP signals was not necessarily made better when considering the distributions in Figures 6.12 and 6.13. As can be seen in the distribution of Figure 6.11, the number of matching features between individuals was most commonly either 0 or a number of matches between 3 and 23. In Figure 6.12, the number of matching features for the same individual roughly followed a uniform distribution from 0 to 22 feature matches. Given that these two distribution shapes were not necessarily comparable, Table 6.3 was used to evaluate BVP distinctiveness.

When examining the distinctiveness of BVP over the two sub-populations, it was observed that the B17 sub-population performed in a similar manner to the sample popula-

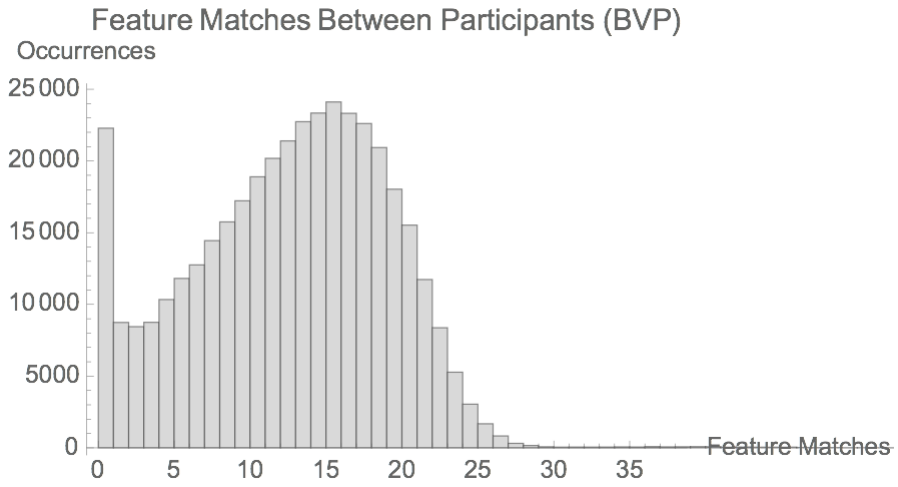

Figure 6.13: Histogram of BVP feature matches between participants (sample population)

Feature matches same (Mean, Mode, Max)	Feature matches different (Mean, Mode, Max)
11.5473, 18, 28	12.167, 15, 55

Table 6.4: Evaluating the distinctiveness of derived BVP signals overall

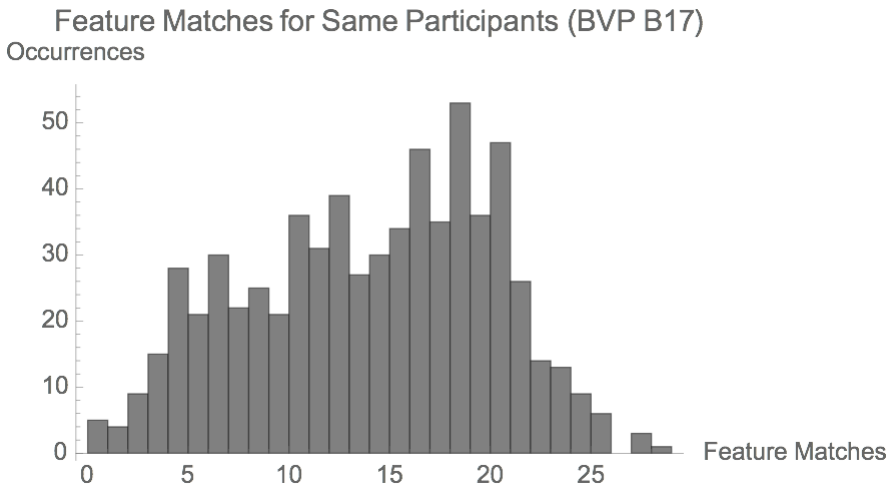

Figure 6.14: Histogram of BVP feature matches for same participant (B17 lab)

Feature matches same (Mean, Mode, Max)	Feature matches different (Mean, Mode, Max)
13.5045, 18, 28	13.5572, 15, 53

Table 6.5: Evaluating the distinctiveness of derived BVP signals (B17 lab)

tion. The student commons sub-population performed worse than the sample population. As can be observed in Table 6.4, the B17 sub-population had a mean number of features for the same individual that was nearly identical to the mean number of features between individuals. Additionally, the B17 sub-population expressed the same sample population trends of having a larger mode number of features for the same individual and having a larger maximum number of features between individuals. The student-commons population performed worse with respect to all summary statistics used in Table 6.5.

After evaluating the distinctiveness of the derived BCG and BVP signals across our populations, the next step was to evaluate the temporal variance of those same signals. In Figure 6.18 the temporal variance of BCG signals over the sample population can be observed. Similarly, in Figure 6.19 the temporal variance of the BVP signals over the sample population can be observed. In both cases, the figures also show the temporal

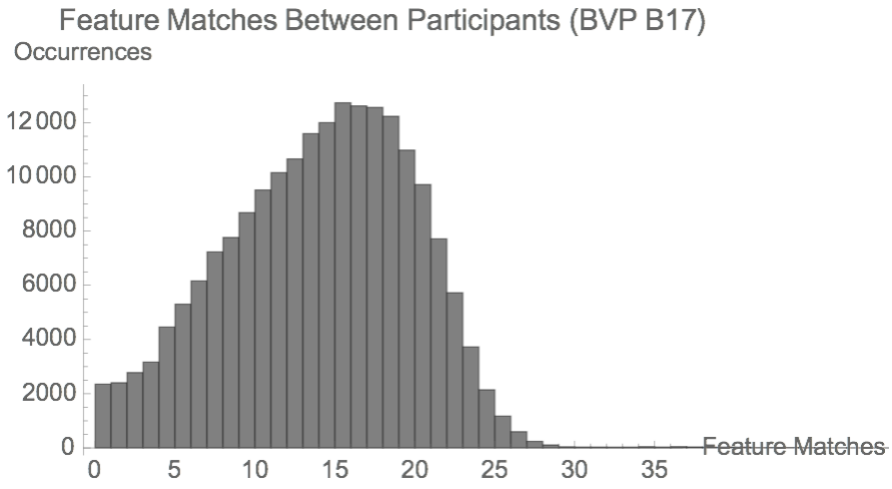

Figure 6.15: Histogram of BVP feature matches between participants (B17 lab)

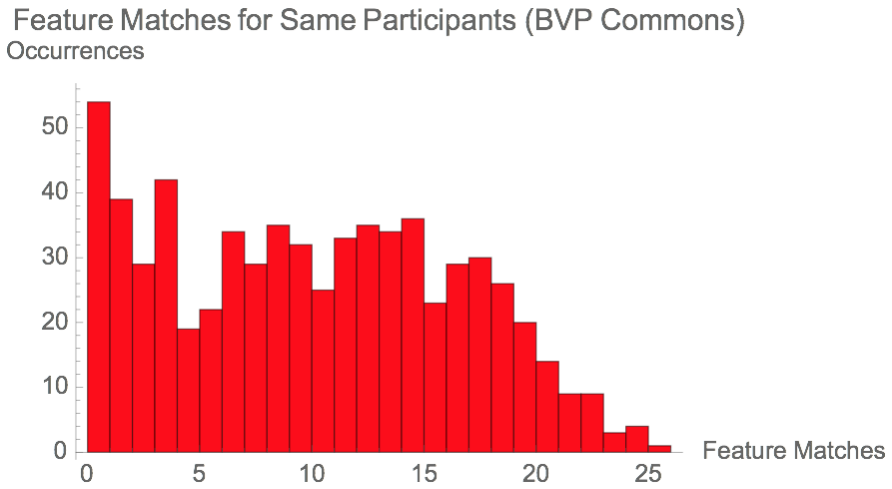

Figure 6.16: Histogram of BVP feature matches for same participant (Commons)

Feature matches same (Mean, Mode, Max)	Feature matches different (Mean, Mode, Max)
9.59009, 0, 25	9.92759, 0, 55

Table 6.6: Evaluating the distinctiveness of derived BVP signals (Commons)

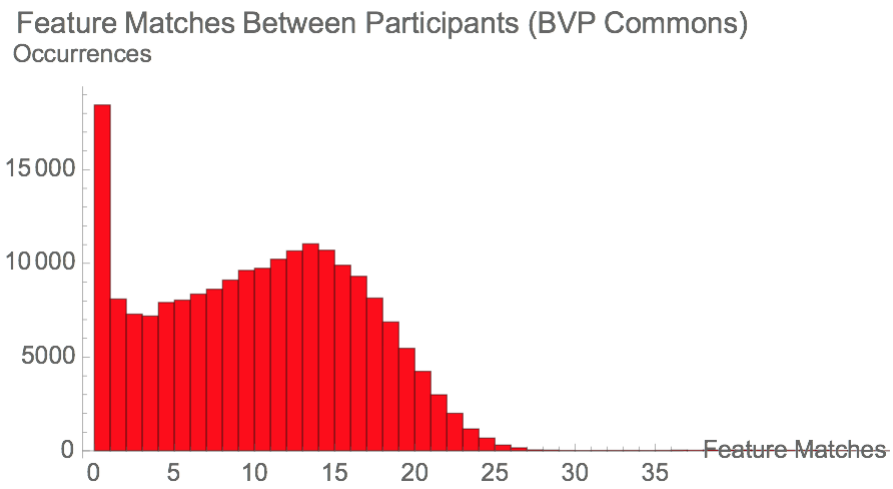

Figure 6.17: Histogram of BCG feature matches between participants (Commons)

variance for each sub-population. When reviewing Figure 6.18, it was shown that there was very little temporal variance for our derived BCG signals. In fact, only one participant from the student commons sub-population experienced a significant decline in the number of matching features after an offset of 40 segments (i.e., units of 7.68 seconds). On the other hand, in Figure 6.19 it was shown that there was more temporal variance for BVP signals. In nearly all instances a gradual decline in the number of matching features over time was observed.

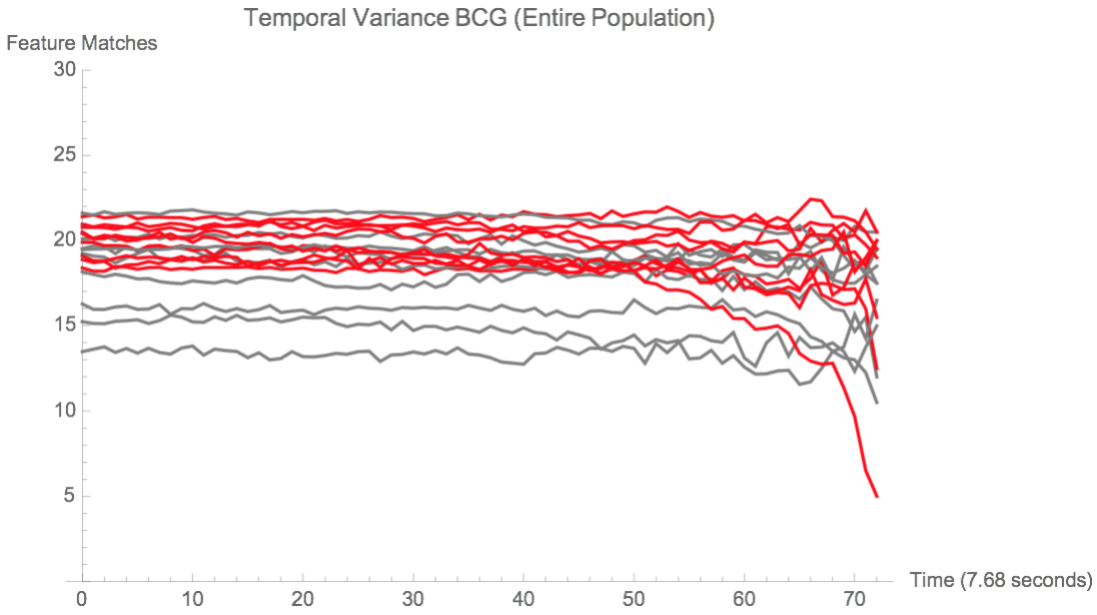

Figure 6.18: Temporal variance of BCG signals (red is student commons, gray is B17 lab)

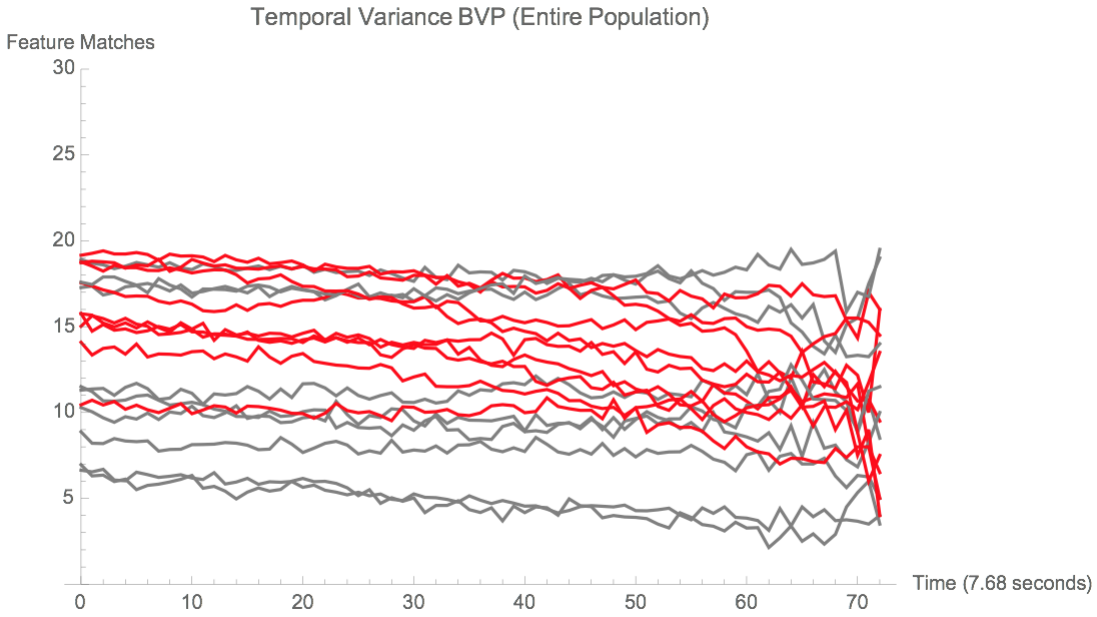

Figure 6.19: Temporal variance of BVP signals (red is student commons, gray is B17 lab)

Chapter 7

Discussion

As the results indicated, neither our derived BCG signals nor our derived BVP signals were able to satisfy the design goals stated in physiological signal based key agreement [3]. One potential cause for this poor performance could have been due to an issue in using the Android Sensor API to sample our sensors. In particular, when a developer uses the API he or she has the ability to provide a recommended sampling rate by specifying a delay in microseconds. Unfortunately, the API provides no guarantee that the sensors will actually sample at that exact sampling rate. Consequently, there are some small **polling inaccuracies** that can accumulate over time, especially over a duration as long as 10 minutes. Inaccuracies of this nature could have allowed for more features to match for different time offsets when evaluating temporal variance. Additionally, these inaccuracies could also have the potential to reduce the number of matching features for signals derived from the same individual.

Another potential source of error could have been that **we did not use interpolation** to account for the inaccuracy of the Android Sensor API. If interpolation had been used, we would have been able to artificially simulate a sampling rate of exactly 100 Hz by filling in any instances of missing points. This would have eliminated any accumulation of sampling inaccuracies over time. Use of the technique could likely have improved the number of feature matches for the same individual as well as temporal variance. However,

we did not evaluate the use of any interpolation functions, so the effect of applying them is not known. Here we are merely assuming that interpolation would have helped by filling in missing data.

Lastly, another source of error could have been that half of the data from our sample population was collected from the student commons. This particular location had far more sources of **background noise** present in its environment when compared to the calm laboratory setting from which the other half of our data was collected. Our evaluation of both sub-populations ultimately provides some information relating to this point. Namely, a comparison between Tables 2 and 3 and Tables 4 and 5 ultimately indicate that data collected from the student commons had lower mean and mode feature matches both between and from the same individual. Therefore, where we sampled from could have been a source of error.

Chapter 8

Conclusion and Future Work

In conclusion, our approach of using derived physiological signals to perform key distribution was not successful. While part of this lack of success may be attributable to the sources of error mentioned in our discussion, it is likely that our techniques may also not have worked. This might include our use of the filtering techniques mentioned in [4] and [5] or the manner in which we generated features according to [3]. Regardless, it may still be possible to achieve secure key distribution through the use of derived physiological signals. Unfortunately, we were not able to experience such an outcome with our collected data and testbed and analysis implementations. The results of the physiological signal based key agreement paper in [3] had demonstrated the ability to perform key distribution when measuring PPG and EKG signals using dedicated hardware. If derived physiological signals can be acquired just as accurately, it should be possible to use them for key distribution.

Given that WIoT devices reside in close proximity to the human body, it is rather natural to think of using the data that they regularly collect to help them perform key distribution in a dynamic way. The benefit of approaching key distribution in this physiological manner is that it can be performed without the need for any user involvement. As WIoTs become more widespread, ensuring that they can secure their wireless communication channel in a usable way will be increasingly important.

To continue work in this domain, it would likely be useful to explore different methods for both deriving physiological signals and generating features. Once suitable physiological signal derivation and feature generation methods are found, it would be best to evaluate their performance in a more active setting. As opposed to an environment in which the WIoT wearer is still, an active setting would allow for an understanding of how well such a system would operate under real world usage scenarios. This is essentially what we would have done had our results indicated a successful outcome.

Appendix A

IRB Consent Form

Informed Consent Agreement for Participation in a Research Study

Investigator:
Krishna Kumar Venkatasubramanian

Contact Information:
Location: Fuller Labs 137,
Department: Computer Science
Email: kven@wpi.edu
Telephone: (508)-831-6571

Title of Research Study:
Using gyroscope-derived ballistocardiography signals to perform key distribution in body-area-networks

Sponsor:
N/A

Introduction:
You are being asked to participate in a computer security research study on developing a way to secure wireless communications occurring between devices that are on the surface of the human body. Before you agree, however, you must be fully informed about the purpose of the study, the procedures to be followed, and any benefits, risks or discomfort that you may experience as a result of your participation. This form presents information about the study so that you may make a fully informed decision regarding your participation.

Purpose of the study:
The purpose of the study is to determine whether subtle cardiac movements detectable by gyroscope sensors can be successfully used to assist in securely distributing cryptographic key information to devices residing within a body-area-network. If this indeed is possible, then the resulting technology will be used to provide plug-and-play setup of secure communication channels in body-area-networks.

Procedure to be followed:
You will first be asked to firmly fasten a smartwatch onto each one of your wrists. Next, you will then be asked to sit in a fixed chair with your arms resting on a table. Next, the experimenter will then initiate data collection from the smartwatches via a laptop. Once this happens, you will remain in your sitting position for a total of 10 minutes, which you will be made aware of through the words "finished sending" appearing on each watch face. While you are seated during the 10 minute period you do not need to do anything, but it is advised that you do not talk or intentionally move. During this data collection process we plan to record the following information:

- Your subtle arm movements through accelerometer and gyroscope sensors present in the two smartwatch devices (from which your cardiac movement information will be extracted).
- Your heartrate
- Your gender
- Your age
- Whether you had engaged in exercise prior to participating in the study

APPROVED BY
WPI IRB1
3/27/17 to 3/26/18

Note that the collected data will be used to detect the performance of the smartwatch devices in their ability to use the data to successfully distribute cryptographic key information. The data will not be used in any of its original or derived forms to inform any participant in this study of a medical condition that may or may not be determinable through further analysis of the data.

Risks to study participants:
We do not anticipate any risks or adverse events wearing the two smartwatches for such a short period of time. If, however, you are feeling uncomfortable at any stage of the data collection, please stop. At that time if you do not wish to continue, all your data will be erased immediately.

Benefits to research participants and others:
The concept of e-healthcare is likely to continue to grow in the near future. Like all medical information, data generated by devices in body-area-networks will need to be protected. This protection includes protection of the data while it is being communicated wirelessly within the network. Being able to perform key distribution automatically without any human involvement is a first step in providing a means for convenient communication channel security.

Record keeping and confidentiality:
We do not plan to collect any personally identifiable information as part of this study. We will assign each participant of the study with a random ID number. Any publication or presentation of the data will not identify you. All demographic data we collect will be reported in the aggregate and will not single out an individual participant's response.

Compensation or treatment in the event of injury:
You do not give up any of your legal rights by signing this statement. There is no potential medical risk or injury to the participants of this study. If the participant is injured there will be no compensation from anyone involved with the study and all medical expenses will be borne by the participant or their insurer.

For more information about this research or about the rights of research participants, or in case of research-related injury, contact:

Professor Krishna Venkatasubramanian
Telephone: (508)-831-6571
Email: kven@wpi.edu

WPI IRB Chair, Professor Kent Rissmiller
Telephone: (508)-831-5019
Email: kjr@wpi.edu

WPI Compliance Officer, Jon Bartleson
Telephone: (508)-831-5725
Email: jonb@wpi.edu

Your participation in this research is voluntary:
Your refusal to participate will not result in any penalty to you or any loss of benefits to which you may otherwise be entitled. You may decide to stop participating in the research at any time without penalty or loss of other benefits. The project investigators retain the right to cancel to postpone the experimental procedures at any time they see fit.

APPROVED BY
WPI IRB1
3/27/17 to 3/26/18

By signing below:
You acknowledge that you have been informed about and consent to be a participant in the study described above. Make sure that your questions are answered to your satisfaction before signing. You are entitled to retain a copy of this consent agreement.

Study participant signature	Date
Study participant name (please print)	
Signature of person who explained this study	Date

Special Exceptions:
Under certain circumstances, and IRB may approve a consent procedure, which differs from some of the elements of informed consent set forth above. Before doing so, however, the IRB must make findings regarding the research justification for different procedures (i.e., a waiver of some of the informed consent requirements must be necessary for the research is to be "practicably carried out."). The IRB must also find that the research involves "no more than minimal risk to the subjects." Other requirements are found at 45 C.F.R. §46.116.

APPROVED BY
WPI IRB1
3/27/17 to 3/26/18

Bibliography

[1] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.

[2] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, "A comprehensive survey of wireless body area networks," *Journal of medical systems*, vol. 36, no. 3, pp. 1065–1094, 2012.

[3] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2010.

[4] J. Hernandez, D. J. McDuff, and R. W. Picard, "Bioinsights: extracting personal data from "still" wearable motion sensors," in *Wearable and Implantable Body Sensor Networks (BSN), 2015 IEEE 12th International Conference on*, pp. 1–6, IEEE, 2015.

[5] J. Hernandez, Y. Li, J. M. Rehg, and R. W. Picard, "Bioglass: Physiological parameter estimation using a head-mounted wearable device," in *Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on*, pp. 55–58, IEEE, 2014.

[6] M. Li, S. Yu, W. Lou, and K. Ren, "Group device pairing based secure sensor association and key management for body area networks," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9, IEEE, 2010.

[7] G. Selimis, L. Huang, F. Massé, I. Tsekoura, M. Ashouei, F. Catthoor, J. Huisken, J. Stuyt, G. Dolmans, J. Penders, *et al.*, "A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design," *Journal of medical systems*, vol. 35, no. 5, pp. 1289–1298, 2011.

[8] F. Gandino, R. Ferrero, and M. Rebaudengo, "A key distribution scheme for mobile wireless sensor networks: q-s-composite," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 34–47, 2017.