PRIVACY-PRESERVING ECG BASED ACTIVE AUTHENTICATION (PPEA2) SCHEME FOR IOT DEVICES

A Thesis

by

GHANSHYAM BHUTRA

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	Rabi Mahapatra
Committee Members,	Dilma Da Silva
	Krishna Narayanan
Head of Department,	Dilma Da Silva

December 2017

Major Subject: Computer Science

ABSTRACT

Internet of things (IoT) devices are becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, to industrial control systems. On a larger scale, live stream of sleep patterns data recorded via fitness tracker devices was utilized to quantify the effect of a seismic activity on sleep. While the benefits of IoT are undeniable, IoT ecosystem comes with its own set of system vulnerabilities that include malicious actors manipulating the flow of information to and from the IoT devices, which can lead to the capture of sensitive data and loss of data privacy. My thesis explores a Privacy-Preserving ECG based Active Authentication (PPEA2) scheme that is deployable on power-limited wearable systems to counter these vulnerabilities.

Electrocardiogram (ECG) is a record of the electrical activity of the heart, and it has been shown to be unique for every person. This work leverages that idea to design a feature extraction followed by an authentication scheme based on the extracted features. The proposed scheme preserves the privacy of the extracted features by employing a light-weight secure computation approach based on secure weighted hamming distance computation from an oblivious transfer. It computes a joint set between two participating entities without revealing the keys to either of them.

To My Grand Parents, Mr. Sitaram Bhutra And Mrs. Narabda Bhutra And My Uncle Mr. Pawan Kumar Bhutra For All The Support They Have Given Me.

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. Rabi Mahapatra, and my committee members, Dr. Dilma Da Silva, and Dr. Krishna Narayanan, for their knowledge, patience, motivation, and support throughout this research.

I would like to express my gratitude to Dr. Amar Rasheed from Armstrong State University for guidance, ideas and for sharing their immense knowledge on this subject.

Thanks also go to my friends Swaroop Pal, Siddhant Rath my colleagues and the department faculty and staff for their contributions and making my time at Texas A&M University a great experience.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supported by a dissertation committee consisting of Dr. Rabi Mahapatra and Dr. Dilma Da Silva of the Department of Computer Science and Engineering and Dr. Krishna Narayanan of the Department of Electrical and Computer Engineering.

All work for the thesis was completed independently by the student.

Funding Sources

There are no funding contributions related to the research and compilation of this document.

NOMENCLATURE

ECG	Electrocardiogram
PPEA2	Privacy preserving ECG based Active Authentication
WBSN	Wireless Body Sensor Network
BAN	Body Area Network
DSIP	Distributed Set Intersection Protocol
OT	Oblivious Transfer
IoT	Internet of Things
BPM	Beats per minute
CWT	Continuous wavelet transform
FWT	Fast wavelet transform
BSN	Body Sensor Network
MSB	Most Significant Bit
LSB	Least Significant Bit
TRR	True Rejection Rate
TAR	True Acceptance Rate
FRR	False Rejection Rate
FAR	False Acceptance Rate
ROC	Receiver Operating Characteristics

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

1.1 Generalizations in IoT

The world is going through a dramatic transformation, rapidly moving from isolated systems to internet-enabled ‘things’ which connect to a shared infrastructure and work in harmony with other devices. This new communication paradigm has shown tremendous potential in enriching everyday life, increase business productivity and efficiency of many processes. In this internet of things or IoT [1], all kinds of devices connected to the network irrespective of their computational capabilities and can be broadly segregated into three layers, Device Server, Smart Devices and the End Devices.

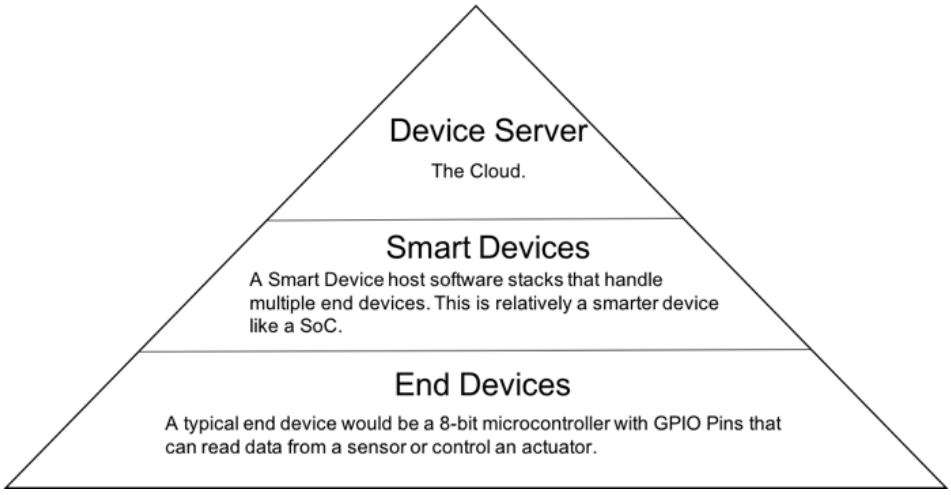


Figure 1.1 Device layers in IoT

Following this three-tier classification, represented in figure 1.1, is an IoT application in the healthcare domain, the Wireless Body Sensor Network (WBSN) [2,3] or Body Area Network (BAN). WBSN/BAN is a network of embedded or wearable

physiological sensors that stream data on the users' health into a sink, typically a smartphone for processing. Physiological sensors for ECG, EEG, blood pressure, temperature and motion sensors, etc. continuously monitor the user in real-time. This stream of data allows for quicker diagnostics, comprehensive patient history, monitor fitness objectives, etc.

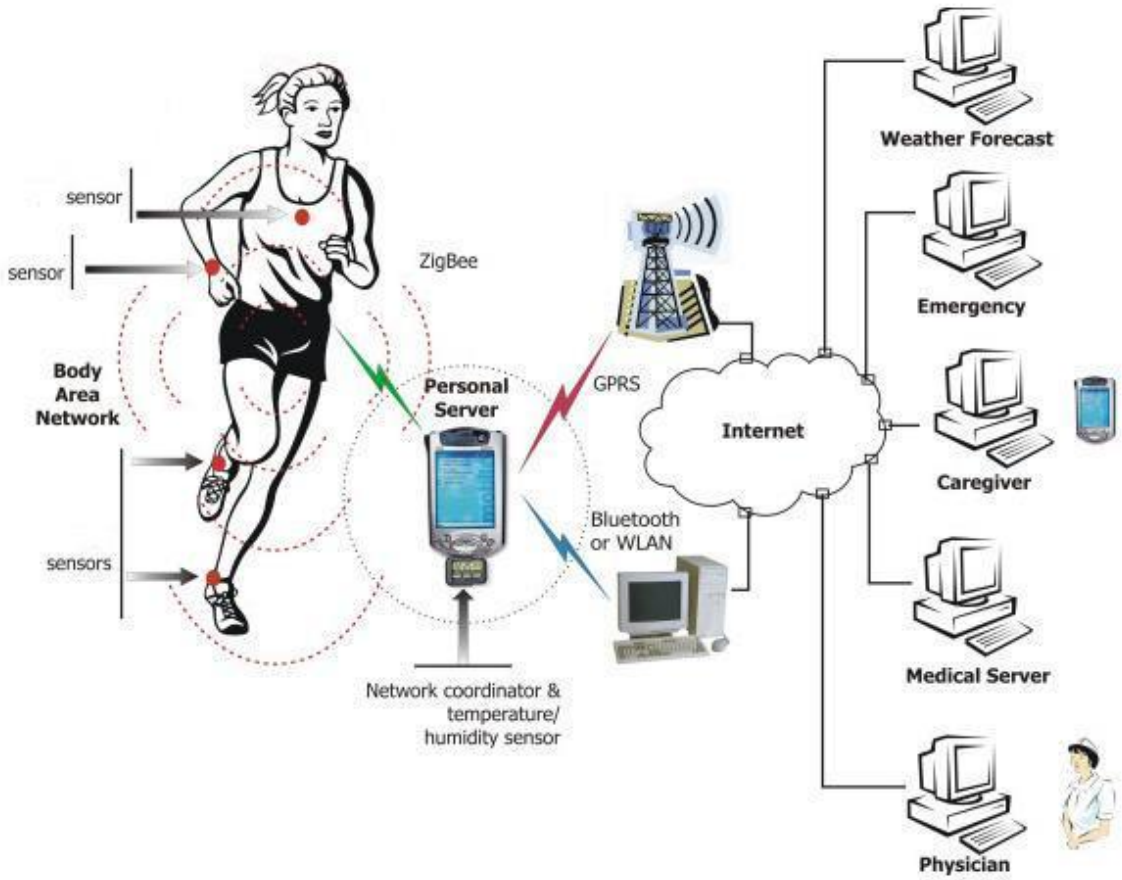


Figure 1.2 Wireless Body Sensor Network Architecture. Reprinted from Wikimedia Commons [4]

Figure 1.2 shows a typical architecture of a WBSN. The sensors here on the person are the end devices connected to the smartphone a smart device which is connected to the cloud the device server.

1.2 Security objectives and challenges

The nature of data flowing through a WBSN is sensitive and private as it contains crucial information about the user's health and physical state. Regardless of the sensitivity of the data, due to the potential benefits, more and more people are getting comfortable with the idea. There is no denying the benefits of WBSNs or other wireless sensor networks, but as is the nature of wireless communication it is easy for an adversary to alter the transmitted messages or inject malicious data into the message stream. This intrusion could be fatal especially in the case of WBSNs where the data is sensitive to the user's health and physical state.

In the literature, there are two proposed solution to this problem cryptography and authentication [5]. By using cryptographic primitives, the messages could be encrypted by the sender and decrypted by the receiver using a shared key. However, traditional public key cryptography requires storage and processing of significant number certificates which impractical in the sensor networks due to the constrained power and computational resources. Also, cryptographic techniques have inherent key management problem which deals with generating and sharing of the keys. The problem is exacerbated by low power and headless nature of these devices.

1.3 Authentication

Authentication is establishing and verifying the identity of an individual. It is applicable wherever it is required to prevent unauthorized access to information, physical locations, etc. With the advent of the communication paradigm IoT, where devices are

communicating with other devices, and more sensitive data online a secure authentication scheme is essential. Typically, an individual's identity can be established by a unique pattern of behavioral or physiological characteristics. A behavioral trait used for identification of a person is unique but has to be consistent and repeatable like a signature, a pattern of dots, password. On the other hand, there are physiological traits also known as biometric data like facial features, fingerprints, iris scan ECG, etc. can also be used for identification. In a typical authentication protocol, the server uses the information from the client to compare one or more of these traits to the pre-registered set which validates the identity.

Traditional authentication methods rely on numerical or graphical passwords which are vulnerable to surfing attacks. With a weak password, an attacker can get access via a line-of-sight from a short distance, social engineering, phishing, etc. The user could also either forget or share the password as well. Masdari et al. study a potential list of possible security attacks against authentication schemes in body sensor networks [6]. Biometric authentication is more reliable than their credential based counterpart. A biometric system requires a physiological or behavioral characteristic of the user which is unique and universal [7]. Fingerprint and iris are examples of such physiological features whereas gait and speech are behavioral Unlike the credential based method, a biometric feature cannot be forgotten or shared and depending on the kind of signal used cannot be duplicated either.

1.4 Related work

There has been a considerable amount of research in the wearable medical sensors space [8]. These sensors can pick up all kinds of physiological signals like beats per minute, perspiration, EEG, ECG, perspiration, motion, etc. Since the mid-2000s authentication in sensor networks has been an active research area. In 2006 Luk et al. proposed a list of security requirements for an ideal sensor network [9]. They showed that most authentication techniques at that time met only a subset of those requirements.

In [7] Wayman et al. show security benefits of a biometric authentication system and following the improvements in sensor technology it has become possible to authenticate users even in a sensor network biometrically. In 2002 the Fuzzy vault scheme was proposed by Jules and Sudan et al. [10]. In this scheme, the biometric feature vector is projected into polynomial which is created using a shared key. These projected values are mixed with random chaff points and then sent to the receiver. The receiver recreates those projected values using its key and the feature template, and if it has enough overlap with the set of values received from the source, then the authentication is successful. As the sender does not send its features values in the channel, this scheme preserves the privacy of the biometric features. In [11] Karthik et al. show the implementation of this fuzzy vault technique with fingerprints.

CHAPTER II

BIOMETRIC AUTHENTICATION

2.1 Introduction

Biometric authentication is authentication using biometric data. It involves a biometric data capture system and an authentication protocol which matches the captured biometric data to a pre-registered template. There are two types of biometric features physiological and behavioral. Physiological features, as the name suggests are internal features and not in control of the user like the fingerprint and iris patterns. Voice and gait are examples of behavioral features. Physiological features provide better reliability and stronger security as they are not in control of the user and do not change significantly over time. Behavioral features are more susceptible to spoofing attacks.

There are a lot of human identification methods proposed in the literature. Physiological features like face, eyes, fingerprints-palm and behavioral features like voice, gait [12-15], have been successfully shown to identify a person from a group. These systems are based on quantifiable features unique to every person and do not change over time. The method of feature extraction varies from one method to the other depending on the input type and in the computation requirement, and the reliability is measured by the false acceptance rate (FAR), true acceptance rate (TAR) [16].

2.2 ECG vs. other biometrics

[17] The electrocardiogram(ECG) is a record of the electrical activity of the human heart. It is typically used extensively for diagnosing irregularities in the heart. Research from the last decade suggests that it is unique for everyone and could be used for identification. The uniqueness of ECG makes diagnosis a challenge but is an advantage for biometric authentication systems. An ECG based system has a distinct advantage over other physiological features, and that is it's an internal signal. There have been ways to copy a fingerprint, iris pattern of a person as they are both external signals but the ECG signal cannot be reproduced, and unless the health of the person is compromised it doesn't change. It has inherent liveness, real-time properties so it cannot be used if the user is deceased. Other advantages of using ECG is the cost of the sensor is cheaper compared to the previously mentioned methods.

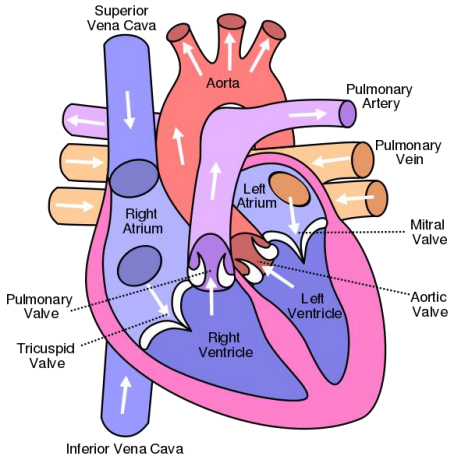


Figure 2.1 The human heart. Reprinted from Wikimedia Commons [18]

Figure 2.1 shows chambers of the heart, the right and left atrium and the right and left ventricles. A group of cells initiates a heartbeat in the right atrium called the sinoatrial node (SA node). SA node is the natural pacemaker of the heart initiates an electrical

disturbance results in alternating contraction and relaxation of the heart muscles, the myocytes.

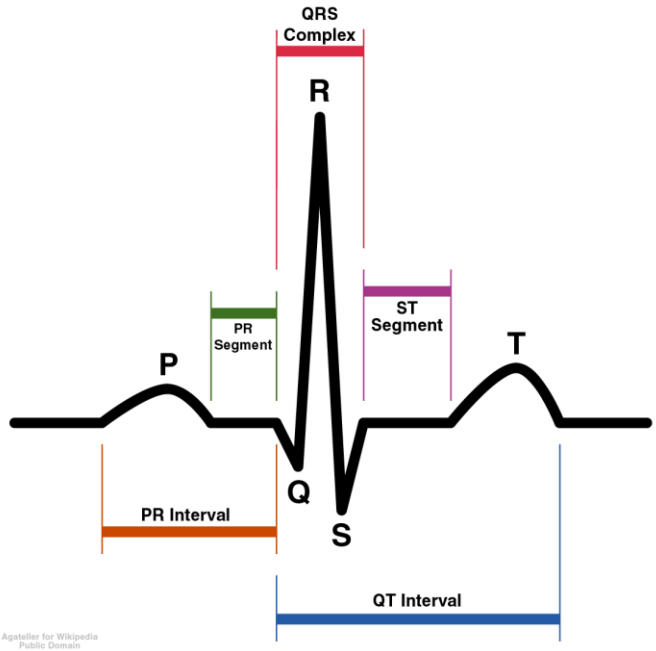


Figure 2.2 Typical ECG wave representing a cardiac cycle. Reprinted from Wikimedia Commons [19]

Figure 2.2 shows a typical ECG trace of a normal heartbeat. It is a one-dimensional time-varying signal. The electrical disturbance starts at the sinoatrial node (SA Node), the natural pacemaker and then radiates outwards causing the myocytes to depolarize and compress rapidly. Specific segments of the plot represent a different phase of the cardiac cycle as mentioned below: -

- **P-wave**: represent atrial depolarization. It precedes the QRS complex.
- **PR-interval**: represent the time taken for electrical activity to move between the atria and ventricles.
- **QRS-complex**: represents depolarization of the ventricles.

- **ST segment:** represents the time between depolarization and repolarization of the ventricles (i.e., contraction).
- **T-wave**: represents ventricular repolarization. It follows the QRS complex

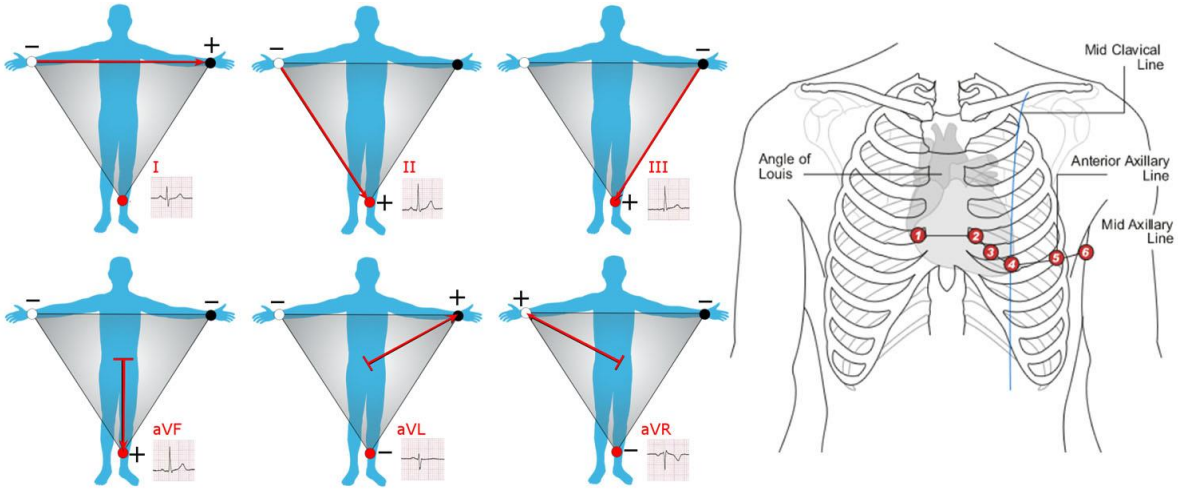


Figure 2.3 ECG collection leads. Reprinted from Wikimedia Commons [20]

In clinical diagnostics, ECG is collected from 12 leads from a combination of ten electrodes as listed below. Figure 2.3 shows the placement of all the leads.

- Lead I: right arm – left arm
- Lead II: right arm – left leg
- Lead III: left arm – left leg
- aVR lead: right arm
- aVL lead: left arm
- aVF lead: left leg
- V1 – V6: chest leads

The twelve leads help the diagnostician to look at the electrical conduction system of the user from different vantage points. In the last decade, ECG signals have shown potential as a physiological feature in this identification problem. The earliest work by Biel et al. [21] was using temporal, amplitude, and slope features from the ECG for identification. Israel et al. [22] proposed identification using only temporal features and claimed that the temporal characteristics are agnostic of the anxiety of the individual. A similar claim by Janani et al. [23] using a combination of accelerometer and ECG signals to identify people in different physical states. The above-mentioned work also indicates that ECG from a single lead has all the physiological parameters for it to be unique and we don't need all the twelve leads for identification purposes.

The fingerprint is the oldest and most prevalent form of biometric authentication used. It is an exterior characteristic, and it is possible for an adversary to capture and replay it for authentication resulting in a false positive. This biometric signal is also susceptible to damage resulting in false negatives. The article in [24] demonstrates the vulnerability of commercial cell phones using fingerprint-based authentication. Another approach to preserving the privacy of is cryptography. The sensors would transmit encrypted data, and the network edge would decrypt using a shared secret key. This method works for a user-facing system it is not ideal sensor networks due to the crucial inherent agreement, and in the event of a breach, the system remains vulnerable unless the key is changed. Due to the resource limitation on the sensors we cannot use stronger encryption techniques.

2.3 ECG based authentication challenges

Unlike other biometric sources, ECG signal or features extracted from the ECG signal contains very sensitive data to the user's health. As proposed in [22, 23] the extracted temporal features from the ECG signal are a function of the morphology of the heart. Transmitting raw features over a wireless network is a potential vulnerability. An adversary could gain access to the features and reverse engineer the information about the physical well-being of the user. The adversary could also intercept the message and add unwanted and malicious code into the data stream. This is also dangerous as the altered message could lead to faulty diagnostic information. This calls for an authentication mechanism which hides these features in some way without losing the potential benefits of identification.

2.4 Related work

Since it has been shown that ECG could be used to identify people in a group, there has been a bunch of work done to use that idea in the context of wearable sensor networks. In 2016, Falconi et al. proposed the idea of using extracted ECG features to authenticate in mobile devices [25]. In 2012, Zhang et al. proposed an algorithm based on the fuzzy vault scheme but without the key distribution overhead [26]. In [27-32] different feature extraction methods are considered for ECG based authentication.

CHAPTER III

ECG BASED IDENTIFICATION

3.1 Overview

As mentioned in the previous chapter, it has been shown that the normalized temporal distance between the fiducial points in a cardiac cycle remains consistent for an individual and are independent of the anxiety state. Since the fiducial points indicate the beginning, the end and the peak of an electrical activity the temporal distance between them is a function of the heart's physiology and is independent of heart rate. This distance remains constant in a developed human heart and does not change over time. A set of features are calculated from the ECG wave, and then that is used for authentication.

Based on the feature extraction techniques in the above-mentioned works they can be grouped as fiducial point based techniques. Identification by ECG can be classified into two categories fiducial point and non-fiducial point based [29]. In the fiducial point based method, fiducial points (P, Q, R, S, T) are identified in the ECG signal, and the features are extracted from those [7,8]. In the non-fiducial point based approach the feature vector is extracted from a signal segment. Plataniotis et al. [30] use the coefficients from a discrete cosine transform of an autocorrelated signal segment as the feature set. Another approach by Yarong et al. [31] uses coefficients from a Fourier transform for their feature set. Tantawi et al. [32] proposed a method for using discrete wavelet transform. The R-R signal segment is processed using the discrete bi-orthogonal wavelet, and the non-informative coefficients are removed to reduce the feature set size.

3.2 Feature Extraction

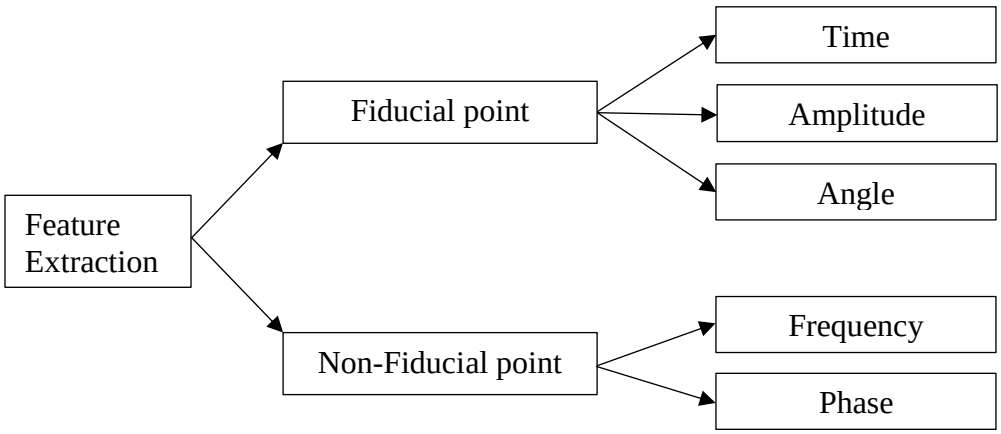
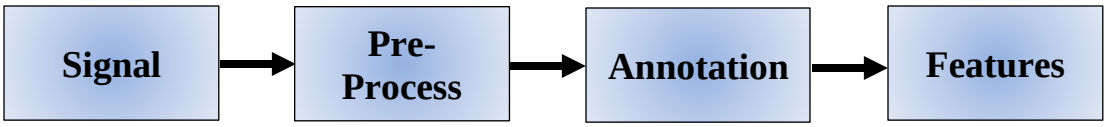


Figure 3.1 Taxonomy of feature extraction

Feature extraction in ECG can be categorized into two broad categories, fiducial point based and non-fiducial point based. In the fiducial point method, the fiducial points P, Q, R, S, T, etc. of the wave are identified, and then authentication features are extracted from these points. The features could be the temporal distance between two fiducial points, a difference in amplitude or angle of the wave between two fiducial points. The non-fiducial point method does not require identification of any points on the wave instead they take the coefficients of a signal transform or a neural network as the authentication features. Figure 3.1 shows the taxonomy of feature extraction in ECG based identification.

Figure 3.2 Feature Extraction steps



The feature extraction process can be split into four steps. Signal, Pre-Processing, Annotation, Extraction. Figure 3.2 gives a diagrammatical representation of the steps.

Signal: This simulates the ECG wave from a person. It accumulates the signal over a period of three seconds and passes it to the next block for processing. Specifically, three seconds is chosen such that at least one complete cardiac cycle is recorded. The ECG signal is read from a file. Figure 3.3 below shows a stream of raw ECG signal sampled at 500Hz.

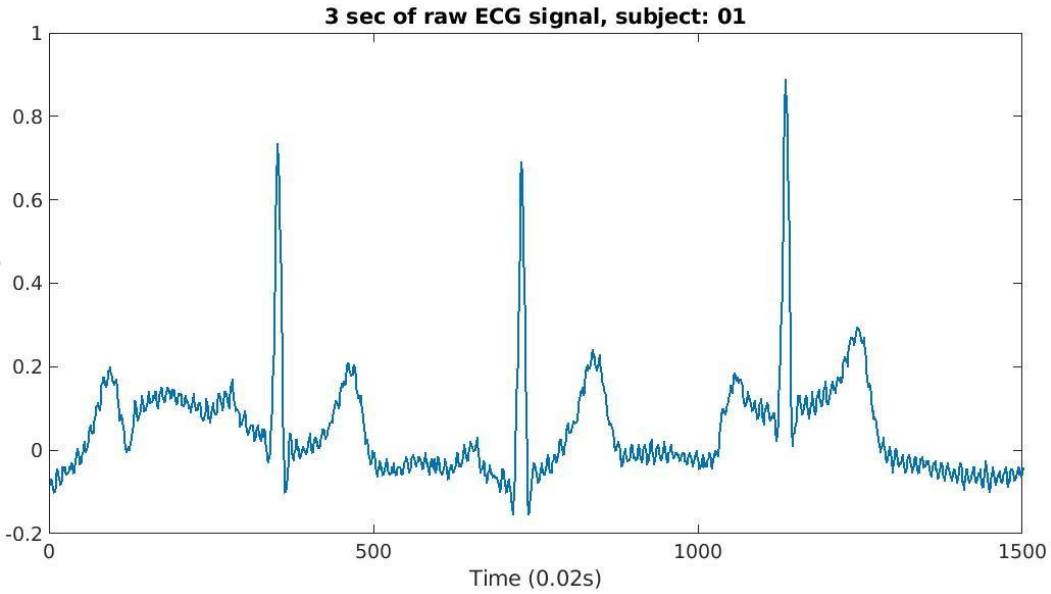


Figure 3.3 Raw ECG wave

Pre-Process: This step is done to facilitate accurate feature extraction from the ECG wave. The figure showing the raw signal shows a noisy version of the actual signal. It has both high and low-frequency components. The primary source of the high-frequency noise is the 50Hz or 60Hz power to which the ECG collection system is connected. The low frequency is probably due to the variation in the baseline voltage of the contacts. We remove these noise components using a bandpass filter. This step increases the efficiency of the following annotation step adding robustness to the design.

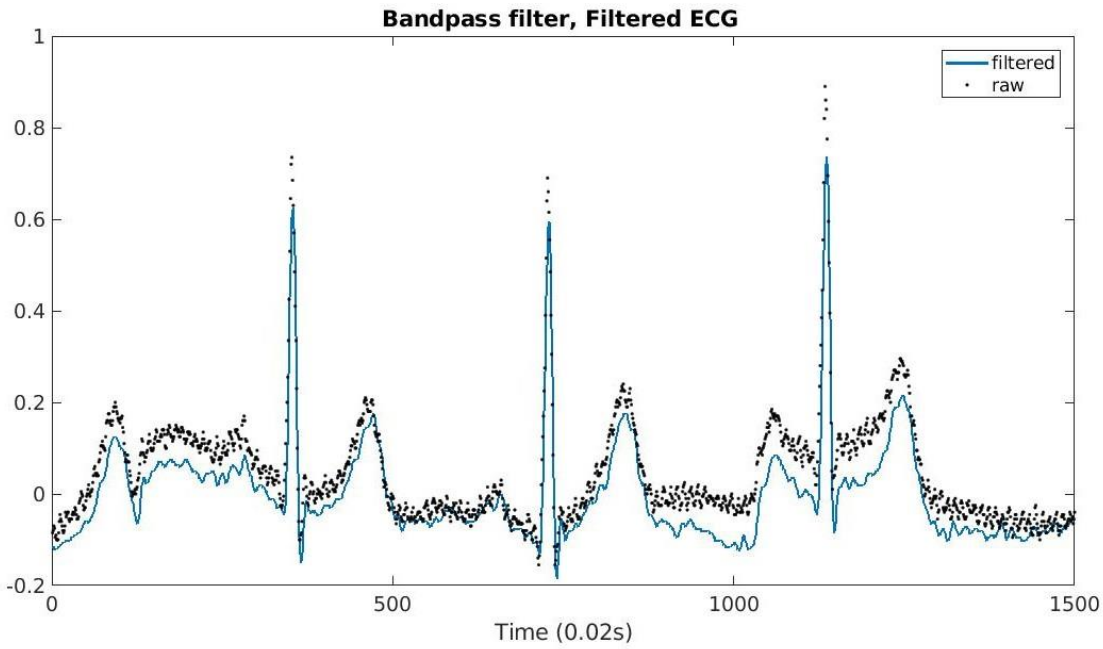


Figure 3.4 Filtered ECG wave

Figure 3.4 shows the filtered ECG signal along with the with the raw signal overlay. Both the high frequency and the low-frequency noise components are significantly reduced.

Annotation: In this step, the fiducial points in the signal are identified. Continuous wavelet transform and fast wavelet transform are used for identifying the fiducial points. The annotation is done in two phases, in the first phase the high frequency QRS complex. The QRS complex is the representation of ventricular contraction, and it is distinctively high as the contraction of the ventricles requires the highest energy. In the second phase,

the low-frequency P and T waves are identified between the R-R intervals extracted from the first phase.

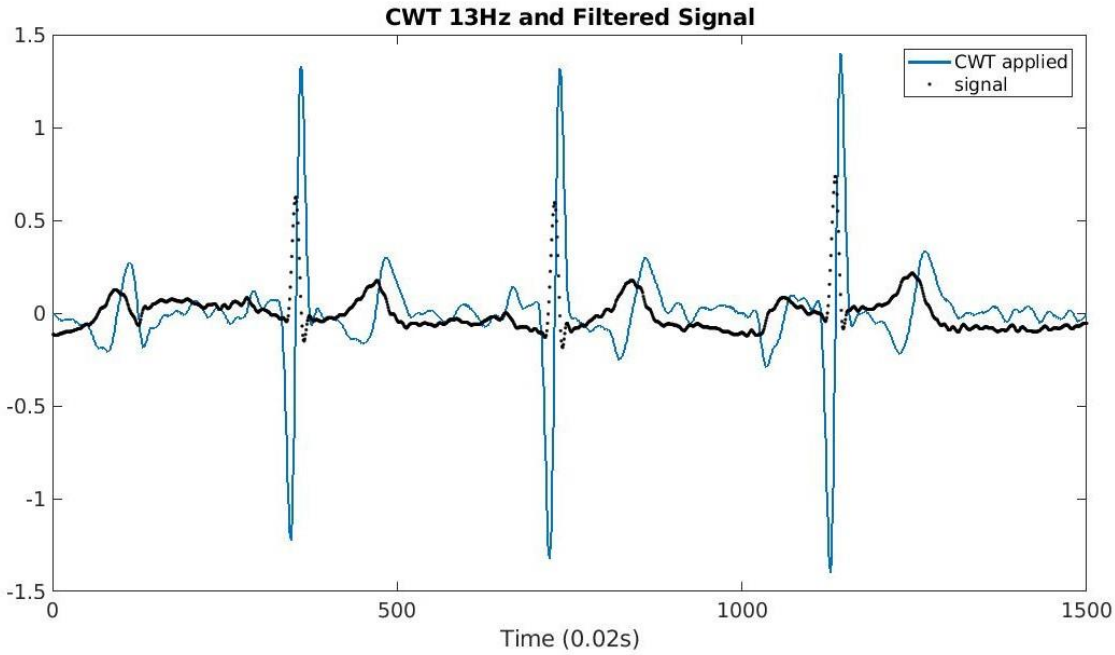


Figure 3.5 Amplified QRS

QRS detection [33]: A continuous wavelet transform is applied 13Hz with an inverse wavelet. The resultant spectrum is filtered again to remove any frequency component below 30 Hz. This amplifies the QRS complex removes all the low-frequency components.

$$S(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{+\infty} x(t)\Psi^* \left(\frac{t-b}{a}\right) dt$$

Where Ψ^* is the complex conjugate of the inverse wavelet function, and a dilation parameter and b the location of the wavelet. This operation amplifies the QRS complex and attenuates the P and the T wave. As shown in figure 3.5

After CWT, we perform a fast wavelet transform (FWT) is used remove all the frequency components below 30 Hz by making all the corresponding coefficients zero. Another round of filtration leaves us with a signal which only has the QRS complex. The diagram below shows the transformations and the result for a sample ECG wave.

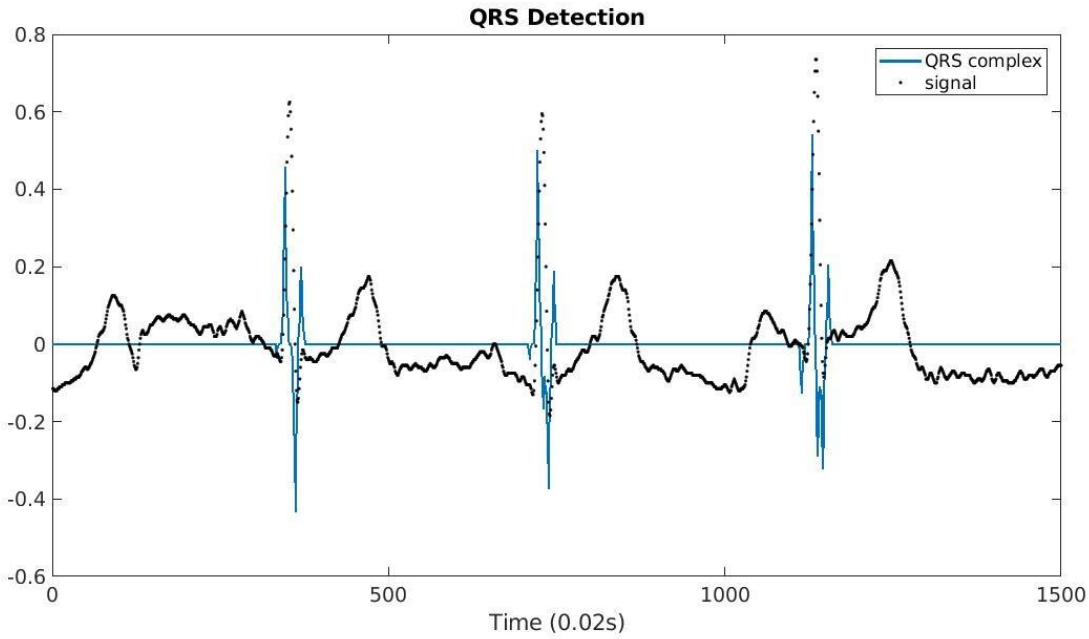


Figure 3.6 QRS identification result

Figure 3.6 shows the reconstructed signal from the filtration. It has non-zero values at the location of QRS complex and zeroes everywhere else.

P and T wave detection: After calculating the positions of the QRS signal the signal is segmented between R-R intervals. An R-R interval has precisely one T wave for the depolarization of the ventricles followed by a single P wave for the polarization and depolarization of the atriums. A transformation using CWT with a 3Hz inverse wavelet gives a spectrum with min and max values corresponding to the T wave boundary. The

peak is then identified as the highest voltage between this limit. Similarly, a transformation using 9Hz inverse wavelet identifies the P wave.

Now that we have the locations of the Q, R, S points on the signal. The next stage is the detection of the T wave. Considering the most extended possible duration of the T wave, it can be analyzed by CWT at the 3 Hz frequency. The peak of the T wave is shown as zero in the CWT spectrum, and the min and max values correspond to the beginning and end respectively. A similar thing is done to extract the P waves at 9Hz. The following figure shows the original signal with all the labels. Figure 3.7 shows all the annotated points on the filtered signal for sour subjects.

Features: The feature extraction process for both fiducial point based and non-fiducial point based methods is same till the QRS detection. In the non-fiducial point-based features we need to isolate individual cardiac cycles. The following section gives details about the features extracted in both scenarios.

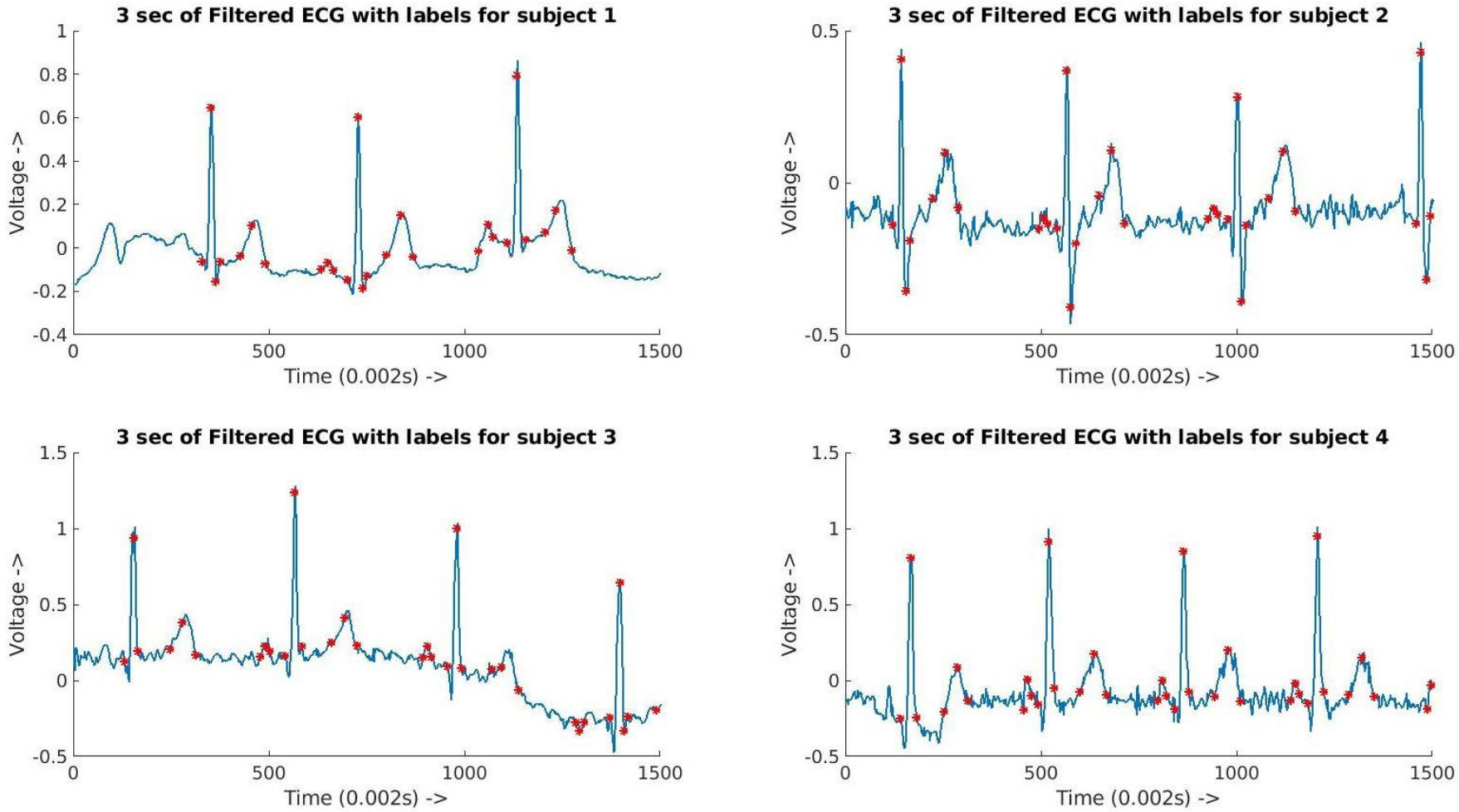


Figure 3.7 Annotation results

3.3 Fiducial points based vs. non-fiducial point-based features

Israel et al. [22] showed successful identification using a set of 15 temporal features. They proposed that the temporal distance between fiducial points, as shown in figure 3.8 below, is the time it takes for the ions to move from one place to the other (atriums to ventricles or vice versa). The time taken by the ions to move inversely proportional to the distance which ultimately makes the temporal features a function of the physiological properties of the heart. A significant advantage of this approach is the extracted features are agnostic of the mental state of the person.

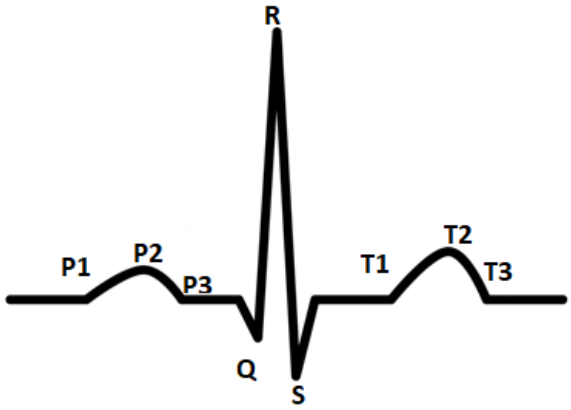


Figure 3.8 Identified fiducial points on the ECG

Following the above-mentioned method, the number the following features are extracted:

1. R-Q
2. S-R
3. R-P2
4. R-P1
5. R-P3
6. T2-R
7. T1-R
8. T3-R
9. P3-P1
10. T3-T1
11. T2-S
12. Q-P2
13. T2-P2
14. Q-P1
15. T3-S

All the fifteen values are non-negative and are normalized by dividing each value by the length of the entire beat T3-P1 and clamped to a 16-bit value. The normalization steps also make the features independent of the heartbeat as shown in [22]. This set of 15 16-bit values constitute the feature vector for an individual.

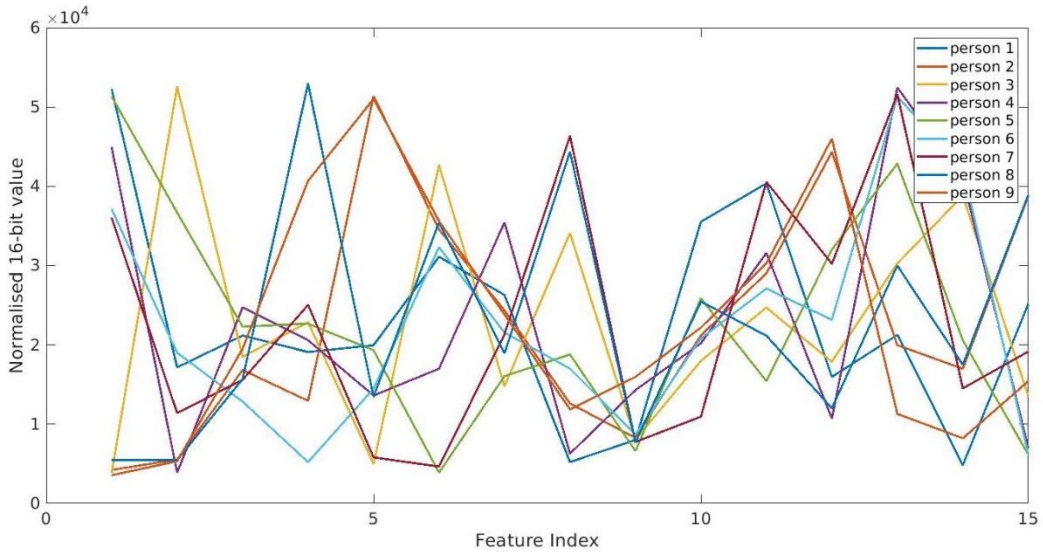


Figure 3.9 Parallel coordinates plot of feature templates from six individuals

The mean feature vector extracted from six different individuals is shown as a parallel coordinate plot in figure 3.9. Since none of the lines overlap, it shows that these feature vectors could be used as for identifying a specific person.

For the non-fiducial point-based approach, we need to isolate individual cardiac cycles from the original signal. As the signal contains repetition of the cardiac cycle isolating them improves the feature extraction. Any cardiac cycle starts with the P wave followed by the QRS complex and at the end the T wave. Straightforward partitioning of the signal between the start of P wave and at the end of the T wave results in a set of samples that vary in length. A linear interpolation of these isolated beats leads to too much

variation in the wave. To resolve this problem, we center the isolated wave around R by taking the maximum of the difference between T3R and RP1 and taking that many samples around R. As the QRS complex is the most distinct portion of the heartbeat this approach generates fixed size signal template consistent for an individual.

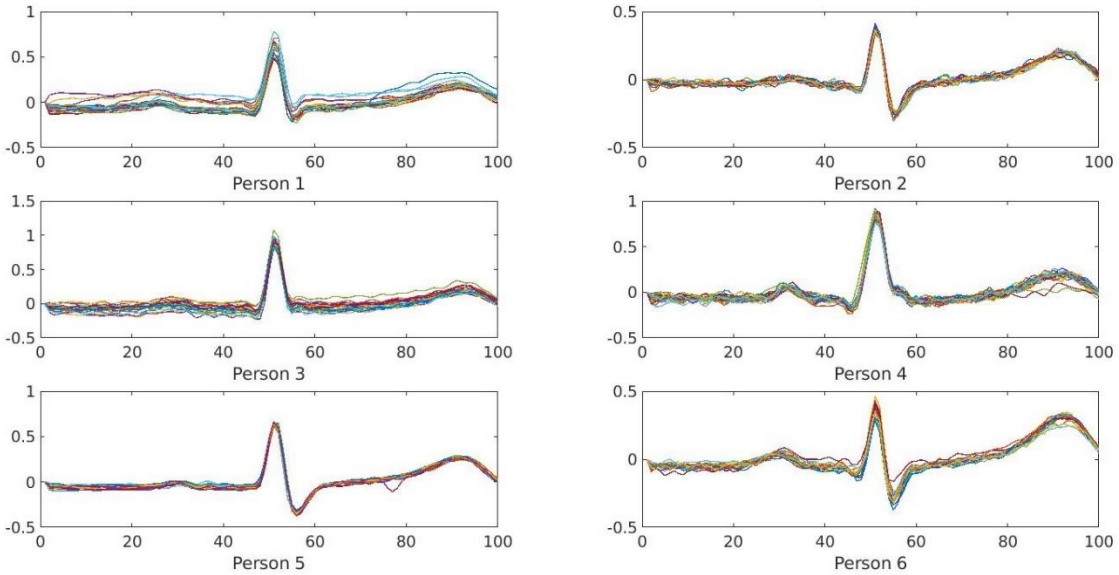


Figure 3.10 Non-fiducial point based feature template for six people.

Figure 3.10 shows the translated individual beats for six individuals. The beat in downsampled to a vector of size 100 and as evident from the plot the wave of a cardiac cycle does not change for an individual, and it is unique. In the following section, we analyze the consistency and the uniqueness of these features using histogram plots. This vector of size 100 is used as a feature vector.

3.4 Analysis

For an accurate authentication or identification, we want the features from the same individual to be as consistent as possible and as different as possible from others.

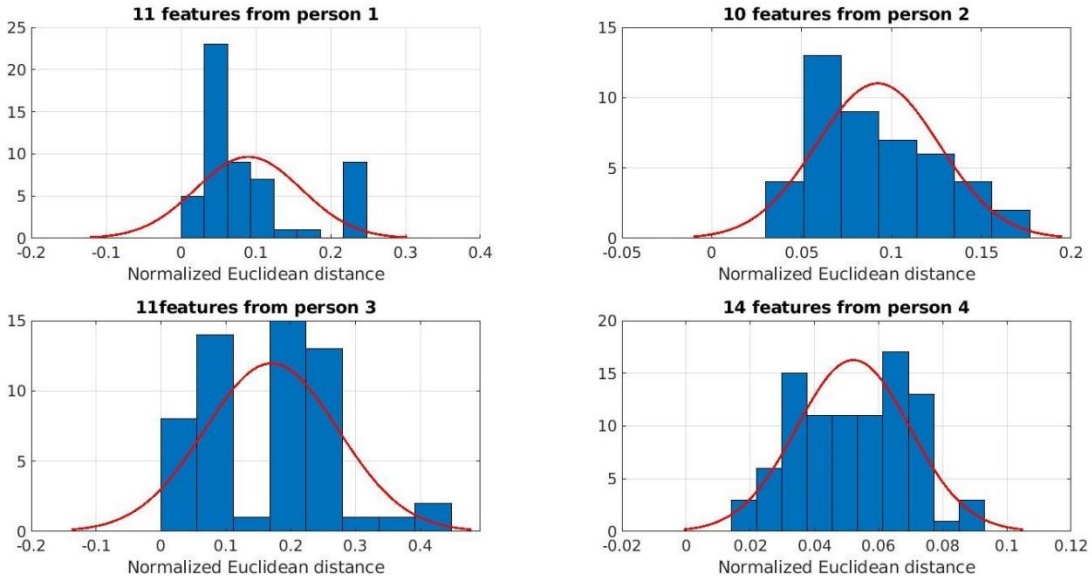


Figure 3.11 Histogram plot of pairwise distance between the features of the same individual for six people.

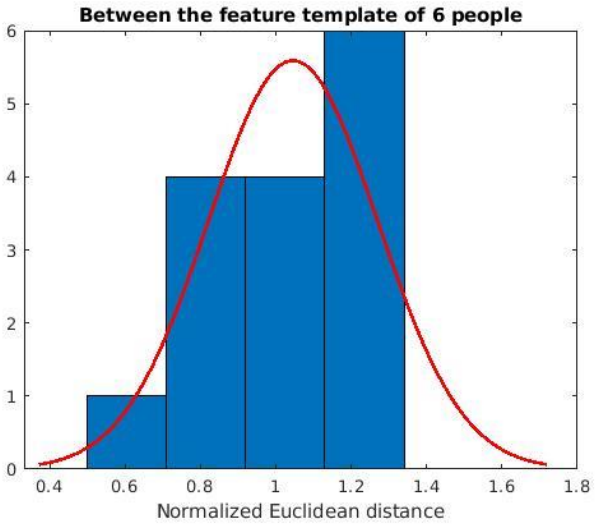


Figure 3.12 Histogram plot done between the feature template of different people.

The mean normalized Euclidean distance between features from the same individual is between 0 and 0.2 calculated for 40 people. Figure 3.11 shows a histogram plot of the first four subjects. The same distance among the feature templates of 30 people was found between 0.6 and 1.0 as shown in figure 3.12. Although more samples will result in a better analysis this group of 40 people shows that the extracted features are unique and consistent enough for an authentication system.

Although the non-fiducial based approach is less computationally intensive, it generates a lot more features. The excess number of features translates to more number of messages in the authentication, and more messages come at the increased cost of power. The following chapter presents an authentication protocol based on a privacy-preserving set intersection protocol by Amar et al. [34].

CHAPTER IV

AUTHENTICATION PROTOCOL

4.1 Introduction

This section presents the next half of the work in which the extracted features from ECG are used to authenticate the user. In the context of IoT, a Body Area Network (BAN) is a wireless network of wearable devices or physiological sensors. BANs have been proposed to provide real-time health information for the user through wearable or embedded sensors. They offer quicker diagnostics, granular health information by tracking movements, sleep patterns, eating habits, etc. In 2015, Gia, Tuan Nguyen, et al. propose the idea of fog computing in healthcare systems [35]. The idea is that the data collected by BAN's gets processed by a network edge, typically a smartphone for processing the data and to the cloud for synchronization. The middle tier devices like the smartphone are not as resource constrained as they used to be, hence having them process the stream of data from the sensors would result in faster results and reduced the load on the cloud.

In 2016, Yeh et al. introduce a secure IoT based health care system which operates through BSN (Body Sensor Network) architecture [36]. The proposed system is designed to work with public communication infrastructure and uses robust crypto-primitives to ensure transmission confidentiality and entity authentication of devices in all three layers of the device stack. It is pointed out that the security approach must be IoT specific for optimal performance as the existing security measures work best for high-level traffic

through the internet. Ex. Firewalls were containing management control protocols which do not work for end devices.

Luk et al. [9] propose a list of seven desired seven properties in a network broadcast authentication. It is also claimed that none of the existing network broadcast authentication strategies has all seven of these fundamental properties.

1. Resilience against node compromise: Isolating a compromised node. One of the solutions is Asymmetric authentication.

2. Low computation overhead: Since we are dealing with sensor nodes, typically they are computationally constrained. The authentication scheme has to be aware of this.

3. Low communication overhead: This talks about the sensor nodes being power constrained as radio signals consume a lot of power and an authentication scheme with very high MAC would become impractical.

4. Robustness to packet loss: This is a network problem which could also be the work of an attacker. The man in the middle attack.

5. Immediate authentication: Some sensor network applications require instant validity as it may contain critical information which should not be delayed. This is an application constraint.

6. Messages sent at irregular times

7. High message entropy.

In the following sections, an authentication mechanism is demonstrated which satisfies all the criteria.

4.2 Privacy-preserving set intersection protocol

Privacy-preserving set intersection protocols are algorithms that involve two systems holding a set of inputs and want to compute a set intersection of their inputs without revealing the inputs to each other. Consider a two people A, B each having X, Y amount of money respectively. They want to know who is more prosperous but don't want to reveal their net worth. To do this calculation, they would have to use privacy preserving operation on their private values and obtain the result for themselves. These algorithms are based on the work done by Yao [37] for secure computations on data sets.

Oblivious transfer (OT) is cryptographic primitive where a sender sends one out of many inputs to the receiver but remains oblivious as to which inputs are transferred. A more practical flavor OT is the 1-2 oblivious transfer proposed by Even et al. in [38]. In this method, the sender sends two values to the receiver each with a probability of ½ of transferring.

Amar et al. [34] proposed a set intersection protocol that enables two agents to jointly compute the Hamming distance between their keys without revealing the actual keys, the distributed set intersection protocol. The protocol utilizes secure hamming distance computation from oblivious transfer to compute a joint set between two system's input datasets of length n. The proposed protocol achieves full security in the semi-honest model and preserves the privacy of the input data set. The approach combines hamming distance and oblivious transfer technique.

4.3 Proposed algorithm

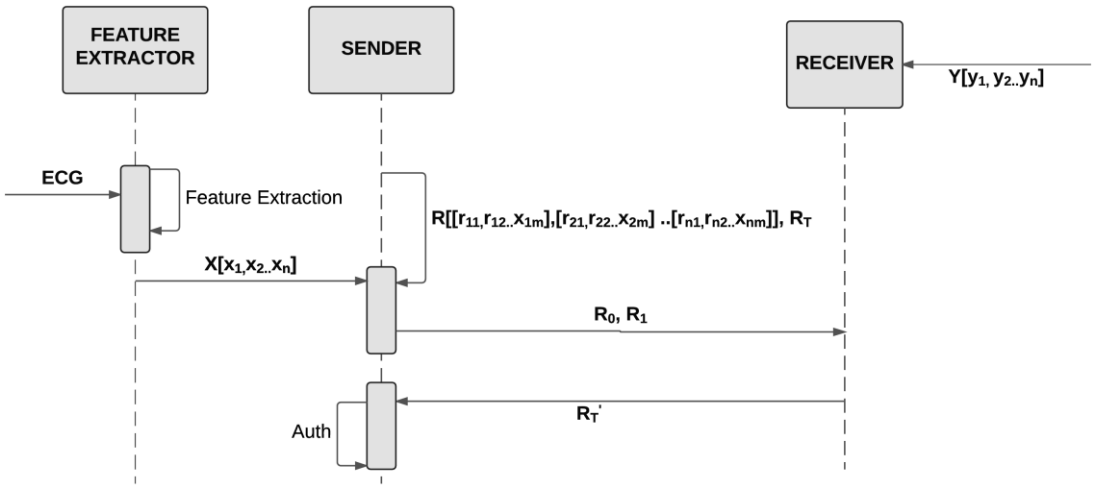


Figure 4.1 Distributed Set Intersection flow.

In this section, the algorithm for authentication is described as shown in figure 4.1. Let's consider two entities R *and* S for receiver and sender respectively where the sender gets the ECG signal and extracts the feature vector in real-time. The receiver R has a feature vector of m-bit values, and size n, Y= $[y_1, y_2 .. y_n]$ and the sender has extracts a feature vector of similar dimensions X= $[x_1, x_2 .. x_n]$. We want to calculate how similar is X to Y without revealing any part of X to the receiver and Y to the sender and the result of that computation tells us if the sender is the valid user or not.

The algorithm in [34] outputs a hamming distance between X and Y. Hamming distance between two vectors only gives the information about the number of bit-positions the value is different between them. A difference in the bit value of the most significant bit (MSB) or least significant bit (LSB) has no consequence on the result. This would suffice when we try to match exact vectors, but as ECG is a real-time, the feature values

remain close to each other but never the same. This results in a not so ideal scenario of lower false negatives and higher true negatives hence that algorithm cannot be used as it is. The following paragraph shows the modification which returns a weighted Hamming distance measurement.

The algorithm has three phases, in the first phase the sender S generates a set R with $n * m$, m-bit random values such that

$$R = [[r_{11}, r_{12}..r_{1m}], [r_{21}, r_{22}..r_{2m}]..[r_{n1}, r_{n2}..r_{nm}]]$$

and the key R_K is calculated by

$$R_K = \sum_{i=1}^{n}\sum_{j=1}^{m} r_{ij}$$

Next step is garbling the bits of X into two matrices the R_0 and R_1 such that

$$R_0 = \{R\colon \forall r_{i,j} \in R,\ r_{ij} = (r_{ij} + (x_i\ AND\ (1 \ll j - 1)))\}$$

$$R_1 = \{R\colon \forall r_{i,j} \in R,\ r_{ij} = (r_{ij} + (\bar{x_i}\ AND\ (1 \ll j - 1)))\}$$

Where $i \in [1, n]$, and $j \in [1, m]$. The sender sends these garbled values to the receiver followed by the R_K and the first phase of the protocol concludes. The original protocol only adds the bit x_i to the LSB position of r_{ij} and does not consider the significance of the bits. In the second phase of the algorithm, the receiver on receiving R_0 and R_1 calculates a R'_K by:

$$R'_K = \sum_{i=1}^{n}\sum_{j=1}^{m} \begin{cases} R_{0ij} \oplus y_i\ AND\ (1 \ll j - 1), & if\ \ 0 = \left(y_i\ AND\ (1 \ll j - 1)\right) \\ R_{1ij} \oplus y_i\ AND\ (1 \ll j - 1), & if\ 1 = \left(y_i\ AND\ (1 \ll j - 1)\right) \end{cases}$$

This step essentially calculates $\left(r_{ij} + \left(y_{ij} \oplus x_{ij}\right)\right)$, where y_{ij}, x_{ij} are j^{th} position bits of the i^{th} value in the set Y and X respectively. If the bits are same, the correct random

value gets added else an increased value corresponding to the significance of the bit is added to key R'_K.

The last phase of the protocol is a simple step of comparing the key to the calculated key at the receiver. If the difference of between them is less than a certain threshold, then the sender is genuine.

$$Auth = \begin{cases} 1, & (R'_K - R_K < thresh) \\ 0, & otherwise \end{cases}$$

The receiver can authenticate the sender without any actual exchange of keys. In the following sections, we experiment with ECG data from 40 different individuals and find the ideal threshold to get the highest accuracy. A comparison of the accuracy using the original protocol is also presented.

4.4 Security analysis

In this section, we analyze how the proposed algorithm measures up to the list of requirements of a sensor network authentication.

1. Resilience: The authentication is not based on any key hence if a node is compromised it does not affect the other nodes.
2. Low computation overhead: The complexity if the algorithm is O(n) where n is the number of bits of the feature vector. The most demanding step is the calculation of the garbled data (R_0, R_1).
3. Low communication overhead: The message complexity is also similar to the time complexity of the algorithm and is linearly dependent on the number of bits in the feature vector.

4. Robustness to packet loss: Although packet loss in phase 2 of the algorithm would lead to a false rejection the low computation overhead of the system allows for a restart again. This in conjunction with a real-time ECG signal makes the authentication robust to packet loss.
5. Immediate authentication: Once the algorithm concludes the results are valid for the next set of features arrive from the ECG feature extraction module. The algorithm does not have any delay modules and would be able to authenticate as soon as it receives all the messages. The only part where delay could be introduced is the communication channel.
6. Message sent at irregular times: If all the messages arrive at the receiver the receiver should be able to run the authentication algorithm. The order of messages does not matter.
7. High message entropy: For every authentication cycle the ender calculates a new set R and the values from ECG are never the same as well. This increases the entropy of the messages in the system.

CHAPTER V

SIMULATION

5.1 Overview

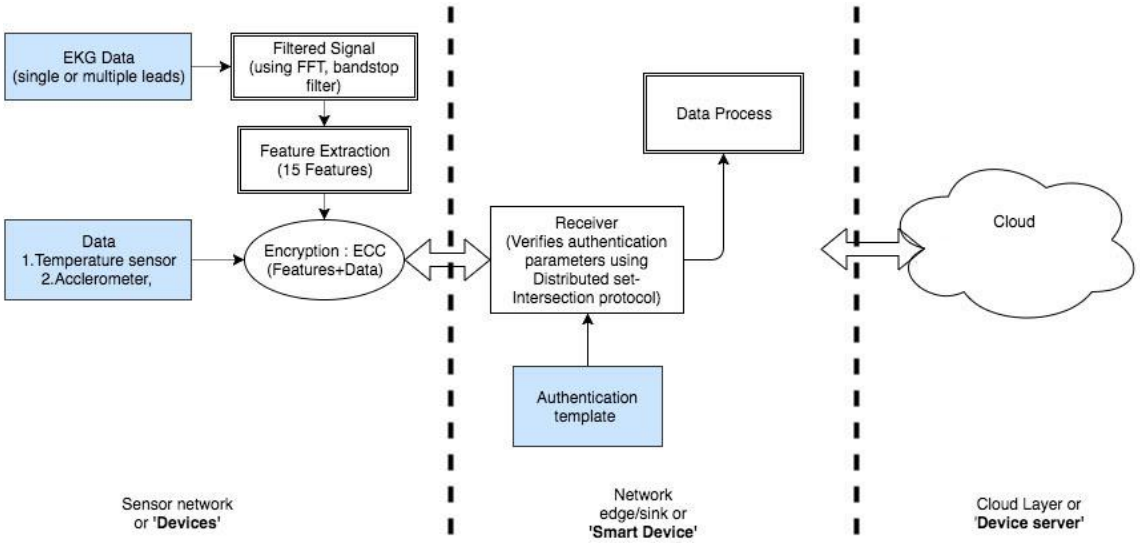


Figure 5.1 Overview of the simulation

In this section, the simulation is described for testing the proposed feature extraction techniques and the authentication protocol. Figure 5.1 shows the flow of information from sensors to the smart device. The ECG data is read from a file and partitioned into 3 sec worth of samples. From an empirical constant of the min bpm 20 beats per minute, a 3 sec ECG wave will have at least one cardiac cycle. This three second of the signal is then filtered and passed to a feature extractor module which extracts the feature vector and initiated the communication protocol. The garbled data is transmitted the to the receiver with a message id. The message id and the key remain valid the next three seconds. If the receiver computed key is received back from the receiver, and the

weighted hamming distance is less than the threshold, then the receiver is authenticated. Otherwise, the authentication failed.

5.2 Omnetpp

For the network simulation, the Omnetpp network simulator was used. It is an open source and generic discrete event simulation environment. It has proven to be useful in numerous domains from queuing network simulations to wireless and ad-hoc network simulations, from business process simulation to peer-to-peer network, optical switch and storage area network simulations. The main advantage of using Omnetpp is that it abstracts out the underlying infrastructure and allows us to focus on the main problem. It's based on C++ and allows for fine-grained control of the entire system.

Figure 5.2 Device model in Omnetpp

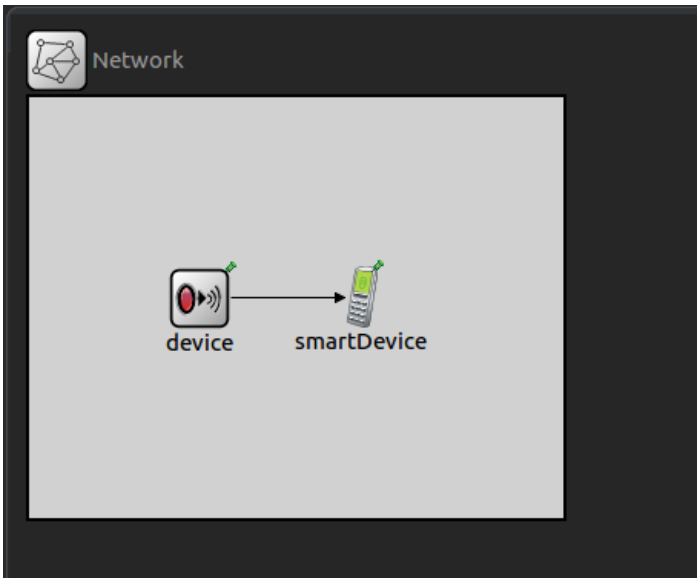


Figure 5.3 Simple network model in Omnetpp

We model two device categories the sensor which collects the ECG and other physiological data and the smart device. Figure 5.2 shows the model of the device. The subcomponents in the device model are made for implementation simplicity. Figure 5.3 shows a simple network model where a device is connected to a smart device. Every device type object is linked to a binary file which has the ECG data. The smart device is also linked to an ECG data file and can accept multiple input connections and queues the messages for processing.

5.3 Physionet database

For the simulation of the ECG signals, we will use the ‘mit-bh’ and ‘ecgid’ databases from www.physionet.org. PhysioBank hosted within physionet.org is a large and growing archive of well-characterized digital recordings of physiological signals and related data for use by the biomedical research community.

The data from Physionet is stored in a binary format to save space. A C++ wrapper was developed with the Omnetpp to extract the files from the binary files. The testing was done on ECG collected for 40 different people. Every person has at least two 20 seconds recordings.

5.4 Experiments

To calculate the accuracy of the system in authenticating the people, two experimental configurations were used one to calculate the false acceptance ratio (FAR) and false rejection ratio (FRR) and another configuration to calculate the true acceptance rate (TAR) and true rejection rate (TRR). The false acceptance ratio is the ratio between the number of people who were wrongly identified and the total number of authentication requests. FRR or false rejection ratio is the inverse of FAR that is the total number of people correctly denied authentication vs. the total number of authentication requests. TAR is the measure of people who were authenticated successfully, and TRR is the ratio between the number of people incorrectly denied access.

A good authentication system should have high TAR, FRR, and low TRR and FAR. These ratios depend on the threshold value used in the last step of the authentication protocol. The following experimental setups are designed to calculate these ratios at different threshold values, and the results of the experiment would tell us the accuracy of the system.

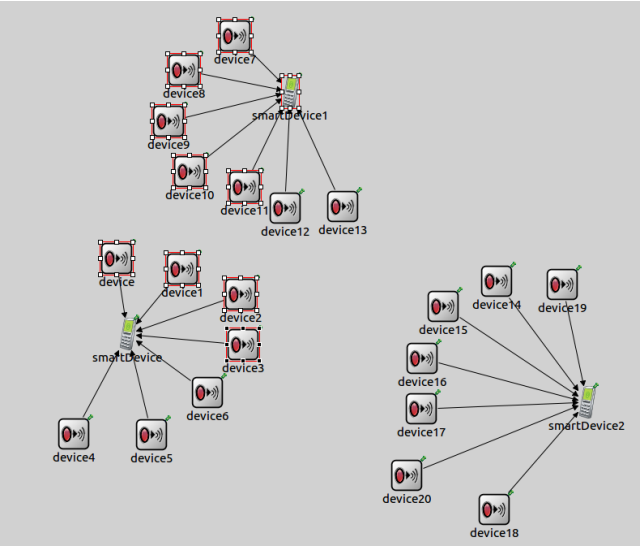


Figure 5.4 Network model for testing FAR and FRR

To measure the FAR and FRR we connect multiple devices to the smart device and make sure that none of them are linked to the same ECG file as shown in figure 5.4. The TAR and TRR can be tested with a relatively simpler network in which every smart device is connected to a device, and both are linked to the same ECG file. Both these configurations were tested with the algorithm proposed, and the distributed set intersection protocol and the following chapter shows the results.

CHAPTER VI

CONCLUSION AND RESULTS

6.1 Simulation Results

This section presents the results calculated by simulating the fiducial point based technique for feature extraction of ECG and the authentication protocol which outputs the weighted hamming distance. The results from the simulation of the original Distributed Set Intersection Protocol (DSIP) is also presented as a comparison to the proposed protocol.

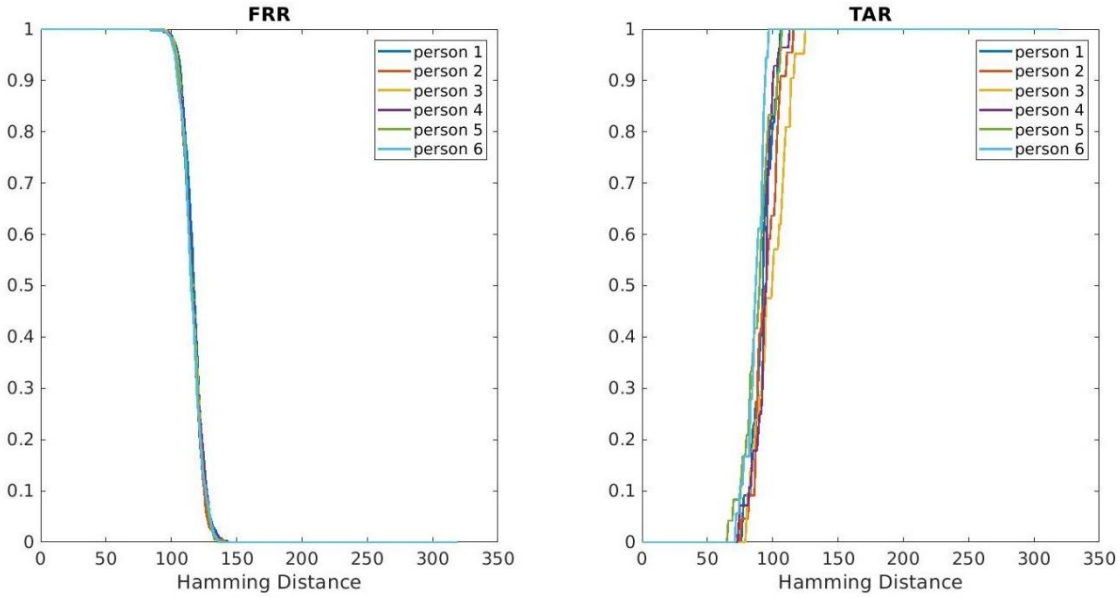


Figure 6.1 FRR and TAR using DSIP

Figure 6.1 shows the hamming distance vs. the false negatives on the left and hamming distance vs. true positives on the right for six different individuals. The ideal

value of the hamming distance would maximize both TAR and FRR, and from the plots, we can see that it would be somewhere between 50 and 150

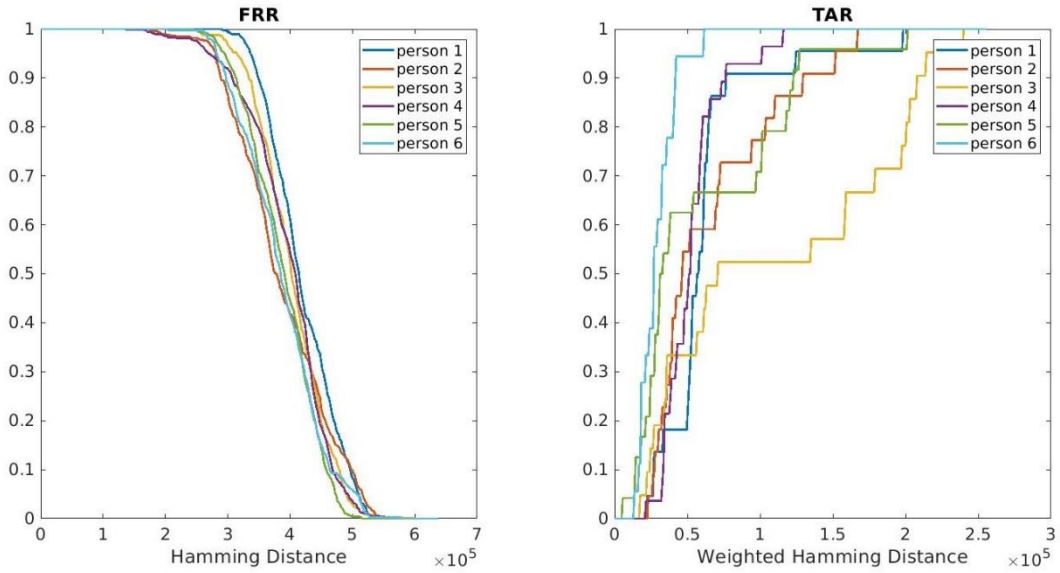


Figure 6.2 FRR and TAR using modified DSIP

As the previous figure, figure 6.2 shows FRR (left) and TAR (right) with weighted hamming distance obtained from the modified protocol. This plot indicates an ideal threshold value somewhere between 50000 to 300000.

To calculate both the ideal threshold of the hamming distance and the weighted hamming distance we calculate the FRR, FAR, TRR, TAR for all the feature vectors from all the 40 individuals. For every individual, we have two records worth 10 seconds each which means ~160 feature vectors considering a mean of 60 beats per minute (BPM) which results in total number of authentications ~20000

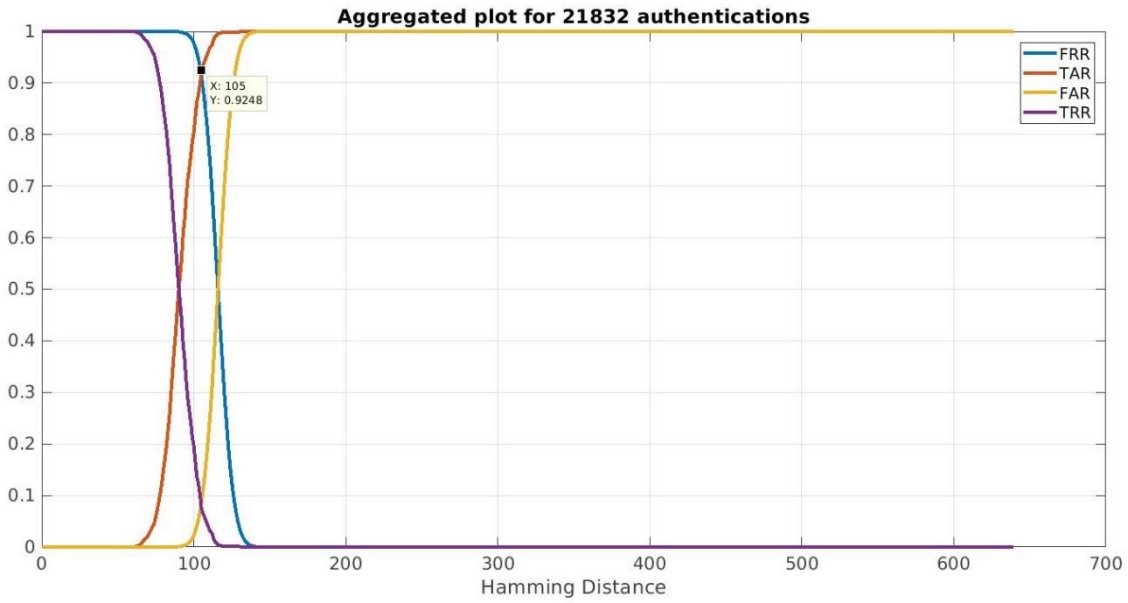


Figure 6.3 Aggregated plot with hamming distance using DSIP

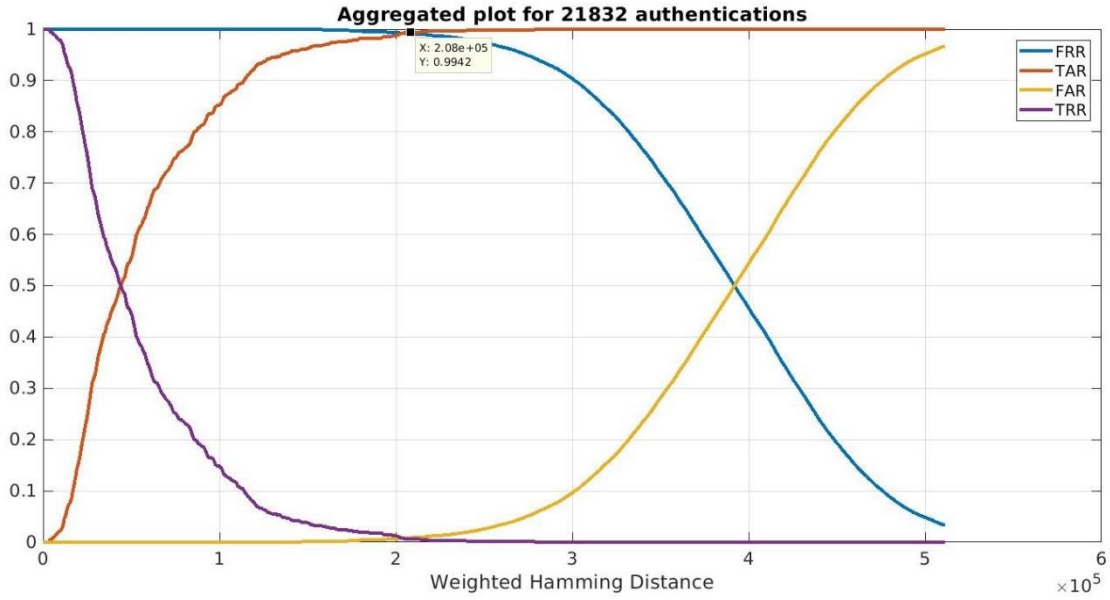


Figure 6.4 Aggregated plot with secured hamming distance using the proposed algorithm

Figure 6.3 and 6.4 showed the aggregated plots of TAR, TRR, FAR, FRR for 21832 authentication attempts vs. hamming distance and weighted hamming distance respectively. From figure 6.3 the ideal threshold hamming distance is calculated at 106, and the accuracy of the protocol using that threshold value is given by:

$$\text{Accuracy} = \frac{true\ positives + false\ negative}{true\ positives + false\ negatives + true\ negatives + false\ positives}$$

Here $(true\ positives + false\ negatives)$ are the correct results with true positives indicating a correct person rightfully granted access and the false negatives indicating the wrong person rightfully denied access divided by the all the total results.

For hamming distance=106, accuracy=91.2%

Similarly, for the weighted hamming distance case, the ideal threshold is found at 203200

For weighted hamming distance=203200, accuracy=99.2%

This shows the advantage of the modified protocol which has a gain of ~8% in accuracy. Now, we check the individual accuracy for the 40 subjects at the calculated threshold to see the spread. Ideally, the accuracy for an individual should not vary at all otherwise it would mean that the algorithm works only for a certain set of individuals and lose generality. The following plots give an idea about the spread of the accuracy using both hamming and weighted hamming distance.

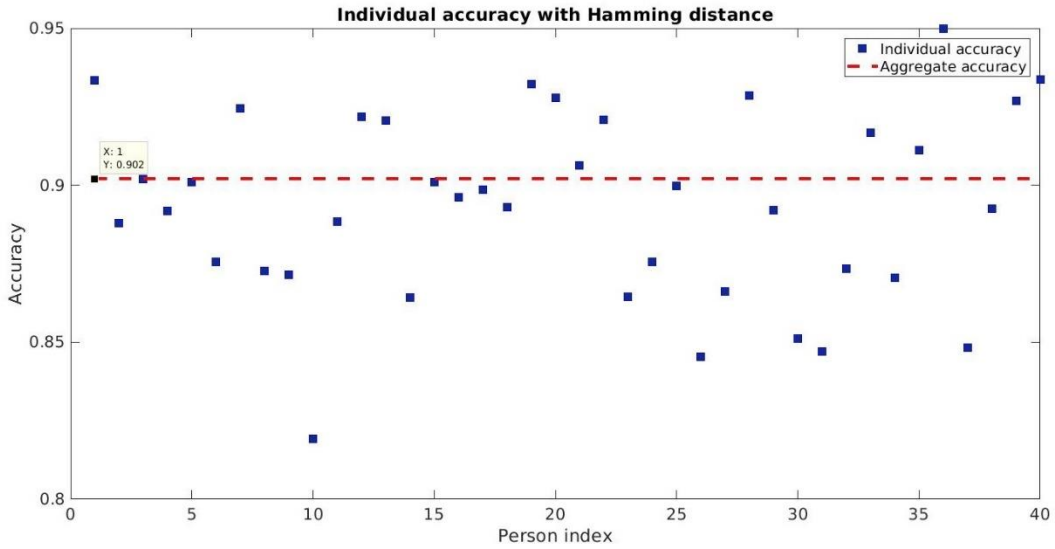


Figure 6.5 Accuracy vs. person index for DSIP

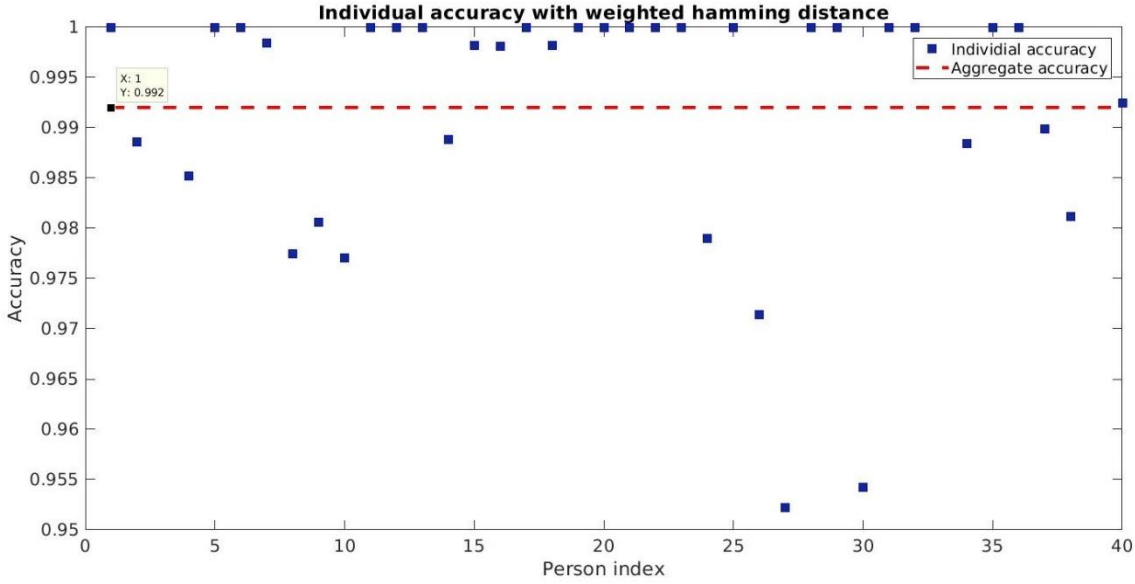


Figure 6.6 Accuracy vs. person index for the proposed protocol

Figure 6.5 and 6.6 showed the spread of the accuracy using the Hamming distance from the DSIP and weighted hamming distance from the proposed protocol respectively. In figure 6.5, showing the hamming distance approach, the accuracy varies between 0.82-

1.0 and the mean as indicated by the red line at 0.91. For figure 6.6 the accuracy between 0.95-1.0 with the mean at 0.992. This shows that the results are consistent across individuals with irrespective of the protocol being used.

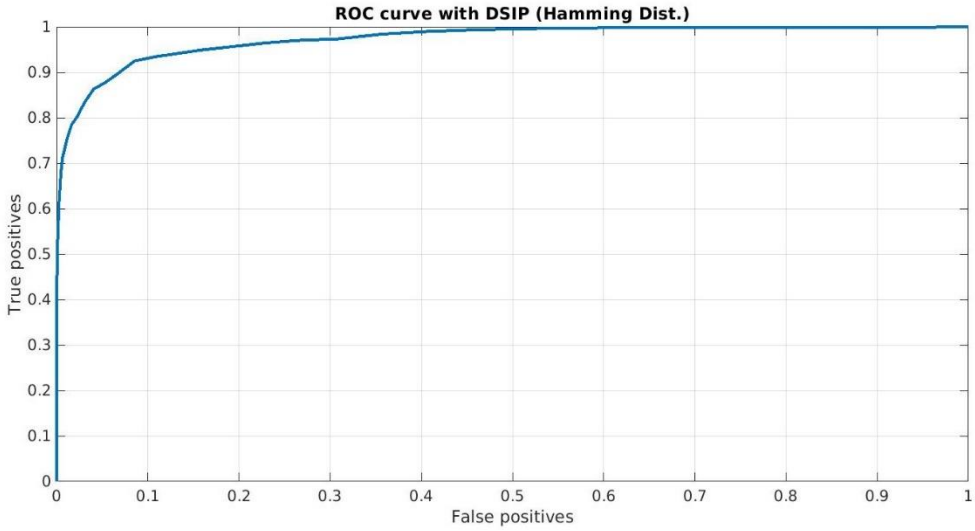


Figure 6.7 Receiver operating characteristics for DSIP

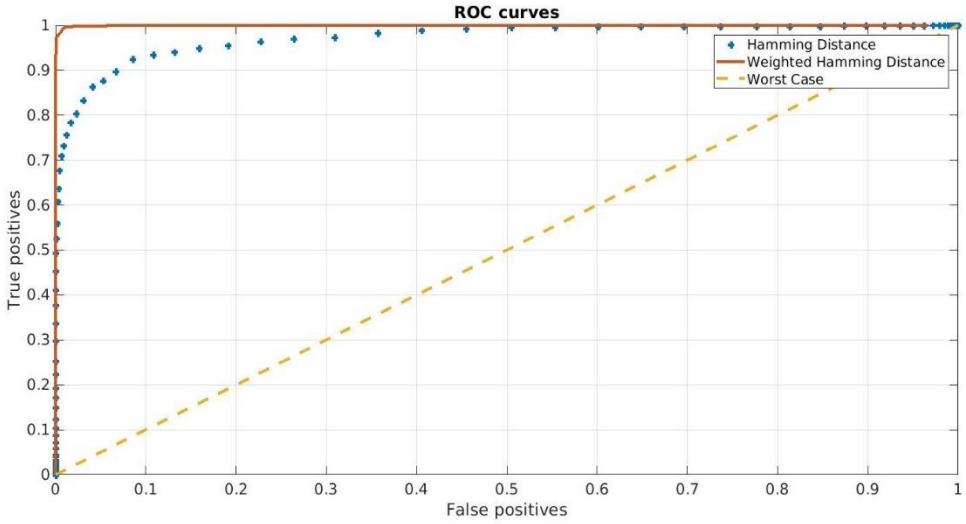


Figure 6.8 Receiver operating characteristics for modified DSIP

Another plot that shows the accuracy of the system is the Receiver operating characteristics curve or the (ROC). The ROC plot was historically used in radar to indicate the performance of radar to successfully identify the target object. The ROC plots the number of true positives per every false positive at different thresholds. Figure 6.7 shows the ROC curves for both the original DSIP protocol and figure 6.8 shows the modified DSIP. A straight line (y=x) indicate that the system is essentially guessing and the number of false positives = number of true positives. As expected from above the figure shows that the modified DSIP offers more accuracy without any extra computational overhead.

6.2 Conclusion

The presented work is a complete end-to-end authentication system between the bottom and middle tier of the IoT ecosystem particularly wireless body sensor networks. All the steps including filtration, feature extraction, and the authentication protocol are covered. It shows the potential of using ECG signal for biometric authentication data in the context of sensor networks.

As discussed, the temporal features extracted from the fiducial points provide a smaller set of unique features than any non-fiducial point based method. The experiments also indicate that the fiducial point based features were more accurate as they had relatively high Signal to Noise Ratio (SNR) compared to the non-fiducial point based method. However, this comes at the cost of computational complexity of detecting the fiducial points. Due to the non-stationary nature of ECG using CWT for detecting the fiducial point gives robust and accurate results as continuous wavelet transform gives good

time resolution and poor frequency resolution at higher frequencies and vice-versa. The computational complexity of CWT is $O(n^2)$, where n is the number of samples being processed, it is still manageable in the computationally constrained sensors as n is very small. The minimum sampling rate for an ECG is 150 Hz which puts n in the order of 450 for 3 seconds or 1 cardiac cycle. Moreover, with new developments in the wearable sensor space, the sensors are not as resource constrained as they used to be.

The proposed protocol offers privacy preserving and secure set intersection calculation which could be used with ECG features to authenticate. The modification of the algorithm has no overhead regarding computational complexity or message complexity but improves the accuracy of the system. Also, the algorithm is generic and could be used where just the Hamming distance between the set does not provide a good measure of the distance between the sets.

The entire proposed scheme is deployable on a wireless body sensor network with an ECG sensor, and any wireless medium with sufficiently low loss rate like Bluetooth, Internet Protocol (IP) based like the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), etc. Depending on the type of the application the presented scheme could be integrated with other forms of identification methods like an accelerometer-based to detect gait etc. to get a multi-modal authentication scheme for stronger guarantees.

REFERENCES

[1] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

[2] Hao, Yang, and Robert Foster. "Wireless body sensor networks for health-monitoring applications." Physiological measurement 29.11 (2008): R27.

[3] Lo, Benny PL, et al. "Body sensor network–a wireless sensor platform for pervasive healthcare monitoring." (2005): 77-80.

[4] "File:Body Area Network.jpg." Wikimedia Commons, the free media repository. 1 Jun 2014, 03:15 UTC. 22 Oct 2017, 23:01 <https://commons.wikimedia.org/w/index.php?title=File:Body_Area_Network.jpg&oldid=125447087>.

[5] Zebboudj, Sofia, et al. "Secure and efficient ECG-based authentication scheme for medical body area sensor networks." Smart Health (2017).

[6] Masdari, Mohammad, and Safiyyeh Ahmadzadeh. "A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems." Journal of Network and Computer Applications 87 (2017): 1-19.

[7] Wayman, James, et al. "An introduction to biometric authentication systems." Biometric Systems (2005): 1-20.

[8] Patel, Shyamal, et al. "A review of wearable sensors and systems with application in rehabilitation." Journal of neuroengineering and rehabilitation 9.1 (2012): 21.

[9] Luk, Mark, Adrian Perrig, and Bram Whillock. "Seven cardinal properties of sensor network broadcast authentication." Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks. ACM, 2006.

[10] Juels, Ari, and Madhu Sudan. "A fuzzy vault scheme." Designs, Codes and Cryptography 38.2 (2006): 237-257.

[11] Nandakumar, Karthik, Anil K. Jain, and Sharath Pankanti. "Fingerprint-based fuzzy vault: Implementation and performance." IEEE transactions on information forensics and security 2.4 (2007): 744-757.

[12] H. Sellahewa, S. A. Jassim, "Image-quality-based adaptive face recognition", IEEE Trans. Instrum. Meas., vol. 59, no. 4, pp. 805-813, Apr. 2010.

[13] M. S. Hosseini, B. N. Araabi, H. Soltanian-Zadeh, "Pigment melanin: Pattern for iris recognition", IEEE Trans. Instrum. Meas., vol. 59, no. 4, pp. 792-804, Apr. 2010.

[14] J. Doi, M. Yamanaka, "Discrete finger and palmar feature extraction for personal authentication", IEEE Trans. Instrum. Meas., vol. 54, no. 6, pp. 2213-2219, Dec. 2005.

[15] S. Engelberg, Y. Saidoff, Y. Israeli, "Voice identification through spectral analysis", IEEE Instrum. Meas. Mag., vol. 9, no. 5, pp. 52-55, Oct. 2006.

[16] S. K. Dahel, Q. Xiao, "Accuracy performance analysis of multimodal biometrics", Proc. IEEE Syst. Man Cybern. Soc. Inf. Assurance Workshop, pp. 170-173, Jun. 2003.

[17] Wikipedia contributors. "Electrocardiography." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 22 Oct. 2017. Web. 23 Oct. 2017.

[18] "File:Diagram of the human heart (cropped).svg." Wikimedia Commons, the free media repository. 26 Apr 2016, 20:52 UTC. 22 Oct 2017, 23:59

<https://commons.wikimedia.org/w/index.php?title=File:Diagram_of_the_human_heart_(cropped).svg&oldid=194599161>.

[19] "File:SinusRhythmLabels.svg." Wikimedia Commons, the free media repository. 27 Sep 2017, 14:37 UTC. 23 Oct 2017, 00:02 <https://commons.wikimedia.org/w/index.php?title=File:SinusRhythmLabels.svg&oldid=260036882>.

[20] "File:Limb leads of EKG.png." Wikimedia Commons, the free media repository. 23 Nov 2016, 21:40 UTC. 23 Oct 2017, 00:03 <https://commons.wikimedia.org/w/index.php?title=File:Limb_leads_of_EKG.png&oldid=218319987>.

[21] Biel, Lena, et al. "ECG analysis: a new approach in human identification." IEEE Transactions on Instrumentation and Measurement 50.3 (2001): 808-812.

[22] Israel, Steven A., et al. "ECG to identify individuals." Pattern recognition 38.1 (2005): 133-142.

[23] Sriram, Janani C., et al. "Activity-aware ECG-based patient authentication for remote health monitoring." Proceedings of the 2009 international conference on Multimodal interfaces. ACM, 2009.

[24] (2013). Chaos Computer Club breaks Apple TouchID. [Online].Available: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[25] Arteaga-Falconi, Juan Sebastian, Hussein Al Osman, and Abdulmotaleb El Saddik. "ECG authentication for mobile devices." IEEE Transactions on Instrumentation and Measurement 65.3 (2016): 591-600.

[26] Zhang, Zhaoyang, et al. "ECG-cryptography and authentication in body area networks." IEEE Transactions on Information Technology in Biomedicine 16.6 (2012): 1070-1078.

[27] Hejazi, Maryamsadat, et al. "ECG biometric authentication based on non-fiducial approach using kernel methods." Digital Signal Processing 52 (2016): 72-86.

[28] Simon, Biju P., and C. Eswaran. "An ECG classifier designed using modified decision based neural networks." Computers and Biomedical Research 30.4 (1997): 257-272.

[29] Hussein, Ahmed F., et al. "An IoT Real-Time Biometric Authentication System Based on ECG Fiducial Extracted Features Using Discrete Cosine Transform." arXiv preprint arXiv:1708.08189 (2017).

[30] Plataniotis, Konstantinos N., Dimitrios Hatzinakos, and Jimmy KM Lee. "ECG biometric recognition without fiducial detection." Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the. IEEE, 2006.

[31] Yarong, Wang, and Zheng Gang. "Study of human identification by electrocardiography frequency features." International Symposium on Computers and Informatics (ISCI 2015). 2015.

[32] Tantawi, Manal M., et al. "A wavelet feature extraction method for electrocardiogram (ECG)-based biometric recognition." Signal, Image and Video Processing 9.6 (2015): 1271-1280.

[33] Chesnokov, Y. C., D. Nerukh, and R. C. Glen. "Individually adaptable automatic QT detector." Computers in Cardiology, 2006. IEEE, 2006.

[34] Rasheed, Amar, et al. "Private matching and set intersection computation in multi-agent and industrial control systems." Proceedings of the 12th Annual Conference on Cyber and Information Security Research. ACM, 2017.

[35] Gia, Tuan Nguyen, et al. "Fog computing in healthcare internet of things: A case study on ecg feature extraction." Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on. IEEE, 2015.

[36] Yeh, Kuo-Hui. "A Secure IoT-Based Healthcare System With Body Sensor Networks." IEEE Access 4 (2016): 10288-10299.

[37] Yao, Andrew C. "Protocols for secure computations." Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on. IEEE, 1982.

[38] Even, Shimon, Oded Goldreich, and Abraham Lempel. "A randomized protocol for signing contracts." Communications of the ACM 28.6 (1985): 637-647.