6-30-2016

Authentication in Wireless Body Area Networks (WBAN)

Nagalaxmi Yenuganti
University of South Florida, nagalaxmi.y1509@gmail.com

Authentication in Wireless Body Area Networks (WBAN)

by

Nagalaxmi Yenuganti

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Computer Science
Department of Computer Science and Engineering
College of Engineering
University of South Florida

Major Professor: Yao Liu, Ph.D.
Jay Ligatti, Ph.D.
Yicheng Tu, Ph.D.

Date of Approval:
May 26, 2016

Keywords: Sensors, Accelerometer, Smart Phones, FFT, Coherence

DEDICATION

I would like to dedicate this thesis to my family, along with my professors who have constantly been a great source of inspiration and support.

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my advisor Dr. Yao Liu for her support and guidance in my research. I would like to thank Dr. Yicheng Tu and Dr. Jay Ligatti for serving on my thesis defense committee. I appreciate their valuable feedback and review comments on this work. I would like to thank Mr. Hari Krishna Jonnalagadda for his contribution in developing accelerometer android app.

Finally, I would like to thank my department, all of my professors, and everybody who made this experience a very cherishing one.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

With the advancements in technology and computing environment capabilities, the number of devices that people carry has increased exponentially. This increase initially occurred as a result of necessity to monitor the human body condition due to chronic diseases, heart problems etc. Later, individuals' interest was drawn towards self-monitoring their physiology and health care. This is achieved by implanting various sensors that can proactively monitor the human body based on medical necessity and the health condition of the user. Sensors connected on a human body perceive phenomena such as locomotion or heartbeat, and act accordingly to form a Body Area Network. The primary concern of these sensors is to ensure a secure way of communication and coordination among the devices to form a flawless system. A secondary concern is wireless sensor authentication, which ensures trustworthiness and reliable gathering of a user's data. To address this concern, we designed a secure approach using low cost accelerometers to authenticate sensors in Body Area Networks.

To ensure authentication in on-body sensor networks, we need a mechanism which intuitively proves all the communicating nodes are trusted ones. In order to achieve sensor authentication, we used accelerometer data gathered from sensors to distinguish whether or not the devices are carried on waist of same individual's body. Our approach is focused at analyzing walking patterns recorded from smartphone accelerometers placed in the same location of the user's body, and we present results showing these sensors record similar pattern.

CHAPTER 1: INTRODUCTION

Internet of Things(IoT), the latest buzz word in this era, is a result of advancements in technology and the coupling of different technologies. It is expected by 2020, IoT will make a revenue of around $300 billion. Many software, product based and service based companies are coming forward to invest in the IoT market. Several other industries are also trying to make the most out of IoTs, one such industry being health care. Due to its ubiquity, it is fundamental to understand the fascinating term IoT. In simple words, IoT is a network of physical devices implanted with sensors, network connectivity, software programs, etc. with the goal of gathering, exchanging and analyzing data over the network. Wireless Body Area Networks (WBAN), which provides communication interface between the implanted sensors on human body, is also a part of IoT. In today's scenario, people of different age groups are coming forward to experience the advancements of the wearable devices which monitor blood pressure, blood glucose levels, heartbeat, sleeping patterns, etc. As the number of medical devices connected to the human body increases, so does the amount of clinical data they collect and collaborate. Collection of data from the sensors might be of no use, unless the data is analyzed to trigger reactive actions in emergency. Limited resources of on-body sensors, fail to analyze the data they sense. Data analysis is thus, delegated to the remote cloud services, who continuously analyze the data received from sensors to detect emergency, well ahead of time. This raised issues on concerning user trust, privacy and data security. Since the data is exchanged over the internet, security becomes a greater concern for the end users and the devices connected.

A security research team formed by Scott Erven stated in April 2014, after a two-year period of study, they could eavesdrop to a deeper level of health and security of the users. They concentrated on the activities like monitoring and controlling the dosage levels of drug infusion pumps and implanted defibrillators of a few users using medical devices connected through wireless medium. A patient with chronic disease, if treated with inappropriate drug dosage levels for a long time, might suffer from serious illness or even death in some cases. So one can imagine the importance of the security and trust of the wearable sensor devices. In order to gain the trust of the end user, manufacturer should ensure implanted devices on a user's body communicate with each other rather than with some random attacker. One way to do this is to establish secret key over a secure communication channel among the implanted devices on a patient's body. This produces the need to uniquely identify a communicating entity. We have existing mechanisms, like Universally Unique Identifier (UUID) or Unique Device Identifier (UDID), digital fingerprinting, MAC address, IP addresses and electronic serial number (ESN), which can act as unique identifiers. However, there are some limitations and tampering techniques of these identification mechanisms which make them highly vulnerable to attacks. Adding to the existing security concern, each of these identifiers can be easily modified using piece of software code [6], [7]. For example, UNIX operating system provides us with a unique command called "macchanger" which forges the MAC address of an Ethernet wireless device. As a result, using these existing fingerprinting techniques poses a serious threat and risk for the users of wireless body area networks.

Additionally, size of the sensors and front end electronics hindered the growth of the wearable technology ubiquitously in the past. As a result of advancements in sensor technology and miniaturization of circuitry, data processing and analysis, wearable sensors are widely used in

the recent times. However, authentication of the user is a major concern in wearable sensor technology. Most of the wearable sensors lack in high computational power and hardware support which makes the usage of existing cryptographic mechanisms difficult to accomplish authentication. So, there is a need to come up with some technique which is computationally low and easy to embed in these miniature devices.

Accelerometer, an inexpensive sensor and easy deployable device which is widely used in tracking and the classification of human daily activities [1], [2]. Recent study proved accelerometers can be used in detecting areas of human body affected by Parkinson disease. Another study claimed that low cost sensors can be used in designing a wearable sensor network for home monitoring system [5].

Given examples motivated us to investigate the methods to authenticate on-body wearable sensors with low cost accelerometers. Accelerometer sensor measures the acceleration of the device in two or three axial dimensions. In today's scenario most of the smart phones are embedded with sensors like accelerometer, gyroscope, magnetometer, light sensor, etc. Android platform provides with an interface which can monitor available hardware-based sensors like accelerometer and gyroscope in smartphones. An accelerometer app developed for an android mobile can be used to record acceleration versus time profile data. We then gathered accelerometer data from two different smartphones of similar make from different individuals. According to our expectation if the two smartphones are carried on nearby locations of body by a same person, the acceleration patterns recorded by them should be similar enough. Here are few aspects to be taken into consideration:

- Can accelerometer data provide us with reliable information to verify, whether the two sensors are carried by the same person?

- What is the best active motion of an individual to track the similarities in the profile data?

We present relevant answers for each of these questions and scenarios how placing of the smartphones affect the acceleration versus time patterns. From the recorded patterns we find the similarities among the two different patterns of an individual, and uniqueness of each pattern among the profiles of different individuals. In other words, the acceleration versus time profile of each individual would result in a unique pattern. This unique property of each acceleration versus time profile can be replicated from the walking motion of an individual. In order to get reliable patterns, we placed two smartphones side by side in a fanny bag worn on an individual's waist. We finally posed a scheme of authenticating sensors in Body Area Networks using acceleration versus time profiles.

CHAPTER 2: RELATED WORK

WBAN, consisting of miniature sensor devices provides novel health monitoring opportunity ranging from day-to-day activities to chronic diseases. Sensors accomplish monitoring activity by collecting and managing sensitive user information, then communicates with the base station in order to send the data to the respective health monitoring systems. Typically, communication in WBAN is categorized into three types: On-body, In-body and Off-Body communication. When the communication is among on-body sensors then it is known as On-body communication, In-body communication takes place between implanted devices and an external authorized equipment device. Off-body communication happens between a base station and a transceiver at user's end. Our concentration is on On-body communication of Wireless Body Area Networks. The deployment requirements of WBAN depends on the domain it is monitoring for, such as health monitoring WBAN needs to be very secure and avoid any malicious intervention activities. Compromised WBAN can lead to serious risks such as irrevocable condition or even death in some user cases. A WBAN is said to be secure if it ensures privacy, confidentiality, integrity and authentication. However, to provide a high-level security mechanism is a primary challenge to the system designers, due to limited power and infrastructure of the WBAN system. Authentication is a very crucial aspect in any network of communicating devices, especially in the areas where security compromise lead to serious level of damage. We mainly focus on the authentication of on-body nodes or sensor devices in the WBAN.

Authentication of nodes in the WBAN is of great concern. Suspicious node in WBAN can intercept the communication between the legitimate nodes, as a result compromising privacy of

the whole network. On this note, secure node and data authentication is crucial for user and WBAN security and privacy. Research interest so far on authentication mechanisms for WBAN can be divided into cryptographic and non-cryptographic authentication mechanisms. Cryptographic authentication mechanism adapts light weight traditional cryptographic schemes. Non-cryptographic authentication approaches [8] can be divided into biometric-based, channel-based and proximity-based authentication systems.

2.1 Traditional Authentication Mechanisms

We have existing cryptography based authentication mechanisms in past research, such as pre-distribution of secret keys among the wireless nodes, MAC based authentication etc. Research in the past [9], 10] used the pre-distribution of keys among the nodes in a Wireless Sensor Networks. There are few limitations when this key distribution technique is applied to WBAN, such as prior trust among the nodes and secrecy of pre-shared keys. More over cryptographic based authentication methods are computationally high which makes them infeasible for constrained WBAN. In addition, key management techniques are of high cost.

An identity-based cryptographic authentication [11] is developed for Wireless Body Sensor Networks, also known as light-weight cryptographic scheme. This scheme provides a secure WBAN with high flexibility in managing and accessing data. However, it involves high user-intervention which is not a suitable attribute for WBAN.

A public key cryptography based system called elliptical curve cryptography [12] has been successfully deployed in wireless sensor networks. Though these systems are feasible for WBAN, elliptical curve cryptosystems consume higher levels of energy when compared to symmetric cryptosystems.

TinySec [13] is an approach for providing authentication in WBAN. In this scheme, every sensor is programmed with a common key before the deployment of the sensor network. For further communication in the network, like message or packet encryption is done using this common key. A key drawback of this system is a compromised sensor can cause the leakage of complete information of the sensor network, hence whole system will be in risk.

So, the traditional authentication schemes mentioned above either lack security or requires high computational power which makes them infeasible for WBAN.

2.2 Biometric-Based Authentication Mechanisms

Biometric-based authentication schemes are aimed at finding a unique feature from human body and then using these traits as an authentication identity. Unique features are derived from behavioral or physiological characteristic exhibited by a human, which helps in identifying a person. Common primitives used by biometrics systems are fingerprint, face, hand geometry, iris, voice etc. These systems overcome the problem of distributing pre shared keys among sensors, which was a common drawback in most of the traditional cryptosystems. The principle of biometric-based mechanisms is to measure and compare the physiological signals at both sender and receiver end. Researchers [14], [15], [16] have exploited physiological parameters such as electrocardiogram (ECG) and photoplethysmogram (PPG), heartbeats, fingerprint etc. Efficiency of these authentication mechanisms lies in the correlation coefficient of physiological parameters calculated at sender and receiver. Reason for dissimilar physiological signals is due to the position of sensors at different parts of human body. Restricting the position of sensors in WBAN would be a strong assumption. Moreover, biometric based systems require specialized sensing hardware which is an overhead for the miniature on-body sensors.

2.3 Channel Characteristic-Based Authentication Mechanisms

Channel Characteristic-based Authentication mechanisms are also known as location-based authentication systems, is built on the basis of variations in Received Signal Strength (RSS). Researchers have leveraged the variations in RSS over time to authenticate WBAN. Zeng [18] proposed a secure device pairing scheme using differential RSS for proximity detection. However, this system relies on two receiver antennas which is an additional hardware overhead. Patwari [19] by using channel impulse response generated a temporal link signature for each device in the wireless channel, but the system requires additional hardware such as GNU Radio and an extensive learning stage. BANA [17], a light weight authentication scheme is built on the observation that RSS variations are distinct for on-body and off-body communication channels. They found a way to differentiate the signals from legitimate node and an attacker by performing clustering analysis on average RSS variation. This system takes around 12seconds to authenticate the on-body sensors. In most of the WBAN systems, authentication and key extraction need to be perceived simultaneously with wireless channel characteristics alone. However, BANA when combined with existing key generation mechanisms, it is tough to extract an authenticated secret key even with minor adjustments. An extended version ASK-BAN [28], with wireless channel alone works concurrently to generate a key and node authentication. They have employed static channel for authentication and dynamic channel for key generation. This system takes around 12seconds for authentication and 15.9seconds for key generation. However, ASK-BAN requires additional nodes between the Central Unit (CU) and the sensor node. Additionally, on-body sensor nodes are to be deployed half wavelength apart from each other to check the feasibility of Multi hop relay node security system. On the other hand, during the authentication phase of the system subjects are restricted from making any body movements.

2.4 Proximity-Based Authentication Mechanisms

Amigo [8] with the help of Diffie-Hellman key exchange and device co-location verification authenticates the devices. This system uses Diffie-Hellman algorithm to establish a shared-secret key among two devices. This key exchange might not be sufficient to ensure trusted communication. Therefore, each device in the communication range monitors the radio channel for a short span of time. Later, each device generates a signature by measuring the variations in the signal strength and exchanges it with the other. Each device without any intervention of other devices carries out a comparison of received signature with the self-generated one. If both the signatures are similar enough then the system infers the devices are legitimate to communicate further. Ensemble [29] used trusted on-body personal devices as receivers and devices for pairing as transmitters of the signals. After reception phase, personal devices conclude the proximity by monitoring the received transmissions. In similar fashion, Mathur [30] by using environment signals developed a pairing scheme based on device co-location. However, these systems require on-body sensor nodes to be deployed half wavelength apart from each other. As a result, sensors are restricted in their positioning.

Recent breakthrough [20] by a private IT security firm, provides proximity-based authentication collaborated with hands-free approach for healthcare domain. This technology is very user friendly, fast and operates on wireless channel to verify One-Time-Pad (OTP) from user's mobile device. Verification process does not require user's interaction as the system leverages wireless Bluetooth connectivity to automatically acquire and verify the OTP from a mobile device. However, Bluetooth technology [21] allows only eight devices to be connected simultaneously.

Existing techniques for authenticating body area network discussed above have limitations either in terms of security or requires high computational power and hardware. In order, to address the aforementioned concerns of WBAN, we investigate an approach that uses low cost accelerometers to determine whether or not the two sensors are carried on the waist by the same person. Accelerometers are low cost electromagnetic devices and consumes low power for computation. Researchers exploited the benefits of accelerometers and used them in device association and gesture recognition. Our method measures the acceleration forces experienced by the two sensor nodes and then correlates them using coherence estimate. A detailed overview of our work is given in further sections of the document.

CHAPTER 3: ACCELEROMETER SENSORS

Accelerometer is an electromagnetic device with vast sensing capabilities and measures acceleration, which is the rate of change of velocity. It can measure acceleration in one, two or three orthogonal axes and its units can be expressed in terms of meters per second squared or g. g is a gravitational force and it is equivalent to $9.8 m/s^2$ on earth. They are generally low-power consuming devices and their current consumption falls in the range of milli or micro ampere. Three different types are accelerometers are being used in the commercial domain such as piezoelectric, piezoresistive and capacitive ones [22]. High temperature, high frequency and easy mounting are the suitable conditions for piezoelectric accelerometers. Piezoresistive accelerometers are used in applications with sudden and acute vibrations. Applications built on silicon-micro machined sensor material and suits low frequency range as 1 kilohertz prefer capacitive accelerometers.

At the present time, accelerometers with simple, reliable and cost effective attributes are preferred. Micro Electro-Mechanical System (MEMS) accelerometers are manufactured with the above mentioned features and are widely used nowadays. Our study makes use of smartphones to measure the acceleration of a person carrying it, so we give brief details on the working principle of accelerometers in smart devices.

Smartphone accelerometer consists of a circuit with seismic mass, which is made from silicon and it is the heart of the sensor. With a change in the orientation of the device, seismic mass changes its position. As a result, sensor records the changes in the capacitance or equivalent current, when the smart phone changes its orientation or tilts. Following figures depicts the working.

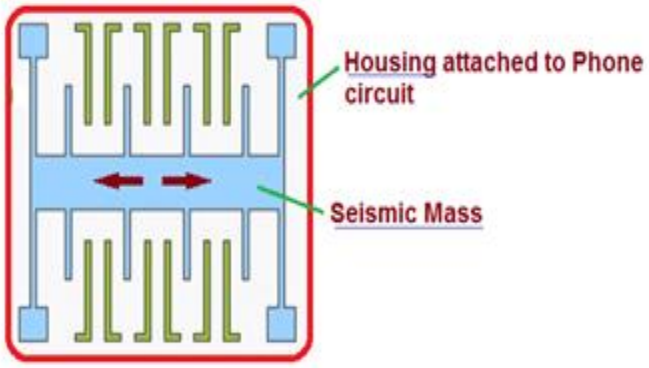

Figure 1. Internal Structure of Smart Phone Accelerometer

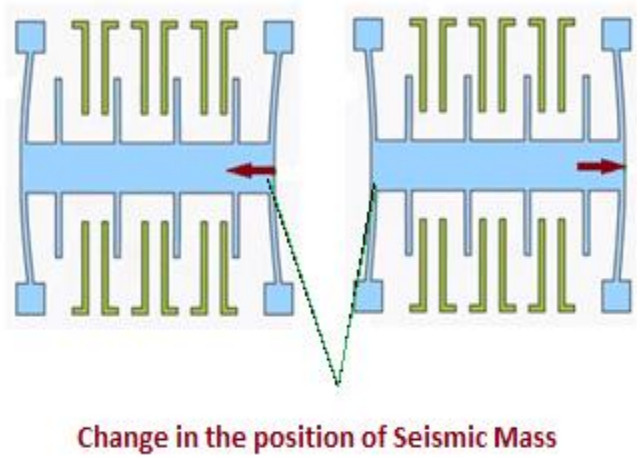

Figure 2. Seismic Mass Tilt

Therefore, smartphone accelerometer is simply a MEMS based circuit which senses and records the acceleration due to the gravity of motion or a change in orientation. Our basic idea is to use smartphone accelerometers to verify if the sensors are attached to the same person's waist. Our approach is explained in detail in the following sections.

CHAPTER 4: PROPOSED METHOD

As discussed in the previous sections, authentication in body area networks should occur with minimal human or user interaction. So we analyzed few activities performed by the user carrying the sensors on his/her body. Activities included walking, jogging, running and exercising. Apart from walking, other activities were found to be unsuitable for the analysis. The periodic nature of walking activity makes it suitable as an input to the system aimed at distinguishing the users of the sensors. In addition to the high periodicity, human walking motion is regular in nature and does not require any external factors to simulate the action.

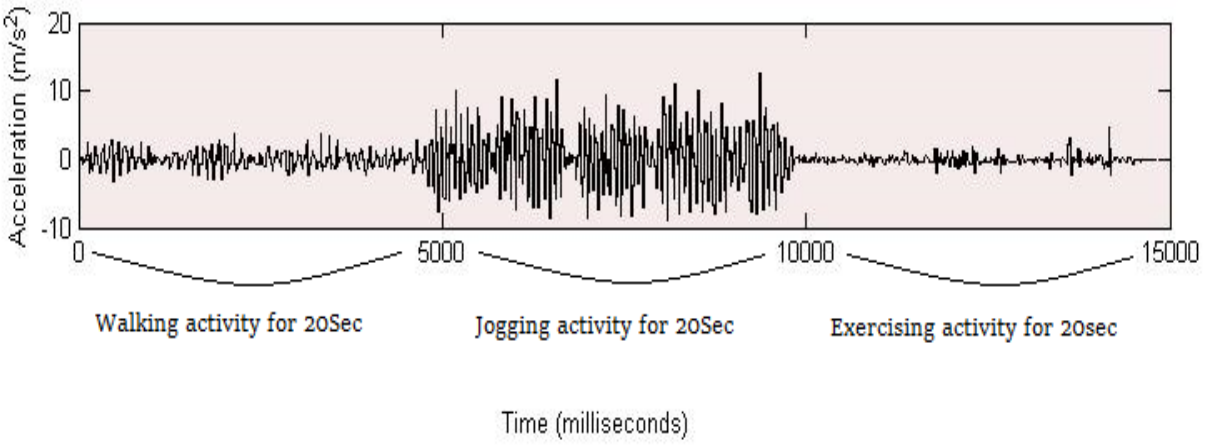

Figure 3. Acceleration Versus Time Data Representing Walking, Jogging and Exercising Activities

Human locomotion highly depends on the body geometry, moreover its repeated behavior contributes for the analysis in frequency domain and also overcomes the necessity for expensive analytical models. Graphical representation of different human activities is presented in the above figure.

Two android platform smartphones of similar configuration were used for our experiments. We examined smartphones from different manufacturers like Samsung, Motorola and opted to perform experiments on Samsung make. Below table shows the specifications of the accelerometer sensors in these android devices.

Table 1. Accelerometer Specifications in Two Different Android Devices

Accelerometer Name	**Vendor**	**Resolution**	**Max Range**	**Power**
K330 3-axis Accelerometer	STMicroelectronics	5.985504E-4	19.6133	0.25mW
LIS3DH 3-axis Accelerometer	ST Micro	0.009810001	39.24	0.25mW

4.1 Accelerometer App

An accelerometer app is developed to record the acceleration measured by the accelerometer sensor. In order to find the acceleration applied on a device, accelerometer sensor measures the forces that are experienced by itself. This relation can be shown as below:

Acceleration of the device = - Force experienced by the sensor/ Mass of the device

However, the measured acceleration also includes the force of gravity ($g = 9.8 m/s^2$). In order to eliminate the effect of earth's gravity, we subtract the magnitude of g from the acceleration measured. The Android platform provides an interface to access the hardware-based sensor, accelerometer. SensorManager class provided by Android SDK helps to access the accelerometer sensor. SensorEvent is associated with the sensor and it returns multi-dimensional array of sensor values. As a result, the accelerometer returns acceleration data in three axes (X-axis, Y-axis and Z-axis) for a single sensor event. When the sensor is in moving state, onSensorChanged event is triggered and acceleration values can be saved.

Our app exploits the above mentioned existing android classes and events to capture the acceleration data along with the time. Accelerometer app home screen displays measured acceleration in X, Y and Z axes. In addition, start and stop buttons helps in saving the recorded data into an excel file. Clicking start button initiates the saving operation, and stop button quits the save operation. Contents saved in the excel file are acceleration forces in X-axis, Y-axis, Z-axis and the timestamp at which the forces are measured. To efficiently track the change in the magnitude of the acceleration, values are captured with a recording interval of 5ms. Home screen of the accelerometer app is shown in Figure 4.

4.2 Supported Functions

This section presents a list of functions used in our study. Functions include Square Root, Fast Fourier Transform (FFT) and Magnitude-Squared Coherence.

4.2.1 Square Root

Smartphone accelerometers used in our study provide the measured acceleration forces in 3-dimensional axes. This data can be processed in two ways, one is to consider each axis independently and second is to consider three axes as a single entity. In order, to eliminate the randomness, effect of orientation changes, we prefer calculating the magnitude of the acceleration forces of all three axes by using Square Root function as presented below. This derives a resultant acceleration independent of orientation.

$$A_d = \sqrt{A_{dx}^2 + A_{dy}^2 + A_{dz}^2}$$

4.2.2 Fast Fourier Transform (FFT)

Data recorded by the accelerometer app is represented using time domain. Fourier Transform converts the time domain input signal to output signal in frequency domain. FFT [23] efficiently estimates the component frequencies in the output data from a discrete set of input. The

MATLAB tool provides with inbuilt functions for Fourier analysis. Different variations of FFT function are available in MATLAB. Since our input data is magnitude of acceleration force which is one dimensional in nature, we use FFT in its simplest form. fft function [23] takes an input vector x and returns Direct Fourier Transform (DFT) y using a fast Fourier Transform algorithm.

$$op = fft(in)$$

The equation for fft function is shown above, where in is the input vector and op is the DFT form of the output vector. The window length for the transformation is obtained from the size of the input vector, and same length is applied to the output as well.

4.2.3 Magnitude-Squared Coherence

For acceleration versus time series signals depicted in figure 1, it is required to find a reliable method to analyze the data and draw a conclusion from the analysis. A research work by Ben-Pazi [25] examined the origin of real tremors in a Parkinson's patient by using biological accelerometer data, and analyzing the data with coherence estimate. This motivated us to extend the usage of coherence function to time series acceleration signals. As we measure the acceleration data from two smartphone accelerometers for our experiments, we find how well the two input sets are co-related with the help of magnitude-squared coherence function.

Magnitude-Squared Coherence function is an estimate function of frequency range between 0 and 1. This Coherence estimate demonstrates how well an input set relates to the other at each frequency. Let, the acceleration data from two smartphones be represented by x and y, then the magnitude-squared coherence function is denoted by $C_{xy}(f)$ [24]. $C_{xy}(f)$ function depends on power spectral densities, $P_{xx}(f)$ and $P_{yy}(f)$, of x and y respectively and also the cross power spectral density, $P_{xy}(f)$ of x and y as shown below.

$$\boldsymbol{C_{xy}(f)} = \frac{\left|\boldsymbol{P_{xy}(f)}\right|^2}{\boldsymbol{P_{xx}(f)P_{yy}(f)}}$$

The MATLAB inbuilt function mscohere [24] uses Welch's averaged modified periodogram method to obtain the magnitude-squared coherence estimate, C_{xy}, of the given input signals x and y as presented below.

$$C_{xy} = mscohere(x, y)$$

The above equation produces high coherence value (nearly equal to 1), if the two signals are highly correlated and low coherence value (nearly equal to 0) for uncorrelated signals at each frequency value. Since coherence estimate is a function of frequency, we need an approach to compute a scalar quantity from the coherence curve to determine the similarity. Integral of coherence curve can be a simple approach to obtain a scalar quantity. By using the MATLAB, trapz [26] function the scalar measure of similarity is calculated for our experiments as shown below.

$$C_s = trapz(CoherenceCurve)$$

The trapz function returns the appropriate integral of the given input using trapezoidal method. In the above equation, C_s represents the similarity measure of two different acceleration inputs. We made use of integration method which is fast and computationally inexpensive when compared to other complex methods to quantify the coherence outcome.

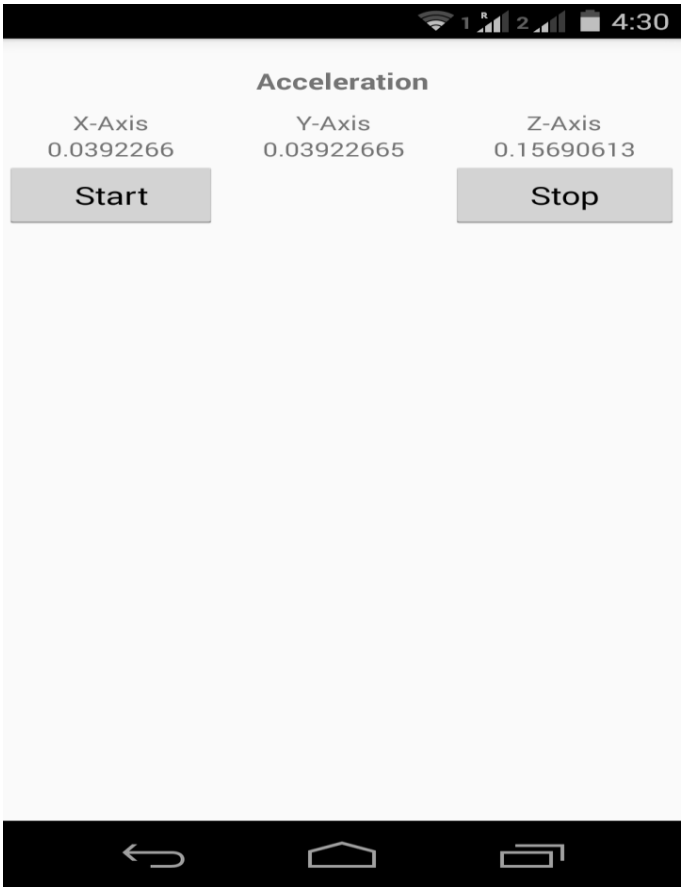

Figure 4. Acceleration App Home Screen

CHAPTER 5: ACCELEROMETER DATA COLLECTION

The outline of this section provides a description of the process of data collection and the analysis done on the acceleration signals. Experiments were carried in two different ways on three subjects, single-subject walking experiment and two-subjects walking experiment.

5.1 Experimental Setup and Data Collection

In this section we describe the experimental setup for the data collection. Throughout the process of accelerometer data collection, smartphones were carried in a fanny bag which is wrapped around the subject's waist. In the first type of experiment, each subject carried two smartphones and performed walking activity for approximately 20seconds. In each smartphone, accelerometer app is opened before starting the walking activity. Once the walking activity is initiated by the subject, start button in the app screen is clicked explicitly in order to start the saving operation. After 20seconds of the activity, stop button is clicked to end the save operation. 5 trails are made for each subject, and each trail produces two accelerometer signals from two smartphones respectively. So, with 3 subjects and 5 trails for each one, gave 30 time-variant acceleration signals for further analysis in the single-subject walking experiment.

The process of gathering the accelerometer data is same for two-subjects walking experiment as well. However, in this experiment two subjects walk simultaneously with a smartphone carried by each of them. In this experiment, each subject walked with other two subjects forming a total of 3 pairs. Each pair of subjects performed 5 trails of walking activity for approximately 20seconds. So, with 3 pairs of subjects and 5 trails for each pair, gave 30 time-variant acceleration signals for further analysis in the two-subjects walking experiment.

Due to the manual triggering of save operation using start and stop buttons in the app, there might be some latencies in the data collection. In order to reduce the effect of latencies, we manually trim the recordings so that all the recordings would be of equal length. The following sections provide more details on the analysis of two types of experiments.

5.2 Single-Subject Walking Trail

The aim of single-subject walking experiment is to demonstrate the high coherence of the two recorded patterns of a single subject.

Figure 5 represents the data collected from subject A. Acceleration magnitude data from two smartphone accelerometers recorded for approximately 20seconds is used to obtain the FFT spectra using fft function. Later, coherence measure is calculated using mscohere function.

The two signals presented in the figure 5 are recorded on the same subject, during the same trail of walking activity. One important observation to be noted from the figure 6 of this experiment is, the two FFT spectra of the input signals look similar as the patterns are of same subject waist.

The coherence plot depicted in figure 7, shows the two acceleration signals are highly correlated at majority of frequency values.

5.3 Two-Subjects Walking Trail

The aim of single-subject walking experiment is to demonstrate the low coherence of the two recorded patterns of two different subjects.

Figure 8 represents the data collected from subject A and subject B. Acceleration magnitude data from two smartphone accelerometers recorded for approximately 20seconds is used to obtain the FFT spectra using fft function. Later, coherence measure is calculated using mscohere function. The two signals presented in the figure are recorded on two different subjects, during the same trail of walking activity.

One important observation to be noted from the figure 9 of this experiment is, the two FFT spectra of the input signals are not similar as the patterns are of two different subjects.

The coherence plot depicted in figure 10, shows the two acceleration signals are slightly correlated at majority of frequency values.

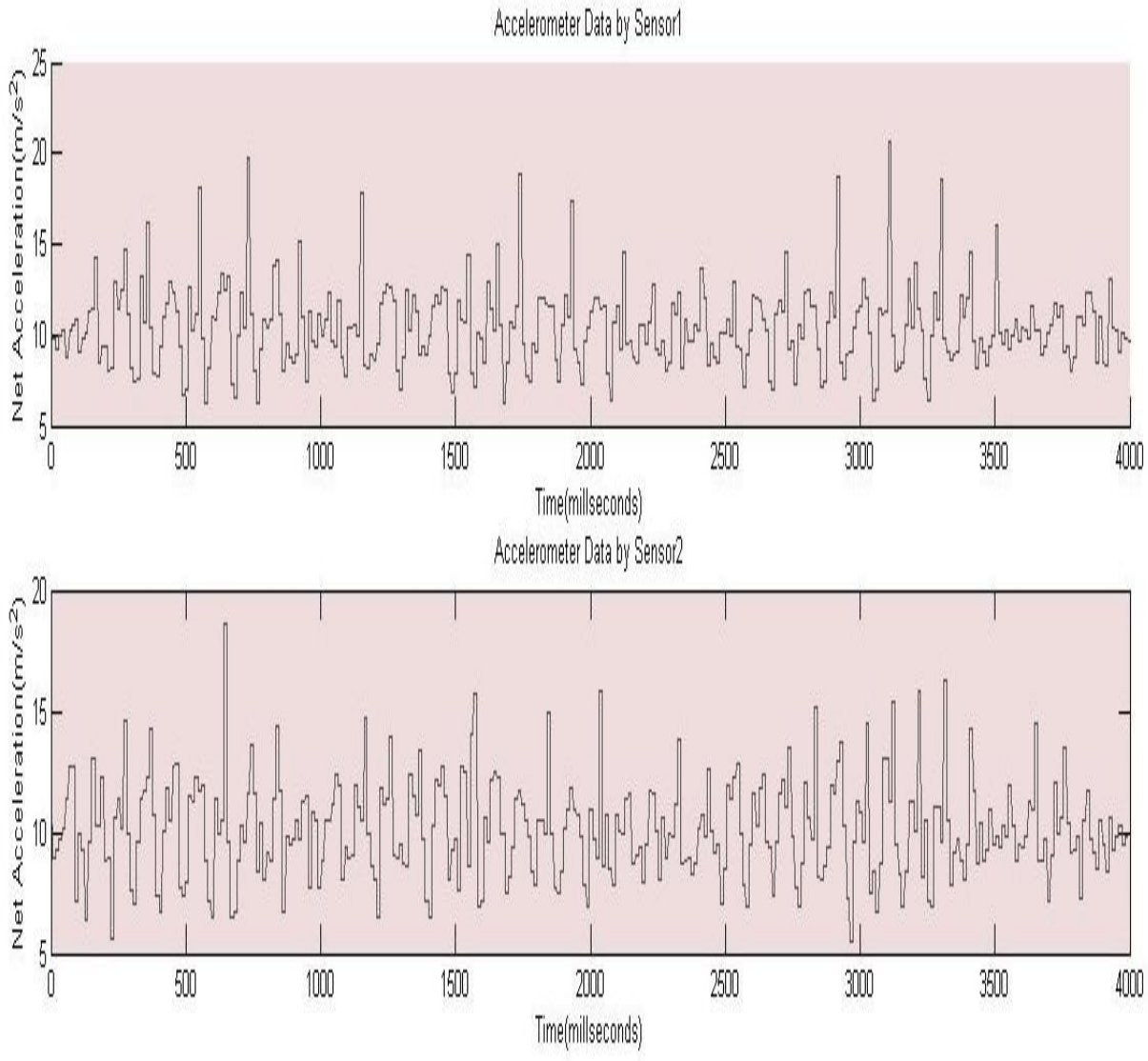

Figure 5. Acceleration Data of Subject A

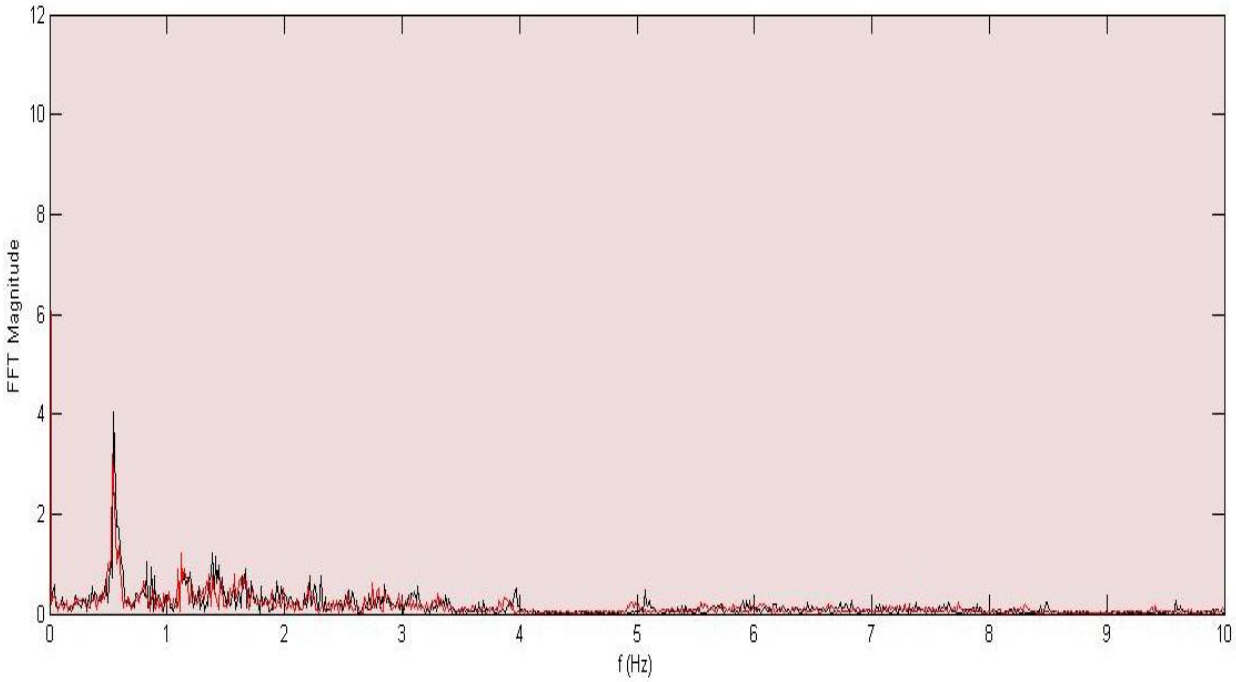

Figure 6. FFT Spectra of Subject A's Acceleration Data

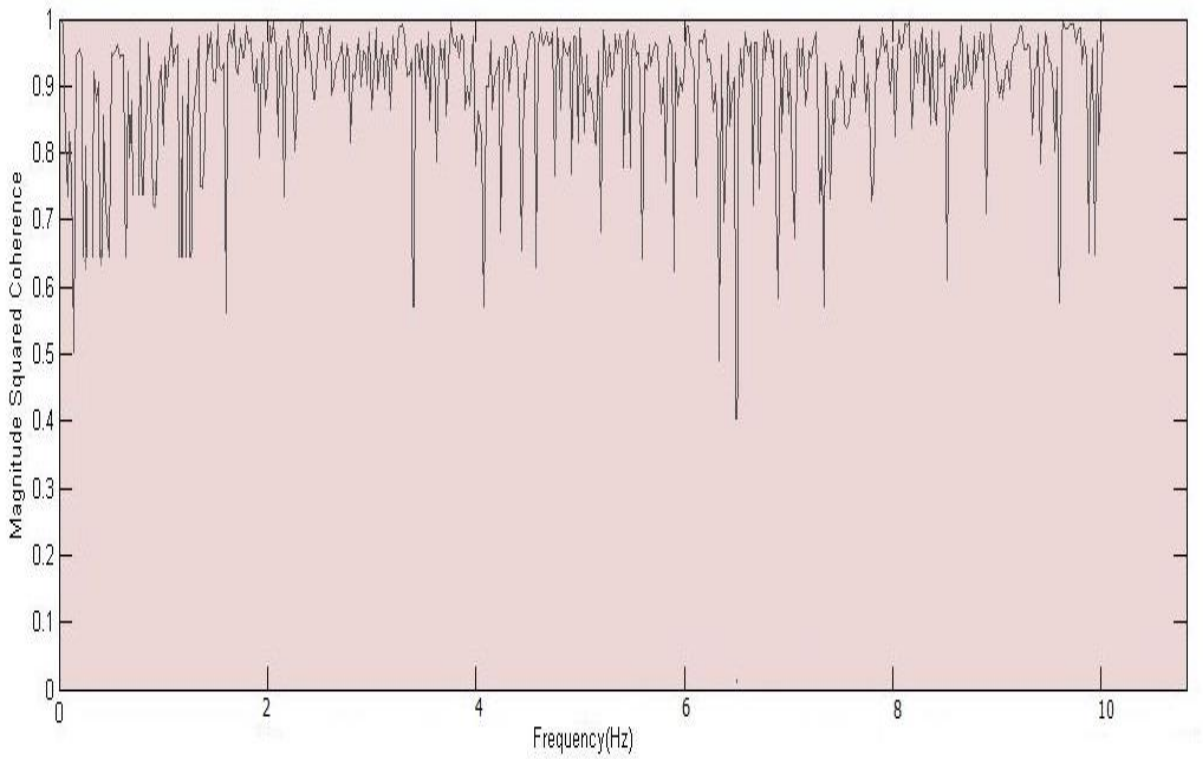

Figure 7. Coherence Curve of Subject A's Acceleration Data

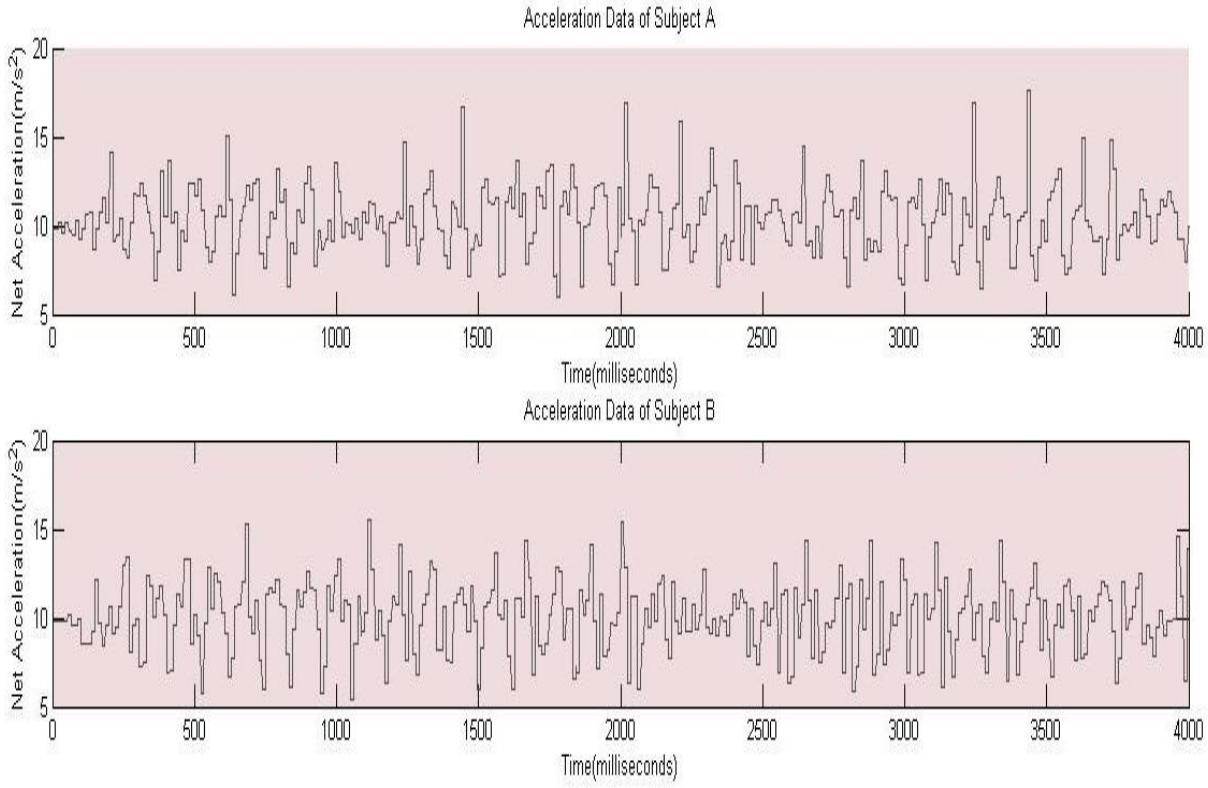

Figure 8. Acceleration Data of Subject A and Subject B

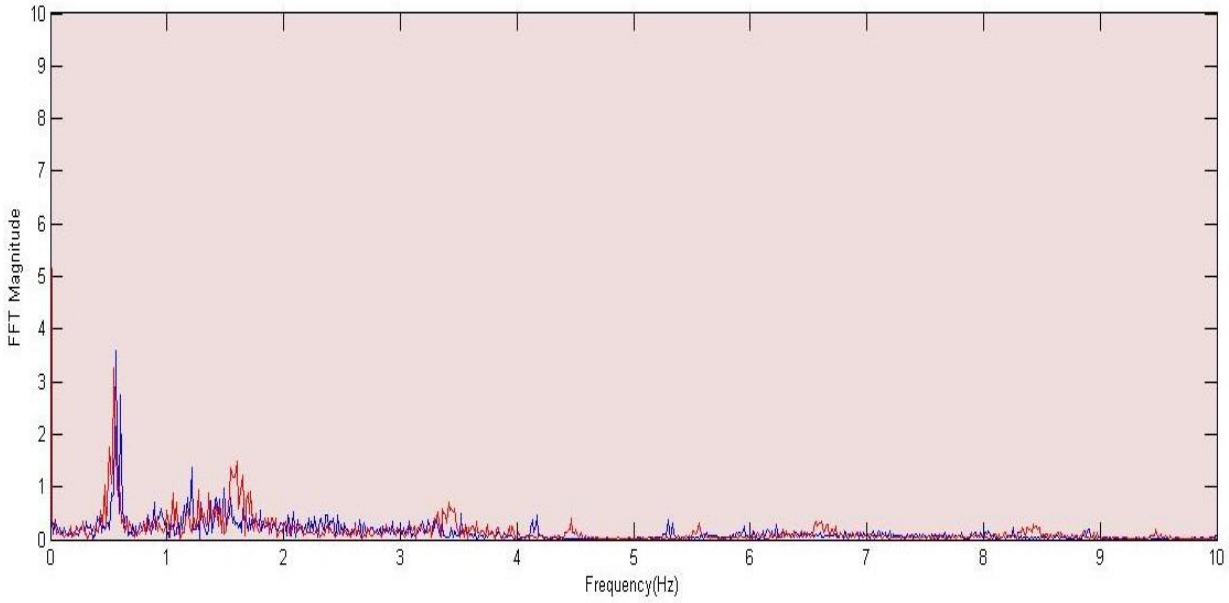

Figure 9. FFT Spectra of Subject A and Subject B's Acceleration Data

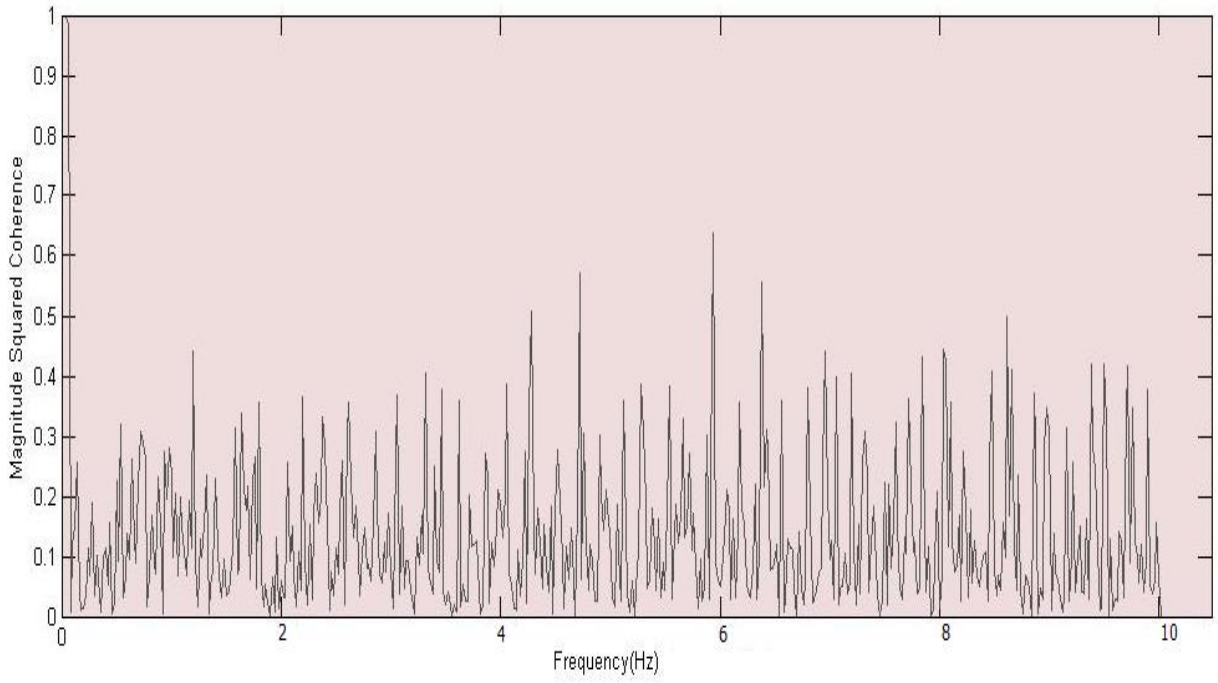

Figure 10. Coherence Curve of Subject A and Subject B's Acceleration Data

5.4 Experimental Results

Figure 11 shows the coherence measure calculated from two signals recorded on Subject A, B and C. In a trail, only one subject performed walking activity for 20seconds, carrying two smartphones in a fanny bag. Each subject performed five walking trails. Twenty seconds of acceleration data is given as input to FFT function, which results in FFT spectra as output. Magnitude squared coherence is calculated from FFT spectra. In order to find a scalar measure of coherence, we integrate magnitude squared coherence curve.

Coherence measure is greater than hundred for most of the walking trails as shown below. The two signals in this experiments are highly correlated at most of the frequencies, therefore the scalar coherence measure is high. Hence, we conclude the two sensors are carried on same individual's waist, if the coherence measure is greater than hundred.

Figure 12 shows the coherence measure calculated from two signals recorded on Subject A, B and C. In a trail, only two subjects performed walking activity for 20seconds, each of them carrying a smartphone in a fanny bag. Each pair of subjects performed five walking trails. Twenty seconds of acceleration data is given as input to FFT function, which results in FFT spectra as output. Magnitude squared coherence is calculated from FFT spectra. In order to find a scalar measure of coherence, we integrate magnitude squared coherence curve. Coherence measure is less than hundred for most of the walking trails as shown below. The two signals in this experiments are slightly correlated at most of the frequencies, therefore the scalar coherence measure is low. Hence, we conclude the two sensors are not carried by the same individual, if the coherence measure is less than hundred.

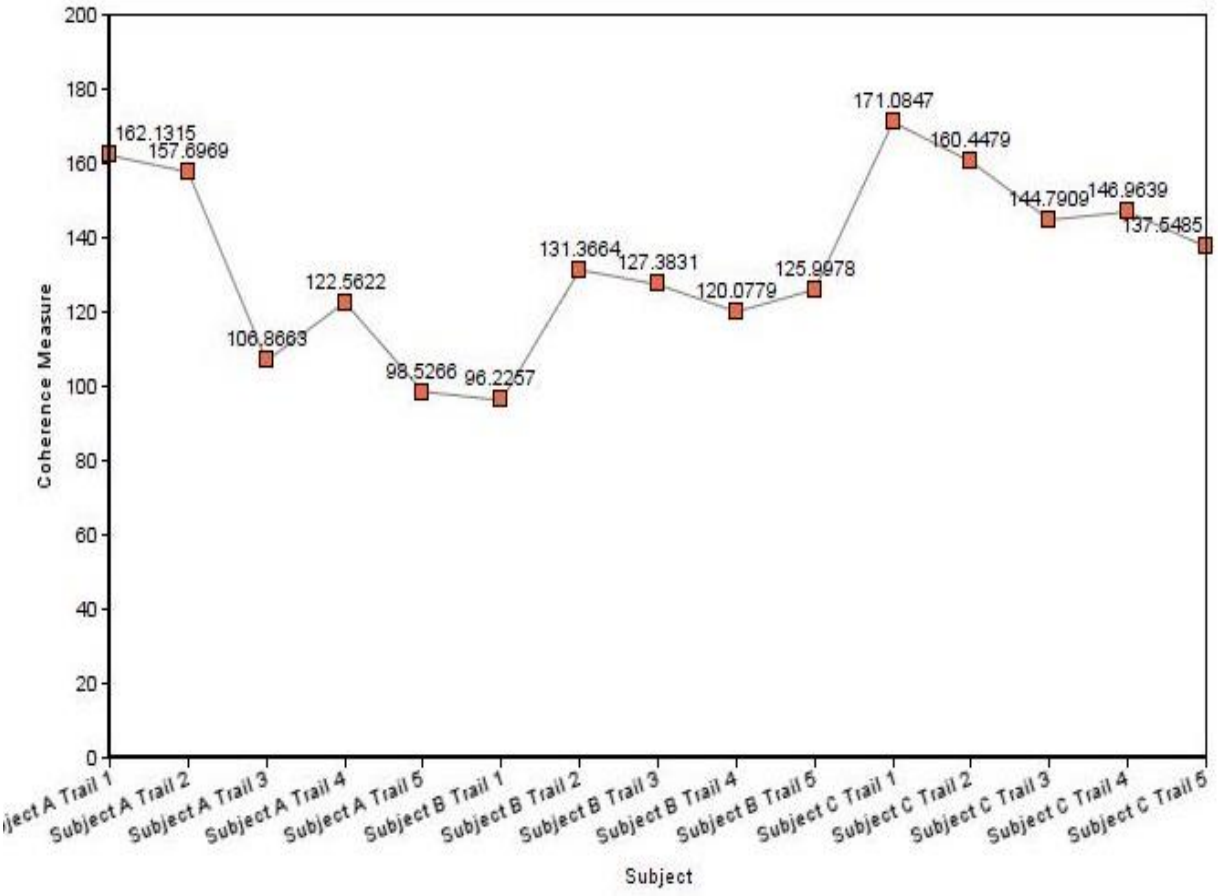

Figure 11. Coherence Measure of Single-Subject Walking Trails

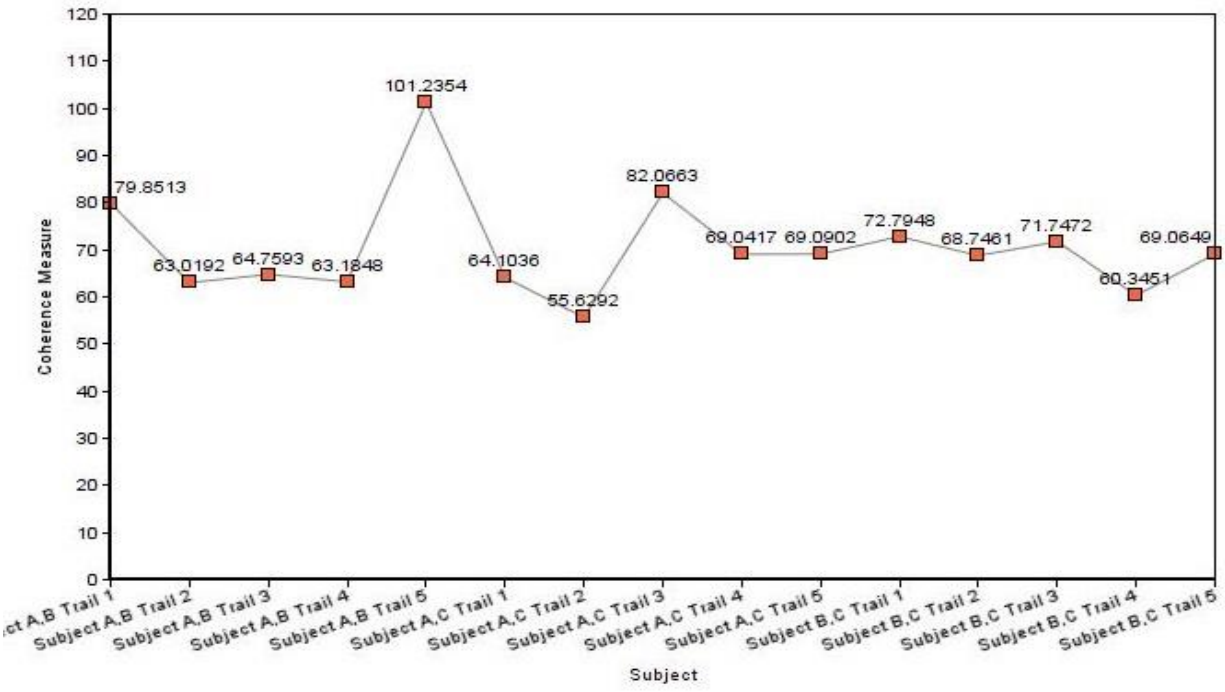

Figure 12. Coherence Measure of Two-Subjects Walking Trails

CHAPTER 6: PRACTICAL CONSIDERATIONS

The experimental results considered so far were generated from the walking activity for 20sec. Throughout the study, data is collected using accelerometer app, which needs manual operation for saving the acceleration data. This results in uneven window sized data, for example 22sec of data. In order to find a common measure, we manually trim the recorded data to obtain a window size of 20seconds. We also considered different small sized walking data to check if they provide enough details. However, small sized windows can also be a measure for coherence, but longer sized windows provide more information for analysis.

Another consideration, during the app development is how often the values are to be captured while recording the walking activity. After analyzing data over three different recording intervals, we captured acceleration values for every 5millseconds. This recording interval gave us the most accurate changes in the acceleration values with the time.

In addition, one important consideration is the communication latencies between the two accelerometer sensors. It is better to have a system which is insensitive to the delays, but the available wireless synchronization methods are too power consuming ones. The work similar to ours [4] depicted their simulation results, which states even with a 500ms communication delay and with large-sized windows the success rate is greater than 95%. So, delays to some extent still produce reliable results. Likewise, our approach has some communication delay of 20msec to 25msec. However, it exhibits some insensitivity towards the coherence values which makes our approach tolerant enough for communication latencies.

We also present a theoretical algorithm to show the authentication of On-body sensors using accelerometer sensors. Authentication can happen in two ways: Centralized and peer-to-peer. In centralized authentication, the two communicating sensors record the acceleration data individually, then sends their data to the centralized node or a controller. The controller then, applies FFT on the raw data received from the two sensor nodes. Then, it calculates the coherence measure to determine if the two sensors are authenticated ones to communicate.

In peer-to-peer communication, series of steps occur during the process of authentication. In the first place, the sensors should agree upon a time duration and then collect the raw acceleration versus time data. Next, FFT is applied on the recorded data by each sensor. Either of the sensor nodes can perform the calculation of coherence measure. For example, if sensor2 agrees upon calculating the coherence, sensor1 should share its FFT curve with sensor1. Then, sensor1 calculates coherence measure and determines whether to proceed the communication process with sensor2. In both the scenarios, a complex coordination process ensures a complete secure scheme.

CHAPTER 7: CONCLUSION AND FUTURE WORK

Our study primarily concentrates on two aspects of On-body sensors. First, to determine if accelerometer sensors can be used to authenticate on-body sensors. Second, to show low-cost accelerometers are sufficient to accomplish the task. The experimental results presented provides us with positive conclusions for both the aspects. By recording 20sec of acceleration data, we could reliably determine the probability of two sensors carried by the same individual is high. There by, we present an answer for our question posed earlier: Can accelerometer data provide us with reliable information to verify, whether the two sensors are carried on waist by the same person? We also examined few human daily activities to find the answer for our second question: What is the best active motion of an individual to track the similarities in the profile data? Experiments showed that walking motion is the most suitable activity to track the similarities, as the two sensors carried by an individual on waist records similar profile data.

As the frequency of human locomotion lies in the frequency range of 0-10Hz and accelerometer can sample the data with a frequency lower than 20Hz. This capability of accelerometer makes them suitable for small and lower power devices.

Since our focus is on walking activity, we used low frequency levels to determine the coherence measure, by calculating the area under magnitude squared coherence curve. This provided us with a rough likelihood and this estimate gave us good results to determine whether the two sensors are carried by same individual or not. Our first type of experiment gave us a success rate of 86.6%, which exhibits the sensors if carried on same individual's waist exhibit high coherence value.

Similarly, our second type of experiment presented a success rate of 93%, which shows the sensors if carried by different individuals exhibit very low coherence values.

We also present a theoretical algorithm to authenticate on-body sensors. It determines whether the two sensors are authentic enough to communicate. However, we have to perform an extensive study to show that are approach best suites the wireless body area network.

The major limitations of our approach: one the subject is required to perform walking activity. Second, the sensors are placed in a fanny bag worn around the subject's waist for conducting the experiments. Other human activities require advanced tools for analysis, as a result the devices need high computational capabilities.

In future, we would like to extend our study to other daily life activities like sitting, typing etc. Also, to the sensors located or worn on different parts of human body. Once sensors are known to be on same individual, next step in authentication process is to share a secret key among the sensors. We plan to explore the secret key extraction from the coherence curve derived from our experimental results in future work.

REFERENCES

[1] B.P. Clarkson. Life Patterns: Structure from Wearable Sensor. PhD Thesis, MIT Media Lab, 2002.

[2] J. Lester, T. Choudhury, N. Kern, G. Borriello, and B. Hannaford, "A Hybrid Discriminative/Generative Approach for Modeling Human Activities," in Proc. 9th Int. Joint Conf. Artif. Intell., Edinburgh, Scotland, 2005, pp. 766-772.

[3] X. Long, B. Yin, and R. Aarts, Single accelerometer-based daily physical activity classification, in 31st Annual International Conference of the IEEE EMBS, 2009, pp. 61076110.

[4] "Are you with me?" Using accelerometers to determine if two devices are carried by the same person

[5] E. Kantoch, J. Jaworek, P. Augustyniak, "Design of a wearable sensor network for home monitoring system," Federated Conf. on Computer Science and Information Systems (FedCSIS), pp. 401-403, 2011.

[6] J. R. Douceur, "The sybil attack," in Proc. First International Workshop on Peer-to-Peer Systems, ser. IPTPS '01, 2002, pp. 251–260.

[7] J. Yang, Y. Chen, and W. Trappe, "Detecting sybil attacks in wireless and sensor networks using cluster analysis," in Proc. The 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Atlanta, GA, USA, Sep. 2008, pp. 834–839.

[8] A. Varshavsky, A. Scannell, A. LaMarca, and E. De Lara. Amigo: proximity-based authentication of mobile devices. In Proceedings of the 9th international conference on Ubiquitous computing, UbiComp '07, pages 253–270, Berlin, Heidelberg, 2007. Springer-Verlag.

[9] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE S & P ’03, page 197, 2003. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 62–71. ACM, 2003.

[10] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili. A pairwise key predistribution scheme for wireless sensor networks. ACM Transactions on Information and System Security (TISSEC), 8(2):228–258, 2005.

[11] C. C. Tan, H. Wang, S. Zhong, and Q. Li. Body sensor network security: an identity-based cryptography approach. In ACM WiSec ’08:, pages 148–153, 2008.

[12] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, “NanoECC: testing the limits of elliptic curve cryptography in sensor networks,” in Proceedings of the 5th European Conference on Wireless Sensor Networks, pp. 305–320, Bologna, Italy, February 2008.

[13] C. Karlof, N. Sastry, and D. Wagner, “TinySec: a link layer security architecture for wireless sensor networks,” in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, (SenSys '04), pp. 162–175, Baltimore, Md, USA, November 2004.

[14] K. Venkatasubramanian and S. Gupta. Physiological value-based efficient usable security solutions for body sensor networks. ACM Transactions on Sensor Networks (TOSN), 6(4):1–36, 2010.

[15] K. K. Venkatasubramanian and S. K. S. Gupta. Physiological value-based efficient usable security solutions for body sensor networks. ACM Trans. Sen. Netw., 6:31:1–31:36, July 2010.

[16] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In The 30th IEEE International Conference on Computer Communications (INFOCOM 2011), pages 1862 – 1870, Shanghai, P.R.China, April 2011.

[17] Lu Shi, Ming Li, Shucheng Yu, Jiawei Yuan, BANA: body area network authentication exploiting channel characteristics, Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, April 16-18, 2012, Tucson, Arizona, USA.

[18] L. Cai, K. Zeng, H. Chen, and P. Mohapatra. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In Network and Distributed System Security Symposium, 2011.

[19] N. Patwari and S. Kasera. Robust location distinction using temporal link signatures. In Proceedings of the 13th annual ACM international conference on Mobile computing and networking, pages 111–122. ACM, 2007.

[20] https://www.imprivata.com/company/press/imprivata-introduces-breakthrough-proximity-based-hands-free-authentication-solution

[21] http://www.instrumentationtoday.com/accelerometer/2011/08/

[22] http://www.techulator.com/resources/8930-How-does-smart-phone-accelerometer-work.aspx

[23] http://www.mathworks.com/help/matlab/math/fast-fourier-transform-fft.html

[24] http://www.mathworks.com/help/signal/ref/mscohere.html

[25] Ben-Pazi, H., Bergman H., Goldberg J. A., Giladi N., Hansel D., Reches A., and Simon E. S.: Synchrony of Rest Tremor in Multiple Limbs in Parkinson's Disease: Evidence for Multiple Oscillators. In: Journal of Neural Transmission, Vol. 108 (3) (2001) 287–296

[26] http://www.mathworks.com/help/matlab/ref/trapz.html

[27] Lee, S.W., Mase, K. Activity and location recognition using wearable sensors. Pervas. Comput.July/September 2002:24–32.

[28] L. Shi, J. Yuan, S. Yu, and M. Li, "ASK-BAN: Authenticated secret key extraction utilizing channel characteristics for body area networks," in Proc. 6th ACM conference on Security and privacy in wireless and mobile networks (WiSec '13), 2013, pp. 155-166.

[29] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca. Ensemble: cooperative proximity-based authentication. In Proceedings of the 8th international conference on Mobile systems, applications, and services, MobiSys ’10, pages 331–344, New York, NY, USA, 2010. ACM.

[30] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam. Proximate: proximity-based secure pairing using ambient wireless signals. In Proceedings of the 9th international conference on Mobile systems, applications, and services, pages 211–224. ACM, 2011.