Three Cyberspace Applications for IoT RF Cloud in Localization, Motion Detection, and Security

A Thesis

Submitted to the Faculty of the

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfillment of the requirements for the

Degree of Doctor of Philosophy in

Electrical and Computer Engineering

by

January 2021

APPROVED:

Professor Kaveh Pahlavan, Major Dissertation Advisor

Professor Xinrong Li, Thesis Committee

Professor Ziming Zhang, Thesis Committee

Professor Donald Richard Brown, Head of Department

Abstract

Internet of Things (IoT) has emerged as a new trend to provide novel technical solutions to cyberspace applications. The IoT network mainly consists of small wearable or implantable sensor nodes, using a variety of RF technologies such as Wi-Fi, Bluetooth, ZigBee, and Ultra-Wideband (UWB). The RF signals radiating from these devices create a RF cloud that we can benefit from to design novel cyberspace applications such as positioning, motion and gesture detection and security.

Currently, the most popular indoor geolocation technique in smart devices is the RSS-based Wi-Fi positioning. This technology takes advantage of existing RF cloud from Wi-Fi infrastructure deployed for wireless communications by fingerprinting the RF signals radiated from these devices. With the emergence of IoT, low power devices with diversified power levels are deployed with a higher density, which enables precise indoor geolocation with IoT RF cloud without a need for time consuming fingerprinting.

Motions of objects close to the wireless devices cause temporal fluctuations of characteristic of RF cloud. These characteristics introduce a variety of features that we can benefit from for activity, motion, and gesture detection.

Secure transmission of data is another major unsolved concern in IoT networks, with the demand of a practical authentication policy. We can also benefit from RF cloud of IoT devices to create secure communications.

In this dissertation we study three novel examples of cyberspace applications of IoT RF cloud in localization, motion detection and security key generation.

(1) We explore how IoT devices with diversified power level can affect the localization performance in dense IoT environment. We apply probability of coverage

into the empirical CRLB calculation and show how low power devices can improve the positioning precision and eliminate the need for expensive fingerprinting.

(2) We extract both temporal and spatial IoT RF cloud characteristics and use these features for motion detection. Different detection approaches have been tested, and we conclude that RF cloud information can improve the detection accuracy.

(3) We use multipath propagation characteristics from UWB sensors and generate a shared security keys using PHY-based schemes. Our analysis demonstrates the spatial performance of RSS-based schemes and TOA-based schemes from the aspect of Bit Match Rate (BMR), Key Generation Rate (KGR), and scalability, which opens possibilities for new RF solutions to IoT network security.

Acknowledgements

In this dissertation I describe the research I conducted in pursuit of my Doctor of Philosophy Degree in Electrical and Computer Engineering in Worcester Polytechnic Institute.

Firstly, I would like to offer my sincerest gratitude to my research advisor, Professor Kaveh Pahlavan, for leading me into the world of research, for sharing his life experience, and for providing long term financial support so that I could fully devote myself into the Ph.D. study. Professor Pahlavan is a kindly mentor and he has been so much more than that. In addition to the skills and knowledges I have learnt from him, his words of insight and sagacity encouraged me and held me in good stead. Throughout the past five years, when I feel anxious, worried, hesitated, or confused, professor Pahlavan always encouraged me and spread his energy so that I can carry on to fulfil my dreams.

An extra special thanks is due to professor Xinrong Li and professor Ziming Zhang for their thoughtful suggestions on my dissertation.

Words can not express my gratefulness to my dear parents for their care and support and their important responsibility for enabling me in reaching this point of my life. Finally, I would like to dedicate this work to my wife Mengjun for her love and support during this journey. Being with her, I get all the perseverance for facing challenges and overcoming obstacles.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Nowadays, over a billion Wi-Fi access points deployed worldwide connect our mobile, personal, and fixed devices to the Internet and the cyberspace. They have become an essential part of our lives to the extent that some people take Wi-Fi as the foundation of human needs.

In late 1990s the IEEE 802.15 standardization activities began and introduced Bluetooth, ZigBee, and Ultra-Wideband (UWB) technologies for personal area networking [5]. Radio Frequency Identification (RFID) technologies has emerged as the icon of supply chain management, inventory control, and many other applications [6]. More recently, with the emergence of millimeter wave (mmWave) technology for Wi-Fi and cellular networks, leading manufacturer such as Texas Instrument have introduced short range radar sensor devices employing this technology [7]. Today, the RF signal radiating from over a billion Wi-Fi access points, several hundred thousand of cell towers, and trillions of IoT devices using Bluetooth, ZigBee, UWB, mmWave, and RFID technologies invites innovative opportunistic Big Data application developments for the cyberspace [8]. The RF signals radiating from these devices create an RF cloud reachable to any device with an RF front end to sense

their signals. The features of these RF signals such as received signal strength (RSS), time of arrival (TOA), direction of arrival (DOA), channel impulse response (CIR), and channel state information (CSI), provides a fertile ground for numerous innovative opportunistic cyberspace applications.

the RF cloud radiated from wireless devices surrounding us contain a huge source of information. Each wireless device has a unique address and if fixed, a unique location, and it radiates an RF signal with different coverage, which changes its features with motions. One can create a database of these addresses and the available signal features (RSS, TOA, DOA, CIR and CSI) associated with the addresses to develop opportunistic cyberspace applications, which have evolved around the RF cloud from wireless devices. The most popular cyberspace applications of RF cloud have evolved for indoor positioning using wireless signals of opportunity

Wireless positioning taking advantage of signals from existing Wi-Fi infrastructure deployed for wireless communications was the first popular application of RF cloud. In that application, we read the address of a Wi-Fi access point from its floating broadcast packets and we record the RSS feature of the channel, to develop our positioning system.

Motions of the wireless device or objects close to the antennas of the wireless devices cause temporal fluctuations of characteristic of RF cloud features measured at the receiver antennas. Recently, a number of researchers have studied these characteristics of RF cloud from wireless devices for activity, motion and gesture detection.

In recent years, several researchers have shown interest in developing authentication and security applications benefitting from big data embedded in the RF cloud. These researchers look into various kind of devices, including Wi-Fi, Bluetooth, Zigbee and RFID, to evaluate the threat, to assess vulnerability of the systems, and to

propose frameworks for specific authentication and security schemes.

1.1 Contribution

The dissertation consists of three major sections and the major contribution of this dissertation has been listed as follows:

Chapter 3:

we tried to explore how the coverage probability can affect the procedure of CRLB calculation and consequently the performance evaluation. The calculation of coverage probability is specifically derived as the basic foundation of the follow-up CRLB calculation. Scenarios are designed for conducting experiments which is based on the infrastructure of Atwart Kent Laboratory (AKL). Both 2D and 3D scenarios are designed and comparisons are made accordingly.

Chapter 4:

A model-based RF hand motion detection system is presented to detect horizontal hand motion. Experiments are conducted to illustrate the detection performance by different RF sources.

Chapter 5:

We designed a general architecture of a secure-IoT for e-Health application and looked into the requirements to secure the system. We discussed the possible solutions and how location and behaviour analysis can be applied to fulfil the security needs.

1.2 Dissertation Outline

The remainder of this dissertation is organized as follow: Chapter 2 introduced the research background of the entire dissertation. We start the discussion from general body area network, and then move to the radio propagation channel modeling for body area network, and finaly briefly introduced the existing applications for body area network.

In Chapter 3 CRLB using PoC has been derived in dense IoT environment, we conclude that with the help of low power devices, localization accuracy can be improved and the load of fingerprinting can be eliminated.

Chapter demonstrates two examples of motion detection using UWB and mmWave signals, showing that in both cases, we can reach more than 90 Thirdly, we utilize UWB multipath characteristics for security key generation and prove that both RSS-based and TOA-based schemes perform precise BMR. CRLB of these two schemes are derived to further validate experiment.

Chapter 5 proposed how we utilize UWB multipath characteristics for security key generation and prove that both RSS-based and TOA-based schemes perform precise BMR. CRLB of these two schemes are derived to further validate experiment.

Finally, Chapter 6 presents the conclusion to this dissertation and discussion of the future works.

Chapter 2

Background

2.1 RF Cloud for Emerging IoT Usage

The holistic view of wireless data communications for office information networking emerged in the mid-1980s [1, 2] and the IEEE 802.11 standardization activity for wireless local area networking, commercially known as Wi-Fi, began in late 1980s to address this industry. Today, when we arrive at a hotel registration desk, the first fundamental questions we ask related to our basic needs are: Where is my room? Where is the restaurant? And how can I connect to the Wi-Fi? Over a billion Wi-Fi access points deployed worldwide connect our mobile, personal, and fixed devices to the Internet and cyberspace. They have become an essential part of our lives to the extent that some people take Wi-Fi as the foundation of human needs, where Maslows hierarchy of human needs lands on (Figure 1, [3,4]). In the late 1990s the IEEE 802.15 standardization activities began and introduced Bluetooth, ZigBee, and Ultra-Wideband (UWB) technologies for personal area networking [5]. Radio Frequency Identification (RFID) technologies have emerged as the icon of supply chain management, inventory control, and many other applications [6]. More

recently, with the emergence of millimeter wave (mmWave) technology for Wi-Fi and cellular networks, leading manufacturers such as Texas Instruments have introduced short range radar sensor devices employing this technology [7]. Today, the RF signal radiating from over a billion Wi-Fi access points, several hundred thousands of cell towers, and trillions of IoT devices using Bluetooth, ZigBee, UWB, mmWave, and RFID technologies invites innovative opportunistic big data application developments for cyberspace [8]. The RF signals radiating from these devices create an RF cloud reachable to any device with an RF front end to sense their signals. The features of these RF signals such as received signal strength (RSS), time of arrival (TOA), direction of arrival (DOA), channel impulse response (CIR), and channel state information (CSI), provide a fertile ground for numerous innovative opportunistic cyberspace applications.

This thesis provides a visionary overview of these emerging cyberspace applications and explains how they benefit from RF cloud to operate. We first discuss the big data contents of features of the RF cloud. Then, we explain how innovative cyberspace applications are emerging to benefit from the big data in these features. We begin with explaining opportunistic wireless positioning benefitting from big data from the RF cloud. Then, we explain how researchers are studying applications of these features for motion, activity and gesture detection as well as authentication and security to open a new horizon for human-computer interaction.

2.2 IoT Applications

2.2.1 RF Cloud for Localization

In late 1990s, indoor geolocation science and technology began to evolve to extend the coverage of Global Positioning System (GPS) to indoor areas. The high

cost of dense infrastructure, needed for proper operation of these systems, moved this industry towards opportunistic positioning using RF cloud data from the existing Wi-Fi access point infrastructure. A Real Time Localization System (RTLS) industry, with a limited vertical market, evolved around this idea for applications in specific areas, such as museums, warehouses, and hospitals. Fingerprinting of the RF cloud for RTLS systems are done manually by surveying inside the building for the site of application. Manual sight survey is expensive and that restricts scaling to large areas of coverage. In the mid-2000s the Wireless Positioning System (WPS) industry evolved around the same idea with a new method for fingerprinting. In WPS, the RF cloud fingerprinting takes place by driving in the streets and tagging the collected data using a GPS receiver. This automated process enabled WPS systems to scale to metropolitan areas. For that reason, WPS was adopted for the original iPhone and it became integrated in all smart phones and smart devices since. In the remainder of this section, we explain how WPS works and how it is evolving to enhance the opportunistic wireless positioning industry.

Today, the most popular positioning system is WPS, which is the main positioning engine for hundreds of thousands of applications on smart devices. Skyhook, Google, and Apple own the three major Wi-Fi location databases of access points (APs) for these systems. The database of Skyhook, the pioneer of the technology, receives over a billion hits per day and includes close to a billion Wi-Fi access point addresses with their estimated locations. In the original WPS systems, cars driving in the streets of a city collected the RSS fingerprint of Wi-Fi devices identified by their MAC addresses provided in the floating beacon packets and tags them with the GPS readings of the locations. Intelligent algorithms process the big database of these readings to estimate the location of any device from its Wi-Fi readings in an unknown location. Therefore, WPS relies on GPS because it is a database asso-

ciating Wi-Fi addresses with GPS readings in the streets. The advantage of WPS is that it works indoors, where GPS does not work.

Initially cars driving in the streets of different cities collected the database. Then, organic RSS reading data from devices searching for their unknown location augmented the database of access point addresses and locations. The accuracy of WPS systems are typically around 10-15 meters [9], which is on the order of the average coverage of Wi-Fi. This accuracy is adequate for turn-by-turn navigation of cars in streets to differentiate building addresses from each other in urban areas. To increase the precision of WPS for indoor positioning applications, demanding a few meter accuracy to differentiate different rooms from each other, we need indoor manual fingerprinting, similar to RTLS, and that is expensive.

GPS is a physical real time system providing position information based on current readings of TOA from satellites. WPS is a cyberspace information system built on a big database and an intelligent search engine with intelligent algorithms.

Each time we agree that an application on our smart device can use our location address, we send a packet to the WPS database and WPS knows our device location. With around one billion hits per day, WPS service providers can extract cyberspace intelligence about our location. We can use this new outcome of WPS technology to implement location-time traffic analysis, geo-fencing (for supporting elderly people, animals, prisoners, and suspicious people), real-world consumer behavior analysis, location certification for security and privacy, positioning IP addresses, and customizing content and experiences [10]. These are secondary outcomes of WPS technology, enabling other cyberspace applications for location intelligence.

As we mentioned in section III.A.1, the current state of the art WPS technology without indoor fingerprinting has 10-15m accuracy. For accuracy in the range of meters, we need expensive indoor site surveys and fingerprinting. Typical smart

devices carry a number of other sensors such as accelerometer, gyroscope, magnetometer, barometer, step counter and compass. These devices provide information on speed and direction of movements of the device. Using hybrid AI algorithms, we can integrate these motions related information with the absolute position estimate from the WPS to enhance the positioning and to refine the tracking in indoor areas [10, 18-20].

Wi-Fi access points are installed in office buildings approximately 30 meters apart. In a typical office building such as Atwater Kent Laboratory at the Worcester Polytechnic Institute (approximately 50mX100m), each floor is covered only with 3-7 Wi-Fi access points. That is why we need fingerprinting to increase the precision to a few meters to differentiate rooms from each other. With the increase in smartness of office buildings, every room of this building has at least two IoT devices controlling the light and the temperature. IoT devices use Bluetooth Low Energy (BLE), ZigBee or other active RFID technologies, which have smaller coverage than Wi-Fi. Smaller coverage indeed helps the precision. Imagine we have an RFID with coverage of one meter, if we read its signal, we know our location with one-meter accuracy. With such density of deployment of small coverage IoT devices, we may not need indoor fingerprinting anymore. It can be shown that the precision of Wi-Fi positioning in a typical building (e.g. WPIs Atwater Kent Laboratory), with three Wi-Fi APs in 90 RSS based Wi-Fi positioning is a device-based positioning system. The metric data used for positioning is collected by the device independent from the communication network provider. We can apply this technology to cell tower positioning using fingerprinting of cell towers [23]. The advantage of this approach for cell tower positioning is that the positioning system takes advantage of cell towers from all cellular providers without any specific coordination. The positioning service provider drives in the streets to identify cell towers and develop a

database of their fingerprints tagged with the GPS location. Then using the RSS readings of the cell towers around a device, the service provider can come up with a position estimate for the device. The device needs to have a cellular chipset to read the RSS values of the cell towers.

As compared with Wi-Fi positioning, the density of cellular networks is far less: we have billions of Wi-Fi access points as compared with hundreds of thousands of cell towers worldwide. Therefore, the accuracy of these RSS based cell-tower positioning systems (CPS) is around 100-250 meters, which is significantly lower than WPS [9, 23]. However, CPS has a more comprehensive coverage, which includes highways as well as urban areas. The original iPhone did not include GPS and it used CPS as a backup for WPS for these areas. With the increase in density of deployment in 5G and 6G cellular networks, the gap between precision of WPS and CPS should reduce significantly. This intuitive observation needs to be justified by empirical research data.

WPS, CPS and GPS are device-based positioning systems, in which the device measures the features of the RF cloud for positioning. Another approach to positioning is network-based positioning, where cell towers or access points measure the features of RF signals from the device and send that to a central computational server to locate the device. The first popular application of this approach was the Uplink-Time Difference of Arrival (U-TDOA) positioning systems, designed in 2G cellular networks to comply with FCC regulations for E911 services for cell phones [10]. These TOA based systems utilize the difference between arriving signals from a cell phone to locate the device. One of the advantages of this approach is that we can locate a device without its active participation in the positioning process.

The U-TDOA provides for approximately 100m precision for E-911 service using existing cell tower signals [24]. This level of precision is not adequate for many

popular indoor and urban area positioning and navigation applications, but it has a comprehensive coverage, which makes it appealing for emergency response.

The U-TDOA was a patch solution to position because 2G standard organizations had not included positioning in their agenda. If we consider positioning as a part of the standardization of communication protocols, we should be able to achieve higher precisions using TOA and DOA technologies. The fundamental challenge for TOA based systems are sensitivity to multipath effects and need for atomic clock synchronization to achieve sub-meter precision. By integrating GPS clock with the cellular system standards, we can have a practical solution for synchronization, but multipath effects are serious, in particular with indoor areas [12].

Ultra-wideband transmission controls the effects of multipath arrivals by isolating them from one another, antenna beamforming focuses the transmission to a single path, and we can design algorithms for positioning in the absence of direct path [25]. The emerging 5G and 6G cellular system with massive MIMO and mmWave technologies benefit from ultra-wide band transmission as well. In theory, these characteristics of 5G/6G technologies can enable high precision TOA based positioning. However, implementation of these systems to make it available for precision sensitive positioning applications needs algorithm and system design with focus on performance evaluation in realistic positioning application scenarios. In general, standards organizations are focused on the increase in capacity, which directly affect the user experience. They need to increase their attention to positioning and navigation as a fundamental enabling technology for millions of applications. More details on design and performance evaluation of positioning systems are available in the lead authors recent book in this area [10].

2.2.2 RF Cloud for Motion Detection

Motions of the wireless device or objects close to the antennas of the wireless devices cause temporal fluctuations of characteristic of RF cloud features measured at the receiver antennas. Recently, a number of researchers have studied these characteristics of RF cloud from wireless devices for activity, motion and gesture detection. This area of research expects to revolutionize human-computer interaction and introduce a variety of other cyber space applications by taking advantage of the variations in RF cloud features due to motions in the environment.

Wireless communication receivers measure features of the RF cloud reflecting motions in the environment. Signal processing techniques help detect these motions and prepare them for cyberspace application development. Figure 9 illustrates the temporal variations of RSS of a receiver antenna in proximity of a transmitting antenna. The figure also shows the Fourier transform of the signal representing the Doppler spectrum and the short-term Fourier transform representing its spectrogram. Figure 9a shows a situation with no-motion, Figure 9b shows a situation with a hand held between the two antennas, and Figure 9c shows the results when the hand moves between the antennas. As the speed of motions increases, the bandwidth of the Doppler spectrum and the contrast of colors in the spectrogram increases. We can benefit from this change in depiction of the RSS characteristics, to develop hand motion related applications. All modern wireless devices measure RSS and many other features of the RF cloud that are available and accessible with software, opening an interesting area for motion related cyberspace applications.

The mmWave radar development environment (Fig. 5) also supports other aspects helpful in classification of motions. Figure 10 shows the range-velocity profile of the device illustrating motions of the finger in different directions. The mmWave sensor extracts velocity information, and consolidates it with the range data to

form the range-velocity profile. Figure 10a shows a hand, which is a strong reflector, at close distance from the radar and its corresponding profile. Figure 10b and 10c demonstrate that the finger movement creates radical velocities relative to the radar, and thus mirrored in the profile below. These depictions of motions open an opportunity for micro-gesture detection from finger motions.

In recent years, a number of researchers have benefited from RF cloud features to introduce innovative cyberspace applications. As a simple example, using an algorithm measuring variations of the RSS above its average value, one could detect the number of people attending a class [26], or monitor newborn babies in a hospital [27]. More complex cyberspace applications using opportunistic signals available in the RF cloud is achievable by using artificial intelligence algorithms and taking advantage of more complex features of the signal, such as CIR, CSI, TOA, and DOA. In recent years, a number of research laboratories have pursued this idea.

At the Worcester Polytechnic Institute, variations of the RSS of body-mounted sensors is used for activity monitoring of first responders to find out if a fire fighter carrying a device is standing, walking, laying down, crawling, or running [28-30]. These states of motion reflect the temporal behavior of the fire fighter, revealing the seriousness of the situation she or he is facing. The work in [28] uses traditional characteristics of the fading, such as coherence time, rms Doppler spread, and threshold crossing rate of the RSS of simple devices such as Bluetooth, to differentiate different motions and the work presented in [29] integrates AI algorithms into the motion detection process. The work presented in [30] benefits from more complex CSI signals of Wi-Fi devices along with more complex AI algorithms such as Long-short-term-memory Regressive Neural Network (LSTM-RNN), to increase the capacity of the system in differentiating different motions on a flat floor or when climbing the stairs. As we explained in section II.B.2, CSI provides multiple streams of RSS and more

diversified variations of the signal. In [31], the research group demonstrates the use of mmWave radar in tracking the motion of a finger, opening up further study in gesture-based application controls in the human-computer interaction (HCI) research area.

Researchers at the University of Washington [32] have used Wi-Fi signals for hand gesture recognition to differentiate nine different hand motions. Multiple RSS stream from different channels of the OFDM signal of Wi-Fi are depicted by a spectrogram to generate frequency-time characteristics color images. The AI algorithm classifies the image to detect the nine gestures of the hand motion. At Michigan State University [33], the CSI of a Wi-Fi signal is use for keystroke detection. When typing a certain key, the hands and fingers move in a unique formation and direction, there is a unique pattern of CSI RF fingerprint. By training an AI algorithm, they have detected the keystrokes of the keyboard user. At the Massachusetts Institute of Technology [34], researchers have used radar signals similar to the Wi-Fi signals with multiple antennas, for human pose estimation through walls and occlusions. They demonstrated detection of multiple human postures through the walls using the RF signal and a neural network algorithm. They used visual data captured by a camera during the training period for the AI algorithm. At Stanford University [35], commodity Wi-Fi signals are used for tracking hand motion for virtual reality applications to replace existing infrared devices.

In parallel with academic studies, practical applications of RF signals for motion and gesture detection and tracking are emerging in industry. As an example, Google [36] uses RF radar signals at mmWave frequencies obtained from antenna arrays, for micro-motion tracking of hand and finger gestures for applications such as connection less winding or rolling over the surface of a wristwatch. RF signal variations can replace any application using mechanical sensors. For example, the interactive

electronic games commonly use mechanical sensors such as an accelerometer, and an accelerometer mounted on the gait of a patient has been used to measure the extent of progress in Parkinson decease [37, 38]. The RF cloud of UWB devices, measuring the CIR, can replace many of these mechanical sensors and be used in interactive electronic gaming [39], to help visually impaired [40]; and to provide gait motion detection.

Building on the advances in motion, activity and gesture detection using RF Cloud, researchers have begun to explore the possibilities for future HCI applications. Early work explored using unmodified GSM signals to enable recognition of eight tapping gestures, four hover gestures and two sliding gestures around a mobile device, to enable incoming call management as well as phone navigation from a distance [41]. More recent work, has demonstrated an mmWave gesture recognition pipeline [36] as well as the recognition of eleven gestures with short-mmWave radar with a goal of them being used in human-computer interaction [42]. Other work explored mmWave gesture recognition for in-car infotainment control [43]. Radar signals have also been explored for automatically classifying everyday objects to support various applications including a physical object dictionary that looks up objects that are recognized, context-aware interaction, as well as future applications such as automatic sorting of different types of waste, assisting the visually impaired and smart medical uses [44]. Using radio signals and one external sensor hanging on the wall, researchers have demonstrated that gait velocity and stride length, which are important health indicators, can be monitored, enabling health-aware smart homes [45]. Taking advantage of indoor WiFi signals to identify motion direction, researchers have created a contactless dance exergame [46] as well as sign language gesture recognition [47]. Other work demonstrated that 5GHz WiFi can be used to achieve decimeter localization accuracy of up to four users as well as activity

recognition of up to three users doing six different activities [48].

2.2.3 RF Cloud for Security

In recent years, several researchers have shown interest in developing authentication and security applications benefitting from big data embedded in the RF cloud. These researchers look into various kind of devices, including Wi-Fi, Bluetooth, Zigbee and RFID, to evaluate the threat, to assess vulnerability of the systems, and to propose frameworks for specific authentication and security schemes.

To analyze the security of the networks, it is customary to refer to a layered architecture [49]. Figure 11 shows a general layered architecture and the relations among different layers. The architecture of the security system in this figure consists of three layers: perception layer, network layer, and application layer. The functionality of the perception layer is data collection, preprocessing of data, and secure transition of this data to the network layer. The network layer checks the security of data and transmits it to the application layer. The application layer analyzes and process the data to support the application.

Since most of the RF data collection sensors are deployed in environments with no human supervision, and the data is collected through a wireless medium, this data can be easily monitored, intercepted and modified. In these environments, an attacker can access the sensor and take control of the device or damage these sensors or physically remove them from their assigned location. As a result, most of the security designers for RF cloud applications implement their measures at the perception layer.

Application of machine learning methods for classification of devices for authentication and security has been very popular in the recent literature [50]. The time-domain features of the RF cloud from Wi-Fi have been used to train a classifier

to differentiate between trusted and un-trusted devices operating in close vicinity of each other [51]. Researchers have also examined physical authentication using a unique coding technique to generate location-related public keys based on RF cloud signature in a given location [52].

At the perception layer of security systems, we can use the fingerprint of these feature for RF authentication. Fingerprinting is the process of identifying radio transmitters by examining their unique transient characteristics at the beginning of transmission. A complete identification system has been presented, which includes data acquisition, transmission detection, RF fingerprint extraction, and a variety of classification subsystems [53]. Following this pioneering work, a number of researchers have examined different machine learning methods for RF cloud related research in authentication and security.

Using non-parametric and multi-class ensemble classifiers for RF fingerprinting, researchers demonstrated improved ZigBee device authentication over the traditional algorithms [54]. Other work extracted novel RF fingerprint features to design a hybrid and adaptive classification scheme adjusting to the environment conditions, and carries out extensive experiments to evaluate the performance of these systems [55]. A low-cost system has been introduced for bit-level network security, benefitting from physical unclonable functions, which is challenging to replicate [56]. A device recognition algorithm based on RF fingerprint has also been proposed [57]. In this work, a Hilbert transform and principal component analysis are used to generate the RF data fingerprint of the device and traditional machine learning algorithms are used to classify the devices. The accuracy of RF fingerprinting employing low-end receivers has been evaluated showing that receiver impairment effectively decreases the success rate of impersonation attack on RF fingerprinting [58].

Another area of emerging security and authentication research related to RF cloud applications is the design of testbeds for risk analysis for IoT-based physically secure systems. To assess security risks, researchers have proposed testbeds and methodologies for risk analysis and evaluation of vulnerability [59][60]. There are other works proposing a testbed for authentication of IoT objects benefiting from RF fingerprinting, along with a machine learning technique [61, 62].

The general architecture of a WBAN is depicted in Fig. 2.1. As is shown in this figure, the patient wears a couple of sensors that monitor the patient's vital signs, such as blood glucose level, blood pressure, pulse rate, electrocardiograph (ECG) patterns and respiration rate; In the meantime, smart phone plays an important role in WBAN, since it is embedded with transceivers that enable both WiFi and Bluetooth connection for data transmission, as well as a rich amount of sensors that can provide patient's location and motion information, which further improve the e-health system. The on-body sensors, are consistently communicating with the local wireless sensor network (WSN), which consists of local servers (laptops, tablets and other smart phones) that can access to the local data, the wireless cameras, and environmental sensors, which can measure the important parameters such as temperature, air pressure and humidity. All the data gathered from local WSN then gets processed, aggregated and transferred to a remote network, where it is stored in a centralized healthcare database for permanent records and accessed by remote server for further clinical analysis and diagnosis.

The adoption of WBAN technology is promising to enhance the current healthcare system, but several security and privacy issues should be carefully addressed and dealt with before this idea is widely accepted by the public. First of all, the

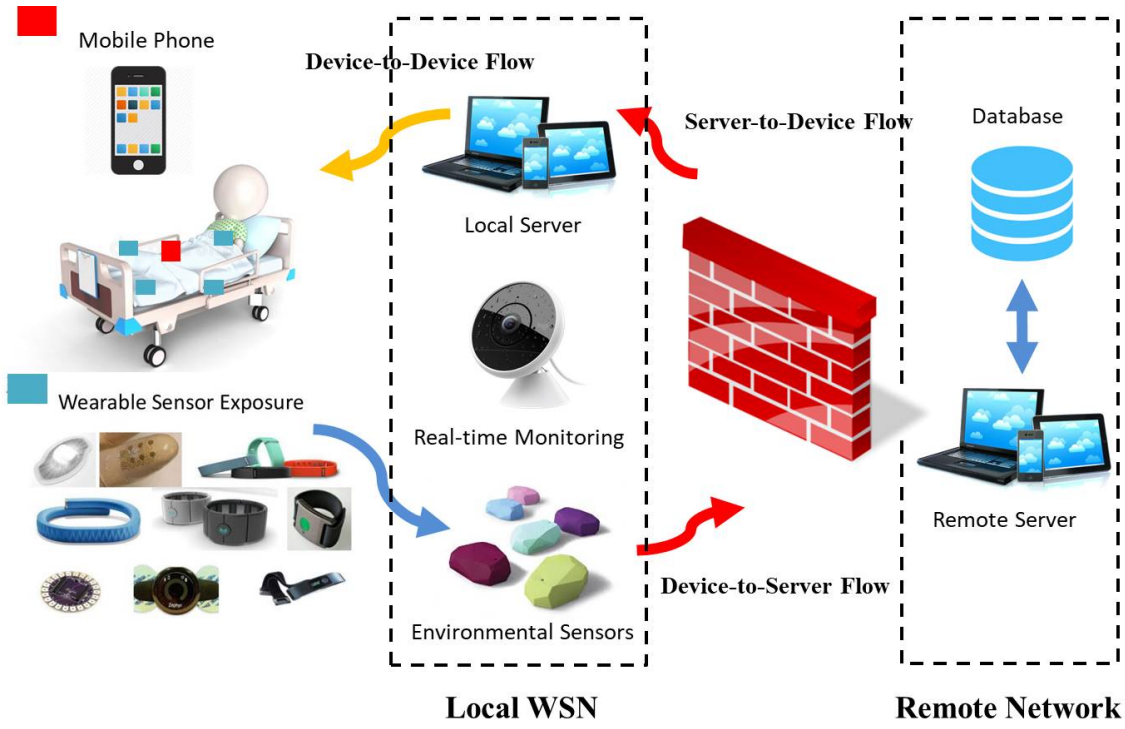


Figure 2.1: General Architecture

small, low-power, and low-weight wireless sensors on one hand can grant the system mobility, while on the other hand, are subjected to compromise. The sensor nodes can be easily captured by malicious people which may lead to disclosure of data. Therefore, it is important to design reliable sensors, in which data is well encrypted and stored. Secondly, malicious activities may occur during data transmission, and the attacker can modify the data by either altering control message field or forwarding routing messages with falsified values, causing redirection of network traffic and DoS attacks. The WBAN should be built upon reliable transmission where malicious activities can be detected and prevented. The third thing that needs to be mentioned is how these sensors should be authorized and how the data can be accessed. Even if there is no external attack, the issue of data privacy is still a key point of the entire system. To sum up, an effective e-health system with WBAN falls into:

- Designing reliable sensors
- Ensuring reliable transmission of data
- Providing privacy with authentication and access control

Since the patient-related data stored in the WBAN plays a critical role in medical diagnosis and treatment, it is essential to ensure the security of these data. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments.related data is often stored in a distributive manner; the open and dynamic nature of the WBAN makes the data prone to being lost. Therefore, it is equally important to protect patient-related data against malicious modification and to ensure its dependability (i.e., having it readily retrievable even under node failure).

Meanwhile, we must address various privacy concerns that may hinder wide public acceptance of WBAN technology. Especially access to patient-related data must be strictly limited only to authorized users; otherwise, the patients privacy could be abused. As a governmental initiative, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [4] has specified a set of mandatory privacy rules to protect sensitive personal identifiable health information. However, in WBANs distributively stored private data may easily be leaked due to physical compromise of a node. Therefore, data encryption and cryptographically enforced access control is needed to protect the privacy of patients.

So far, although there are already several prototype implementations of WBANs, studies on data security and privacy issues are few, and existing solutions are far from mature. For example, in the CodeBlue project [3] a medical monitoring sensor network is developed for pre-hospital care and emergency response. To cope with the dynamic environment of emergency response, an elliptic curve cryptography (ECC)-

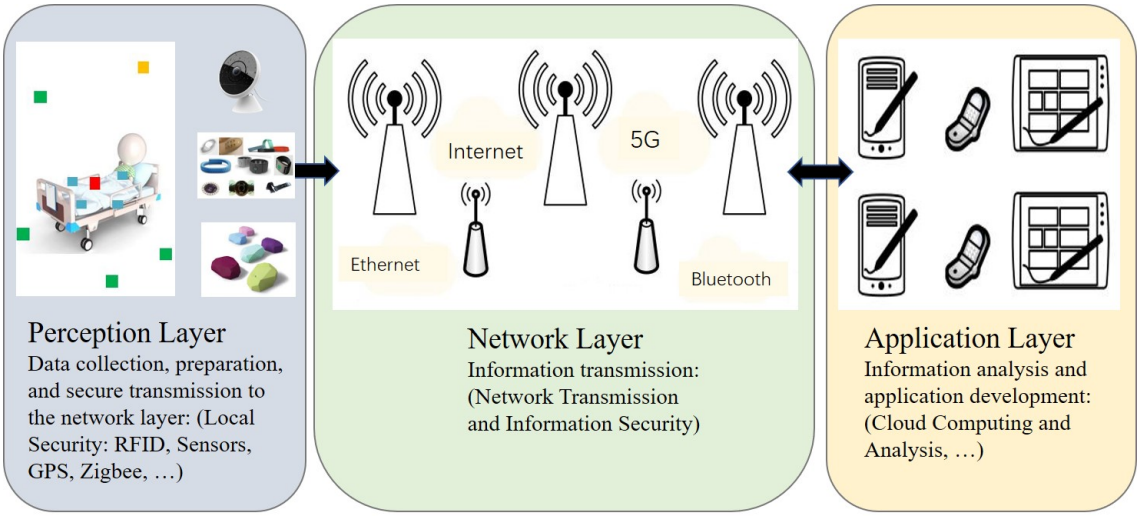


Figure 2.2: Architecture of a IoT System with three security layers

based public key encryption scheme is used for authentication. However, there are no further mechanisms to protect the security of the stored data and control access to it.

To satisfy the above requirements in WBAN, we face several important challenging issues, most of which arise from efficiency and practicality aspects. These issues constrain the solution space, and need to be considered carefully when designing mechanisms for data security and privacy in WBANs. Conflict between security and efficiency: High efficiency is strongly demanded for data security in WBANs, not only because of the resource constraints, but also for the applications. Wearable sensors are often extremely small and have insufficient power supplies, which render them inferior in computation and storage capabilities. Thus, the cryptographic primitives used by the sensor nodes should be as lightweight as possible, in terms of both fast computation and low storage overhead. Otherwise, the power and storage space of the nodes could be drained quickly. In addition, a DoS attack could easily overwhelm the whole WBAN if the authentication protocol is not fast

enough. Conflict between security and safety: Whether the data can be accessed whenever needed could be a matter of patients safety [2]. Too strict and inflexible data access control may prevent the medical information being accessed in time by legitimate medical staff, especially in emergency scenarios where the patient may be unconscious and unable to respond. On the other hand, a loose access control scheme opens back doors to malicious attackers. It is hard to ensure strong data security and privacy while allowing flexibleaccess. In CodeBlue [3], when there is network coverage, stronger user authentication is achieved by contacting an authority; when no infrastructure exists such as during disaster response, weaker or no authentication is adopted. Their approach can be regarded as the first step towards addressing the conflict between security and safety.

Conflict between security and usability: The devices should be easy to use and foolproof, since their operators might be non-expert patients. As the setup and control process of the data security mechanisms are patient-related, they shall involve few and intuitive human interactions. For instance, to bootstrap initial secure communication between all the nodes in a WBAN for secure data communication, device pairing techniques can be adopted. However, directly applying device pairing requires O(N2) human interactions, which is obviously not easy to use. However, increasing usability by omitting some manual steps may not be good for security. As another example, for Peter to give access to his data to an emergency medical staff person who was not originally authorized, it is better to have some second-factor authentication mechanisms.

Requirement for device interoperability: Patients may buy sensor nodes from different manufacturers, among which it is difficult to pre-share any cryptographic materials. It is difficult to establish data security mechanisms that require the least common settings and efforts, and work with a wide range of devices.

2.3 Sensors in IoT

Nowadays, smartphone is embedded with various sensors, among which, multiple sensors can be used for localization. Localization sensors measure certain characteristics related to the location of an object such as a device, person, car or drone, to position the object on a map. These sensors either provide us information on the distance from reference points to help us calculate the absolute location or they provide us with the velocity and direction of movement for calculation of displacement or the relative location of the object. One of the fundamental differences between the two methods is that the absolute localization needs an infrastructure of reference points but relative localization position the object relative to its previous location. Figure 2.3 shows two examples of the results of localization using absolute and relative positioning systems on a square route in a typical office building. Figure 2.3a shows the results of absolute Wi-Fi localization. The estimated locations (dots) are randomly distributed around the path of movement (solid line) of the object. Figure 2.3b shows the results of localization using an Inertia Motion Unit (IMU) device measuring the speed and direction of the movement. The estimated path of movement follow a straight line but, because of errors in angle and speed of movements, the location estimate gradually drifts from the actual path. Hybrid algorithms combine the results of the two class of sensor to achieve a more reliable navigation. These algorithms use the absolute localization to reduce the drift of IMU and use the IMU result to smooth the location estimates of the absolute location.

The most popular absolute positioning systems (GPS, WPS and CPS) sense

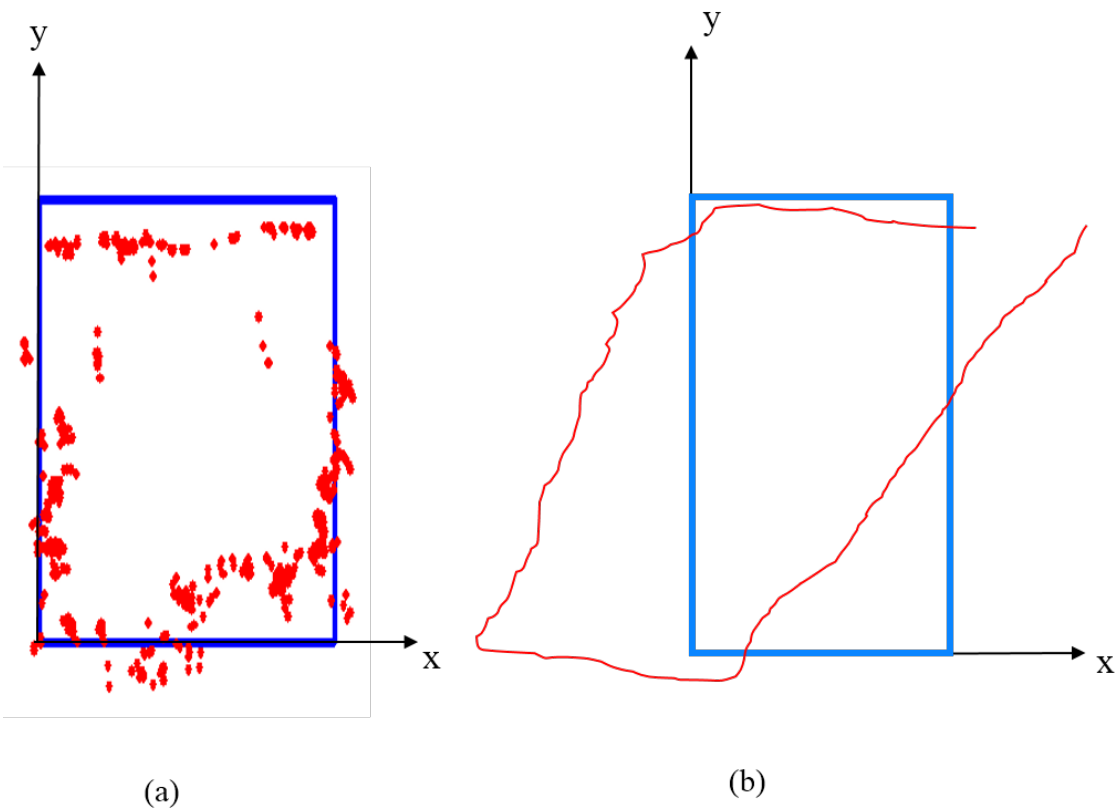


Figure 2.3: Results of localization with two classes of location sensing in square corridor route of an office (a) absolute localization using RSS of Wi-Fi access points (b) relative localization using IMU devices

features of the RF signals to measure the distance between the object and the reference points. The 26 satellites used as the reference points for GPS infrastructure are deployed for the purpose of positioning, while WPS and CPS opportunistically use the Wi-Fi and cell phone signals for localization. There are other opportunistic signals which can be used to measure the distance from a reference location. We can use TV or radio station transmitted RF signals and estimate the distance of a receiver from their towers. We can use an RFID reader to estimate the distance from an RFID and we can use the wireless video capsule endoscope transmitted signal to measure its distance from a body mounted sensor. Any wireless device, RF or optical, is a potential location sensor for absolute localization. Since absolute RF localization is the most fundamental and the most complex element of positioning in chapters 2-6 we discussed the behavior of RSS- and TOA-based ranging in different environments. In this chapter we present a brief discussion on the behavior of other sensors used for relative localization.

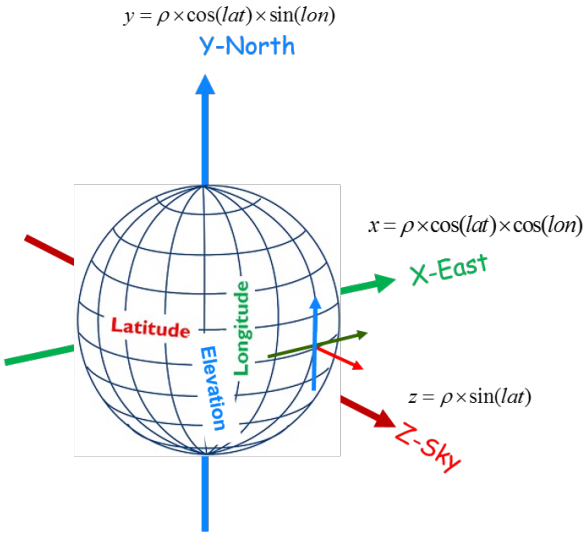
Relative positioning or inertial navigation uses the speed and direction of movement to locate a thing from a starting point without using any external reference. In classical navigation systems this approach is referred to as Dead Reckoning and the systems using them are called Inertial Navigation Systems. In relative positioning the sensor measures the speed and direction of movements of the Thing and does not need any infrastructure. We can measure the speed and direction using mechanical motion sensor or electronic devices. Accelerometers are mechanical devices measuring the speed (integral of acceleration) and gyroscopes measure the rotation angle. We can measure the speed also by number of rotations of the wheel (speedometer), Doppler spectrum of a received RF signal, the number of steps that a pedestrian walks, or similarities between the consecutive pictures taken by a video camera. We can measure direction using a compass or video pictures as well. Inertial navigation

is the classical techniques for military and commercial airplanes, ships, submarines, missiles and unmanned vehicle applications in GPS denied environments. In WPS commercial applications the speed and direction of motion are measures by counting the number and location of access points observed by a moving person or vehicle [Alizadeh, Ruijun]. In modern time IMU devices are used in robotics [Yunxing], interactive electronic gaming [Png pong], motion detection [Ruijun, Yishuang] and gesture detection [Washington U]applications.

2.3.1 Coordinate Systems to Visualize the Location

In order to position a location on a map we need a coordinate system to visualize the location information. For global positing of a location, we need to refer to the global 3D coordinates of the earth. The most commonly 3D coordinates of the Earth (Fig. 2.4a) are the geographical polar coordinates commonly referred to as: longitude, latitude and altitude (θ, ϕ, ρ). Longitude expresses angular deviation from east to west on the surface of the Earth in degrees and latitude is the angular deviation from north to south in degrees. Elevation shows the distance from the center of the Earth and it is usually given with respect of the sea level height. In the aerial vehicle applications elevation is referred to as altitude.

Ground navigation systems for outdoor and indoor areas track movements of the vehicles or robots on 2D maps such as layout of a floor of a building or 2D map of streets of an urban area in area for which altitude does not change substantially. Even in multi-floor 3D applications we use a 2D map with the floor number (a representative of altitude). Cartesian coordinates provide a better tool for visual tracking for most of popular applications in indoor and urban areas. Therefore, we usually convert longitude, latitude, and altitude to a Cartesian form using:



(a)

```
%       Prepared by: Michael Kleder, April 2006
function [lat,lon,alt] = ecef2lla(x,y,z)
% WGS84 ellipsoid constants:
a = 6378137;
e = 8.1819190842622e-2;
% calculations:
b   = sqrt(a^2*(1-e^2));
ep  = sqrt((a^2-b^2)/b^2);
p   = sqrt(x.^2+y.^2);
th  = atan2(a*z,b*p);
lon = atan2(y,x);
lat = atan2((z+ep^2.*b.*sin(th).^3),(p-e^2.*a.*cos(th).^3));
N   = a./sqrt(1-e^2.*sin(lat).^2);
alt = p./cos(lat)-N;
% return lon in range [0,2*pi)
lon = mod(lon,2*pi);
% correct for numerical instability in altitude near exact poles:
% (after this correction, error is about 2 millimeters, which is about
% the same as the numerical precision of the overall function)
k=abs(x)<1 & abs(y)<1;
alt(k) = abs(z(k))-b;
return
```

(b)

Figure 2.4: (a) Earth 3D polar coordinate system with elevation, longitude and latitude, (b) MATLAB code for conversion of (lat, lon, alt) coordinates to Cartesian coordinates [Kle06]

$$\begin{cases} X = \rho \times \cos(lat) \times \cos(lon) \\ Y = \rho \times \cos(lat) \times \sin(lon) \\ Z = \rho \times \sin(lat) \end{cases}$$

Figure 2.4b shows the MATLAB code to map the polar coordinates to 3D Cartesian coordinates using above equations. The LLA2ECEF in MATLAB convert latitude, longitude, and altitude to earth-centered, earth-fixed (ECEF) Cartesian coordinates.

In absolute positioning, a GPS, CPS or WPS location fix in polar or in Cartesian coordinate, represent a point in the 3D world frame coordinate. In relative positioning we represent the velocity and direction as vectors at each location. Accelerometers and gyroscopes are mechanical devices used for measurements of differential vectors for acceleration and rotation. We integrate the differential acceleration

to determine the instantaneous velocity vector and we integrate the rotation vectors to determine the direction of motion.

In the universal Cartesian reference coordinate system, shown in Fig. 2.5a, an acceleration or velocity vector in X-axis defines a vector tangential to the ground at the measurement sensor's current location pointing to the East. The vector in Y-axis is tangential to the ground at the measurement sensor's current location and pointing towards magnetic north. A vector in Z-axis points towards the sky and perpendicular to the ground at the location of the measurement sensor. However, as shown in Fig. 2.5b, measurement sensors are MEM devices installed in a device, such as a smart phone, and their coordinates are defined relative to the devices screen and not the universal earth coordinate. When a device is held in its default orientation, the X-axis is horizontal and points to the right side of the device, the Y-axis is vertical and points up to the top of the device, and the Z-axis points toward the outside of the screen face. In this system, coordinates behind the screen have negative Z-values.

2.3.2 Sensors and Platforms for Opportunistic Localization

Opportunistic localization is based on the location sensor payload of the platform we want to localize. Platform could be a smart phone, a land robot, a Drone, a car, an autonomous unmanned vehicle AUV), a drone, an airplane, a ship, a submarine, a guided missile, a satellite or a wireless endoscopy capsule. Each of these platforms carry certain number of location sensor and they need certain positioning precision and navigation needs in their environment of operation. A smart phone or an intelligent may carry many sensors for opportunistic localization serving different positioning and navigation needs, a wireless endoscopy capsule may carry only a camera which uses RF signal to carry the images from inside to the surface of the

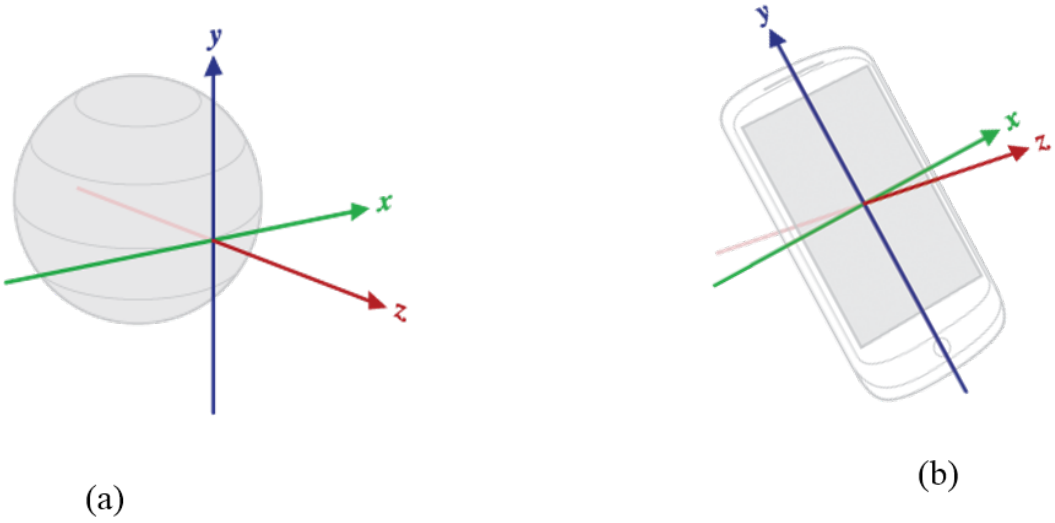


Figure 2.5: Cartesian coordinate system for relative localization vectors (a) in universal frame coordinate: x-axis towards east, y-axis towards north pole and z-axis towards sky (b) local device coordinate relative to the screen: x-axis points to the right, y-axis points to the top, and the z-axis points toward the outside of the screen face.

body.

Typical smart phones carry RF based GPS, Wi-Fi, Cell Phone, and iBeacon (Bluetooth Low Energy) chip sets, which support a variety of opportunistic RF localization capabilities for different environments and precision requirement. In addition, they carry a number of other sensors which can be used to enhance positioning of the device using traditional RF signals. Table 7.1 shows typical sensors available in an Android device and their functionality if they are used for localization [Android1,2]. In addition to the traditional sensors such as gyroscope, magnetometer, accelerometer and barometer, we have sensor for ambient light, temperature, and humidity as well as force of gravity levels, proximity and step counts. The sensors can be beneficial for localization applications to enhance precision of RF localization. We can use the data collected by these sensors for 3D localization, calculation of speed and direction of movements and specifying the environment of operation. Positioning algorithms use RF location and motion information obtained from a variety of sensors. These sensors perform differently in different environments. For example, GPS which provides very reliable information for outdoor navigation does not operate deep in indoor areas. Therefore, in addition to the algorithm to determine the location, we need to have an algorithm to detect the environment to distinguish between the indoor and the outdoor environments. The data from all sensors is available as a resource to a positioning engineer to design different algorithms to achieve the precision requirements in the environment of operation.

Other platforms carry different sets of sensors. A ground robotic platforms usually carries a camera similar to a smart phone but the camera is always on because robots do not have battery restrictions of a smart phone. As a result, robots usually use the camera images and the so called Simultaneous Localization And Mapping (SLAM) algorithms [???] to map the environment and localize the

position of the robot on the map. Robots may also carry RF based localization tools such as Wi-Fi, Bluetooth, RFID readers, and optical proximity check devices. The speed of the wheel of the ground robot provides a speedometer and the robot may carry accelerometer, gyroscope, magnetometer or many other sensors useful for localization. Depending on the environment and precision needed for the application a navigation engineer may use any or a set of theses sensors. For example, a vacuum cleaner robots may use SLAM with one or multiple cameras to create a map of the environment to be cleaned and the location of the robot in the map to provide an intelligent cleaning service with comprehensive coverage of the area to be cleaned. A robot operating in a warehouse for automated movement of the material on the warehouse floor may use an RFID reader and install RFID enabled floor tiles to support sub-meter accuracies in warehouse floors. For cooperative robot operations one may resort to multi-sensor hybrid localization to combine the speed of the wheels and direction of movement from IMU with the RF localization capabilities of the robot [Nader]. A wireless video capsule endoscope operating inside the human body may use the videos and RSS and/or TOA of the RF signal carrying the video images from inside to the surface of the body to map the route inside the small intestine and location of the peel on the route [Bao].

Aircrafts mainly rely on IMU devices and GPS for navigation. Car navigation systems also rely on GPS and can use speedometer (number of rotations of the wheel) and front wheel angle to supplement GPS in GPS denied areas such as tunnels or environments challenging GPS precision such ad inside urban canyons. Cameras and optical sensors in the cars can be used for collision detection and automated navigation on the road. The navigation systems of automated unmanned vehicles can also benefit from mechanical IMU devices for more precise measurements of speed and angle of movement. With increase in popularity of Wi-Fi for car com-

munications, Wi-Fi localization can also be thought as a supplementary positioning tool for the cars. An in-car geolocation system may use Bluetooth signal used for hand-free communication between phones and the car to locate things inside the cars or to detect gestures of the driver [??].

2.3.3 Physical IMU Device Sensors

Opportunistic localization of smart phones are more challenging than localization of other platforms such as cars, robots or drones because smart phone platforms are designed to implement millions of applications and they operate indoors, outdoors and sometimes even under the water. As a result, smart phone carry a relatively large number of sensors. Table 7.1 outlines typical smart phone sensors and classifies them into three category. These sensors are used for opportunistic positioning and tracking of the device as well as sensing the environment of operation. Mechanical and electromagnetic sensors can provide information on velocity and direction, and environmental sensors can be used for differentiating the environments. We begin by description of characteristics of mechanical and electromagnetic sensors.

IMU devices are perhaps the most popular relative localization systems traditionally used in aircrafts, satellites, UAVs and missiles to provide stability. Another traditional application of these devices is for navigation in GPS denied environments such as inside the jungles, tunnels, inside water or indoor areas and when the GPS signal is jammed by interference. More recently these devices have penetrate consumer device market in smart phone, PC mouse, Drone and even inside iBeacon sensors. IMU devices can be manufactured with a wide raging of sizes and prices going from less than a dollar for a penny size MEMS chip to over hundred thousand dollar for complete navigation back pack unit. Figure 2.5 shows three different IMU

devices with their size and approximated cost.

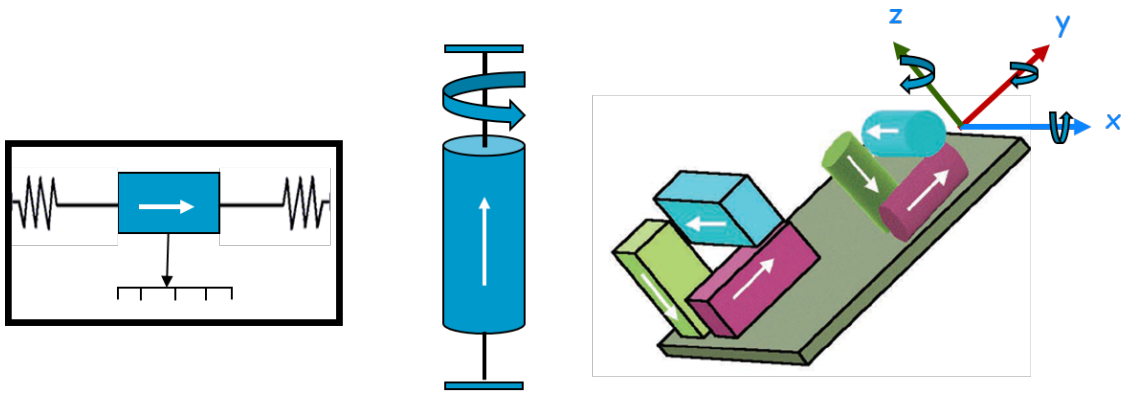
IMU devices carry accelerometer, gyroscope and sometimes magnetometer in one unit and use them for relative localization (Fig. 2.3b). The mechanical accelerometer and gyroscope measure the speed and direction and magnetometer is used for measurement of angular rotations of the device against the gravity of the earth [Gyro]. Today MEMS implement accelerometers, gyroscopes and sometime the magnetometer on small IMU chipsets used in smart phones, robots, computer mouse, interactive electronic games, toys and other smart devices.

2.3.4 Accelerometer Sensor

Accelerometer sensor measuring the acceleration (differential rate of variations of velocity) applied to a device in meter per square second (m/s^2) in the local Cartesian device coordinates (Fig. 2.5b).Figure 2.6a shows the basic concept inside an accelerometer. A weight is hanging between two springs in a box and the displacement of the weight due to external forces moving the box is measured to calculate the acceleration in the direction of movement. The left side of Fig. 2.6c shows how we can measure 3D acceleration of a plate carrying three accelerometer boxes placed in orthogonal directions.

Conceptually, an accelerometer measures the forces applied to the sensor in different directions and using Newtons second equation calculates the acceleration by dividing the force by mass of the sensor. When an IMU device rests in a place on a table in parallel to the earth surface, the accelerometer of the device should read a magnitude of $g = 9.81m/s^2$, the gravity of the earth. When the IMU device is in free-fall and therefore accelerating towards the ground at $9.81m/s^2$, its accelerometer should read a magnitude of $0m/s^2$.

In order to measure the real acceleration of the device, also referred to as



(a) (b) (c)

Figure 2.6: (a) Basic concept of an accelerometer, measuring movement of a weight (b) basic concept of a gyroscope, measure angle of rotation of a weight along an axis, (c) 3D accelerometer and gyroscope differential values in a device.

linear-acceleration, the contribution of the force of gravity must be eliminated. Applying a high-pass filter to the results of accelerometer readings eliminates the slow changes of the readings caused by gravity and detects the fast changes introduced by movements of the device. Conversely, using a low-pass filter isolates the force of **Gravity** and eliminates the fast changes in the acceleration caused by the movements of the device.

2.3.5 Gyroscope Sensor

Gyroscope sensor measure the differential rotation momentum around the local x, y, z axis of the device Cartesian coordinates in radians/second. Figure 2.6b shows the basic concept behind a gyroscope. A cylindrical mass is hanging around a central shaft like a wheel, as we change the direct wheel tits and we measure the angular displacement of the wheel. The coordinate system is the same as the one is used for the acceleration sensor. The right side of Fig. 2.6c shows how we can measure the rotation in 3D around each of three axis of the device by placing three gyroscopes

in orthogonal directions. The output of the gyroscope is integrated over time to calculate a rotation describing the change of angles over time.

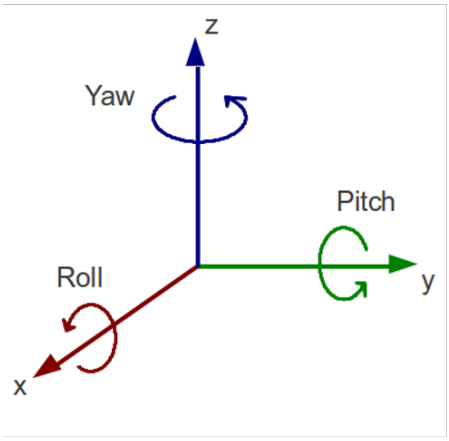
Rotation is positive in the counter-clockwise direction. That is, an observer looking from some positive location on the x, y or z axis at a device positioned on the origin would report positive rotation if the device appeared to be rotating counter clockwise. If we refer to angular speed around the x-axis as ψ angular speed around the y-axis as θ and angular speed around the z-axis as ϕ (Fig. 2.7a). The Eulers transformation maps the accelerometer readings, $a(t)$, from the device coordinates to the universal coordinate:

$$\begin{bmatrix} a_X(t) \\ a_Y(t) \\ a_Z(t) \end{bmatrix} = \begin{bmatrix} \cos\theta\cos\psi & \sin\phi\sin\theta\cos\psi - \cos\phi\sin\psi & \cos\phi\sin\theta\cos\psi + \sin\phi\sin\psi \\ \cos\theta\sin\psi & \sin\phi\sin\theta\sin\psi + \cos\phi\cos\psi & \cos\phi\sin\theta\sin\psi - \sin\phi\cos\psi \\ -\sin\theta & \sin\phi\cos\theta & \cos\phi\cos\theta \end{bmatrix} \begin{bmatrix} a_x(t) \\ a_y(t) \\ a_z(t) \end{bmatrix}$$

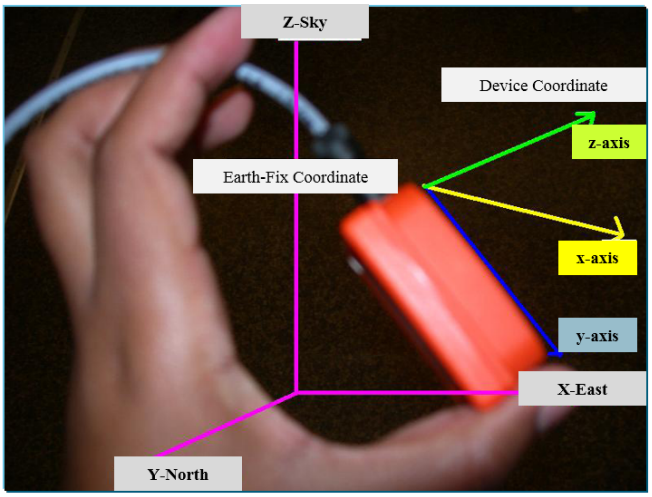
Figure 2.7b shows a typical IMU device with both the device and the earth-fix coordinates. To find the location from the above equation we need to take a double integral. The first integration provides the velocity in each direction and the second integral provides the distance traveled by the device in each direction.

In practice, the gyroscope noise and offset will introduce some errors which need to be compensated for. This is usually done using the information from other sensors. The gyroscope cannot be emulated based on magnetometers and accelerometers, as this would cause it to have reduced local consistency and responsiveness. It must be based on a usual gyroscope chip. Most recent systems are of the strap down type, where the IMU sensor outputs are taken directly and processed to compute the orientation and displacement of the vehicle.

Example 7.1 (motion prediction for a typical IMU unit)



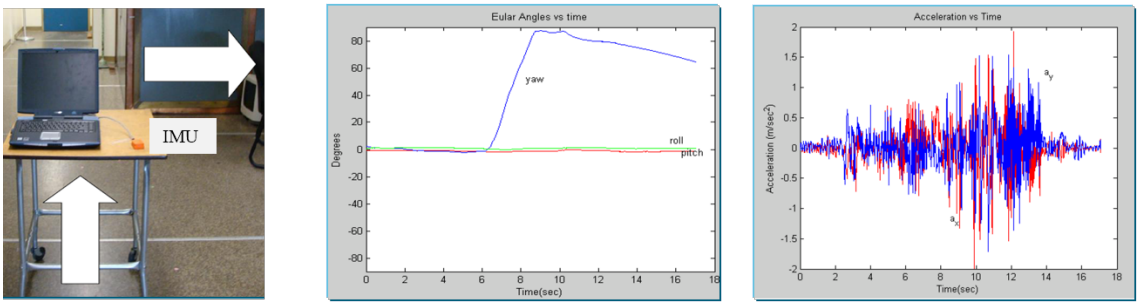
(a)



(b)

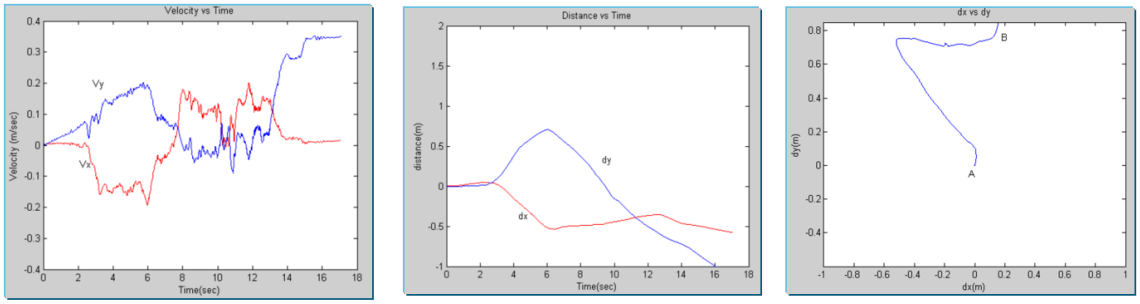
Figure 2.7: (a) Definition of angular rotations Roll, Pitch and Yaw. Direction of rotation is counterclockwise if we look from the origin of the coordinate (b) A typical IMU device with local device coordinates and universal earth-fix coordinates.

Figure 2.8a shown a simple laboratory experiment moving the IMU device shown in Fig. 2.7b forward and then turning to the right. The IMU device is a relatively expensive device purchased in mid-2000 for approximately 3500. Fig. 2.8b, c show the three dimensional readings of the gyroscope and accelerometer of the device. The gyroscope reads the pitch, yaw and roll in radian/second. The only rotation with this scenario of motion is around the z-axis for the yaw angle and pitch and roll remain at zero. Acceleration only has reading in x and y coordinates because we have no vertical motion. These values changes ups and down. Figure 2.9a,b shows the results first and second integral of the results after applying Eulers equation combining the results of accelerometer and the gyroscope (Eq. 7.2). The two figures represent the speed and travelled distance recorded by the laptop. The linear speed that is the square root of the sum of squares of the speeds on the x and y axes should remain relatively constant representing the speed of movement. Figure 2.9c shows the trajectory of the movement of the device as predicted from



(a) (b) (c)

Figure 2.8: (a) Scenario of movement of an IMU device resting on a table and controlled by a laptop (b) readings of angular movements of the gyroscope, (c) readings of the accelerometer.



(a) (b) (c)

Figure 2.9: (a) Integral of the rotated movement after applying Eulers equation, (b) double integral representing motions in x and y axes in time (c) trajectory of movement of the device.

the results of IMU sensors readings. Results are similar to those of Fig. 2.3b, which was obtained from another IMU unit.

2.3.6 Magnetometer

Magnetometer is a magnetic field sensor measuring the ambient magnetic field along the 3 sensor device local x, y and z axis in micro-Tesla (μT). Modern MEMS magnetometers measure the current induced in a coil (Fig. 2.10) due to changes in the magnetic field in the surrounding environment. Figure 2.9a shows the basic

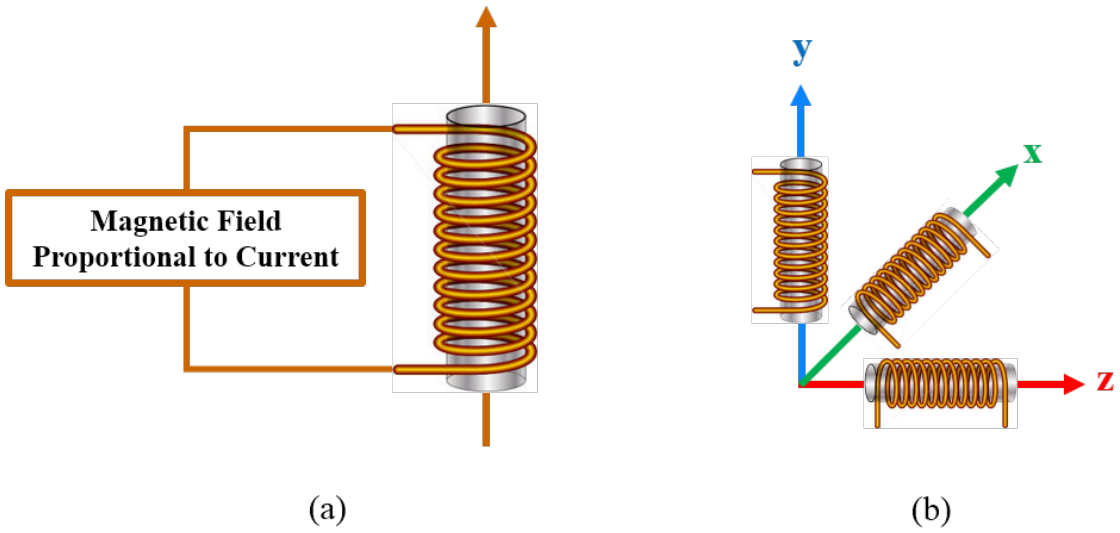


Figure 2.10: (a) Basic concept of a magnetometer (b) implementation of a 3D magnetometer on device coordinate.

concept behind modern magnetometer devices. The intensity of the induced current in the coil is used as a measure for the strength of the magnetic field. Figure 2.9b (similar to Fig. 2.6c) shows how the 3D magnetic field can be measured with a device. Since magnetometers, measure strength and direction of magnetic field, they are also useful for measurement of the direction for localization and tracking. In the next section we explain how we can design an electronic compass from readings of a MEMS magnetometer inside a smartphone.

2.3.7 Virtual IMU Device Sensors

In the previous section we introduced accelerometer, gyroscope and magnetometers to show how they are used for calculation of velocity and direction of movement. The accelerometer provides the velocity and distance travelled, gyroscope is used for measurement of rotations and magneto meter for measuring the ambient magnetic field. By processing measurements from these sensors we are able to sense

other characteristics of the environment useful for positioning and navigation. In our discussion about accelerometer we explained that using a high pass filter we can eliminate the effects of earth gravity to calculate the linear acceleration of a device, which is needed to determine the location displacements of a sensor. Using similar processing techniques we can sense we are able to sense other characteristics of the environment. I this section we introduce a few of these sensors.

2.3.8 Gravity Sensor

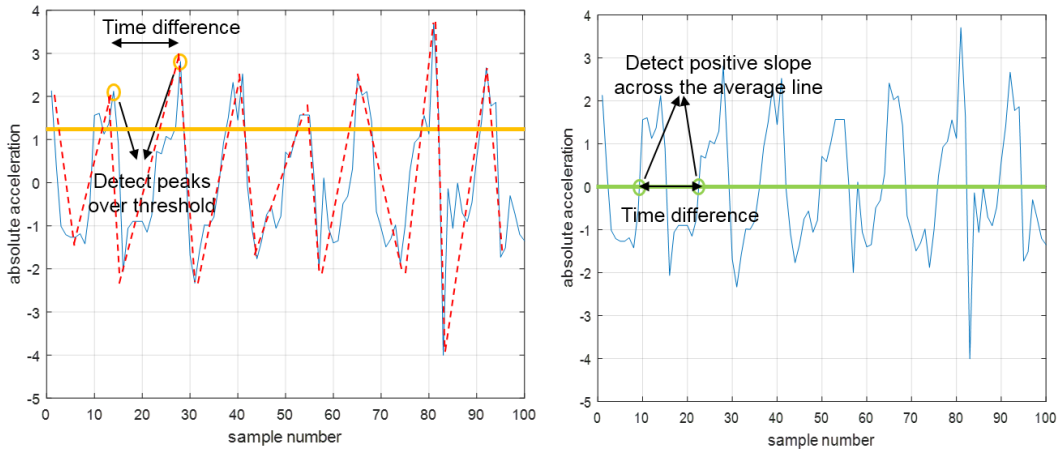
If rather than high pass filtering we low pass filter the measurements from an accelerometer we measure the force of **Gravity** in the device coordinate. The magnitude of this vector is $9.81 m/s^2$ and its 3D (x, y, z) values reflect the effects of gravity on each of the three axis. These are values that we should subtract from the acceleration vector components to determine the linear acceleration. The value of the gravity vector in device coordinate is used for turning the smartphone and pads screens to be in parallel to the eye of the person reading the screen. Considering device coordinates shown in Fig. 2.5b, if the gravity force along y-axis is the highest component, device is in up position and screen with smaller top is used. When the x-axis is the highest device is in the side position and the screen with long top is used. When device is resting on the floor z-axis is the largest value and the screen can be turned off. Results of gyroscope and magnetometer measurements are often used to complement the result of gravity force measurement obtained from the accelerometer. When the device is at rest, the output of the gravity sensor should be identical to that of the accelerometer.

2.3.9 Step Counter Sensor

Step counter counts the number of steps taken by the pedestrian carrying a smart device such as a smartphone or a health monitoring band. The value is in integer and it reset to zero on a system reboot. The timestamp of the event is set to the time when the last step for that event was taken. The obvious application of this sensor is in fitness tracking applications but it is also useful for indoor geolocation using smart devices.

We can implement a step counter by using the measurements from an accelerometer. Figure 2.11 shows hundred samples of magnitude of the accelerometer measurements for an Android phone. Considering Eq. 7.2, the magnitude of the acceleration is $a(t) = \sqrt{a_x(t)^2 + a_y(t)^2 + a_z(t)^2} - g$. Figure 2.4a shows the pattern of changes in acceleration between steps of a pedestrian carrying a device with accelerometer with hands. In each step first the pedestrian increase accretion of the body torso (carrying the hands and the device) using the landing foot and then she/he reduce the speed by applying negative acceleration to land on the other foot. As a result, variations of the magnitude of the accelerometer measurements follows a zigzag pattern on each step. We can detect the number of steps by counting the zigzags and that can be done either by peak detection or by detecting the zero crossing. With the peak detection algorithm we detect all peaks above a threshold and we select the highest in a window of time associated to the time for one step (Fig 2.11a). For zero crossing we find the intersect between the line representing the average acceleration and rising (or falling) parts of the plot (Fig.2.11b).

Using the step counter and the time stamps associated with each step, the average speed and the average step size can be determined and with that we can estimate the linear distance traveled by a pedestrian carrying a device with an accelerometer. To position the location of a pedestrian in a 2D map indoors or



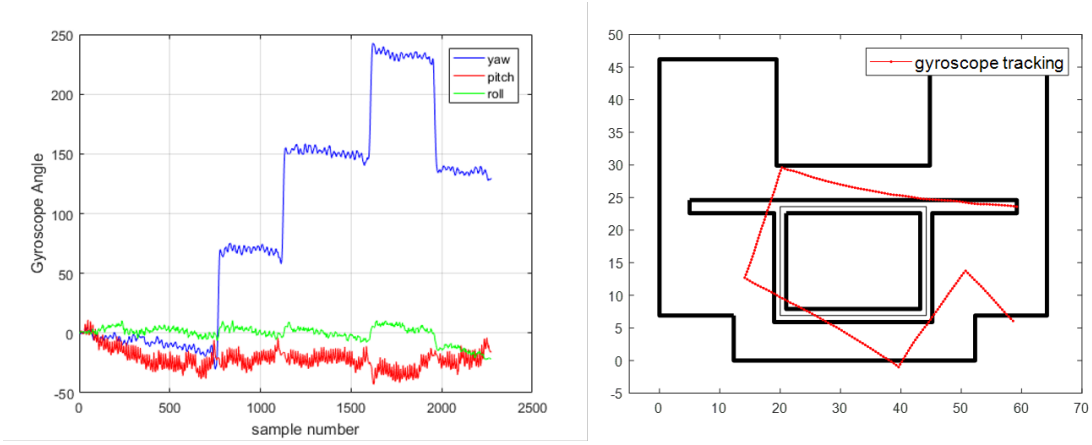
(a) (b)

Figure 2.11: (a) Step count using peak detection, (b) step count using zero crossing.

outdoors we also need to measure the rotations. Rotation can be measured with the results of gyroscope or the compass.

Example 7.2 (positioning using step counter and gyroscope)

Figure 2.12 shows the results of an example relative localization system using the step counter and gyroscope of a typical smartphone at the third floor of the Atwater Kent Laboratory at the Worcester Polytechnic Institute. The schematic of corridors of this floor of building and layout of the exterior of the building in shown on the right figure. A user carrying the smartphone enters the floor from right to and walks straight and then around the central corridors before turning back to the original location. User holds the smartphone in front of the torso in parallel to the ground. In this posture the z-axis of the smartphone is towards the ceiling and the only rotation of the device is around this axis. Figure 2.12a shows the results of gyroscope readings in the three dimensions. There are four jumps in rotations around the z-axis (Azimuth or yaw) associated with four 900 turns in the route of movement of the device. The red line in Fig. 2.12b illustrates the estimated path



(a) (b)

Figure 2.12: (a) Result of 3D gyroscope measurements (b) localization using step count and gyroscope.

of movement when the results of step counts is complemented with the gyroscope readings. Typical increasing pattern of the drift of the location estimate away from the actual path of movement is observed. This type of error pattern is caused from using speed and direction of movement for relative localization and it is similar to the error pattern of Fig. 2.3b.

2.3.10 Electronic Compass

Compass is one of the oldest mechanical magnetometer historically used for navigation. If we lay a compass in parallel to the earth surface the heading of the compass magnet points to the magnetic north. As a results, by rotating the compass to point towards a specific direction we measure the angle of that direction with respect to the magnetic north. This angle provides us with direction for relative navigation. A compass takes advantage of the Earth electromagnetic field to determine the rotation angle of the device. Earth acts like a large dipole magnet with magnetic field lines originating from magnetic south pole (near the geographic south pole) and terminating in magnetic north pole located near the geographic

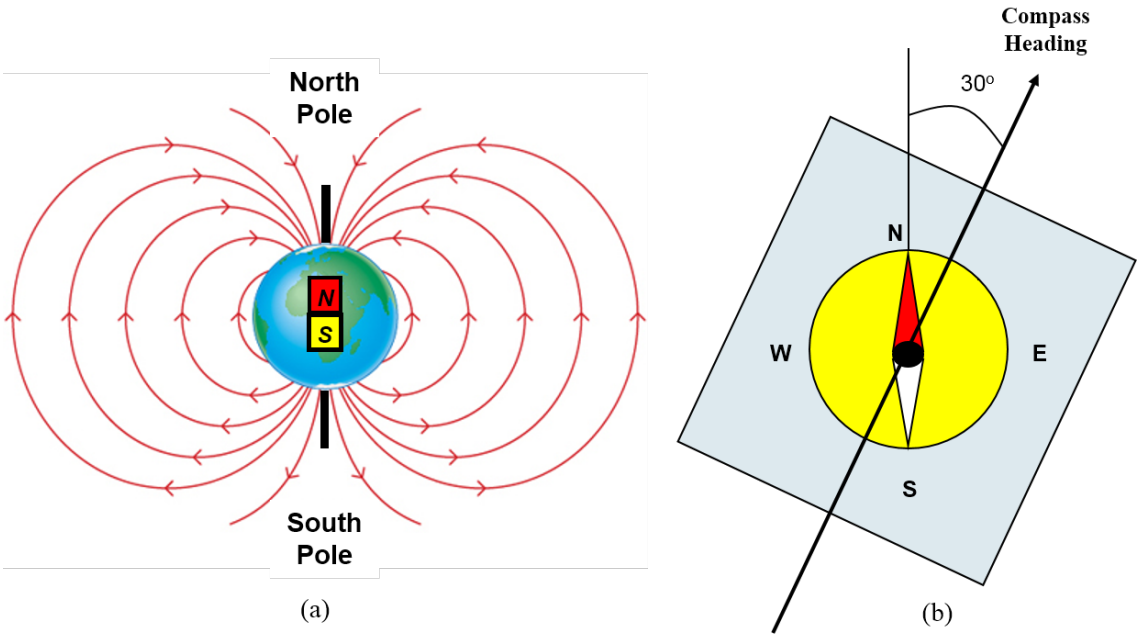


Figure 2.13: (a) Magnetic Field of the Earth and North/South Poles (b) a traditional compass and measurement of compass heading (direction) angle.

north pole (Figure 2.13a). A compass has a small magnet in the center aligning with the magnetic north pole in all locations on the surface of the earth. The angle between the compass heading (the magnetic north) and the geographic north is called the magnetic declination angle (Fig. 2.13b). The value of the decantation angle changes in location as well as in time. If we know the direction of geographical north in a location we can align the compass to that and measure the declination angle as the angle between the heading of the compass magnet and direction of the geometric north. In the east coast of United States inclination angle can go as low as -22° (22°W) and on the west coast it can be as high as 22° (22°E).

Example 7.3 (finding declination angle in a location)

The National Oceanic and Atmospheric Administration (NOAA) has a public web calculator for calculation of magnetic declination angle around the Globe [NOAA]. Using this web site we read $-14^\circ 35'$W on December 22, 2017 in New-

ton, MA at a location with 130ft elevation and longitude, latitude of (42°20′8″N, 71°12′14″W). Results indicate that the accuracy of values are within 22″ and the estimated value declines 4′E each year.

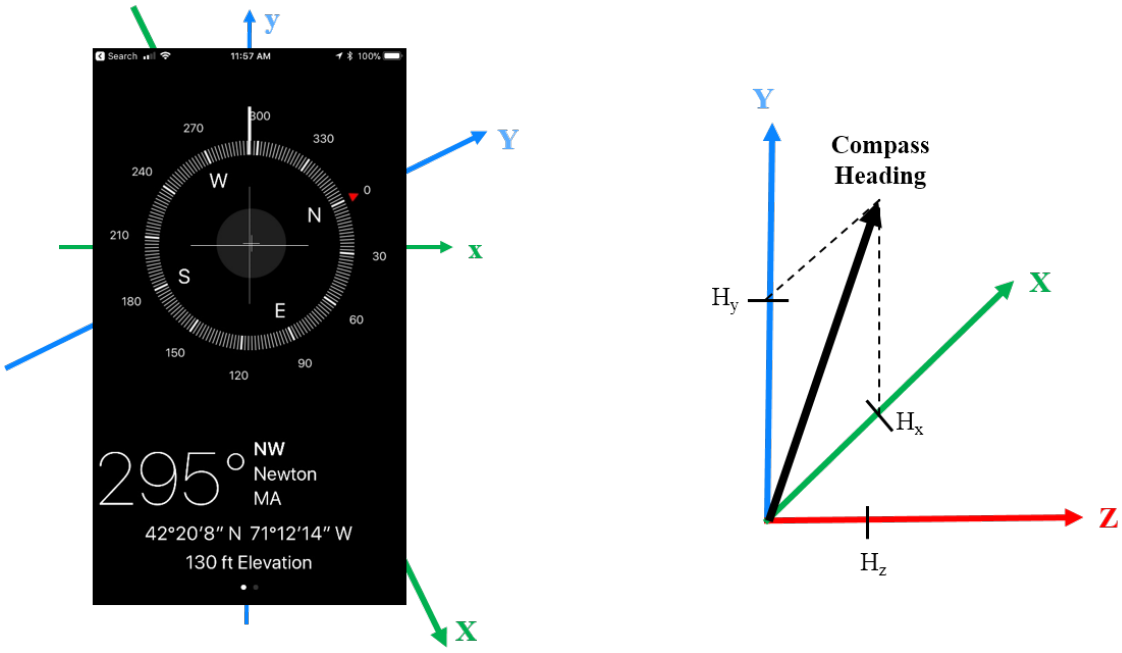
All popular smartphones in the market carry an electronically emulated compass application. These applications typically emulate the compass using the results of magnetometer, commonly available as a part of the IMU chip of the smartphone. Figure 2.13a shows a typical electronic compass implementation on an iPhone when the device is facing upward (z-axis of the device and the Earth fix coordinates are aligned). The scaled round shape on top of the figure allows visualization of the angle between the north axis (y-axis) of the Earth and the device to emulate the appearance of a compass. The Hx and Hy measurements of the magnetometer (Fig. 2.14b) defines the direction of compass heading in degrees using:

$$\theta = \begin{cases} 90 - \arctan\left(\dfrac{H_x}{H_y}\right) \times \dfrac{180}{\pi} & ; H_y > 0 \\ 270 - \arctan\left(\dfrac{H_x}{H_y}\right) \times \dfrac{180}{\pi} & ; H_y < 0 \\ 180^o & ; H_y = 0,\ H_x < 0 \\ 0^o & ; H_y = 0,\ H_x > 0 \end{cases}$$

As we turn the device around its z-axis, while laying the device on a table, the reading of the angle changes. For 346° (−14°) reading, shown in Fig. 2.14a, the device heading points to the geographic north in Newton, MA which has a declination angle of approximately 14° (Example 7.3).

2.3.11 Environment Sensors

In Table 7.1 we introduced a number of sensors commonly available on MEMS chips installed on the emerging smart devices. In the last section we described the



(a) (b)

Figure 2.14: (a) Electronic compass application on an iPhone with device and Earth coordinates (b) compass heading and earth coordinates.

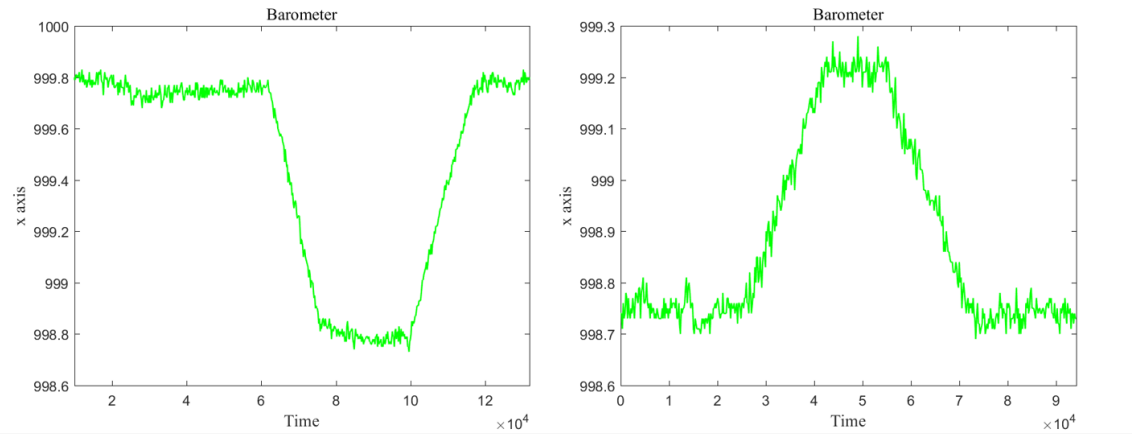
mechanical and electromagnetic groups of these sensors used for measuring velocity and direction of movement. In this section we introduce another group of these sensors which can sense changes in the environment. Modern positioning and navigation systems are designed for ubiquitous mobile and personal operations in different environments. The sensors and algorithms used for localization and the map used to visualization of the results of positioning and navigation are quite different in different environment. Therefore, we need to sense changes in the environment to automate selection of sensor, algorithm and the map for navigation. We want to know whether we are operating outdoors or indoors. If indoors in which specific floor of a building, or perhaps on the stairs or an elevator? Here we provide a short description of the environmental sensors of Table 7.1 and their possible application for intelligent environment recognition.

2.3.12 Barometer

Barometer is a pressure sensor measuring the atmospheric pressure in hPa (millibar). Barometer is used to estimate elevation changes and consequently floor number of operation inside a multi-floor building. The relation between air pressure and height is given by [Yin15]:

$$h \approx -\frac{R \times T_0}{g \times M} \times \ln(\frac{p}{p_0})$$

Using Eq. (7.5) and parameters in Table 7.2, we can calculate altitude from air pressure. Figure 2.15 shows the results of a smartphone barometer measurements in a typical 3-story office building. Figure 2.15a is produced from the results obtained in an elevator elevating three floors of the building and Fig. 2.15b shows the results for climbing one floor of the building using stairs. Both figures demonstrate gradual



(a) (b)

Figure 2.15: Barometer measurement using smart phones in a typical 3-story office building (a) elevating three floors of the building (b) climbing one floor using stairs.

change of the barometer reading during climbing up and down among the floors regardless of the speed and the pattern of motion. Range of variation of measurements in the elevator experiment for climbing three floors are approximately three times larger than that of the measurements for obtained from climbing one floor on the stairs. These observations demonstrate that barometer can be utilized to measure the change in altitude inside the buildings Figure 2.16 shows results of barometer measurements from a smartphone when a user carries the device in four floors of a typical office building in two different time of the same day. Pattern of measurement in different floors are clearly different allowing us to distinguish the floor of operation. However, results of barometer are corrupted by additive Gaussian noise, bias, and it is sensitive to the time of measurement. Methods to mitigate these effects and have a better estimate of the floor number in an office building is discussed in [Yin15].

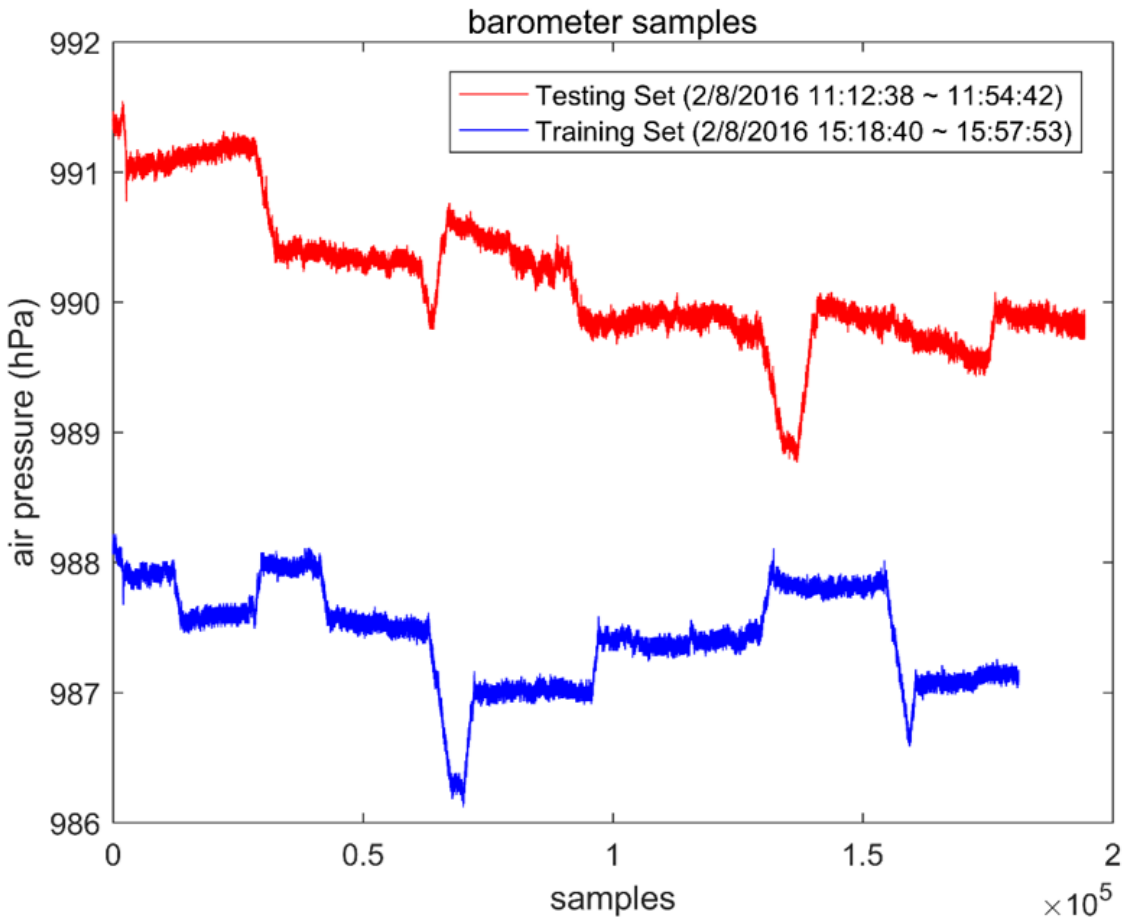


Figure 2.16: Barometer measurement using smart phones in a typical 3-story office building (a) for climbing the stairs (b) for taking the elevator.

2.3.13 Proximity Sensors

Proximity sensors in smartphones measure the distance of the sensor to the closest visible surface. Proximity sensors in smartphones use the infrared (IR) technology, a light emitting diodes (LED) transmits the light and a photo sensitive diode measures the intensity of the reflected received light to estimate the distance. Some proximity sensors only support a binary near or far measurement. In this case, the sensor should report its maximum range value in the far state and a lesser value in the near state. Typical application of this sensor is to detect when the screen is close to ear, when we make a call and turn off the screen light to save the battery. Other technologies such as ultrasound are considered to replace infrared. Smart cars, commercial drones and Robots use Light Detection and Ranging (LiDAR) technology for more accurate measurement of the distance of obstacles close to the sensor. LiDAR uses laser pulses which focus the direction of the light as it is compared with the diffused IR which propagates in all directions. LiDAR has a longer range of operation and a more accurate estimate of distance. The focused beam allows LiDAR to map the proximity obstacle by measuring the distances at different angle of emission. This features allows implementation of more complicated applications such as automatic parking of a vehicle or landing of a drone or adjustment of speed according to the distance for automatic driving.

Table 2.1: shows typical sensors in an Android device.

Sensor Name	**Description**	**Type**	**Common Uses**
BAROMETER	Measures the atmospheric pressure in hPa (millibar).	Environment	Elevation for floor numbering
AMBIENT TEMPRATURE	Measures ambient room temperature in degree Celsius.	Environment	Detecting environment changes
AMBIENT LIGHT	Measures ambient light level in SI lux.	Environment	Detecting environment changes
RELATIVE HUMIDITY	Measures relative ambient air humidity in percent.	Environment	Detecting environment changes
BAROMETER	Measures the acceleration force in m/s2 that is applied to a device on all three physical axes (x, y, and z), including the force of gravity.	Mechanical	Motion detection (shake, tilt, etc.).
GYROSCOPE	Measures a device's rate of rotation in rad/s around each of the three physical axes (x, y, and z).	Mechanical	Rotation detection (spin, turn, etc.).
STEP COUNTERS	Counts the number of steps taken by the person carrying the device.	Mechanical	Measuring travelled distance.
MAGNETOMETER	Measures ambient geomagnetic field strength along the x,y,z axes in micro-Tesla (uT).	Electromagnetic	Creating a compass.
GRAVITY	Measures the force of gravity in m/s2 that is applied to a device on all three physical axes (x, y, z).	Electromagnetic	Motion detection (shake, tilt, etc.).
PROXIMITY	Measures distance from the sensor to the closest visible surface measured in centimeters.	Electromagnetic	Mapping the environment

Table 2.2: Parameters used for calculation of relation between height, h, and pressure, p.

Parameter	**Description**	**Value**
p_0	Standard atmospheric pressure	101325 Pa
R	Universal gas constant	8.31447 J/(mol*K)
T_0	Sea level standard temperature	288.15K
g	Gravitation acceleration	9.81 m/s^2
M	Molar mass of dry air	0.0289644 kg/mol

Chapter 3

RSS-based Localization in IoT and Precision Analysis using CRLB

Recently, various positioning techniques have been developed for accurate indoor geolocation. These techniques can be roughly divided into two classes. The first and most popular one is traditional technique, which measures received signal strength (RSS), time of arrival (TOA) or other signal property matrixes and calculate distance between the transmitter and receiver. Then triangulation is applied to the measured distances and the location can be determined. Another technique is based on pattern recognition, which is more intelligent and can improve the positioning performance when the measurements are not reliable. [1, 6]

In 3D indoor environment, the localization problem becomes extremely complicated. The first consideration is the difference between the techniques utilized in indoor and outdoor geolocation systems. The widely used GPS is no longer an option for the indoor environment since it requires LOS which is blocked in most situations. Many new techniques have been explored recently. The most used one is RF-based technique. Since the properties of RF signals like Received Signal Strength (RSS)

and Time-of-Arrival (ToA) can be utilized to determine to the distance between the transmitter and receiver. Then the triangulation can be applied to find out the location of the mobile points (MPs). [2–4] Recently, more sensor are introduced into the area of indoor geolocation, such as accelerometer, gyroscope, and barometer, which is commonly described as sensor-fusion techniques. [19–21] Moreover, since most of the building will have cameras all over the building for security purposes, the image processing techniques can also be applied in the indoor geolocation area. Another consideration is the difference in the maps used in the outdoor and indoor environment. The Google map can be acquired easily when the users are in the outdoor environment with high-accurate outdoor geolocation. But when one comes indoor, the outdoor map is no longer accurate enough since the outdoor maps cannot show the detailed structure of the indoor environment on different floors and the transition between floors. So indoor maps should be used instead. The last consideration is the 3D geolocation vs 2D geolocation schemes. There have been large amount of researches conducted for the 2D geolocation. But when it comes to 3D scenarios, the problem becomes more complex. For example, the WiFi signal will suffer extra loss when going through the ceilings between floors and the pass loss model should be changed accordingly. In the 2D scenarios, every estimated location is on a certain floor. But in 3D scenarios, more information should be applied such as how to whether the user is inside or outside the building, on which floor is the user located and whether the user is in the elevator or on the stair.

From the considerations above, it is crucial to look deeply into the 3D indoor geolocation problems from different aspects. Cramer-Rao Lower Bound (CRLB) is a typical method which evaluates the positioning performance of different techniques. It can give the lower bound for the positioning schemes so that all the techniques can be compared accordingly. CRLB has been well explored in many

previous researches, but none of them consider the factor of certainty of coverage. As we all know, when signal goes from the transmitter to the receiver, it will suffer all kinds of fading and losses. There is a possibility that the transmitted signal becomes lower than the receiver's sensitivity so that it cannot be detected. In this case, the location is out of coverage and cannot used for position detection. Considering the matter of coverage, it is essential to determine the probability that one location is within the coverage before we start to calculate CRLB. [7, 11]

In this study, we tried to explore how the coverage probability can affect the procedure of CRLB calculation and consequently the performance evaluation. The calculation of coverage probability is specifically derived as the basic foundation of the follow-up CRLB calculation. Scenarios are designed for conducting experiments which is based on the infrastructure of Atwart Kent Laboratory (AKL). Both 2D and 3D scenarios are designed and comparisons are made accordingly.

3.1 Background

Since smart phone is powerful with various embedded sensors (Barometer, Gyroscope, etc.) and other applications (WiFi, GPS), approach for intruder detection can be implemented in multiple methods. Some related work has been done related to this topic. Smart devices have become essential parts of our daily life. Smart phone owners can not only use their phones to make phone calls, but also access a wide range of services and information. They can read breaking news, conduct transaction through online banking, and even get information about their health condition from the small but smart devices. Another important application of smart phones is localization and navigation. With various embedded sensors,

location can be estimated by different techniques which makes smart phone a good candidate for both outdoor and indoor geolocation. GPS is reliable and accurate in the outdoor localization. By acquiring the Line-of-Sight from the satellites, location can be calculated by using triangulation. Other sensors can also be utilized for indoor localization, such as Wi-Fi, barometer, accelerometer, gyroscope and etc. Wi-Fi signal is the most popular technique that is used in the indoor localization. From the received signal strength (RSS) or time of arrival (ToA), distance from the access points (APs) can be calculated and triangulation can be applied to acquire the estimated location as well. Barometer is good in determine the height of the user inside the building, since altitude is closely related to the air pressure measured by the barometer. Accelerometer is used for measuring the acceleration of the movement. By calculating the second integral of the acceleration, distance of movement can be calculated. Gyroscope is helpful in detecting motion and by looking into the data gathered from this sensor, every motion can be detected so that the location can be estimated according to that. [9, 10]

Although indoor geolocation has been explored for a couple of years, there are still challenging problems in this area, among which the map selection and performance evaluation problem are the most crucial and critical. The commonly used Google maps have good performance in the outdoor localization and navigation. By using Google maps, one can be guided to a place with high speed and accuracy GPS application. However, the Google maps do not pay much attention to the indoor environment, in which the detailed layout should be displayed. So it is crucial for us to find out whether the smart phone is operating in the outdoor or indoor environment and the correct map can be selected accordingly. Also, in multiple-floor buildings, layout differs from different floors. Therefore, we should also find out the which floor the smart phone user is currently located in so that the corresponding

map can be displayed. The first part of the map selection problem can be described as outdoor-indoor transition detection and the second part as multi-floor transition detection. To solve these to detection problems, proper sensor selection is the very first step, after which scenarios and algorithms can be designed and consequently experiments can be conducted. [13–15]

For any indoor geolocation problem, it equally important to evaluate the performance. It is essential since a criterion is needed for designing algorithm and deploying the APs so that we can compare different techniques that are used and choose the one with the best performance. But there are still some challenging issues related to this problem. A general and efficient way should be provided and we can utilize it to analyze any indoor geolocation system. The approach can also be modified since for different localization schemes, other sensors will be fused and the modified scheme is able to respond to any change.

The work described by [18] presents an approach which detects intruder for WLAN access. Least Mean Square (LMS) and Prioritized Maximum Power (PMP) are used as two RSS-based matching algorithms. Their performance of accuracy are compared in indoor and outdoor-indoor areas and PMP algorithm provides a better performance than LMS in positioning application.

An approach using fusion of sensors, WLAN signals and building information for indoor/campus localization is developed by [21]. This method shows the possibilities of combing the measurements from different sensors and building information to obtain accurate indoor localization as well as the possibilities that sensors can aid in intruder detection [5, 6].

Some indoor personal navigation applications are introduced in [6]. Map Matching Algorithms are implemented, which make the Pedestrian Navigation Module (PNM) have the capbility to provide localization results even with bad reception of

GPS signals.

Another approach is described in [8, 12] which fuse dead reckoning (DR) algorithm, GPS, and RFID for pedestrian positioning. This method is implemented as software module with web-based APIs on computing systems which shows that GPS and the active RFID tag system can seamlessly and effectively adjust estimation errors in DR as well as possibilities for sensor fusion localization. To analyze the coverage certainty, we should start from the commonly used path loss model in decibels, which is given by:

$$L_p = L_0 + 10\alpha \log_{10} r \tag{3.1}$$

Where L_p is the total path loss from the transmitter to receiver. L_0 is the normalized path loss, which is the power loss at 1 m. α is the gradient indicating the relation between distance and power. In the environment of office buildings, the materials of the buildings are brick, wood, metal, and other composites. These materials have different gradients from 2 to 6. In large office area, α is changeable according to different r, which indicates the distance from the transmitter to the receiver.

The transmitted signal is also expected to have different path losses in different directions, causing power variation when it reaches to receiver. This variation is commonly called shadow fading or large-scale fading since its cause is obstruction by objects around the receiver. It is not feasible to model shadow fading in a deterministic way, and therefore we usually use statistical models instead. We define l as the shadow fading in the radio propagation, which is a zero mean normally distributed random variable with a standard deviation of σ. The probability

distribution function (PDF) for shadow fading can be written as:

$$f(l) = \frac{1}{\sqrt{2\pi}\sigma} e^{-l^2/2\sigma^2} \tag{3.2}$$

Every receiver has its own sensitivity, which is the minimum RSS that it can recognize. Given the PDF of the shadow fading, we can calculate the probability that the RSS in one location will be lower that the sensitivity (Outage) as well as the probability that it is higher than the sensitivity (Coverage). It is obvious that the sum of the two will be one and we only need calculate one of them. We denote s as the difference between transmitted power and the sensitivity, which indicates the maximum power loss for effective transmission. Then the probability of coverage can be derived as follow:

$$\begin{aligned} Prob(Coverage) &= Prob(L_p + l < s) = Prob(l < s - L_p) \\ &= 1 - \int_{s-L_p}^{\infty} f(l)dl \\ &= 1 - \int_{s-L_p}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-l^2/2\sigma^2} dl \\ &= 1 - \frac{1}{2} erfc(\frac{s - L_p}{\sqrt{2}\sigma}) \end{aligned} \tag{3.3}$$

Where $erfc()$ is the complementary error function, and $erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt$. Then we can replace L_p with Equation (1), and the coverage probability is written as:

$$Prob(Coverage) = 1 - \frac{1}{2} erfc(\frac{s - L_0 - 10\alpha \log_{10} r}{\sqrt{2}\sigma}) \tag{3.4}$$

From Equation (3.4), we can see that all the factors are constant except d, which

means that the probability is a function of the distance between the transmitter and receiver.

3.2 Channal Modelling with Probability of Coverage

Path loss model plays an important role in designing localization algorithms and performance evaluation. There has been numerous researches that focus on channel modelling for wide and local area networks. The empirical path loss model is no longer fit for Indoor 3D environment. In multistory building, the power-distance gradient α will change according to different distances, so the commonly used path loss model is given:

$$L_p = L_0 + \begin{cases} 20log_{10}r, & (10 \geq r \geq 1m) \\ 20 + 30log_{10}\dfrac{r}{10}, & (20 \geq r > 10m) \\ 29 + 60log_{10}\dfrac{r}{20}, & (40 \geq r > 20m) \\ 47 + 120log_{10}\dfrac{r}{40}, & (r > 40m) \end{cases} \tag{3.5}$$

From Equation (3.5), it is clear that path loss becomes greater when the distance between the transmitter and receiver becomes larger. But the method that we use to calculate coverage certainty stay the same. Equation (3.8) can still be used in 3D scenarios and the only difference is that we should replace the empirical path loss model with the 3D distance-partitioned model, which creates a different L_p.

However, in reality, in some occasions, the RSS cannot be detected in indoor environment because of severe shadow fading. In this case, the typical method of channel modelling is not suitable since the data is incomplete so that we can not

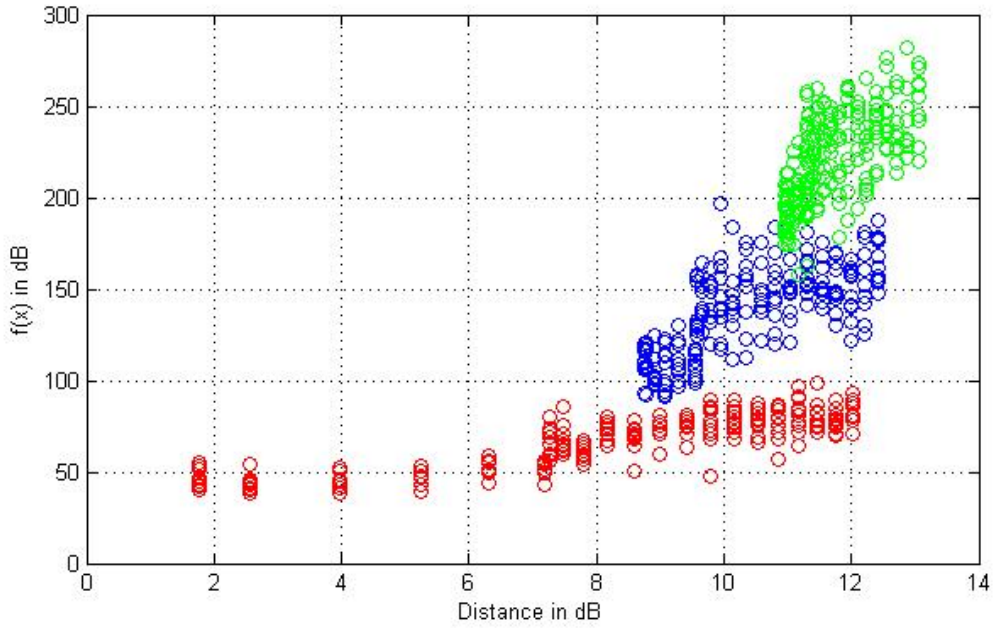


Figure 3.1: Channel Modeling

find out a optimized fit for the RSS data.

With the concern of probability of coverage, we can find receive the supposed RSS even if the interference from the surrounding is severe and then we can apply the commonly used linear fit method to model the indoor channel.

The concept of Probability-of-Coverage (PoC) starts from the commonly used RF path loss model [13], which represents the distance-power relationship in different environment and scenarios of operation:

$$L_p = L_0 + 10\alpha \log_{10} r \tag{3.6}$$

Where L_p is the total path loss from the transmitter to receiver and L_0 is the power loss at first meter. r is denoted as the distance from the transmitter to the receiver. α is the gradient indicating the relation between distance and power. In the envi-

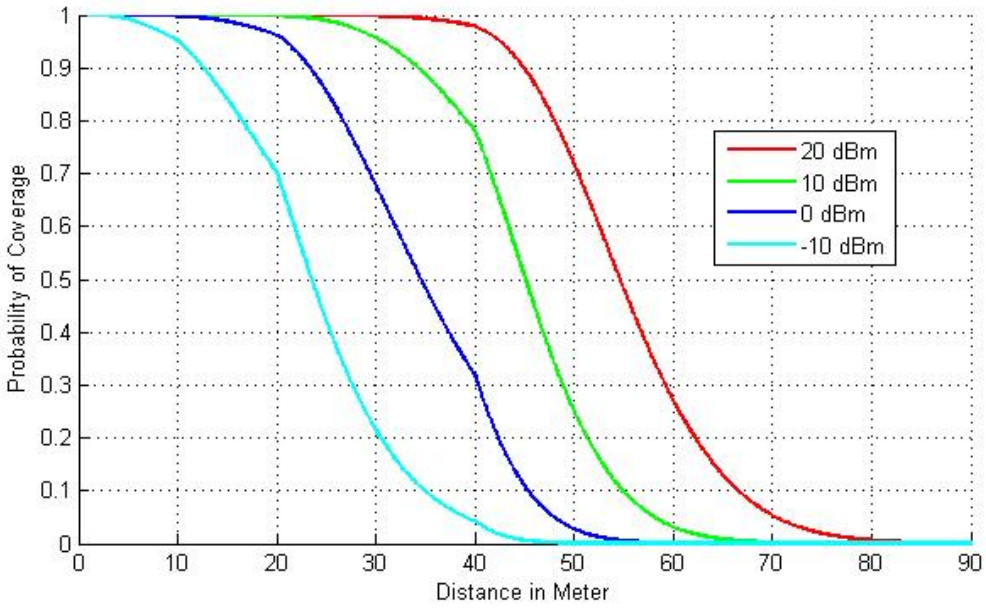


Figure 3.2: Probability of Coverage in Different Transmitted Power

ronment of office buildings, the materials of the buildings are brick, wood, metal, and other composites. These materials have different gradients from 2 to 6. Thus, α is changeable according to different environment so that various path loss models have been designed in literature.

The transmitted signal is also affected by shadow fading or large-scale fading, which can be denoted as $X(\sigma)$ and it is a zero mean normally-distributed addictive random variable with a standard deviation of σ. The probability distribution function (PDF) for shadow fading can be written as:

$$f(X(\sigma)) = \frac{1}{\sqrt{2\pi}\sigma} e^{-X(\sigma)^2/2\sigma^2} \tag{3.7}$$

We all know that every device has its own sensitivity, which is the minimum RSS that it can recognize. Therefore, with the variation of shadow fading, RSS at a certain location may goes below the sensitivity of the mobile device. Given the

PDF of the shadow fading, we can calculate the probability that the RSS in one location will be lower that the sensitivity (Outage) as well as the probability that it is higher than the sensitivity (Coverage). We denote Lp_{max} as the difference between transmitted power and the sensitivity, which indicates the maximum power loss for effective transmission. Then the Probability-of-Coverage (PoC) can be derived as follows:

$$\begin{aligned} Prob(Coverage) &= Prob(L_p + X(\sigma) < Lp_{max}) \\ &= Prob(X(\sigma) < Lp_{max} - L_p) \\ &= 1 - \int_{Lp_{max}-L_p}^{\infty} f(X(\sigma))dl \\ &= 1 - \int_{Lp_{max}-L_p}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-X(\sigma)^2/2\sigma^2} dl \\ &= 1 - \frac{1}{2} erfc(\frac{Lp_{max} - L_p}{\sqrt{2}\sigma}) \end{aligned} \tag{3.8}$$

Where $erfc(\cdot)$ is the complementary error function. From Equation (3.6) and (3.8), we can see that PoC is closely related to the specific path loss model, the standard deviation of shadow fading σ as well as the sensitivity and transmitted power s. Note that althogh PoC is derived from the empirical path loss model here, we can replace L_p in Equation (3.8) with any other path loss model which fits a specific scenario. Fig. **??** shows the effect of transmitted power from -10 dBm to 20 dBm at different distances, where free-space path loss model is used ($\alpha = 2$) and standard deviation of shadow fading is set as 5 dB.

3.3 CRLB with Bayes' Theorem

Let's assume that a mobile device is moving in an environment where N access points are deployed. These fixed access points can be any kind of IoT devices with different transmitted power, frequencies and radio propagation characteristics. Then deviation of CRLB start from the empirical pathloss model:

$$Lp_i = L_0 + 10\alpha_i log_{10}(r_i) + X(\sigma) \tag{3.9}$$

where distance from mobile device to ith access point can be calculated as $r_i = \sqrt{(x - x_i)^2 + (y - y_i)^2}$. In this case, the estimator is the coordinate of the mobile device's location, which can be denoted as $\theta = [x \quad y]^T$, and (x_i, y_i) is the coordinate of the ith access point.

Then the probability distribution function of observation (pathloss) given certain estimator can be determined as:

$$p_i(Lp_i/\theta) = \frac{1}{\sqrt{2\pi}\sigma} exp(-\frac{1}{2\sigma^2}[Lp_i - L_0 - 10\alpha_i log_{10} r_i]^2) \tag{3.10}$$

We also have the probability of coverage as $p_i(\theta)$. From Bayesian Theory, we also know that:

$$p_i(Lp_i; \theta) = p_i(Lp_i/\theta) \cdot p_i(\theta) \tag{3.11}$$

All the observations can be considered as addictive and independent from one another, thus the joint PDF for the observations can be derived as:

$$\begin{aligned} p(\boldsymbol{Lp}; \theta) &= \prod_{i=1}^{N} p_i(Lp_i; \theta) \\ &= \prod_{i=1}^{N} p_i(Lp_i/\theta) \cdot p_i(\theta) \end{aligned} \tag{3.12}$$

From the theory of CRLB we also know that it is the inverse of Fisher Information Matrix, which is denoted as $\boldsymbol{I}(\theta)$ and can be calculated as follows:

$$\boldsymbol{I}(\theta) = \begin{bmatrix} -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial x^2}] & -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial x \partial y}] \\ \\ -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial x \partial y}] & -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial y^2}] \end{bmatrix}$$

Since

$$\begin{aligned} ln(p(\boldsymbol{Lp};\theta)) &= ln(\prod_{i=1}^{N} p_i(Lp_i/\theta) \cdot p_i(\theta)) \\ &= \sum_{i=1}^{N} [ln(p_i(Lp_i/\theta)) + ln(p_i(\theta))] \end{aligned}$$

We can rewrite the Fisher matrix as:

$$\boldsymbol{I}(\theta) = \boldsymbol{I}_1(\theta) + \boldsymbol{I}_2(\theta) \tag{3.13}$$

where

$$\boldsymbol{I}_1(\theta) = \sum_{i=1}^{N} \begin{bmatrix} -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial x^2}] & -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial x \partial y}] \\ \\ -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial x \partial y}] & -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial y^2}] \end{bmatrix}$$

and

$$\boldsymbol{I}_2(\theta) = \sum_{i=1}^{N} \begin{bmatrix} -E[\frac{\partial^2 ln(p_i(\theta))}{\partial x^2}] & -E[\frac{\partial^2 ln(p_i(\theta))}{\partial x \partial y}] \\ \\ -E[\frac{\partial^2 ln(p_i(\theta))}{\partial x \partial y}] & -E[\frac{\partial^2 ln(p_i(\theta))}{\partial y^2}] \end{bmatrix}$$

So that

$$cov(dr) = \boldsymbol{I}(\theta)^{-1} = \begin{bmatrix} \sigma_x^2 & \sigma_{xy}^2 \\ \sigma_{xy}^2 & \sigma_y^2 \end{bmatrix} \tag{3.14}$$

CRLB is the trace of the covariance matrix, which means that $\sigma_r^2 = \sigma_x^2 + \sigma_y^2$. In this way, the total CRLB can be calculated no matter how many APs are covered.

Actually, we can find out the close form of $\boldsymbol{I_1}(\theta)$ and $\boldsymbol{I_2}(\theta)$:

$$ln(p_i(Lp_i/\theta)) = ln(\frac{1}{\sqrt{2\pi}\sigma}) - \frac{(Lp_i - L_0 - 10\alpha_i log_{10}(r_i))^2}{2\sigma^2} \tag{3.15}$$

Then:

$$\frac{\partial ln(p_i(Lp_i/\theta))}{\partial x} = 0 - \frac{1}{2\sigma^2} \cdot \frac{\partial [Lp_i - L_0 - 10\alpha_i log_{10}(r_i)]^2}{\partial x} \tag{3.16}$$

Let's take $\phi = Lp_i - L_0 - 10\alpha_i log_{10}(r_i)$, so that:

$$\frac{\partial ln(p_i(Lp_i/\theta))}{\partial x} = -\frac{1}{2\sigma^2} \cdot \frac{\partial \phi^2}{\partial x} \tag{3.17}$$

3.4 CRLB with Probability of Coverage

In this section, we provide the general description of pathloss models, according to which, CRLB and probability of coverage can be derived in multiple-dimension scenarios. Since the commonly-used CRLB does no include the effect of transmitting power (proved in later section), we hybrid both of CRLB and probability of coverage in pursuing more reliable performance evaluation.

3.4.1 Cramer-Rao Lower Bound

Cramer-Rao Lower Bound (CRLB) indicates the smallest estimation error under given observations and is frequently used in evaluating the performance of localization systems.

The usage of matrix only fits the condition that there are more than 2 APs. If only one AP is available, another method should be applied instead.

In this case, the partial differential equation should be:

$$dL_{pi}(r) = \frac{10\alpha_i}{ln10}\frac{dr}{r}, i = 1, 2, ..., N \tag{3.18}$$

Then the location error can be estimated as follow:

$$dr = \frac{ln10 \cdot r}{10\alpha_i} dL_p i(r), i = 1, 2, ..., N \tag{3.19}$$

And covariance of dr can be derived:

$$\begin{aligned} cov(dr) &= (\frac{ln10 \cdot r}{10\alpha_i})^2 cov(dL_p i(r)) \\ &= \sigma^2 (\frac{ln10 \cdot r}{10\alpha_i})^2, i = 1, 2, ..., N \end{aligned} \tag{3.20}$$

which is also the variance of dr, so the CRLB in this case is

$$\sigma_r = \frac{ln10 \cdot r}{10\alpha_i}\sigma, i = 1, 2, ..., N \tag{3.21}$$

In order to investigate the relation between the location error and signal strength error, we apply a differential operation to both sides of Equation (3.6) with respect to two coordinates x and y, then we have:

$$dL_{pi}(x, y) = \frac{10\alpha_i}{ln10}(\frac{x - x_i}{r_i^2}dx + \frac{y - y_i}{r_i^2}dy), i = 1, 2, ..., N \tag{3.22}$$

where L_{pi} is the total path loss from AP_i to the location of (x, y); (x_i, y_i) is the coordinate of AP_i; α_i is the power-distance gradient for signal coming from AP_i; r_i is the distance between the receiver and AP_i, and $r_i = \sqrt{(x - x_i)^2 + (y - y_i)^2}$; N is the number of APs.

The set of Equation (3.22) can be written in matrix form as:

$$d\boldsymbol{L_p} = \boldsymbol{H} \cdot d\boldsymbol{r} \tag{3.23}$$

Where

$$d\boldsymbol{L_p} = \begin{bmatrix} dL_{p1} \\ dL_{p2} \\ \vdots \\ dL_{pi} \end{bmatrix}, d\boldsymbol{r} = \begin{bmatrix} dx \\ dy \end{bmatrix}, \boldsymbol{H} = \begin{bmatrix} \frac{10\alpha}{ln10}\frac{x-x_1}{r_1^2} & \frac{10\alpha}{ln10}\frac{y-y_1}{r_1^2} \\ \frac{10\alpha}{ln10}\frac{x-x_2}{r_2^2} & \frac{10\alpha}{ln10}\frac{y-y_2}{r_2^2} \\ \vdots & \vdots \\ \frac{10\alpha}{ln10}\frac{x-x_N}{r_N^2} & \frac{10\alpha}{ln10}\frac{y-y_N}{r_N^2} \end{bmatrix}$$

From Equation (3.23), we can estimate the location error.

$$d\boldsymbol{r} = (\boldsymbol{H'H})^{-1}\boldsymbol{H'}d\boldsymbol{L_p} \tag{3.24}$$

Since the path loss estimation error is identical to the error caused by shadow fading, which has zero mean and variance of σ^2, and these errors for different APs are independent with each other, then we can have the two equations as follow:

$$\boldsymbol{E}[d\boldsymbol{L_{pi}}] = 0, cov(d\boldsymbol{L_{pi}}, d\boldsymbol{L_{pj}}) = \begin{cases} \sigma^2, i = j \\ \qquad i, j = 1, 2, ..., N \\ 0, i \neq j \end{cases} \tag{3.25}$$

Then the covariance matrix of the location error $d\boldsymbol{r}$ is given by

$$cov(d\boldsymbol{r}) = \sigma^2(\boldsymbol{H'H})^{-1} = \begin{bmatrix} \sigma_x^2 & \sigma_{xy}^2 \\ \sigma_{xy}^2 & \sigma_y^2 \end{bmatrix} \tag{3.26}$$

The standard deviation of location error is finally derived as

$$\sigma_r = \sqrt{\sigma_x^2 + \sigma_y^2} \tag{3.27}$$

From Equation (3.27), we can see that if the transmission environment is given, the location error only relies on the coordination of the receiver (x, y), and we can calculate the CRLB at any location according to that.

In the previous sections, all we have discussed are focused on the analysis in 2D condition. But in reality, 3D geolocation schemes are more important in indoor environment. Therefore, we should have a deeper look at how to expand our methods to 3D environment.

The calculation for CRLB needs more expansion since the coordinate of every location becomes three dimensional. In 3D environment, we use similar method to start the derivation of CRLB.

To analyze the relation between RSS and the least location error (CRLB), we can apply partial differential to Equation (**??**) [11, 12]. Then we have

$$dP_i(x, y, z) = -\frac{10\alpha}{ln10}\left(\frac{x - x_i}{r_i^2}dx + \frac{y - y_i}{r_i^2}dy + \frac{z - z_i}{r_i^2}dz\right) \tag{3.28}$$

In this case, the matrix form should also be expanded to three dimension, where

$$d\boldsymbol{r} = \begin{bmatrix} dx \\ dy \\ dz \end{bmatrix}, \boldsymbol{H} = \begin{bmatrix} \frac{10\alpha_1}{ln10}\frac{x-x_1}{r_1^2} & \frac{10\alpha_1}{ln10}\frac{y-y_1}{r_1^2} & \frac{10\alpha_1}{ln10}\frac{z-z_1}{r_1^2} \\ \frac{10\alpha_2}{ln10}\frac{x-x_2}{r_2^2} & \frac{10\alpha_2}{ln10}\frac{y-y_2}{r_2^2} & \frac{10\alpha_2}{ln10}\frac{z-z_2}{r_2^2} \\ \vdots & \vdots & \vdots \\ \frac{10\alpha_N}{ln10}\frac{x-x_N}{r_N^2} & \frac{10\alpha_N}{ln10}\frac{y-y_N}{r_N^2} & \frac{10\alpha_N}{ln10}\frac{z-z_N}{r_N^2} \end{bmatrix}$$

By using the same least-square estimation method we mentioned before, estimation of the location error can be evaluated:

$$d\boldsymbol{r} = (\boldsymbol{H}'\boldsymbol{H})^{-1}\boldsymbol{H}'d\boldsymbol{P} \tag{3.29}$$

and the covariance matrix of the location error is

$$cov(d\boldsymbol{r}) = \sigma^2(\boldsymbol{H}'\boldsymbol{H}) = \begin{bmatrix} \sigma_x^2 & \sigma_{xy}^2 & \sigma_{xz}^2 \\ \sigma_{xy}^2 & \sigma_y^2 & \sigma_{yz}^2 \\ \sigma_{xz}^2 & \sigma_{yz}^2 & \sigma_z^2 \end{bmatrix} \tag{3.30}$$

Then the CRLB can be calculated as follow:

$$\sigma_r = \sqrt{\sigma_x^2 + \sigma_y^2 + \sigma_z^2} \tag{3.31}$$

Since every coverage probability and CRLB is redefined here, the 3D CRLB can be calculated in the same way which is described in Equation (3.35).

3.4.2 CRLB Concerning Probability of Coverage

From the previous section, we can calculate the probability that a location can be covered by a AP as well as the CRLB which shows the minimum location error under this condition. It is reasonable for us that calculate the CRLB concerning the effect of coverage certainty, so that the total CRLB will be more reliable and accurate.

We denote p_i as the probability that a certain location can be covered by AP_i, which can be calculated by Equation (3.4). Suppose there are N APs in total, the probability that k APs are covered can be calculated according to the probabilities we calculated before. The number of combinations C of selecting k elements out of N can be calculated as

$$C = \binom{N}{k} = \frac{N!}{k!(N-k)!} = \frac{N(N-1)\cdots(N-k+1)}{k(k-1)\cdots 1}$$

To calculated the CRLB concerning coverage certainty, all the probabilities for the combinations should be explored and the total CRLB should be the summation of every individual CRLB times its corresponding probability. For example, if only 1 AP is covered, then there are N combinations ($C = N$) in this case. Suppose AP_1 is the one that is covered, then the probability for this condition is given from the concept of probability theory

$$Prob_k = \sum_{i,j}^{C} [\prod_{i}^{k} p_i * \prod_{j,j\neq i}^{N-k} (1 - p_j)] \tag{3.32}$$

Where $Pron_k$ is the probability that only AP_1 is covered while others are not. Note that we should skip the situation when all the APs are not covered. In this condition, no location estimation can be made, since no information can be used to determine the location of the receiver. Therefore, it is useless to discuss this situation.

However, we should mention that when $i = 0, 1, 2$, which means that no AP or only one/two APs are covered, matrix $H'H$ will be singular and CRLB cannot be determined. It is reasonable since we are able to find the location estimation only when more than 3 APs are accessible. In this case, $Prob_0 - 2$ can no longer be used in computing the PCRLB and we should normalize the probabilities by:

$$Prob_k{}' = \frac{Prob_k}{\sum_{k=2}^{N} Prob_k} \tag{3.33}$$

And,

$$\sum_{k=0}^{N} Prob_k{}' = 1 \tag{3.34}$$

Similarly, we can calculate the probabilities for all the other conditions ($Prob_2, Prob_3, \cdots, Prob_N$). Then the total CRLB can be calculated as follow

$$CRLB_{total} = \sum_{i=0}^{N} CRLB_i \cdot Prob_i' \tag{3.35}$$

In this way, we can calculate the total CRLB no matter how many APs are covered.

3.4.3 Scenarios Design

To compare different geolocation systems, the very first step is to design test scenarios so that their performance can be evaluated in a same way.

We have designed 5 scenarios which can be divided into two types, 2D scenarios and 3D scenarios. The first 3 scenarios are designed on the same floor and we can compare these 3 scenarios for the effects of AP number. In Scenario 4 and 5, APs are deployed in multiple floors, and we can compare the effect of 3D scenarios. The detailed scenario description is given as follow:

- Scenario 1: 3 APs are placed on the ceiling of the same floor (at 3 of the 4 corners).
- Scenario 2: 4 APs are placed on the ceiling of the same floor (at the 4 corners).
- Scenario 3: 5 APs are placed on the ceiling of the same floor (at the 4 corners and the middle).
- Scenario 4: 4 APs are placed on the ceiling of the 1st floor (at the 4 corners), and we calculate the total CRLBs of the three floors.
- Scenario 5: 4 APs are placed on the ceiling of every floor (at the 4 corners, 12 APs in total), and we calculate the total CRLBs of the three floors.

We assume that every floor has a space of 30m×30m and a height of 5 meter. Every floor is sampled in every 0.1 meter (the 4 edges are not includes), so we have $299 \times 299 = 89401$ samples in total for every scenario.

3.4.4 Limits and Challenges of Combined CRLB

There are two aspects that we should pay extra attention to.

First of all, the increase of access number will dramatically increase the amount of possibilities as well as the amount of computation. For instance, when we have only have 4 APs, there are $\frac{4!}{3!1!} = 4$ possibilities that 3 of them can cover the mobile device. When the number increase to 5, we have $\frac{5!}{3!2!} = 10$ possibilities. When the number becomes to 6, we will have $\frac{6!}{3!3!} = 20$ possibilities. So it is obvious that the amount of computation will increase greatly even if we only add one access point. The most reliable way is to limit the amount of access points used in localization so that the computation can also be limited within a reasonable range. This means we will pick the most useful points in estimating the receivers location, i.e.

The other aspect is the consideration of H matrix. For every deployment we can find a H matrix respectively. But not all of the matrix are full-ranked. If one matrix are singular, we cannot find its inverse matrix so that we cannot calculate the CRLB according to that. This will happen when all the access points are located at the same plane so that two of the columns in the H matrix will have the same or opposite values. To avoid this situation, we have to remove the combination that will cause singular H matrix from our possibility set. Also, we do not consider the situation when 0, 1, or 2 access points are covered since the amount of APs are too small and we cannot estimate the mobile device's location according to the information. But note that we can still have the probability that get these situations, thus when

calculating the combined CRLB, we use normalized probability instead of the one we calculated before.

Cramer-Rao Lower Bound (CRLB) indicates the smallest estimation error under given observations and is frequently used in evaluating the performance of localization systems [12, 17]. The derivation of CRLB has been widely used in many researches but as described before, all the calculation of CRLB is under the assumption that the mobile device is covered by all the access points, which is impossible in the environment full of low-energy IoT devices, whose coverage is not as wide as the high-power wireless devices. In this section, attempts are made to combine the CRLB with PoC to fit it into the IoT environment so that more reasonable conclusions are guaranteed.

Let's assume that a mobile device is moving in an environment where N access points are deployed. These fixed access points can be any kind of IoT devices with different transmitted power, frequencies and radio propagation characteristics. Then deviation of CRLB start from the empirical pathloss model:

$$Lp_i = L_0 + 10\alpha_i log_{10}(r_i) + X(\sigma) \tag{3.36}$$

where distance from mobile device to ith access point can be calculated as $r_i = \sqrt{(x - x_i)^2 + (y - y_i)^2}$. In this case, the estimator is the coordinate of the mobile device's location, which can be denoted as $\theta = [x \quad y]^T$, and (x_i, y_i) is the coordinate of the ith access point.

Then the probability distribution function of observation (pathloss) given certain estimator can be determined as:

$$p_i(Lp_i/\theta) = \frac{1}{2\pi\sigma^2} exp(-\frac{1}{2\sigma^2}[Lp_i - L_0 - 10\alpha_i log_{10} r_i]^2) \tag{3.37}$$

We also have the probability of coverage as $p_i(\theta)$. Then

$$p_i(Lp_i;\theta) = p_i(Lp_i/\theta) \cdot p_i(\theta) \tag{3.38}$$

All the observations can be considered as addictive and independent from one another, thus the joint PDF for the observations can be derived as:

$$\begin{aligned} p(\boldsymbol{Lp};\theta) &= \prod_{i=1}^{N} p_i(Lp_i;\theta) \\ &= \prod_{i=1}^{N} p_i(Lp_i/\theta) \cdot p_i(\theta) \end{aligned} \tag{3.39}$$

From the theory of CRLB we also know that it is the inverse of Fisher Information Matrix, which is denoted as $\boldsymbol{I}(\theta)$ and can be calculated as follows:

$$\boldsymbol{I}(\theta) = \begin{bmatrix} -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial x^2}] & -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial x \partial y}] \\ \\ -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial x \partial y}] & -E[\frac{\partial^2 ln(p(\boldsymbol{Lp};\theta))}{\partial y^2}] \end{bmatrix}$$

Since

$$\begin{aligned} ln(p(\boldsymbol{Lp};\theta)) &= ln(\prod_{i=1}^{N} p_i(Lp_i/\theta) \cdot p_i(\theta)) \\ &= \sum_{i=1}^{N} [ln(p_i(Lp_i/\theta)) + ln(p_i(\theta))] \end{aligned}$$

We can rewrite the Fisher matrix as:

$$\boldsymbol{I}(\theta) = \boldsymbol{I}_1(\theta) + \boldsymbol{I}_2(\theta) \tag{3.40}$$

where

$$\boldsymbol{I}_1(\theta) = \sum_{i=1}^{N} \begin{bmatrix} -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial x^2}] & -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial x \partial y}] \\ \\ -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial x \partial y}] & -E[\frac{\partial^2 ln(p_i(Lp_i/\theta))}{\partial y^2}] \end{bmatrix}$$

and

$$\boldsymbol{I}_2(\theta) = \sum_{i=1}^{N} \begin{bmatrix} -E[\frac{\partial^2 ln(p_i(\theta))}{\partial x^2}] & -E[\frac{\partial^2 ln(p_i(\theta))}{\partial x \partial y}] \\ \\ -E[\frac{\partial^2 ln(p_i(\theta))}{\partial x \partial y}] & -E[\frac{\partial^2 ln(p_i(\theta))}{\partial y^2}] \end{bmatrix}$$

So that

$$cov(dr) = \boldsymbol{I}(\theta)^{-1} = \begin{bmatrix} \sigma_x^2 & \sigma_{xy}^2 \\ \\ \sigma_{xy}^2 & \sigma_y^2 \end{bmatrix} \tag{3.41}$$

CRLB is the trace of the covariance matrix, which means that $\sigma_r^2 = \sigma_x^2 + \sigma_y^2$. In this way, the total CRLB can be calculated no matter how many APs are covered.

However, in the traditional derivation of CRLB, $p_i(\theta)$ is always considered as 1, which means that $\boldsymbol{I}_2(\theta)$ is zero and the key parameters that affect the performance of system are the deployment of access points and the pathloss model. In fact, when devices with various transmitted power are deployed, they will not perform the same way even if they share the same progagation characteristic.

There are two aspects that we should pay extra attention to. First of all, from Equation (3.40), the increase of access number will add more information to the Fisher matrix so that when we take the inverse of it, the value in the covariance matrix will become smaller which indicates that the estimators are less deviated. This makes sense that when more information are provided, the better localization performance would be. However, in fact, when the number of access points reaches a certain value, the densely-deployed sensors can no longer improve the localization precision. They will interfere with one another and affect the entire system's perfor-

mance. So it is crucial that we explore how the number of access points will affect the CRLB and what is the best strategy for the deployment of IoT devices.

Another issue falls into the other part of Fisher matrix, which is how the PoC may affect the performance of the entire system. From the same equation we can see that, when $\boldsymbol{I}_2(\theta)$ is included in the calculation of CRLB, it also leads to a decrease ofthe value in covariance matrix. It is because, when PoC is considered, the calculation of Fisher matrix will be biased so that the information from APs with higher PoC will be more weighted than the ones with lower PoC, and thus, generate more accurate location estimation. It will be further proved by a simulation in the following section.

3.5 Results & Analysis

In this section, we will present the results and give our analysis from which conclusions can be made.

3.5.1 Contours of CRLB in Three Scenarios

We illustrate the contours of CRLB for the three Scenarios in Figure 2-4. In the figures, characteristic of error performance is clearly presented.

Note that although the space is 30m $\times$ 30m, we do not include the observations on the edges. Consequently, the contour shows a $29.9m \times 29.9m$ space instead of a $30m \times 30m$ one.

3.5.2 CDFs of Different Scenarios

When we explore more about the statistical characteristic of the performance, we illustrate the CDFs of different scenarios under both RSS-only and Barometer-assisted CRLB, which is shown in Figure 5.

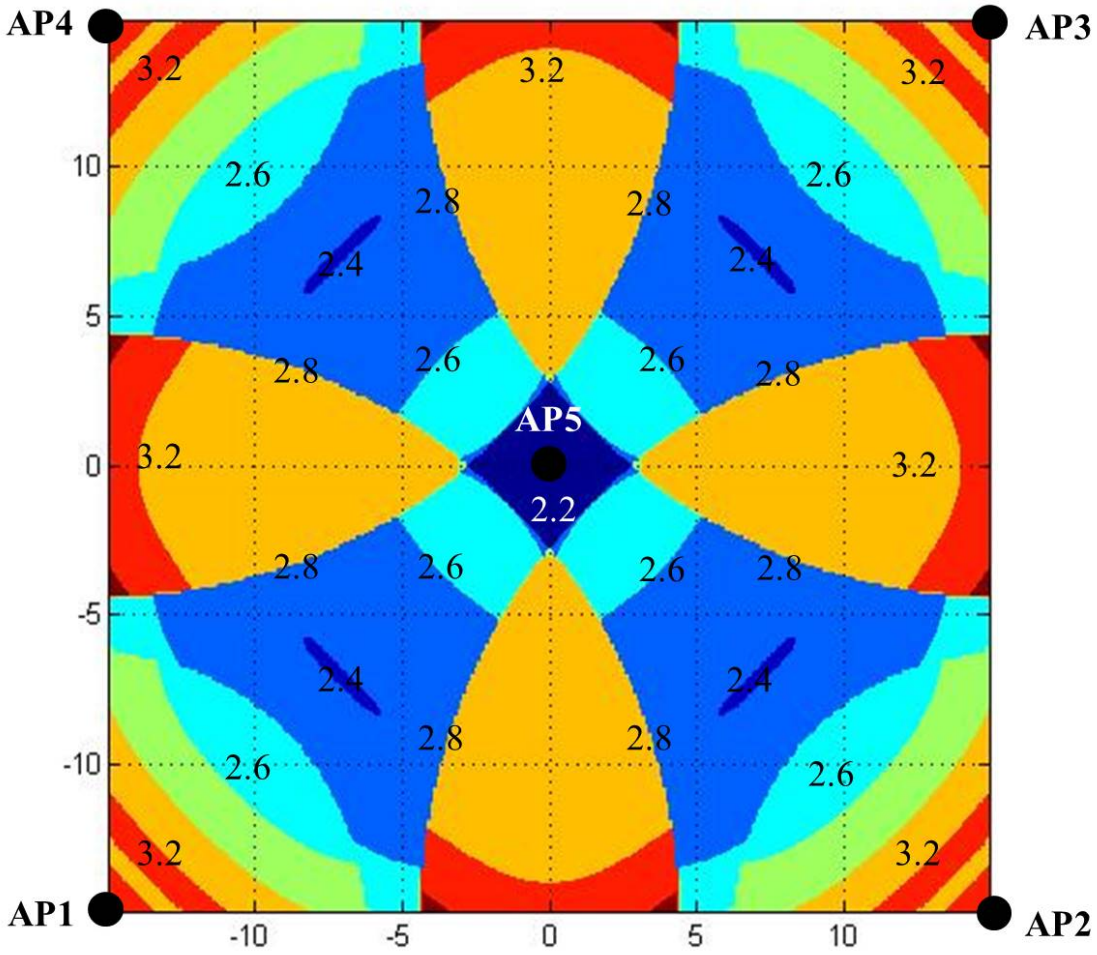


Figure 3.3: Contour of CRLB in Scenario 1

From the figure, we can see that the location error is decreased when more information from other floors is applied. Moreover, if the barometer assist the cal-

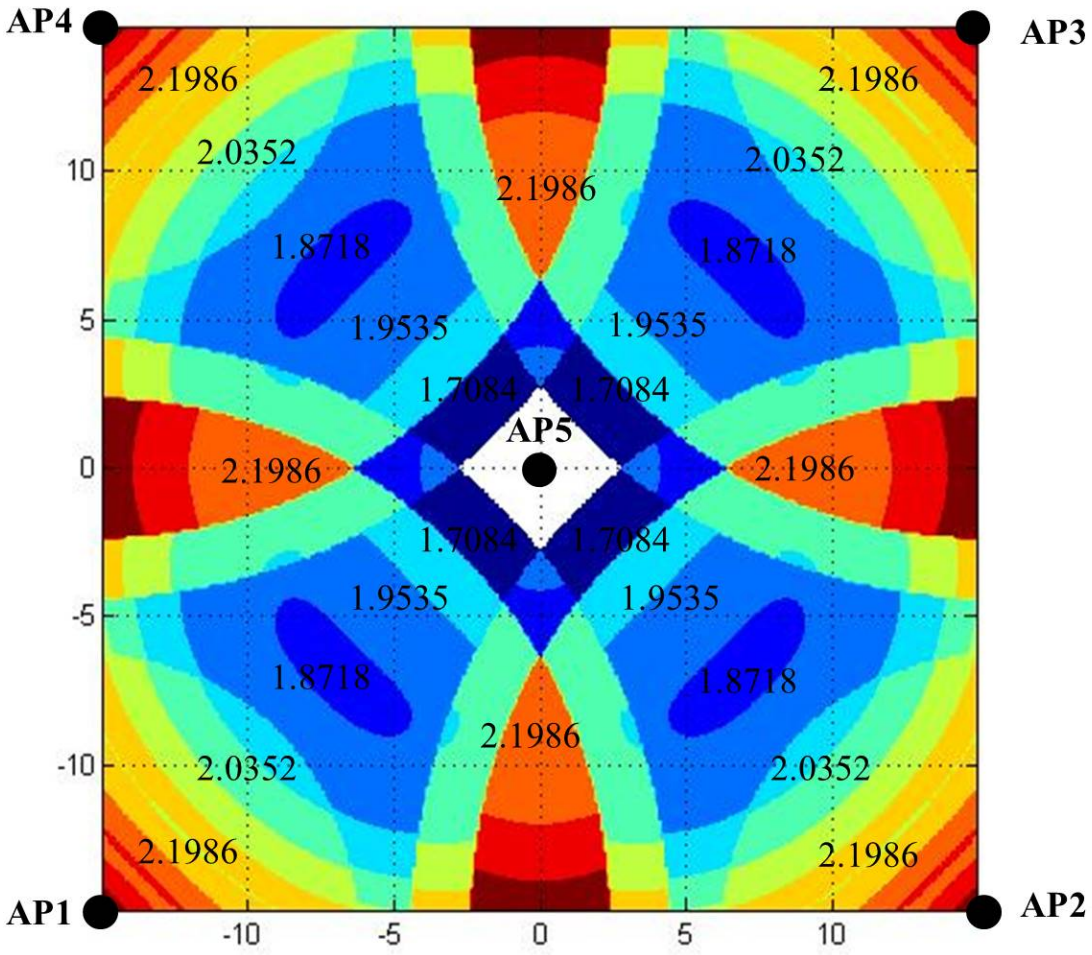


Figure 3.4: Contour of CRLB in Scenario 2

culation of the CRLB, the performance is greatly improved.

3.5.3 CRLB & PCRLB Comparison

Maximum, minimum, and mean CRLB value of the three scenarios using these two methods are listed in Table II. From the table, we can find that by adopting the barometer-assisted method, a 41.67%, 29.29%, and 19.20% improvement can be achieved under the Scenarios 1, 2, and 3 respectively.

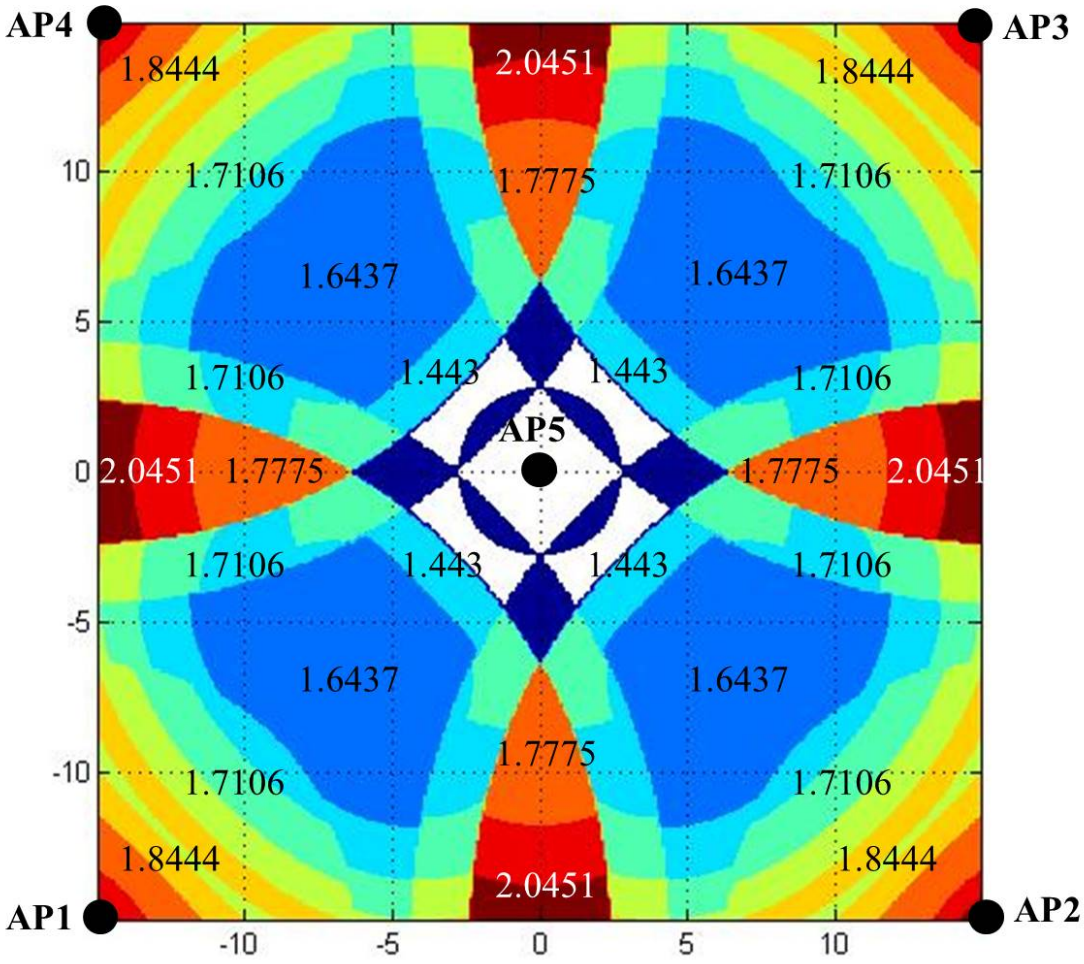


Figure 3.5: Contour of CRLB in Scenario 3

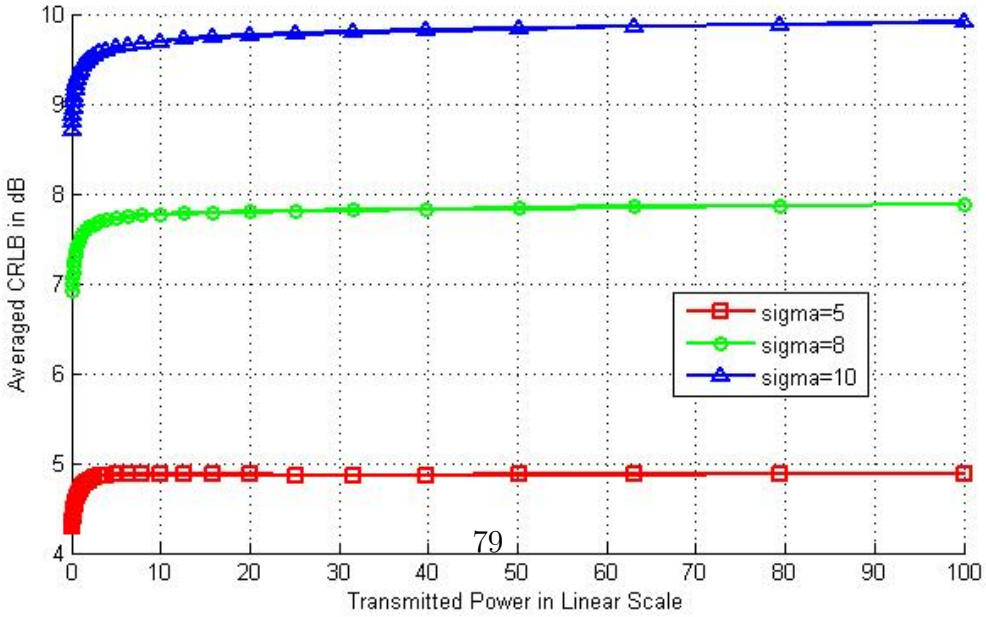


Figure 3.11: average CRLB in different transmitted power linear

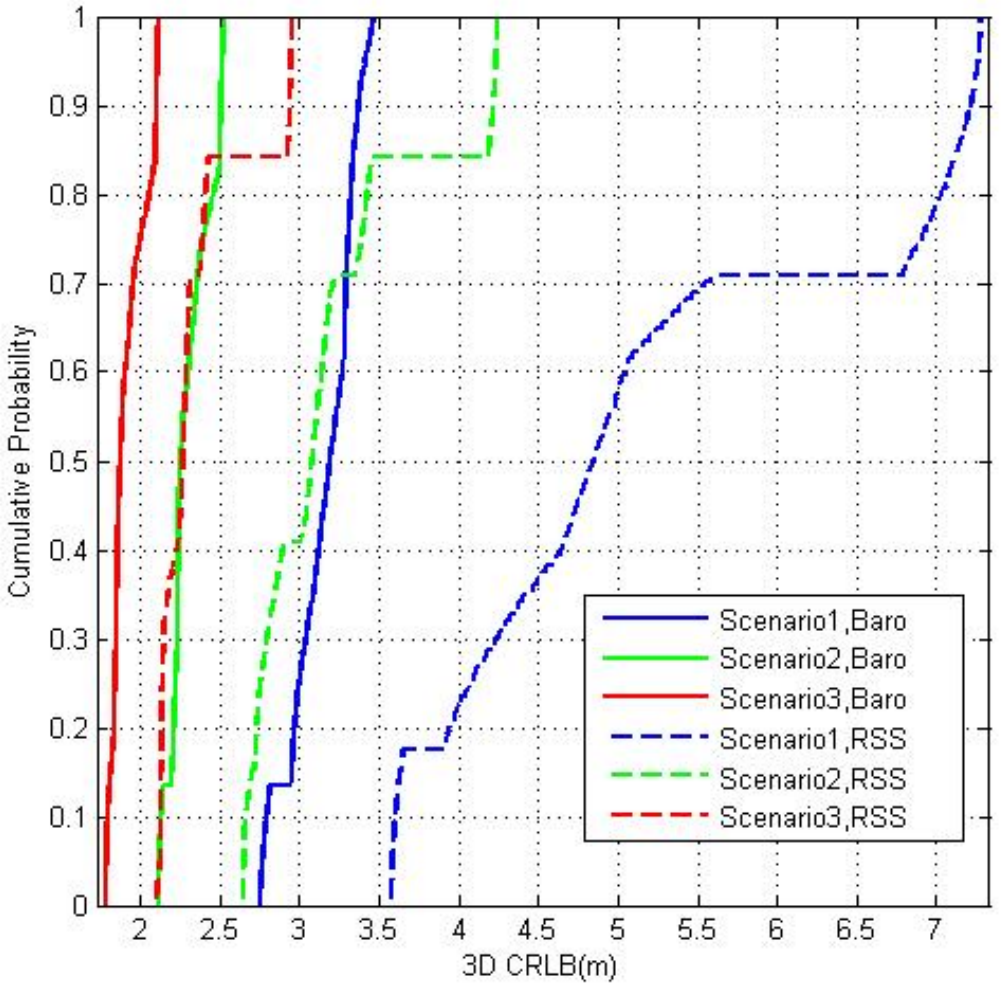


Figure 3.6: CDFs for Three Scenarios

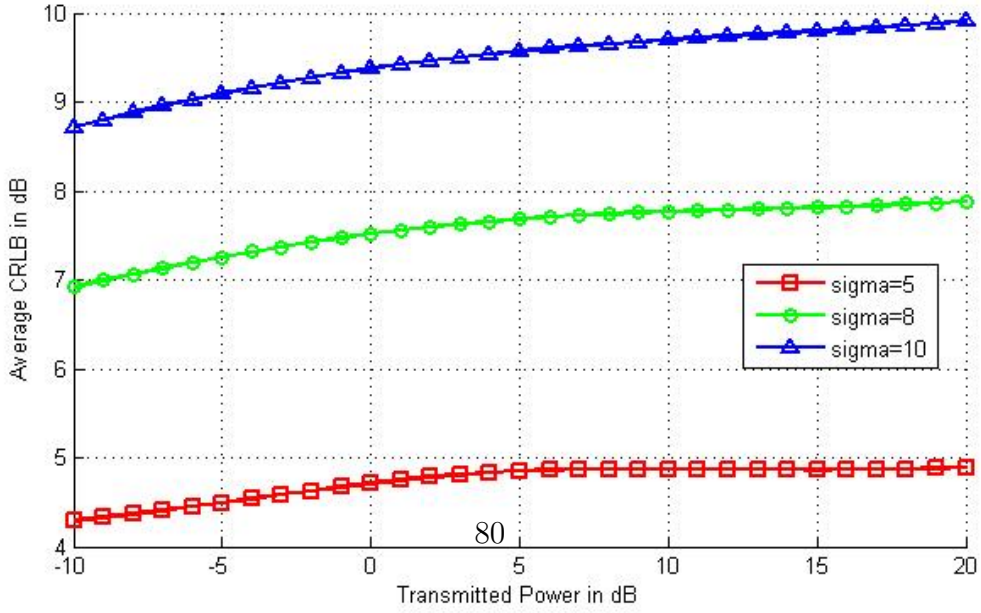


Figure 3.12: average CRLB in different transmitted power

3.5.4 Scenarios Design

To compare different geolocation systems, we designed 3 scenarios which can be used in checking the effect of multiple parameters. The detailed scenario description is given as follow:

- Scenario 1: 3 High-Power (HP) APs are placed on the ceiling and 27 Low-Power (LP) APs are placed in grid on the 3rd floor of Atwater Kent Laboratory, which is shown in Fig. 3.13. The red dots represent the HP Wi-Fi routers while the black ones represent the LP RF devices, such as iBeacons or smart bumps. $N(3-8)$ APs with the smallest path-loss will be selected for localization instead of all the APs, since we find that the rest APs can hardly contribute to the improvement of localization precision;

- Scenario 2: The deployment of the APs is the same as Scenario 1. The transmitted power is set to different levels so that how it can influence the localization precision can be investigated;

- Scenario 3: The deployment of HP APs stays the same while the LP APs is deployed randomly in on the floor so that the effect of different deployment can be explored;

The HP devices are set with a transmitted power of 20dBm and the LP devices from -10dBm to 20dBm in different scenarios. The channel model that is used is

Table 3.1: Barometer-Assisted Method vs. RSS-Only Method in Error Performance

CRLB (m)	Maximum	Minimum	Mean
Scenario 1 (Baro)	3.4641	2.1274	2.8113
Scenario 1 (RSS)	7.2791	2.5492	4.8193
Scenario 2 (Baro)	2.5254	1.6267	2.0658
Scenario 2 (RSS)	4.2394	1.9236	2.9214
Scenario 3 (Baro)	2.1120	1.3761	1.7286
Scenario 3 (RSS)	2.9488	1.5440	2.1393

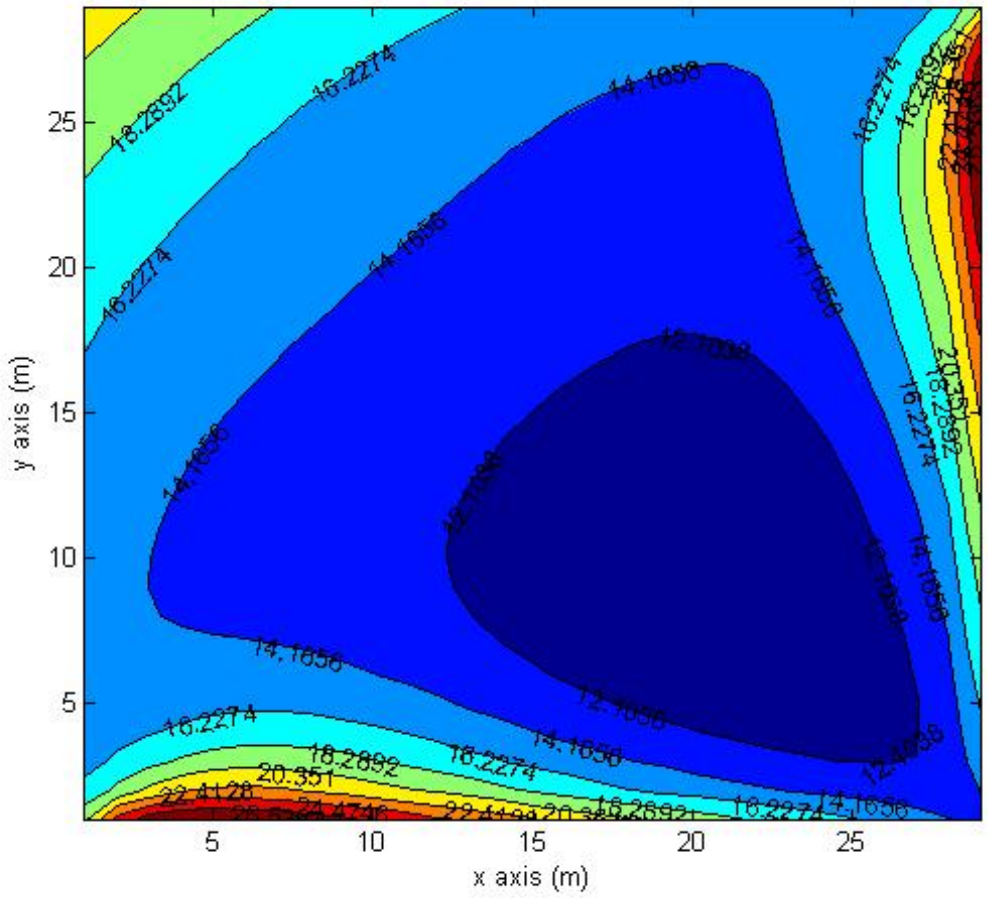


Figure 3.7: Contour for Scenario 1

the distance-partitioned model with operating frequency as 2.4GHz. The 3rd floor has a space of 23m×16m and a height of 5 meter. Samples are taken in every 0.1 meter (the 4 edges are not includes), so we have $229 \times 159 = 36411$ samples in total for every scenario.

3.5.5 CRLB with Different LP Device Number

The CDFs of CRLB with different selected APs number are shown in Fig. 3.14. We can see that, when the number increases, the range becomes narrower, which

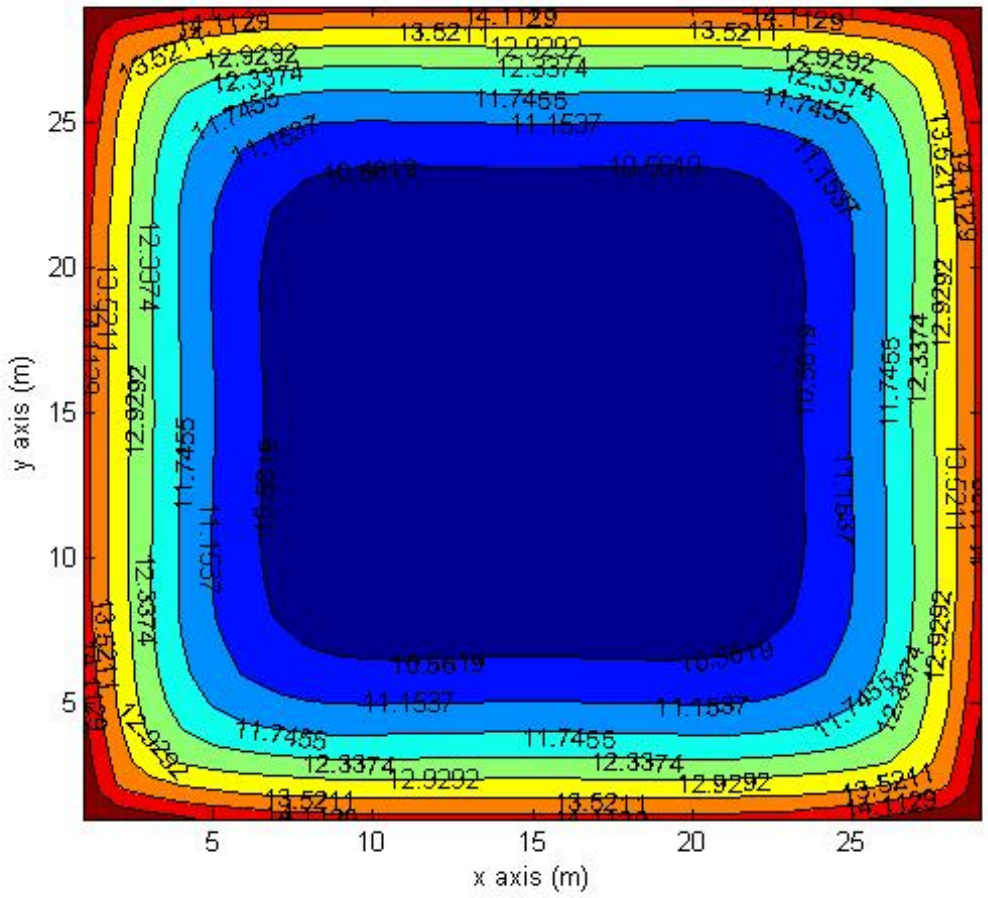


Figure 3.8: Contour for Scenario 2

indicates higher localization accuracy. But one thing should be paid attention to. As the selected APs number increases, the computational complexity will also increase exponentially. As described before, the complexity will be proportional to the factorial of the number N. Therefore, it is crucial to choose a suitable number so that the system can achieve highest efficiency with shortest processing time and reasonable localization precision. Table 1 illustrate the mean CRLB with different APs number vs. computational complexity. We cam easily find that, it is a wise choice to pick 5 or 6 APs since the complexity becomes too large afterwards.

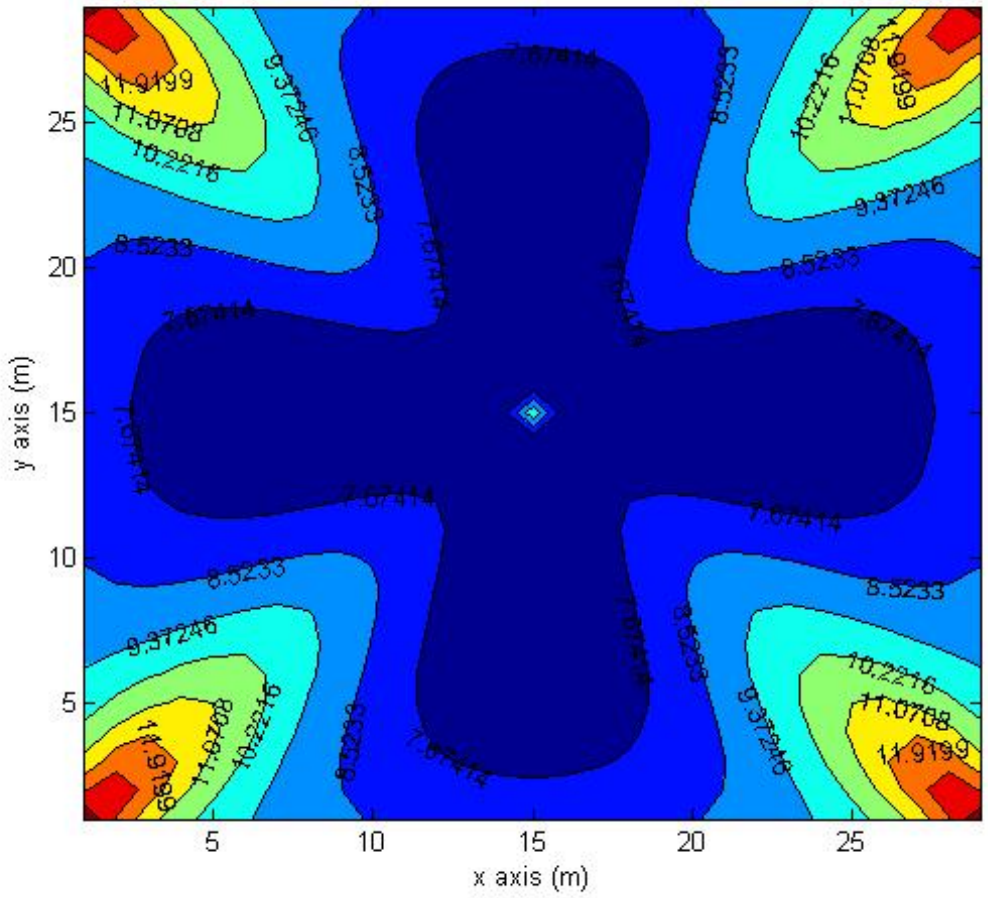


Figure 3.9: Contour for Scenario 3

Table 3.2: CRLB vs. Computational Complexity

n	$\mu(CRLB)$	$O(n!)$
3	4.68889	6
4	3.78545	24
5	3.40171	120
6	3.11401	720
7	2.92253	5040
8	2.80453	40320

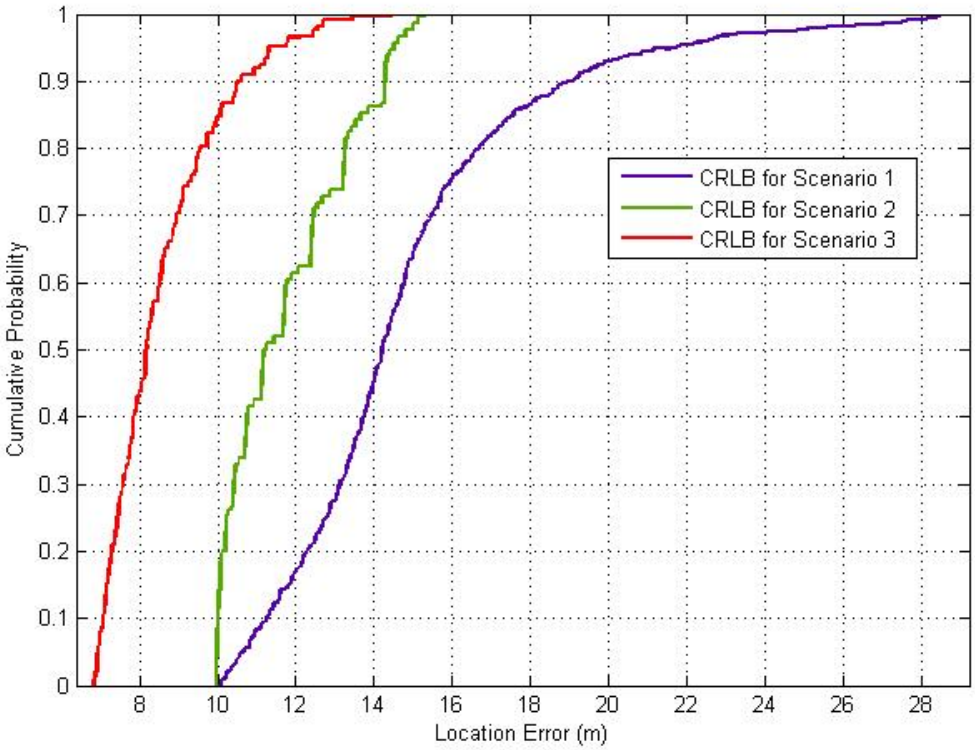


Figure 3.10: CDFs for 3 Scenarios in 2D

It is also worthwhile to mention that why we do not increase the number of HP devices. In the IoT environment, WiFi routers will be placed every several meters. So in our scenarios, three HP devices are quite enough to cover the entire area, which is exactly how our department deploy the routers. On the other hand, since the LP devices only cover comparatively smaller areas, and they are widely used and deployed, we can investigate more on these devices, and see how it may affect the localization precision when the number of LP devices changes.

3.5.6 CRLB in Different Transmitted Power

We illustrate the CDFs of CRLB for Scenario 2 in Fig. 3.15. In this figure, characteristic of error performance under different sets of transmitted power is

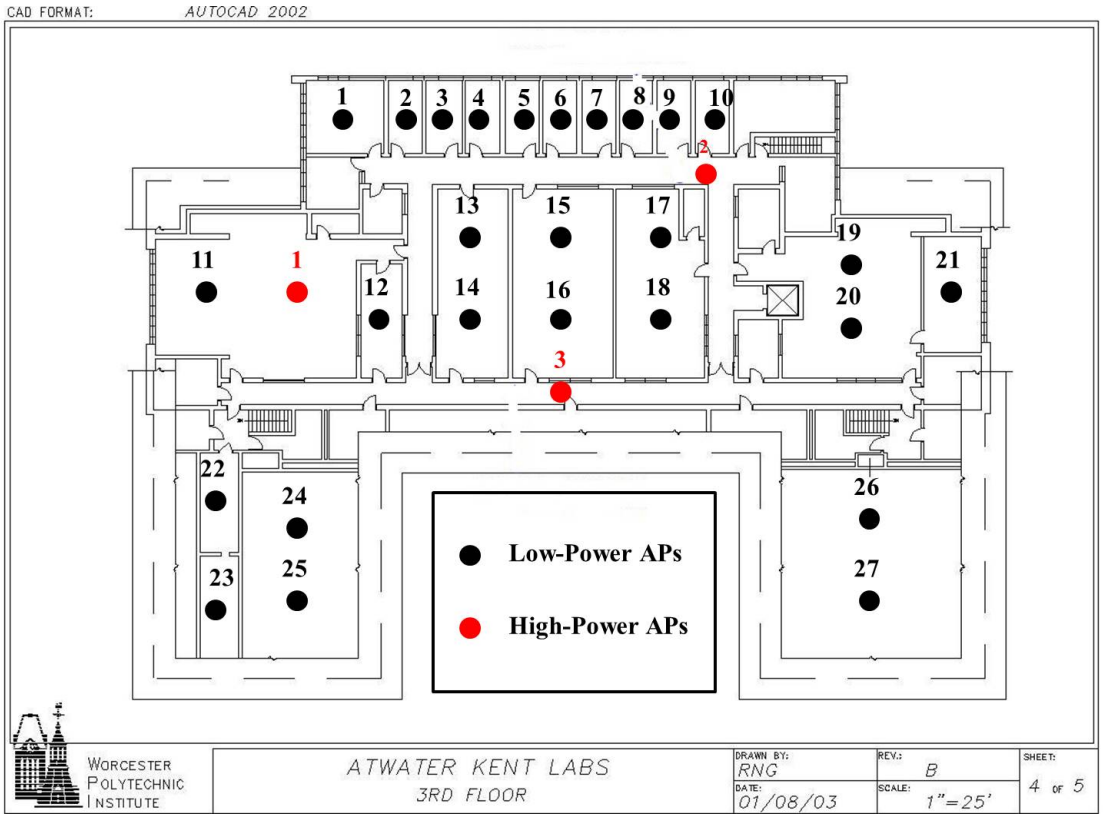


Figure 3.13: Deployment of APs in AK Building

clearly presented. Note that the CRLB will increase as the power level increases. It is because that when transmitted power becomes greater, more error from longer distance will be counted so that the localization precision will be worse than the ones with lower power level. Moreover, we can see that when standard deviation σ increases, the CRLB will also increase, indicating worse localization accuracy.

3.5.7 CRLB with Different LP Device Deployment

We also investigate how different deployment schemes can affect the CRLB. As is demonstrated in Fig. 3.16, it is straightforward that the random deployment will degrade the system localization performance. However, it is still crucial to explore

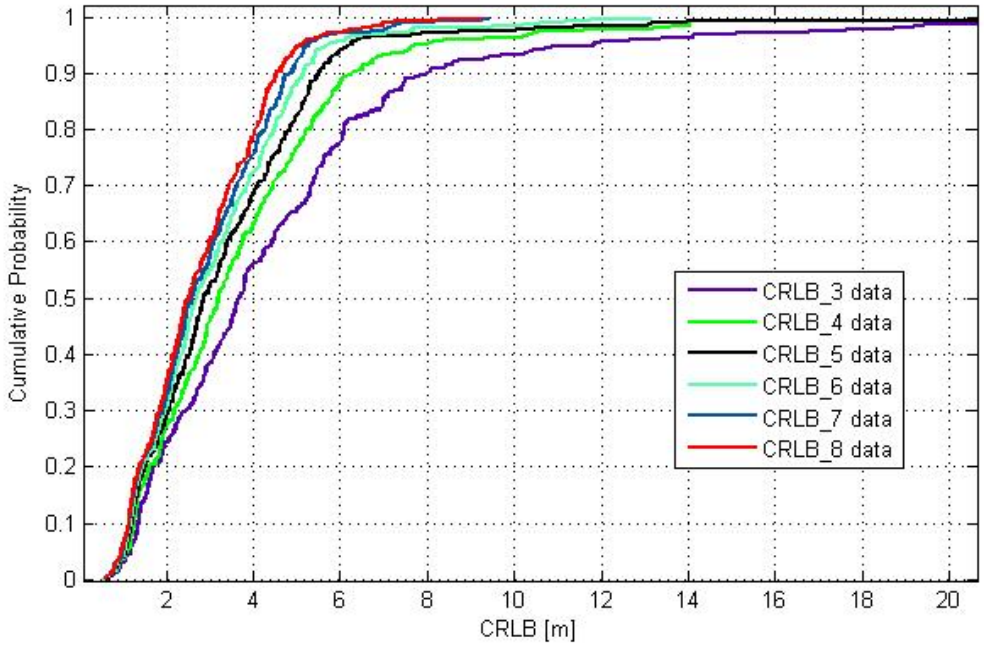


Figure 3.14: CRLB with Different Number of Selected APs

how much worse random deployment can be than grid, since most of time the LP devices are not fixed, their location will change and they can be anywhere generating information in the IoT environment.

3.6 Summary

In this paper, we present an approach to improve the performance of a 3D RSS-based geolocation system by using barometer in smart devices. A modified 3D path loss model is presented which brings penalty of ceilings into consideration. Based on the pressure-height physical law, we characterize the vertical estimation and fit it into a Gaussian Distribution. Calculation of 3D CRLB is provided as an expansion of the original 2D CRLB for performance evaluation. Moreover, We design 3 scenarios of different floors with various AP deployment strategies and

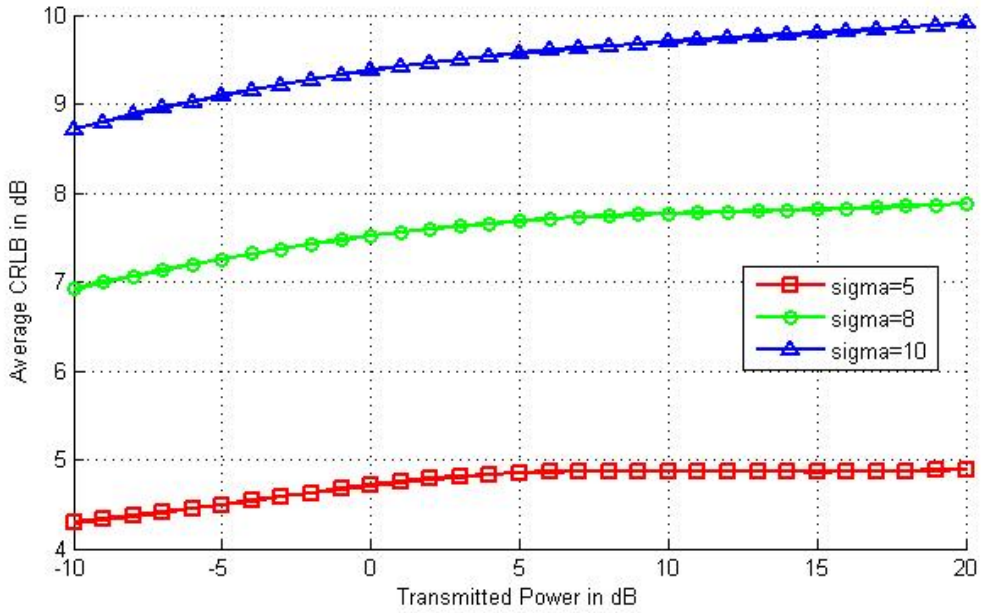


Figure 3.15: Average CRLB in Different Transmitted Power

conduct series of experiments for comparison. The improvement is specified with contour and CDFs of the scenarios and quantified from a comparison table.

Future work includes: To expand our system to buildings with more complicated architecture, which will make the research more related to the real world. Fully combining the barometer and RSS signal should also be explored, so that smaller error can be reached. It is also feasible if we integrate our technique with other sensors in smart phones to find if more improvement can be reached.

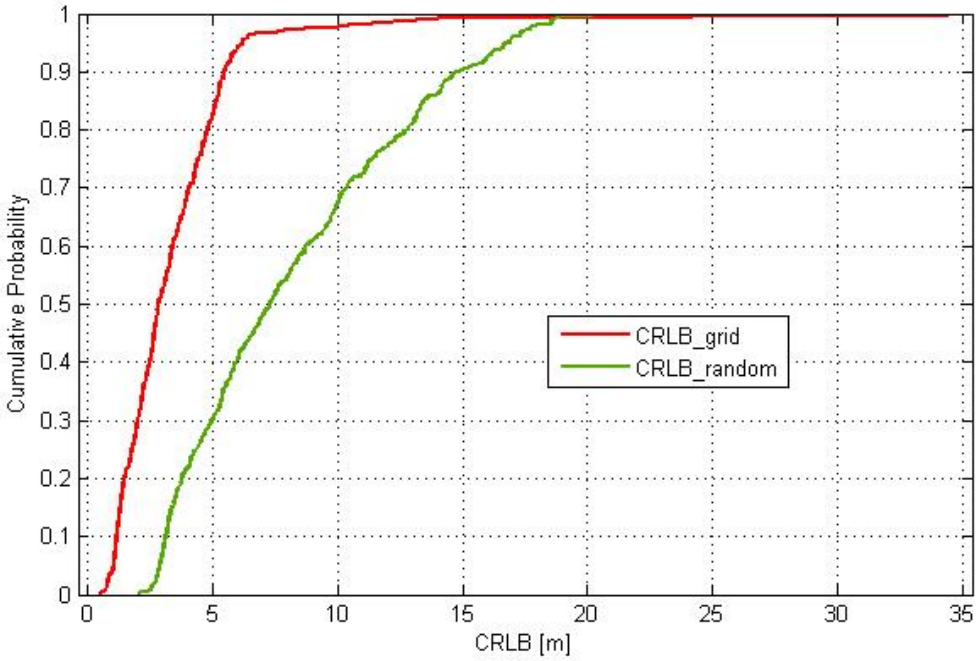


Figure 3.16: CRLB with Grid vs. Random Deployment

Chapter 4

Motion Detection using RF Features in IoT and Accuracy Analysis

4.1 Introduction

With the development of electronic and computer technologies, the idea of smart home [1-4] is widely spread. Numerous devices, not only computers and smartphones but also lights, cameras, windows, door bells, appliances and cooking utensils, etc. are connected through wireless signal to communicate and share information with one another, and take peoples commands, so that common tasks can be done in a cooperative way. Along with this, motion detection using various kinds of wireless signal can be efficiently utilized for health care [4,5], entertainment and social security, which have addressed increasing attentions. Compared with conventional motion detection systems using sensor [6], vision and radar, CSI based systems have the great advantage of device-free or device-independent, which needs

no extra and specific devices and provides non-invasive detection. For smart home, the communication service is already established and additional recognition devices are not necessary, therefore, CSI based system can be constructed at a low cost, with a wide range of applications [7]. Recently, CSI has been researched for various human motions such as fall detection [8,9], gesture detection [10], mouth movements detection [11] and even gait detection [12], etc. Among those, there is not a system specified for motions both on flat floor and staircase at home. As we know, motions on staircase are very common and meaningful in our daily life. For example, human especially elderly has a greater probability of falling on staircase than on flat floor. Thus, detection of falling on staircase is more essential than on flat floor for the case of health care; in addition, detection of walking on staircase can be leveraged to identify which direction human is walking: upstairs or downstairs, so that the system can automatically manage the power supply of lighting fixtures in different floor. Moreover, as individual has unique motion characteristics distinguished with others [12] such as: action habit, motion magnitude, etc. For example, juniors always walk much faster and powerful than seniors. Therefore, CSI can also be implemented for human identification to boost the security of smart home. In this work, we address the issues of motion detection and human identification for smart home applications and propose the system of WiHome. Numerous experiments of detecting most frequently appearing motions have been conducted to validate the robustness and accuracy, the candidate motion set includes: 1) Motions of walking, running, sitting and falling in flat floor environments such as corridor and living room; 2) Motions of walking upstairs, walking downstairs and falling in staircase environment at home.

Motions of the wireless device or objects close to the antennas of the wireless devices cause temporal fluctuations of characteristic of RF cloud features measured

at the receiver antennas. Recently, a number of researchers have studied these characteristics of RF cloud from wireless devices for activity, motion and gesture detection. This area of research expects to revolutionize human-computer interaction and introduce a variety of other cyber space applications by taking advantage of the variations in RF cloud features due to motions in the environment.

4.2 Background

Wireless communication receivers measure features of the RF cloud reflecting motions in the environment. Signal processing techniques help detect these motions and prepare them for cyberspace application development. Figure 9 illustrates the temporal variations of RSS of a receiver antenna in proximity of a transmitting antenna. The figure also shows the Fourier transform of the signal representing the Doppler spectrum and the short-term Fourier transform representing its spectrogram. Figure 9a shows a situation with no-motion, Figure 9b shows a situation with a hand held between the two antennas, and Figure 9c shows the results when the hand moves between the antennas. As the speed of motions increases, the bandwidth of the Doppler spectrum and the contrast of colors in the spectrogram increases. We can benefit from this change in depiction of the RSS characteristics, to develop hand motion related applications. All modern wireless devices measure RSS and many other features of the RF cloud that are available and accessible with software, opening an interesting area for motion related cyberspace applications.

The mmWave radar development environment (Fig. 5) also supports other aspects helpful in classification of motions. Figure 10 shows the range-velocity profile of the device illustrating motions of the finger in different directions. The mmWave

sensor extracts velocity information, and consolidates it with the range data to form the range-velocity profile. Figure 10a shows a hand, which is a strong reflector, at close distance from the radar and its corresponding profile. Figure 10b and 10c demonstrate that the finger movement creates radical velocities relative to the radar, and thus mirrored in the profile below. These depictions of motions open an opportunity for micro-gesture detection from finger motions.

In recent years, a number of researchers have benefited from RF cloud features to introduce innovative cyberspace applications. As a simple example, using an algorithm measuring variations of the RSS above its average value, one could detect the number of people attending a class [26], or monitor newborn babies in a hospital [27]. More complex cyberspace applications using opportunistic signals available in the RF cloud is achievable by using artificial intelligence algorithms and taking advantage of more complex features of the signal, such as CIR, CSI, TOA, and DOA. In recent years, a number of research laboratories have pursued this idea.

4.2.1 Scenario Design

Figure 4.1 shows ascenario for hand motion inside a room. Two antennas are one meter apart and a hand moves between the two antennas. When the hand is closing to the antennas we have a direct path and a path reflecting from the hand. When hand blocks the direct path we have two diffracted paths from sides of the hand. Assuming the width of the hand is 12cm, emulate the received signal when hand swings in one meter betweent he antennas. Assume reflection coefficient is 0.7 and the diffraction coefficient is 0.01(??). The geometry of hand motion detection scenario is as shown in Figure 2, where the hand is modeled as an elliptic cylinder with length w and the single-tone RF signal is emitted from Tx to Rx with a distance

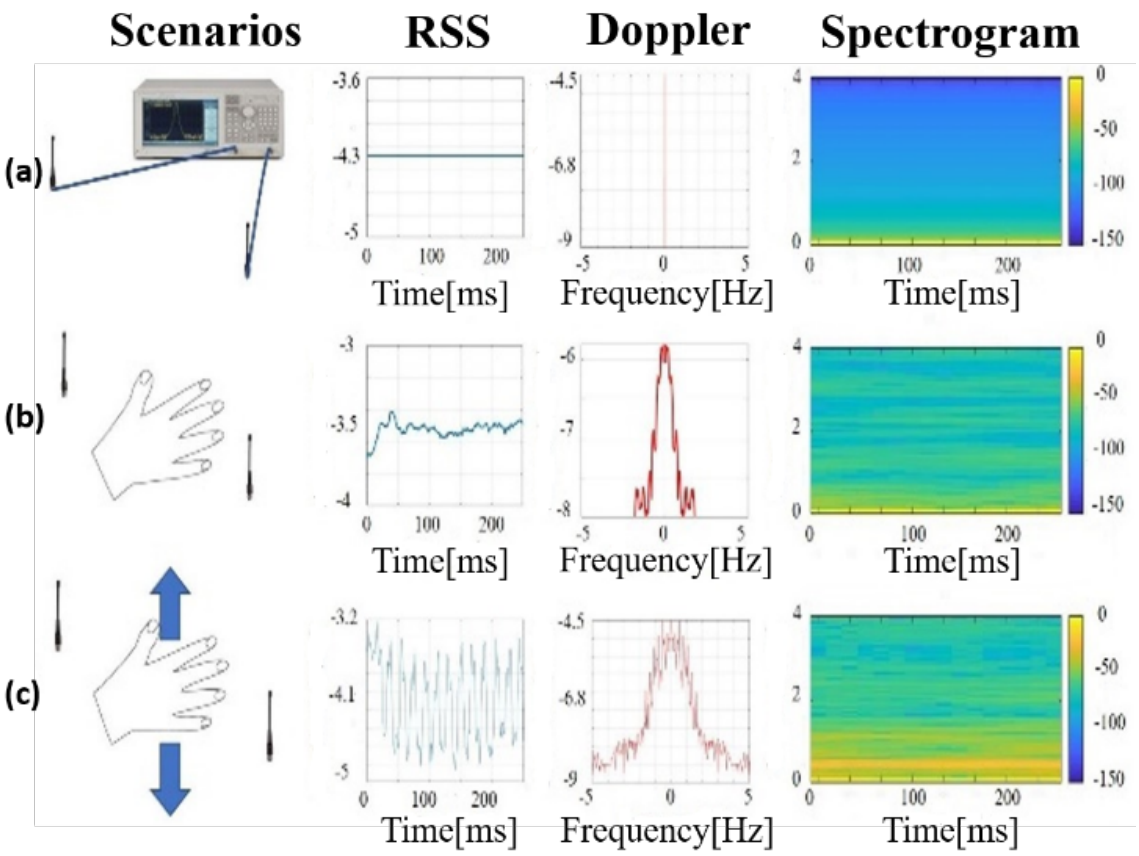


Figure 4.1: Power and Phase Variation Caused by Hand Motion

of l. For a better description of hand motion, three coordinate axes are applied: the X, Y and Z-axis, each is perpendicular to the other two. The distances that the hand moves along the three axes are set as variables x, y and z respectively. The origin is located in the middle of the LOS path and is also the original hand location before the hand starts to move. When the Tx-Rx are close enough, the received signal is mainly affected by the two diffracted paths, which are also illustrated in Figure 2. In fact, the radio waves from Tx can arrive at Rx by the double-wedge hand diffraction at points s1 and s2, and we label the two diffracted paths as d1 and d2. According to the geometry in Figure 2, we can calculate the distances of the two diffraction paths as follows:

4.2.2 RF Cloud Signal Characteristics

As CSI is fine-grained data, numerous characteristics in both time and frequency domain can be potentially extracted to form concrete feature profiles of candidate motions and humans. Firstly, based on the theoretical analysis of radio propagation model, six most useful and meaningful features in time domain are adopted to present the characteristics of candidate motions and humans: 1) The normalized standard deviation (STD), it is calculated for reflecting the scale of dynamic motion and a dramatic scale motion always results in large STD; 2) Median absolute deviation (MAD) is utilized as a robust measurement of the variability of a univariate sample of quantitative data. The sum of squared MAD can express the concentrating of data; 3) Interquartile Range (IR) is also extracted to indicate the dispersion of CSI variance; 4) Signal Shannon's entropy (SSE) is a generic measure of system disorganization and adopted to reflect the disorganization of CSI variance; 5) Peak to peak (PtP) indicates the difference between maximum and minimum amplitude of received signal; and 6) Time duration (TD) of each kind motion is unique and essential for the accuracy of classification. Apart from analyzing features in time domain, frequency features also benefit the accuracy of motion detection and human identification. As mentioned in Section 3.4, some similar motions can be easier discriminated through leveraging the energy distribution on frequency components. We applied the doppler spectrum for extracting the features in frequency domain. The doppler power spectrum has been adopted in [6] to analyze on-body channel variances and improves the wearable sensor based motions detection for the safety of firefighters. Which also has the ability of presenting the temporal variation of CSI frequency components caused by motions, especially for some similar motions that cant be easily discriminated only based on time features such as walking and running. The doppler power spectrum can be calculated through applying a

fast-Fourier transform (FFT) to the preprocessed CSI variances in time domain as Equation (7). The profiles of walking and running on flat floor are measured in time and frequency domain in Figure 6, respectively. As expected, motion of running has more energy distributions on higher frequency components than walking both in time and frequency domain.

4.2.3 Motion Detection Schemes

In our experiments, signal transmitter is a common commercial WiFi router with two antennas and receiver is a laptop equipped with Intel 5300 NIC. The CSI collection software is the open source CSI-tools presented by Halperin et al. and the Intel 5300 NIC reports CSI for 30 subcarriers spreading evenly among the 56 subcarriers of 20MHz channel or the 114 carriers in 40 MHz channel [28]. For detection of candidate motions and humans with the proposed device-free CSI based system, RF approach has been employed to achieve multiple candidate classification. RF is a machine learning algorithm that integrates multiple trees through the idea of integrated learning. In our work, multiple decision trees with an empirical selected amount are trained as the elementary elements and further integrated as RF. In order to validate the efficiency of RF, support vector machine (SVM) and k-nearest neighbor (KNN) are also introduced to discussion as well. In addition, considering some features are quite correlated with others, we propose a stepwise method to check the correlations of candidate features and limit the redundancy in classification process using a subset of all available features. The core idea is that we first check the correlation coefficients of all available features and then evaluate the combined effect of candidate features by take-away one feature at one time. Classification consists of two basic parts: training and testing. The training phase is responsible for construction of the database when features of each motion are extracted from CSI

data in the preprocessing phase. We conducted experiments with eight volunteers aged 20 to 29 years and mixed with four males and four females. They performed each candidate motion in motion set repeatedly in three typical home environments such as corridor, living room and staircase at Atwater Kent laboratories building of Worcester Polytechnic Institute. The motion set consists of seven most frequently appearing motions at home and has been divided into two categories: 1) Motions of walking, running, siting and falling in flat floor environment including living room and corridor; 2) Motions of walking upstairs, walking downstairs and falling in staircase environment. Since motions performed in different locations make different multipath effects, volunteers always perform motion in the middle of transmitter and receiver and the distance between transmitter and receiver is 4 to 5 meters. The experimental setting is illustrated in Table 2 and environments are shown in Figure 7.

4.3 Detection Accuracy Comparison

Wireless positioning taking advantage of signals from existing Wi-Fi infrastructure deployed for wireless communications was the first popular application of RF cloud. In that application, we read the address of a Wi-Fi access point from its floating broadcast packets and we record the RSS feature of the channel, to develop our positioning system. Motions of the wireless device or objects close to the antennas of the wireless devices cause temporal fluctuations of characteristic of RF cloud features measured at the receiver antennas. Recently, a number of researchers have studied these characteristics of RF cloud from wireless devices for activity, motion and gesture detection. This area of research expects to revolutionize the human-computer interactions and introduce a variety of other cyber space applications by

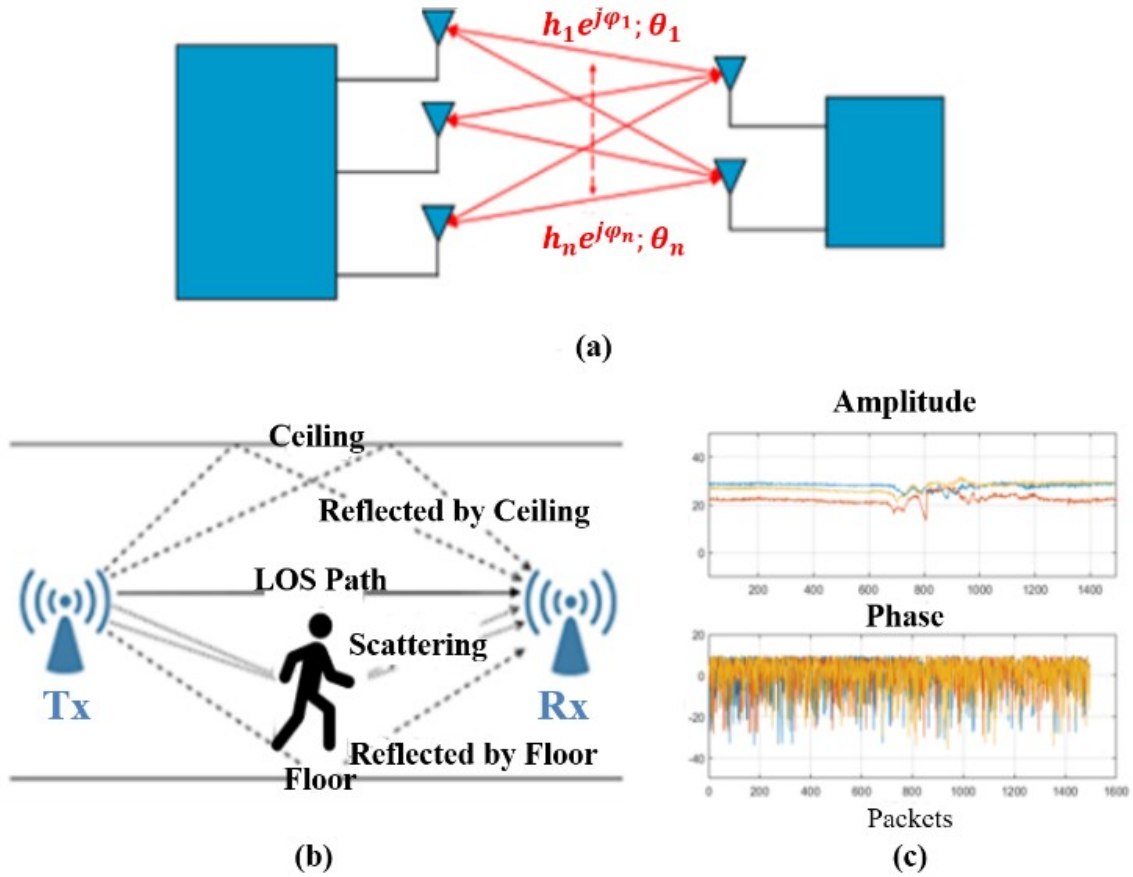


Figure 4.2: Power and Phase Variation Caused by Body Motion

taking advantage of the variations in RF cloud features due to motions in the environment.

Depiction of RF Features due to Motion Wireless communication receivers measure features of the RF cloud reflecting motions in the environment. Signal processing techniques help depicting these motions and prepare them for cyberspace application development. Figure 4.1 illustrates the temporal variations of RSS of a receiver antenna in proximity of a transmitting antenna. The figure also shows the Fourier transform of the signal representing the Doppler spectrum and the short-term Fourier transform representing its Spectrogram. Figure 9a associates with a situation with no-motions, Figure 9b belongs to a hand with natural motions held

between the two antennas, and Figure 9c shows the results when the hand moves between the antennas. As the speed of motions increases, the bandwidth of the Doppler spectrum and the contrast of colors in the Spectrogram increases. We can benefit from this change in depiction of the RSS characteristics, to develop hand motion related applications. All modern wireless devices measure RSS and many other features of the RF cloud that are available and accessible with software, opening an interesting arena for motion related cyberspace applications.

The temporal variations of RSS for a receiver antenna in proximity of a transmitting antenna and its Doppler Spectrum and Spectrogram (a) with no-motion, (b) with a hand with natural motions, (c) with a moving hand between the antennas. The mmWave radar development environment (Fig. 5c) also supports similar graphic information data from the Fourier transform over the range profiles to depict motions. This phase-based knowledge is essentially objects velocities at different ranges and the Fourier transform indeed presents the so-called range-Doppler profile illustrated in Figure 10. The mmWave sensor extracts phase information, and consolidates it with the range data to form the range-Doppler profile. Figure 10.a shows a strong reflector at close distance of the corresponding profile. Figure 10b and 10c demonstrate that the finger movement creates radical velocities relative to the radar, and thus mirrored in the profile above. These depictions of motions open an opportunity for micro-gesture detection from motion of fingers. 2) Motion Related Cyberspace Applications In recent years, a number of researchers have benefited from depictions of RF cloud features to introduce innovative cyberspace applications. As a simple example, using an algorithm measuring variations of the RSS above its average value, idea presented in [26] detects number of people attending a class, or in [27] monitors newborn babies in a hospital. More complex cyberspace applications using opportunistic signals available in the RF cloud is achievable by

benefiting from artificial intelligence algorithm and taking advantage of more complex features of the signal, such as CIR, CSI, TOA, and DOA. In recent years, a number of research laboratories have pursued this idea.

At the Worcester Polytechnic Institute, variations of the RSS of body-mounted sensors is used for activity monitoring of first responders to find out if a fire fighter carrying a device is standing, walking, laying down, crawling, or running [28-30]. These states of motion reflect the temporal behavior of the fire fighter, describing seriousness of the situation she or he is facing. The work in [28] uses traditional characteristics of the fading, such as coherence time, rms Doppler spread, and threshold crossing rate of the RSS of simple devices such as Bluetooth, to differentiate different motions and the work presented in [29] integrates AI algorithms into the motion detection process. The work presented in [30] benefits from more complex CSI signals of Wi-Fi devices along with more complex AI algorithms such as Long-short-term-memory Regressive Neural Network (LSTM-RNN), to increase the capacity of the system in differentiating different motions on a flat floor or when climbing the stairs. As we explained in section II.B.2, CSI provides multiple streams of RSS and more diversified variations of the signal. In [31], the research group demonstrates the use of mmWave radar in tracking the motion of a finger, opening up further study in gesture-based application controls in the Human Computer Interaction (HCI) arena. Researchers at the University of Washington [32] have used Wi-Fi signals for hand gesture recognition to differentiate nine different hand motions. Multiple RSS stream from different channels of the OFDM signal of Wi-Fi are depicted by a Spectrogram to generate frequency-time characteristics color images. The AI algorithm classifies the image to detect the nine gestures of the hand motion. At Michigan State University [33], the CSI of Wi-Fi signal is use for keystroke detections. Since during typing of a certain key, the hands and fingers of a user move

in a unique formation and direction, it generates a unique pattern of CSI RF fingerprint. By training an AI algorithm, they have detected the keystrokes of the user of a keyboard. At the Massachusetts Institute of Technology [34], researchers have used signals similar to the Wi-Fi signals a radar with multiple antennas, for human pose estimation through walls and occlusions. They demonstrated that they can detect multiple human postures through the walls using the RF signal and a neural networking algorithm. The used visual data during the training period for the AI algorithm. At Stanford University [35] commodity Wi-Fi signals are used for tracking hand motion for virtual reality applications to replace existing infrared devices. In parallel with academic studies, practical applications of RF signals for motion and gesture detection and tracking are emerging in industry. As an example, Google [36] uses RF radar signal at mmWave frequencies obtained from antenna arrays, for micro-motion tracking of hand and finger gestures for applications such as connection less winding or rolling over the surface of a wristwatch. In general, RF signal variations can replace any application using mechanical sensors. For example, electronic gaming industry commonly uses mechanical sensors such as accelerometer for interactive electronic gaming, or health-monitoring industry considers using accelerometer mounted on the gait of a patient to measure the extent of progress in Parkinson decease [37, 38]. We can benefit from RF cloud of UWB devices, measuring the CIR, to implement interactive electronic gaming [39], we can consider UWB signals to help visually impaired [40], or we can possibly use UWB signal features for gait motion detection.

Building on the advances in motion, activity and gesture detection using RF Cloud, researchers have begun to explore the possibilities for future HCI. Early work explored using unmodified GSM signals to enable recognition of eight tapping gestures, four hover gestures and two sliding gestures around a mobile device, to enable in-

coming call management as well as phone navigation from a distance [41]. More recent work, has demonstrated an mmWave gesture recognition pipeline [36] as well as the recognition of eleven gestures with short-mmWave radar with a goal of them being used in human-computer interaction [42]. Other work explored mmWave gesture recognition for in-car infotainment control [43]. Radar signals have also been explored for automatically classifying everyday objects to support various applications including a physical object dictionary that looks up objects that are recognized, context-aware interaction, as well as future applications such as automatic sorting of different types of waste, assisting the visually impaired and smart medical uses [44]. Using radio signals and one external sensor hanging on the wall, researchers have demonstrated that gait velocity and stride length, which are important health indicators, can be monitored, enabling health-aware smart homes [45]. Taking advantage of indoor WiFi signals to identify motion direction, researchers have created a contactless dance exergame [46] as well as sign language gesture recognition [47]. Other work demonstrated that 5GHz WiFi can be used to achieve decimeter localization accuracy of up to four users as well as activity recognition of up to three users doing six different activities [48].

4.4 Summary

The success of wireless networks has resulted in the deployment of a huge infrastructure as well as development of inexpensive wireless devices. Big data from the RF cloud of the infrastructure and devices has enabled a number of intelligent cyberspace applications in motion and gesture detection. With the help of various AI algorithms, more and more precise detection can be made, which can benefit our daily life in the future.

Chapter 5

PHY-based Key Generation using RF Cloud

5.1 Introduction

The continual development of faster automatic information processing systems has created a need for high data rate communications systems. Ultra-wideband (UWB) wireless communications systems have been proposed for next generation wireless because of their high data rate capacity as wells as their robustness, capability for signal transmission through standard building materials, and simplicity of system design. However, a disadvantage of existing wireless communications systems is the danger of the integrity of the communications being compromised. Wireless systems send electromagnetic waves through open space that passive eavesdroppers can intercept. Thus, the security sub-system in wireless systems has a more important role than in wireline systems. A challenge for the designers of UWB wireless systems is to develop methods for data integrity and security. Recently, a novel technique has been developed to use direct UWB channel characterization to generate

the secret keys to provide security in the physical layer of wireless communications systems. UWB channel measurements are used to create shared cryptographic secret keys for each given pair of communicating terminals. The automated generation of a secret key is intrinsically spatially and temporally specific, increasing security. Indoor UWB channels have been found to be independent for antenna separation distances of more than 15.2 cm. Therefore, if a reasonable distance separates the eavesdroppers from each of the legitimate users, the channel impulse response between legitimate users becomes a source of shared unique secret information.

5.2 Problem Formulation

5.2.1 System Model

Fig. 2.12 shows the physical scenario, where users A and B communicate via an UWB channel and generate a shared secret key based on the received signals. The channel from A and B is modelled as a multipath fading model with channel impulse response, which is essentially invariant during the period of coherence time. Both users are assumed to be half-duplex in the sense that they cannot transmit and receive signals at the same frequency simultaneously. The channel between A and B is reciprocal, which means by transmitting signals in forward and backward directions, the legitimated users can develop correlated information for key bit extraction. (The underlying noise in each channel is additive white noise with uniform distribution.) Each user possesses a maximum likelihood estimator for amplitude and phase estimation. We also assume that the network possesses a common time reference and is well synchronized.

5.2.2 Threat Model

Following the same assumptions in most PHY-based key generation schemes in literature [??], we assume there is a passive adversary, who can eavesdrop all the communications between legitimate users. The adversary knows the whole key generation protocol, and it can also perform amplitude/phase estimation based on received signals during key generation process. The adversary aims to derive the secret key, while it is not interested in disrupting the key establishment by jamming the communication channels. In addition, we assume that the participating users are all trusted, and node compromise or other types of attacks are not considered here as described in previous section.

5.2.3 Multipath Fading Channel Characteristics

When the magnetic waveform propagates through a wireless channel, due to reflection, diffraction and scattering caused by the objects between and around the transceivers, the signal arrives the receiver in multiple paths. The received signal is a summation of signals from multiple paths with different delays. This summation can be either constructive or destructive, which depends on the relative propagation delays of signals. Furthermore, relative movement between the environment and the mobile terminals can change the paths randomly, which leads to random fluctuation in the phase and amplitude of the received signal. This random fluctuation gives birth to the following three properties that serve as the basis for key generation using characteristics of fading channels.

Temporal Variation: Due to the movement of the entities in the environments as well as the communicating parties themselves, the received signal experiences

different fadings along time. Theoretically the fading at two time points are independent if the interval between the two time points is larger than the channel coherence time. In wireless communications, coherence time is a statistical measure of the time duration over which the channel impulse response is essentially invariant, and quantifies the similarity of the channel response at different times.

Spatial Variation: In a multipath environment, receivers at different locations receive signals that experience different and independent fadings from the same transmitter. According to communication theory, an entity that is at least half the wavelength away from the network nodes experiences fadings statistically independent of the fadings between the communicating nodes.

Reciprocity: The signals transmitted between a transmitter and receiver pair experience the same fading in the coherence time. This is because the propagation paths of the forward link and backward link are theoretically identical during the coherence time. It is obvious that while the temporal and spatial variations can be exploited to meet the security goals, the reciprocity property can be exploited for key generation.

5.3 Key Generation Protocols

The common randomness is either extracted from the amplitude or phase of the received signals. Generally, a key generation scheme consists of three steps: Channel probing, Measurement quantization, and Error correction.

5.3.1 Security Key Extraction from Received Signal Strength

Recently, practical RSS-based key generation schemes have been extensively studied. However, the key bit generation rate supported by these approaches is very low. This significantly limits their practical usage given the intermittent connectivity in mobile environments. To address the problem, several enhanced schemes are proposed to increase the key bit generation rate.

The basic schemes mainly consist of the following three steps:

Step 1: channel probing. In the first timeslot, A transmits a known sequence to B. Upon receiving the signal, B measures and records the RSS values of the sequence. In the second timeslot, B transmits a known sequence to A. Upon receiving the signal, A measures and records the RSS values. The length of the time slot is usually set as half of the channel coherence time. If multiple rounds of channel probings are run during the same coherence time period, the randomness of the generated key bits is decreased.

Step 2: measurement quantization. Both A and B convert their RSS measurements into random key bits using a quantizer.

When the impulse response is obtained, with the help of peak detection algorithm, the signals received from direct path and reflected path can be identified. For example, Fig 1 shows a typical CIR generated from ray tracing, after peak detection, we can detect the first 5 peaks shown with red stems.

With the amplitude of each detected path, key generation algorithm can be applied for security keys. We denote Pr_i as amplitude of each path, then the difference of the maximum and minimum power will be used for quantization, which can be written as $D = max(Pr_i)$, where D is the total power difference. If we want to generate N bits public key, each level of bit will take $d = \frac{D}{2^N}$.

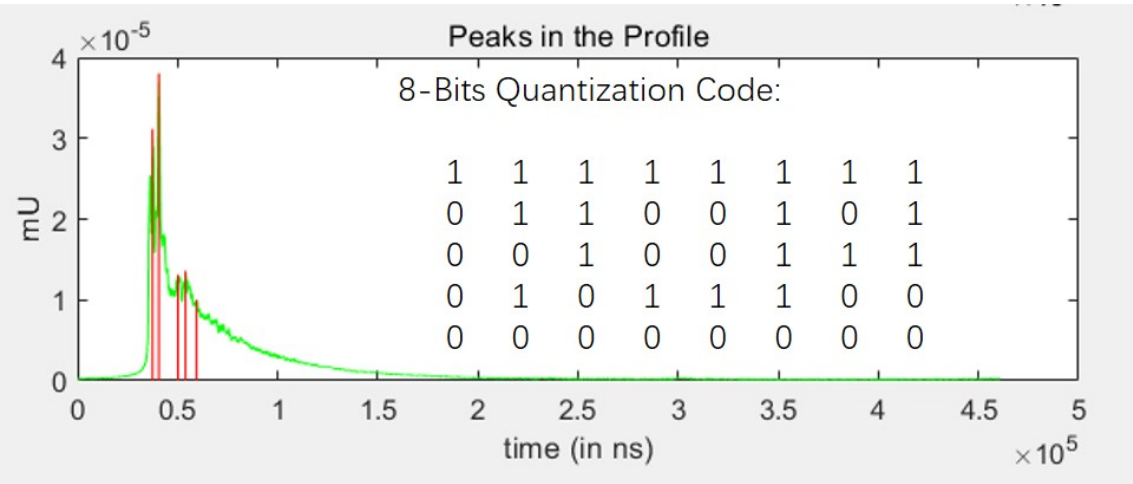


Figure 5.1: Security Key Generated from Ray tracing

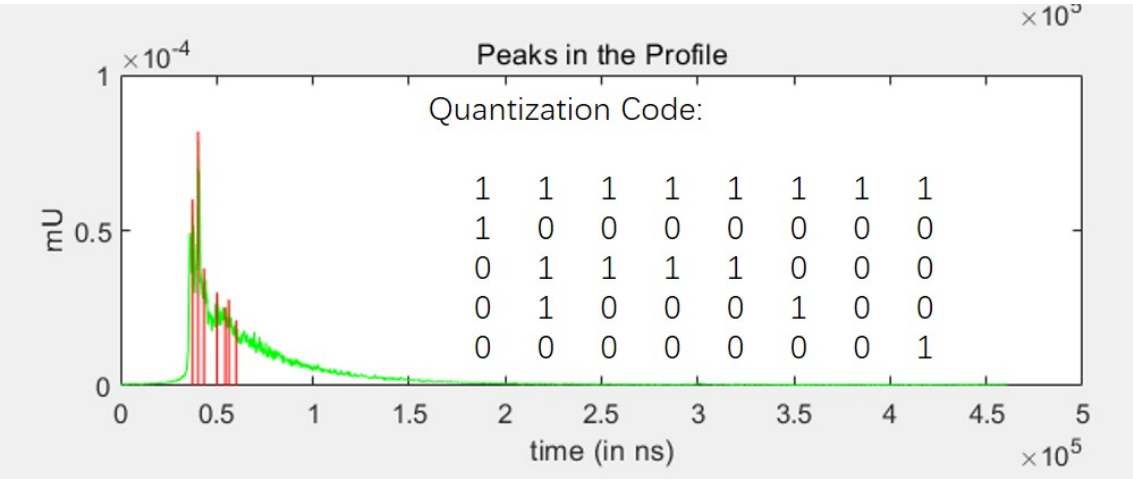


Figure 5.2: Security Key Generated after Adding Noise

Then we add a Gaussian noise to the each of the bits to model the effect of shadow fading at the transceiver. We denote Pr_i as the real power level of the received amplitude, then after adding the noise n with zero mean and standard deviation of σ, the received power becomes

$$Pr_i = Pt - 20log(r_i) + n \tag{5.1}$$

It is obvious that when the power level falls outside the range of $[-\frac{d}{2}, \frac{d}{2}]$, an

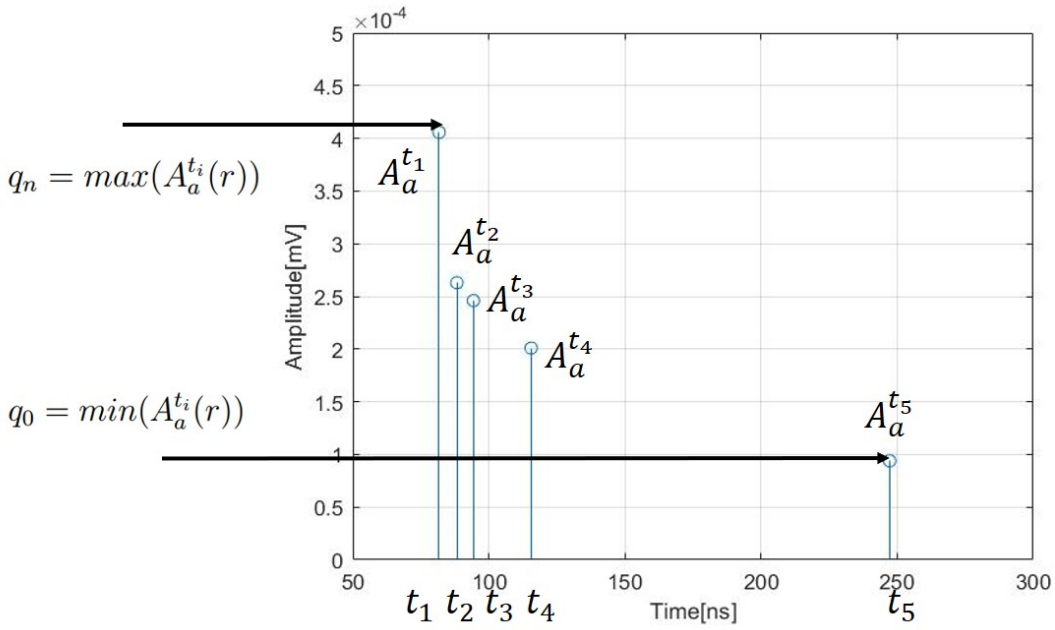


Figure 5.3: RSS-based Key Generation

error appears. Then the probability of error can be derived as

$$Pe_i = P(Pt-20log(r_i)+n > (\lfloor\frac{Pt-20log(r_i)}{d}\rfloor+1)*d)+P(Pt-20log(r_i)+n < (\lfloor\frac{Pt-20log(r_i)}{d}\rfloor)*d) \tag{5.2}$$

which can be further calculated by the complementary function

$$Pe_i = P(n > \frac{d}{2}) + P(n < -\frac{d}{2}) \tag{5.3}$$

which is simply related to r_min the distance from the direct path.

$$Pe_i = P(n > \frac{Pt-20log(r_{min})}{2*2^N}) + P(n < -\frac{Pt-20log(r_{min})}{2*2^N}) \tag{5.4}$$

$$P_e = \frac{1}{d}\int_{-\frac{d}{2}}^{\frac{d}{2}}[\frac{1}{2}erfc(\frac{d}{2}-x)+\frac{1}{2}erfc(\frac{d}{2}+x)]dx \tag{5.5}$$

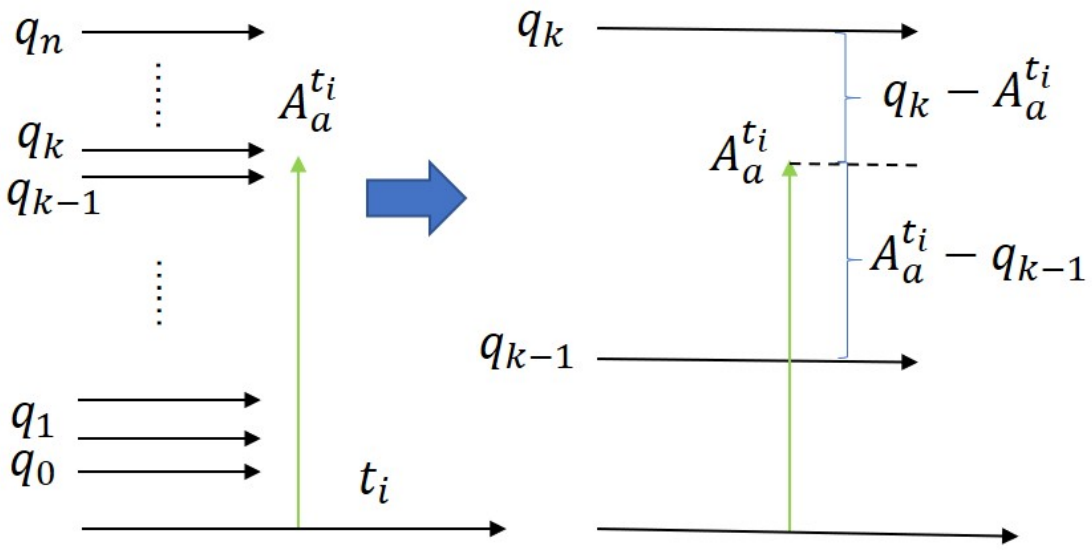


Figure 5.4: Upper and Lower Bound of RSS-based Key Generation Schemes

Since the integral of the complementary function can be calculated as

$$\int erfc(b+az)dz = -\frac{b}{a}erf(b+az) + z * erfc(b+az) - \frac{e^{-b^2-2abz-a^2z^2}}{a\sqrt{\pi}} \tag{5.6}$$

Then the probability of error can be derived in the closed form of

$$\int_{-\frac{d}{2}}^{\frac{d}{2}} erfc(\frac{d}{2}-x)dx = \frac{d}{2}erf(\frac{d}{2}-x) + x * erfc(\frac{d}{2}-x) - \frac{e^{-(\frac{d}{2})^2+dx-x^2}}{\sqrt{\pi}} \tag{5.7}$$

which is

$$[d * erf(0) - \frac{1}{\sqrt{\pi}}] - [d * erf(d) - \frac{e^{-d^2}}{\sqrt{\pi}}] \tag{5.8}$$

and

$$\int_{-\frac{d}{2}}^{\frac{d}{2}} erfc(\frac{d}{2}+x)dx = -\frac{d}{2}erf(\frac{d}{2}+x) + x * erfc(\frac{d}{2}+x) - \frac{e^{-(\frac{d}{2})^2 - dx - x^2}}{-\sqrt{\pi}} \tag{5.9}$$

which is

$$[d * erf(0) - \frac{1}{\sqrt{\pi}}] - [d * erf(d) - \frac{e^{-d^2}}{\sqrt{\pi}}] \tag{5.10}$$

Then the closed form will be the sum of (6) and (8), which is

$$Pe_i(r) = \frac{1}{2}erf(r) + \frac{e^{-r^2}}{r\sqrt{\pi}} \tag{5.11}$$

Then the total probability of error would be:

$$Pe(r) = 1 - \prod_{i=1}^{N}(\frac{1}{2}erf(r) + \frac{e^{-r^2}}{r\sqrt{\pi}}) \tag{5.12}$$

$$q_0 = min(A_a^{t_i}(r)) \tag{5.13}$$

$$q_n = max(A_a^{t_i}(r)) \tag{5.14}$$

$$d = \frac{q_n - q_0}{n} \tag{5.15}$$

$$P_e^i(r) = P(A_a^{t_i} + N > q_k | A_a^{t_i} \in [q_{k-1}, q_k]) + P(A_a^{t_i} + N < q_{k-1} | A_a^{t_i} \in [q_{k-1}, q_k]) \tag{5.16}$$

$$P_e^i(r) = 1 - \int_{q_{k-1}-A_a^{t_i}}^{q_k - A_a^{t_i}} \frac{1}{2\sqrt{\pi}\sigma} e^{-\frac{x^2}{4\sigma^2}} dx \tag{5.17}$$

$$P_e^i(r) = 1 - \frac{1}{2}[erf(\frac{q_k - A_a^{t_i}}{2\sigma}) - erf(\frac{q_{k-1} - A_a^{t_i}}{2\sigma})] \tag{5.18}$$

$$Pe_{total}(r) = 1 - \prod_{i=1}^{N} \frac{1}{2}[erf(\frac{q_k - A_a^{t_i}}{2\sigma}) - erf(\frac{q_{k-1} - A_a^{t_i}}{2\sigma})] \tag{5.19}$$

$$\sigma^2 = W * N0 = -168 + 10log_{10}(W) \tag{5.20}$$

$$\sigma_t^2 >= \frac{1}{\rho^2 \beta^2} \tag{5.21}$$

$$P_e^i(r) = P(t_i + N > t_{t+1} | t_i \in [t_{i-1}, t_{i+1}]) + P(t_i + N < t_{i-1} | t_i \in [t_{i-1}, t_{i+1}]) \tag{5.22}$$

$$P_e^i(r) = 1 - \int_{t_{i+1}-t_i}^{t_i - t_{i-1}} \frac{1}{2\sqrt{\pi}\sigma_t} e^{-\frac{x^2}{4\sigma_t{}^2}} dx \tag{5.23}$$

$$P_e^i(r) = 1 - \frac{1}{2}[erf(\frac{t_i - t_{i-1}}{2\sigma_t}) - erf(\frac{t_{i+1} - t_i}{2\sigma_t})] \tag{5.24}$$

Step 3: Error correction. A and B reconcile the bit discrepancies between their generated keys. The bi discrepancies may be caused by noise, interference, hardware variations, and half-duplex probing signal transmission. Common practice is to use key reconciliation and privacy amplification techniques for achieving key agreement.

The key generation schemes based on RSS are subject to a tradeoff between key

bit generation rate and key bit mismatch rate. Since too many quantization levels may increase the key bit mismatch rate, they determine the quantization level by estimating the entropy of the measurements. In addition, they use a guard band between quantization bins to further guard the key agreement rate. The resulting key bit generation rate is increased by more than four times compared to that of single-antenna system.

It is observed that non-simultaneous channel measuring undermines the link reciprocity, while fractional interpolation can recover the reciprocity of the link.

5.3.2 Secret Key Extraction from Channel Phase

Compared to RSS-based key generation schemes, channel-phase-based methods have three major advantages. First, the channel phase of the received signal has uniform distribution under narrowband fading channels. Second, the existing signal processing techniques allows for high resolution estimation of phase of the received signal, which implies that higher key bit generation rate is achievable. Third, the phase estimates can be accumulated across multiple nodes, which enables efficient group key generation.

Step 1: Channel probing. This step is similar to its counterpart in RSS-based methods. The phase difference between the two single-tone sinusoid signals is computed and recorded for quantization.

Step 2: Measurement quantization. Different from RSS-based schemes, channel-phase-based schemes adopt a quantization approach that employs the uniformness of the channel phase distribution.

Similar to RSS-based key generation schemes, with the help of peak detection algorithm, the signals received from direct path and reflected path can be identified.

For example, Fig 2.12 shows a typical CIR generated from ray tracing, after peak detection, we can detect the first 5 peaks shown with red stems.

With the TOA of each detected path, key generation algorithm can be applied for security keys. We denote t_i as TOA of each path, then the difference of the maximum and minimum time delay will be used for quantization, which can be written as $D = max(t_i) - min(t_i)$, where D is the total power difference. If we want to generate N bits public key, each level of bit will take $d = \frac{D}{2^N}$.

Then we add a Gaussian noise to the each of the bits to model the effect of shadow fading at the transceiver. We denote t_i as the real time delay of the received amplitude, then after adding the noise n with zero mean and standard deviation of σ, the TOA becomes

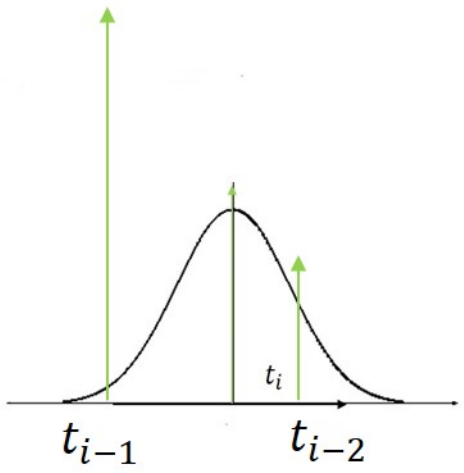


Figure 5.5: Phase-based Key Generation

Then the probability of error can be derived as

$$\sigma^2 = W * N0 = -168 + 10log_{10}(W) \tag{5.25}$$

$$\sigma_t^2 >= \frac{1}{\rho^2 \beta^2} \tag{5.26}$$

$$P_e^i(r) = P(t_i + N > t_{t+1} | t_i \in [t_{i-1}, t_{i+1}]) + P(t_i + N < t_{i-1} | t_i \in [t_{i-1}, t_{i+1}]) \quad (5.27)$$

$$P_e^i(r) = 1 - \int_{t_{i+1}-t_i}^{t_i - t_{i-1}} \frac{1}{2\sqrt{\pi}\sigma_t} e^{-\frac{x^2}{4{\sigma_t}^2}} dx \quad (5.28)$$

$$P_e^i(r) = 1 - \frac{1}{2}[erf(\frac{t_i - t_{i-1}}{2\sigma_t}) - erf(\frac{t_{i+1} - t_i}{2\sigma_t})] \quad (5.29)$$

Since the integral of the complementary function can be calculated as

$$\int erfc(b + az)dz = -\frac{b}{a} erf(b + az) + z * erfc(b + az) - \frac{e^{-b^2 - 2abz - a^2 z^2}}{a\sqrt{\pi}} \quad (5.30)$$

Then the probability of error can be derived in the closed form of

$$\int_{-\frac{d}{2}}^{\frac{d}{2}} erfc(\frac{d}{2} - x)dx = \frac{d}{2} erf(\frac{d}{2} - x) + x * erfc(\frac{d}{2} - x) - \frac{e^{-(\frac{d}{2})^2 + dx - x^2}}{\sqrt{\pi}} \quad (5.31)$$

which is

$$[d * erf(0) - \frac{1}{\sqrt{\pi}}] - [d * erf(d) - \frac{e^{-d^2}}{\sqrt{\pi}}] \quad (5.32)$$

and

$$\int_{-\frac{d}{2}}^{\frac{d}{2}} erfc(\frac{d}{2}+x)dx = -\frac{d}{2}erf(\frac{d}{2}+x) + x * erfc(\frac{d}{2}+x) - \frac{e^{-(\frac{d}{2})^2 - dx - x^2}}{-\sqrt{\pi}} \quad (5.33)$$

which is

$$[d * erf(0) - \frac{1}{\sqrt{\pi}}] - [d * erf(d) - \frac{e^{-d^2}}{\sqrt{\pi}}] \quad (5.34)$$

Then the closed form will be the sum of (6) and (8), which is

$$Pe_i(r) = \frac{1}{2}erf(r) + \frac{e^{-r^2}}{r\sqrt{\pi}} \quad (5.35)$$

Then the total probability of error would be:

Step 3: Error correction. Similar to RSS-based schemes, the key reconciliation and privacy amplification techniques used in RSS-based methods are all applicable to channel-phase-based method.

5.4 Analytical Results

In this work, our algorithms for key generation and agreement has been simulated with two different decoding methods. The simulated communication channel model is the UWB channel model CM1 from the IEEE p802.15 standard. The sample time has been set to 0.167 nano-seconds. The detectors of this system are simple non-coherent envelope detectors. The transmitted pulse signal s(t) is a raised cosine signal with a pulse duration of T = 20ps with the energy value of Es = 1.

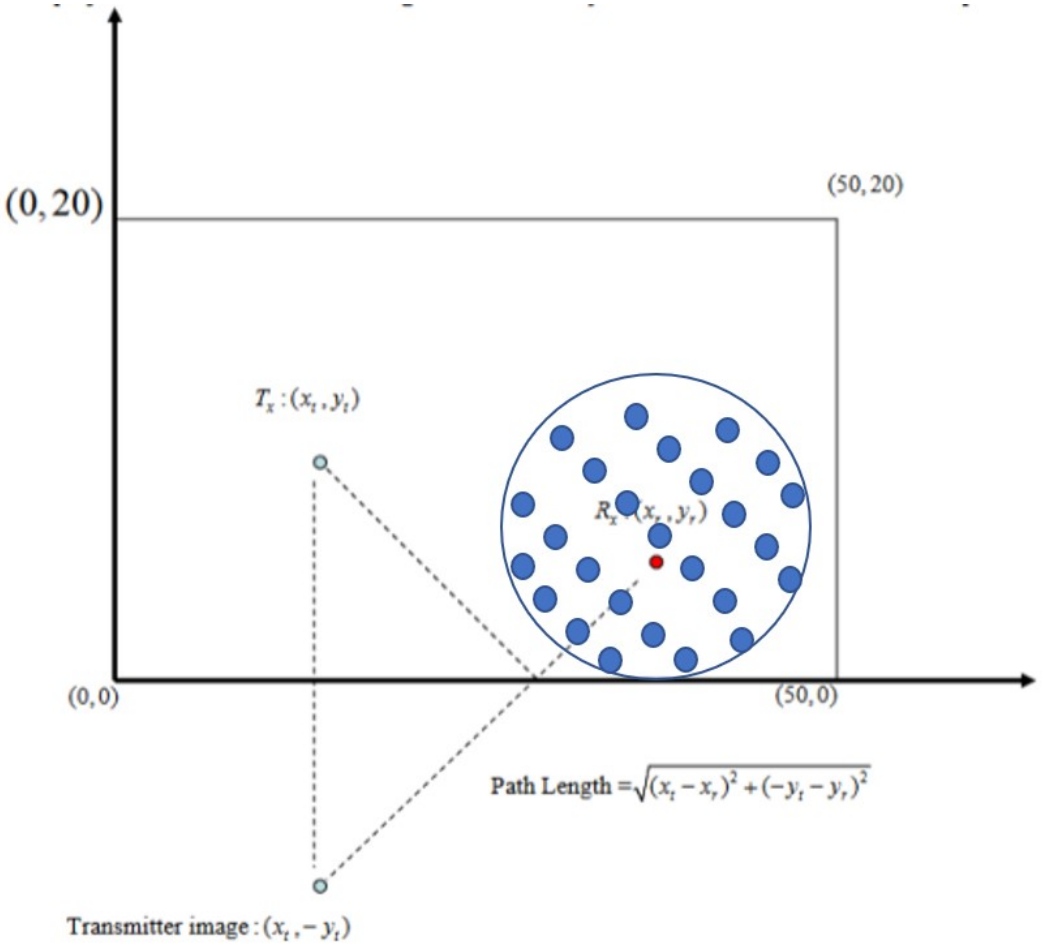


Figure 5.6: Ray tracing scenatio

The LDPC code used to generate the decoder has a code rate of 1/2, a code length of n = 64800, and a message length of k = 32400. Fig. 5 shows the cumulative distribution function for key agreement error versus different key length and signal-energy-to-noise-power ratio (SNR). Here, we do not have a consistent definition of SNR with what generally is used in data communication systems. So that, the signal is not tranmitted as data but it is to measure the channel characteristic. When the SNR is increased, the difference between the received signal for A and B decreases so the probability of key disagreement decreases. The key rate in this simulation is the code rate of LDPC decoding, 1/2, times the code rate of Hamming decoding,

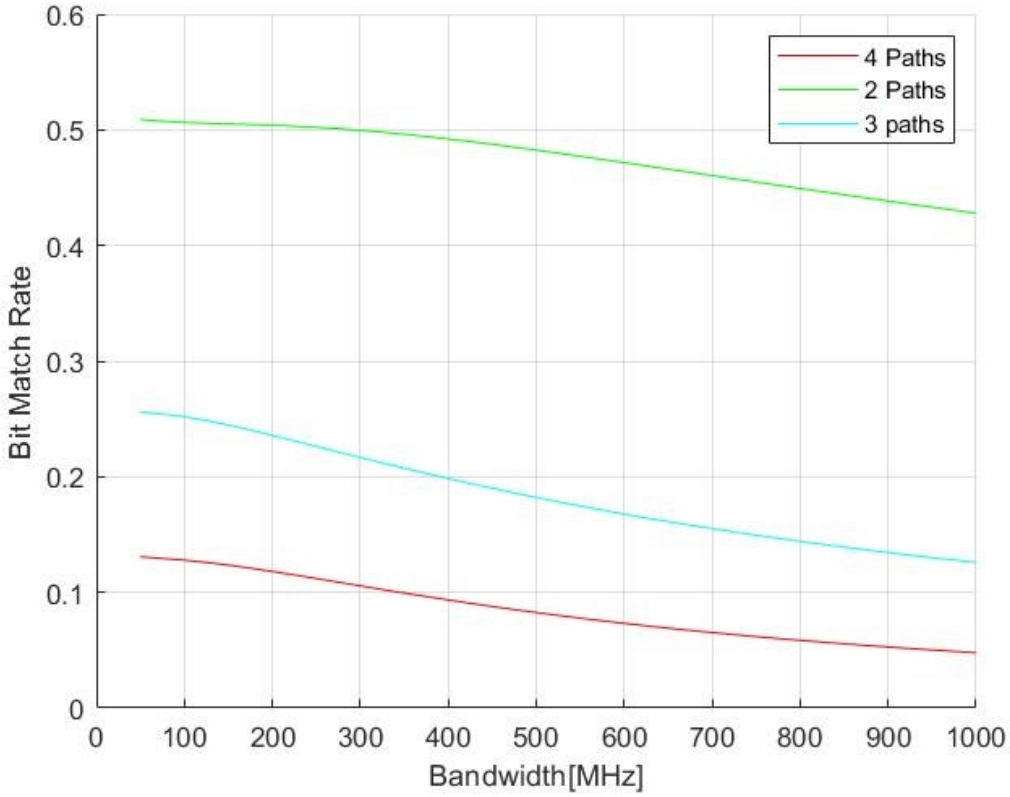


Figure 5.7: Bit Match Rate with Different Bandwidth

3/7, is equal 3/14. From each 14 bits of channel samples, 3 bits can be shared secret bits for the secret key. To calculate the probability of error the algorithm has been run 100 times and the number of key disagreements was recorded. For comparison, the result of the authors previous work [7] has been shown in Fig. 6. In this algorithm a three bits linear quantizer had been used instead of LLR computation and LDPC decoder blocks. In this prior work, a (3,1) repetition code was used for public discussion instead of the Hamming (7,3) code proposed in this work. with the above mentioned codes, the syndrome has two bits length. The key rate of this algorithm is 1/3. In Fig. 7 the CDF of agreement error for SNR = 5dB with new and previous methods has been shown. with the comparison of the results of the two algorithms, it is obvious that there is an improvement in key agreement

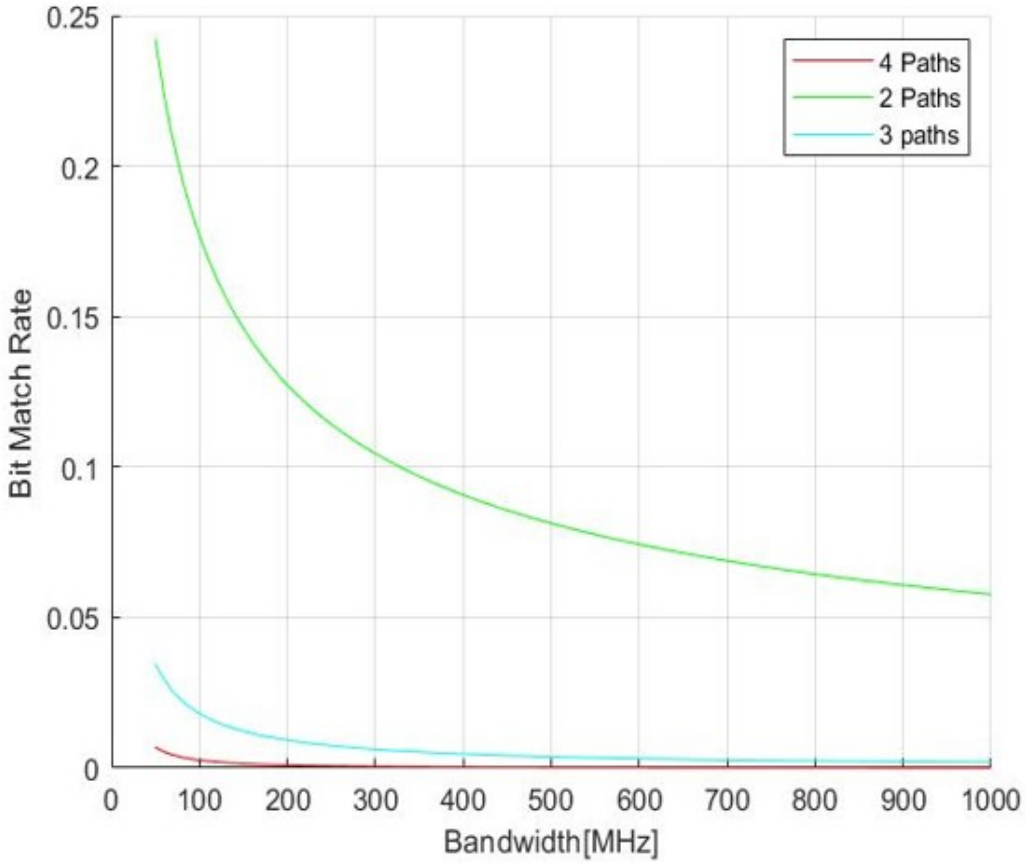


Figure 5.8: Bit Match Rate with Transmitted Power

algorithm with LDPC and hamming (7,3) algorithm. In this method the probability of error has been decreased 10 times with respect to the previous algorithm, three bits quantizer and (3,1) repetition code.

5.4.1 Performance Comparison

Key disagreement probability: KDP refers to the portion of different bits in the key bit string prior to error correction. A high KDP dramatically decreases the efficiency of the key generation protocol, and even makes the protocol fail due to the failure of key reconciliation. The KDP of RSS-based schemes is determined by

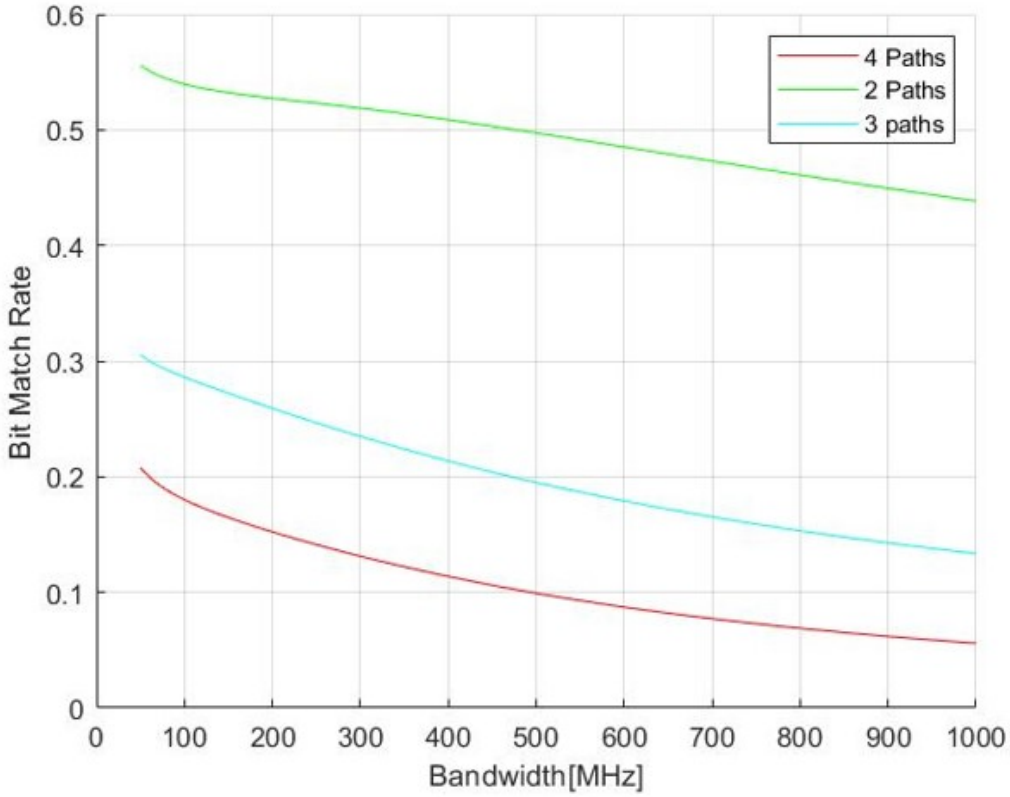


Figure 5.9: Bit Match Rate with Different Power Level

the variations of wireless channel. In a stationary environment, RSS-based methods have a high KDP of about 50 Key generation rate: The basic RSS-based key generation schemes have very low KGR. This is because they have to strike a balance between KGR and KDP as well as randomness of the key. First, to decrease the KDP, they have to extract only one bit out of m consecutive measurements above the upper bound or below the lower bound and discard all the other measurements. Second, KGR of the basic schemes suffers from limited level-crossing rate of the Rayleigh fading channel. Oversampling the channel can produce highly correlated measurements which result in keys with low entropy.

The random initial phase introduced in the probing signals causes the randomness of the key without only relying on fast variations of the channel.

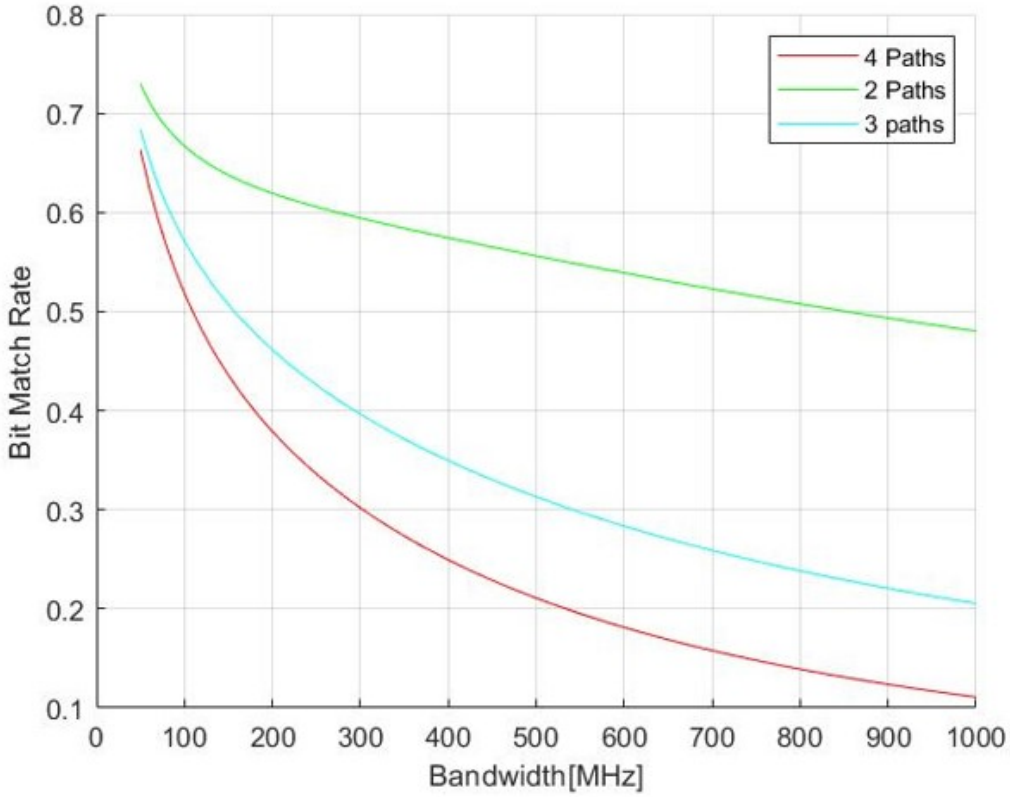


Figure 5.10: Bit Match Rate with Different Power Level

The use of multibit extraction is very suitable for channel-phase-based key generation schemes as channel phases are uniformly distributed.

Key bit randomness: A cryptographic key should be substantially random; otherwise the adversary can crack the key with low time complexity. For the RSS-based schemes there is a tradeoff between key bit randomness and key bit generation rate. That is, key bits should be extracted at different channel coherence time intervals to ensure the key bit randomness. Compared to the RSS-based methods, the channel-phase-based scheme does not have such a constraint. This is because the random initial phase and channel phase both contribute to the randomness of the generated key. Even if the channel remains constant, the random initial phase can guarantee high entropy of the generate key bits.

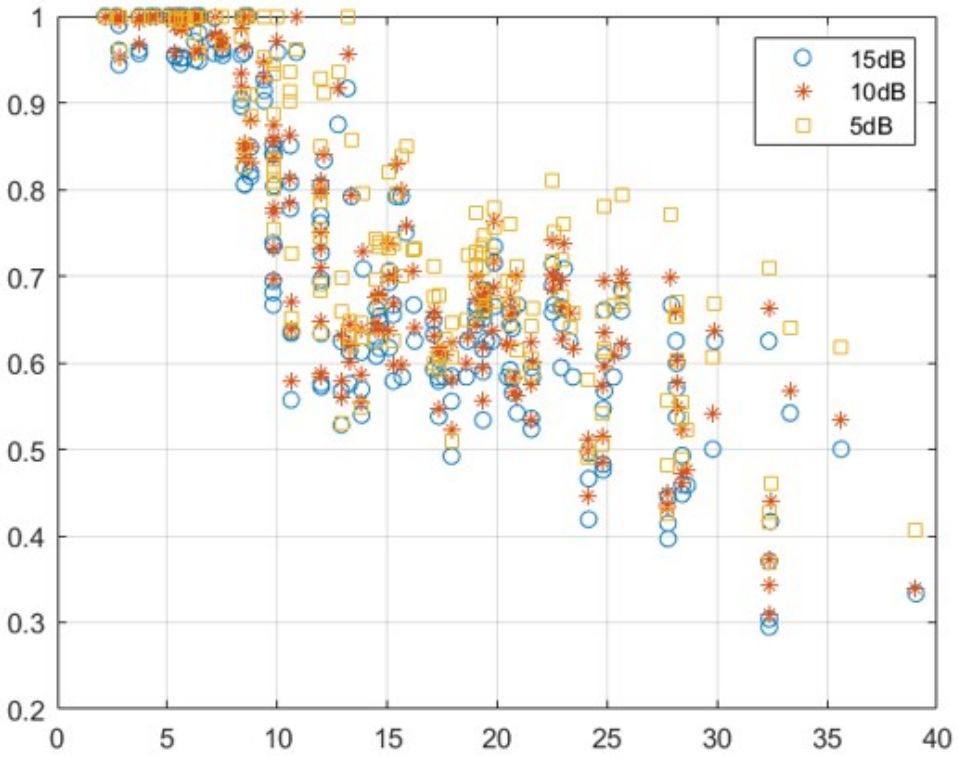


Figure 5.11: Accuracy of Key Generation with different scenatio

Scalability: For applications where multiple parties are involved, a group key needs to be established for securing he group communication. Obviously, the nave method of constructing a group key is to run the pairwise key generation protocol multiple times. However, such a centralized group key generation protocol suffers from low efficiency when the size of the group grows. The scalability of the scheme is constrained by the coherence time and SNR. On one hand, as size of the group increases, the transmission time of the probing signals along the clockwise and anticlockwise circuits increases. Thus, a single round of bit generation should finish within the minimum coherence time; otherwise, the channel reciprocity cannot be maintained. On the other hand, both SNR and size of the group affect the KDP due to the accumulation of estimation errors. Lower SNR or a larger group size can

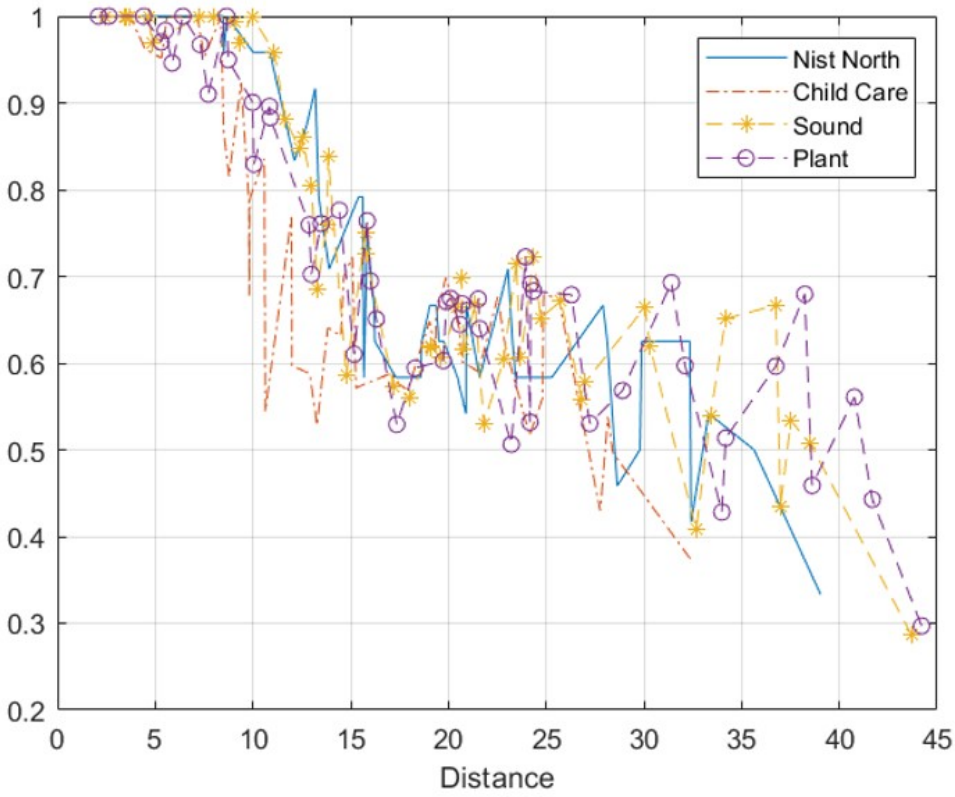


Figure 5.12: Accuracy of Key Generation with different nosie level

greatly increase KDP.

Implementation Issues: The RSS-based key generation methods can use off-the-shelf hardware for implementation, as the measurement of RSS can easily be read from a wireless card on a per frame basis. The channel-phase-based schemes seem to have the best overall performance; however their implementation is nontrivial. They require an analog-to-digital converter (ADC) working at Nyquist frequency of the single-tone carrier. The hardware complexity also depends on the operating frequency band of the radio system. Most existing studies on PHY-based key generation usually assume a passive adversary. However, a PHY-based key generation protocol may also be subject to active attacks such as modification, insertion, and jamming in practice. So far the problem of key generation in the presence of an

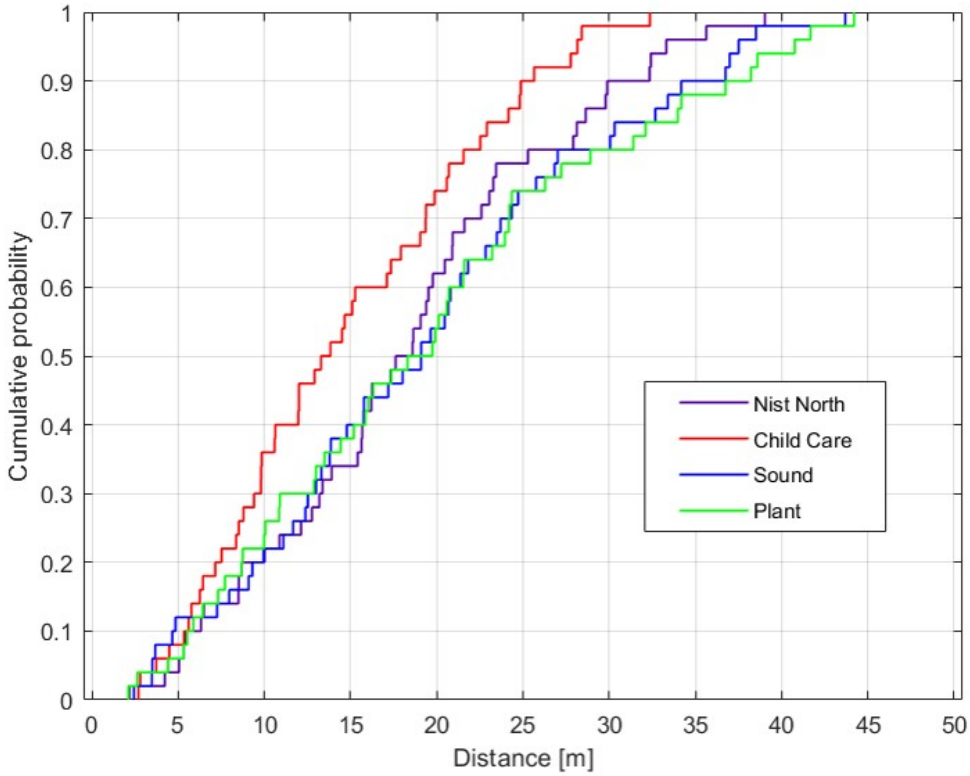


Figure 5.13: Distribution of Nist Distance

active adversary has only received limited attention.

Chapter 6

Conclusion

In this dissertation, we presented three challenging problems in the field of IoT related precise localization and motion detection, and secure key generation. All three challenging problems can be regarded as emerging fundamental areas for scientific research and engineering developments.

Firstly, CRLB using PoC has been derived in dense IoT environment, we conclude that with the help of low power devices, localization accuracy can be improved and the load of fingerprinting can be eliminated.

Secondly, we demonstrate two examples of motion detection using UWB and mmWave signals, showing that in both cases, we can reach more than 90 Thirdly, we utilize UWB multipath characteristics for security key generation and prove that both RSS-based and TOA-based schemes perform precise BMR. CRLB of these two schemes are derived to further validate experiment.

As one of booming research field, there are much more IoT related problems remain unsolved. I wish this dissertation can serve as an inspiration to other researchers and encourage more devotion to the area.

Bibliography

[1] Pahlavan, Kaveh, Xinrong Li, and J-P. Makela. "Indoor geolocation science and technology." Communications Magazine, IEEE 40.2 (2002): 112-118.

[2] Jiang J A, Zheng X Y, Chen Y F, et al. A distributed RSS-based localization using a dynamic circle expanding mechanism[J]. IEEE Sensors Journal, 2013, 13(10): 3754-3766.

[3] Catarinucci L, De Donno D, Mainetti L, et al. An IoT-aware architecture for smart healthcare systems[J]. IEEE Internet of Things Journal, 2015, 2(6): 515-526.

[4] Rusli M E, Ali M, Jamil N, et al. An improved indoor positioning algorithm based on rssi-trilateration technique for internet of things (iot)[C]//2016 International Conference on Computer and Communication Engineering (ICCCE). IEEE, 2016: 72-77.

[5] He J, Geng Y, Pahlavan K. Toward Accurate Human Tracking: Modeling Time-of-Arrival for Wireless Wearable Sensors in Multipath Environment[J]. Sensors Journal, IEEE, 2014, 14(11): 3996-4006.

[6] He J, Geng Y, Liu F, et al. CC-KF: Enhanced TOA Performance in Multipath and NLOS Indoor Extreme Environment[J]. Sensors Journal, IEEE, 2014, 14(11): 3766-3774.

[7] Iadanza E, Dori F, Miniati R, et al. Patients tracking and identifying inside hospital: A multilayer method to plan an RFId solution[C]//Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE. IEEE, 2008: 1462-1465.

[8] Liu G, Geng Y, Pahlavan K. Effects of calibration RFID tags on performance of inertial navigation in indoor environment[C]//Computing, Networking and Communications (ICNC), 2015 International Conference on. IEEE, 2015: 945-949.

[9] Pahlavan K, Krishnamurthy P, Geng Y. Localization Challenges for the Emergence of the Smart World[J].

[10] Alemdar H, Ersoy C. Wireless sensor networks for healthcare: A survey[J]. Computer Networks, 2010, 54(15): 2688-2710.

[11] Li Z, Yang Y, Pahlavan K. Using iBeacon for In-Room Newborns Localization in Hospital//International Symposium on Medical Information and Communication Technology (ISMICT'16).

[12] Wang Y, Fu R, Ye Y, et al. Performance bounds for RF positioning of endoscopy camera capsules[C]//Biomedical Wireless Technologies, Networks, and Sensing Systems (BioWireleSS), 2011 IEEE Topical Conference on. IEEE, 2011: 71-74.

[13] Pahlavan K, Levesque A H. Wireless information networks[M]. John Wiley & Sons, 2005.

[14] Amendola S, Lodato R, Manzari S, et al. RFID technology for IoT-based personal healthcare in smart spaces[J]. IEEE Internet of things journal, 2014, 1(2): 144-152.

[15] Manaffam S, Jabalameli A. RF-localize: An RFID-based localization algorithm for Internet-of-Things[C]//2016 Annual IEEE Systems Conference (SysCon). IEEE, 2016: 1-5.

[16] Geng Y, Pahlavan K. Design, Implementation and Fundamental Limits of Image and RF Based Wireless Capsule Endoscopy Hybrid Localization[J]. 2015.

[17] Chen Y, Kobayashi H. Signal strength based indoor geolocation[C]//Communications, 2002. ICC 2002. IEEE International Conference on. IEEE, 2002, 1: 436-439.

[18] McAllister T D, El-Tawab S, Heydari M H. Localization of health center assets through an iot environment (locate)[C]//2017 Systems and Information Engineering Design Symposium (SIEDS). IEEE, 2017: 132-137.

[19] Julang Ying, Chao Ren and Kaveh Pahlavan, On Automated Map Selection Problem in Indoor Navigation for Smart Devices, The Workshop of IEEE 2015 Wireless Telecommunications Symposium (WTS), New York City, USA, April 15-17, 2015.

[20] Shit R C, Sharma S, Puthal D, et al. Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure[J]. IEEE Communications Surveys & Tutorials, 2018, 20(3): 2028-2061.

[21] Li S, Geng Y, He J, et al. Analysis of three-dimensional maximum likelihood algorithm for capsule endoscopy localization[C]//Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on. IEEE, 2012: 721-725.

[22] Pahlavan, K., 1985. Wireless communications for office information networks. IEEE Communications Magazine, 23(6), pp.19-27.

[23] Pahlavan, K., 1988. Wireless intra-office networks. ACM Transactions on Information Systems (TOIS), 6(3), pp.277-302.

[24] Berk-Tek, A NEXANS Company. "Basic Human Needs: Food, shelter, and-Wireless??" Aug 15th, 2017 https://eipblog.net/2017/08/15/basic-human-needs-food-shelter-andwireless/

[25] Pace Technical. "Is Fast WiFi the Most Basic of Human Needs?" https://www.pacetechnical.com/fast-wifi-basic-human-needs/

[26] Siep, T.M., Gifford, I.C., Braley, R.C. and Heile, R.F., 2000. Paving the way for personal area network standards: an overview of the IEEE P802. 15 Working Group for Wireless Personal Area Networks. IEEE Personal Communications, 7(1), pp.37-43.

[27] Weinstein, R., 2005. RFID: a technical overview and its application to the enterprise. IT professional, 7(3), pp.27-33.

[28] Iovescu, C. and Rao, S., 2017. The fundamentals of millimeter wave sensors. Texas Instruments.

[29] Banerjee, A., Chakraborty, C., Kumar, A. and Biswas, D., 2020. Emerging trends in IoT and big data analytics for biomedical and health care technologies. In Handbook of Data Science Approaches for Biomedical Engineering (pp. 121-152). Academic Press.

[30] Pahlavan, K., Akgul, F., Ye, Y., Morgan, T., Alizadeh-Shabodz, F., Heidari, M. and Steger, C., 2010. Taking positioning indoors. Wi-Fi localization and GNSS. Inside GNSS (May 2010).

[31] Pahlavan, K., 2019. Indoor Geolocation Science and Technology. River Publishers.

[32] Pahlavan, K. and Levesque, A.H., 2005. Wireless information networks (Vol. 93). John Wiley & Sons.

[33] Ruiz, A.R.J. and Granja, F.S., 2017. Comparing ubisense, bespoon, and decawave uwb location systems: Indoor performance analysis. IEEE Transactions on instrumentation and Measurement, 66(8), pp.2106-2117.

[34] Halperin, D., Hu, W., Sheth, A. and Wetherall, D., 2011. Tool release: Gathering 802.11 n traces with channel state information. ACM SIGCOMM Computer Communication Review, 41(1), pp.53-53.

[35] Pahlavan, K., Krishnamurthy, P. and Beneat, A., 1998. Wideband radio propagation modeling for indoor geolocation applications. IEEE Communications Magazine, 36(4), pp.60-65.

[36] Pahlavan, K., Li, X. and Makela, J.P., 2002. Indoor geolocation science and technology. IEEE Communications Magazine, 40(2), pp.112-118.

[37] X. Li and K. Pahlavan, M. Latva-aho, and M. Ylianttila, "Indoor Geolocation using OFDM Signals in HIPERLAN/2 Wireless LANs", IEEE PIMRC'2000, London, Sep. 2000.

[38] Bahl, P., Padmanabhan, V.N., Bahl, V. and Padmanabhan, V., 2000. RADAR: An in-building RF-based user location and tracking system.

[39] Ye, Y., Akgul, F.O., Bardshady, N. and Pahlavan, K., 2011, April. Performance of hybrid WiFi localization for cooperative robotics applications. In IEEE

International Conference on Technologies for Practical Robot Applications (pp. 11-12).

[40] Bargshady, N., Pahlavan, K. and Alsindi, N.A., 2015, February. Hybrid WiFi/UWB, cooperative localization using particle filter. In 2015 International Conference on Computing, Networking and Communications (ICNC) (pp. 1055-1060). IEEE.

[41] Bargshady, N., Garza, G. and Pahlavan, K., 2016. Precise tracking of things via hybrid 3-D fingerprint database and kernel method particle filter. IEEE Sensors Journal, 16(24), pp.8963-8971.

[42] Ying, J., Pahlavan, K. and Li, X., 2017, October. Precision of RSS-based indoor geolocation in IoT applications. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-5). IEEE.

[43] Ying, J. and Pahlavan, K., 2019. Precision of RSS-based localization in the IoT. International Journal of Wireless Information Networks, 26(1), pp.10-23.

[44] F. Akgul, K. Pahlavan, Location Awareness for Everyday Smart Computing, ICT'09, Marrakech, Morocco, May 2009.

[45] Mia, R.S. and Anderson, R.J., Skyhook Holding Inc, 2012. Sparsed U-TDOA wireless location networks. U.S. Patent 8,242,959.

[46] Pahlavan, K., Akgul, F.O., Heidari, M., Hatami, A., Elwell, J.M. and Tingley, R.D., 2006. Indoor geolocation in the absence of direct path. IEEE Wireless Communications, 13(6), pp.50-58.

[47] Yang, Y., Li, Z. and Pahlavan, K., 2016, March. Using iBeacon for intelligent in-room presence detection. In 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA) (pp. 187-191). IEEE.

[48] Li, Z., Yang, Y. and Pahlavan, K., 2016, March. Using iBeacon for newborns localization in hospitals. In 2016 10th International Symposium on Medical Information and Communication Technology (ISMICT) (pp. 1-5). IEEE.

[49] Fu, R., Ye, Y., Yang, N. and Pahlavan, K., 2011, September. Doppler spread analysis of human motions for body area network applications. In 2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications (pp. 2209-2213). IEEE.

[50] Geng, Y., Chen, J., Fu, R., Bao, G. and Pahlavan, K., 2015. Enlighten wearable physiological monitoring systems: On-body rf characteristics based human motion classification using a support vector machine. IEEE transactions on mobile computing, 15(3), pp.656-671.

[51] Dong, Z., Li, F., Ying, J. and Pahlavan, K., 2018. Indoor motion detection using Wi-Fi channel state information in flat floor environments versus in staircase environments. Sensors, 18(7), p.2177.

[52] Li, Z., Lei, Z., Yan, A., Solovey, E. and Pahlavan, K., ThuMouse: A Micro-gesture Cursor Input through mmWave Radar-based Interaction. In 2020 Proceedings of IEEE International Conference on Consumer Electronics (ICCE), Los Vegas, NV, Jan 4-6, 2020

[53] Pu, Q., Jiang, S. and Gollakota, S., 2013, August. Whole-home gesture recognition using wireless signals (demo). In Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM.

[54] Ali, K., Liu, A.X., Wang, W. and Shahzad, M., 2015, September. Keystroke recognition using wifi signals. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (pp. 90-102). ACM.

[55] Zhao, M., Li, T., Abu Alsheikh, M., Tian, Y., Zhao, H., Torralba, A. and Katabi, D., 2018. Through-wall human pose estimation using radio signals. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 7356-7365).

[56] Kotaru, M. and Katti, S., 2017. Position tracking for virtual reality using commodity wifi. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 68-78).

[57] Lien, J., Olson, E.M., Amihood, P.M. and Poupyrev, I., Leland Stanford Junior University and Google LLC, 2019. RF-based micro-motion tracking for gesture tracking and recognition. U.S. Patent Application 10/241,581.

[58] Moore, S.T., MacDougall, H.G., Gracies, J.M., Cohen, H.S. and Ondo, W.G., 2007. Long-term monitoring of gait in Parkinson's disease. Gait & posture, 26(2), pp.200-207.

[59] Abujrida, H., Agu, E. and Pahlavan, K., 2017, November. Smartphone-based gait assessment to infer Parkinson's disease severity using crowdsourced data. In 2017 IEEE Healthcare Innovations and Point of Care Technologies (HI-POCT) (pp. 208-211). IEEE.

[60] Zheng, Y., Zang, Y. and Pahlavan, K., 2016, January. UWB localization modeling for electronic gaming. In 2016 IEEE international conference on consumer electronics (ICCE) (pp. 170-173). IEEE.

[61] Zang, Y., Pahlavan, K., Zheng, Y. and Wang, L., 2016, March. UWB gesture detection for visually impaired remote control. In 2016 10th International Symposium on Medical Information and Communication Technology (ISMICT) (pp. 1-4). IEEE.

[62] Zhao, C., Chen, K.Y., Aumi, M.T.I., Patel, S. and Reynolds, M.S., 2014, October. SideSwipe: detecting in-air gestures around mobile devices using actual GSM signal. In Proceedings of the 27th annual ACM symposium on User interface software and technology (pp. 527-534).

[63] Lien, J., Gillian, N., Karagozler, M.E., Amihood, P., Schwesig, C., Olson, E., Raja, H. and Poupyrev, I., 2016. Soli: Ubiquitous gesture sensing with millimeter wave radar. ACM Transactions on Graphics (TOG), 35(4), pp.1-19.

[64] Smith, K. A., Csech, C., Murdoch, D. and Shaker, G., 2018. Gesture recognition using mm-wave sensor for human-car interface. IEEE sensors letters, 2(2), pp.1-4.

[65] Yeo, H.S., Flamich, G., Schrempf, P., Harris-Birtill, D. and Quigley, A., 2016, October. Radarcat: Radar categorization for input & interaction. In Proceedings of the 29th Annual Symposium on User Interface Software and Technology (pp. 833-841).

[66] Hsu, C.Y., Liu, Y., Kabelac, Z., Hristov, R., Katabi, D. and Liu, C., 2017, May. Extracting gait velocity and stride length from surrounding radio signals. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 2116-2126).

[67] Qian, K., Wu, C., Zhou, Z., Zheng, Y., Yang, Z. and Liu, Y., 2017, May. Inferring motion direction using commodity wi-fi for interactive exergames. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 1961-1972).

[68] Ma, Y., Zhou, G., Wang, S., Zhao, H. and Jung, W., 2018. Signfi: Sign language recognition using wifi. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(1), pp.1-21.

[69] Tan, S., Zhang, L., Wang, Z. and Yang, J., 2019, May. MultiTrack: Multi-user tracking and activity recognition using commodity WiFi. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-12)..

[70] Zhao, K. and Ge, L., 2013, December. A survey on the internet of things security. In 2013 Ninth international conference on computational intelligence and security (pp. 663-667). IEEE.

[71] Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K. and Shieh, S., 2014, November. IoT security: ongoing challenges and research opportunities. In 2014 IEEE 7th international conference on service-oriented computing and applications (pp. 230-234). IEEE.

[72] Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A.R. and Tarkoma, S., 2017, June. Iot sentinel: Automated device-type identification for security enforcement in iot. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (pp. 2177-2184). IEEE.

[73] Ali, B. and Awad, A.I., 2018. Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors, 18(3), p.817.

[74] Chatterjee, B., Das, D., Maity, S. and Sen, S., 2018. RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. IEEE Internet of Things Journal, 6(1), pp.388-398.

[75] Di Domenico, S., Pecoraro, G., Cianca, E. and De Sanctis, M., 2016, October. Trained-once device-free crowd counting and occupancy estimation using WiFi: A Doppler spectrum based approach. In 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 1-8). IEEE.

[76] Zhang, Z., Guo, X. and Lin, Y., 2018. Trust management method of D2D communication based on RF fingerprint identification. IEEE Access, 6, pp.66082-66087

[77] Ureten, O. and Serinken, N., 2007. Wireless security through RF fingerprinting. Canadian Journal of Electrical and Computer Engineering, 32(1), pp.27-33.

[78] Patel, H.J., Temple, M.A. and Baldwin, R.O., 2014. Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting. IEEE Transactions on Reliability, 64(1), pp.221-233.

[79] Peng, L., Hu, A., Zhang, J., Jiang, Y., Yu, J. and Yan, Y., 2018. Design of a hybrid RF fingerprint extraction and device classification scheme. IEEE Internet of Things Journal, 6(1), pp.349-360.

[80] Williams, M.D., Temple, M.A. and Reising, D.R., 2010, December. Augmenting bit-level network security using physical layer RF-DNA fingerprinting. In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010 (pp. 1-6). IEEE.

[81] Wang, S., Song, J., Lien, J., Poupyrev, I. and Hilliges, O., 2016, October. Interacting with soli: Exploring fine-grained dynamic gesture recognition in the radio-frequency spectrum. In Proceedings of the 29th Annual Symposium on User Interface Software and Technology (pp. 851-860).

[82] Rehman, S.U., Sowerby, K.W. and Coghill, C., 2014. Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers. Journal of Computer and System Sciences, 80(3), pp.591-601.

[83] Dabbagh, Y.S. and Saad, W., 2019. Authentication of wireless devices in the Internet of Things: learning and environmental effects. IEEE Internet of Things Journal, 6(4), pp.6692-6705.