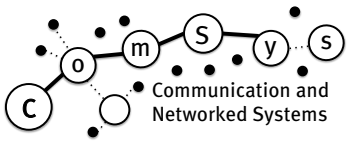
FACULTY OF
COMPUTER SCIENCE



Communication and Networked Systems

Master Thesis

Received Signal Strength Based Indoor Positioning Using Bluetooth Low Energy

Mansour Abboud

Betreuer: Prof. Dr. rer. nat. Mesut Güneş
Betreuender Assistent: M. Sc. Ali Nikoukar

Institut für Intelligente Kooperierende System, Otto-von-Guericke-Universität Magdeburg

March 2, 2018

Acknowledgements

First I would like to take the opportunity to thank my advisor Ali Nikoukar for introducing me to the research area and for his extreme support and guidance in this work.

I would like also to express my deepest gratitude to my parents for their encouragement and support all the time.

Finally, a big thank to everyone not mentioned by name who has ever helped in this work.

Contents

List of Figures

List of Tables

Source Code

Acronyms

ACK Acknowledgement. 5, 37, 42

ADV Advertisement. 1, 3–6, 18, 24–27, 29–33, 38, 47, 48, 52, 53, 61

AFH Adaptive Frequency Hopping. 42

AoA Angle of Arrival. 10

AP Access Point. 16, 19, 29, 35, 36

APs Access Points. 8, 16

ATT Attribute Protocol. 21

BC Bluetooth Classic. 17–19

BLE Bluetooth Low Energy. 1, 3–9, 18–20, 22–33, 35–38, 42, 43, 46–48, 52, 61

BR Basic Rate. 17

CRC Cycle Redundancy Check. 22–24, 44, 45

EDR Enhanced Data Rate. 17

GAP Generic Access Profile. 22

GATT Generic Attribute Profile. 21

GFSK Gaussian Frequency Shift Keying. 27, 42

GPS Global Positioning System. 3, 7

HCI Host Controller Interface. 22

HS High Speed. 17

IEEE Institute of Electrical and Electronic Engineers. 16, 17, 23, 28

IoT Internet of Things. 1, 3, 6, 8, 10, 15, 16, 18, 19, 32

IPS Indoor Positioning System. 3, 5, 8, 18, 29

IPSs Indoor Positioning Systems. 8

ISM Industrial, Scientific, and Medical. 5, 16

L-NDM Log-Normal Distance Model. 1, 14, 28, 29

L-NSM Log-Normal Shadowing Model. 1, 4, 5, 15, 28, 29, 32–34, 56, 61

L2CAP Logical Link Control and Adaptation Protocol. 21

LE Low Energy. 23, 27, 28

LL Link Layer. 6, 22–24, 26, 35, 36, 38, 42, 44

LOS Line-of-Sight. 10, 16, 35, 36, 39

LS Least Square. 29

LSE Least Square Estimation. 9

MCU Microcontroller Unit. 21, 36

NFC Near Field Communication. 15

NLOS Non-Line-of-Sight. 14

PCNF0 Packet Configuration. 43, 45

PCNF1 Packet Configuration. 43, 45, 46

PDU Protocol Data Unit. 23–26, 39, 43

PER Packet Error Rate. 33, 37

PHY Physical layer. 1, 22, 27, 28, 43

PLE Path Loss Exponent. 29

PLEN Preamble Length. 43

RF Radio Frequency. 17, 23, 33

RSS Received Signal Strength. 1, 3–5, 8, 9, 11–18, 28–33, 37, 38, 40, 47, 52, 53, 57, 60, 61

RSSI Received Signal Strength Indicator. 8, 11, 28, 30

RToF Return Time of Flight. 12

SIG Bluetooth Special Interest Group. 17, 18, 21

SMP Security Manager Protocol. 21

SoC System on Chip. 42

TDoA Time Difference of Arrival. 28, 29

ToA Time of Arrival. 11, 12

ToF Time of Flight. 3, 4, 9, 11, 12

TRM Two-Ray Model. 14

TRRLS Trust Region Reflective Least Squares. 33, 53

UART Universal Asynchronous Receiver-Transmitter. 22, 41

WLAN Wireless Local Area Network. 16

WSN Wireless Sensor Networks. 17, 28

Abstract

The idea behind the Internet of Things (IoT) is to connect every object to the Internet. According to Gartner, the number of IoT devices will reach up to 20.4 billion by 2020. However, the large number of connections is only feasible with the help of wireless technologies. Bluetooth Low Energy (BLE) is a widely-used wireless technology in the IoT domain. The Physical layer (PHY) of this standard has been redesigned resulting in two types of channels. Namely: Advertisement (ADV) and data channels. ADV channels are responsible for devices discovery, connection initiation and information broadcast. Data channels are used only to exchange information during connections. In 2013, Apple introduces iBeacon which operates on these ADV channels. Beacon broadcast enabled new areas of applications such as product advertisement, medical monitoring, and indoor positioning. Among these mentioned applications, indoor positioning is the one receiving a considerable attention. BLE based indoor positioning relies on Received Signal Strength (RSS) technique for point-to-point distance estimation. This technique requires a path loss model to estimate the distance based on the received power. The Log-Normal Distance Model (L-NDM) is a general path loss model for every environment. However, this model has been improved to consider the multipath fading effects in indoor environments, and the result is the Log-Normal Shadowing Model (L-NSM). Yet, the later lacks generalization for every environment and frequency. There exist a considerable research of path loss characterization on Wi-Fi and ZigBee but to the best of our knowledge, an extensive study on BLE ADV channels is missed.

This thesis addresses this research gap through conducting experiments in various conditions such as different indoor and outdoor environments, different transmit power settings, background noise and antenna orientation. Path loss models based on the results of this research can be directly used for range estimation and simulation tools for modeling BLE ADV channels. The obtained results show the complexity of indoor environments and their considerable impact on RSS due to multipath fading and interference with other presented devices. The comparison of outdoor and indoor results highlights this claim.

CHAPTER 1

Introduction

1.1 Background

The idea behind the Internet of Things (IoT) [1] is to connect every object to the Internet. According to Gartner [2], the IoT domain will reach up to 20.4 billion devices by 2020. This includes domains such as industrial 4.0, smart cities, home automation, healthcare, logistics, etc [3]. This large number of connections is only feasible with the help of wireless technologies. To fulfill the requirements of IoT connectivity, the desired technology needs to be low-power, available, inexpensive, reliable, and provide mechanisms to support interference [4]. To this end, Bluetooth Low Energy (BLE) [5] is a widely-adopted wireless technology that satisfies most of the IoT requirements. In addition to the low-power consumption, this technology provides a set of three Advertisement (ADV) channels, which are primarily used for device discovery, connection initiation and information broadcast. In 2013, Apple introduces iBeacon [6] which operates on the ADV channels. Beacon broadcast over these channels enables a set of applications such as indoor positioning, product advertisement, and medical monitoring [7]. Nowadays, indoor positioning is one of the major applications of BLE beacons. It is reported that 75% of top US retailers have already deployed BLE beacons in their locations, and 84% of international airports will by 2019 [8]. Additionally, the global market for indoor positioning service in 2016 was $5.22 billion and it is expected to grow up to $40.99 billion by 2022 with an annual growth rate of 42.0% [9].

The concept of indoor positioning is similar to the Global Positioning System (GPS) [10]. The basic step is point-to-point distance estimation. Commonly, there are two techniques for distance estimation: Time of Flight (ToF) and Received Signal Strength (RSS) [11] (refer to Ch 2). Time of Flight (ToF) is based on the time taken by a signal to travel over the air from one node to another. This technique provides a reliable accuracy but however, taking into consideration that radio waves travel at the speed of light, devices relying on ToF for positioning require a highly precise clock system to deal with such tight timing. Additionally, the clocks of nodes have to be strictly synchronized in order to obtain the exact travel time [12]. These mentioned problems increase the hardware design cost and the complexity of the ToF based Indoor Positioning System (IPS). RSS is based on signal path loss characteristics where the received power can be modeled as a function of

distance [13]. The advantage of RSS is the simplicity and low cost since most of wireless devices can easily obtain the RSS parameter. Therefore, RSS is widely preferred over ToF and particularly in BLE beacon positioning. However, the simplicity and cost-effectiveness of this technique has the disadvantage of lower accuracy and reliability. The major problem of RSS is signal fluctuation due to several factors such as multipath and interference with other devices [14] which results in errors in distance estimation. In theory, the signal power decays with the square of distance according to the free space path loss model [15] while in obstructed environments, the signal power fluctuates due the above mentioned factors. This behaviour can be seen in Fig. 1.1 where the line curve demonstrate the theoretical loss of signal power with respect to distance, and the doted curve represents the actual RSS.

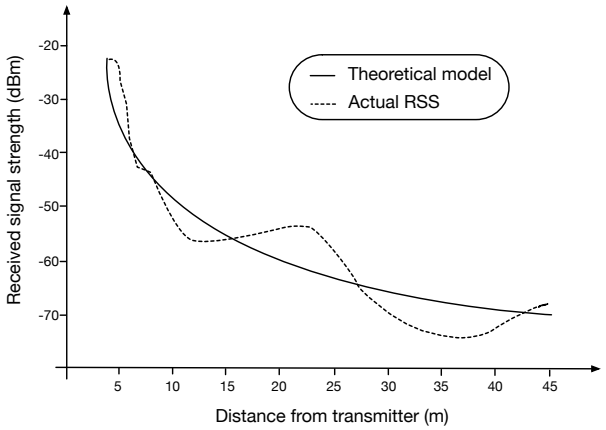


Fig. 1.1: The relationship between received power and distance

1.2 Problem Statement

As mentioned earlier, BLE based indoor positioning relies on RSS technique for point-to-point distance estimation. The challenging issue is that RSS is highly dependant on how well the signal propagates in the wireless channel. Obstacles such as walls, interference with other devices and even the motion of people cause signal fluctuation which results in errors in distance measurement. Therefore, it is essential to characterize the wireless channel to improve the reliability of the this technique in BLE based positioning. The Log-Normal Shadowing Model (L-NSM) [16] is inherited from the free space path loss model, and researchers claim that it provides a relatively accurate distance estimation in the presence of multipath effects. However, this is highly dependant on the input parameters that play the key role in the reliability of this model (refer to Ch 2). Based on this fact, the input parameters have to be estimated and optimized. This is achievable empirically since these parameters are environment dependant. In this thesis, we characterize the signal propagation of BLE ADV channels in different environments. Additionally, we optimize the input parameters of the L-NSM in order to improve its reliability in range estimation.

1.3 Research Objectives

1. To analyze the characteristics of BLE ADV channels in different environments.
2. To develop a testbed for BLE RSS based distance estimation.
3. To optimize the L-NSM parameters for BLE based indoor positioning.

1.4 Scope of the Study

In the field of indoor positioning, few technical parameters are important [17]. These parameters are shown in Fig. 1.2. The highlighted ones are the parameters that have been considered in this research.

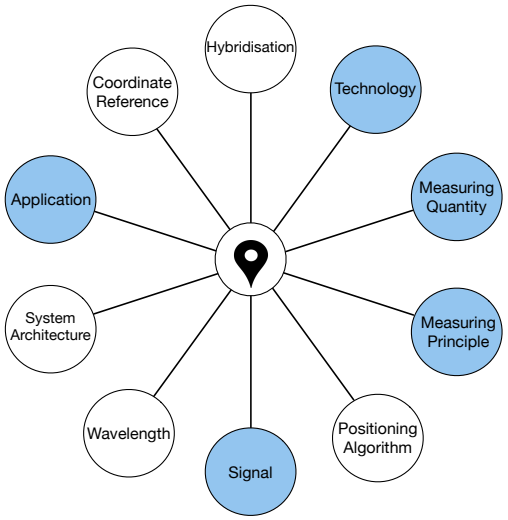


Fig. 1.2: IPS key technical parameters

This research focuses on using BLE technology which operates in the license free 2.4 GHz Industrial, Scientific, and Medical (ISM) band. This technology has been selected due to its low-power consumption and beaconing feature in addition to the wide availability in many devices. The research has been experimentally implemented in four different environments. These environments can be categorized into indoor and outdoor (refer to Section 4.2). The indoor environments are a classroom hall and a corridor located inside the faculty of Informatics at Otto von Guericke University Magdeburg. Outdoor environments are two open fields which are Nordpark and Stadtpark that are located in the city of Magdeburg, Germany. The experiments were conducted as point-to-point transmission between a transmitter and a receiver where the later only receives packets without replying Acknowledgement (ACK). The aim of this transmission is to analyze the signal behavior in addition to the effect of antenna direction on RSS. The selected transmission channels are based on BLE ADV channels (2402, 2426 and 2480 MHz). Additionally different transmission powers have been considered in order to improve the reliability of the experiments. Furthermore, two different BLE devices have been selected based on the comparison done in Table 4.1. For

programming these devices, embedded C programming language has been used through the integrated development environments Keil MDK-ARM and Code Composer Studio. Moreover, two BLE software stacks provided by Nordic and Texas Instruments have been used. The Link Layer (LL) of BLE has been implemented on Nordic devices in order to solve: 1) few limitations presented by the BLE standard such as the inability to scan on a specific advertising channel. (2 issues in timers synchronization encountered while using the software stack provided by Nordic. Finally, the results of the research are plotted using Python matplotlib.

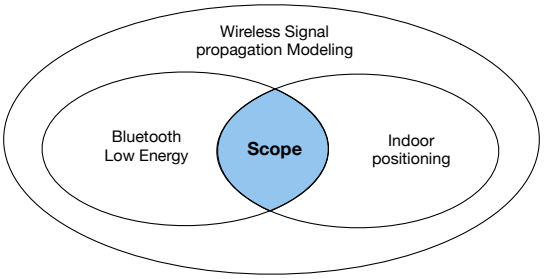


Fig. 1.3: Scope of the study

1.5 Significance of the Study

Indoor positioning is critical in many application domains. This includes industry, location-based services, smart cities, healthcare, etc [17]. For example, it is important to track patients at hospitals and monitor their health conditions. There are many wireless technologies involved in indoor positioning. BLE is an emerging low-power wireless technology that is widely available in most of smart-phones and IoT devices. It supports the beaconing feature which has a significant contribution in the field of indoor positioning. Unfortunately, there is a lack of study on BLE ADV channels and a specific path loss model for range estimation. Moreover, there is also a need for a reliable path loss model in simulation environments in order for researchers to implement their ideas without the need of real hardware deployment [16]. Therefore, the results of this research can help in improving simulation studies. Additionally, the outcome of this study helps in a better understanding of the characteristics of each factor that affects on the signal behavior and causes fluctuations.

1.6 Thesis Outlines

The rest of the thesis is organized as follows. Chapter 2 provide an overview of wireless communications, indoor positioning methods and applications. BLE technology in addition to the related works. Chapter 3 describes the methodology and the steps that have been taken to achieve the defined objectives. Chapter 4 presents the software and hardware implementation steps. Chapter 5 demonstrates the collected datasets, results and discussion. Finally, Chapter 6 presents the summary and conclusion in addition to the future work.

CHAPTER 2

Literature Review

2.1 Introduction

This chapter provides the basic concepts of the related topics to this research. First, Section 2.2 starts with an overview of wireless communications. Then Section 2.3 presents the importance of indoor positioning and its applications. Section 2.4 describes the commonly used methods and techniques in the context of indoor positioning as well as the characteristics of signal propagation and channel modeling. An overview of the commonly used wireless technologies for indoor positioning is present in Section 2.5. Additionally, BLE technology which has been used in this research is explained in Section 2.6. Finally, Section 2.7 discusses the related work that has been done in this area of research.

2.2 Introduction to wireless communication

Wireless communications differ from wired ones in which they rely on radio channels instead of cables in order to exchange information [15]. They have become a critical component in daily life as they provide several advantages over wired communications. Wiring is costly to install and replace specially in large infrastructures. Besides, in harsh environments such as jungles or mountains, it is difficult to provide a cable connection. Moreover, mobility is an important aspect and it is almost impossible with cables. For example, tracking humans, animals or moving objects is only feasible with wireless communications. Therefore, by removing the limitations of wires, researchers were able to introduce new applications such as GPS and satellite communications. These advantages usually make wireless communications more prefered over wired ones but however, the wireless communication is complex and has some drawbacks particularly in the context of indoor positioning. This is because radio propagation is unreliable and the behaviour of wireless channels differs from one environment to another. For instance, a communication in free space is different than a communication inside buildings where obstacles such as walls are present. Obstructed environments causes the power on wireless channels to fluctuate up and down which may lead to a bad received signal. Furthermore, the signal loses its power as it travels over long distances. However, increasing transmission power means more energy consumption partic-

ularly for IoT devices. In other words, there are many factors that affect the behaviour of wireless channels which in turn affects the received signal quality such as multipath fading which is explained in 2.4. Therefore, for some use cases of wireless communications such as indoor positioning, it is important to model the behaviour of the wireless channel in order to represent the impact of these factors.

2.3 Applications of Indoor Positioning

Indoor positioning is critical in many application domains. For example, it is important to track patients in hospitals and monitor their health conditions. Other domains include industry, location-based services, disaster recovery, smart cities, logistics, etc [17]. One of the earliest Indoor Positioning Systems (IPSs) is the RADAR system [18] which was developed by Microsoft research group. The system utilizes existing Wi-Fi Access Points (APs) inside buildings to determine the position of a user. It is based on RSS technique and provides an accuracy between 2 to 3 meters. Another Wi-Fi IPS is the COMPASS system [19]. It also utilizes Wi-Fi APs and digital compasses to locate users inside buildings based on RSS. Moreover, a use case of Wi-Fi indoor positioning is described in [20] where the proposed system is developed for tracking the locations of labor and resources at construction sites.

Indoor positioning with BLE technology has recently gained a significant attention. One of the first BLE contributors in the context of indoor positioning is Apple's iBeacon [6]. iBeacon is the name of Apple's technology which started in 2013. This technology was mainly developed for proximity detection and interaction activities such as location-based services [7] at retail stores, museums and airports. An iBeacon broadcasts messages with a fixed format in one-way communication. Receivers of these messages uses the Received Signal Strength Indicator (RSSI) to estimate their location from the iBeacon. Furthermore, iBeacon technology is not designed to provide a precise positioning. Rather, it defines a relative position estimation within ranges. These ranges are immediate, near, far or unknown. However, deploying several iBeacons can enhance the accuracy of positioning. Additionally, any BLE enabled device can be an iBeacon but this requires obtaining a licence from Apple. An example of commercial beacon product is Estimote [21] that is also based on the iBeacon standard and developed for indoor positioning and interaction applications.

BLE beacons have several uses cases. For example, [22] utilized iBeacons for indoor positioning at hospitals in order to help patients finding their directions and offer them useful information such as the number of patients on the waiting list and the expected waiting time. Their proposed system pointed out the feasibility of using BLE iBeacons for indoor positioning at hospitals and that the system can save time for patients and also save manpower and resources for the hospitals. Another use case in this direction is described in [23]. Moreover, [24] used iBeacons to develop an interaction system between visitors and collections at museums based on visitors location. With the use of this system, visitors can get navigation inside the museums and acquire more information about the collections found there using their smartphones. [25] proposed a system to intelligently control the power saving mode of computers and lights in an office. The system is based on BLE beacons and an application that can determine when a user enters or leaves the office, and then intelligently change the power saving mode of computers and lights in order to efficiently

reduce the power consumption. Also [26] evaluated the possibility of using iBeacons as a solution for the occupancy detection in buildings such as detecting the number of users in a room and gather information about their movements.

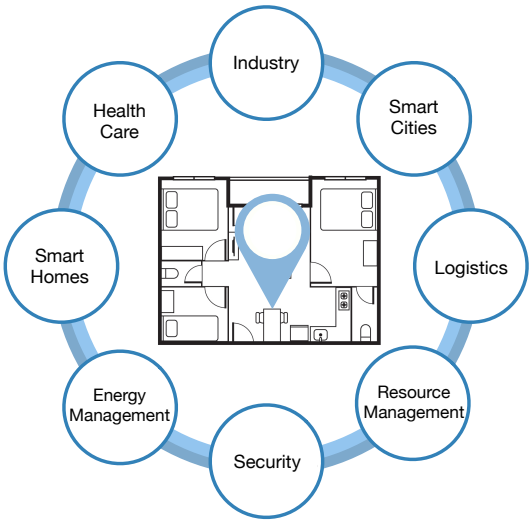


Fig. 2.1: Indoor positioning applications

2.4 Indoor Positioning Methods

Several methods can be used for estimating the position of an object in indoor environments. Trilateration, triangulation and fingerprinting [11] are the commonly used methods which are described below.

2.4.1 Trilateration

Trilateration [27] is a conventional and simple method for positioning using measured distances between a target object and at least three reference points. The reference points which can be three BLE beacons are usually fixed and their coordinates are known. The first step in trilateration is to measure the distances between the object and the reference points which can be done using techniques such as ToF and RSS (explained in the following sections). The second step is to determine the position of the target object using the measured distances. This can be done using mathematical models such as three-border positioning, Least Square Estimation (LSE) or centroid positioning which are discussed in [28]. An illustration of trilateration method is shown in Fig. 2.2. The centers of the three circles represent the reference points $P_1(x_1,\ y_1)$, $P_2(x_2,\ y_2)$ and $P_3(x_3,\ y_3)$. The radii of these circles r_1, r_2 and r_3 are the distances between the target object and the reference points, and the intersection of these circles denotes the position of the target object $T(x,\ y)$ which can be obtained using the three-border positioning Formula 2.1. Moreover, the accuracy of trilateration method is highly dependent on the first step since measuring distances is relatively difficult [29].

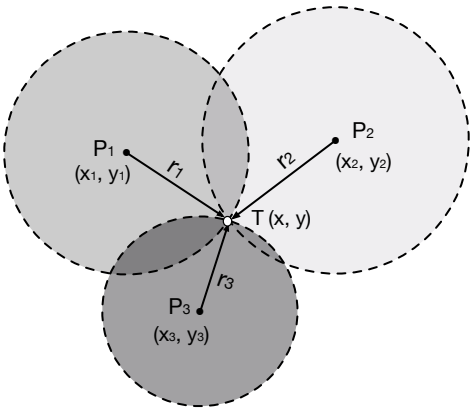


Fig. 2.2: Illustration of trilateration method

$$\begin{aligned}(x-x_1)^2+(y-y_1)^2 &= r_1^2\\ (x-x_2)^2+(y-y_2)^2 &= r_2^2\\ (x-x_3)^2+(y-y_3)^2 &= r_3^2\end{aligned} \tag{2.1}$$

2.4.2 Angulation

Angulation [29] is another method based on angular measurements. It utilizes signal Angle of Arrival (AoA) to determine the angels between the receivers and the source of the signal, here, the target object. This method requires directional antennas or antenna arrays in order to achieve that. Moreover, two reference points (receivers) at least with known coordinates are required to locate the target object. Angulation method is illustrated in Fig. 2.3. Two reference points $P1$ and $P2$ with known coordinates are located on the x-axis and separated by a distance D. The two angles α_1 and α_2 between the reference points and the target object, hence the transmitter T are measured up on receiving the signal from T. With the use of trigonometry, the coordinates of T then can be calculated using Formula 2.2. Angulation has a disadvantage in which devices require customizing their antennas to determine the AoA. Customizing the antennas is costly for IoT devices which are resource constrained. In addition, this method requires a Line-of-Sight (LOS) path between the target object and the reference points which is usually not possible in indoor environments. This makes angulation unviable for indoor positioning.

$$\begin{aligned}x &= \frac{Dtan(\alpha_2)}{tan(\alpha_2)-tan(\alpha_1)}\\ y &= \frac{Dtan(\alpha_1)tan(\alpha_2)}{tan(\alpha_2)-tan(\alpha_1)}\end{aligned} \tag{2.2}$$

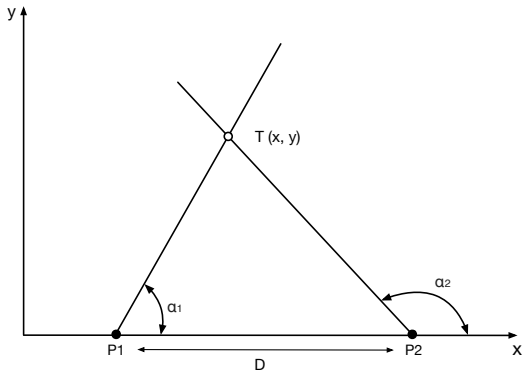


Fig. 2.3: Illustration of triangulation method [29]

2.4.3 Fingerprinting

Fingerprinting [30] is one of the most used methods for indoor positioning. It also RSS but however, not in the sense of path loss and channel modeling. This method divides the environment into multiple grids and uses a pre-recorded set of RSSI for each grid in order to determine the position of an object. Fingerprinting includes two phases [29]. The first phase is the calibration phase where a radio map is made to the whole environment by calibrating RSSI values for each grid and storing these values in a database. The second phase is the positioning phase were RSSI values are obtained in real-time from the target object, and are then compared to the database made in the calibration phase in order to determine the position. There are several approaches used to obtain the position based on the recorded database such as deterministic and probabilistic approaches which are discussed [31]. This method does not require distance measurement as the case with trilateration method and usually results in a good accuracy. Though, the drawback is that it requires a lot of efforts and time for building the radio map of the environment during the calibration phase which is difficult in case of large environments. Beside that, the database has to be large in order to improve the positioning accuracy. This increases the storage size, computational time and power consumption.

2.4.4 Distance Measurement Techniques

As mentioned earlier, positioning methods such as trilateration require in the first step measuring distances between the target object and the reference points. The commonly used techniques for measuring distances can be categorized into ToF and RSS which are discussed below.

Time of Flight (ToF)

ToF or Time of Arrival (ToA) [29] technique utilizes the propagation time of radio signals to calculate the distance between two points, saying, a transmitter and a receiver. Since radio signals travel at the speed of light, the distance can be calculated by multiplying the

speed with the travel time. The distance formula is given by

$$d = (t_a - t_t) * c \tag{2.3}$$

Where t_a is the signal arrival time, t_t is the transmit time and c is the speed of light ($3\ X\ 10^8$ m/s). Moreover, in order to calculate the travel time, the transmitter's and receiver's clocks have to be tightly synchronized [12]. Additionally, the signal must have a time-stamp in order for the receiver to know the exact transmit time. ToF technique usually result in a good distance estimation. However, it has a drawback in which it requires a highly precise clock system in order to deal with the tight signal timing which is costly for most of devices. Besides, an accurate synchronization algorithm is required as a tiny difference in time results in an error in distance measurement. Moreover, ToF accuracy depends also on the modulation schemes and data rates of the wireless system [29]. A variant of ToA is Return Time of Flight (RToF) [11]. RToF measures the time it takes for a signal to travel from the transmitter to the receiver and returns back again. RToF has an advantage in which only one device calculates the round trip time and synchronization between nodes is not required. However, the time that the receiver needs to process the signal and sends it back has to be reported to the transmitter. The distance formula of RToF is given by

$$d = \frac{(t_{a2} - t_{t1}) - (t_{t2} - t_{a1})}{2} * c \tag{2.4}$$

Where $(t_{a2} - t_{t1})$ is the signal round trip time, $(t_{t2} - t_{a1})$ is time taken by the receiver for processing the signal and sends it back, and c is the speed of light.

Received Signal Strength (RSS)

When a radio signal propagates, its loses some of its power as the distance between the transmitter and receiver increases. This relationship between signal power decay and distance is called path loss [32]. Moreover, modeling and characterization of this behavior allows point-to-point distance estimation. There are several path loss models for distance estimation. These models are described below.

Free Space Path Loss Model

The free space path loss model [15] is the simplest model. Since the the main focus of this thesis is on path loss modeling, it is appropriate to provide an explanation of how it is derived since other presented models in this chapter are inherited from it. According to [15], the relationship between the received and transmitted power in free-space for narrow-band signals is given by

$$\frac{P_r}{P_t} = G_r G_t \left(\frac{\lambda}{4\pi d}\right)^2 \tag{2.5}$$

Where P_r is the received power, P_t is the transmitted power, G_t is the transmitter antenna gain in Watt, G_r is the receiver antenna gain in Watt, d is the separation distance between

the transmitter and the receiver in meter, and λ is the signal wavelength. The author simplified this formula by defining $P_0 = P_t G_r G_t (\lambda/4\pi)^2$ as the average received power at a reference distance of 1 meter, which has to be obtained experimentally. Then Formula 2.5 is reduced to

$$P_r = \frac{P_0}{d^2} \tag{2.6}$$

This reveals that the received signal strength is proportional to the square of distance. By taking the logarithm base 10 of both sides in order to deal with decibel values, since RSS is usually measured in decibel, Formula 2.6 becomes

$$PL(d) = PL(d_0) + 20log_{10}\left(\frac{d}{d_0}\right) \tag{2.7}$$

Where $PL(d)$ is the path loss at distance d which is the distance between the transmitter and receiver, $PL(d_0)$ is the path loss at the reference distance d_0 which is typically 1 m for indoor and 100 m or 1 km for outdoor environments [13]. Applying this model in obstructed environments would lead to errors in distance measurement. This is because when a signal propagates in an obstructed environment where obstacles such as walls, equipments and furniture are present, it may get reflected, scattered or diffracted before it reaches the receiver [32]. Reflection, scattering and diffraction are known as propagation mechanisms. These mechanisms are explained in Fig. 2.4. Reflection happens when a signal hits a smooth object that is larger than the signal's wavelength such as large smooth walls. Scattering occurs when a signal hits an object that has irregular dimensions smaller than the signals' wavelength. This phenomena is similar to reflection but it differs from it in which the signal is split into several weaker signals. Diffraction happens when a signal hits an object that has sharp edges like the edges of houses and walls which leads to a change in signal direction.

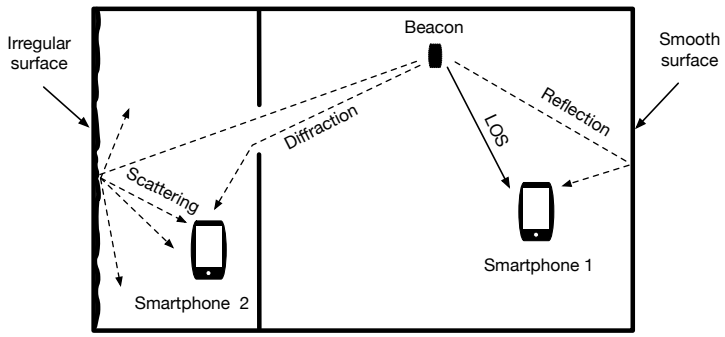


Fig. 2.4: Signal propagation mechanisms in the context of indoor positioning using beacons

As a result of such propagation mechanisms, the signal loses some of its strength before it reaches the receiver due to absorption by objects. Diffraction causes a small variation in signal which is known as shadowing, while scattering causes the signal to arrive at the receiver via multiple paths in which every path has a different delay and causes different

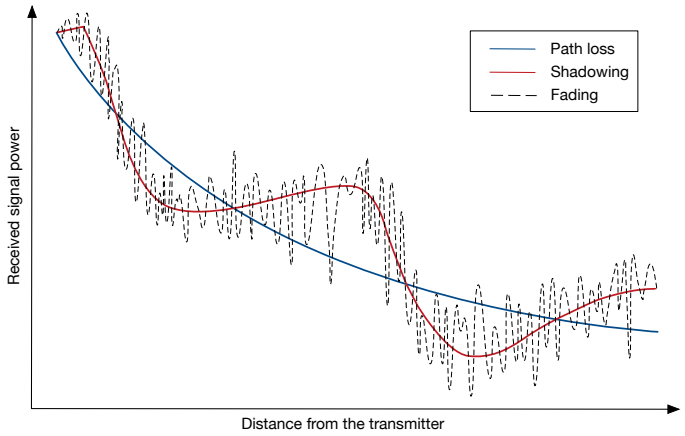


Fig. 2.5: Representation of the free-space path loss model versus the effects of shadowing and multipath fading [32]

signal attenuations. This is referred to as multipath fading [32] which is the major problem of RSS positioning particularly indoors. There are other factors that affect the RSS such as the motion of people in dynamic environments, Non-Line-of-Sight (NLOS) paths, background noise and humidity [14]. Moreover, signal variation due to shadowing and multipath fading can be categorized into large-scale and small-scale. Large-scale refers to the variation of signal due to multipath while small-scale refers to signal variation due to shadowing. An illustration of the free-space path loss versus the effects of shadowing and multipath fading is shown in Fig. 2.5. The first model that represents the reflection phenomena is the Two-Ray Model (TRM) [13]. This model is developed for open fields in order to take the ground reflection into consideration. As seen in Fig. 2.6, a transmitted signal arrives at the receiver from two paths, one is direct and the other is reflected by the ground leading to a multipath effects.

Log-Normal Distance Model (L-NDM)

The L-NDM [13] considers that signal path loss decay is not proportional to the square of distance. Rather, it depends on the properties of the environment and its obstacles which causes signal fluctuation. Therefore, Formula 2.6 is transferred into

$$P_r = \frac{P_0}{d^{\eta}} \tag{2.8}$$

Where η is the path loss exponent which indicates the change rate of path loss. By converting into decibel scale, Formula 2.8 becomes

$$PL(d) = PL(d_0) + 10\eta log_{10}\left(\frac{d}{d_0}\right) \tag{2.9}$$

This model represents the path loss as a function of distance where the value of η is envi-

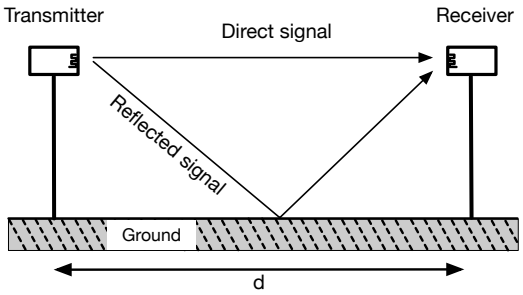


Fig. 2.6: Ground reflection in open fields

ronment dependant and is obtained for each channel through measurements. In free-space, η has a value of 2.

Log-Normal Shadowing Model (L-NSM)

It has been empirically shown that the path loss $PL(d)$ at any distance is random and log-normally distributed around the mean of the measured RSS due to shadowing and multipath effects [13]. Therefor, the L-NSM [16] is developed to characterize these effects. The formula of the L-NSM is giving by

$$PL(d) = PL(d_0) + 10\eta log_{10}\left(\frac{d}{d_0}\right) + N(0, \sigma_{ch}) \tag{2.10}$$

Where $N(0, \sigma_{ch})$ is a Guassian random variable with zero-mean and standard deviation σ_{ch}. The standard deviation represents the variation of signal due to multipath effects which can be obtained empirically.

2.5 Wireless Technologies for Indoor Positioning

Each application has a certain factor in priority list based on user's requirements. For example, Near Field Communication (NFC) technology [33] scarifies the coverage in order to achieve battery less connection. On the other hand, satellites need to cover the entire globe. The scope of this thesis is limited to indoor positioning with IoT devices which usually support Wi-Fi, ZigBee or Bluetooth connectivity with coverage only up to 100 meter. Therefore, high coverage is not required. Moreover, due to the large number of connected devices in the IoT domain, battery consumption has the priority. An overview of the typical data rates and coverage of some of the available wireless technologies is shown in Fig. 2.7.

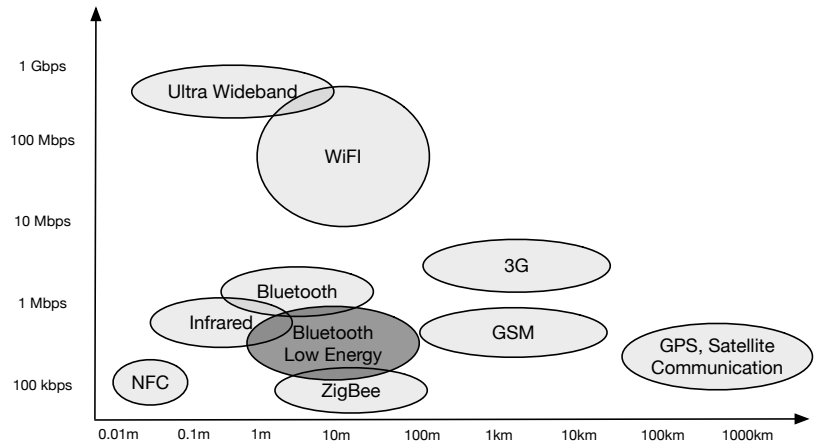


Fig. 2.7: Overview of typical data rates and coverage of some wireless technologies [5]

2.5.1 Wi-Fi

Wireless Local Area Network (WLAN) or commonly known as Wi-Fi [34] is a wireless technology introduced by the Institute of Electrical and Electronic Engineers (IEEE) [35]. The most well-known standards in Wi-Fi are IEEE 802.11b/g/n which operate in the license free 2.4 GHz ISM band. Wi-Fi technology is widely adopted in every smartphone and laptop. It has star based topology in which devices connect to a central Access Point (AP). Due to the availability of this technology in many indoor environments. It is considered one of the optimal candidates for indoor positioning applications. Therefore, researches tried to implement indoor positioning methods based on Wi-Fi. For example, [36] used Wi-Fi based on fingerprinting approach. Another study in [37] preformed RSS based positioning and aimed to increase the accuracy. However, Wi-Fi positioning has some disadvantages. Among these disadvantages is the power consumption which is an important aspect in this context. Wi-Fi power consumption is relatively high, and since most of IoT devices have battery power constraints, how to reduce the power consumption required for positioning remains a challenging issue. Another disadvantage is the interference. Wi-Fi channels might overlap and interfere with each other specially when the number of APs in an environment is increased. Below, a list of advantages and disadvantages of using Wi-Fi for indoor positioning is summarized [38].

Advantages

- Wildly adopted by many devices such as smartphones.
- Already deployed in most of indoor environments.
- LOS path is not required.

Disadvantages

- High power consumption.
- High Intra-network interference.
- Limited number of APs

2.5.2 ZigBee

ZigBee [34] is an emerging wireless technology based on the IEEE 802.15.4 standard which also operates in the 2.4 GHz band. This technology is mainly developed for low-power and low data rate applications and is basically used in Wireless Sensor Networks (WSN). The supported network topology is usually star which is based on several sensor nodes coordinated by at least one device known as coordinator. Though, mesh topology and peer-to-peer are also supported. ZigBee has an advantage in which it is a low-power communication protocol and the number of nodes per network can be high therefor, ZigBee positioning has also been studied by researchers. In [39], fingerprinting approach is utilized for positioning in a ZigBee WSN and in [40] and [41], RSS based positioning has been utilized. However, the major drawback of this technology is that it is not widely adopted and particularly by smartphones. Additionally, ZigBee is mostly asleep technology therefore, real-time tracking is not possible. The advantages and disadvantages of ZigBee are summarized below.

Advantages

- Low power compared to Wi-Fi
- Network topology is scalable.

Disadvantages

- Not widely adopted by smartphones.
- ZigBee sensor nodes are mostly asleep and real-time tracking is not possible.

2.5.3 Bluetooth

Bluetooth or Bluetooth Classic (BC) [5] is a global wireless communication standard administrated by Bluetooth Special Interest Group (SIG) [42]. This technology is mainly developed for short-range applications that require a high throughput such as audio and video applications. It started with Bluetooth Basic Rate (BR) with a maximum data rate of 721 kbps followed by Enhanced Data Rate (EDR) with up to 2.1 Mbps and then Bluetooth High Speed (HS) which increased the data rate up to 24 Mbps. BC supports piconet topology with up to 8 devices. However, this topology can be extended by forming a scatternet network which is composed of multiple piconets. BC also operates in the 2.4 GHz band and defines 79 Radio Frequency (RF) channels with 1MHz spacing. Since this band is shared by many technologies, BC uses frequency hopping approach to overcome the interference in which the radio hopes continuously between channels during connections. There are Moreover, BC is spread widely and can be found in almost all smartphones and laptops. This makes it a good candidates for indoor positioning applications. Several studies such as in [43] [27] [44] [45] used and evaluated BC for indoor positioning based on RSS technique. However, the drawback of BC is the localization latency (10–30s) [38]. This is because BC needs to run the device discovery procedure which has to scan on all channels. Another drawback is the power consumption which is higher than ZigBee. The advantages and disadvantages of BC in the context of indoor positioning are listed below.

Advantages

- Lower power consumption compared to Wi-Fi.

- Uses frequency hopping to overcome the interference issues.

Disadvantages

- Higher power consumption than ZigBee.
- Real-time tracking not feasible due to device discovery procedure.

Bluetooth Low Energy (BLE)

Due to the high demands on low-power applications, Bluetooth SIG introduced BLE [5] in 2010. The protocol stack of its counterpart BC has been redesigned in order to achieve this goal. Previously, BC targeted voice streaming and file sharing applications where the priority of these applications is high throughput. Currently, BLE is developed for other markets and particularly for IoT domain which includes devices such as sensors and actuators. These devices are recourse limited and the power consumption has the priority. BLE also operates in the 2.4 GHz band and uses the frequency hopping approach to compete with interference. Additionally, It supports star and mesh topologies. BLE has several advantages over others. Advertising mode or beaconing is one of these advantages. BLE uses three special channels for beaconing. These channels are called ADV channels and BLE beacons make the use of them in order to operate. BLE beacons are small and easy to install devices. They have many applications in marketing, home automation and indoor positioning as discussed earlier in 2.3. They only broadcast packets with short interval and require no pairing. The broadcasted packets can carry specific data and can be picked up by any BLE enabled device. Additionally, these packets can be used to allow a receiver to estimate its position to some specific beacons with known coordinates based on RSS. Another advantage is this technology is highly integrated into a variety of devices such as new smartphones and wearable. These advantages in addition to the low-power consumption make BLE a promising technology for indoor positioning. Therefor, researchers have recently shown an increased interest in evaluating BLE beacons for indoor positioning. Studies like [56] utilized beacons based on RSS fingerprinting approach while [57] used RSS trilateration due to its simplicity. The advantages and disadvantages of BLE are listed below.

Advantages

- Wildly adopted by smartphones.
- Requires no connection due to beaconing mode.
- Low power compared to Wi-Fi and BC.

Disadvantages

- Beaconing advertising interval is not sufficient for real-time tracking.
- Infrastructure has to be deployed.

A comparison among the above discussed wireless technologies is presented in Table 2.1. The comparison parameters are considered important for choosing the right technology for the implementation of an IPS. Moreover, it is appropriate to note that some values of the parameters are only indicative and the real values can only be determined by evaluation.

Table 2.1: Comparison of different wireless technologies for indoor positioning

	Wi-Fi	**ZigBee**	**BC**	**BLE**
Network topology	Star, ad hoc	Star, mesh, peer-to-peer	Piconet/Scatternet	Star-bus, mesh
Range	Up to 100 m	Up to 100 m	Up to 50 m	Up to 100 m
Power Consumption	High	Very low	Low	Very low
Cost	Medium	Medium/low	Medium	Low
Infrastructure	Existing APs	To be deployed	To be deployed	To be deployed
Smart-phone support	Supported	Not supported	Supported	Supported

2.6 Bluetooth Low Energy (BLE)

As the name states, BLE technology is completely optimized for low-power applications that require only the transfer of small amount of information. It was introduced as part of the Bluetooth 4.0 core specification and has evolved since then. Multiple features and upgrades were added in every release of specifications. A summary of the main upgrades that were added to BLE are listed below.

- **Bluetooth 4.0**: This version was released in June 2010. It is the first to introduced BLE as a standard for low-power applications [46].
- **Bluetooth 4.1**: Released in December 2013. This version added some upgrade such as coexistence support, allowing BLE devices to be peripheral and central simultaneously, privacy aspects in addition to improvements regarding connection typologies [47].
- **Bluetooth 4.2**: Released in December 2014. The major upgrade of this release was increasing the packet payload size by ten times in comparison to previous versions which was limited only to 31 bytes [48].
- **Bluetooth 5.0**: Released in December 2016. This version enhanced BLE technology towards the IoT domain. The key updates in comparison to older versions were four times longer range, two times higher speed, and eight times bigger advertising message capacity [49]. A comparison between different Bluetooth specifications with regard to some parameters is provided in Table 2.2.

2.6.1 BLE applications

In additional to the beaconing feature which enables applications such as indoor positioning. BLE technology has other use cases, some of these use cases are listed below [5].

- Finding and alerting devices.

  BLE can be used for finding misplaced devices such as car keys. For an example, if a car key is misplaced somewhere, it can be easily found by pressing a button on the smart-phone, and the key would then give an alert signal indicating its location. Another scenario would for example be an oven that notifies users on smart-phone once the food is ready.

Table 2.2: Comparison of Bluetooth versions [49]

	BC	BLE 4.0/4.1	BLE 4.2	BLE 5.0			
				LE 1M	LE 2M	LE Coded S=2	LE Coded S=8
Channels	79 (1 MHz)	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)	40 (2 MHz)
Advertising Ch	NS[1]	3	3	3 P[2], 37 Sc[3]	3 P, 37 Sc	3 P, 37 Sc	3 P, 37 Sc
TX power (dBm)	0 to 20	-20 to 10	-20 to 10	-20 to 20	-20 to 20	-20 to 20	-20 to 20
RX sensitivity (dBm)	< -70	< -70	< -70	< -70	< -70	< -75	< -82
Peak current (mA)	<30	<15	<15	<15	<15	<15	<15
Latency (ms)	100	<6	<6	<6	<6	<6	<6
Range (m)	10 - 100	10 - 100	10 - 100	10 - 100	10 - 100	20 - 200	40 - 400
Data rate (Mbps)	1, 2.1, 24	1	1	1	2	0.5	0.125
PDU format	Several	Single	Single	Single	Single	Single (coded)	Single (coded)
Max payload (byte)	1021	37	255	255	255	255	255
Max ADV payload (byte)	NS	37	37	255	255	255	255

[1] Not Supported
[2] Primary Channel
[3] Secondary Channel

- Health Care and fitness.

  BLE has a major use in the healthcare domain. BLE enabled devices such as heart rate monitors, glucose monitors and wearable medical devices can send their measurement data directly to the patient's smart-phone, which can in turn report these data directly to doctors or hospitals. This can insure that patients are monitored at anytime which can in some cases save lives.

- Presence detection.

  BLE beacons can be used for object's presence or absence detection and triggering actions accordingly. As an example of such use case, when a person enters the house, lights and heaters would turn on automatically or would turn off upon leaving.

2.6.2 BLE protocol stack

Like some other wireless standards, BLE implements a layered protocol stack. This stack is composed of three main blocks which are controller, host, and application where each block is split into a number of layers as shown in Fig. 2.8. These blocks and layers are explained below [5].

- **Application**

  The application layer resides on top of the protocol stack. It provides an interface for the user and contains the data processing part of the user application.

- **Host**

  The host defines and manages how devices communicate with each other. It is the software stack which is typically executed on a Microcontroller Unit (MCU). Moreover, the host includes the following layers:

  – Logical Link Control and Adaptation Protocol (L2CAP)

    This layer is responsible for multiplexing data between the host and controller

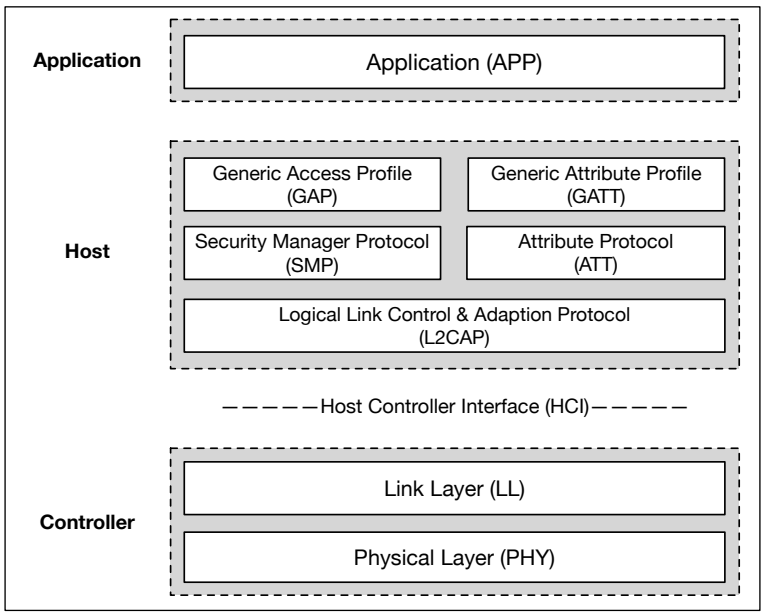


Fig. 2.8: BLE protocol stack

as well as packet fragmentation and reassembly.

– Security Manager Protocol (SMP)

  The SMP defines secure procedures for pairing devices such as key exchange and device privacy as well as data encryption and decryption.

– Attribute Protocol (ATT)

  This layer provides procedures for discovering attributes between devices as well as reading and writing attribute's values. An attribute can be any piece of information such as a temperature value.

– Generic Attribute Profile (GATT)

  The GATT manages the attributes defined by the ATT layer and encapsulates them into profiles as well as defining the attributes' access permissions. An example of a GATT profile is the heart rate profile which is adopted by Bluetooth SIG [50].

– Generic Access Profile (GAP)

  The GAP defines the roles of devices as well as procedures to allow devices to advertise themselves, discover other devices, establish and manage the connections.

- **Controller**

  The controller is responsible for discovering nearby devices and making connections in addition to data packet exchange. It communicates with the host through Host Controller Interface (HCI) which is a standard communication protocol such as Universal Asynchronous Receiver-Transmitter (UART) and USB [49]. Moreover, the controller

includes two layers which are the Link Layer (LL) and the Physical layer (PHY). In this thesis, the focus is only on the controller part and other parts of the protocol stack are not covered.

BLE Link Layer (LL)

The LL is responsible for managing the PHY layer such as establishing and managing links between devices, dealing with timing requirements defined by the standard, selecting frequency channels, data encryption/decryption in addition to Cycle Redundancy Check (CRC) management. There are five different defined states of LL as shown in Fig. 2.9. These states are standby, advertising, scanning, initiating and connection. The focus of this thesis is only on advertising and scanning states which are explained in details in the following sections. A brief discretion of the LL states is provided bellow.

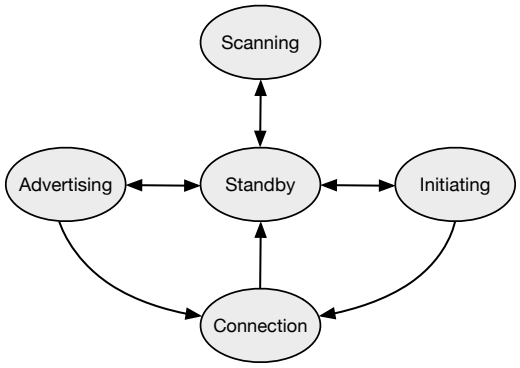


Fig. 2.9: Link layer state machine diagram [5]

- Standby State In this state, the radio is idle and no packet transmission or reception is done.
- Advertising State A BLE device in the advertising state is called advertiser or broadcaster. In this thesis, broadcaster is used. In this state, devices broadcast advertising packets. Additionally, they may listen to requests from other devices and respond accordingly.
- Scanning State A BLE device in the scanning state is called scanner or observer. In this thesis, observer is used. However, in this state, devices scan for advertising packets and can also request some additional information from the broadcasters of these packets.
- Initiating State A device in this state is called initiator. An initiator scans for advertising packets and responds by initiating a connection with a specific broadcaster.
- Connection State LL in the connection state allows applications to exchange data between connected devices. The connection state can implement either a master or a slave role.

BLE Device Address

The device address is the device identity. According to the BLE standard, the device address can be either public or random. The public device address is a globally unique address issued by the IEEE. The random device address is meant for privacy aspects. BLE devices can use a randomly generated device address in order to hide their public addresses and prevent tracking possibilities. Furthermore, the devices address is 6 bytes in length for both public and random addresses.

BLE Air Interface Packet Format

The packet format of BLE standard is illustrated in Fig. 2.10. Each transmitted packet is composed of four mandatory fields which are the Preamble, Access Address, Protocol Data Unit (PDU) and lastly the CRC [49].

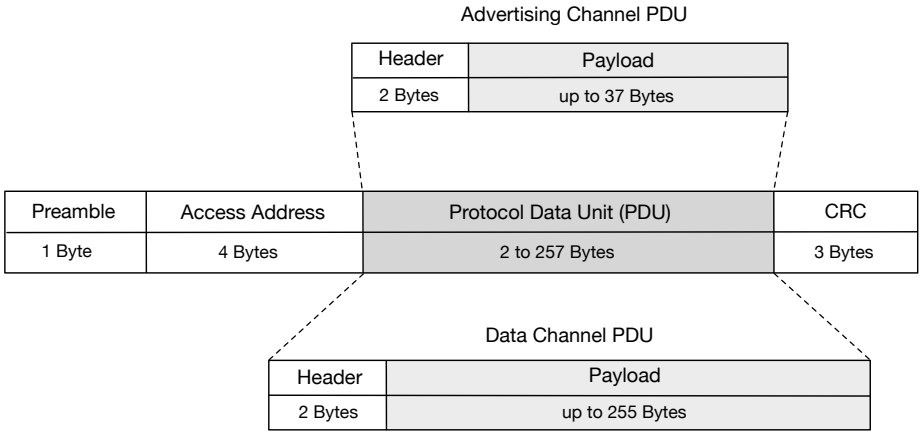


Fig. 2.10: Overview of LE 1M packet format

- **Preamble**: is the first field in the packet. It is 8 bit long and alternates between 0 and 1 bits. The preamble is used at the receiver side for frequency synchronization and symbol timing estimation [49].
- **Access Address**: follows the preamble and has a length of 4 bytes. It is used as a correlation code between two connected devices operating on the same RF channel [5]. This ensures that the transmitted packet is meant only for a specific device having the same access address. Furthermore, each connection between two BLE devices has a different access address that is randomly generated by the LL. For advertising packets, the access address is always fixed to 0x8E89BED6.
- **PDU**: follows the access address and can be either ADV channel or data channel PDU. The ADV PDU is used for the transmission of packets on the ADV channels while data PDU is used for the transmission of packets on the data channels. Moreover, each PDU consists of two fields, a 2 byte header and a payload. The payload size depends on the PDU type in use. and for ADV, it is limited to 37 bytes while for data, the size is up to 255 bytes.

- **CRC**: is the last field in the packet and has a length of 3 bytes. It is used for checksum error which is calculated over the whole PDU and is then added to the packet.

BLE Advertising and Scanning

BLE devices use ADV packets for presenting their presence to other nearby devices in order to allow connections to be established, or to only broadcast user defined data (beaconing).

Advertising Events

ADV packets are transmitted in terms of events [49]. During an advertising event, one packet is usually transmitted on all three primary ADV channels consecutively. However, advertising only on one specific channel is also permitted by the standard. The time between the start of two consecutive events is defined as *T_advEvent* which is calculated for each event according to the following formula

$$T\_advEvent = advInterval + advDelay \tag{2.11}$$

The *advInterval* varies between 20 ms to 10,485 s and can be defined by the user depending on the use case. Where the *advDelay* is a random number between 0 and 10 ms that is added to the ADV interval for every event. This adds randomness in the ADV interval which reduces the possibility of packet collision in case multiple broadcasters exist in the same vicinity. An illustration of advertising events on all ADV channels is shown in Fig. 2.11. The *Adv_idx* represents the channel index number while (1), (n+1) indicate that the same packet is transmitted on all channels consecutively during one event. The timing parameters *T_advEvent*, *advInterval* and *advDelay* are also illustrated in details.

Advertising Channel PDU Types

ADV packets do not require acknowledgement from the receivers and they can be undirected or directed to a specific device, connectable or non-connectable. As seen before in Fig. 2.10, the advertising PDU consists of two fields, a header and a payload, the type of a advertising PDU is defined in the header. The length of the header is 2 bytes and it consists of several sub-fields as shown in Fig. 2.12. The PDU type field determines the type of the transmitted packet, RFU stands for reserved for future use, ChSel denotes the channel index in case advertising extension feature is used [49], TxAdd and RxAdd determine whether the address of the transmitter/receiver is public or random, and finally the Length field which denotes the length of the payload. BLE standard defines seven different PDU types for the ADV

channels which are:

1. ADV_IND: Connectable undirected.
2. ADV_DIRECT_IND: Connectable directed.

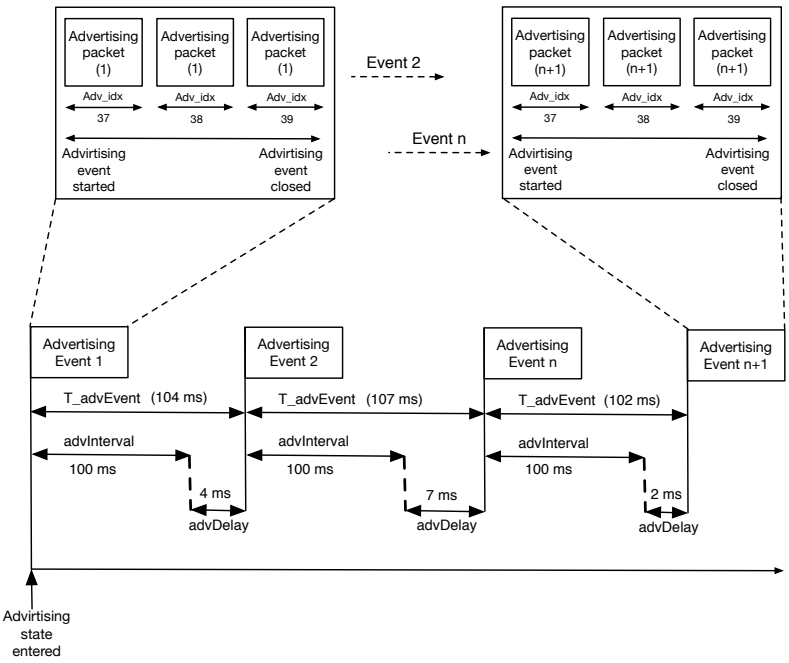


Fig. 2.11: Overview of BLE advertising event and timing

3. ADV_NONCONN_IND: Non-connectable undirected.
4. ADV_SCAN_IDN: Scannable undirected.
5. SCAN_REQ: Scan request.
6. SCAN_RSP: Scan response.
7. CONNECT_REQ: Connection request.

LSB MSB

PDU Type	RFU	ChSel	TxAdd	RxAdd	Length
4 bits	1 bit	1 bit	1 bit	1 bit	8 bits

Fig. 2.12: BLE advertising channel PDU header.

The focus of this thesis is only on the non-connectable undirected advertisements and the rest of PDUs are not covered. The non-connectable undirected PDUs are used in cases where a broadcaster wants only to provide certain information to other devices without pairing. The ADV interval of the the non-connectable undirected PDU is limited to 100 ms [49]. This scenario of one-way communication can be seen in beacon implementation where a BLE beacon would want only to advertise certain data.

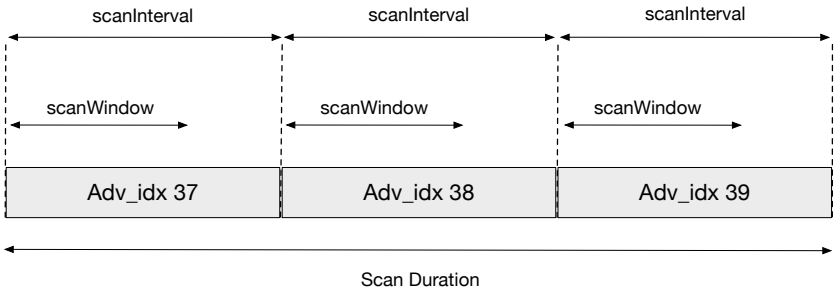


Fig. 2.13: Overview of a scan event

Scanning Events

BLE devices scan for ADV packets in terms of scan events [5]. During a scan event, the radio listens on each of the ADV channels for a duration of time defined as scan window. The time between every two scan windows is defined as scan interval and the total time of the scan event is denoted as scan duration as shown in Fig. 2.13. The scan window and interval can be set by the host and as per specification, these parameters should be less than 40.96 s. Moreover, scanning can be either passive or active. In passive scanning, devices only receive packets while in active scanning, devices can receive ADV packets and may also request some additional information using a scan request SCAN_REQ. It is appropriate to note that BLE standard does not permit scanning on a specific ADV channel, and since the broadcaster and observer are not synchronized, an ADV packet can be received only when the channel index of the observer and broadcaster overlap randomly [51]. Additionally, an ADV packet is missed in case it arrives at a time when the radio is in the process of switching from one channel to another. An illustration of advertising and scanning procedure is shown in Fig. 2.14.

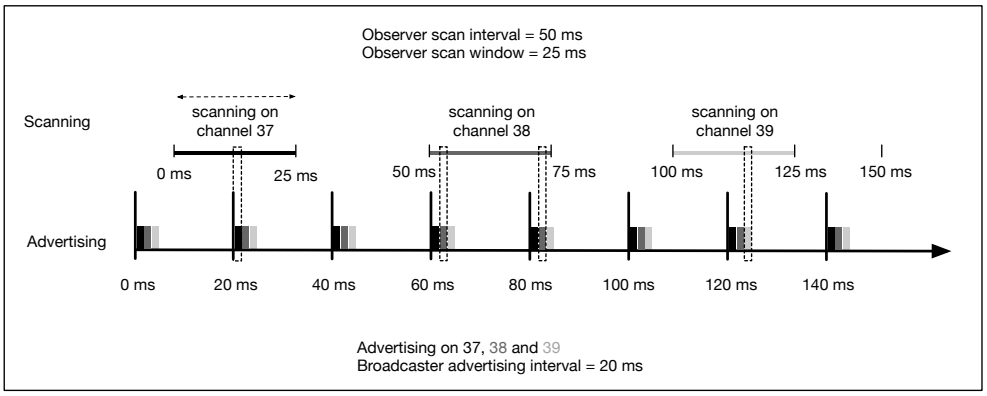


Fig. 2.14: Advertising and scanning [51]

Device Filtering and White List

The white list is a set of specific devices the LL only accepts packets from [5]. It is configured by the host and includes records of the filtered devices where each record contains the device address and its type (random or public).

BLE Physical layer (PHY)

The PHY is the lowest layer in the protocol stack and the one that defines how data is exchanged over the air. It includes the BLE radio chip which operates in the 2.4 GHz frequency band and uses the Gaussian Frequency Shift Keying (GFSK) modulation [5]. As can be seen in Fig. 2.15, BLE standard divides the frequency band into 40 channels with 2 MHz spacing, starting from 2402 MHz to 2480 MHz. Each of these channels has a unique channel index ranging from 0 to 39. These channels are divided into 3 ADV and 37 data channels. ADV channels have the indices 37, 38, and 39 and are used for device discovery, connection initiation and information broadcast (beaconing). They are distributed over the frequency spectrum in a way that reduces the possibility of interference with the most widely used Wi-Fi channels 1, 6 and 11. Moreover, BLE 5 standard defines threePHYs for the operation of the radio. Namely, LE 1M, LE 2M and LE Coded [49]. LE 1M has a data rate of 1 Mbps. It is the default and mandatory PHY in BLE 5 since previous versions of which define only this PHY need to be backward compatible with version 5. The focus of this thesis is only on the ADV channels operating on the LE 1M PHY.

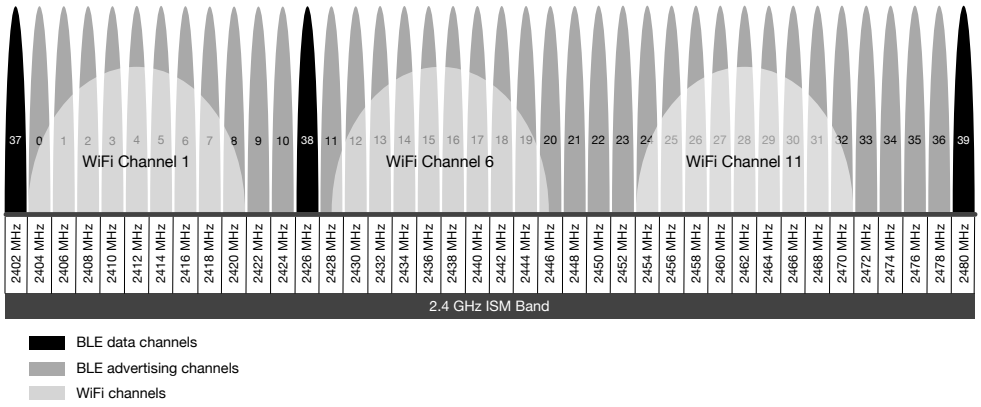


Fig. 2.15: Overview of BLE PHY channels and frequencies

Since the frequency band of BLE is shared by other wireless technologies, BLE uses frequency hopping approach in order to reduce the possibility of interference. The hopping sequence is given by the following formula [51]

$$channel = (curr\_channel + hop)\ mod\ 37 \tag{2.12}$$

Transmit output power

Transmitter power or TX power refers to the amount of energy the radio outputs in the air during transmission. This parameter is a 8-bit signed integer and is usually measured in watt or decibel (dBm). BLE standard defines the range of transmitter output power to be between 0.01 mW (−20 dBm) to 100 mW (+20 dBm).

Receiver sensitivity

Receiver sensitivity refers to the minimum required signal energy at the receiver side which guarantees a proper communication. Like transmitter power, receiver sensitivity is also measured in watt or dBm and BLE devices should have a receiver sensitivity with a minimum of -70 dBm for LE 1M PHY.

2.7 Related Work

A considerable amount of literature on indoor positioning has been published. These studies discussed, deployed and evaluated several positioning methods and techniques in order to bring positioning indoors. The focus of this thesis is on RSS positioning and particularly path loss modeling therefore, this section discuses only the relevant research.

The advantages of using RSS for distance estimation is the low complexity and cost since it can be implemented on any existing hardware that supports the RSSI reading. Based on this fact, a number of studies have examined the feasibility of RSS positioning. In [28], three different triangulation positioning methods based on RSS have been evaluated and compared. The study has been conducted based on Bluetooth technology and the L-NDM has been used. The authors stated that the positioning accuracy highly depends on the proper selection of the path loss model. [52] used the L-NDM for point-to-point distance estimation in a WSN. The study is based on the IEEE 802.15.4 standard where several sensor nodes were deployed in a lab environment. The obtained results reported a mean distance error of 2.25 m with the absence of other 2.4 GHz operating devices during the experiment. Although few precautions have been taken into consideration such as antenna height and direction, the study failed to perform measurements under noisy conditions which is the case of almost every indoor environment. Furthermore, both discussed studies did not consider using the L-NSM instead of the L-NDM. The L-NSM [16] is considered a more general propagation model that suits both indoor and outdoor environments. It has been used in [53] to locate a robot based on ZigBee standard. The study pointed out the big errors occurred in distance measurement indoors using RSS. Therefore, the authors proposed a hybrid RSS and Time Difference of Arrival (TDoA) solution with filtering approaches for restraining the noise and stabilizing the RSS readings. They obtained in their experiment a positioning accuracy of approximately 0.5 meter with the presence of operating Wi-Fi and Bluetooth devices. However, their approach is relatively complex since it utilizes TDoA technique which requires special hardware. [54] conducted experiments in order to compare the the performance of RSS trilateration and fingerprinting methods based on Wi-Fi standard. They utilized the L-NSM for the trilateration method and their experiment showed the importance of the correct deployment of APs as reference points.

Additionally, their results showed that fingerprinting yields better accuracy compared to RSS trilateration. On the other hand, they stated that fingerprinting is time consuming and requires a lot of efforts during the calibration phase. Factors thought to be affecting the RSS have been explored in several studies. In [55], authors pointed out that one of the most important factors in distance measurement is the transmission power where too high or too small transmission power causes misinterpretation in distance measurement. Their experiments have also shown the effect of the used frequency and that some frequencies are subject to more distortion than others particularly in noisy environments. In [14] and [16], the affects of antenna heterogeneity and direction on RSS are discussed. The authors stated that device properties such as antenna design and type is an important factor. Besides, they stated that radio propagation is not isotropic and exhibit significant variations with antenna direction changes. Additionally, the studies also pointed out the effects of background noise and environment properties such as temperature and humidity as well as the transmission power.

Positioning with BLE has gained recently a significant attention due to the wild adoption of this technology in many devices in addition to the low-power consumption and beaconing mode. BLE beacons have a hug potential in the context of indoor positioning. [56] conducted experiments in order to compare the performance of BLE beacons versus Wi-Fi RSS fingerprinting. Their results showed that a significant positioning improvement over Wi-Fi is possible with BLE. Additionally, the authors analyzed the RSS variation of the ADV channels separately but however, they failed to perform experiments in different environments. An IPS based on BLE beacons is proposed in [57]. RSS and trilateration method have been utilized using the L-NDM. The study pointed out that the placement of beacons has a significant impact on positioning accuracy. However, the study lacks information about propagation modeling. The L-NSM has been also used in [58] based on BLE RSS. The authors proposed a series of optimization in order to improve positioning accuracy such as Gaussian filter and Least Square (LS) based fitting for offline training in addition to a collaborative algorithm based on Taylor series expansion. kalman filter has been applied to RSS technique in [59] in order to improve the distance estimation based on the L-NSM. The authors claim that the achieved accuracy of their system is proven to be high. However, they failed to address the different behaviour of the three ADV channels. [60] conducted extensive experiments in order to analyze the behaviour of RSS in a small office scenario. They claim that for short distances less that 3m, the Path Loss Exponent (PLE) is not constant. [61] analyzed the accuracy corresponding to the number of BLE beacons. The study pointed out that the more beacons the more accurate result. A major draw back of this study is that part of it was evaluated through simulation. Particle filtering approach is proposed by [62] to increase the accuracy of micro-location using BLE beacons. Authors pointed out that beacons should be properly placed at higher altitudes in the environment to avoid obstacles' effects. Furthermore, a summer of the studies discussed about BLE RSS positioning is provided in Table 2.3

Overall, these studies highlight the need for comprehensive hardware experiment in different locations and under various conditions. Most of the studies only focus on single environment experiments which may lead to having a highly environment specific results. Additionally, most of the studies considered all three ADV channels as a single channel which leads to a considerable variation in RSS readings. The outdoor and indoor comparison allow to have a precise understanding of factors such as multipath effect and interference which are

negligible in outdoor but have a significant impact is indoor environments. Besides, the studies in the literature do not have sufficient sample size and did not consider different transmit powers in their experiments which results in a poor validity.

Table 2.3: Summary of the related work of BLE positioning

No.	Ref	Approach	Advantages	Disadvantages
Ref.1	[56]	RSSI fingerprinting with BLE Beacons.	BLE has better accuracy than Wi-Fi in the same test environment. ADV channels have different gain and behaviour.	Fingerprinting requires a lot of efforts.
Ref.2	[57]	RSSI trilateration with BLE beacons.	Low complexity. Equidistant placement of beacons on ceiling provides good results.	Less research on ADV channels. Lack of propagation modeling. Single environment experiment.
Ref.3	[58]	RSSI positioning with BLE.	Positioning error is less than 1.5 m.	Requires an offline phase. Less research on BLE ADV channels. Single environment experiment.
Ref.4	[59]	RSSI point-to-point distance estimation using BLE.	Simple approach.	Less research on ADV channels. Single environment experiment.
Ref.5	[60]	RSSI technique for micro-positioning using BLE.	Proposed new path loss model for short distances.	Less research on ADV channels. Single environment experiment.
Ref.6	[61]	RSSI positioning with BLE.	More beacons provides better accuracy.	Done through simulation. Lack of propagation modeling.
Ref.7	[62]	RSSI positioning using particle filter	High accuracy using particle filter approach.	Less research on ADV channels.

CHAPTER 3

Methodology

3.1 Introduction

In this chapter, the methodology used in this research in order to achieve the proposed objectives is described. Additionally, this chapter describes the hardware experiment and the theoretical description of the used methods.

3.2 Operational Framework

The operational framework describes the connection between the steps of the research, and how they work together in order to tackle the research problem. As shown in Fig. 3.1, the operational framework of this research consists of three phases which are explained below.

3.3 Phase-I

Phase-I includes the literature review which provides an overview of wireless communications and their advantages, the importance and applications of indoor positioning in addition to the use cases of BLE beacons, indoor positioning methods and distance measurement techniques, the commonly used wireless technologies in this area of research as well as BLE technology which has been used in the experiments. Following that, previous research efforts and techniques in this area of research are discussed in the related work, and what has been missed by researchers has been identified as the gap of the study. Therefore, approaches and techniques to fulfill the identified gap have been selected in this phase. This includes specifying the scope of the research by choosing the research platform (simulation or hardware experiment), experiment environments, required tools, data collection methods in addition to the implementation.

As mentioned earlier, the set of BLE ADV channels enables a set of applications such as indoor positioning. RSS is the commonly used technique for point-to-point distance estimation based on these channels. However, there are many factors that disturb the reliability of

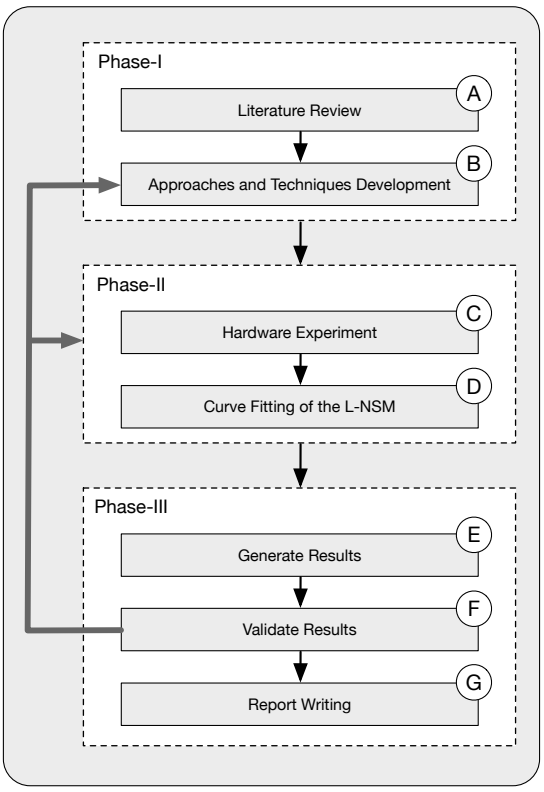


Fig. 3.1: Research operational framework

RSS such as multipath, interference and different frequencies resulting in errors in distance measurement. Therefore, it is important to characterize and model the wireless channel in order to achieve a better reliability. In order to achieve that, hardware experiment is essential. The research has been planned to be experimentally performed using hardware. The reason behind that is simulators usually do not cover all factors that have an impact on RSS [16]. Additionally, the results of this research can provide simulators a realistic assumptions about BLE ADV channels. BLE technology has been selected for the experiment because it is a low-power standard, it supports beaconing, and it is widely integrated into smartphones and IoT devices. The beaconing feature requires no connection establishment and it operates on three channels that have less interference with the widely used Wi-Fi channels 1, 6, and 11. In order to have a better understanding of signal behaviour under various conditions, five different environments (refer to Section 4.2) have been defined as test fields. These environments can be categorized into indoor and outdoor where each environment has unique characteristics such as closed or open space, with obstacle or without.

3.4 Phase-II

This phase deals with the hardware experiments in addition to the approaches and the theoretical description of the used methods for curve fitting of the L-NSM.

3.4.1 Hardware Experiment

In order to perform the experiment, a testbed for measuring the RSS has been developed. The testbed is explained in details in 4.4. It is composed of three main units which are a broadcaster for transmitting packets, an observer for receiving the packets and a 2.4GHz sniffer for measuring the background noise of the environment. Transmission is done on BLE ADV channels: 37 (2402 MHz), 38 (2426 MHz) and 39 (2480 MHz). The measured RSS value of the received packets with respect to different transmission powers are recorded, the background noise level of the environment as well as the Packet Error Rate (PER) of each transmission. Furthermore, the experiment has been performed in two steps. The first step includes performing point-to-point transmission at different broadcaster-observer separation distances. This is to to analyze the path loss characteristics of these channels. The second step includes performing transmission with respect to different antenna directions and with the use of two different hardware. This is to to analyze the effects of antenna heterogeneity and direction on RSS quality. For results validation and avoiding the technical issues, the experiment was repeated five times in each defined distance. A description of the experiments setup is provided in in 4.5. For the reliability of the experiment, different transmission powers have been considered.

3.4.2 Curve Fitting of the L-NSM

The parameters of the L-NSM Formula 2.10 depend on both environmental factors (e.g., obstacles, reflective surfaces, and humidity) and characteristics of RF transceiver (e.g., frequency band, transmit power, and modulation scheme). As these factors do not stay unchanged over time, the variations of signal power over time has to be estimated. To this end, the Trust Region Reflective Least Squares (TRRLS) method [63] from Matlab has been applied to the sampled RSS in order to obtain the best fit for each experimental observation. The least squares method finds a curve that minimizes the sum of the squares of the distances between the measured RSS values and the estimated ones. The trust region reflective algorithm minimizes the function which is $f(d)$ in this case to a lower function value based on the behaviour of $f(d)$ in a neighboring point. Moreover, for path anisotropy approach, we will calculate the mean of the whole antenna rotation in addition to standard deviation.

3.5 Phase-III

This phase includes generating the results of the conducted experiments, validating the results and report writing. The results obtained from the experiments are plotted using Python matplotlib [78]. After that, the results are validated by comparing them to other researchers work and if the results are not suitable, then part (C) in phase-II and part (B) in phase-I must be reconsidered and the experiment parameters need to be modified. Finally, the documentation of every step has been presented in this thesis. A summary of the activities and outputs of each phase is presented in Table 3.1.

Table 3.1: Summary of the activities and outputs of each phase

Phase	Milestone	Activities Involved	Output
I	Perform literature review	Primary study on research domain	Problem background.
			Problem statement.
		Literature review	Research objectives.
			Research scope.
		Discussion on study background	Selection of approaches and techniques.
II	The proposed approaches and techniques	Hardware experiment	Performing L-NSM and path anisotropy experiments.
		Curve fitting of L-NSM	Optimization of η and determination of σ.
			Determination of σ for path anisotropy.
III	Results	Generating the results	Data collection and visualization
	Validation	Result comparison with the literature	Validate results.
	Report writing	Writing the final report.	Submission of the thesis

CHAPTER 4

Experimental Implementation

4.1 Introduction

This chapter describes the implementation of the hardware experiment. Section 4.2 describes the characteristics of the test environments in which the experiment was performed. Then Section 4.3 describes the hardware and software used in this research. The developed testbed is also described in Section 4.4. Section 4.5 describes the implementation of the experiment and the used criteria. Finally, Section 4.6 describes briefly the design of the BLE LL on Nordic nRF52840 development broad.

4.2 Experiment Environments

In order to have a better understanding of signal behaviour under various conditions, four different environments Fig. 4.1 have been selected for conducting the experiment. These environments can be categorized into two outdoors and two indoors where each environment has unique characteristics that may affect signal propagation. Outdoor environments are two open fields which are Stadtpark and Nordpark located in the city of Magdeburg, Germany. Indoor environments are a classroom hall and a corridor located inside the faculty of Informatics at Otto von Guericke University Magdeburg. A further description of each environment is provided below.

- **Stadtpark** Fig. 4.1a is an open field located around the city. The filed is free of trees and other active wireless technologies. While transmission, the broadcaster and observer experience a LOS path.
- **Nordpark** Fig. 4.1b is an open field located in the middle of the city. The field contains trees and plants that are present between the broadcaster and observer. Moreover, the field is free from other operating wireless technologies.
- **Classroom** Fig. 4.1c is located in the 3rd floor of the university building with dimensions of 18*12 m. It contains several tables and chairs in addition to few Wi-Fi APs but the LOS path is present.

a) Stadpark b) Nordpark c) Classroom d) Corridor 4th floor

Fig. 4.1: Experiment environments

- **Corridor 4th floor** Fig. 4.1d is located in the 4th floor of the same university building with dimensions of 31x1.8 m and a LOS path. Additionally, there exist three rooms along the left side of the corridor with Wi-Fi APs as well as few windows on the right side.

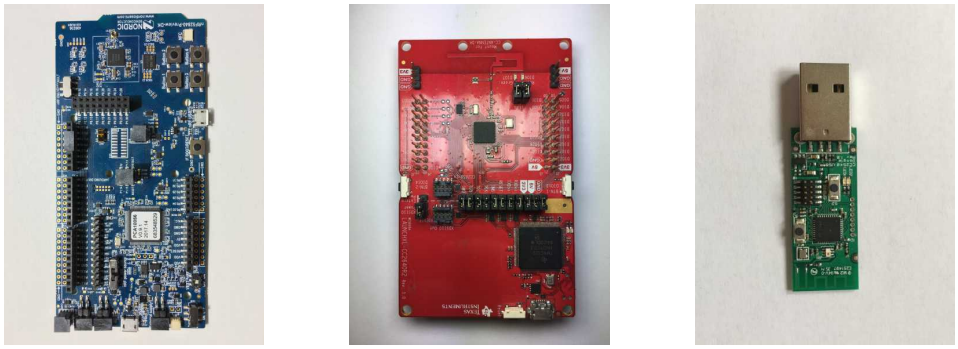
4.3 Hardware and Software platforms

The hardware used during the experiments have been selected based on their technical specifications. A comparison of four different BLE hardware that were available during the research is presented in Table 4.1. Among these, Nordic nRF52840 [67] Fig. 4.2a and TI CC2640R2F [68] Fig. 4.2b BLE development boards have been selected. The reason behind this particular selection is mainly due to their full support of BLE v5, the large RAM and programmable memory size, and the powerful host MCU. Besides, the nRF52840 permits accessing the radio in the 2.4 GHz spectrum which made it possible to design the LL of BLE standard. Finally, TI CC2540 BLE packet sniffer Fig. 4.2c [69] has been used for technical purposes.

Based on the hardware selection, the integrated development environments Keil MDK for ARM based microcontrollers [74] and Code Composer Studio [75] have been selected for programming and debugging the used hardware based on embedded C programming. Additionally, two BLE software stacks have been used. S140-SoftDevice-v5.0.1 provided by Nordic [76] and BLE-STACK v1.35 provided by TI [77]. For cure fitting, Matlab software has been used. Finally, the results of the experiment have been plotted using Python matplotlib [78].

Table 4.1: A comparison of different BLE development boards

	Nordic nRF52832 [70]	Nordic nRF52840 [71]	TI CC2650 [72]	TI CC2640R2F [73]
BLE version	BLE 5	BLE 5	BLE 4.2	BLE 5
Transceiver MCU	ARM Cortex M0	ARM Cortex M0	ARM Cortex M0	ARM Cortex M0
Host MCU	ARM Cortex M4F	ARM Cortex M4F	ARM Cortex M3	ARM Cortex M3
RAM	64 KB	256 KB	28 KB	28 KB
Programmable Memory	512 kB	1 MB	128 KB	275 KB
RX Sensitivity	-96 dBm	-96 dBm	-97 dBm	-96 dBm
TX Output Power	-20 to +4 dBm	-20 to +8 dBm	-21 to +5 dBm	-21 to +5 dBm
RX Consumption	5.4 mA	5.3 mA	5.9 mA	5.9 mA
TX Consumption	5.3 mA at 0 dBm	6.4 mA at 0 dBm	6.1 mA at 0 dBm	6.1 mA at 0 dBm
Standby Current	1.8 uA	1 uA	1 uA	1.1 uA



a) Nordic nRF52840 DK b) TI CC2640R2F DK c) TI CC2540 BLE sniffer

Fig. 4.2: Hardware used for the experiment

4.4 Testbed

The developed testbed for measuring the RSS is composed of three units. A broadcaster for transmitting packets, an observer for receiving the packets and a 2.4GHz sniffer for measuring the background noise of the environment. All units are based on the Nordic nRF52840. Besides, TI CC2640R2F has been added to the experiment as second broadcaster in order to compare the effects of antenna heterogeneity. The testbed units are each fixed on a tripod in order to control the antenna height. The functionality is based on a connectionless one way transmission of a certain number of packets from the broadcaster to the observer without replying any ACK. Transmission is done on the three primary advertising channels of BLE. Channel 37 (2402 MHz), 38 (2426 MHz) and 39 (2480 MHz). Furthermore, each transmitted packet has an index, this is helpful to recognize the exact lost packets. On the observer side, received packets including their indexes and RSS in addition to the PER of each transmission are recorded. The parameters transmission power and antenna height are also considered. Moreover, the functionality of the developed testbed is shown in Fig. 4.3. The observer is the unit that controls both the broadcaster and sniffer. In the first step, the observer sends a control (trigger) packet to the broadcaster where this packet contains

parameters such as channel index, transmission power and packet size. The broadcaster configures its transmission parameters upon receiving the control packet and then it starts transmitting accordingly. Simultaneously, the observer issues control commands to the sniffer such as the channel index to scan on in addition to the duration of scanning. Once transmission is done, the observer processes the recorded data and forwards it to the sniffer which in turns forwards the data to a laptop including the measured background noise.

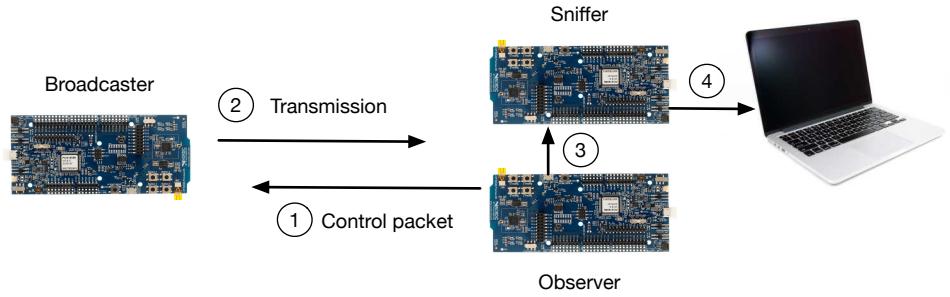


Fig. 4.3: Testbed architecture and functionality

Sniffer

The sniffer is required for the experiment in order to measure the background noise of the environment. Most of the available spectrum analyzers in the market are relatively costly. In addition, they can not be synchronized with the used hardware. Therefor, a 2.4GHz sniffer based on the Nordic nRF52840 chip has been developed. The software design of the sniffer is part of the LL implementation which is explained in 4.6.

4.5 Experimental Setup

This section describes the experimental setup and criteria of the experiments of both path loss and path anisotropy approaches.

4.5.1 Path Loss

This approach is dedicated mainly to analyze the path loss of BLE ADV channels. The experiment was performed in all four defined environments using only Nordic nRF52840 devices. An illustration of the experiment setup is shown in Fig. 4.4. The observer and the sniffer were placed next to each other in a fixed location during the experiment, while the broadcaster unit is the one to be moved after each RSS measurement at each defined distance. A set of distances has been defined. these distances are shown in Fig. 4.4. However, not all defined distances where reached in indoor environments due to the limited length of the test fields. In the classroom, up to 15 m was reached where in both corridors up to 30 m. The antenna height of all units is 1 meter from the ground. The initial separation distance between the broadcaster and observer is 1 meter and is considered the reference distance where $PL(d_0)$ is calculated. Additionally, different transmission powers

were tested (+8, 0, -8 and -20 dBm). The packet size is 9 bytes including the PDU header and device address. Before transmission takes place, 40 thousand samples of the background noise on the used transmission channel are recorded as well as the ambient temperature and the relative humidity. Following that, 1000 packets were transmitted for each defined transmission power and channel at each distance with an interval of 3 ms. For the reliability of the experiment, the transmission at each distance was repeated five times. Moreover, the experiment parameters are listed in Table 4.2 and the software design is illustrated in Fig. 4.5.

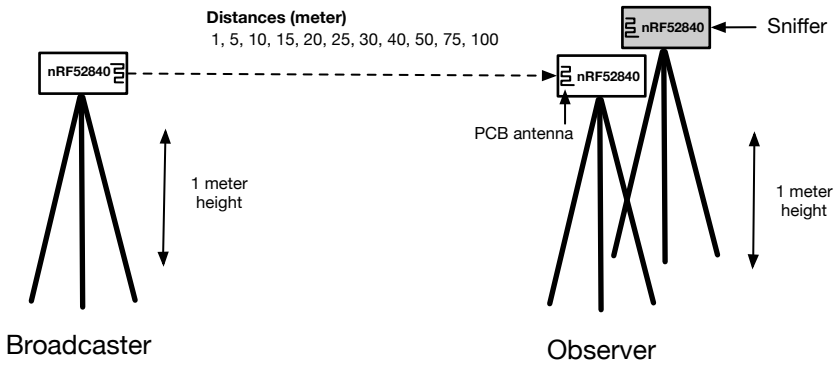


Fig. 4.4: Path loss experimental setup

Table 4.2: Experiment parameters

Parameter	**Stadtpark**	**Nordpark**	**Classroom**	**Corridor 4th floor**	**Corridor 1st floor**
Temperature	11.0	14.8	21.0	21.1	18.2
Humidity	58.1	53.4	48.9	49.0	54.3
Dimensions (m)	Open field	Open field	18×12	31×1.8	31×1.8
No. distances[1]	11	11	4	7	7
No. packet[2]	1000	1000	1000	1000	1000
Packet size (Byte)	9	9	9	9	9
T. interval[3] (ms)	3	3	3	3	3
LOS	Yes	No	Yes	Yes	Yes

[1] Number of distances.
[2] Number of transmitted packets per distance.
[3] Transmission interval.

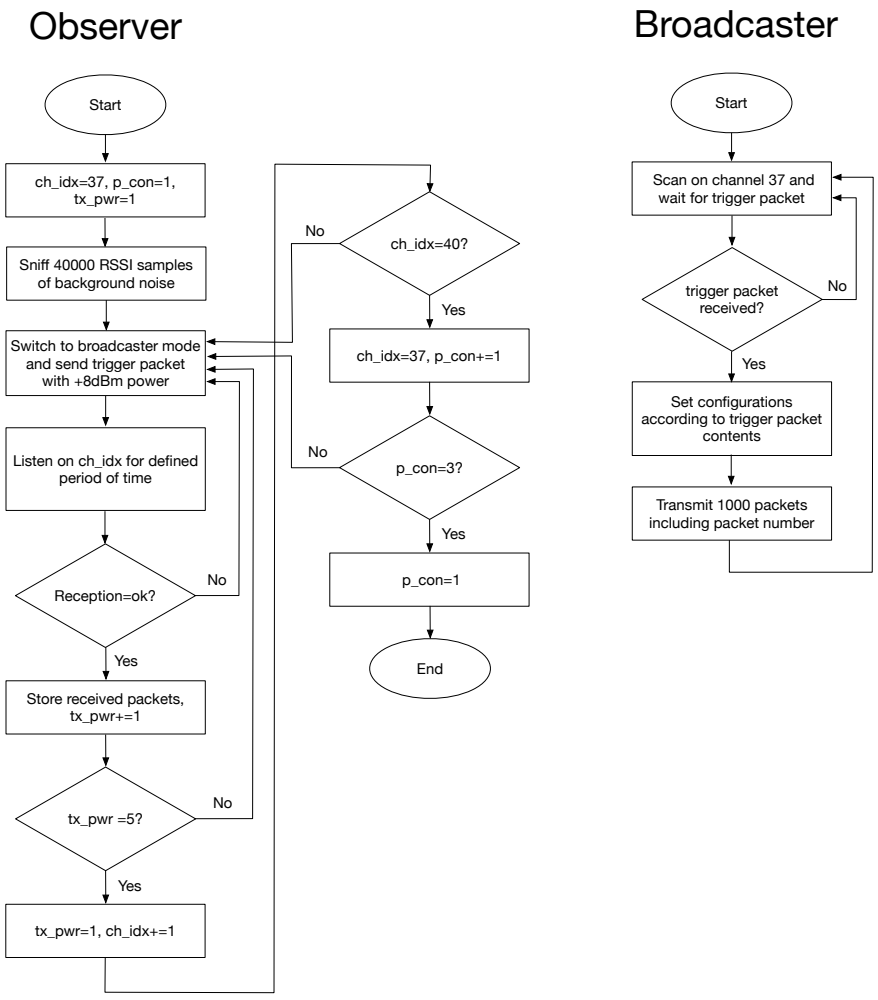


Fig. 4.5: Path loss approach software design

4.5.2 Path Anisotropy

The main aim of this approach is to analyze the impact of antenna heterogeneity and direction on RSS. Nordic nRF52840 and TI CC2640R2F have been used as broadcasters. This is to have a comparison since each of the selected hardware has a different antenna layout. The experiment was performed in two indoor environments. In the corridor 4th floor and in the classroom. An illustration of the experiment setup is shown in Fig. 4.6. The broadcaster was fixed on the rotary device (described below) while the observer and sniffer were placed next to each other in a fixed location during the experiment. Before transmission takes place, 40 thousand samples of background noise on the used transmission channels are recorded. After that, the broadcaster transmits a batch of 100 packets then rotates 5 degrees and does the same again. This process continues until the the broadcaster reaches 355 degrees then it starts again at 0 degree, switch to the next channel and so forth until the measurement is done on all three advertising channels. In the corridor, the RSS measurement was performed at distances of 1, 5, 10 and 20 meter were for the classroom, it was performed at distances of 1, 5 and 15 meter. Additionally, different transmission

powers were tested (0 and -20 dBm) with a packet size of 39 bytes. For the reliability of the experiment, the transmission at each distance was repeated five times. Moreover, the software design of this approach is illustrated in Fig. 4.8.

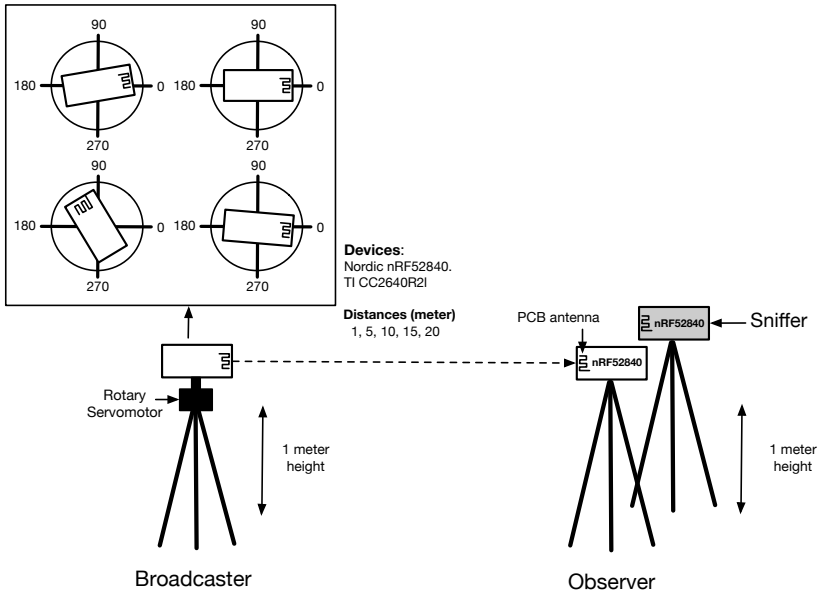


Fig. 4.6: Demonstration of path anisotropy experiment

Rotary Device

The rotary device Fig. 4.7 has been designed in order to change the antenna direction of the broadcaster. This makes the experiment easier to handle and provides an accurate direction adjustments since servo motors can step to the defined degree precisely. The rotary device is composed of two servo motors, a controller unit and an LCD in addition to some control buttons. The servo motors are fixed over each other in order to achieve a complete 360 degree rotation since each servo rotates only 180 degree. Moreover, the rotary device is controlled by the broadcaster unit via the UART interface.

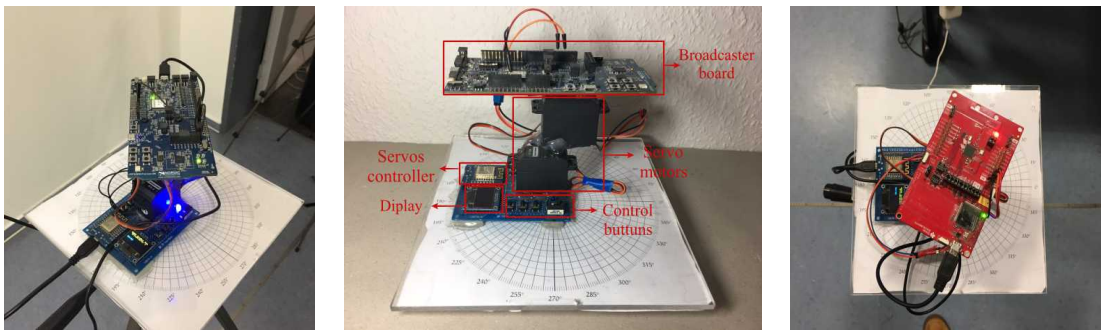


Fig. 4.7: Rotary device

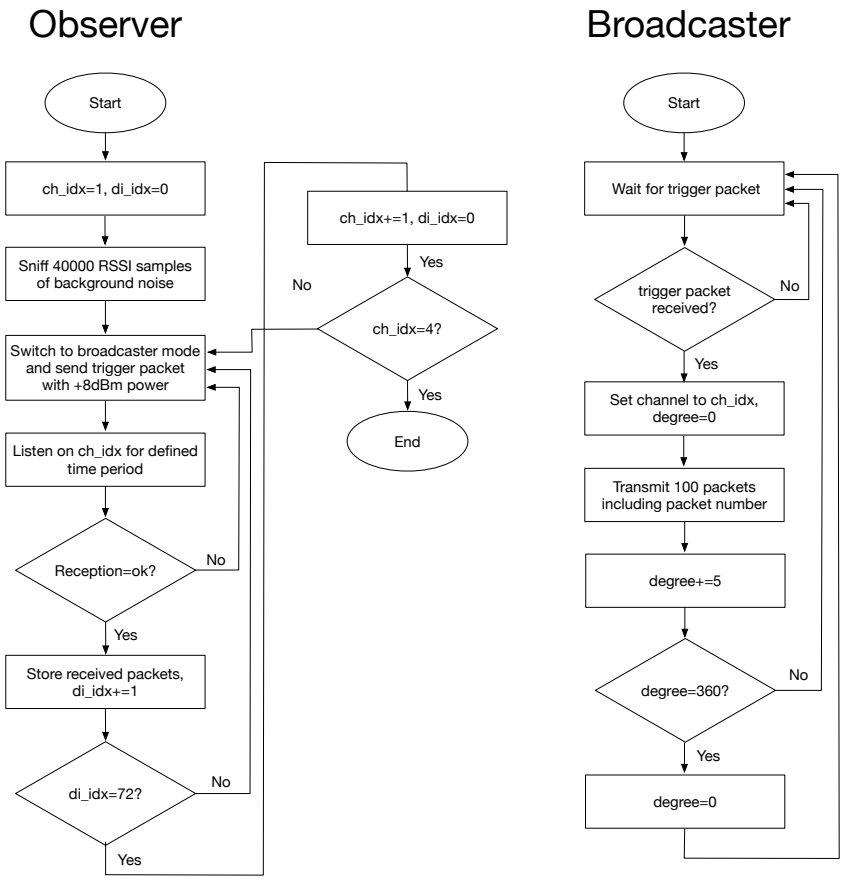


Fig. 4.8: Path anisotropy approach software design

4.6 Link Layer (LL) Implementation

The reason behind the implementation of the BLE LL is to solve: 1) few limitations presented by the BLE protocol stack such as the inability to scan on a specific advertising channel and the inability to transmit for a short period of time (less than 100 ms) using the Non-connectable undirected advertisements [49]. (2 issues in timers synchronization encountered while using the software stack provided by Nordic. The nRF52840 System on Chip (SoC) Fig. 4.9 supports multiple radio features which covers standards such as BLE and IEEE 802.15.4 based protocols. It is also possible to access the radio in the 2.4 GHz frequency band which supports the GFSK modulation. However, since my focus is on path-loss and link quality estimation on specific channels therefore, I only implemented the one way transmission from the broadcaster to the observer without receiving the ACK and I did not cover the Adaptive Frequency Hopping (AFH) in this research.

The BLE LL has been implemented using the nRF5 SDK v13.0.0 which is provided by Nordic Semiconductor [79]. The SDk contains various examples that show how to use the hardware peripherals of the nRF52840 SoC and the implementation was based on the radio example which is located in <SDKInstallationFolder>\examples\peripheral\radio. The example contains two parts, one is dedicated for the transmitter while the second is

dedicated for the receiver. The radio example was modified and extended according to the requirements of the implementation and embedded C programming was used through Keil MDK_ARM integrated development environment [74]. The rest of this section discusses briefly the most important steps of the implementation.

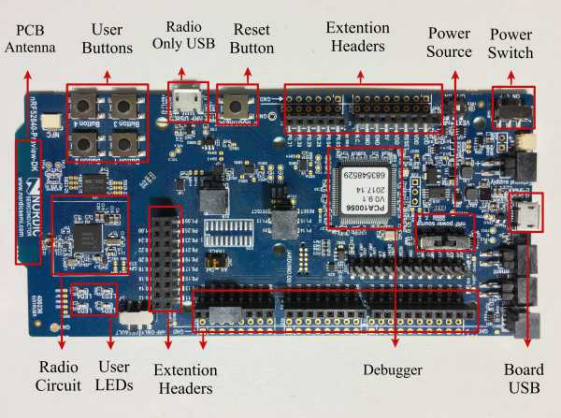


Fig. 4.9: Overview of the nRF52840 development kit

On-air Packet configuration

The first step is to define the required parameters of the radio packet according to BLE standard [49]. Packet structure defines are listed in code 4.1. The on-air packet of the nRF52840 radio includes the following fields: PREAMBLE, RADIO ADDRESS, CI, TERM1, SO, LENGTH, S1, PAYLOAD, CRC and TERM2 as illustrated in Fig. 4.10. Radio packet configuration is done through configuring the Packet Configuration (PCNF0) and Packet Configuration (PCNF1) radio registers.

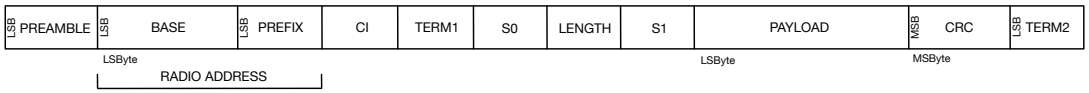


Fig. 4.10: Radio on-air packet structure [71]

• The preamble length for BLE 1Mbit mode is 1 byte and is configured via the Preamble Length (PLEN) field in the PCNF0 register.

• The radio address field will hold the advertising access address define by BLE standard which is 4 bytes long. It consists of two parts which are the base address and the address prefix where the combination of these two parts will form the advertising access address which is fixed to 0x8E89BED6.

• The fields CI, TERM1 and TERM2 shall be omitted when radio operates on BLE 1 Mbit PHY.

• The fields S0, LENGTH and S1 are used as packet control fields. S0 and LENGTH fields will be used to hold the advertising packet PDU header as explained already Fig. 2.10 which

is 16 bits long. The length of S0 field is set to 8 bits as well as for the LENGTH field. S1 field shall be omitted since it is not required for the packet configuration, therefor it is set to 0.

• The PAYLOAD field will contain the actual payload data of the packet. The length of the payload will vary dynamically depending on the selected packet size therefore, it is set initially to the maximum allowed length which is 255 bytes.

• CRC is the last field in the packet with 3 bytes long.

```
#define PACKET_S0_FIELD_LENGTH          1UL     // in bytes
#define PACKET_S1_FIELD_LENGTH          0UL     // in bits
#define PACKET_LENGTH_FIELD_LENGTH      8UL     // in bits
#define PACKET_CI_FIELD_LENGTH          2UL     // in bits
#define PACKET_TERM_FIELD_LENGTH        3UL     // in bits
#define PACKET_BASE_ADDRESS_LENGTH      3UL     // in bytes
#define PACKET_STATIC_LENGTH            0UL     // in bytes
#define PACKET_PAYLOAD_MAXSIZE          255UL   // Maximum allowed payload
#define PACKET_PAYLOAD_MAXSIZE_LE_MIN   7UL     // Minimum packet size
#define PACKET_PAYLOAD_MAXSIZE_LE_ADV   37UL    // Average packet size (Adv)
#define PACKET_PAYLOAD_MAXSIZE_LE_DATA  255UL   // maximum packet size (Data)

#define PDU_HEADER_LENGTH          2UL     // PDU type and length
#define PDU_HEADER_S0_VALUE        2UL     // ADV_NONCONN_IND (0010)
#define PDU_HEADER_S1_VALUE        0UL     // S1 header value
#define PDU_LENGTH_LE_MIN          9UL     // minimum packet size + PDU
#define PDU_LENGTH_LE_ADV          39UL    // ADV packet size + PDU
#define PDU_LENGTH_LE_DATA         257UL   // data packet size + PDU

#define ADV_ACCESS_ADDR     0x8E89BED6     // ADV access address
#define LE_ADDR_LENGTH      6              // length of device address
```

Source Code 4.1: Defines of the LL implementation

Radio Configuration

Before any configurations take place, the radio has to be powered up and all events in the radio have to be cleared as shown in code 4.2

```
void radio_power_up()
{
  NRF_RADIO->POWER = 1U;               // Power up the radio
  NRF_RADIO->EVENTS_DISABLED = 0U;     // Clear events
}
```

Source Code 4.2: Powering up the radio

Radio address configuration:

As mentioned before, radio address field on the nRF52840 consists of two parts, base address and address prefix. The address prefix (PREFIX0) length on nRF52840 is 1 octet, it will hold the first octet of the advertising access address which is (0000008E) where the base address (BASE0) will hold the rest of the octets (89BED600) after being truncated from LSByte. Additionally, to enable transmission and reception on the previously defined access

address, the TXADDRESS and RXADDRESSES registers are configured to use logical address 0. The code 4.3 below shows how the access address is configured.

```
1  void radio_addr_init()
2  {
3   NRF_RADIO->BASE0       = 0x89BED600;
4   NRF_RADIO->PREFIX0     = 0x0000008E;
5   NRF_RADIO->TXADDRESS   = 0x00; // enable transmission on logical address 0
6   NRF_RADIO->RXADDRESSES = 0x01; // enable reception on logical address 0
7  }
```

Source Code 4.3: Initiating radio access address

CRC configuration:

The length of the CRC field is configured via CRCCNF register with the access address skipped during CRC calculation. The polynomial function of CRC is set to 0x00065B via CRCPOLY register and the initial value is set to 0x555555 via CRCINIT register as shown in the code 4.4.

```
1  void radio_CRC_init()
2  {
3   NRF_RADIO->CRCCNF  = (RADIO_CRCCNF_LEN_Three << RADIO_CRCCNF_LEN_Pos) |
4                        (RADIO_CRCCNF_SKIPADDR_Skip << RADIO_CRCCNF_SKIPADDR_Pos);
5   NRF_RADIO->CRCINIT = 0x555555;
6   NRF_RADIO->CRCPOLY = 0x00065B;
7  }
```

Source Code 4.4: Initiating the CRC polynomial function

PCNF0 and PCNF1 registers configurations

As mentioned erlier, radio packet configuration is done through configuring PCNF0 and PCNF1 registers. Code 4.5 shows how the configuration of PCNF0 register is made with respect to the previously defined parameters in 4.1.

```
1  void radio_set_pcnf0_configuration(uint8_t ble_mode)
2  {
3   NRF_RADIO->PCNF0 = (PACKET_S0_FIELD_LENGTH     << RADIO_PCNF0_S0LEN_Pos) |
4                      (PACKET_S1_FIELD_LENGTH     << RADIO_PCNF0_S1LEN_Pos) |
5                      (PACKET_LENGTH_FIELD_LENGTH << RADIO_PCNF0_LFLEN_Pos);
6
7   switch (ble_mode)
8   {
9    case BLE_1MBIT:
10        NRF_RADIO->PCNF0 |= (RADIO_PCNF0_PLEN_8bit << RADIO_PCNF0_PLEN_Pos);
11        break;
12
13   case BLE_2MBIT:
14        NRF_RADIO->PCNF0 |= (RADIO_PCNF0_PLEN_16bit << RADIO_PCNF0_PLEN_Pos);
15        break;
16
17   case BLE_LR500KBIT:
18   case BLE_LR125KBIT:
19        NRF_RADIO->PCNF0 |= (PACKET_CI_FIELD_LENGTH << RADIO_PCNF0_CILEN_Pos) |
```

```
20                              (PACKET_TERM_FIELD_LENGTH << RADIO_PCNF0_TERMLEN_Pos)
21                            | (RADIO_PCNF0_PLEN_LongRange << RADIO_PCNF0_PLEN_Pos);
22        break;
23
24  }
25 }
```

Source Code 4.5: Configurations of PCNF0 register

In PCNF1 register, the requirements of BLE standard such as packet maximum payload size (255 bytes), packet static length (0 byte), bit ordering of the packet (Little Endian) and data whitening (Enabled) are configured as shown in code 4.6. In addition to that, the base address field length shall be configured as well as discussed before.

```
1  void radio_ble_set_pcnf1_configuration(void)
2  {
3    NRF_RADIO->PCNF1 = ((PACKET_PAYLOAD_MAXSIZE      << RADIO_PCNF1_MAXLEN_Pos)  |
4                        (PACKET_STATIC_LENGTH        << RADIO_PCNF1_STATLEN_Pos) |
5                        (PACKET_BASE_ADDRESS_LENGTH  << RADIO_PCNF1_BALEN_Pos)   |
6                        (RADIO_PCNF1_ENDIAN_Little   << RADIO_PCNF1_ENDIAN_Pos)  |
7                        (RADIO_PCNF1_WHITEEN_Enabled << RADIO_PCNF1_WHITEEN_Pos)
8                       );
9
10 }
```

Source Code 4.6: Configurations of PCNF1 register

Setting radio operating mode

Radio operating mode is configured via MODE register and is set up according to the required mode as shown in code 4.7.

```
1  void radio_ble_set_mode(uint8_t mode)
2  {
3   switch (mode)
4    {
5     case BLE_1MBIT:
6          NRF_RADIO->MODE = (RADIO_MODE_MODE_Ble_1Mbit << RADIO_MODE_MODE_Pos);
7          break;
8
9     case BLE_2MBIT:
10         NRF_RADIO->MODE = (RADIO_MODE_MODE_Ble_2Mbit << RADIO_MODE_MODE_Pos);
11         break;
12
13    case BLE_LR500KBIT:
14         NRF_RADIO->MODE = (RADIO_MODE_MODE_Ble_LR500Kbit << RADIO_MODE_MODE_Pos);
15         break;
16
17    case BLE_LR125KBIT:
18         NRF_RADIO->MODE = (RADIO_MODE_MODE_Ble_LR125Kbit << RADIO_MODE_MODE_Pos);
19         break;
20   }
21 }
```

Source Code 4.7: Setting radio operating mode

CHAPTER 5

Experimental Results

This chapter presents and discusses the obtained results in this research. First, Section 5.1 presents the results of the background noise that was measured during the experiment. Then Section 5.2 presents the results obtained from path loss approach. Finally Section 5.3 presents and discusses the results obtained from path anisotropy approach.

5.1 Background Noise

The source of noise in wireless communications can be environmental such as humidity or it can be interference with other devices operating on the same frequency [80]. measuring the background noise of the environment is important in order to characterize its impact on RSS.

Results Discussion

The results of the background noise for the ADV channels are shown in Fig. 5.2 for channel 37, Fig. 5.3 for channel 38, and Fig. 5.4 for channel 39. The results show 40 thousand samples that have been taken during the experiments. As can be seen in the figures, noise variation in outdoor is not significant while indoor environment suffers from interference caused mostly by Wi-Fi. The outdoor result comparison between Nordpark and Stadtpark shows negligible change. This means the source of noise in indoor environments is due to interferes. IEEE802.11b/g/n standard is the common source of this interference. The standard has 11 channels with 22MHz width but only channel 1, 6 and 11 are commonly used due to none-overlapping feature. However, noise emission caused by these channels are not limited to 22MHz boundary. In Fig. 5.1, it can be seen that BLE channel 38 gets effected by channel 6 of IEEE802.11b/g/n. This explains the large noise values in channel 37 and 38 compared to channel 39 in indoor environments. In BLE, channel 39 has been placed apart from other channels and Wi-Fi has minimum effect on it.

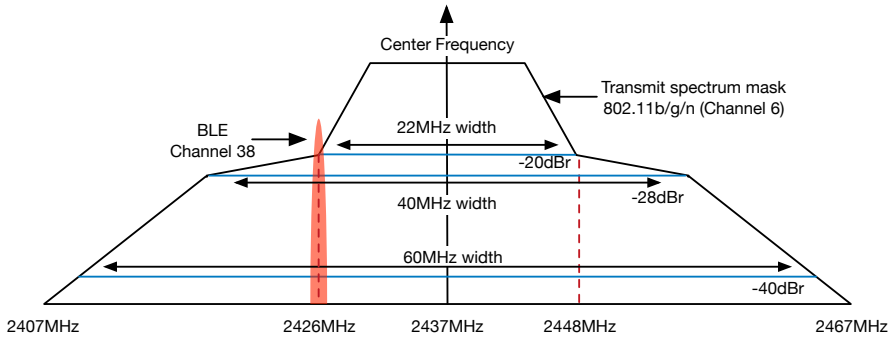


Fig. 5.1: Channel 6 for IEEE802.11b/g/n versus BLE ADV channel 38

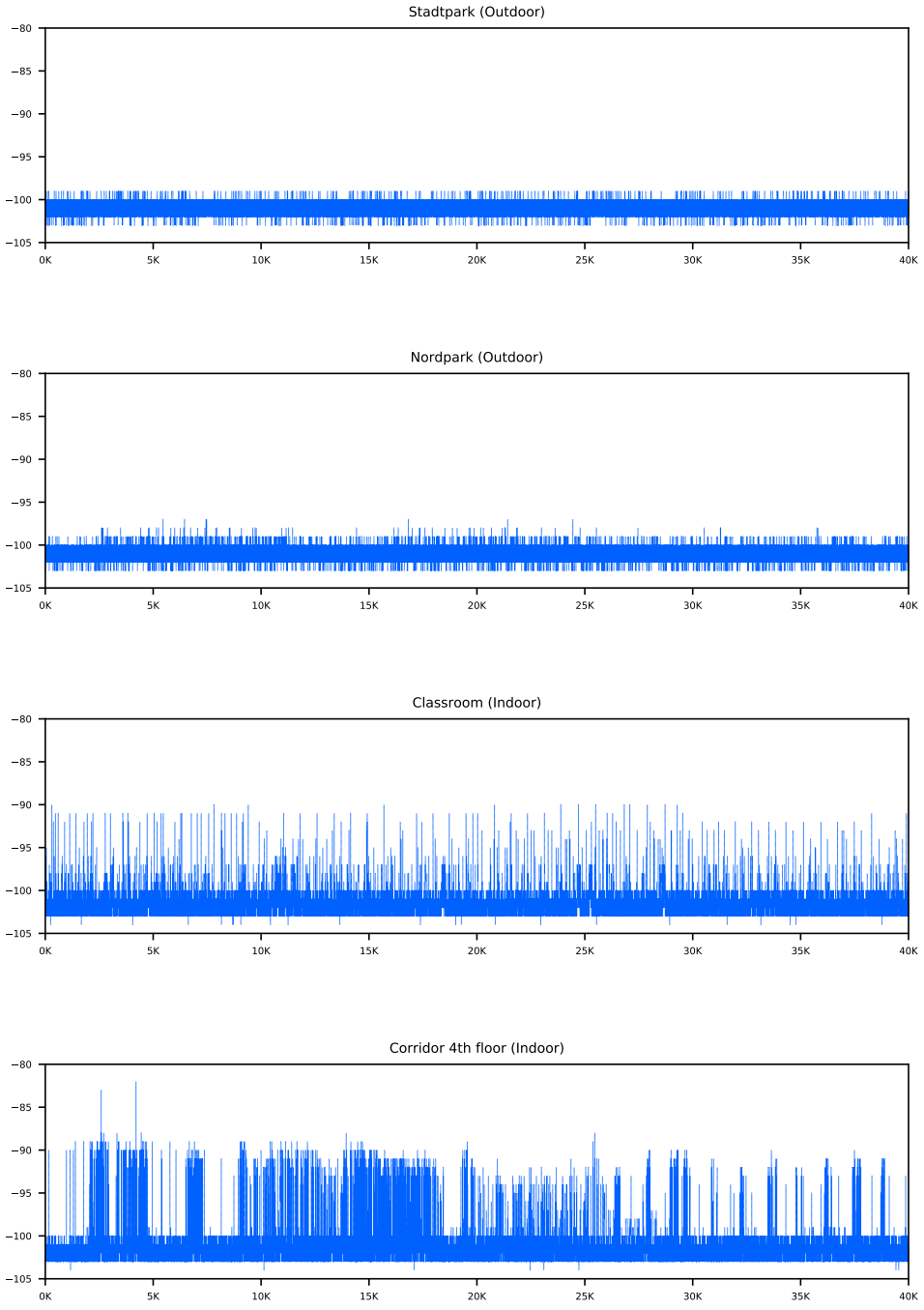


Fig. 5.2: Noise on channel 37

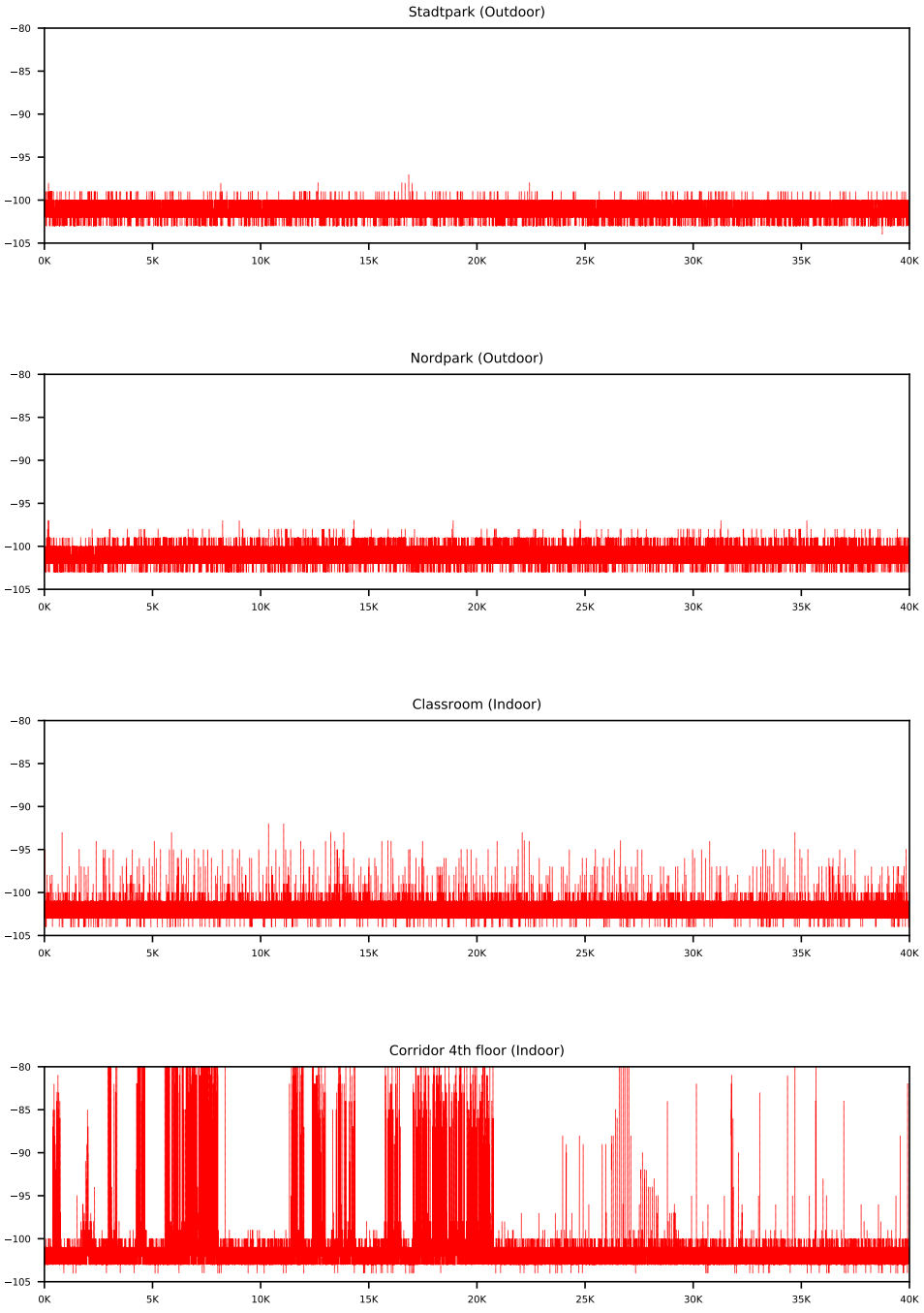


Fig. 5.3: Noise on channel 38

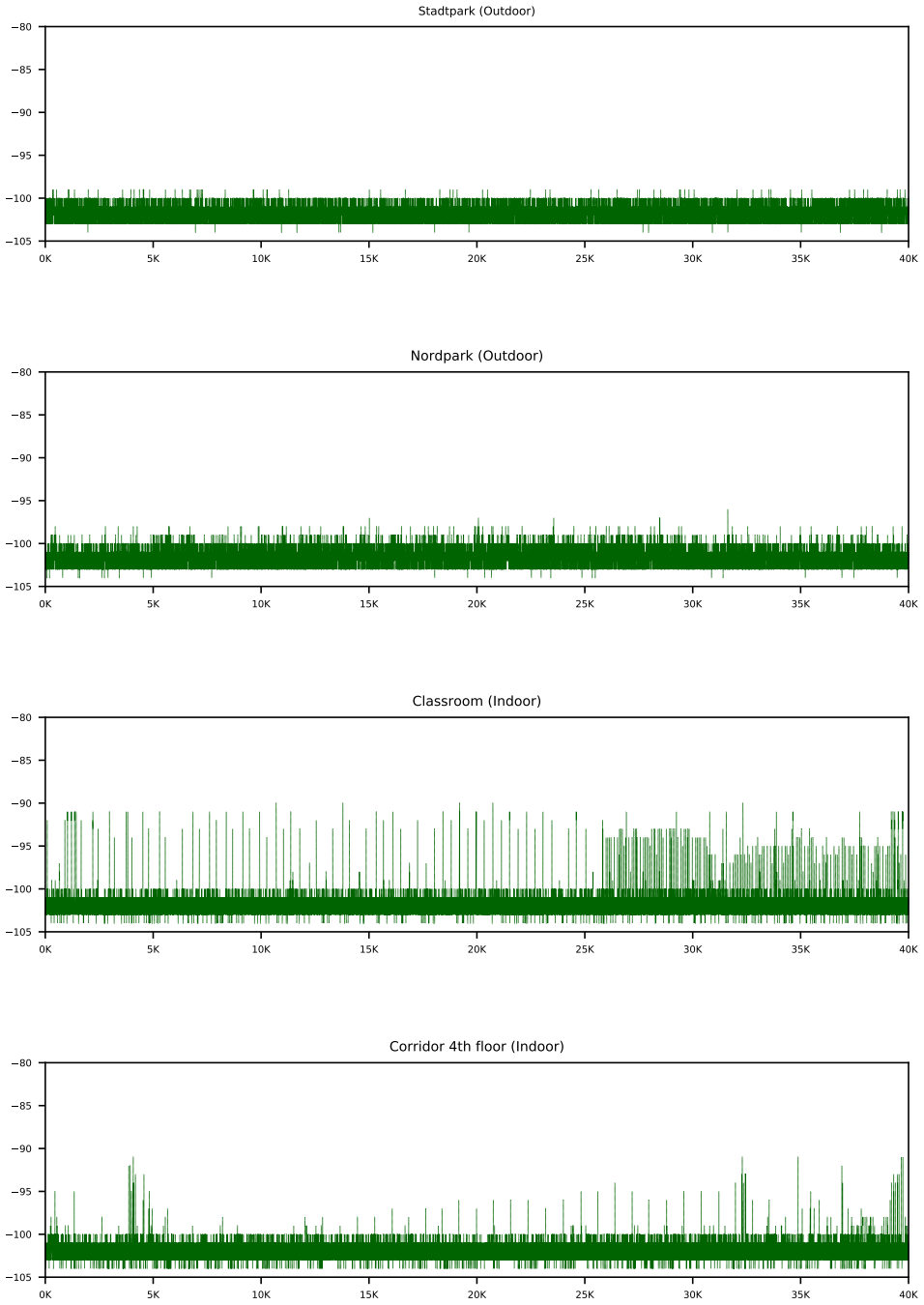


Fig. 5.4: Noise on channel 39

5.2 Path Loss

Box Plot

Since box plots are used to show the variation of RSS, it is appropriate to provide and over view of them. Box plots are a way to visually display data sets in order to show their distribution and where exactly most of the values lie [82]. This is done by characterizing data samples into four quartiles. An illustration of a box plot is shown in Fig. 5.5. The box in the middle is called the inter quartile range (IQR= Q3-Q1) and it represents the middle 50% of the data where the center of these data is denoted by the median which has a green color. The upper quartile (Q3) represents 25% of IQR above the median while the lower quartile (Q1) represents 25% of IQR under the median. The lines extending from the IQR box are called whiskers, and they extend to the minimum and maximum value of the data set unless outliers exist. Outliers are either much bigger than Q3 or much smaller than Q1. The above outliers are any value that is bigger than Q3+1.5(IQR) while lower outliers are any value that is smaller than Q1-1.5(IQR).

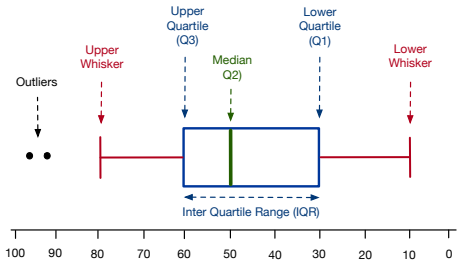


Fig. 5.5: Overview of box plot components

Standard Deviation

In order to calculate the path loss of BLE ADV channels, the standard deviation has been used. The standard deviation σ [83] shows the density of the observed data from the mean value μ. Fig. 5.6 illustrates a set of observations that are normally distributed which is the case of RSS. One standard deviation from the mean μ (on X axis) in both right and left sides represents around 68% of the data. And two standard deviations represent roughly 95% of the data while three standard deviations represent around 99%.

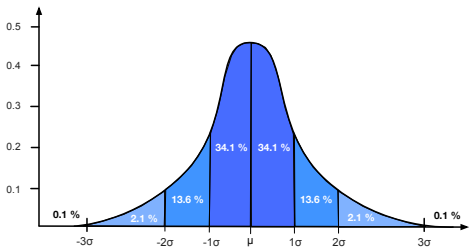


Fig. 5.6: Normal distribution and standard deviation

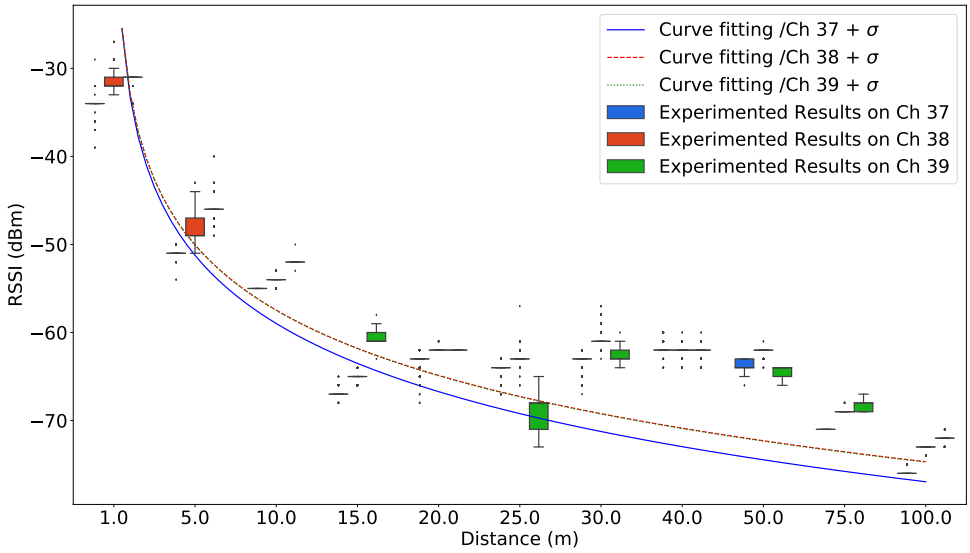
Curve Fitting

As we discussed in Ch 3, in order to optimize the value of η in Formula 2.10, we used the TRRLS which finds the curve that best fits all observed RSS. The results obtained for outdoor environments are shown in Fig. 5.7 while for indoor environments, they are shown in Fig. 5.8. The plots show the collected RSS samples for ADV channels represented by colored box plots at each defined distance. The x-axis indicates the distance between broadcaster and observer, and y-axis represents RSS from the receiver's point of view. The figures show the observation and optimization for 0dBm transmit power while the detailed information for all the environments and transmit powers is summarized in Table 5.1.

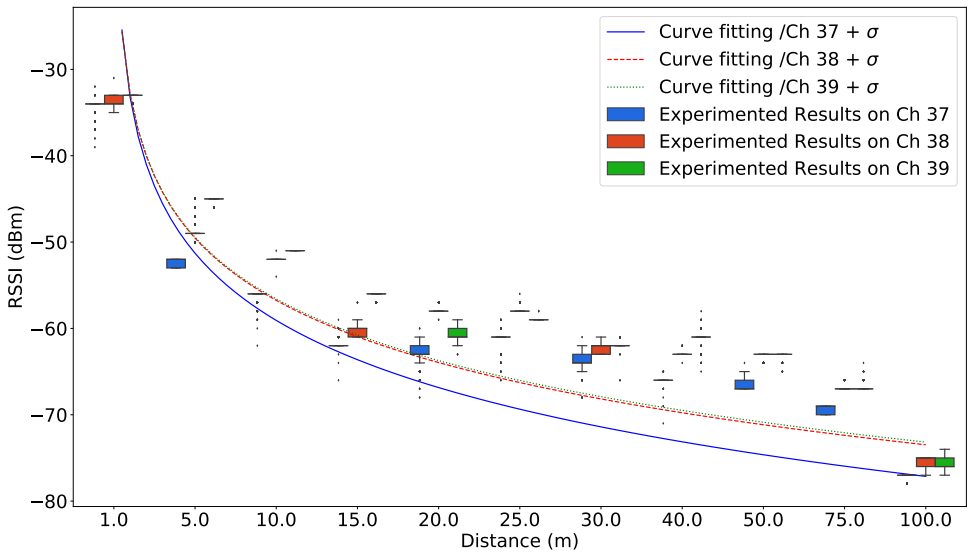
Results Discussion

The main observation from Fig. 5.7 and in Fig. 5.8 is that ADV channels are behaving differently due to frequency difference, narrow width and possibility of interference. This has been also reported in [56]. In Fig. 5.7 the slight variation of RSS may be caused by fading due to ground reflection or hardware inaccuracy. Additionally, the RSS value for distances 30, 40 and 50 meter is almost the same. This phenomenon is known as signal aliasing [84] where different points that are far away from each other may have similar RSS characteristics. The reason for signal aliasing is also multipath and the properties of the environment. In [84], an algorithm has been developed to tackle this issue. Almost the same phenomena exists in Nordpark Fig. 5.7b. Although Nordpark has trees present as obstacles between the broadcaster and observer, we can see that the trees did not effects much on RSS. Another common observation of all environments is that for small distances, RSS decays fast while it decays slowly for longer distances.

Comparing outdoor results with indoor, outdoor environment show a stable decay in signal power versus distance, and the indoor environments show significantly higher variations around the fitted lines particularly in the corridor environment Fig. 5.8b. This can be related to the narrow width of the corridor and the effects of windows which may cause signal scattering leading to a high multipath effects. For the classroom Fig. 5.8a, we can see that RSS behaves better than in the corridor. The reason could be the classroom is wider than the corridor in terms of width reduces the multipath effects. In general, indoor environments cause higher shadowing and multipath effects due to the existence of obstacles such as walls. The shadowing and multipath effects result in a random behavior and may cause either signal attenuation or amplification [15]. Signal amplification occurs when the phases of the overlapping signals are similar, otherwise, attenuation happens. Therefore, as a change in distance results in a new wireless channel between the broadcaster and observer, we can observe significant RSS variations around the fitted lines. The second cause of indoor variations is Wi-Fi interference, which directly contributes to a node's perception of RSS. Another reason behind RSS fluctuations is signal propagation and antenna anisotropy. Studies such in [16] shows that signal propagation around a transmitter, as well as the capability of an antenna to capture a signal arriving from different directions, are not anisotropic. Therefore, as movement of nodes changes the angles of signals arrival, different RSS values are observed. Furthermore, the results of this study support the importance of channel characterization under various conditions.

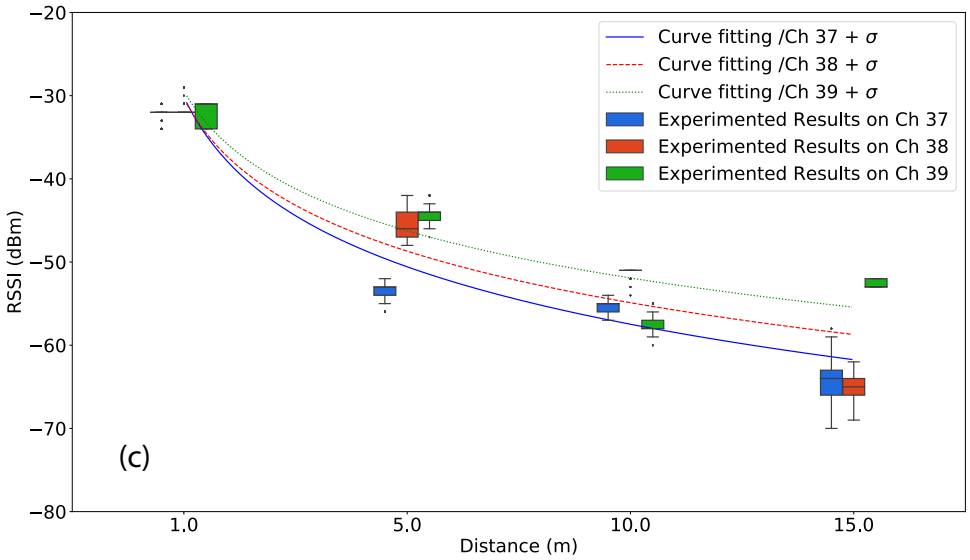


a) Stadtpark

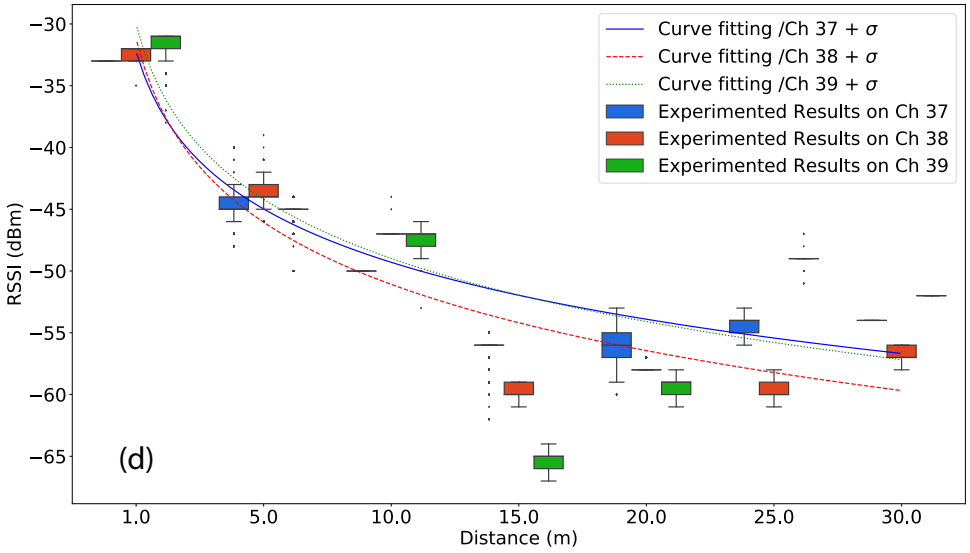


b) Nordpark

Fig. 5.7: Curve fitting of all three channels outdoors



a) Classroom



b) Corridor

Fig. 5.8: Curve fitting of all three channels indoors

Table 5.1: Summary of the L-NSM Parameters

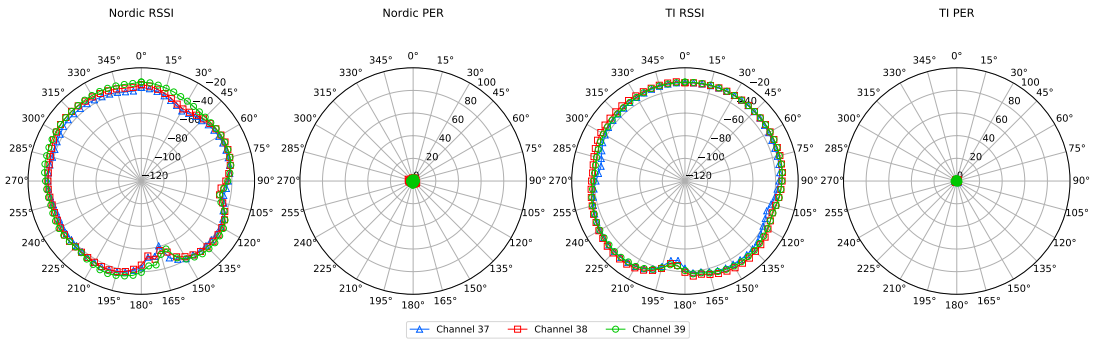
Power	Parameter	Channel	Stadtpark	Nordpark	Classroom	Corridor
+8 dBm	η	37	1.98	1.99	2.43	1.69
		38	2.09	1.90	2.35	1.82
		39	2.00	1.87	2.09	1.75
	σ	37	0.91	0.76	1.76	1.18
		38	0.46	0.33	0.89	0.44
		39	0.46	0.36	0.27	0.49
	$PL(1)$	37	34	34	32	32
		38	32	33	31	32
		39	31	33	31	31
0 dBm	η	37	2.05	2.06	2.62	1.64
		38	2.07	1.87	2.35	1.91
		39	2.14	1.91	2.16	1.82
	σ	37	0.48	0.56	1.13	0.57
		38	0.58	0.39	0.99	0.56
		39	0.59	0.29	0.97	0.73
	$PL(1)$	37	34	34	32	33
		38	32	34	32	32
		39	31	33	31	31
-8 dBm	η	37	2.02	2.03	2.62	1.62
		38	2.10	1.93	2.35	1.87
		39	2.03	1.82	2.16	1.77
	σ	37	0.30	0.36	1.09	0.64
		38	0.38	0.32	0.62	0.40
		39	0.31	0.33	0.33	0.30
	$PL(1)$	37	34	34	32	33
		38	31	33	31	32
		39	31	34	31	31
-20 dBm	η	37	2.06	2.03	2.65	1.71
		38	2.07	1.83	2.30	1.83
		39	1.98	1.79	2.06	1.78
	σ	37	0.42	0.45	0.67	0.23
		38	0.33	0.39	0.60	0.40
		39	0.39	0.25	0.63	0.41
	$PL(1)$	37	34	34	33	33
		38	32	34	32	33
		39	32	34	32	31

5.3 Path Anisotropy

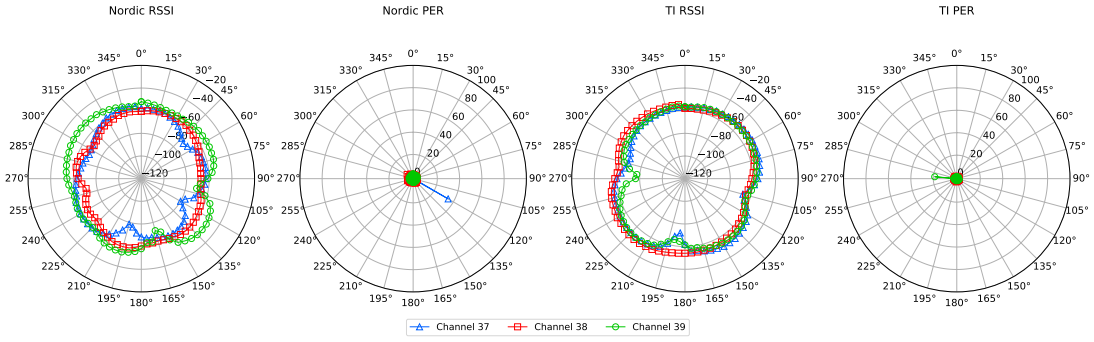
This Section presents the results obtained from path anisotropy experiment. As mentioned earlier, the aim of this experiment was to analyze the effects of antenna orientation and hardware heterogeneity on RSS. The experiment was performed in two indoor environments. In the classroom and in the corridor using two different nodes as broadcasters. Nordic nRF52840 and TI CC2640R2f. Moreover, the tested transmission power were 0dBm and -20dBm. The results are presented in Fig. 5.9 for the classroom, distances 1 and 15 m. Where Fig. 5.10 presents the results obtained in the corridor, distances 1 and 20m. The detailed observation values are present in Table 5.2.

Results Discussion

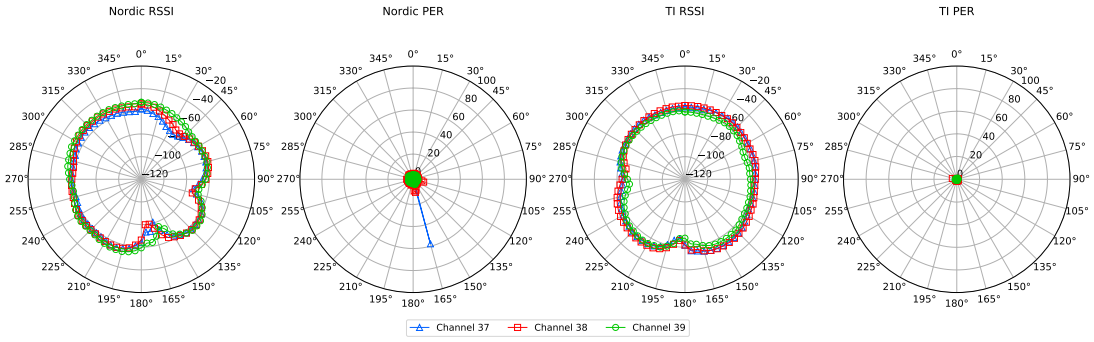
As expected, RSS varies by the rotation of the node antenna, and in lower powers, it results in a high packet loss. The observation shows that TI CC2640Rf2 has more stable performance in comparison to Nordic nRF52840. This also can be seen in Fig. 5.9b. Despite the different distance and transmission powers, the radio of both devices has the same patterns in both environments, for example, the drop in RSS for TI happens between degree 180 and 195 most of the times. This can be explained by the effect of reflection caused by obstacles. The same phenomena can be seen for Nordic where the drops of RSS tends to be always at degrees between 150 and 165. For example, in comparison between Fig. 5.9d and Fig. 5.10d for the two environments, we can see that the PER of Nordic on distance 15m is more than on distance 20m although the later is more far in terms of distance.



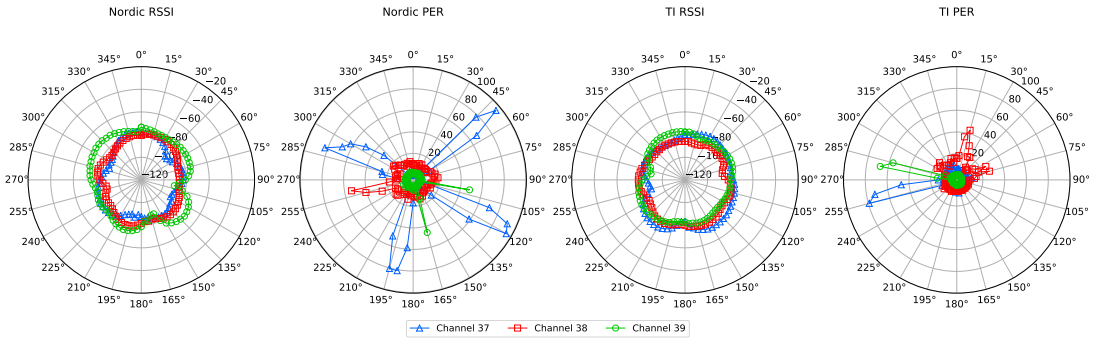
a) Distance 1 meter, 0dBm Tx power



b) Distance 15 meter, 0dBm Tx power

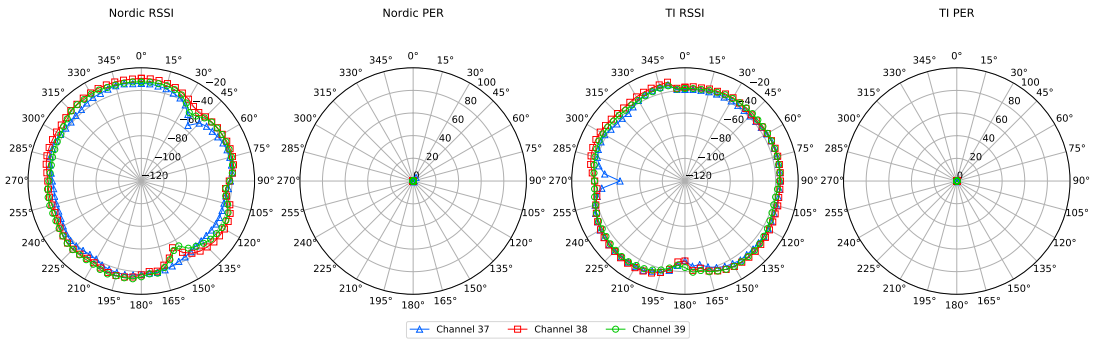


c) Distance 1 meter, -20dBm Tx power

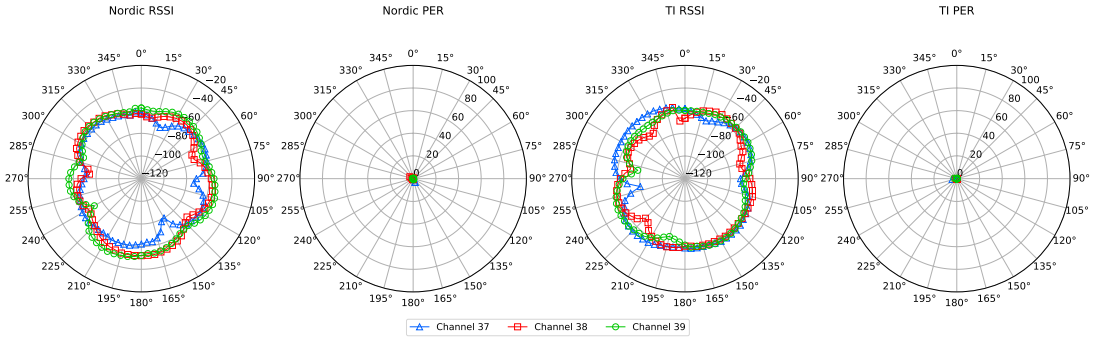


d) Distance 15 meter, -20dBm Tx power

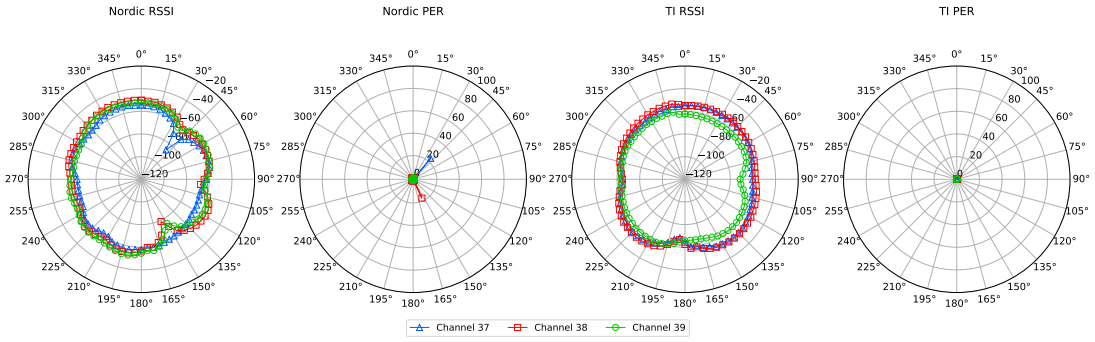
Fig. 5.9: Path anisotropy classroom results



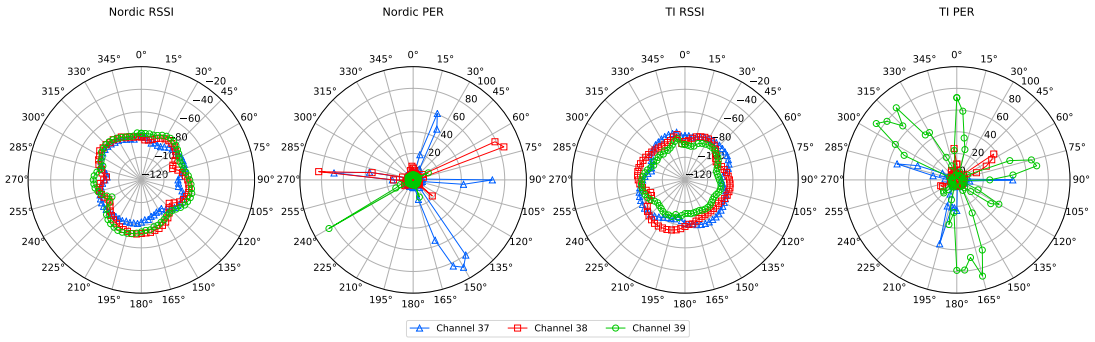
a) Distance 1 meter, 0dBm Tx power



b) Distance 20 meter, 0dBm Tx power



c) Distance 1 meter, -20dBm Tx power



d) Distance 20 meter, -20dBm Tx power

Fig. 5.10: Path anisotropy Corridor 4th floor results

Table 5.2: Summary of path anisotropy results

Tx	Parameter	Device	Classroom									Corridor 4th floor								
	Distance		1 m			5 m			15 m			1 m			5 m			10 m			20 m		
	CH		37	38	39	37	38	39	37	38	39	37	38	39	37	38	39	37	38	39	37	38	39
0 dBm	μ[1]	Nordic	40.9	39.5	37.5	53.3	50.6	48.9	64.6	62.6	55.6	39.2	35.6	38.0	57.3	56.3	50.7	55.1	53.5	60.4	63.1	59.9	57.0
		TI	36.6	34.6	35.2	48.2	45.6	49.0	56.9	55.1	58.2	37.5	35.3	36.5	55.5	53.3	57.0	58.2	58.2	55.4	58.9	61.3	60.3
	σ[2]	Nordic	4.26	5.33	4.87	4.88	4.35	3.85	5.84	3.12	4.63	4.17	4.83	5.87	5.77	3.95	3.22	5.52	5.57	4.85	4.67	5.39	4.15
		TI	4.22	2.81	2.99	4.47	4.56	2.74	5.00	2.93	5.27	4.01	3.61	2.23	4.74	4.66	5.77	5.20	4.94	3.56	4.94	4.82	4.77
	PER[3]	Nordic	085	224	175	053	160	147	105	112	122	001	001	003	015	003	010	005	012	009	007	000	007
		TI	042	048	083	040	054	051	024	060	050	000	001	002	002	052	120	001	011	000	003	005	001
-20 dBm	μ	Nordic	61.4	59.6	57.6	74.2	71.8	69.7	84.2	82.9	76.1	60.5	57.1	57.3	77.6	75.7	71.2	76.2	74.4	81.2	82.9	79.9	77.8
		TI[4]	57.4	57.1	61.7	72.1	72.2	73.4	77.9	79.9	80.5	58.2	57.1	63.6	72.1	73.6	71.3	73.0	73.1	78.2	81.7	81.7	87.4
	σ	Nordic	5.77	5.84	5.26	4.18	4.87	4.86	4.35	3.04	4.25	5.12	5.53	4.66	5.04	4.24	4.45	5.15	5.24	3.95	3.63	4.58	4.09
		TI	2.74	3.36	3.50	4.00	2.98	3.83	4.72	4.45	3.48	3.28	3.76	2.22	4.17	4.76	2.92	4.00	2.92	5.11	3.75	3.99	3.19
	PER	Nordic	123	149	072	062	368	171	1317	961	300	008	088	000	328	005	000	241	017	660	809	328	115
		TI	018	041	022	179	344	070	532	921	286	000	005	001	053	185	004	033	005	127	467	303	1779

[1] Average RSS of whole rotation (-dBm)
[2] Standard deviation of whole rotation
[3] Number of lost packets out of 7200 packets for whole rotation
[4] On TI CC2640R2f, -20dBm Tx power option is not available therefor -21dBm has been used instead

CHAPTER 6

Conclusion

6.1 Summary and conclusion

The main aim of this research was to analyze the characteristics of BLE ADV channels for indoor positioning, and to propose a robust path loss model to overcome issues such as interference, obstacles, and hardware design which lowers the accuracy of point-to-point distance estimation. Extensive hardware experiments have been conducted in different environments, with different transmission power settings and with the consideration of the impact of antenna orientation on RSS. The importance of BLE ADV channel characterization is presented. The presented results show that BLE ADV channels have different gains. Additionally they show the complexity of indoor environments and their considerable impact on RSS variation due to multipath fading and interference with other presented devices. The comparison of outdoor and indoor results highlights this claim. Although ADV channels are placed in a way that reduces the interference with channel 1, 6 and 11, Wi-Fi still has an effect on these channels. Moreover, the effect of antenna orientation and the heterogeneity of the hardware indicate the amount of variation that can be caused by hardware design. The observation later have been modeled by curve fitting optimization to achieve the optimal parameters of the L-NSM for each condition. The outcome of this research can be employed in many applications, simulation tools and positioning algorithm design.

6.2 Future work

This research can be extended by analyzing the optimal transmit power to increase the efficiency of L-NSM and by conducting more experiments with different hardware. In addition, a blocked line of sight and mobility effects can be analyzed in future research.

Bibliography

[1] In Lee and Kyoochun Lee. The internet of things (iot): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4):431–440, 2015.

[2] Gartner forecasts. `https://www.gartner.com/newsroom/id/3598917`. (visited on 25 January 2018).

[3] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on*, pages 257–260. IEEE, 2012.

[4] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung. Emerging wireless technologies in the internet of things: a comparative study. *arXiv preprint arXiv:1611.00861*, 2016.

[5] Naresh Gupta. *Inside Bluetooth Low Energy, Second Edition*. Artech House, London, United Kingdom, 2016.

[6] Getting Started with iBeacon. `https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf`.

[7] Markus Koühne and Jürgen Sieck. Location-based services with ibeacon technology. In *Artificial Intelligence, Modelling and Simulation (AIMS), 2014 2nd International Conference on*, pages 315–321. IEEE, 2014.

[8] The Rise of Beacon Technology. `https://blog.bluetooth.com/the-rise-of-beacon-technology`. (visited on 30 January 2018).

[9] Indoor Location Market by Component Deployment Mode, Application, Vertical, and Region - Global Forecast to 2022.". `https://www.marketsandmarkets.com/Market-Reports/indoor-positioning-navigation-ipin-market-989.html`. (visited on 30 January 2018).

[10] Dharma Prakash Agrawal and Qing-An Zeng. *Introduction to Wireless and Mobile Systems, Fourth Edition*. Cengage Learning, Boston, USA, 2016.

[11] Hui Liu, Houshang Darabi, Pat Banerjee, and Jing Liu. Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 37(6):1067–1080, 2007.

[12] Subrata Goswami. *Indoor location technologies*. Springer, New York, USA, 2013.

[13] Theodore Rappaport. *Wireless Communications: Principles and Practice, Second Edi-*

tion. Pearson, Delhi, India, 2010.

[14] Gang Zhou, Tian He, Sudha Krishnamurthy, and John A Stankovic. Models and solutions for radio irregularity in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(2):221–262, 2006.

[15] Kaveh Pahlavan and Allen H. Levesque. *Wireless Information Networks, Second Edition*. John Wiley Sons, New Jersey, USA., 2005.

[16] Behnam Dezfouli, Marjan Radi, Shukor Abd Razak, Tan Hwee-Pink, and Kamalrulnizam Abu Bakar. Modeling low-power wireless communications. *Journal of Network and Computer Applications*, 51:102–126, 2015.

[17] Rainer Mautz. Indoor positioning technologies. 2012.

[18] Paramvir Bahl and Venkata N Padmanabhan. Radar: An in-building rf-based user location and tracking system. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 775–784. Ieee, 2000.

[19] Thomas King, Stephan Kopf, Thomas Haenselmann, Christian Lubberger, and Wolfgang Effelsberg. Compass: A probabilistic indoor positioning system based on 802.11 and digital compasses. In *Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation & characterization*, pages 34–40. ACM, 2006.

[20] Sunkyu Woo, Seongsu Jeong, Esmond Mok, Linyuan Xia, Changsu Choi, Muwook Pyeon, and Joon Heo. Application of wifi-based indoor positioning system for labor tracking at construction sites: A case study in guangzhou mtr. *Automation in Construction*, 20(1):3–13, 2011.

[21] Estimote. `https://estimote.com`.

[22] Jingjing Yang, Zhihui Wang, and Xiao Zhang. An ibeacon-based indoor positioning systems for hospitals. *International Journal of Smart Home*, 9(7):161–168, 2015.

[23] Xin-Yu Lin, Te-Wei Ho, Cheng-Chung Fang, Zui-Shen Yen, Bey-Jing Yang, and Feipei Lai. A mobile indoor positioning system based on ibeacon technology. In *Engineering in Medicine and Biology Society (EMBC), 2015 37th Annual International Conference of the IEEE*, pages 4970–4973. IEEE, 2015.

[24] Zhiqiang He, Binyue Cui, Wei Zhou, and Shigeki Yokoi. A proposal of interaction system between visitor and collection in museum hall by ibeacon. In *Computer Science & Education (ICCSE), 2015 10th International Conference on*, pages 427–430. IEEE, 2015.

[25] Moonok Choi, Wan-Ki Park, and Ilwoo Lee. Smart office energy management system using bluetooth low energy based beacons and a mobile app. In *Consumer Electronics (ICCE), 2015 IEEE International Conference on*, pages 501–502. IEEE, 2015.

[26] Andrea Corna, L Fontana, AA Nacci, and Donatella Sciuto. Occupancy detection via ibeacon on android devices for smart building management. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, pages 629–632. EDA Consortium, 2015.

[27] Fazli Subhan, Halabi Hasbullah, Azat Rozyyev, and Sheikh Tahir Bakhsh. Indoor positioning in bluetooth networks using fingerprinting and lateration approach. In *In-*

formation Science and Applications (ICISA), 2011 International Conference on, pages 1–9. IEEE, 2011.

[28] Yapeng Wang, Xu Yang, Yutian Zhao, Yue Liu, and Laurie Cuthbert. Bluetooth positioning using rssi and triangulation methods. In *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, pages 837–842. IEEE, 2013.

[29] Alan Bensky. *Wireless Positioning Technologies and Applications, Second Edition.* Artech House, London, United Kingdom, 2016.

[30] Suining He and S-H Gary Chan. Wi-fi fingerprint-based indoor positioning: Recent advances and comparisons. *IEEE Communications Surveys & Tutorials*, 18(1):466–490, 2016.

[31] Chris Rizos, Andrew G Dempster, Binghao Li, and James Salter. Indoor positioning techniques based on wireless lan. 2007.

[32] Jr. Robert W. Heath. *Introduction to Wireless Digital Communication.* Pearson Education, USA., 2017.

[33] Roy Want. Near field communication. *IEEE Pervasive Computing*, 10(3):4–7, 2011.

[34] Bhavneet Sidhu, Hardeep Singh, and Amit Chhabra. Emerging wireless standards-wifi, zigbee and wimax. *World Academy of Science, Engineering and Technology*, 25(2007):308–313, 2007.

[35] Institute of Electrical and Electronic Engineers. `https://www.ieee.org/index.html`.

[36] Nicolas Le Dortz, Florian Gain, and Per Zetterberg. Wifi fingerprint indoor positioning system using probability distribution comparison. In *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*, pages 2301–2304. IEEE, 2012.

[37] Atreyi Bose and Chuan Heng Foh. A practical path loss model for indoor wifi positioning enhancement. In *Information, Communications & Signal Processing, 2007 6th International Conference on*, pages 1–5. IEEE, 2007.

[38] Luca Mainetti, Luigi Patrono, and Ilaria Sergi. A survey on indoor positioning systems. In *Software, Telecommunications and Computer Networks (SoftCOM), 2014 22nd International Conference on*, pages 111–120. IEEE, 2014.

[39] Tareq Alhmiedat, Ghassan Samara, and Amer O Abu Salem. An indoor fingerprinting localization approach for zigbee wireless sensor networks. *arXiv preprint arXiv:1308.1809*, 2013.

[40] Wen-Hsing Kuo, Yun-Shen Chen, Gwei-Tai Jen, and Tai-Wei Lu. An intelligent positioning approach: Rssi-based indoor and outdoor localization scheme in zigbee networks. In *Machine Learning and Cybernetics (ICMLC), 2010 International Conference on*, volume 6, pages 2754–2759. IEEE, 2010.

[41] Chih-Ning Huang and Chia-Tai Chan. Zigbee-based indoor location system by k-nearest neighbor algorithm with weighted rssi. *Procedia Computer Science*, 5:58–65, 2011.

[42] Bluetooth Special Interest Group. `https://www.bluetooth.com/`.

[43] Silke Feldmann, Kyandoghere Kyamakya, Ana Zapater, and Zighuo Lue. An indoor

bluetooth-based positioning system: Concept, implementation and experimental evaluation. In *International Conference on Wireless Networks*, pages 109–113, 2003.

[44] AKM Mahtab Hossain and Wee-Seng Soh. A comprehensive study of bluetooth signal parameters for localization. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5. IEEE, 2007.

[45] Ling Pei, Ruizhi Chen, Jingbin Liu, Heidi Kuusniemi, Tomi Tenhunen, and Yuwei Chen. Using inquiry-based bluetooth rssi probability distributions for indoor positioning. *Journal of Global Positioning Systems*, 9(2):122–130, 2010.

[46] Bluetooth 4.0 Core Specification. `https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737`.

[47] Bluetooth 4.1 Core Specification. `https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=282159`.

[48] Bluetooth 4.2 Core Specification. `https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439`.

[49] Bluetooth v5.0 Core Specifications. `https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=421043&_ga=2.74406034.1850233121.1512529605-1686893139.1487028212`.

[50] GATT Specifications. `https://www.bluetooth.com/specifications/gatt`.

[51] Akiba Kevin Townsend, Carles Cufí and Robert Davidson. *Getting Started with Bluetooth Low Energy*. O'Reilly Media,, 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA., 2014.

[52] Praveen Kumar, Lohith Reddy, and Shirshu Varma. Distance measurement and error estimation scheme for rssi based localization in wireless sensor networks. In *Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on*, pages 1–4. IEEE, 2009.

[53] Long Cheng, Cheng-Dong Wu, and Yun-Zhou Zhang. Indoor robot localization based on wireless sensor networks. *IEEE Transactions on Consumer Electronics*, 57(3), 2011.

[54] Sujittra Boonsriwai and Anya Apavatjrut. Indoor wifi localization on mobile devices. In *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2013 10th International Conference on*, pages 1–5. IEEE, 2013.

[55] Abdalkarim Awad, Thorsten Frunzke, and Falko Dressler. Adaptive distance estimation and localization in wsn using rssi measures. In *Digital System Design Architectures, Methods and Tools, 2007. DSD 2007. 10th Euromicro Conference on*, pages 471–478. IEEE, 2007.

[56] Ramsey Faragher and Robert Harle. Location fingerprinting with bluetooth low energy beacons. *IEEE journal on Selected Areas in Communications*, 33(11):2418–2428, 2015.

[57] Mohamed Er Rida, Fuqiang Liu, Yassine Jadi, Amgad Ali Abdullah Algawhari, and Ahmed Askourih. Indoor location position based on bluetooth signal strength. In *Information Science and Control Engineering (ICISCE), 2015 2nd International Conference on*, pages 769–773. IEEE, 2015.

[58] Zhu Jianyong, Luo Haiyong, Chen Zili, and Li Zhaohui. Rssi based bluetooth low energy indoor positioning. In *Indoor Positioning and Indoor Navigation (IPIN), 2014 International Conference on*, pages 526–533. IEEE, 2014.

[59] Georgia Ionescu, Carlos Martınez de la Osa, and Michel Deriaz. Improving distance estimation in object localisation with bluetooth low energy. *SENSORCOMM*, 2014:45–50, 2014.

[60] Subha Viswanathan and Sreedevi Srinivasan. Improved path loss prediction model for short range indoor positioning using bluetooth low energy. In *SENSORS, 2015 IEEE*, pages 1–4. IEEE, 2015.

[61] Myungin Ji, Jooyoung Kim, Juil Jeon, and Youngsu Cho. Analysis of positioning accuracy corresponding to the number of ble beacons in indoor positioning system. In *Advanced Communication Technology (ICACT), 2015 17th International Conference on*, pages 92–95. IEEE, 2015.

[62] Faheem Zafari and Ioannis Papapanagiotou. Enhancing ibeacon based micro-location with particle filtering. In *Global Communications Conference (GLOBECOM), 2015 IEEE*, pages 1–7. IEEE, 2015.

[63] Andrew R Conn, Nicholas IM Gould, and Ph L Toint. *Trust region methods*, volume 1. Siam, 2000.

[64] Thomas F Coleman and Yuying Li. An interior trust region approach for nonlinear minimization subject to bounds. *SIAM Journal on optimization*, 6(2):418–445, 1996.

[65] George Tzeremes and CG Christodoulou. Use of weibull distribution for describing outdoor multipath fading. In *Antennas and propagation society international symposium, 2002. IEEE*, volume 1, pages 232–235. IEEE, 2002.

[66] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.

[67] Nordic nRF52840 preview development kit. `https://www.nordicsemi.com/eng/Products/nRF52840-Preview-DK`.

[68] Texas Instruments CC2640R2F LaunchPad development kit. `http://www.ti.com/tool/LAUNCHXL-CC2640R2`.

[69] TI CC2540 BLE Packet Sniffer. `http://www.ti.com/tool/PACKET-SNIFFER`.

[70] Nordic nRF52832 Datasheet. `http://infocenter.nordicsemi.com/pdf/nRF52832_PB_v1.4.pdf`.

[71] Nordic nRF52840 Datasheet. `http://infocenter.nordicsemi.com/pdf/nRF52840_PB_v1.0.pdf`.

[72] Texas Instruments CC2650 Datasheet. `http://www.ti.com/lit/ds/symlink/cc2650.pdf`.

[73] Texas Instruments CC2640R2F Datasheet. `http://www.ti.com/lit/ds/symlink/cc2640r2f.pdf`.

[74] Keil MDK for ARM microcontrollers. `http://www2.keil.com/mdk5/`.

[75] Texas Instruments Code Composer Studio IDE. `http://www.ti.com/tool/CCSTUDIO`.

[76] BLE 5 software stack of Nordic company. `https://www.nordicsemi.com/eng/nordic/Products/%20216%20nRF52840/S140-SD-v5/60624`.

[77] BLE 5 software stack of Texas Instruments company. `http://www.ti.com/tool/BLE-STACK`.

[78] J. D. Hunter. Matplotlib: A 2d graphics environment. *Computing In Science & Engineering*, 9(3):90–95, 2007.

[79] Nordic Semiconductor nRF5 SDK 13.0.0. `http://infocenter.nordicsemi.com/index.jsp?topic=%2Fcom.nordic.infocenter.sdk5.v13.0.0%2Findex.html`.

[80] Martin Haenggi, Jeffrey G Andrews, François Baccelli, Olivier Dousse, and Massimo Franceschetti. Stochastic geometry and random graphs for the analysis and design of wireless networks. *IEEE Journal on Selected Areas in Communications*, 27(7), 2009.

[81] Behnam Dezfouli, Marjan Radi, Kamin Whitehouse, Shukor Abd Razak, and Hwee-Pink Tan. Cama: Efficient modeling of the capture effect for low-power wireless networks. *ACM Transactions on Sensor Networks (TOSN)*, 11(1):20, 2014.

[82] Robert McGill, John W Tukey, and Wayne A Larsen. Variations of box plots. *The American Statistician*, 32(1):12–16, 1978.

[83] Saralees Nadarajah. A generalized normal distribution. *Journal of Applied Statistics*, 32(7):685–694, 2005.

[84] Youngjune Gwon, Ravi Jain, and Toshiro Kawahara. Robust indoor location estimation of stationary and mobile users. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 2, pages 1032–1043. IEEE, 2004.

Appendix