Tampere University

Tommi Kaivola

BLUETOOTH DIRECTION FINDING

Application to Local Positioning

Master of Science Thesis
Faculty of Management and Business
Examiner: Professor Tarmo Lipping
Examiner: University Lecturer Jari Turunen
October 2022

ABSTRACT

Tommi Kaivola: Bluetooth Direction Finding
Master of Science Thesis
Tampere University
Master's Degree Programme in Management And Information Technology
October 2022

In recent years local, or indoor, positioning for situations where satellite-based positioning systems are not suitable has been the subject of great interest. There is a need for such a positioning system for example for operators in industry, logistics, trade and the public sector. Applications range from tracking containers in a container harbour to locating people in a shopping mall. Various commercial solutions do exist, but there is a clear commercial need for new cost-effective, accurate, easy-to-implement and easy-to-maintain systems.

Current Bluetooth-based positioning systems generate location information mainly based on signal strength, and the location information achieved with this technology is often not reliable enough to be useful. The Bluetooth 5.1 standard introduces a technology that enables the determining of the direction of arrival of a radio signal. The purpose of this technology is to improve the usability of Bluetooth-based systems for indoor positioning.

The aim of this thesis was to investigate indoor positioning and the technology enabling the determining of the angle of arrival of the radio signal. The first step was to make a survey of existing indoor positioning technologies. The basics of the different techniques are explained in this thesis, and some parameters for evaluating the suitability of the system for the intended use are presented. A few commercial indoor positioning systems are also superficially introduced in this thesis.

When implementing the direction finding operationality introduced in the Bluetooth 5.1 standard, an algorithm must also be implemented to filter out noise caused by multipath propagation of the signal. For this reason, three angle-of-arrival detection algorithms based on measuring the amplitudes and phase differences of signals arriving at an antenna array are presented in this thesis, and the accuracy and computational complexity of the algorithms are compared.

The measurements were made on a development platform made by U-Blox, which consists of one Bluetooth beacon, one antenna unit, and software for both the beacon and the antenna unit. Measurements were made with the system, which were used to study the accuracy of the system's angle determining.

The most significant result can be considered to be the discovery of the dependence of the determined angle of the Bluetooth channel, as well as the strong dependence of the algorithm used on the development platform on the advertising interval of the Bluetooth beacon.

Keywords: Bluetooth 5.1, MUSIC, OGSBI, PDDA, Indoor positioning, Direction Finding, RTLS

TIIVISTELMÄ

Tommi Kaivola: Bluetooth Direction Finding
Diplomityö
Tampereen yliopisto
Johtamisen ja tietotekniikan maisteriohjelma
Lokakuu 2022

Viime vuosina paikallinen, tai sisätilan, paikannus tilanteisiin, joihin satelliittipohjaiset paikannusjärjestelmät eivät sovellu, on ollut suuren mielenkiinnon kohteena. Tarvetta tällaiselle paikannusjärjestelmälle on esimerkiksi teollisuuden, logistiikan, kaupan alan ja julkisen sektorin toimijoilla. Käyttökohteet vaihtelevat aina konttien seuraamisesta konttisatamassa ihmisten paikantamiseen kauppakeskuksessa. Erilaisia kaupallisia ratkaisuja on kyllä olemassa, mutta uusille kustannustehokkaille, tarkoille, helposti käyttöönotettaville ja helposti ylläpidettäville järjestelmille on selvää kaupallista tarvetta.

Nykyiset Bluetooth-pohjaiset paikannusjärjestelmät tuottavat sijaintitiedon pääasiassa signaalin voimakkuuden perusteella, ja tällä tekniikalla saavutettava sijaintitieto ei usein ole riittävän luotettavaa ollakseen hyödyksi. Bluetooth 5.1 -standardi esittelee radiosignaalin saapumissuunnan tunnistamisen mahdollistavan tekniikan. Tämän tekniikan tarkoitus on parantaa Bluetooth-pohjaisten järjestelmien käyttövalmiutta sisätilapaikannuksessa.

Tämän diplomityön tavoitteena oli tutkia sisätilapaikannusta ja radiosignaalin saapumiskulman tunnistamisen mahdollistavaa tekniikkaa. Työ aloitettiin tekemällä selvitys olemassa olevista sisätilapaikannustekniikoista. Selvityksessä selvitetään eri tekniikoiden perusteet, ja esitellään joitain suureita järjestelmän käyttökohteeseen soveltuvuuden arvioimiseen. Työtä varten tutustuttiin myös pintapuolisesti muutamaan kaupalliseen sisätilanpaikannusjärjestelmään.

Bluetooth 5.1 -standardissa esiteltyä kulmantunnistustoiminnallisuutta toteutettaessa tulee toteuttaa myös algoritmi, jolla saadaan suodatettua pois signaalin monitie-etenemisen aiheuttamat häiriöt. Tämän vuoksi työssä esitellään myös kolme erityyppistä antenniryhmään saapuvan signaalin amplitudin ja vaihe-erojen mittaamiseen perustuvaa saapumiskulmantunnistusalgoritmia, ja vertaillaan algoritmien tarkkuutta ja suoritusmonimutkaisuutta.

Käytännön mittaukset tehtiin U-Bloxin valmistamalla kehitysalustalla, joka koostuu yhdestä Bluetooth-majakasta, yhdestä antenniyksiköstä ja tarvittavasta ohjelmistosta. Järjestelmällä pystyttiin tekemään mittauksia, joilla todennettiin järjestelmän kulman mittaamisen tarkkuutta.

Työn tuloksista merkittävimpinä voidaan pitää käytännön mittauksissa havaittua kulman riippuvuutta Bluetooth-kanavasta, sekä kehitysalustalla käytössä olleen algoritmin voimakasta riippuvuutta Bluetooth-majakan mainostusintervallista.

Avainsanat: Bluetooth 5.1, MUSIC, OGSBI, PDDA, Sisätilapaikannus, Suunnan tunnistaminen, RTLS

PREFACE

This thesis was done as a part of Masters studies in Computer Science as part of the Faculty of Management and Information Technology. The thesis was made for Huld Oy.

I would like to thank Mikko Vulli, Tarmo Lipping, and Jari Turunen for their help in making this thesis happen.

Tampere, 9.10 2022

Tommi Kaivola

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AoA	Angle of Arrival
AoD	Angle of Departure
ARMSE	Average Root Mean Square Error
API	Application Programming Interface
AWGN	Additive White Gaussian Noise
BLE	Bluetooth Low Energy
BR	Basic Rate
CFR	Channel Frequency Response
CIR	Channel Impulse Response
CRB	Cramér-Rao Bound
CS	Compressive Sensing
CSI	Channel State Information
CTE	Constant Tone Extension
DMA	Direct Memory Access
DoA	Direction of Arrival
EDR	Enhanced Data Rate
FDMA	Frequency Division Multiple Access
GNSS	Global Navigation Satellite System
GPIO	General Purpose Input/Output
HCI	Host Controller Interface
IoT	Internet of Things
IQ	In-phase and Quadrature
ISM	Industrial, Scientific, and Medical
kNN	k-Nearest Neighbor
LE	Low Energy
LED	Light Emitting Diode
LO	Local Oscillator
LoS	Line of Sight
MAC	Media Access Control
MAP	Maximum a Posteriori
ML	Maximum Likelihood
MMV	Multiple Measurement Vector
MUSIC	Multiple Signal Classification
NFC	Near Field Communication
OGSBI	Off-Grid Sparse Bayesian Learning
PDDA	Propagator Direct Data Acquisition
PHY	Physical layer in Bluetooth terminology
PoA	Phase of Arrival
PoI	Point of Interest
PHY	Physical Layer, the bottom layer of BLE stack
RFID	Radio Frequency Identification Device
RN	Reference Node
RSS	Received Signal Strength
RSSI	Received Signal Strength Indicator
RTLS	Real Time Locating System
RToF	Return Time of Flight
SBL	Sparse Bayesian Learning
SDK	Software Development Kit
SIG	Special Interest Group
SNR	Signal to Noise Ratio
SoC	System on Chip
SPI	Serial Parallel Interface

SVM	Support Vector Machine
TDMA	Time division multiple access
TDoA	Time Difference of Arrival
ToA	Time of Arrival
ToF	Time of Flight
UART	Universal Asynchronous Receiver/Transmitter
UID	Unique Identifier
ULA	Unified Linear Array
URA	Unified Rectangular Array
UWB	Ultra-Wideband
VLC	Visible Light Communication

1. INTRODUCTION

Indoor, or local, positioning systems have been of interest for many years, with interest increasing due to the potential wide range of services that ***Internet of Things*** (IoT) can provide [1]. Indoor positioning is a process in which a location of a device or user in an indoor or local setting is obtained. Indoor positioning has been investigated extensively in the last few decades, focusing mostly to industrial settings for wireless networks and robotics [1]. The designing of a wireless local positioning system can be divided into two basic approaches: using existing wireless infrastructure, such as ***WiFi*** networks, or designing the wireless system solely for the purpose of positioning [2]. Indoor positioning can be used to localize and track users and devices. In [1] health sector, industry, disaster management, building management, surveillance, and other sectors are cited as possible applications for local positioning. Wireless positioning systems could be, for example, used in hospitals to find out the whereabouts of hospital equipment, or to locate a child in an amusement park [3]. A smart shopping cart could also utilise positioning data in helping the customer locate products in a grocery store or shopping mall [4]. ***Global Navigation Satellite System*** (GNSS) has a limitation for use in local indoor places, such as apartments, subways and shopping malls as the satellite signal is blocked by the structures [5].

Bluetooth 5.1 introduced means for acquiring phase and amplitude data from incoming signals, which can then be used to determine the angle from which the signal is received. This in theory helps to provide more accurate results in positioning systems than traditional Bluetooth based locating where positioning is done using the signal strength.

This thesis comprises six chapters, of which this introduction is the first. The second chapter provides context for indoor positioning domain by introducing some commonly used technologies and techniques and parameters for estimating the suitability of a technique to a use case. The third chapter introduces three different types of algorithms that can be used for determining the angle of a radio signal by using antenna arrays. The fourth chapter introduces Bluetooth standard, focusing on the low energy standard relevant for the angle detection. The fifth chapter presents some practical tests with a development kit, and the sixth chapter summarizes the thesis and presents the conclusions.

The local positioning study was done using studies and whitepapers from several online sources. The angle determining algorithms were also selected and studied through

online research. The selection of the three algorithms presented was done based on availability of research papers and material, as well as to display different approaches to the algorithm design.

The most significant findings of the practical tests were the channel and advertisement interval dependency in the angle calculation. In other findings it was determined that Bluetooth direction finding brings a new tool for local positioning, which has some benefits in relation to other current methods. One of these benefits is that Bluetooth is a thriving ecosystem with billions of devices already deployed. This makes it easier to adopt, as companies already have an understanding of it, and possess tools for development and manufacturing. The direction finding operationality could be integrated to an existing Bluetooth application, and the devices used for direction finding could also serve as indoor air quality measurement devices, or as monitors for manufacturing machinery usage rate, or provide information for predictive maintenance.

2. LOCAL POSITIONING SYSTEMS

This section presents the technologies and techniques for local positioning, introduces a few examples of existing commercial positioning solutions, and gives some quantities by which the suitability of a technology or technique to an application can be evaluated.

2.1 Technologies

WiFi is a colloquial term for IEEE 802.11 standard. WiFi is used for providing wireless networking capabilities for devices in private, public, and commercial environments. It is also one of the most widely studied positioning techniques in literature. [1]

Many portable devices, such as tablets and smartphones, have WiFi capability. Many public spaces also have WiFi access points for users, such as a coffee shop for their patrons. Because of existing WiFi infrastructure there is no need to deploy additional infrastructure, as the WiFi routers can be used as reference points for positioning signals. This makes WiFi a good candidate for positioning. However, WiFi networks are deployed to provide maximal networking coverage and data throughput instead of positioning capability. This creates a need to develop algorithms to improve existing WiFi infrastructure accuracy for positioning use. WiFi positioning accuracy is also affected by the uncontrolled interference present in The ***Industrial, Scientific and Medical*** (ISM) band of 2.4 GhZ. [1]

IEEE 802.15.1, colloquially known as ***Bluetooth***, can be used with various positioning techniques such as ***Received Signal Strength Indicator*** (RSSI), ***Angle of Arrival*** (AoA), and ***Time of Flight*** (ToF). Most of the existing Bluetooth based positioning systems rely on ***Received Signal Strength*** (RSS) based inputs. This is because RSS based solutions are less complex than other solutions. Two ***Bluetooth Low Energy*** (BLE) based solutions have been proposed, being ***iBeacon*** by Apple and ***Eddystone*** by Google, to be used for context aware proximity solutions. [1]

ZigBee is built on the IEEE 802.15.4 standard. Zigbee defines the higher levels of the protocol stack and is used in wireless sensor networks. Zigbee is not good for locating users because it is not readily available in a majority of the user devices. [1]

Radio Frequency Identification Device (RFID) is a technology mostly used for transferring and storing data from a device containing a transmitter to a device that has a compatible radio circuit. Two basic types of RFID systems exist: active RFID, and passive RFID. Active RFIDs can be used for locating and asset tracking because their range

is reasonable, and their cost is low. RFID devices can be easily attached to the objects that they are used to track. Sub-meter accuracy is not achievable with active RFID technology. Active RFID technology is not as commonly available on handheld devices as passive RFID is. Passive RFID devices are smaller, and they cost less than active RFID devices, but their range is limited. They can be used for proximity-based services, but this requires modification to the normal procedure used by passive RFID. The modification can be for example to transmit an ID that is used to identify the RFID at a choke point. [1]

Ultra Wideband (UWB) is a wireless technology, in which short pulses with time period of less than a nanosecond are transmitted over a large bandwidth in the frequency range from 3.1 to 10.6 GHz with a low duty cycle. The technology has been primarily used for short-range communication systems. UWB has a different signal type and radio spectrum makes than other commonly used radio technologies. This makes it an attractive technology for indoor positioning. Because of the difference it is immune to interference to signals from more common radio devices. The UWB signal can penetrate various materials, including walls. UWB pulses have a short duration, which makes them less sensitive to the effects of multipath propagation. The use of UWB in consumer products has been limited by the slow progress of the standard development. [1]

Visible Light Communication (VLC) is a technology that uses visible light between 400 and 800 THz, and it is modulated and emitted by ***light emitting diodes*** (LED). Positioning systems that utilise VLC communication measure the position and direction of LED emitters by using light detecting sensors. ***Angle of Arrival*** (AoA) is considered the most accurate positioning technique for visible light. AoA however requires a ***line of sight*** (LoS) between the LED and the sensors for accurate positioning, which is a severe limitation. [1]

Acoustic signals can be used for positioning. One application of this technology uses the microphones in smart-phones to capture acoustic signals that are modulated. The signals contain timestamps or other temporal information. These signals can then be used for ***Time of Flight*** (ToF) estimation. The velocity of a moving smart phone has also been deduced by analysing the phase and frequency shift caused by the Doppler effect in acoustic signal. Positioning systems based on acoustic signals have been shown to achieve high localization accuracy, but because of the smart-phone microphone limitations only audible band acoustic signals can provide accurate estimates. This in turn means that the transmission power should be low enough so that signal is not audible to human ear, and advanced algorithms are needed to improve the signal detection at the receiver. This solution also creates a need for extra infrastructure and cause battery drain

in the receiving device due to a high sampling rate, making this a non-favourable solution for local positioning. [1]

Ultrasound based positioning techniques mainly rely on ToF measurements of ultrasound signals. Sound velocity is used to calculate the distance between a transmitter and receiver node. Ultrasound based solutions have been shown to provide centimetre level accuracy, and to be able to track multiple mobile nodes at the same time with high energy efficiency. The problem in this solution is, that the sound velocity varies significantly when humidity and temperature change, creating the need to also deploy temperature sensors along the system. A permanent source of noise can also degrade the system performance severely.[1]

2.2 Techniques

This section provides a short and non-exhaustive description for the most common metrics used for positioning.

Received Signal Strength Indicator (RSSI) is a very widely used approach for indoor positioning [1]. The ***Received Signal Strength*** (RSS) is the power density of an electromagnetic wave over a free-space path. It is proportional to transmitted power and inversely proportional to the square of the distance to the source [3]. RSSI is an indicator that has arbitrary units and is mostly defined by each chip vendor [1].

Using the RSSI and a path-loss propagation model the distance d between devices can be derived from

$$\mathrm{RSSI} = -10nlog_{10}(d) + A, \tag{1}$$

where n is the path loss exponent, d is the distance between the transmitter and receiver, and A is the RSSI value at a reference distance from the receiver. [1]

N-point lateration, for example trilateration, can then be used to determine a device's position in relation to fixed anchor points [1]. Figure 1 illustrates RSSI based positioning utilising trilateration. In Figure 1, the signal strengths from three different radio sources are used to calculate the device's position relative to the ***reference nodes*** (RN).

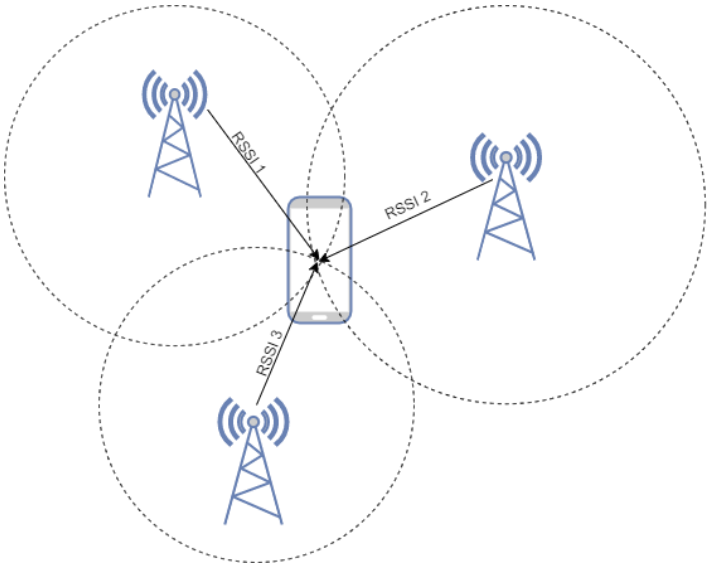

Figure 1: *Positioning a mobile phone in relation to three reference nodes using trilateration based on the received signal strength indicator*

The RSS based approach is affected by additional signal attenuation from non-LoS signals, such as transmission through walls and multipath fading. Filters or averaging mechanisms can be used, but it is unlikely to achieve high positioning accuracy without using complex algorithms. [1]

Channel State Information (CSI) is a technique that in addition to the amplitude of the signal, like in RSSI, utilises for example the ***Channel Frequency Response*** (CFR) or ***Channel Impulse Response*** (CIR). This information can be retrieved by the upper software layers as CSI. It has a higher granularity than RSS. In the context of positioning, granularity means that with low granularity the transmitter can be located to for example a certain building, and with high granularity it can be located for example into a room in a building. The CSI is a complex quantity and can be written in polar form as

$$H(f) = |H(f)|e^{j\angle H(f)}, \tag{2}$$

where $|H(f_i)|$ is the amplitude response and $\angle H(f_i)$ is the phase response of the channel for the frequency f_i. There are many IEEE 802.11 network interface controllers that provide subcarrier-level channel measurements, which can give this information. [1]

RSS and CSI based approach can be improved further by utilising a concept called ***fingerprinting***, or ***scene analysis*** [1]. This type of method usually involves two phases: an offline training phase and an online position determining phase [6]. Different RSSI measurements are performed and collected during an offline training phase [6]. In the offline training phase, the signal strengths are measured from key locations in the area of interest. This produces a data set called a radio map [6]. On system deployment the online

results are paired with the previously collected offline measurements [1]. The pairing can be done for example with probabilistic methods, ***k-Nearest Neighbour*** (kNN) method, or utilising artificial neural networks or a ***Support Vector Machine*** (SVM) [1].

Time of Arrival **(ToA)** or ToF or both exploit the signal propagation time. The distance between the transmitter and receiver is calculated using this information. The ToF value is converted to physical distance between the transmitter and the receiver by multiplying it with the speed of light. The transmitter can then be positioned with respect to the receivers using for example trilateration. Signal bandwidth and receiver sampling rate are key factors for ToF. Low sampling rate reduces the resolution. A strict synchronization between transmitter and receiver is needed, and in many cases, timestamps are transmitted with the signal. Because the emitted signals are deflected by the obstacles causing them to traverse a longer path which increases the time it takes for the signal to propagate, having no LoS between the transmitter and receivers causes significant positioning errors in ToF based methods. Figure 2 shows an example of ToF based positioning. [1]

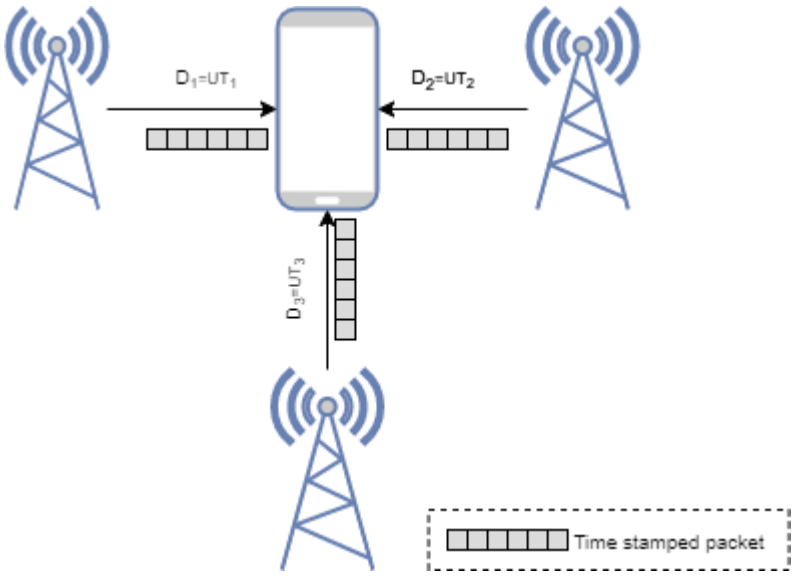

Figure 2: *Locating a mobile phone in relation to three reference nodes based on trilateration using time of flight technique*

In ***Time Difference of Arrival*** (TDoA) positioning technique a radio signal is sent repeatedly from a transmitter and received by multiple receivers. The location of the receivers needs to be known in advance, and the receivers need to have strict time synchronization. The difference in the time of arrival of the signal to each receiver can be used to calculate the difference in distances between the receiver and two transmitters using the equation

$$\Delta d = c \cdot \Delta t. \quad (3)$$

In (3), c is the speed of light and Δt is the difference in arrival time at two different receivers. In a two-dimensional case this leads to the equation

$$\Delta d = \sqrt{(x_2 - x)^2 - (y_2 - y)^2} - \sqrt{(x_1 - x)^2 - (y_1 - y)^2}. \quad (4)$$

In (4), (x_1, x_2) and (y_1, y_2) are the positions of the receivers. This equation can be converted to a hyperbola using non-linear regression. The location of the transmitter is on this hyperbola, and by calculating more hyperbolas the transmitter can be positioned by finding the intersection of the hyperbolas. [7]

The TDoA estimation accuracy is dependent of the signal bandwidth and receiver sampling rate. TDoA also requires a direct LoS between the transmitter and the receivers. [1]

Return Time of Flight (RToF) uses a similar ranging mechanism as ToF, but in this case the round-trip time of the signal is measured. The main benefit is that it requires only a relatively moderate clock synchronization between the transmitter and receiver. Sampling rate, LoS between the transmitter and receiver, and signal bandwidth all affect the accuracy of RToF positioning. The effects are more severe than in ToF as the signal is transmitted and received twice. In addition, the response delay at the receiver also affects RToF based positioning systems. The delay time depends highly on the receiver electronics and protocol overheads. If the response time is small when compared with the propagation time between the transmitter and receiver the overhead can be neglected. The propagation time, however, is short for local positioning cases, so the delay time cannot be neglected. [1]

Methods based on ***Phase of Arrival*** (PoA) estimate the distance between the transmitter and the receiver by utilising the phase of the carrier signal. It is commonly assumed that the transmitted signals are purely sinusoidal and have the same frequency and no phase offset. PoA methods utilise an antenna array, and the phase difference between separate antennas is used to deduce the distance of the transmitter. [1]

Angle of Departure (AoD) and ***Angle of Arrival*** (AoA) of a radio signal can be used to determine a transmitter's position in relation to the receiver [8]. In Angle of Arrival direction finding the transmitter has a single antenna, while the receiving unit has an antenna array [8]. The receiving unit switches antennae while receiving packages, capturing samples which can be used to calculate the phase difference in the received signal [8]. Figure 3 illustrates this idea.

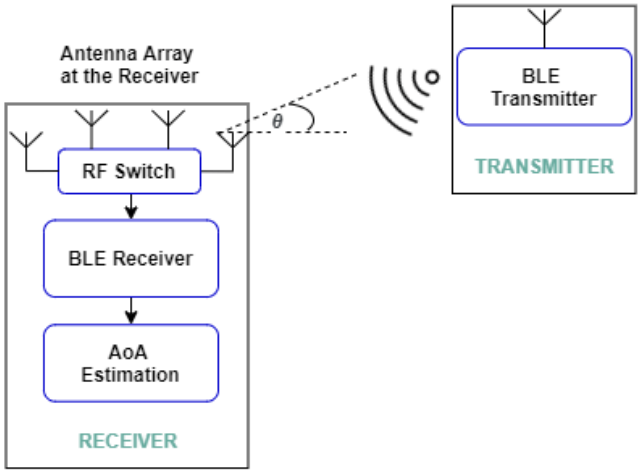

Figure 3: *System for AoA determining with a single antenna in the transmitter and an antenna array and an antenna switch in the receiver [9]*

Figure 4 illustrates a signal arriving to the antennae. For the sake of simplicity, the antenna array is presented as two antennas.

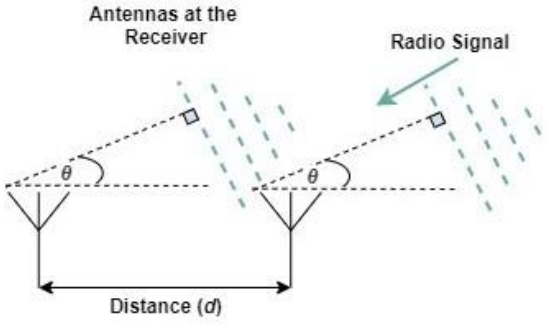

Figure 4: *Radio signal impinging on two antennas that form an antenna array in an AoA system [9]*

In Figure 4, d denotes the distance between two antennas. The phase difference, ψ, between the signals arriving at the two antennas is calculated in the following way:

$$\psi = \frac{2\pi d cos\theta}{\lambda}, \tag{5}$$

where λ is the signal wavelength, and θ is the AoA. To avoid the aliasing effect, the maximum value of d must be $\lambda/2$. Solving the above equation in relation to the angle gives us:

$$\theta = cos^{-1}\left(\frac{\psi\lambda}{2\pi d}\right). \tag{6}$$

In AoA, the sampling of the antenna array must be done in some suitable sequence, so that each sample can be attributed to a specific antenna [10].

AoD method is used to determine the angle in which the signal departs from a transmitter [9]. An example of a Bluetooth LE system capable of AoD determining consists of a single antenna at the receiver and multiple antennas at the transmitter [9]. The transmitter can make its angle of departure detectable by transmitting packets while switching antennas during the transmission [9]. The receiver has a single antenna with which it receives the packets and collects the samples [9]. The direction of the signals is then determined from the delay between the signals from the multiple antennas in the sender [9]. Figure 5 shows an example setup for BLE AoD direction finding.

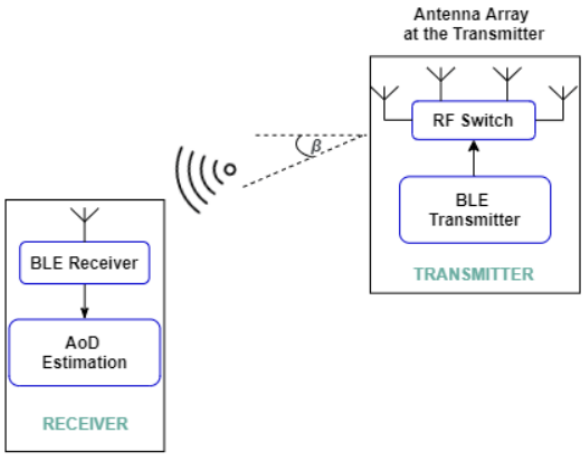

Figure 5: *System for AoD determining with an antenna array and an antenna switch in the transmitter and a single antenna in the receiver [9]*

Figure 6 illustrates a transmitter with two antennae separated by distance d transmitting signal to a receiver with a single antenna.

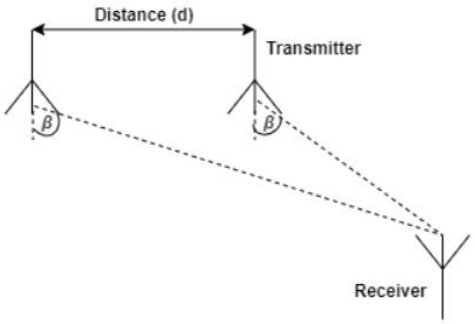

Figure 6: *Two radio signals sent from two antennas that form an antenna array impinging on the receiver antenna* [9]

The phase difference ψ between the signals being transmitted from the two antennas is calculated as

$$\psi = \frac{2\pi d sin\beta}{\lambda}. \quad (7)$$

In (5), signal wavelength is denoted with λ, and β is the angle of departure. Rearranging (5) gives us the formula for calculating angle of departure:

$$\beta = sin^{-1}\left(\frac{\psi\lambda}{2\pi d}\right). \quad (8)$$

It is notable, that in AoD the antenna array and the antenna switch is in the transmitter, and the receiver performs the sampling by taking measurements with a single antenna.

Antenna arrays used in direction finding can have many different numbers of antennae as well as different antenna designs. Examples of these arrays are ***Uniform Linear Array*** (ULA), ***Uniform Rectangular Array*** (URA), and ***Uniform Circular Array***, each of which an example is illustrated in Figure 7. [10]

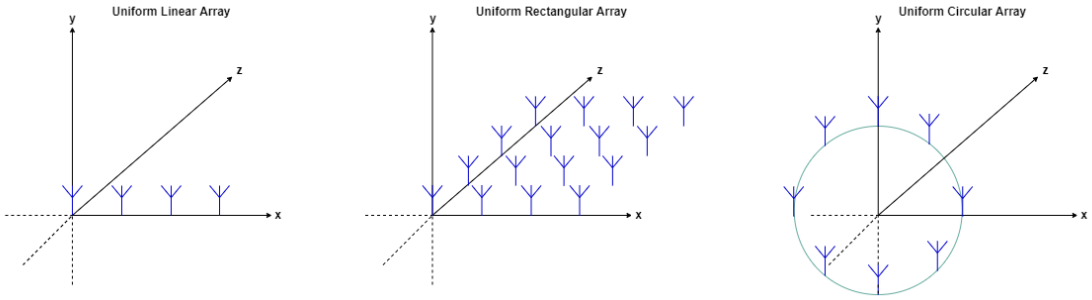

Figure 7: *An illustration of three different antenna array configurations used for radio signal direction finding [9]*

In a uniform linear array, the antennas are in a single line. In a uniform rectangular array, the antenna elements are placed on a rectangular grid. The antennae can be in e.g. $4x4$ configuration, or in an L-shaped configuration. In a uniform circular array, the antenna elements are placed in a circumference of a circle. The geometry of a ULA allows only a single angle to be calculated, while the more complex antenna array designs allow for calculation of two or three angles (for example elevation and azimuth angle) in relation to a reference plane. Figure 8 shows the concept of elevation and azimuth angles. [9]

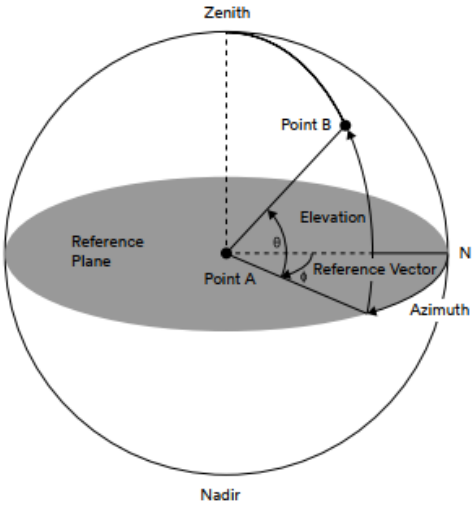

Figure 8: *An illustration of a reference plain that is formed by the azimuth angle and the elevation angle that is in relation to the plane formed by the azimuth angle [10]*

The azimuth and elevation angles can be used together to determine an object's location in three-dimensional space. In a three-dimensional positioning system, the object's xy-coordinates will be known in a horizontal plane, and the elevation angle is known as an angle above or below the reference height determined by the xy-plane. [10]

2.3 Real Time Locating Systems

All local positioning techniques and technologies discussed in this section can be used to create a ***Real Time Locating System*** (RTLS). An RTLS comprises a mobile device that is enabled with location technology (for example a tag or a beacon), a locator (for example a location determining gateway, or reference node) that has a known position, a location engine that communicates with the location sensor and determines the location of the asset being monitored, middleware that exists between the positioning engine and the business applications, which can have an ***Application Programming Interface*** (API), and the end user application that uses the middleware (for example an application that shows the location of a shopping mall patron on a map screen in a handheld device). Figure 10 illustrates an example RTLS. [11]

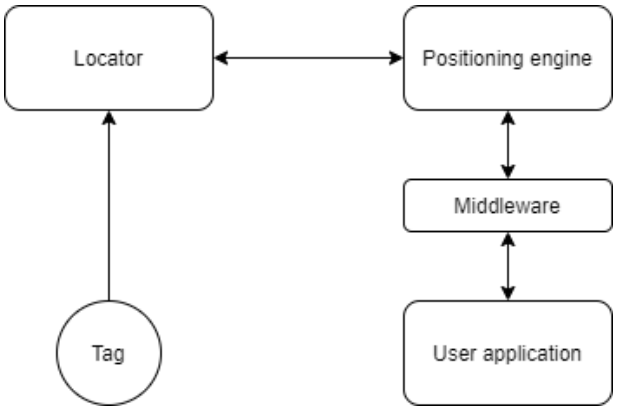

Figure 9: *Components of an RTLS and their relationship*

International Organization for Standardization and the International Electrotechnical Commission has a standard regarding RTLS, the ISO/IEC 24730 series which currently has several standards published. The standard defines several air interface protocols and one API for use in asset management. [12]

2.4 Commercially available RTLS solutions

This section gives brief examples of four commercially available RTLSs. All companies presented in Table 1 offer complete RTLS with tags for asset tracking, locators and gate-ways, positioning engine, API, and application.

Table 1: *Commercially available RTLS solutions*

Company	Technique	Technology	Accuracy (m)	Scalability (assets)
Bluelot	AoA	BLE	0.1-0.5	N/A
Quuppa	AoA	Proprietary 2.4 GHz	<1	Up to thousand
Sewio	N/A	UWB	0.3	Unlimited
Pozyx	TDoA, TWR	UWB	0.1	Thousands

All information was retrieved from the companies' websites. The accuracies given are in line with the theoretical maximum accuracy for each technology. For AoA bases solutions a direct LoS is needed, so the performance is most likely worse in real-life situations where there is no LoS between the asset and the locator.

2.5 Parameters for evaluating the suitability of techniques for various applications

This chapter presents some parameters that can be used when selecting a positioning technique for an RTLS. The demands for the RTLS come from the use case. The use case defines, for example, the size of the area of interest, maximum amount of trackable

devices, the desired deployment and maintenance cost for the whole system, system latency, and the need for scalability. The parameters discussed here are accuracy, precision, coverage, hardware and software complexity, cost, latency, and scalability.

Accuracy is evaluated by how accurately the estimated position matches the true position and is often measured by mean distance error [2]. Precision is evaluated by the consistency of the estimated position and can be measured by for example standard deviation in the location error [2]. If the system has some demand for accuracy and precision, the selected technique needs to be capable to deliver the demanded accuracy and precision. If an accuracy of a few centimetres is needed, the technique needs to capable of that precision. For example, UWB positioning precision varies from a few centimetres to tens of centimetres, while RSSI based Bluetooth positioning precision varies from tens of centimetres to tens of meters [13].

Coverage describes the area of interest for the positioning system. Different techniques have different coverages, so for techniques with a limited range more devices are needed to cover the area of interest. [13]

Complexity of an RTLS can be divided into hardware complexity and software complexity. Hardware complexity can lead to high cost for a single unit, large devices, or the need for more devices than with some solution that has lower complexity. Software complexity is mostly due to the computational algorithm used for positioning. If the algorithm is complex, it takes more time and energy to calculate the position. [2]

Cost factor can include things such as time, space, energy, weight, and money. Time can attribute to the installation and maintenance cost for the system. The size and density of the positioning devices is a space cost [2]. Energy is also one cost for the system, for example a mobile device with a rechargeable battery may need to be recharged often [1]. The energy efficiency of a positioning system can be affected by for example the frequency of transmitting the reference signal for positioning, transmission power of the transmitter, and the computational complexity of the positioning algorithm, especially if the algorithm is running on a battery-operated device [1].

An RTLS should by definition be real-time, and thus have a low latency. If a granularity in the milliseconds is desired, the system cannot perform extensive measurements or complex time-consuming signal processing. The system needs to be able to convert only few reference signals to position data in under milliseconds. [1]

Scalability means that the RTLS should have the capability to position many users in a large space [1]. When more area is covered, or units are crowded in the area, wireless

signals may become congested and there may be need for more calculation [2]. Scalability is more challenging to systems that compute the location on the user device when compared to systems that compute the location on a server [1].

3. METHODS FOR ANTENNA ARRAY BASED RADIO SIGNAL DIRECTION FINDING

This section describes three methods that can be used to calculate the angle of arrival from phase and amplitude information of a signal. As the Bluetooth 5.1 specification only provides the samples containing the phase and amplitude information, and not the algorithm, it is up to the application developer to select and implement the algorithm.

3.1 MUSIC

Multiple signal classification (MUSIC) was proposed by Schmidt in 1979. It is a high-resolution direction-finding algorithm. MUSIC is the most common approach for determining the AoA from measured phase delay [14]. MUSIC belongs to the family of subspace-based direction-finding algorithms [15]. In this context subspace refers to linear subspace, which in turn is a vector space. A vector space is a nonempty set of vectors, which must satisfy ten axioms related to addition and multiplication by scalars. A subspace is a vector space that consists of an appropriate subset of vectors from another, larger vector space [16]. MUSIC can be implemented as an algorithm, and it can provide estimates of signal parameters, including the ***Directions of Arrivals*** (DoAs), the number of signals, and polarizations [17].

MUSIC creates a signal model and uses eigenvalue decomposition for the covariance matrix of the received phase and amplitude data snapshots. The eigenvectors that correspond to the positive eigenvalues span the signal subspace, and the eigenvectors that correspond to the zero eigenvalues span the noise subspace. MUSIC then constructs a power expression called the MUSIC pseudospectrum, which is dependent on the angle of arrival. The peaks of this pseudospectrum are the angles of arrival. [15]

Root-MUSIC is a variation of MUSIC which can be used with a ULA antenna array[15].

3.2 OGSBI

A signal is considered sparse if there are more zero values than non-zero values. In a real-world situation a sparse signal could be formed from a signal with a small number of significant coefficients, and the insignificant coefficients can be set to zero. Sparse signals can be reconstructed from a smaller set of measurements than conventionally required by the signal bandwidth. This type of smaller set can be the result of an efficient

sampling strategy, where the lowest possible number of measurements is acquired. This is called ***Compressive Sensing*** (CS). [18]

Sparse Bayesian Learning (SBL) is a CS theory, which is used for signal reconstruction from compressive measurements. SBL uses previously known sparse distributions of the incident signals at all snapshots. In situations with few snapshots these types of CS-based techniques can improve the estimation resolution. The method however has difficulties in practical situations, where the correct DoAs are not located on the sampling grid. An extensive sampling grid could be used, but it results in highly correlated matrix. This in turn breaks the conditions required for sparse signal recovery. An ***off-grid Sparse Bayesian Inference*** (OGSBI) estimation algorithm can overcome these issues in SBL-based approaches. [19]

OGSBI estimation algorithm creates an observation model based on the notion that time delays at different antennas can be represented by simple phase shifts. An off-grid model is created, and an algorithm is derived in the ***Multiple Measurement Vector*** (MMV) case. For DoA estimation both the sparse signals and the off-grid difference need to be found. A sparse noise model and a signal model are formulated. OGSBI creates an estimation using a ***maximum a posteriori*** (MAP) estimate. [19]

3.3 PDDA

This algorithm will be introduced more in-depth than the previous two algorithms, as it is used in the development kit used for the practical tests. In [20] a new AoA method is presented, called ***Propagator Direct Data Acquisition*** (PDDA), which is based on computing a propagator vector. The propagator vector represents the cross correlation between the data that is received from the transmitters. The method has a low complexity. The advantage of PDDA over MUSIC is that it does not require a priori information on the number of signals arriving to the antenna array. PDDA also does not require the construction of a covariance matrix or matrix inversion. [20]

PDDA uses a data model which assumes that D incoming signals, $\mathbf{s}(t)$ arrive from different directions and are received by M sensors. Each component's time sample $\mathbf{X}(t)$ of the received signal contains also Average Gaussian White Noise (AWGN) noted as $\mathbf{N}(t)$. The time sample can thus be defined by:

$$\mathbf{X}(t) = \mathbf{A}(\theta)\mathbf{S}(t) + \mathbf{N}(t) \tag{9}$$

In equation (9), $\mathbf{A}(\theta) = [\boldsymbol{a}(\theta_1)\, \boldsymbol{a}(\theta_2) \ldots \boldsymbol{a}(\theta_D)]$ is the arriving signal steering matrix for D signals. $\mathbf{S}(t) = [\boldsymbol{s}_1(t)\boldsymbol{s}_2(t) \ldots \boldsymbol{s}_D(t)]^{\mathrm{T}}$ is the $D \times N$ incident signals, and $\mathbf{N}(t)$ is an array

of AWGN for each channel. A $M \times N$ data matrix $\mathbf{X}(t)$, that contains N samples of data obtained from M sensor, can be written as follows:

$$\mathbf{X}(t) = \begin{bmatrix} x_1(t_1) & x_1(t_2) & \cdots & \cdots & x_1(t_N) \\ x_2(t_1) & x_2(t_2) & \vdots & \vdots & x_2(t_N) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_M(t_1) & x_M(t_2) & \cdots & \cdots & x_M(t_N) \end{bmatrix} \tag{10}$$

A propagator vector **p** can be computed by first dividing the matrix into two sub-matrices:

$$\mathbf{h} = [x_1(t_1) \quad x_1(t_2) \quad \cdots \quad \cdots \quad x_1(t_N)] \tag{11}$$

$$\mathbf{H} = \begin{bmatrix} x_2(t_1) & x_2(t_2) & \vdots & \vdots & x_2(t_N) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_M(t_1) & x_M(t_2) & \cdots & \cdots & x_M(t_N) \end{bmatrix} \tag{12}$$

In (11) and (12) $\mathbf{h}$ represents the first row of the matrix $\mathbf{X}$, and $\mathbf{H}$ represents the rest of $\mathbf{X}$. Propagation vector **p** can now be computed:

$$\mathbf{p} = \frac{\mathbf{h}\mathbf{H}^{\mathrm{H}}}{\mathbf{h}\mathbf{h}^{\mathrm{H}}}. \tag{13}$$

(13) gives the cross-correlation of the time-series from each element with that of the first element. Now a unit element that represents the correlation of the first row with itself is added:

$$\mathbf{e} = [1 \ \mathbf{p}]^{\mathrm{T}}. \tag{14}$$

$\mathbf{e}$ is a vector of size $1 \times M$. The spatial power spectrum can be obtained from vector $\mathbf{e}$ like this:

$$\mathbf{P}(\theta) = |\mathbf{a}(\theta) \ \mathbf{e}|^2. \tag{15}$$

To obtain narrower peaks and to minimize side-lobe levels, the following approach is proposed. First the maximum point in $\mathbf{P}(\theta)$ is found:

$$w = \max(\mathbf{P}(\theta)) \tag{16}$$

In (16), w is a scalar value. The value of the global maximum is then subtracted from other values in (15), producing this equation:

$$\mathbf{P}_s(\theta) = w - \mathbf{P}(\theta) \tag{17}$$

After (17), nulls in the direction of incoming signal have been achieved. The PDDA can now be expressed as this formula that acquires maximum peaks in the AoA:

$$\mathbf{P}_{PDDA}(\theta) = \frac{1}{\mathbf{P}_S(\theta) + \varepsilon}. \tag{18}$$

In (18), ε is a small scalar value added to avoid possible singularities. (18) is highly non-linear, thus exaggerating signals close to w and it also suppresses side-lobes. If ε is selected properly, a threshold value can be applied so that genuine peaks can be separated from side-lobes. [20]

Program 1 contains the pseudo code for PDDA algorithm.

```
1. Divide the matrix to two portions as given in (11) and (12)
2. Construct the propagator vector by applying (13)
3. Compute the vector e as given in (14)
4. Construct the pseudospectrum by scanning e as in (15)
5. Find the maximum global point in the spatial spectrum as in (16)
6. Subtract the maximum value from other values by applying (17)
7. Plot the pseudospectrum by using (18). The AoAs are the peaks.
```

Program 1: *Pseudocode for PDDA [21]*

3.4 Comparisons of method performance

When comparing direction-finding methods, a concept called ***Cramér-Rao Bound*** (CRB) is good to be introduced. According to Friedlander, it is a useful tool for assessing the accuracy of parameter estimation methods, as it provides a lower bound on the accuracy of any unbiased estimator [22]. This means that the CRB can be used as an algorithm-independent benchmark for various algorithms. In [23] MUSIC performance is compared against the CRB, stating that if $\mathbf{P}$ is diagonal the accuracy approaches the CRB asymptotically as the number of samples increases. For a nondiagonal $\mathbf{P}$, the accuracy of MUSIC is strictly larger than CRB. In [20] a selection of AoA algorithms including MUSIC, OGSBI, and PDDA are compared. Both the performance and computational complexity are compared.

The computational complexity for MUSIC, OGSBI, and PDDA algorithms is shown in Table 2. In Table 2 δ represents a scanning step, which can be for example 0.5 degrees.

Table 2: *A comparison of the computational complexity of AoA algorithms [20]*

Method	Computational complexity
MUSIC	$O(M^2N + M^3 + M^2(180/\delta))$
OGSBI	$O(max(M\ (180/\delta)^2, M\ N\ (180/\delta))\ per\ iteration$
PDDA	$O(M\ N + M(180/\delta))$

Table 2 shows that MUSIC is the most complex, OGSBI is less complex, and PDDA is the least complex. OGSBI needs more iterations than one, so the complexity can be larger than the one presented when multiple iterations are needed. [20]

In [20] the performance is compared by making a Monte Carlo simulation for each algorithm using four different scenarios: number of snapshots taken, ***Signal to Noise Ratio*** (SNR), the correlation between sources of the incident signals, and the execution time. A snapshot is one sample data capture from the antennae. [20]

For the first three scenarios, the ***Average Root Mean Square Error*** (ARMSE) is computed for the criteria. ARMSE is defined as

$$ARMSE = \frac{1}{K}\sum_{j=1}^{K}\sqrt{\frac{1}{D}\sum_{k=1}^{D}\left[\left(\theta_k - \hat{\theta}_k\right)^2\right]} \tag{19}$$

In (19), D is the number of signals arriving, θ_k is the actual angle, $\hat{\theta}_k$ is the estimated angle, and K is the number of Monte Carlo simulation trials. [20]

For comparison of number of snapshots, PDDA gives the best result for a single snapshot with OGSBI being very close. At 2 and 3 snapshots, PDDA and OGSBI are convergent and give the best performance. At 4 snapshots PDDA, OGSBI and MUSIC have roughly the same performance. At 5 snapshots, MUSIC is the best with OGSBI in second place and PDDA in third place. [20]

For comparison of SNR, the number of snapshots is limited to 3, but a differing SNR value in the input of the sensor array is tested. MUSIC algorithm has the best performance in low SNR situations, while PDDA gets better when the SNR is reduced. When SNR is 10 dB, OGSBI gives the best performance. [20]

Correlation between the arriving signals has a negative impact on the performance of direction estimation systems. The correlation simulation was run for two correlated signals with correlation coefficient 0.95 incident on a linear array. The number of samples is 10 and SNR is 1 dB. PDDA performed best in this test, while MUSIC also gives a good result. OGSBI is based on Bayesian compressed sending, and thus it has a high sensitivity to correlated signals. [20]

4. BLUETOOTH DIRECTION FINDING

This chapter provides a short description of Bluetooth, focusing on the LE specification, to provide basis for the Bluetooth AoA/AoD signals and operationality. The signals and sampling schemes introduced in Bluetooth core specification for direction finding are also introduced.

4.1 Bluetooth overview

IEEE 802.15.1, colloquially known as Bluetooth, is a wireless technology for short range communications systems. In [8] it is stated that Bluetooth is intended to replace cables connecting portable and/or fixed electronic devices.

Bluetooth is a global standard, and it is short-range, low-power, low-cost and small form-factor. Over the years Bluetooth use cases have grown to exchanging files between PCs and mobile phones, music streaming over the air, transmitting data to a printer, and transmitting audio on Bluetooth headsets for mobile phone calls. [24]

Bluetooth comprises two forms of wireless technology systems: ***Low Energy*** (LE) and ***Basic Rate*** (BR). Connection establishment, connection mechanisms and device discovery is included in both systems. Optional ***Enhanced Data Rate*** (EDR) extensions to ***Media Access Control*** (MAC) and ***Physical*** (PHY) layers is included in the BR system. [8]

The LE system has features that are designed for products that require low current consumption, low complexity and low cost as compared to BR/EDR. The Bluetooth LE radio operates in the 2.4 GHz ISM band. LE system utilises a frequency hopping transceiver to reduce the effects of interference and fading, and it utilises a binary frequency modulation to minimize transceiver complexity. [8]

The Bluetooth core system comprises a Host and one or more Controllers. A Host is defined as an entity comprising all layers below the non-core profiles. The Host is above the ***Host Controller Interface*** (HCI). A Controller is an entity defined as all layers below HCI. A high-level illustration of Bluetooth architecture is shown in Figure 10, in which the black line between the controller and host shows where the HCI exists. [8]

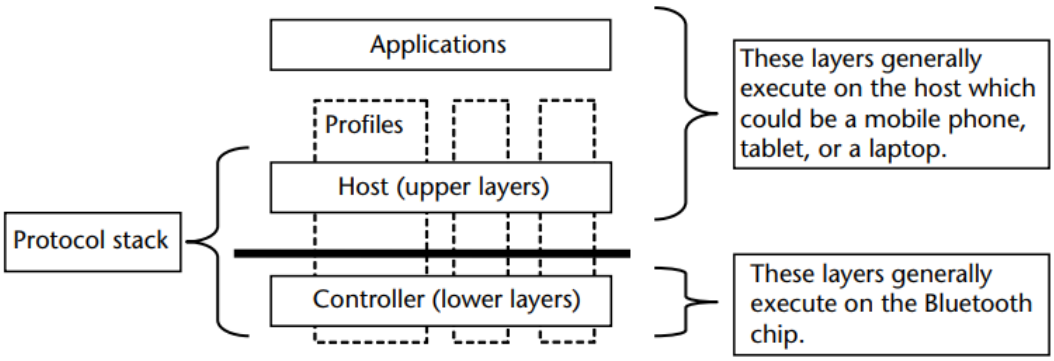

Figure 10: *An illustration of the bluetooth high-level architecture [24]*

Figure 10 shows, that generally the lower layers are executed on the Bluetooth chip, and the HCI provides access to the Bluetooth chip from a host. The lower layers, or Controller, comprises the layers responsible for low level operations, such as discovering devices, connecting to devices, exchanging data packets, and security. The bottom layer is called the ***physical layer*** (PHY). The upper layers utilize the functionality that the lower layers provide, providing functionality such as serial port emulation, or splitting data to smaller chunks and rearranging the data to make it possible to transfer large chunks of data. [24]

Multiple access scheme is a technique, that allows two or more users to share radio frequency spectrum. Bluetooth LE employs two multiple access schemes, being ***Frequency Division Multiple Access*** (FDMA) and ***Time Division Multiple Access*** (TDMA). The FDMA scheme uses 40 physical channels separated by 2 MHz. Three of the 40 channels are used as primary advertising channels and 37 are used as general-purpose channels. When a device transmits a packet at a predetermined time, and corresponding device responds with a packet after a predetermined interval, a TDMA based polling scheme is used [8]. Figure 11 shows the Bluetooth LE physical and RF channels. It is notable that even though the advertisement channels are numbered from 37 to 39, they are in the start, lower middle, and end of the physical channel.

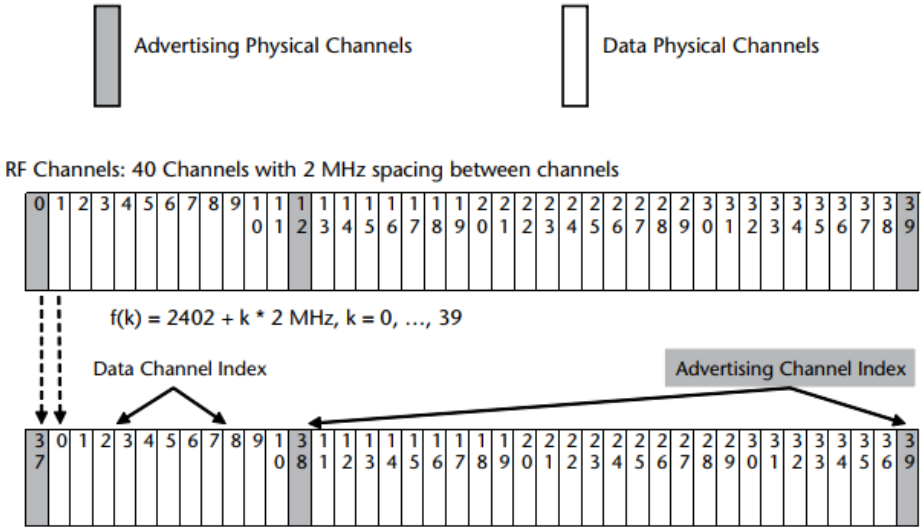

Figure 11: *An illustration of the Bluetooth LE physical and RF channels showing the location of the advertisement channels in the spectrum [24]*

The physical channel is sub-divided into time units. These time units are known as events. Data is transmitted between LE devices in packets that are positioned in these events. Bluetooth LE has the following events: Advertising, Extended Advertising, Periodic Advertising, Connection, and Isochronous Events. [8]

Devices that transmit advertising packets are called advertisers. Devices that receive these advertising packets without intention to connect to the device are called scanners. Data transmission on the advertising physical channel is done in advertising events. Should a device need to connect to an advertising device, it scans for connectable advertisement packages, and makes a connection request on the same advertising channel in which the connectable packet was received. The initiating device becomes the master device, and the advertising device becomes the slave device. This arrangement is referred to as a piconet. [8]

Figure 12 shows two possible topologies for Bluetooth LE. Scenario A comprises one advertiser and two scanners. The advertiser sends advertising packets on the advertising channel. The scanners can request more information or send a request to connect to the advertiser. Scenario B shows a piconet. In this piconet, one master is connected to three slaves and the data is exchanged on the data physical channels. [24]

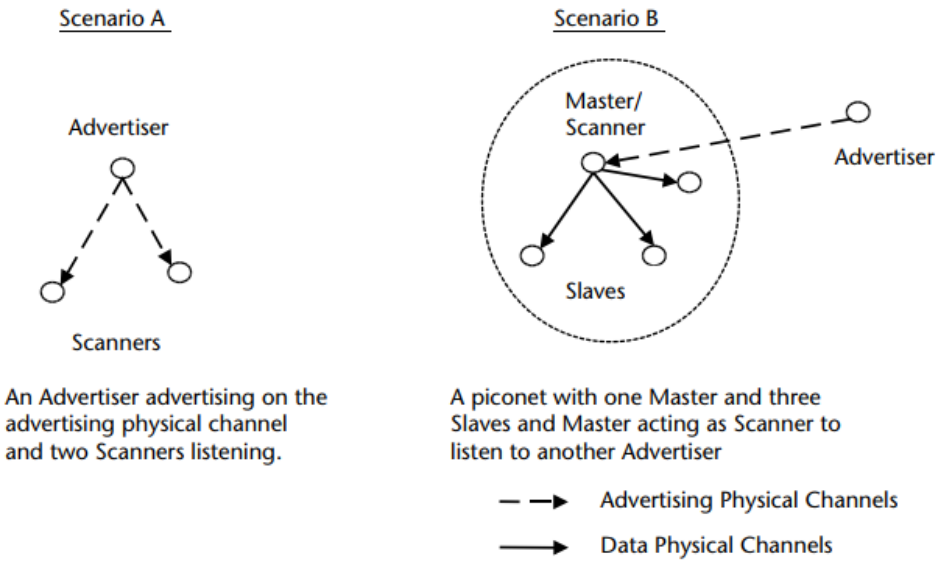

Figure 12: *An illustration of two examples of Bluetooth LE topology [24]*

Bluetooth direction finding enhancements presented in Bluetooth Core Specification 5.1 can work both connectionless (advertising) and connection-oriented mode [10].

4.2 BLE direction finding signals and sampling

New direction finding signals have been introduced to the Bluetooth standard, and they are an essential part of how Bluetooth direction finding works. The direction finding signals provide a source of constant signal material. [10]

The sampling process for direction finding signals is known as In-phase and Quadrature Sampling, often abbreviated as IQ sampling. In this sampling, several phase and amplitude measurements are taken in precise intervals. A single IQ sample comprises the wave's amplitude and phase angle represented in Cartesian coordinates. The Cartesian representation can then be transformed into corresponding polar coordinates that have the phase angle and the amplitude value. The IQ plane and an example IQ value are shown in Figure 13. [10]

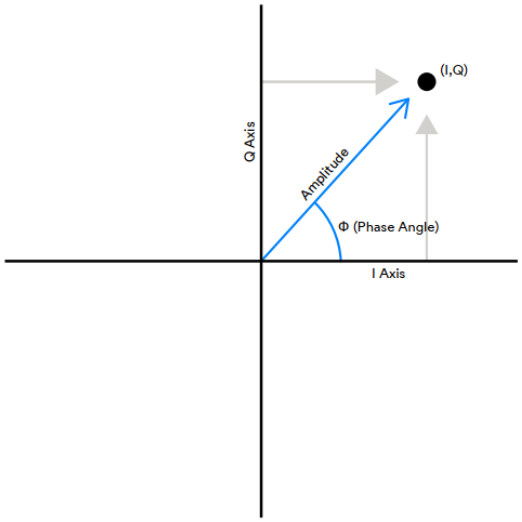

Figure 13: *An illustration of phase angle and amplitude as (I,Q) Cartesian coordinates in the IQ plane* [*10]*

In IQ sampling the incoming signal is mixed with a Local Oscillator (LO) at 0 and 90 degree offsets. This creates two orthogonal functions, I and Q. [25]

Bluetooth LE uses two frequencies within a selected radio channel. One of the frequencies represents zeros, and the other ones. These frequencies are deduced by adding or subtracting a value called the frequency deviation to or from the channel's center frequency. The wavelength of the signal is affected by this frequency change. Because the wavelength is critical for the calculation of the IQ samples, the core specification has introduced a Constant Tone Extension (CTE). [10]

CTE is only supported in LE uncoded PHYs (LE 1M and LE 2M). CTE is used for packets on all physical channels. Each packet comprises four mandatory fields, and the CTE as a fifth optional field. Figure 14 shows the structure of one packet. [8].

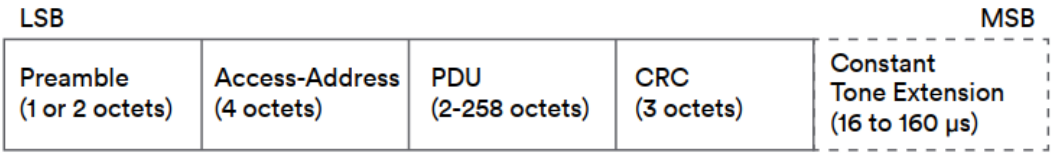

Figure 14: *Uncoded PHY packet format showing the location of the CTE [10]*

The CTE has a variable length, from 16 µs to 160 µs. The content is a constantly modulated series of 1s. Whitening is not applied to the CTE. [8]

In the AoA method, the device switches between antennas when receiving the signal. The standard defines time periods that are called switch slots, and the switching is done during these time periods. The CTE is divided into these slots, and the first 4 µs of the CTE is called the guard period. The next 8 µs is called the reference period. The IQ

samples are captured during this reference period and during time periods that are called sample slots by the Link Layer of the receiving device. [8]

In AoD method the transmitter contains the antenna array, but the IQ sampling is still done in the receiver. This means that there needs to be a way of providing the receiver with the details of the antenna array. Bluetooth SIG will publish profiles that define how to do this in the future. [10]

There are recommendations for the sampling to ensure that the sampled data is of good quality for angle estimation. The IQ samples are recommended to be taken at the same point within each IQ Sampling Window, starting 0.125 µs after the beginning and ending 0.125 µs before the end of each µs period. If 2 µs samples lots are used, the sampling is recommended to be done during the latter microsecond. [8]

The RSSI of the received packets can be measured from the body of the packet of which the CTE is a part of, and be used for e.g. positioning [8].

In AoA, antenna switching is needed only when receiving a CTE, but not when transmitting. Figure 15 shows the timing rules for AoA CTE.

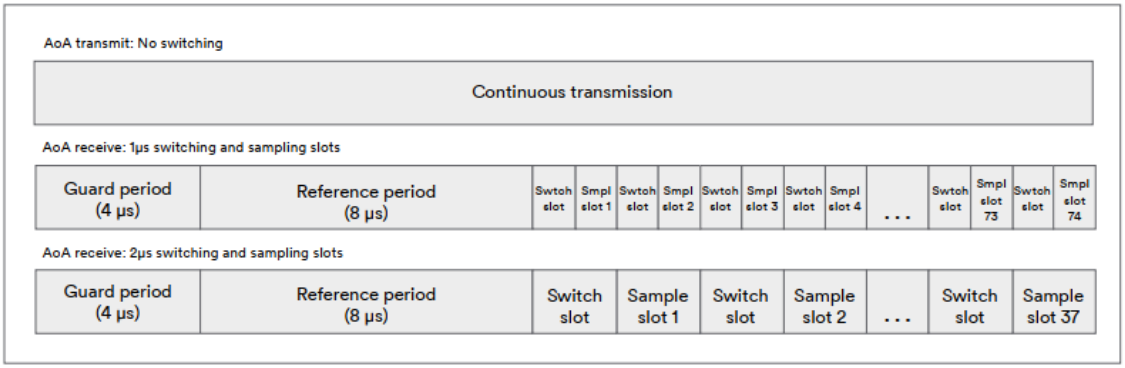

Figure 15: *AoA CTE timing rules showing the transmit and receive guard and reference periods and switching slots [10]*

The guard periods are there to ensure that there is a gap between adjacent transmission. This prevents the transmissions interfering with each other. [10]

In AoD, the transmitter contains the antenna array, but the receiver performs the IQ sampling by taking measurements with a single antenna. The receiver needs to know the details of the design of the antenna array in the transmitter, creating the need to provide the receiver with details of the antenna array in the transmitter. Profiles for defining this will be published by the Bluetooth SIG in the future. [10]

In AoD, antenna switching is required when transmitting CTE, but not when receiving. AoD transmission timings are shown in Figure 16.

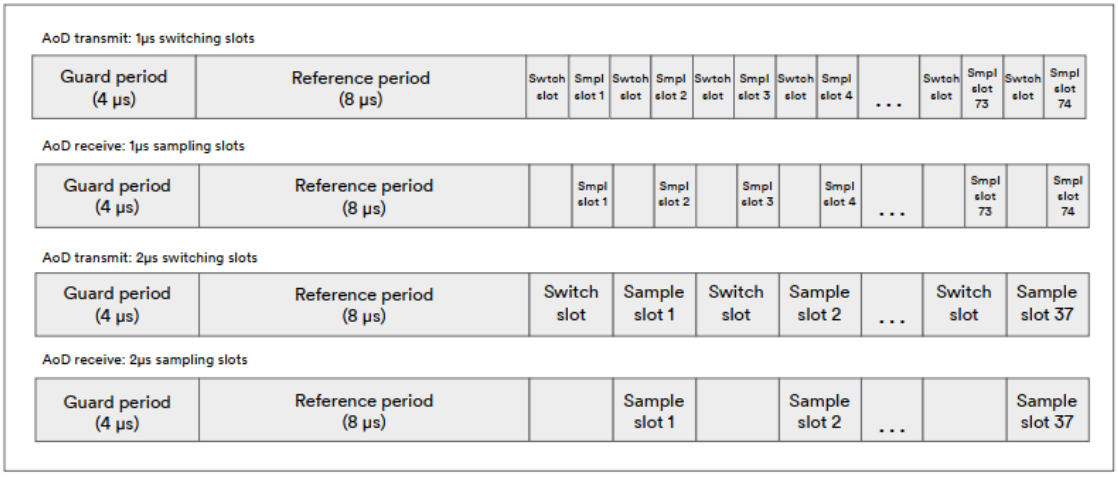

Figure 16: *AoD CTE timing rules showing the transmit and receive guard and reference periods and switching slots [10]*

The timing rules shown in Figure 15 and Figure 16 are to be used when implementing an antenna switching operationality for AoA or AoD.

4.3 Application-level considerations for direction-finding

The enhancements in Bluetooth 5.1 allow the raw material of direction finding to be produced, but the applications created for direction finding take responsibility for the actual application of the raw data, including calculating the angle from IQ samples. [10]

A few of these responsibilities are brought to attention in [10]. The application can determine the location of a beacon in regard to either global or local coordinates. It can determine a point or points of interest near the calculated location, or determine the phone orientation in 3D space. Details of the antenna array can be determined in the application. The CTE parameters can be configured using the application, and the IQ sampling can be configured. The algorithms and calculation of angles from IQ data also need to be done on application level. [10]

4.4 Commercial chipsets

There are many commercially available chipsets that support BLE direction finding. As the sending the CTE requires special hardware, not all chipsets that support Bluetooth 5.1 are capable of transmitting or receiving the signals related to AoA. Table 3 gives a few examples of commercial chipsets that can be used for BLE AoA.

Table 3: *Commercial chipsets that support BLE direction finding*

Manufacturer	Chipset	Notes
Texas Instruments	CC2642R	
	CC2642R-Q1	Automotive qualified
	CC2652RSIP	
	CC2652PSIP	
	CC2652P7	
	CC2652R7	
	CC2652RB	
	CC2652P	
	CC2652R	
Silabs	EFR32BG22	
	EFR32MG22	
	EFR32BG24	
	EFR32MG24	
Dialog Semiconductor	DA1469x	
Nordic Semiconductor	nRF52833	
	nRF52820	
	nRF52811	

All of the manufacturers mentioned in Table 3 provide also software support for direction finding, as well as tutorials and instructions for easy adaptation to their platform and product.

4.5 nRF52833 SoC and nRF Connect SDK

This chapter will introduce nRF52833 chipset, as it is used in the development kit that was used for the measurements in this thesis.

nRF52833 is a ***System on Chip*** (SoC) comprising an ARM Cortex M4 processor and several peripherals, including a dedicated radio transceiver module which in turn is used to implement the radio protocols. Other peripherals include an analog to digital converter, general input/output module, and a ***near field communication*** (NFC) module [26]. The nRF52833 also has modules for multiple serial communication protocols, including I2C compatible two-wire module, ***universal asynchronous receiver/transmitter*** (UART), and ***serial peripheral interface*** (SPI). Figure 17 shows the block diagram for nRF52833. [26]

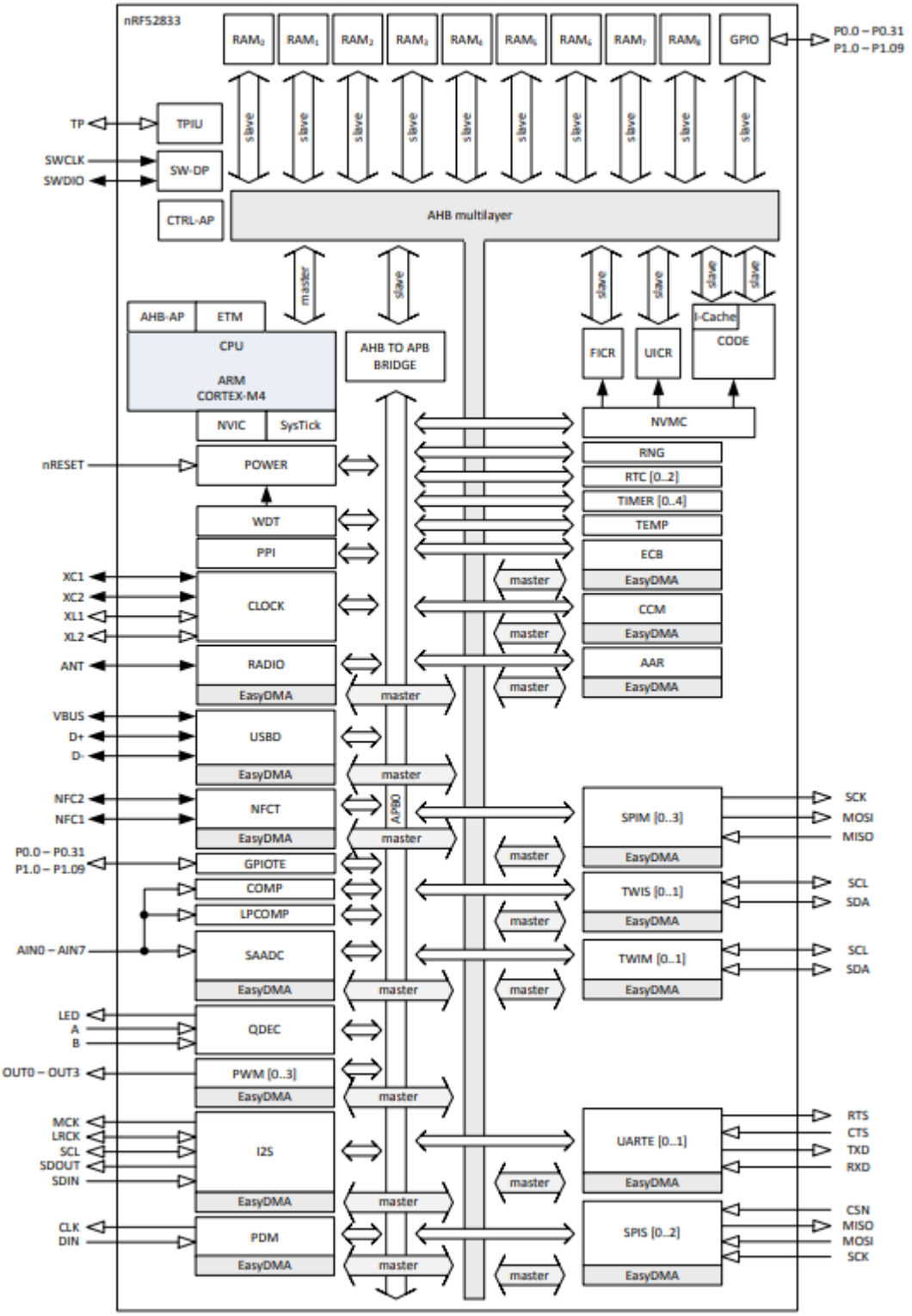

Figure 17: *NRf52833 block diagram showing the connections between the different peripherals, buses, and pins [26]*

The nRF52833 has 512 kB of flash memory and 128 kB of RAM memory. nRF52833 has **direct memory access** (DMA), which allows automated data transfers between memory and peripherals.

The radio transceiver in the Nordic SoC is compatible with multiple radio standards. These standards include IEEE 802.15.4 250 kbps mode, 1 Mbps and 2 Mbps BLE modes, and Long Range (125 kbps and 500 kbps) BLE modes. The module is also compatible with Nordic's proprietary radio protocols 1 Mbps and 2 Mbps modes. The module also has dedicated operationality that supports the direction finding. [26]

The direction finding mode can be selected using register DFEMODE. Figure 18 shows different DFEMODE settings.

		DFEMODE			
		AOA		AOD	
		TX	RX	TX	RX
AoA/AoD Procedure	Generating and transmitting CTE	x		x	
	Receiving, interpreting, and sampling CTE		x		x
	Antenna switching		x	x	

Figure 18: *nRFf52833 DFEMODE selection configuration register [26]*

Inline configuration can also be used. With inline configuration, further configuration of the AoA/AoD procedures are performed based on values in the received packet, namely CP bit and CTEInfo octet. If the inline configuration is not in use, the antenna switching and sampling are controlled using a register. [26]

Up to 8 ***general purpose input/output*** (GPIO) pins can be controlled by the radio module to control external antenna switches used in AoA direction finding. During receiving or transmitting each pin is controlled by the radio module. When not receiving or transmitting, each pin is controlled by the GPIO module. The switching pattern for antennas can be configured using the SWITCHPATTERN register. The SWITCHPATTERN register comprises 32 bits, of which the eight least significant bits each represent a GPIO pin. The pins which each bit represents are configured in eight registers named PSEL.DFEGPIO[n], where n represents each register. [26]

The radio uses direct memory access to write the IQ samples received during the CTE to RAM memory. Alternatively, the samples can be recorded to a register. The samples are recorded with respect to the RX carrier frequency. The format of the samples is in Figure 19.

SAMPLETYPE	Field	Bits	Description
0: I_Q (default)	Q	31:16	12 bits signed, sign extended to 16 bits
	I	15:0	
1: MagPhase	reserved	31:29	Always zero
	magnitude	28:16	13 bits unsigned. Equals 1.646756*sqrt(I^2+Q^2)
	phase	15:0	9 bits signed, sign extended to 16 bits. Equals 64*atan2(Q, I) in the range [-201,201]

Figure 19: *nRF52833 IQ sample format configuration register [26]*

Oversampling can be configured separately for the reference period and for the time after the reference period. [26]

Nordic Semiconductor also develops, maintains, and distributes a ***software development kit*** (SDK) called nRF Connect. The SDK comprises hardware abstraction layers for the chipset peripherals and a Bluetooth stack that supports mainly BLE. The stack is based on Zephyr Bluetooth Protocol Stack. [27]

The on Zephyr Bluetooth Protocol stack provided in nRF Connect SDK has 3 main layers:

- Host, which sits right below the application and comprises multiple network and transport protocols that enable applications to communicate with peer devices.
- Controller, which implements the Bluetooth Link Layer. It schedules the packet reception and transmission and guarantees the delivery of data.
- Radio hardware, which implements the required analog and digital baseband blocks that permit the link layer firmware to send and receive packets.

Figure 20 shows the stack architecture for single chip configuration.

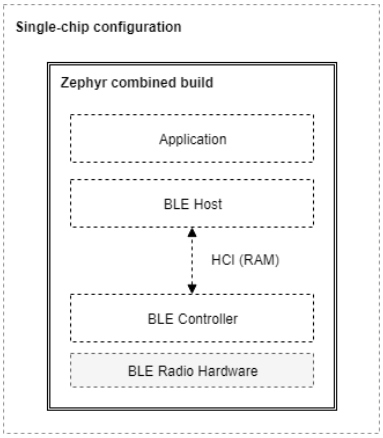

Figure 20*: Zephyr Bluetooth Stack Architecture [27]*

In addition to a single-chip configuration the stack can also be used in a dual-chip setting, where the application runs on a different SoC, which is connected to the radio SoC over UART or SPI. [27]

5. TESTING WITH XPLR-AOA-1 KIT

Bluetooth 5.1 direction finding exploration kit XPLR-AOA-1 by uBlox was used to test the BLE angle detection in practice. The kit comprises one antenna board and one tag. The antenna board is based on uBlox NINA-B411 series Bluetooth LE module, and the tag is based on Nina-B406 module. Both modules have Nordic Semiconductor nRF52833 SoC as the application and radio chipset.

5.1 uBlox XPLR-AOA-1

The test system comprises a tag that sends out broadcast data with CT extension, and an anchor point which determines the angles based on the received signal.

The antenna configuration on the anchor point board can be seen in Figure 21.

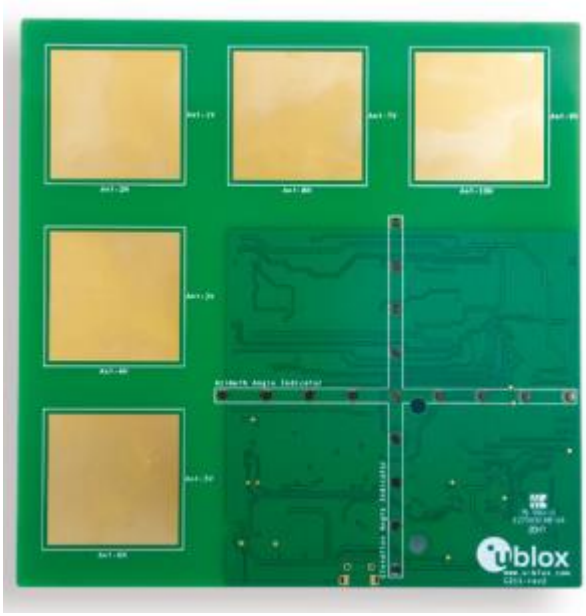

Figure 21: C211 Anchor Point Board

The antenna array comprises five dual-polarized antennas in a linear L-shape configuration. The antenna board has a NINA-B411 BLE module.

The u-Connectlocate software provided by uBlox uses all five antennas to calculate two angles: the azimuth and the elevation angle. The software uses the PDDA algorithm. The software boasts a ±5° mean error in angle calculation.

The tag is in Figure 22.

Figure 22: C209 tag

The tag has a Nina-B406 module which is visible in the right in Figure 22. The module has a built-in antenna. The tag has an acceleration sensor and a humidity sensor.

The tag transmits Eddystone ***Unique Identifier*** (UID), which is a 16-byte unique identifier by which different tags can be separated from each other. The benefit of using this type of advertising data for identification instead of using e.g. the MAC address is that the hardware can be replaced by providing a new tag that is configured to advertise the same UID. In case of MAC address being used the system needs to be updated to accommodate for the new MAC address.

5.2 Test description

The purpose of the test was to evaluate the UBlox kit angle determining capability by testing a single position with different settings, as well as to evaluate BLE AoA suitability for positioning.

In the test the locator board was attached to a tripod at 1.5 meter height, and the beacon was placed on a table at the same height at 3 meter distance from the locator. A piece of tin foil was also used to produce reflections for some of the tests. The tin foil was placed both in front of the beacon as well as behind the locator for different tests. This was done to determine whether the system is prone to errors due to signal reflections. The foil simulates situations where either the locator or the beacon are installed near metal surfaces.

The nine different measurements are referred to as Measurement 1 through 9. The measurement setups and names are in Table 4.

Table 4: *Measurement setups and descriptions*

Measurement name	Measurement setup
Measurement 1	1000 ms advertisement interval
Measurement 2	100 ms advertisement interval
Measurement 3	20 ms advertisement interval
Measurement 4	1000 ms advertisement interval, foil behind locator
Measurement 5	100 ms advertisement interval, foil behind locator
Measurement 6	20 ms advertisement interval, foil behind locator
Measurement 7	1000 ms advertisement interval, foil behind tag
Measurement 8	100 ms advertisement interval, foil behind tag
Measurement 9	20 ms advertisement interval, foil behind tag

The angle data provided by the locator over a virtual COM port was stored to a text file and the data was analysed using a Python script with Pandas and Seaborn libraries for visualization.

Here is one row of output as an example of output from the u-Connectlocate software:

```
+UUDF:CCF9579D6FB0,-79,4,-58,0,38,"CCF9579B22A1","",5951
```

The fields are separated by commas. The first field is the Eddystone UID of the tag, the second field is the RSSI of the first polarization, the third field is the azimuth angle, the fourth field is the elevation angle, the fifth field is the RSSI of the second polarization, which is removed from current SW releases and thus is 0 all the time. The sixth field is the advertisement channel, the seventh field is the antenna board ID, the eighth field is a user string that can be set to anything in the u-Connectlocate software, and the ninth field is the timestamp as milliseconds from the device boot.

Output from each test run was converted to a Pandas dataframe, and the Seaborn library was used to visualize the data.

5.3 Test results

The first notable result was that with 1000 millisecond advertisement interval the RSSI and azimuth and elevation angle results were dependent of the advertisement channel.

Figure 23 shows the azimuth angle for measurement 1 with data from different channels shown in different colors.

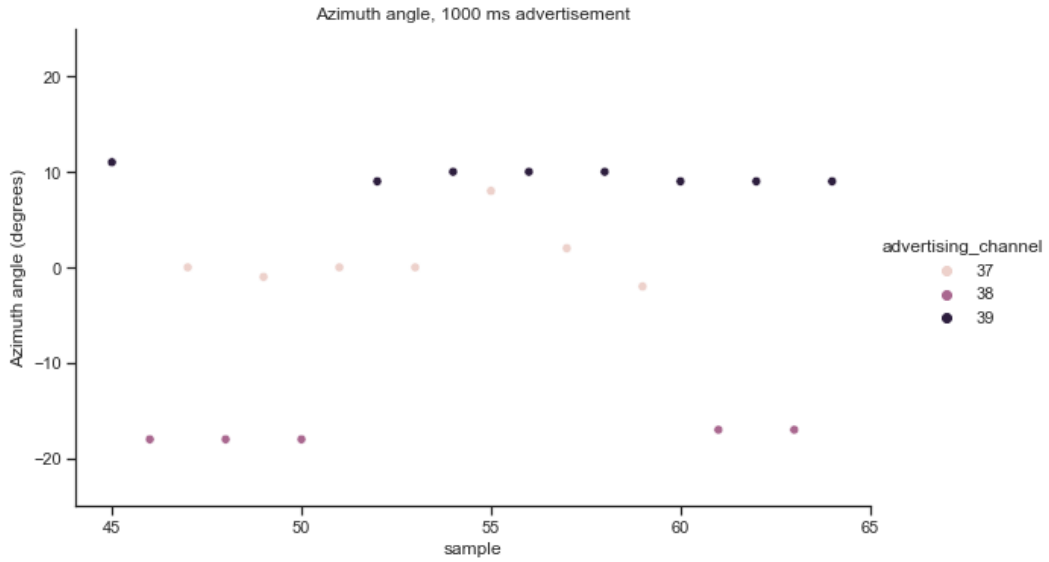

Figure 23: *Measurement 1 azimuth angle with channels shown in separate colors*

Figure 24 shows the elevation angle for 1000 ms advertisement interval. The same channel dependency can be seen for the elevation angle: the different channels produce consistently different angles.

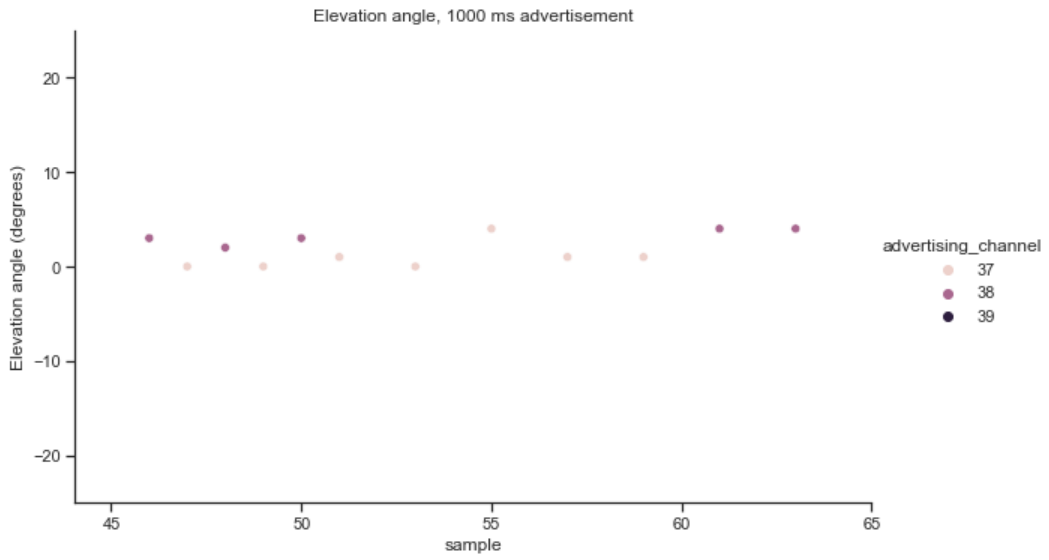

Figure 24: *Measurement 1 elevation angle with channels shown in separate colors*

The difference between channels can be best seen in a density plot, which plots the density of the angle values separately for each channel. Figure 25 shows the density plot for azimuth angle measurement for each channel.

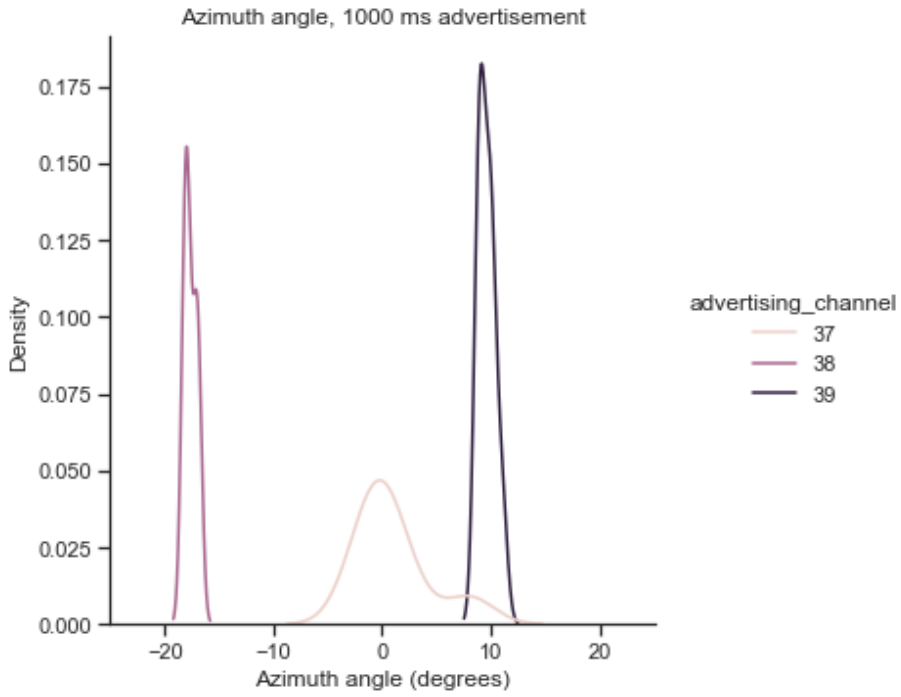

Figure 25: *Measurement 1 azimuth density plot per channel*

As it can be seen in Figure 25, channel 37 produces angle data around 0 degrees, whereas channel 38 produces values around -19 degrees, and 39 around 10 degrees. The difference between channels is well beyond the ±5 degrees accuracy given in the development kit description. The angle calculated from channel 37 is closest to the expected 0 degrees.

The RSSI also displays channel dependency, with Figure 26 showing the RSSI for 1000 millisecond advertisement.

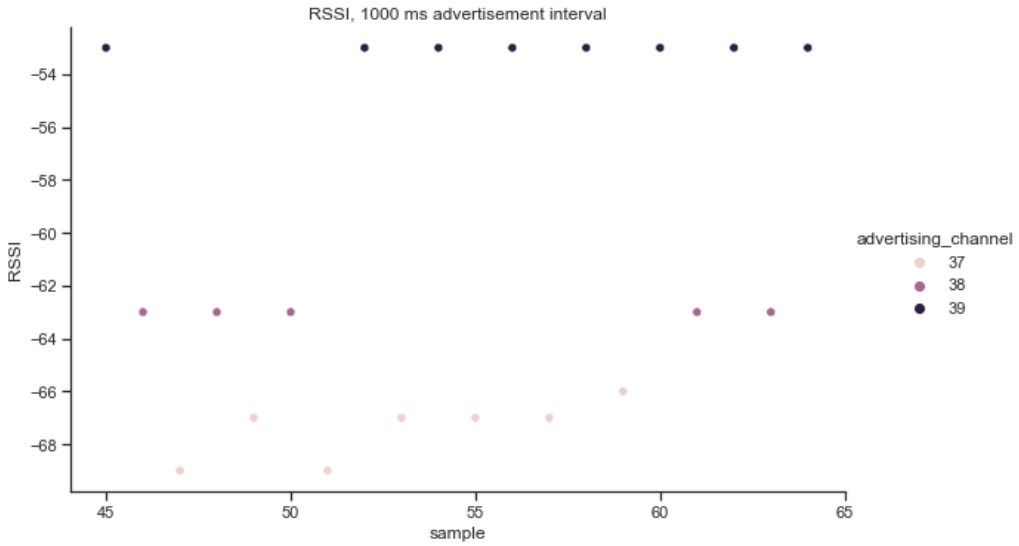

Figure 26: *Measurement 1 RSSI with channels shown in separate color*

Measurement 2 was done otherwise similarly, except with a 100 ms advertisement interval. The density plot in Figure 27 for the azimuth angle shows that the perceived angle is less dependent on the channel, and close to the expected 0 degrees

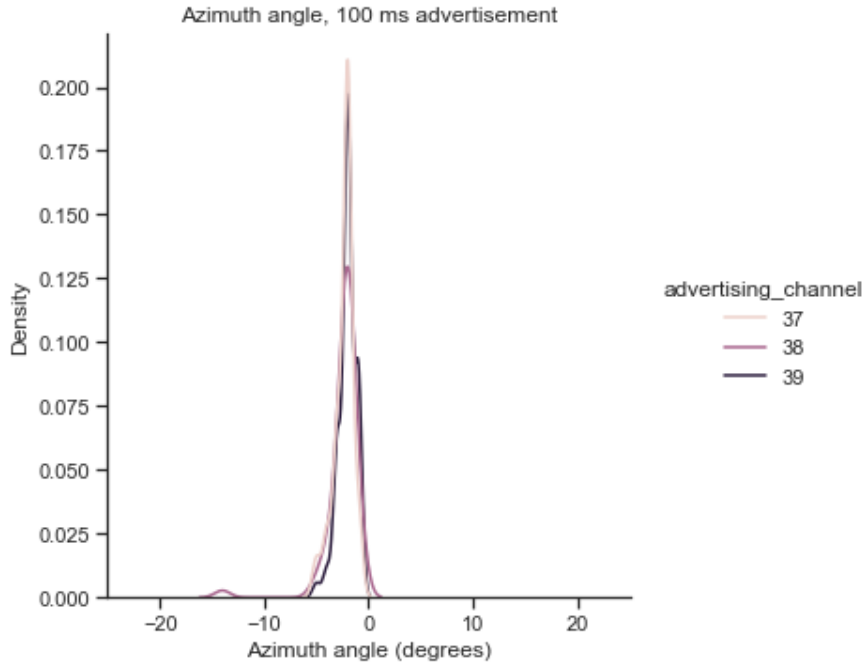

Figure 27: *Measurement 2 azimuth angle density plot*

The same applies for elevation angle shown in Figure 28.

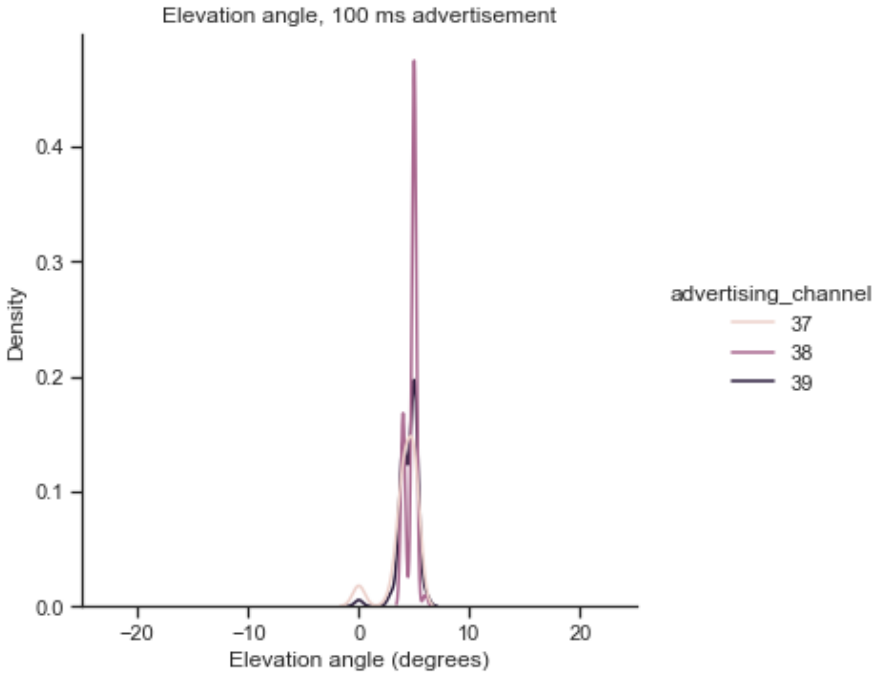

Figure 28: *Measurement 2 elevation angle density plot*

RSSI also is less dependent of the advertisement channel.

In Measurement 3 the advertisement interval was increased to 20 ms, and the results are even more accurate as seen in Figure 29. The resulting density plot has two small side lobes, which are well within the ±5 degrees accuracy.

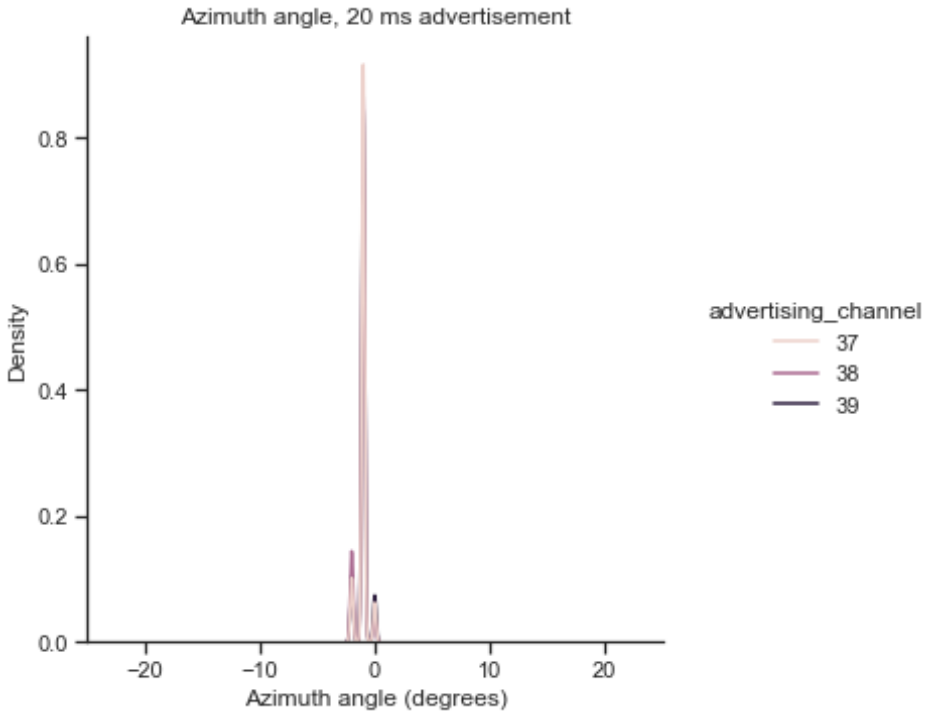

Figure 29: *Measurement 3 azimuth angle density plot*

From the results of measurements 1 through 3 it can be determined that the advertisement interval produces a difference in the accuracy of calculated angle. The channel-dependency reduces when the advertisement interval is increased, and the density plots become narrower, meaning that there is less divergence with the values. The resulting values are also close to the expected 0 degrees.

The foil placement behind the tag or locator changed the results somewhat, which can be interpreted so that the reflections are have some effect in the angle calculation accuracy for the PDDA algorithm implementation used in this devkit. Figure 30 shows the azimuth angle from Measurement 6 as an example. There are two peaks almost as high a degree apart, but all of the values are still within the ±5 degrees accuracy.

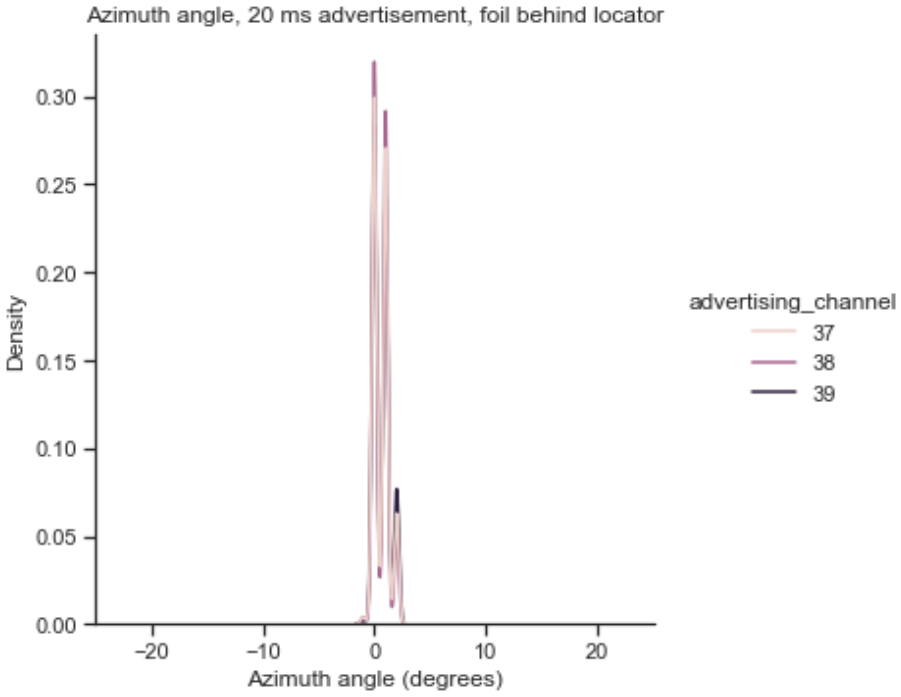

Figure 30: *Measurement 6 azimuth angle density plot*

Placing the foil behind the tag had some effect to the results. As Figure 31 shows, for 1000 millisecond advertisement interval the resulting angles were dispersed over a 20 degree range ranging from -10 to 10 degrees with heavy channel dependency.

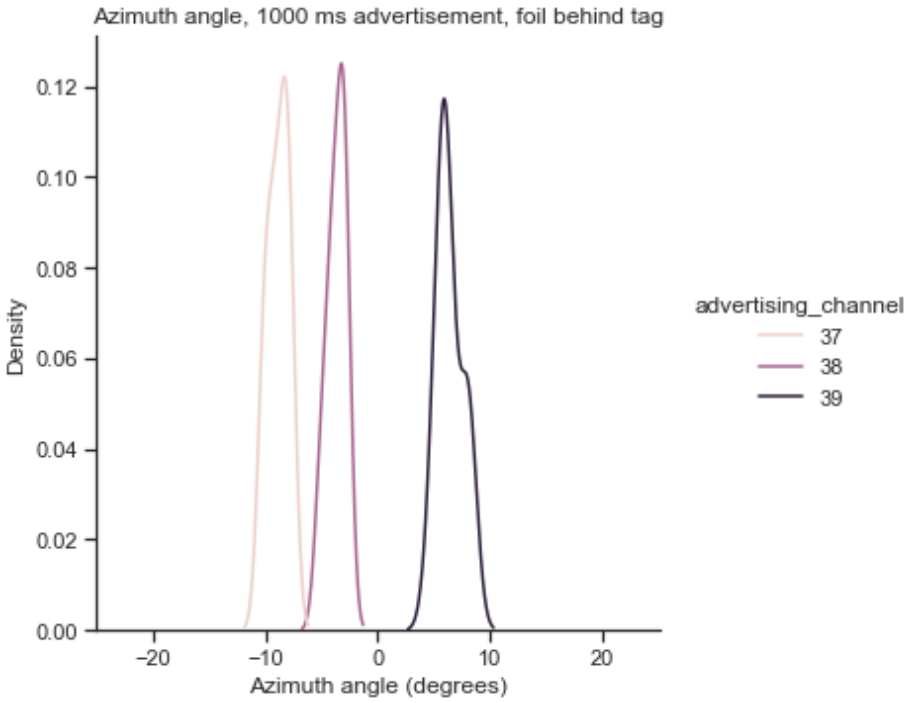

Figure 31: *Measurement 7 azimuth angle density plot*

For 20 millisecond advertisement there was a 20 degree error as can be seen in Figure 32. This could be interpreted so that only reflected signals were used in angle calculation, and the reflection came from a 20 degree angle.

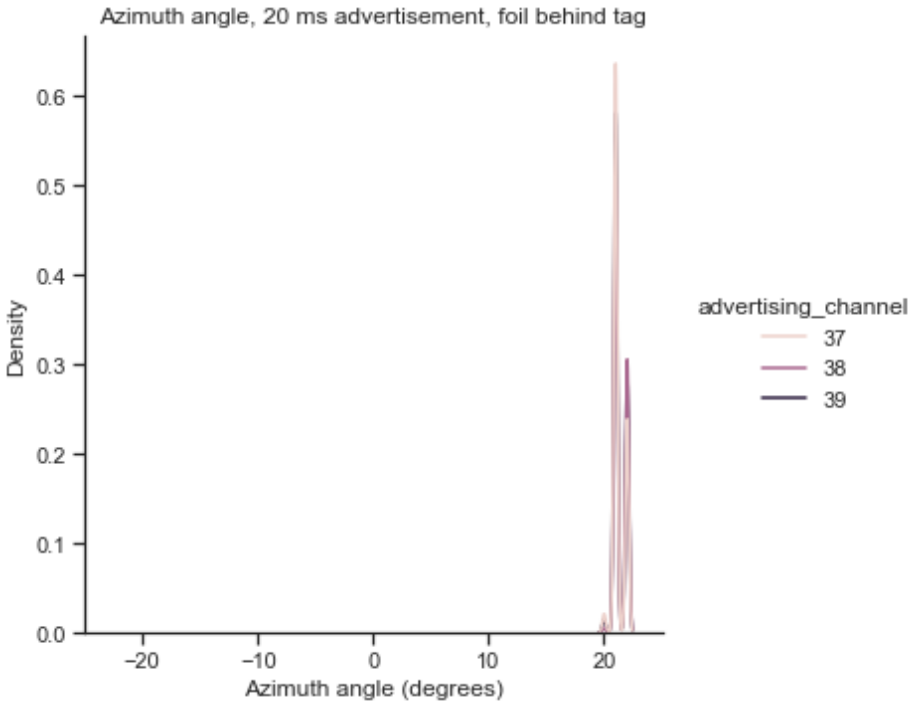

Figure 32: *Measurement 9 azimuth angle density plot*

Statistical variables were also calculated for each measurement to further see how much difference the tin foil and advertisement interval make.

The azimuth angle mean and standard deviation of each measurement over all channels is in Table 5.

Table 5: *Measurement mean and standard deviation over all channels*

Measurement	Azimuth Mean	Azimuth Std deviation
Measurement 1	-0.200000	11.161965
Measurement 2	-2.270000	1.214279
Measurement 3	-1.055000	0.405141
Measurement 4	-2.250000	10.661663
Measurement 5	1.085000	0.518768
Measurement 6	0.618000	0.668223
Measurement 7	-1.950000	6.723682
Measurement 8	28.150000	1.369994
Measurement 9	21.304000	0.493789

Table 5 shows that the standard deviation is smaller with higher advertisement interval, meaning that there is less variation in he angle calculation when the CTE is transmitted more often. The deviation is largest in Measurement 1, Measurement 4, and Measurement 7, which indicates that the advertisement interval is a large factor in the accuracy of the measurements.

6. CONCLUSIONS

Evaluating Bluetooth AoA through the performed tests using parameters given in chapter 2.5, we see that the accuracy and precision are greatly affected by reflections and advertising interval. The coverage of Bluetooth AoA can be derived from the maximum range of 100 meters, although the need for direct LoS means that in an indoor setting that has many walls there might be need for many locators to ensure direct LoS in every place. The hardware complexity is not a huge matter, as BLE chipsets are small, and do not take much current. Software complexity could be somewhat of an issue, as there is most likely need for a complicated algorithm for both determining the angle of arrival, and for positioning. The cost of the system could be affected by the energy needs for the algorithms, the need for a large number of locators because of the need for direct LoS, and the need to replace batteries or units with non-replaceable batteries. The latency could also become an issue if the algorithms take a long time to complete. Scalability is affected by the already congested 2.4 GHz operation frequency, and the need for LoS from the asset to the locator, possibly leading to a very large number of locators needed to cover a large space. The servers or locators could also get congested by the computational load presented by the heavy algorithms needed.

Even though there are many downsides, Bluetooth direction finding seems like a promising addition to the local positioning domain. The already existing Bluetooth ecosystem and tools make adopting the technique easy. However, the problems for direction finding are the same as for all radio signal based positioning, being multi-path propagation and non-LoS propagation. This makes the positioning work unreliably in settings where there are a lot of walls dividing the space, or a lot of moving obstacles, such as crowds in shopping malls, or maritime ports, which both are potential locations for local positioning.

The development kit for practical tests was selected purely by availability, as the currently unfolding global microchip shortage has severely affected manufacturers and retailers. The tests that were done in the practical tests were selected based on the feasibility of conducting such experiments with the tools available. The development kit and included software did not provide means to extract raw phase and amplitude data, so the algorithms could not be put to test. Also, only one development kit was purchased, meaning that the actual positioning could not be tested as it requires three units, limiting the experiments to testing the accuracy of the received angle instead of actual positioning.

As the practical test demonstrates, the advertisement interval of the transmitting device can be crucial factor in the angle detection, which also means higher current consumption than the minimum values given by manufacturers. The channel dependency exhibited in some of the tests is also an interesting phenomenon, which could cause issues with positioning accuracy. It would be interesting to know whether this is a common phenomenon with Bluetooth direction finding, or just limited to this chip vendor, or the PDDA algorithm implementation used in the uConnectlocate software.

REFERENCES

[1] F. Zafari, A. Gkelias, and K. K. Leung, “A Survey of Indoor Localization Systems and Technologies,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019, doi: 10.1109/COMST.2019.2911558.

[2] H. Liu, H. Darabi, P. Banerjee, and J. Liu, “Survey of wireless indoor positioning techniques and systems,” *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 37, no. 6. pp. 1067–1080, Nov. 2007. doi: 10.1109/TSMCC.2007.905750.

[3] A. Bensky, *Wireless positioning technologies and applications*, Second edition. Boston,Massachusetts: Artech House, 2016.

[4] A. Hameed and A. Ahmed, *Survey on indoor positioning applications based on different technologies*. 2018.

[5] P. S. Farahsari, A. Farahzadi, J. Rezazadeh, and A. Bagheri, “A Survey on Indoor Positioning Systems for IoT-based Applications,” *IEEE Internet Things J*, 2022, doi: 10.1109/JIOT.2022.3149048.

[6] M. Youssef and A. Agrawala, “The Horus location determination system,” *Wireless networks*, vol. 14, pp. 357–374, 2007.

[7] B. O’keefe, “Finding Location with Time of Arrival and Time Difference of Arrival Techniques,” 2017. https://sites.tufts.edu/eeseniordesignhandbook/files/2017/05/FireBrick_OKeefe_F1.pdf (accessed Sep. 20, 2022).

[8] Bluetooth Special Interest Group, “Bluetooth ® Specification Bluetooth Core Specification Rev. v5.2,” 1999. https://www.bluetooth.com/specifications/adopted-specifications

[9] Mathworks, “Bluetooth Location and Direction Finding - MATLAB & Simulink - MathWorks Nordic,” 2022. https://se.mathworks.com/help/comm/ug/bluetooth-direction-finding.html (accessed Dec. 28, 2021).

[10] M. Woolley, “Bluetooth Direction Finding A Technical Overview,” 2021. https://www.bluetooth.com/bluetooth-resources/bluetooth-direction-finding/ (accessed Sep. 11, 2022).

[11] A. Malik, “RTLS for DUMMIES,” *Wiley Publishing*, 2009.

[12] “International Organization for Standardization.” https://www.iso.org/home.html (accessed Sep. 20, 2022).

[13] M. Md Din, N. Jamil, J. Maniam, and M. Afendee Mohamed, “Indoor positioning: technology comparison analysis,” *International Journal of Engineering & Technology*, vol. 7, no. 2, pp. 133–137, 2018.

[14] M. Cominelli, P. Patras, and F. Gringoli, “Dead on Arrival: An Empirical Study of The Bluetooth 5.1 Positioning System,” *ACM WiNTECH 2019*. https://doi.org/10.48550/arXiv.1909.08063 (accessed Sep. 19, 2022).

[15] Mathworks, “MUSIC Super-Resolution DOA Estimation.” https://se.mathworks.com/help/phased/ug/music-super-resolution-doa-estimation.html (accessed Apr. 02, 2022).

[16] D. C. Lay, *Linear Algebra and its Applications (Fourth edition)*, 4th ed., no. 3. Addison-Wesley, 2012.

[17] R. O. Schmidt, “Multiple emitter location and signal parameter estimation,” *IEEE Trans Antennas Propag*, vol. AP-34, no. 3, pp. 276–280, 1986, doi: 10.1109/tap.1986.1143830.

[18] L. Stanković, E. Sejdić, S. Stanković, M. Daković, and I. Orović, “A Tutorial on Sparse Signal Reconstruction and Its Applications in Signal Processing,” *Circuits Syst Signal Process*, vol. 38, no. 3, pp. 1206–1263, Mar. 2019, doi: 10.1007/s00034-018-0909-2.

[19] Z. Yang, L. Xie, and C. Zhang, “Off-grid direction of arrival estimation using sparse bayesian inference,” *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 38–43, 2013, doi: 10.1109/TSP.2012.2222378.

[20] M. A. G. Al-Sadoon *et al.*, “A new low complexity angle of arrival algorithm for 1D and 2D direction estimation in MIMO smart antenna systems,” *Sensors (Switzerland)*, vol. 17, no. 11, Nov. 2017, doi: 10.3390/s17112631.

[21] M. A. G. Al-Sadoon, “Direction finding and beamforming techniques using antenna array for wireless system applications,” University of Bradford, Bradford, 2019.

[22] B. Friedlander, “Wireless Direction-Finding Fundamentals,” in *Classical and Modern Direction-of-Arrival Estimation*, 2009. doi: 10.1016/B978-0-12-374524-8.00001-5.

[23] P. Stoica and A. Nehorai, “MUSIC, maximum likelihood and Cramer-Rao bound: further results and comparisons,” in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 1989, vol. 4, pp. 2605–2608. doi: 10.1109/icassp.1989.267001.

[24] N. Gupta, *Inside Bluetooth Low Energy*, Second edition. London: Artech House, 2016.

[25] Nordic Semiconductor, “Direction Finding,” 2020. https://infocenter.nordicsemi.com/pdf/nwp_036.pdf (accessed Sep. 11, 2022).

[26] Nordic Semiconductor, “Objective Product Specification v0.7,” 2019. https://infocenter.nordicsemi.com/pdf/nRF52833_OPS_v0.7.pdf (accessed Sep. 11, 2022).

[27] Zephyr Project, “Bluetooth Stack Architecture,” Sep. 11, 2022. https://developer.nordicsemi.com/nRF_Connect_SDK/doc/latest/zephyr/connectivity/bluetooth/bluetooth-arch.html (accessed Sep. 11, 2022).