# INVESTIGATION OF RANGING CAPABILITIES WITH BLUETOOTH LOW ENERGY

Bachelor Thesis

*Submitted in fulfillment of the requirements for the degree of Electrical Engineering Bachelor*

*By*

Danilo TOAPANTA

*Under the supervision of:*

Chair: Prof.dr.ir. Andre Kokkeler
&
Supervisor: Dr.ing. Anastasia Lavrenko
Dr. Siavash Safapourhajari

UNIVERSITY OF TWENTE.

Electrical Engineering, Mathematics and
Computer Science Department (EEMCS)
Radio Systems Group (RS)

June 28, 2021

UNIVERSITY OF TWENTE

# *Abstract*

Bachelor of Engineering

**INVESTIGATION OF RANGING CAPABILITIES WITH BLUETOOTH LOW ENERGY**

by Danilo TOAPANTA

With the rapid advancement of wireless technologies, positioning systems have become very popular. Applications in the area of logistics such as asset tracking or inventory management require localization accuracy in the range of a few meters. Among available solutions Bluetooth Low Energy (BLE) is an innovative technology that delivers high accuracy while maintaining low power consumption. In order to locate a device, several approaches can be used. In this report we investigate a phase-based ranging system that makes use of the complete bandwidth of Bluetooth and study how practical system constraints affect distance estimation accuracy.

# Contents

# 1 Introduction

In positioning, ranging is one of the key components for distance estimation. With the advancement of technology, many robust and sophisticated positioning systems have been designed. Most of them, however, tend to be bulky and demand a great amount of power for proper functioning [1]. These are therefore not viable solutions for applications where power consumption is a constraint. Fortunately, in 2011 Bluetooth Low Energy (BLE) was introduced, a wireless technology that offers localization services with low-energy consumption. Since then, research has been conducted to leverage the functionalities that this technology offers. One of them is the new possibility to utilize the new packet structure to enable ranging [2]. The latter being the topic of this thesis and further elaborated in the following sections.

## 1.1 Motivation

This thesis is a collaborative work with the BouWatch company. BouWatch is a firm that provides temporary surveillance and monitoring solutions in construction sites [3]. Every year, construction companies incur losses due to the misplaced or stolen materials and tools. For that reason, besides the 360°cameras service, the company has been looking into smart software technologies to enhance their services. Naturally, this is the case for distance estimation as a great part of security relies on the underlying concept of tracking and ranging calculations. Moreover, due to the ever increasing deployment of construction tools with built-in BLE chips, the interest of the research community and the private sector has turned towards the opportunities it offers [4].

## 1.2 Research Question

The main question that this paper will address is the following:

> Q. How can we effectively estimate the range between a (commercial off the shelf) BLE beacon and a BLE receiver (locator)?

More specifically, this thesis aims to investigate the capabilities that BLE offers to determine the distance between two antennas, i.e., transmitter and receiver, under non-ideal conditions.

## 1.3 Procedure & Timeline

Previous work on this assignment, a preparation period to understand the different ranging techniques and its relation with BLE was conducted. For that, several papers were studied and later on used to understand the research question. Similarly, to tailor and narrow down the research question, an introductory meeting was held at Bouwatch at the beginning of this

project. To structure and organize the workflow of this thesis a Gantt chart was constructed. This can be found in the Appendix section [16].

## 1.4 Thesis Outline

The rest of the report is structured as follows:

**2 Background** gives an overview of current ranging techniques and introduces the importance of BLE in this thesis report.

**3 Ranging Algorithm** introduces the algorithm for distance estimation and explains how it works.

**4 Simulations & Results** explores the different parameters that affect range estimation and presents results based on simulations.

**5 Conclusions & Future Work** summarizes the findings and suggests future work to further improve the performance of the algorithm.

# 2 Background

This section presents the background and relevant information to understand the problem of range estimation. Additionally, it covers the importance of BLE in the context of ranging and provides a general overview of how low-cost electronic devices may be used to estimate distance.

## 2.1 Ranging Techniques

Wireless localization techniques have become popular in recent years. With the internet-of-things, accurate and scalable systems are much needed. Localization systems can be categorized as indoors and outdoors depending on the use-case. In this report, an outdoor setting is considered. For that, in order to estimate the distance between two antennas three main approaches can be found in the literature [5]. These are: time-based, power-based and phase-base approaches.
In this section a description per each method is provided and at the end, the phase-base approach is discussed in more detail.

### 2.1.1 Time-based methods

In a time-based approach, the distance between two devices is calculated based on propagation time delay. With that, one can use the speed of light and thus calculate the distance traveled from one device to another. Here, techniques such as Time of Flight (ToF), Time of Arrival (TDoA) or Round Trip Time of Flight (RT-ToF) can be found in the literature [5]. All of these methods however, require strict time synchronization. In order to accurately calculate the distance, high synchronization of clocks and local oscillators must be accomplished.

### 2.1.2 Power-based methods

The next category are power-based approaches. Here, the distance between the transmitter and receiver is calculated based on the attenuation of the incoming signal. This method is referred as Received Signal Strength Indicator (RSSI) and unfortunately is highly dependant on environmental conditions such as multi-path fading or moving objects [6]. For that reason, this approach may not deliver accurate results.

### 2.1.3 Phase-based methods

This is the last group in the list and the approach that will be the focus of this thesis. Phase-based ranging techniques utilize phase measurements in order to calculate the distance between two electronic devices i.e one beacon and one transmitter. In order to calculate a

distance, a transmitter (Tx) sends a signal which is echoed back from a receiver (Rx) and compared to the transmitted signal. By measuring the phase shift between these two the distance can be calculated [7]. The following figure illustrates this procedure:

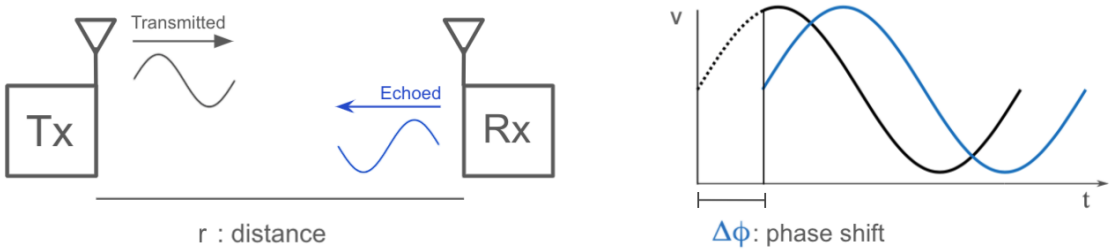



Figure 1: Distance estimation using phase-based approach.

On the left-hand side, fig. 1 shows a typical set up for range estimation. A transmitter sends a tone signal and a receiver gets this tone and forwards it back to the transmitter. At Tx, the echoed and transmitted tone can be seen on the right-hand side of fig. 1. What is important here is the phase shift that the tone undergoes while traveling a distance $r$. This is essentially the principle of phase-based approaches. The phase shift is related to the distance the tone traveled [8]. If we can estimate the phase shift then we can determine the distance.

Naturally, a system as such would be able to calculate distances in the range of meters and even kilometers. The problem however, is that more than one antenna is required to attain these results and certainly the procedure becomes not power-friendly. For these reasons, when looking into wireless technologies that can estimate distance in the range of meters without compromising power consumption, Bluetooth Low Energy appears as an available solution. In the following section the importance of this technology to distance estimation is discussed.

## 2.2 Bluetooth Low Energy

Bluetooth Low Energy, or BLE in short, is a wireless technology first introduced in 2011 by the Special Interest Group (SIG) [9]. It operates in the band between 2400 MHz and 2485 MHz. It focuses on low power consumption and is well suited for coin cell batteries or energy-harvesting devices. That means applications in healthcare, fitness, security and home entertainment fields are now able to utilize small electronic devices as to perform certain activities, among those is range estimation. The table below summarizes the main technical specifications that are relevant to this thesis.

Table 1: BLE Technical Specifications [10]

| Parameter | Value |
|---|---|
| Total no. Channels | 40 |
| Advertisement Channels | 37, 38, 39 |
| Frequency hop | 2MHz |
| Frequency band | 2.4GHz |
| Modulation technique | GFSK |
| Package length | 72-216$\mu$s |
| Min. SNR allowed | 21dB |

### 2.2.1 Features of BLE v5.1 for ranging

Recently, in 2019, SIG released a new version for Bluetooth Low Energy, BLE v5.1. In that release two important features that allow ranging calculations were defined. Following is a short summary of each one.

- **Constant Tone Extension**
  At the link layer, a new field called Constant Tone Extension (CTE) was defined. The purpose of this field is to send a single tone wave that can later be used for IQ sampling [11]. IQ sampling is the process of sampling a valid packet. By doing that, phase information among other parameters can be obtained. Below the structure of an advertisement packet with the inclusion of CTE is presented [6].

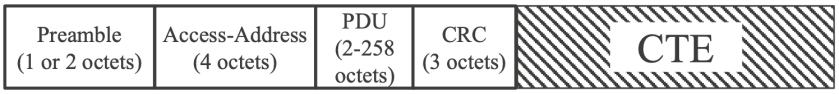



Figure 2: Advertisement Packet Structure BLE v5.1

The fields of fig. 2 are described as follows:

- Preamble: used for frequency synchronization and timing estimation at the receiver.

- Access Adress: fixed number per each Link Layer connection.

- PDU: field where data information is sent. A breakdown of this field can be found in the appendix of this report, namely fig. 17.

- CRC: error-correction code used to detect errors in the packet.

- CTE: sine tone wave with 16 to 160 $\mu s$ time duration.

- **Periodic Advertisement Package**
  With the addition of CTE, periodic advertisement was included. Before BLE v5.1 when sending advertisement packages a randomness in event scheduling used to be the case [12]. Now, with the inclusion of this feature, SIG introduces the ability to perform periodic and deterministic advertising. This allows scanners, Rx, to synchronise their timing and expect packets within a deterministic time. This not only allows power efficiency because the receiver will now have a pre-determined time to expect a package but also provides the user with control over utilized channels.

- **Secondary Advertisement Channels**
  Secondary channels are channels that are not dedicated solely for advertisement. These run from channel 0 to 36th. The importance of this with ranging lies in the fact that now IQ sampling can be done not only in one advertisement event but also over remaining secondary channels [13]. This is important because multiple phase measurements can lead to improvements in range estimation performance as it will be discussed in the following chapter. As an illustration the following figure elaborates on how this feature works.

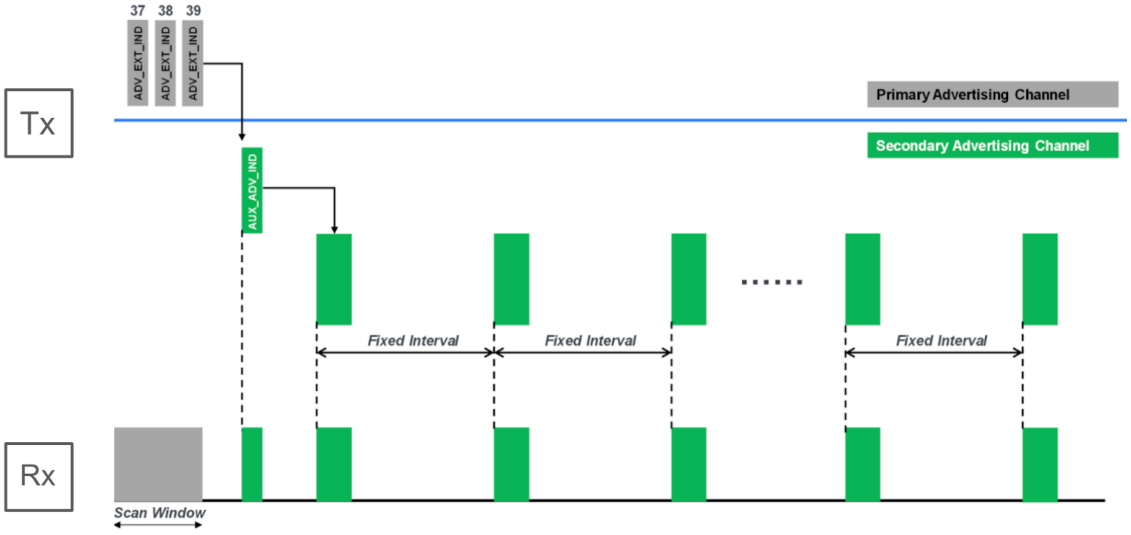



Figure 3: Periodic advertisement and use Secondary channels in BLE v5.1

Fig. 3 shows the sending of packets over secondary channels. These are depicted in green color. Previous to that, a series of connection events happen in the primary advertisement channels which is represented by the grey box in the left corner of the figure. There, two antennas are shown. These are represented by Tx, Rx and stands for transmitter and receiver, respectively. Additionally, it can be seen that the sending of packets by secondary channels are governed by a fixed internal which explains the functioning of periodic advertisement.

# 3 Ranging Algorithm

This chapter is dedicated to answer the research question and will be divided in two sections. The first being how to determine the range and the second how to improve these results based on the exploration study that was carried out.

## 3.1 How to calculate range?

To determine the distance between a transmitter and a receiver, the change in phase due to the distance the radio signal travels can be used. Consider the following scenario. Tx sends a tone with frequency $f_k$ to Rx. For ease of index notation the transmitting side will be called Initiator (I) and the receiving side, the Reflector (R). To describe a sinusoidal signal the following equation can be used:

$$u(t, f_k) = \cos(2\pi f_k t + \varphi_I) \tag{1}$$

Eq. 1 is a transmitted carrier signal at $f_k$. Here the term $\varphi_I$ accounts for an unknown phase offset of the initiator. Note, the amplitude was intentionally set to one as phase information is contained within the argument of the cosine and does not depend on the amplitude of the signal.

In a pure Line-of-Sight (LOS) radio channel, the electromagnetic signal will experience a phase delay at the receiving side. The reflector is located at a distance $r$ from the transmitter and therefore receives a phase delayed tone compared to the initiator. [6] More specifically, the reflector before demodulation receives the following tone:

$$u(t, f_k, r) = \cos(2\pi f_k t + \varphi_I + 2\pi f_k \frac{r}{c} - \varphi_R) \tag{2}$$

In eq. 2, two new phase terms are introduced. The first, $2\pi f_k \frac{r}{c}$, is the propagation term which contains distance information; $c$ stands for the speed of light. The second term, $\varphi_R$, is an unknown phase offset with respect to the reflector.

Certainly without any more information, finding the distance that separate these two devices would be an impossible task to accomplish. There are two unknowns for one equation. Here is where the solution comes in.

The reflector demodulates eq. 2 and down-converts the tone to DC.

$$u'(f_k, r) = cos(\varphi_I + 2\pi f_k \frac{r}{c} - \varphi_R) \tag{3}$$

The down-converted signal, eq. 3 is now passed to the IQ sampler where phase information

is extracted:

$$\phi_R(f_k, r) = 2\pi f_k \frac{r}{c} + \varphi_I - \varphi_R \tag{4}$$

The reflector now sends back a tone to the initiator and at the same time the phase information obtained in eq. 4. To accomplish that, the packet structure of BLE v5.1 is used. In the PDU data field of an advertisement package, the reflector encodes $\phi_R$ and sends this to the initiator. Additionally, in the same advertisement packet, the reflector is able to send a tone under the CTE field. This tone contains the same frequency as the initiator.

The attentive reader, may ask how does the reflector know which frequency to use? The answer for that is a series of connection events that happened before this procedure. Namely, these events account for timing synchronization and channel frequency selection [11]. Thus, this is a handled procedure that is not relevant for the problem at hand. What is important for the ranging problem is the following.

At the initiator, two important pieces of information are conveyed. One of them is the term $\phi_R$ and the other the tone sent by the reflector from which phase information can be extracted. That is:

$$\phi_I(f_k, r) = 2\pi f_k \frac{r}{c} + \varphi_R - \varphi_I \tag{5}$$

It follows now, by adding equation 4. and 5. that:

$$\phi_{2w}(f_k, r) = \phi_R + \phi_I = 4\pi f_k \frac{r}{c} \tag{6}$$

Where, $2w$ represents a two way communication system i.e., initiator and reflector. An expression for $r$ at the transmitting side is obtained:

$$r = \frac{c}{4\pi} \frac{\phi_{2w}}{f_k}, \quad \mathrm{mod}(2\pi) \tag{7}$$

From eq. 7 one can derive the following conclusions:

1. The unknown phase offsets, $\varphi_R$ and $\varphi_I$, do not play a role when calculating range. They cancel out in eq. 6. Fortunately, this would be the same outcome, if for instance, a connection between initiator and a new reflector is to occur.

2. Range calculations are susceptible to range ambiguity. That is, at $2\pi$ phase measurements the range calculations will roll back and provide a misleading result.

3. An expression to estimate the maximum range when using a single tone can be found.

For any $f_k$ provided that max $\phi_{2w} = 2\pi$ an expression for $r_{max}$ can be found:

$$r_{max} = \frac{c}{2f_k} \tag{8}$$

It follows from eq. 8 that when using the lowest frequency and therefore the first channel in BLE, the maximum range that can be estimated without any range ambiguity is $r_{max} = 0.06m$. This is a rather small distance which can be further improved. The following section explains exactly how to do this.

## 3.2 MCPD Algorithm

In the previous section it was found that the maximum range when using a single tone lies in the range of centimeters. A quick look at eq. 8 reveals a way to increase the range. That is by decreasing $f_k$. However, this is not attainable because the bandwidth of BLE starts at 2.4GHz. What is possible, however, is the following.

After sending a tone with frequency $f_k$, the initiator repeats the same procedure as before but now with a frequency tone $f_{k+1}$. A new phase difference, $\phi_{2w}(f_{k+1}, r)$, can then be estimated. The result of these two tone exchanges is shown in the figure below:

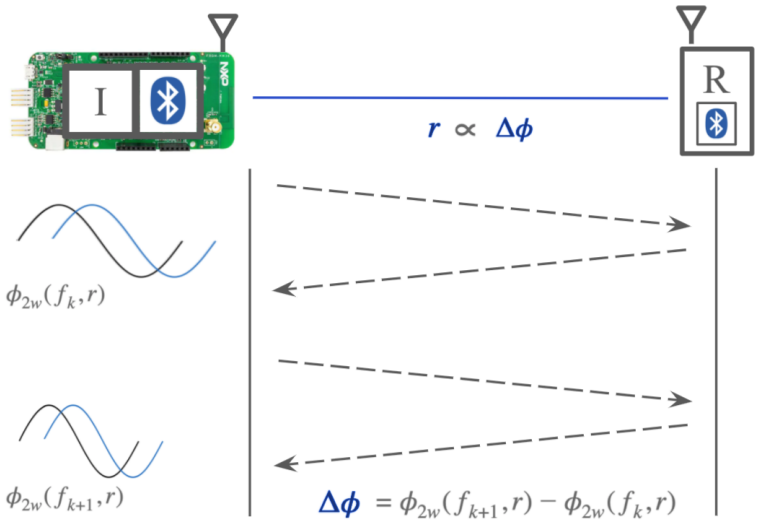



Figure 4: Two tone exchanges between Initiator (I) and Reflector (R).

From fig. 4 it can be shown that, by subtracting $\phi_{2w}(f_{k+1}, r)$ and $\phi_{2w}(f_k, r)$ an expression to find $r$ can be found. That is:

$$\Delta\phi = \phi_{2w}(f_{k+1}, r) - \phi_{2w}(f_k, r) = \frac{4\pi\Delta f r}{c} \tag{9}$$

Where $\Delta f = f_{k+1} - f_k$. Now, solving for $r$ yields the following expression:

$$r = \frac{c}{4\pi}\frac{\Delta\phi}{\Delta f}, \quad \text{mod}(2\pi) \tag{10}$$

Similarly, as in the case for one tone exchange and provided $\Delta\phi_{max} = 2\pi$, a new expression for $r_{max}$ can be found:

$$r_{max} = \frac{c}{2\Delta f} \tag{11}$$

According to the Bluetooth Core Specifications, the hop between two adjacent channels is $\Delta f = 2$MHz [11]. This is a crucial parameter since now, the unambiguous range is defined by the frequency difference between two adjacent channels and is always fixed.

It follows from eq. 11, that the maximum range which can be estimated without any range ambiguity is $r_{max} = 75$m. This is an unquestionable improvement to the case of one tone exchange. However, while the range can be estimated from eq. 10, it has been shown in [14] that it is prone to errors in the presence of noise. As a way to mitigate the influence of noise, an extension of the basic method has been proposed [15]. This is described in detail in the following subsection.

### 3.2.1 Slope Method

Here a continuation of how to improve the calculations of range in the presence of influencing factors such as noise is presented. Recall from last section, when using two tones, the distance of a node in a radius of 75m can be calculated. This is depicted in the figure below:

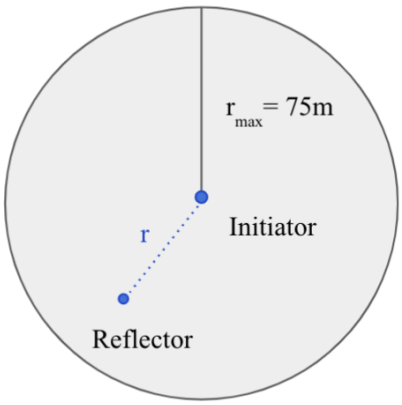



Figure 5: Maximum range when using two tones

Similarly, it was found that in order to calculate the distance between initiator and reflector eq. 10 can be used:

$$r = \frac{c}{4\pi}\frac{\phi_{2w}(f_{k+1},r)-\phi_{2w}(f_k,r)}{f_{k+1}-f_k}, \quad \text{mod}(2\pi) \tag{12}$$

From eq. 12, two conclusions can be drawn:

1. An increase in $f_k$ will result in an increase on $\phi_{2w}(f_k,r)$. This follows directly from eq. 6 where a direct proportionality between phase measurements and frequency can be seen.
2. The term $\frac{\phi_{2w}(f_{k+1},r)-\phi_{2w}(f_k,r)}{f_{k+1}-f_k}$ represents the slope of a line.

That is, if more points are to describe the slope of this line, i.e. sending 37 tones, then when non-ideal factors are to affect phase measurements, a curve fitting algorithm could be used to compensate for inaccurate results.

To make this possible, the features of BLE v5.1 come in handy again. In order to send 37 tones, periodic advertisement should be enabled. By doing that, the secondary channels of BLE, 0-36th, can now be used to send tones and thus obtain 37 calculations of the distance. The procedure of sending more than two tones is called Multi Carrier Phase Difference (MCPD) and the curve fitting procedure, the Slope Method [6]. Following is an example of the Slope Method.

Consider two nodes separated from each other by 40 meters. When using MCPD, a graph of the tone $f_k$ versus $\phi_{2w}(f_k,r)$ phase measurements can be found. Additionally, to simulate inaccurate values in the presence of noise, random noise is added to the phase measurements. The following graph is obtained using eq. 6 and $f_k$ for the complete bandwidth of BLE:

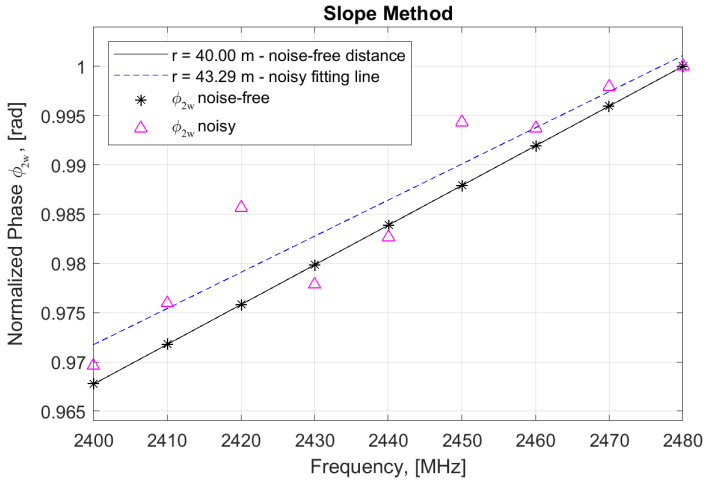



Figure 6: Slope method using MCPD algorithm

In fig. 6, two distinguishable lines can be seen. The black line represents the ideal case when frequency $f_k$ against phase $\phi_{2w}(f_k,r)$ is plotted. The black asterisks denote the frequencies that were used to calculate the slope and therefore the distance. Thus, the black line shows a distance $r = 40m$ as expected. Now, analysing the non-ideal case, the magenta triangles represent the inaccurate phase measurements in the presence of noise. These values are used to create an estimate for the slope which is drawn in a dashed blue line. This turns out to yield a distance $r = 43m$.

Naturally, the tones sent by each device at the end of a radio transmission, undergo a number of effects that affect the accuracy of the distance estimation. These effects are described, simulated and analysed in the following chapter.

# 4 Simulations & Results

In this chapter the MCPD algorithm is simulated and tested. Special attention is given to its performance. Desirably, we would like to know how the algorithm performs close to the maximum range limit. This is mainly because we would like to see whether a solution like the one investigated in this report could be realized as a part of the software solutions that BouWatch would like to implement.

Initially, the test is conducted under a noise-free channel followed by the inclusion of parameters that may lead to inaccurate values. For the simulation set up, a similar case like the one described in fig. 4 is used. The distance that separates these two is varied and for reliability of results 1000 simulations are run for each value.

## 4.1 Multi-tone Exchange

In this section, the MCPD is tested without interfering factors under a noise-free channel. For that, two scenarios are considered. The first one is the case where the initiator sends two tones only. The remaining, where 37 tones are used.

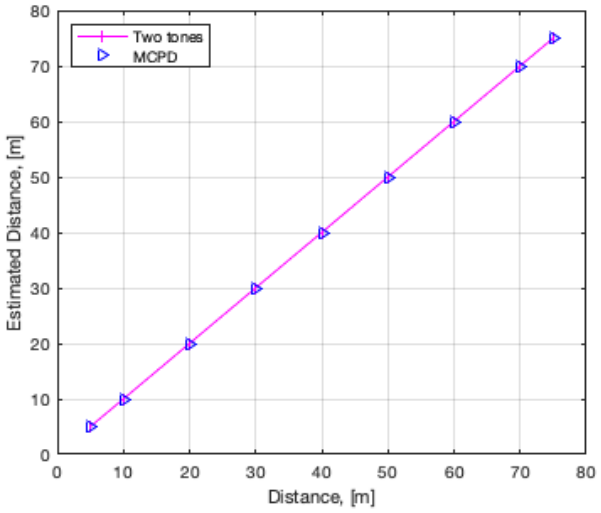



Figure 7: Distance calculation for Two tones and Multi-tones exchange

Fig. 7 shows the calculated distance against the true value for two and 37 tones exchange. Both methods yield the same results, the distance calculated and the true value are exactly the same. This is not surprising as without perturbations the algorithm will perform at its best.
Let's now consider a more realistic scenario.

## 4.2 Noise & Non-idealities

In this section the inclusion of a White Gaussian Noise Channel (AWGN) is studied. Additionally, the effects of inaccuracies of crystal oscillators is studied.

### 4.2.1 AWGN Channel

Initially, when calculating the distance between two devices a noise-free channel was considered. Here, a more realistic scenario is presented. At both ends of the transmission a AWGN channel is added. This is shown in the next figure:

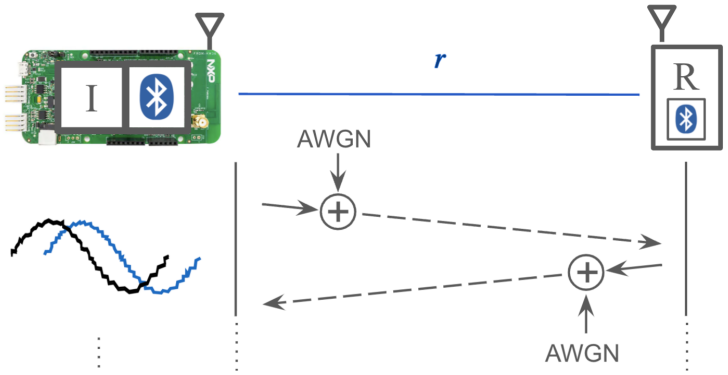



Figure 8: Inclusion of AWGN channel

To describe the influence of the noisy channel, the signal to noise ratio (SNR) of a tone in the presence of AWGN is used. When consulting the Bluetooth Core Specifications for a Gaussian Frequency Shift demodulation, it is found that the minimum SNR ratio allowed in a channel is 21dB [16]. This value comes from the fact that for a reliable connection, a Bit Error Rate (BER) of less than 0.1% is recommended. BER is the percentage of bit errors to the total number of bits received. In other words if the signal strength at the reflector is less than 21dB then errors start to occur. This is better described in the following figure:

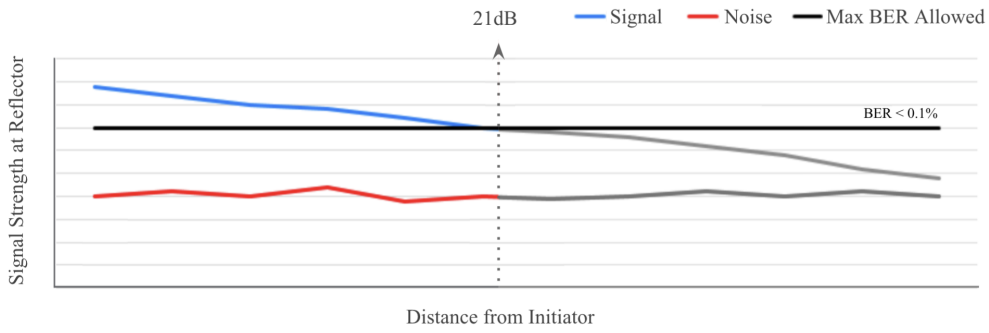



Figure 9: Min. SNR value for a BER $< 0.1\%$ [17]

Fig, 9 shows the distance from the initiator versus the signal strength at the reflector. There, three lines are shown. The blue one is the tone that is sent by an initiator which contains range information. It can be seen that the larger the distance from the initiator, the lower the signal strength is at the reflector. This is because the intensity of electromagnetic waves decays with distance [18]. The red line is the AWGN channel and the black line a threshold on the maximum BER percentage allowed before bit errors in the encoders of each device starts to yield inaccurate values.

Intuitively, in the absence of noise or a very large SNR, the MCPD and the two tone exchange will result in a graph similar to the one shown in fig. 7. The question now is: How well will the MCPD algorithm perform against two tone exchange in the presence of noise? To answer this question, a simulation set up like the one described in fig. 8 is used and a new graph is obtained:

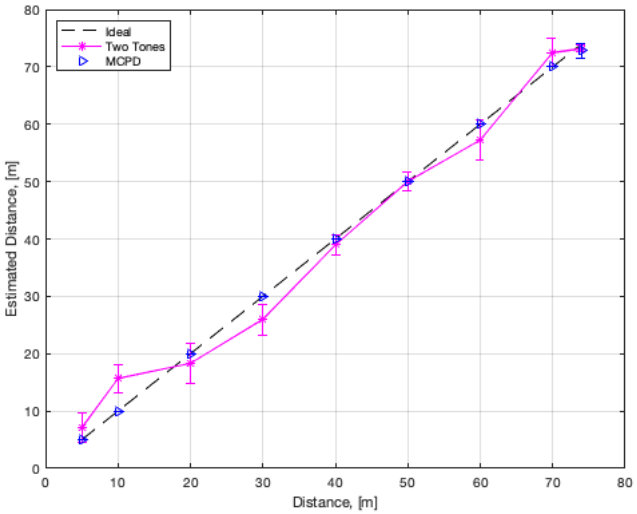



Figure 10: Distance calculation for Two tones and MCPD algorithm
+ AWGN Channel with SNR: 16dB

Fig. 10 shows the calculated distance against the true value when two and 37 tone exchange is simulated. There, three lines are shown. The dash line represents the ideal case when calculated and the true distance yield the same result. The magenta line simulates the sending of two tones and the blue marker the MCPD algorithm. Both lines are plotted with their respective error bars. The error bars represent the uncertainty of range estimation when using low SNR value. For this plot an SNR of 16dB was simulated. Looking at the graph, it can be seen that by sending more than two tones, a better estimation for the range is obtained. This is seen on the deviation of the magenta line from the ideal model. Furthermore, it can be seen that the error bars of the two tones sending is significantly bigger than the MCPD

algorithm. This indicates that by sending more than two tones, a better estimation for the range can be accomplished.

Now, the performance of the algorithm when close to the maximum range limit is studied. In order to evaluate this, the Root Mean Square Error (RMSE) is used. RMSE determines how far the calculated and the true distance are from each other [19]. In other words, it determines the precision of the algorithm. For that, a plot of RMSE versus SNR is plotted for distances close to the maximum measurable range.

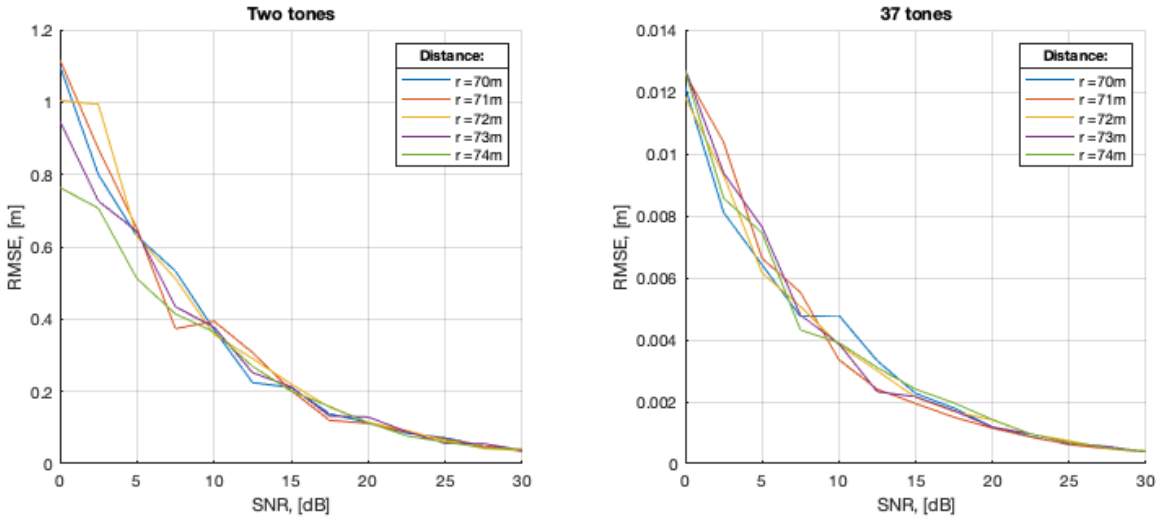



Figure 11: SNR vs RMSE for two and 37 tones exchange

From fig. 11 the accuracy of the MPCD algorithm against two tone sending is compared. On both plots, a similar trend can be observed. At high SNR values, a better range estimation is obtained. The difference between the two is in the order of error that they can provide. At the right hand side, it can be seen that at values of SNR close to the recommended value for a BER <0.1%, the algorithm performs better when sending two tones only. Similarly, an improvement in range estimation even at low SNR values is obtained.

In the next section, the effects of inaccuracies in the frequency carrier due to crystal oscillators are addressed.

### 4.2.2 Crystal offsets

Until now, the frequency carrier, $f_k$, from both sides of the transmission was modeled assuming the absence of frequency offset. In reality, depending on the specifications of each device, the crystal oscillators that are used to generate these tones are not ideal.

For instance, when considering the imperfections of a crystal oscillator the output frequency at the initiator and reflector can be expressed as follows:

$$f_k^I = (1+n_I)f_k \quad (13)$$
$$f_k^R = (1+n_R)f_k \quad (14)$$

Here, $n_I$ and $n_R$ are the crystal offsets at the initiator and reflector, respectively. These values are typically expressed in part-per-million (ppm), or $10^{-6}$, and represent the variation of the output frequency around a nominal value [20]. For instance, if the crystal offset at the initiator is measured to be $n_I = 5$ ppm and the nominal frequency is $f_k = 1$KHz, then $f_k^I$ will be in the range of 5 ppm around 1KHz.

If the same crystal oscillator is used for clock-generation then, the measurement-timing can be defined as follows:

$$T_k^R = (1+n_R)(t_k+T_w) \quad (15)$$
$$T_k^I = (1+n_I)(t_k) \quad (16)$$

Where $T_w$ is the time that the reflector needs to wait before phase measurements are performed.
It can be shown from eq. 1, and 3 that:

$$\phi_R(f_k,r) = 2\pi f_k^R(\frac{r}{c}+T_k^R)+\varphi_I-\varphi_R \quad (17)$$
$$\phi_I(f_k,r) = 2\pi f_k^I(\frac{r}{c}-T_k^I)+\varphi_R-\varphi_I \quad (18)$$

And consequently from eq. 6 that:

$$\phi_{2w}(f_k,r) = 2\pi(f_k^R+f_k^I)\frac{r}{c}+2\pi(f_k^R-f_k^I)(T_k^R-T_k^I) \quad (19)$$
$$\phi_{2w}(f_k,r) = 2\pi[(1+n_R)f_k+(1+n_I)f_k]\frac{r}{c} + 2\pi[(1+n_R)f_k-(1+n_I)f_k][(1+n_R)(t_k+T_w)-(1+n_I)t_k] \quad (20)$$

Using eq. 9 and considering phase measurements are independent on the amount of time a

new channel is selected [21]. Namely, $t_{k+1} - t_k$, one can derive:

$$\Delta\phi = \frac{2\pi\Delta f r}{c}(n_R + n_I + 2) + 2\pi\Delta f(1+n_R)(n_R - n_I)T_w \tag{21}$$

From eq. 21 the following conclusions are drawn:

1. If the inaccuracies due to the crystal oscillator become zero then eq. 9 is obtained, which is the same as in the case of having a zero frequency offset.

2. If the time, $T_w$, becomes zero, then the first term of eq. 21 is still influenced by the inaccuracies of the crystal oscillator.

Because of these findings, when solving for $r$ as in eq. 10, the effects of $n_R$ and $n_I$ will become apparent.
Define:

$$\begin{aligned} \beta &= (n_R + n_I + 2) && (22)\\ &\approx 2 \\ \alpha &= 2\pi\Delta f(1+n_R)(n_R - n_I)T_w && (23)\\ &\approx 2\pi\Delta f(n_R - n_I)T_w && (24) \end{aligned}$$

That is, a new expression to calculate $r$ is found:

$$\begin{aligned} r &= \frac{1}{\beta}\frac{c}{2\pi}\frac{\Delta\phi}{\Delta f} - \frac{c}{2\pi}\frac{\alpha}{\beta} \\ &= \frac{c}{4\pi}\frac{\Delta\phi}{\Delta f} - \frac{c}{2}(n_R - n_I)T_w, \quad \mathrm{mod}(2\pi) && (25) \end{aligned}$$

Comparing eq. 10 with eq. 25, it can be seen that the estimation of the range is now dependent on hardware inaccuracies and the processing time that it takes to perform phase measurements.

$T_w$ can be defined more precisely as follows:

$$T_w = T_{IFS} + T_{pkt} + T_{CTE} \tag{26}$$

Here, $T_{pkt}$ is the amount of time for a packet to be processed, $T_{IFS}$ the time interval between two consecutive packets on the same channel and $T_{CTE}$ the duration of a constant tone which can range from 16 $\mu s$ to 160$\mu s$ . According to the Core Specification for Bluetooth, $T_{IFS}$ has a fixed value of 150$\mu s$ [11]. When using the standard bit rate in BLE, 1MB/s, the packet length $T_{pkt}$ can take the following values:

Table 2: Times for $T_{pkt}$, 18.

| Periodic Adv. | Min. Time | Max. Time |
|---|---|---|
| Disabled | $44\mu$s | $2120\mu$s |
| Enabled | $61\mu$s | $206\mu$s |

Table 2, shows the minimum and maximum values for $T_{pkt}$ when the feature of BLE, periodic advertisement is enabled or disabled. Recall from the second chapter, periodic advertisement allows the sending of multi-tones which in turns is used in the MCPD algorithm. Therefore when considering which values to simulate for $T_{pkt}$, $61\mu s$ and $206\mu s$ are used.

It follows from eq. 26 and using $T_{CTE} = 160\mu s$, to simulate the effect of a varying $T_w$, the range between $371\mu s$ to $516\mu s$ can be used. Additionally, to study what is the effect out of this boundary, the maximum packet length when periodic advertisement is not enable is simulated. Below an analysis on the effect for varying $T_w$ on the deviation error for range calculations :

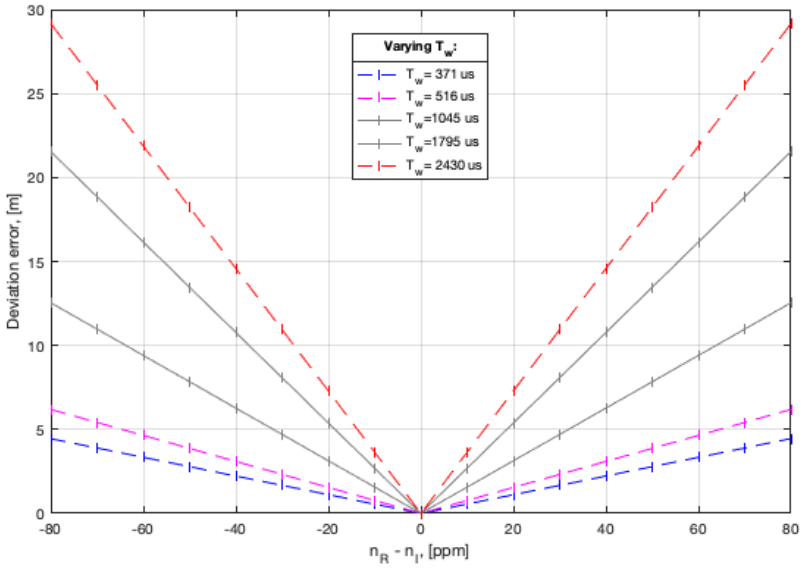



Figure 12: Additional range estimation error due to crystal instability with varying $T_w$ and without AWGN channel.

Fig. 12, shows the the deviation error found in the second term of eq. 25 versus the difference between crystal oscillator offsets, $n_R - n_I$. There, different values of $T_w$ are plotted from which three lines stand out. In the x axis, values range from -80 to 80 ppm. These are the maximum allowed frequency deviations conforming to the Bluetooth Core Specifications when using GFSK modulation [11], [22]. To describe this plot better, the following

conclusions are made:

1. Looking at the blue dashed line. When fixing $T_w$ to the minimum time between a packet is transmitted and phase measurements are performed, a maximum deviation error of around 5m is obtained.

2. Looking at the magenta dashed line. When fixing $T_w$ to the maximum time between a packet is transmitted and phase measurements are performed, a maximum deviation error of around 7m is calculated.

   For completeness, three more different values of $T_w$ have been plotted. These are in the case when periodic advertisement is not used.

3. Looking at the gray lines, it can be observed that the higher $T_w$ becomes, the higher the deviation error results.

4. Looking at the dashed red line, when sending a tone without the help of secondary channels, a deviation error of around 28m is calculated. This is the maximum package length as described in table 2.

From this analysis, it is clear that the larger the value for $T_w$ becomes, the larger the deviation error is. Consequently, in order to decrease the effect of $T_w$, periodic advertisement should be enabled. Following the algorithm is tested in the presence of noise with $T_w = 516\mu s$ and $371\mu s$:

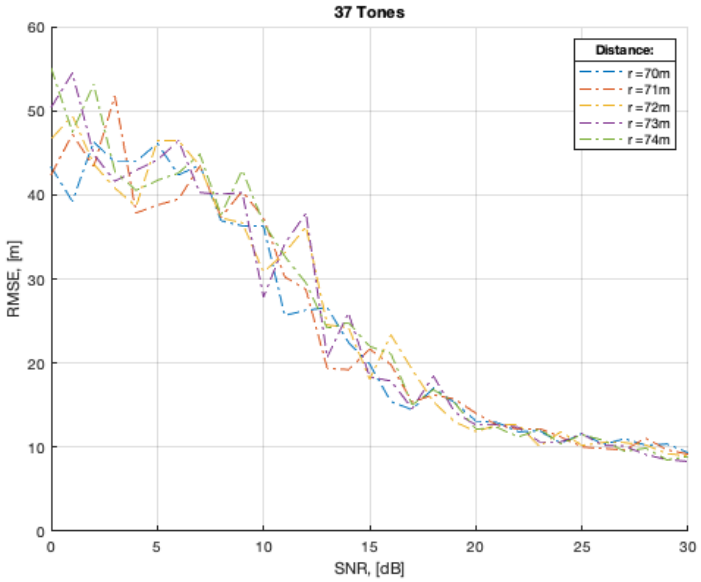



Figure 13: SNR vs RMSE for $T_w = 516\mu s$

Fig. 13, shows the accuracy of the MPCD algorithm in a plot of RMSE versus SNR. This is simulated for different distances close to the maximum limit range. The test was performed using random frequency offsets. In this plot this turns out to be: $n_R = 12$ppm and $n_I = 33$ppm. The following conclusion can be made:

1. For low values of SNR the accuracy of the algorithm decreases. This make calculation of the range unpredictable.

2. At values higher than 15dB, the deviation can be estimated. For at 30dB a deviation of around 10m is estimated.

When plotting a similar graph but this time using $T_w = 371\mu s$ the following graph is found:

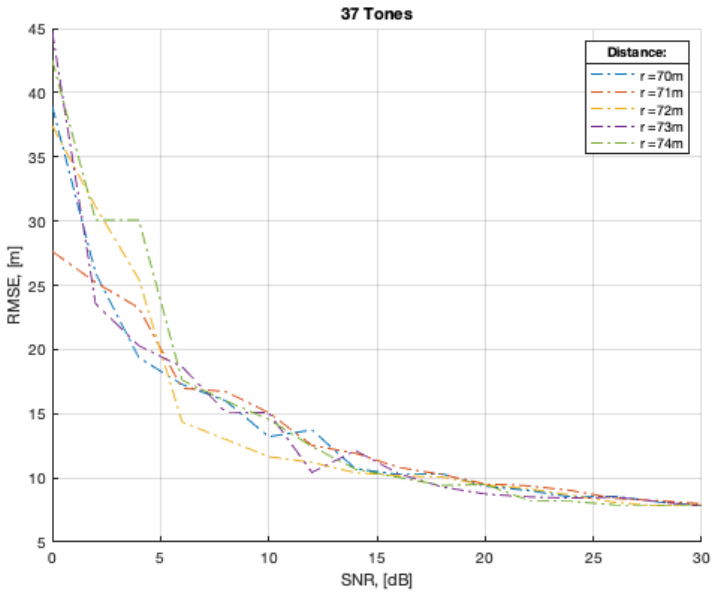



Figure 14: SNR vs RMSE for $T_w = 371\mu s$

Fig. 14 shows an small improvement from the graph presented above which indicates the proportionality as stated in eq. 26. This is noticeable at a SNR = 30dB where a deviation of around 7m is estimated.

To conclude this chapter, a figure of the deviation error when using SNR = 21 dB, $n_R =$ 12ppm, $n_I = 33$ppm, $T_w = 516\mu s$ and $r$=70m is shown below:

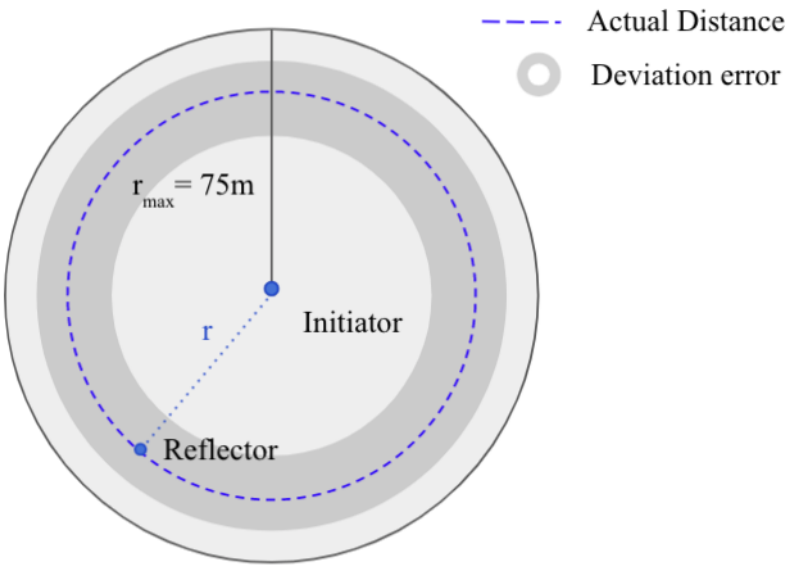



Figure 15: Ranging Estimation

Fig. 15, shows an hypothetical case where the distance between a reflector and an initiator needs to be calculated. The blue dotted line shows the actual distance from I. The grey circle surrounded this line is the deviation error measured after the sending of 37 tones. The dimensions of this grey circle does not correspond with the actual value but is only an indication to illustrate this example. After simulating this scenario, the reflector was found at $r = 67 \pm 11$m from the initiator.

# 5 Conclusions & Future Work

Through the presented exploratory study, the ranging capabilities using Bluetooth Low Energy were investigated. Here is a summary of the main conclusions:

- When calculating range in a two way communication system, the maximum distance that can be calculated without ambiguity depends on the frequency hop of the wireless technology used. In the case of BLE this was found to be 75m. Other wireless technologies with a smaller frequency hop, $\Delta f$, may yield higher values. Nonetheless, if power consumption is a constrain, BLE should be considered.
- To calculate range and compensate for the noise present in an AWGN channel in a 75m radius , secondary channels of BLE can be utilized to obtain better results than using only advertisement channels. This was found to be the best alternative in the presence of a noisy environment when using the so called slope method.
- To relate how well this method performs, several simulations were carried out. In the presence of hardware inaccuracies, it was found that the MCPD algorithm performs better than sending two tones yet not accurate enough as to provide reliable results for low values of SNR. At the recommended SNR, it is found that there is a constant deviation error when calculating range.

Answering the research question, how can we effectively estimate the range between a BLE beacon and a BLE receiver? The answer to that is range can be estimated. However, in order to yield accurate results some pre-parameter corrections must be made. One of them being the frequency carrier offsets. It was seen that crystal oscillator inaccuracies induce an offset in range calculations. Fortunately, using the deviation error found in the second term of eq. 25 the difference, $n_I - n_R$, can be compensated as suggested in [6].

Another way to estimate an better range would be the agreement between initiator and reflector to utilize a minimum CTE. As analysed, the increment of the waiting time is proportional to the error deviation. Using the minimum packet length would then yield better results. Additionally, to increase the performance of the MCPD algorithm an improved curve fitting algorithm could be used. For instance, disregarding outlier values which may affect the slope method.

Lastly, a mesh of antennas proposed in [14] can lead to improvements on range calculations. This may be desired, if for instance, a radius more than the maximum limit discovered is to be protected. Relating to BouWatch, this could be the case if more than one 360°camera is implemented which in most of the cases would be necessary to secure large areas of terrain.

# Bibliography

[1] H. Du, C. Zhang, Q. Ye, W. Xu, P. L. Kibenge, and K. Yao, "A hybrid outdoor localization scheme with high-position accuracy and low-power consumption," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 1–13, 2018.

[2] M. Afaneh, " New Features in Bluetooth Core Specification v5.1." Bluetooth Special Interest Group (ISG). 2019, Apr 16.

[3] BuoWatch, "Temporary security of construction sites." Available at: https://www.bouwatch.nl/oplossingen/tijdelijke-beveiliging/, 2020.

[4] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, "Performance evaluation of bluetooth low energy: A systematic review," *Sensors*, vol. 17, no. 12, p. 2898, 2017.

[5] 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, 2007.

[6] P. Zand, J. Romme, J. Govers, F. Pasveer, and G. Dolmans, "A high-accuracy phase-based ranging solution with bluetooth low energy (ble)," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–8, IEEE, 2019.

[7] M. Pelka, C. Bollmeyer, and H. Hellbrück, "Accurate radio distance estimation by phase measurements with multiple frequencies," in *2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 142–151, IEEE, 2014.

[8] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[9] SIG, "Bluetooth sig extends bluetooth brand, introduces bluetooth smart marks." Available at: http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=138, 2016.

[10] D. Čabarkapa, I. Grujić, and P. Pavlović, "Comparative analysis of the bluetooth low-energy indoor positioning systems," in *2015 12th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*, pp. 76–79, IEEE, 2015.

[11] S. Bluetooth core specification 5.1, Bluetooth Special Interest Group *Jan.*, 2019.

[12] Microchip, Dev., "Bluetooth® Low Energy Connection Process - Connection Events." Available at: https://microchipdeveloper.com/wireless:ble-link-layer-connections, 2018.

[13] R. Kai, "Periodic Advertising Sync Transfer." Available at: https://www.bluetooth.com/blog/periodic-advertising-sync-transfer/, 2019.

[14] P. Boer, J. Romme, J. Govers, and G. Dolmans, "Performance of high-accuracy phase-based ranging in multipath environments," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5, IEEE, 2020.

[15] H. Ólafsdóttir, A. Ranganathan, and S. Capkun, "On the security of carrier phase-based ranging," in *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 490–509, Springer, 2017.

[16] R. Schiphorst, F. Hoeksema, and C. H. Slump, "Channel selection requirements for bluetooth receivers using a simple demodulation algorithm," in *12nd proRISC workshop on Circuits, Systems and Signal Processing*, 2001.

[17] M. Woolley, "Understanding reliability in bluetooth® technology," Bluetooth Special Interest Group (ISG), 2020.

[18] D. J. Griffiths, *Introduction to electrodynamics; 4th ed.* Boston, MA: Pearson, 2013. Re-published by Cambridge University Press in 2017.

[19] S. P. Neill and M. R. Hashemi, "Chapter 8 - ocean modelling for resource characterization," in *Fundamentals of Ocean Renewable Energy* (S. P. Neill and M. R. Hashemi, eds.), E-Business Solutions, pp. 193–235, Academic Press, 2018.

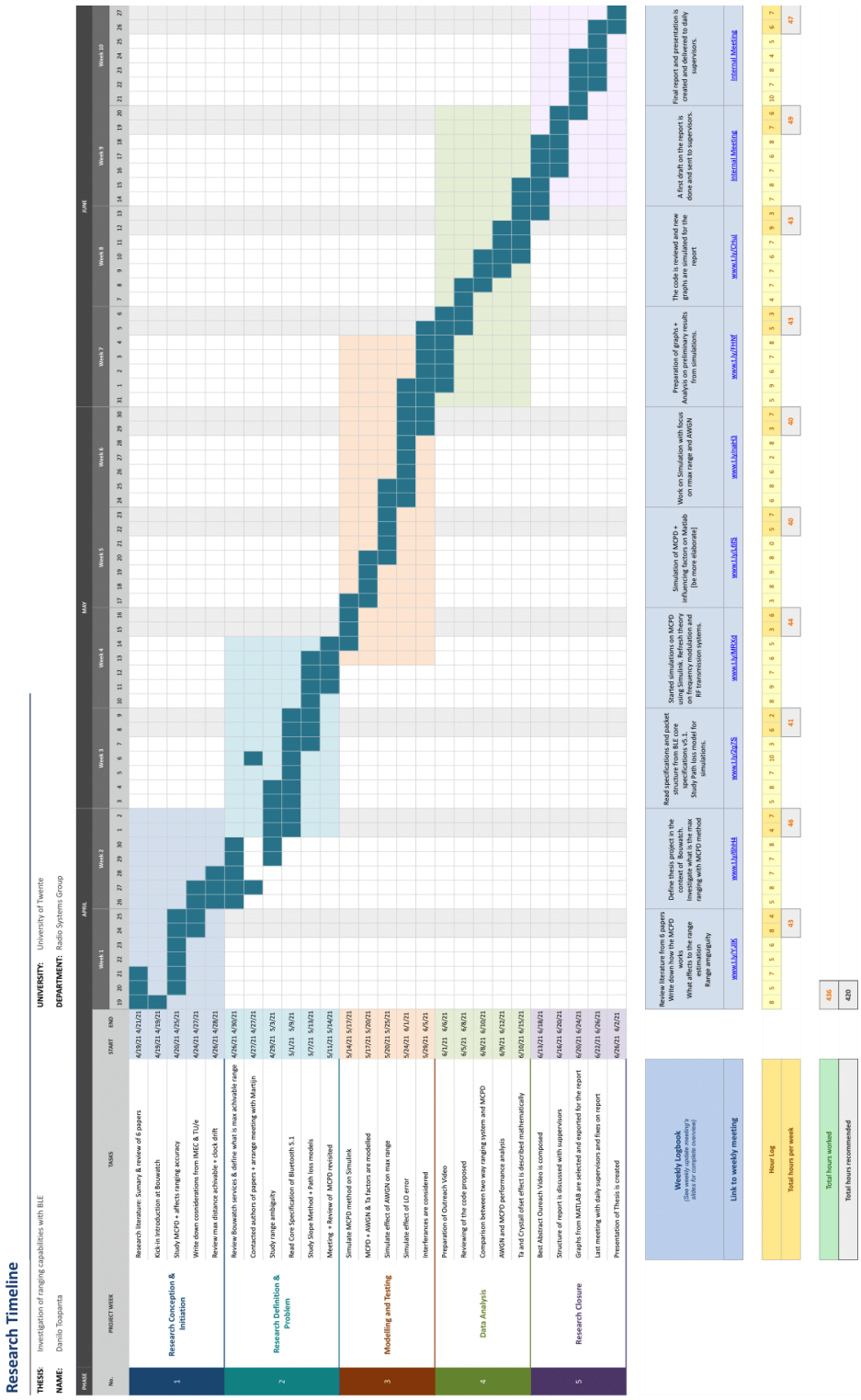
[20] P. Zand, A. Duzen, J. Romme, J. Govers, C. Bachmann, and K. Philips, "A high-accuracy concurrent phase-based ranging for large-scale dense ble network," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–7, IEEE, 2019.

[21] W. Kluge and S. Eric, "Distance measurement between two nodes of a radio network," *uS Patent 9.274,218B2*, vol. 15, Mar. 2016.

[22] Y. Lichen, "Bluetooth Direction Finding," Delft University of Technology, 2018.

# Appendices

## A Gantt Chart



# B BLE v5.1 Features

## Expansion of PDU header

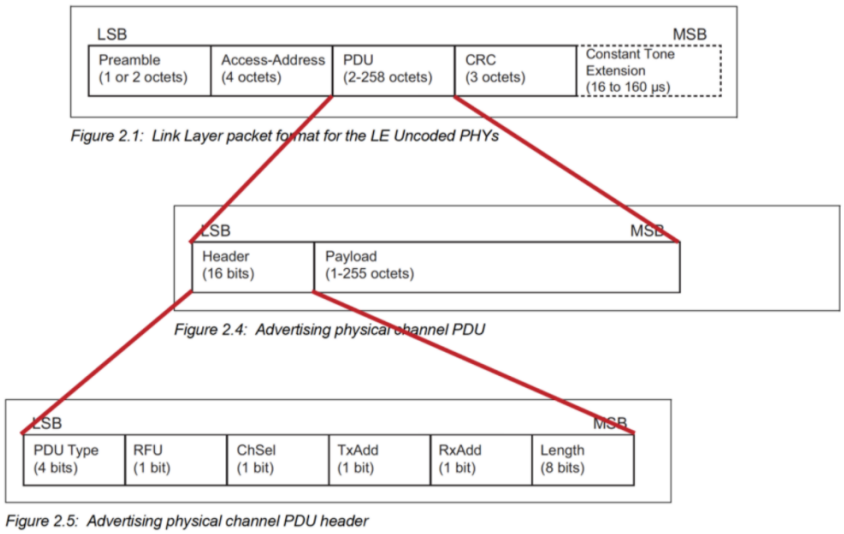



Figure 17: Advertisement Packet Structure Extended

## Calculation of time for different packets size

The length of empty PDU is 10 octets:

| Preamble | Access Address | Header | CRC |
|---|---|---|---|
| 1 | 4 | 2 | 3 |

The length of empty PDU = 1 + 4 + 2 + 3 = 10 octets.

It will consume 40 µs by 2Mb/s because:

$$\frac{10\ octets * 8\ bit}{2Mb/s} = 40\ \mu s$$

Figure 18: $T_{pkt} = 40\ \mu$ s

The maximum data packet length is:

| Preamble | Access Address | Header | Payload | MIC | CRC |
|---|---|---|---|---|---|
| 1 | 4 | 2 | 251 | 4 | 3 |

1 + 4 + 2 + 251 + 4 + 3 = 265 octets

It will consume 2120 µs because:

$$\frac{265\ octets * 8\ bits}{1Mb/s} = 2120\ \mu s$$

Figure 19: $T_{pkt} = 2120\ \mu$ s

## C Matlab Code

```
clc; clear all;

%% Global Parameters
Nsim = 1000;                        % number of simulations
ch = 2;                             % number of channels
delta_f = 1.99*10^6;                % for 02 tones exchange
c = 3*10^8;                         % speed of light
phi0_Tx = pi-2*pi*rand(1,1);        % Unknown phase offset Tx
phi0_Rx = pi-2*pi*rand(1,1);        % Unknown phase offset Rx

% Variables (1st value of each array is not used)
snr = [0, -20:1:20];                        % holds array of SNR values
r = [0, 20, 45]';%(0:10:75)';                   % distances: 75 is MAX
r_max = 75;

%% Run N simulations
deviation_Cur = zeros(Nsim,1);              %saves absolute value
deviation_Cur_rel = zeros(Nsim,1);          %saves relative error

C = zeros(numel(r)-1, numel(snr)-1);        % saves all deviation results
f = zeros(ch,1);                            % holds freq axis

% For debugging
save_distance = zeros(numel(r)-1, numel(snr)-1);
measured_distance = zeros(Nsim,1);
save_phi_d_at_Tx = zeros(ch,numel(snr)-1);
save_phi_d = zeros(ch,numel(snr)-1);
d = zeros(Nsim,1);

for i_r = 2: numel(r)
    temp_r = r(i_r);

    for i_snr = 2: numel(snr)
        temp_snr = snr(i_snr);

        for j = 1:Nsim
            %% Set-up simulation parameters
            fc = 1*10^3;                    % central frequency, ch = 2402
            fs = 1000;                       %10*fc;                        %
                sampling frequenc

            % Calculation of delay due to distance
            tau = temp_r/c;                 % from distance to time delay
            phi_d = 2*pi*fc*tau;            % initial phase delay

            % Transmittion of tonese
            delta_omg = zeros(ch+1,1);      % holds phase diff. for fi

            for i = 1:ch
                t = linspace(0, 1/fc, fs);      % sampling time
                phi_d = 2*pi*fc*tau;            % initial phase delay

                %% Transmitting tone
                % 1. Tone transmitted from Tx
                s = exp(1i*(2*pi*fc*t+phi0_Tx));                % t +
```

```
                phi0_Tx
55              s = awgn(s,temp_snr, 'measured'); %awgn(s,
                    temp_snr);
56
57              % 2. Tone recieved at Rx
58              s_atRx = s.*exp(1i*phi_d).*exp(-1i*phi0_Rx); % t +
                    phi0_Tx + phi_d - phi0_Rx
59
60              % Calculate phase at Rx
61              Rx_sends = s_atRx.*conj(exp(1i*(2*pi*fc*t))); %%%%
                    phi0_Tx + phi_d - phi0_Rx
62              Rx_sends = mean(Rx_sends);
63
64              % 3. Tone transmitted from Rx
65              z = exp(1i*(2*pi*fc*t+phi0_Rx)); % t +
                    phi0_Rx
66              z = awgn(z,temp_snr, 'measured'); %awgn(z,
                    temp_snr);
67
68              % 4. Tone recieved at Tx
69              z_atTx = z.*exp(1i*phi_d).*exp(-1i*phi0_Tx); % t +
                    phi0_Rx + phi_d - phi0_Tx
70
71              % Calculate phase at Tx
72              Tx_measures = z_atTx.*conj(exp(1i*(2*pi*fc*t))); %%%%
                    phi0_Rx + phi_d - phi0_Tx
73              Tx_measures = mean(Tx_measures);
74
75              % Calculate phi_d at Tx
76              Tx_adds = Rx_sends.*Tx_measures; % 2*phi_d
77
78              if Tx_adds < - pi
79                  Tx_adds = Tx_adds+2*pi;
80              end
81
82              save_phi_d(i,i_snr-1) = phi_d;
83              phi_d_at_Tx =  angle(Tx_adds);    %mean((angle(Tx_adds)));
84              save_phi_d_at_Tx(i,i_snr-1) = (phi_d_at_Tx/2);
85
86              delta_omg(i+1) = angle(Tx_adds); %(mean((angle(Tx_adds))));
87
88              f(i) = fc;
89
90              %% Hop to a new tone
91              fc = fc + delta_f;              % new tone central frequency
92              phi_d = 2*pi*fc*tau;            % new phase delay
93
94          end % finish exchange of tones ch [2, 37]
95
96          %% Calculating measured distance 'd'
97          %Slope method
98          delta_omg = delta_omg(2:end);
99          slope = polyfit(f,delta_omg,1);
100
101         d(j)= (c/(4*pi)) * abs(slope(1));       %slope(1);
102
103         if d(j) > r_max
```

```
104                 d(j) = r_max*2-d(j);
105             end
106
107             deviation_Cur(j) = abs(temp_r - d(j));
108             measured_distance(j) = d(j);
109             deviation_Cur_rel(j) = abs(temp_r - d(j))/temp_r;
110
111         end % j = Nsim
112
113         % After Nsim save mean values
114         C(i_r -1, i_snr -1)= mean(deviation_Cur);
115         save_distance(i_r -1, i_snr -1)= mean(measured_distance);
116         RMSE(i_r -1, i_snr -1)= sqrt(mean(deviation_Cur.^2));
117
118     end % change snr
119
120 end % change r
121
122 % Order results
123 C = padarray(C,[1 1],0,'pre'); C(:,1)=[]; C =[r C]; C(1,:)=[];
124 results_C =[snr; C];
125
126 %% Plots
127
128 % SNR vs error
129 figure; tiledlayout(1,2); nexttile
130 for i = 2 : numel(r)
131     hold on; plot(snr(2:end),results_C(i,2:end),'-o','DisplayName', strcat('r
        =',num2str(r(i)),'m'))
132 end
133 legend ('location','northeast')
134 xlabel('SNR, [dB]')
135 ylabel('Deviation error, [m]')
136
137 % Distance vs error
138 nexttile
139 for i = 2 : numel(snr)
140     hold on; plot(r(2:end),results_C(2:end,i),'-o','DisplayName', strcat('SNR
        =', num2str(snr(i)),'dB'))
141 end
142 legend ('location','northeast')
143 xlabel('Distance, [m]')
144 ylabel('Deviation error, [m]')
145
146 % Histogram
147 figure;
148 snr_75 = results_C(2,2:end);
149 histogram(snr_75)
150 xlabel('Absolute error, [m]')
151 ylabel('Frequency')
```