DEGREE PROJECT

Evaluation of Secure Long Distance Communication in Non-Urban Environments

Daniel Nilsson

Space Engineering, master's level
2018

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY

Abstract

The need for wireless communication is present in a range of industries. However, for the industries operating in non-urban environments outside the cellular network this can be problematic. This problem was especially pronounced by the Fire and Rescue Service and their need was what inspired the focus of this work.

This thesis work evaluates different spread spectrum techniques for secure and robust long distance communication in non-urban environments. Two approaches to the spread spectrum technique, the Chirp Spread Spectrum (CSS) and Frequency-Hopping Spread Spectrum (FHSS) is examined in the work, using two different commercially available communication chips. Their suitability is examined from the point of view of a real-time positioning system that could be used by the Fire and Rescue Service.

One of the examined chips is the LoRa SX1279 chip implementing LoRa's approach to CSS modulation. As part of the spread spectrum approach, the SX1279 spreads the signal over a larger bandwidth. As part of the CSS approach the signal is then transmitted as chirps with a linearly changing frequency withing this bandwidth.

Further, the SX Module is also examined as an implementation of the FHSS modulation. In comparison to the linear changing chirps of the CSS modulation, with FHSS the frequency is changing in a non-linear fashion in a predetermined sequence. The technologies are then evaluated from the point of view of applicability in a real-time positioning system. It was shown that both chips are suitable solutions for a real-time positioning system.

However, with the LoRa approach to CSS modulation the data throughput of the system is severely limited. During the testing, a 15 byte transmission took 1.286 seconds to complete using settings optimized for long range transmissions. In comparison, the SX Module would have data throughput of approximately 34-35 kb/s. The long transmission time for the SX1279 also resulted in a decrease in the life time for a battery powered system. Although, the SX Module was not able to transmit as far as the SX1279. Hence, it was concluded that the SX Module is more suited for a system that requires frequent updates for a multitude of users as the channel dwell time is much lower and the battery consumption more limited. The SX1279 could be the technology of choice however for a system that needs to transmit far distances or seldom enough to not clog the network.

Contents

List of Figures

List of Tables

Abbreviations

LPWAN	Low Power Wide-Area Network
SS	Spread Spectrum
CSS	Chirp Spread Spectrum
FHSS	Frequency-Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
SNR	Signal-to-Noise Ratio
FSPL	Free-Space Path Loss
LOS	Line Of Sight
RF	Radio Frequency
VCO	Voltage-Controlled Oscillator
SF	Spreading Factor
LNA	Low Noise Amplifier
EIRP	Effective Isotropically Radiated Power
AES	Advanced Encryption Standard
TDMA	Time Division Multiple Access
CDMA	Code Division Multiple Access
LNA	Low Noise Amplifier

Disclaimer

In this public version, commercially sensitive information has been excluded.
Contact the author for more information.

1 Introduction

Communication is a key aspect in many situations and the development of various Low Power Wide-Area Network (LPWAN) solutions have resulted in the possibility of transmitting data and communicating in remote environments. The idea behind this work was in fact based on discussions with the Swedish Fire and Rescue Service and their communication challenges during forest fires.

Indeed, remote forests include some of the "non-urban environments" referenced in this work. Other typical areas where a LPWAN network could be beneficial is in archipelagos, or on off-shore oil or wind platforms. In general, these are environments where traditional communication solutions in terms of, for instance, stationary cell phone towers are unfeasible for one or several reasons.

These reasons could include price, access to power, maintenance possibilities, number of expected users etc. Examples of these LPWAN systems include LoRa and Sigfox which uses various techniques to achieve a low power wide-area communication solution [1] [22]. Depending on the scenario, different types of solutions might be preferable for different situations.

As an example, off-shore oil platforms are relatively stable environments with a substantial lifetime. Hence, installing fixed communication systems using the infrastructure on the platform is possible. One company with a product suite dedicated to this is Semco's Maritime division [17].

For the Fire and Rescue Service however, the current market solutions are much more limited. Some of the previous solutions dedicated for emergency personnel in Sweden include the TETRA based Rakel network. It was originally intended to have full coverage over mainland Sweden, although this appears yet to be achieved [11].

Hence, this work will examine how different LPWAN could be used to aid the Fire and Rescue Service with their communication during a forest fire located outside the coverage area of both the cellular and Rakel network. It should be noted that this environment differs notably from, for instance, the oil platform scenario.

An oil platform can also be expected to be an area with communication needs that are located outside both the cellular and Rakel network. The difference is that this type of environment is substantially more stationary and predictable compared to a forest fire. During a forest fire there is often no way to tell where in the forest the fire will start and hence where the need for communication will be.

Further, it should be noted that access to power sources will be very limited which creates further challenges to implement a functioning communication network. The general principles behind LPWAN networks does however create potential candidates for solving this problem and that is something this work will examine. The LPWAN's characteristics of covering a wide area whilst using a low power might definitely be a desirable feature for the Fire and Rescue Service.

Previous similar studies have also been made for tracking and monitoring

patients with mental disorders [8]. It has also been examined how suitable certain LPWAN solutions could be for monitoring troop movements which could be said to have many similarities to the problems that could be expected to be experienced by the Fire and Rescue Service [15].

Hence, this work will examine this further and evaluate some potential LPWAN solutions from the point of view that it should be applied in a real-time positioning system. In general, a LPWAN network have a range from a few kilometers and upwards whilst, for the most part also being associated with a low data rate of 10 bps to a few kbps. Especially for small devices in environments lacking infrastructure such as cell phone towers and Wi-Fi-hotspots the system could be thought to be of interest. Typical for, as an example, LoRa is a reliance on a spread spectrum technique to increase the robustness of the signal [3] [23].

However, the benefits of a spread spectrum technique are many and, having gone from being a highly classified military solution to several commercially available systems today, the future is bright for this type of technology [16]. As said before, LoRa is one example which implements the spread spectrum technique, more precisely a Chirp Spread Spectrum technique which will be discussed further in Section 2 [18]. Also discussed in Section 2 is another popular technique, namely a Frequency-Hoping Spread Spectrum technique.

This work will focus on analyzing and comparing the applicability of these two spread spectrum techniques in real-life scenarios. The desire is to achieve a conclusion to be able to clearly show the advantages and disadvantages of the two spread spectrum techniques and indicate their suitability for implementing in a real-time positioning system.

2 Theory

When analyzing radio network performance several aspects are important to consider and certain terminology will be used throughout this work when discussing radio network performance. To begin with, when analyzing radio communication one of the first aspects that needs to be quantified is the strength at which a signal is sent and received. For this, what is known as Decibel-milliwatts (dBm), is used regularly and interchangeably with the more typical Watt for power. Decibel-milliwatt is the power ratio in decibel with respect to 1 milliwatt as described by the function below.

$$P_{dBm} = 10 \cdot \log_{10}\left(\frac{P_W}{0.001}\right) \tag{1}$$

Based on Equation 1 one can also understand that the following is true:

$$P_W = 0.001 \cdot 10^{\frac{P_{dBm}}{10}} \tag{2}$$

However, for practical reasons, peak-to-peak voltage is also used as an equivalent to the power based on Joules law.

$$P_W = \frac{U_{RMS}^2}{R} \tag{3}$$

Assuming a sinusoidal wave $U_{RMS} = \frac{U_{pp}}{2\sqrt{2}}$. For radio systems R in Equation 3 is often set to 50 Ω as will be explained further on. Combining the information above one can easily convert between peak-to-peak voltage and P_{dBm}.

$$U_{pp} = \sqrt{0.4 \cdot 10^{\frac{P_{dBm}}{10}}} \tag{4}$$

$$P_{dBm} = 10 \cdot \log\left(\frac{U_{pp}^2}{0.4}\right) \tag{5}$$

Equation 4 and 5 will be used throughout this work when converting between peak-to-peak voltage measurements and dBm-power measurements. Moving on, one assumption which was used during the derivation should be clarified further. What was derived is only applicable to 50 Ω systems as this is commonly used in the RF-world [6].

When transmitting the produced radio signal one needs to do this in an optimal way to prevent loss and minimize reflection. Basic calculations can show that 50 Ω is very suitable for this purpose and is thus very commonly used today [6]. Several of the radio chips produced today are also recommended to be used with 50 Ω PCB microstrip. Calculating the impedance of a microstrip, as described by Figure 1, is possible through several different equations and formulas of varying degree of accuracy.

Throughout this work the IPC-2141[5] will be used for calculating the impedance of a microstrip. It is not an optimal equation for every impedance but has a

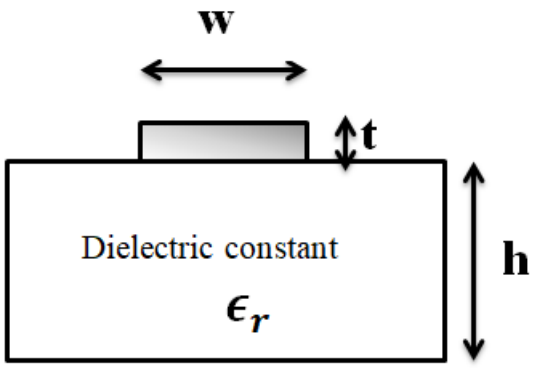

Figure 1: Important constants when designing a microstrip

reasonable accuracy in the 50 Ω region which will be the region of interest as claimed by [2]. The equation is as follows:

$$Z_0 = \frac{87.0}{(\epsilon_r + 1.41)^{1/2}} \ln\left(\frac{5.98h}{0.8w + t}\right) \tag{6}$$

In Equation 6 ϵ_r is the dielectric constant, h the height of the board, t the thickness of the microstrip and w the width of the microstrip as defined by Figure 1. Due to standards in producing PCBs, there are certain values of these variables that are common. As an example, a common PCB with 1 oz copper track on a 1/32 inch substrate would most likely have $t = 35\mu m$ and $\epsilon_r = 4.2$ [2]. The thickness of the PCB, h, is typically 1 mm or 1.6 mm whilst the width of the trace, w, is highly adaptable.

Moving on, another important aspect to quantify when analyzing radio signals is the strength of the signal compared to the strength of the noise. The ratio between the power of the signal and the power of the noise is known as the Signal-to-Noise Ratio (SNR) [7].

$$\text{SNR} = \frac{P_{signal}}{P_{noise}} \tag{7}$$

With the definition according to Equation 7 a SNR < 1 would indicate the power of the incoming signal to be less than the power of the incoming noise. However, it should be noticed that another definition of the Signal-to-Noise Ratio is to use decibel as seen here [7].

$$\text{SNR}_{dB} = 10 \log\left(\frac{P_{signal}}{P_{noise}}\right) \tag{8}$$

In this work SNR_{dB} will note that Equation 8 has been used and SNR will mark usage of Equation 7. Also, a note on the basics of radio communication is what is known as a link budget. A link budget is a tool that can be used to predict

the received signal strength and is thus useful when predicting the distance a signal can be transmitted and still received by the receiver [7].

$$\text{Received power} = \text{Transmitted power} + \text{Gains} - \text{Losses} \tag{9}$$

Equation 9 is a simple description of the definition of how a link budget is calculated. If one is using a pre-manufactured radio chip, the transmitted power is often known. Similarly, any gains are often known variables to the engineer. The losses are however hard to quantify exactly since many factors influence the signal during transmission. Ideal line of sight transmissions however will only experience what is known as a Free-Space Path Loss meaning that if the user knows the lowest power possible to detect with the receiver one can get an approximate understanding of the distance a signal can be transmitted [7].

$$\text{FSPL} = \left(\frac{4\pi r}{\lambda}\right)^2 \tag{10}$$

In Equation 10, r is the distance between the antennas and λ the wavelength of the transmitted signal. Finally, it should be noted that, counterintuitively, for a clear line of sight (LOS) between two antennas it is not necessarily enough with the antennas being in view of each other. This is the result of the Fresnel zone which states that the a wave propagating from a transmitter to a receiver will create a prolate ellipsoidal shape in the space between the antennas. The radius of the zone can be calculated using Equation 11 [7].

$$r_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}} \tag{11}$$

This equation assumes d_1 and d_2 to be greater than λ. n is an indication of the n^{th} Fresnel zone radius and d_1 and d_2 the distances between the antennas and the point of interest. As usual, λ is the wavelength of the signal. Focusing only on the first Fresnel zone radius one can calculate the maximum distance a signal can be transmitted on a flat Earth without being blocked by the ground. Assuming a person is holding the two transmitters they can be said to be located 1.5 meters above ground. For 150 MHz that would mean 4.5 meter is the maximum distance one can transmit before the ground would start interfering with the signal. For 868 MHz, the corresponding number is 13.0 meters.

For many applications however, a slight interference in the Fresnel zone will cause no noticeable problem. Although, the types of antennas will affect the impact the Fresnel zone will have on the transmissions. For a direction antenna one should indeed consider how the Fresnel zone could impact the transmission [7]. Figure 2 shows the first Fresnel zone's theoretical expansion in space for different signals when the distance is one kilometer between the antennas.

2.1 Spread Spectrum

The importance of a spread spectrum technique was briefly mentioned in the introduction, but as this will be a crucial aspect of this work the theory behind

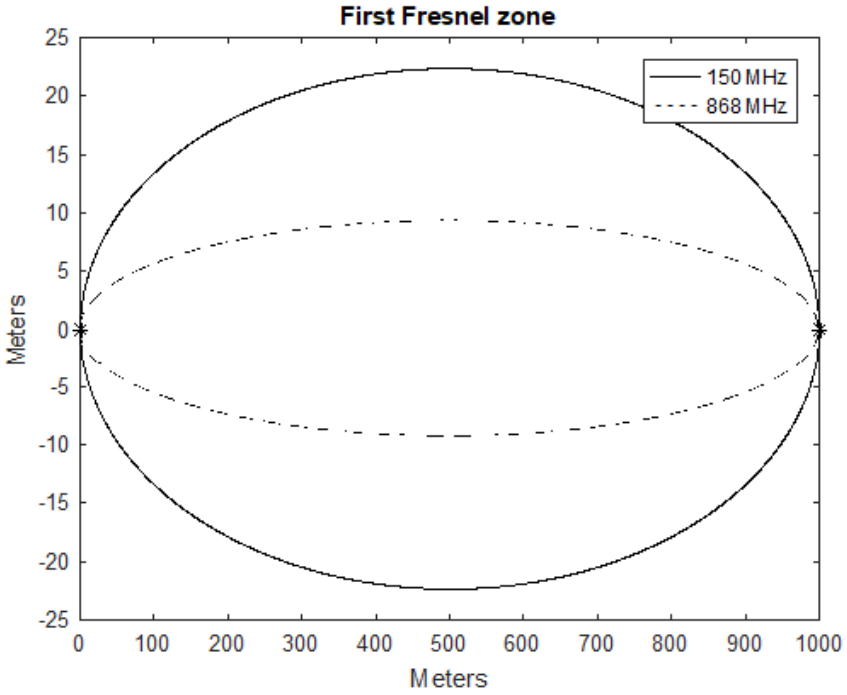

Figure 2: The first Fresnel zone for two antennas located 1 kilometer apart

the spread spectrum technique deserves a more thorough examination. The core of a spread spectrum system is to spread, that is to say, increase the bandwidth of a signal. This can be achieved in a multitude of different ways and the benefits and drawbacks is, and should be, lengthily discussed by R.F engineers proposing to implement this technique [10].

To understand why spread spectrum has increased in popularity one can also analyze what it would mean in terms of channel capacity and for this the fundamental Shannon capacity theorem could be applied [21].

$$C = W \log_2 \left(1 + \frac{S}{N}\right) \tag{12}$$

In Equation 12, C is the channel capacity in bits per second, W the bandwidth and $\frac{S}{N}$ the signal-to-noise ratio. Changing from $\log_2$ to ln and then applying a MacLaurin series expansion would result in

$$\frac{C}{W} = \frac{1}{ln(2)} \cdot \left(\frac{S}{N} - \frac{1}{2}\left(\frac{S}{N}\right)^2 + \frac{1}{3}\left(\frac{S}{N}\right)^3 - ...\right). \tag{13}$$

Assuming a small $\frac{S}{N}$ one could simplify the equation to

$$C = 1.443 \cdot \frac{S}{N} \cdot W. \tag{14}$$

However, as has been observed in real life, infinitely increasing the $\frac{S}{N}$ does not provide an infinitely larger channel capacity. The problem tends to be that the signal does not die out immediately resulting in subsequent pulses [6]. Equation 14 helps to indicate that an increase in bandwidth is beneficial in terms of channel capacity. Further, with a low frequency power density as is associated with the spread spectrum method it does help to provide a convincing case for using a spread spectrum method [12]. The general idea behind a spread spectrum technique is described in Figure 3 [16].

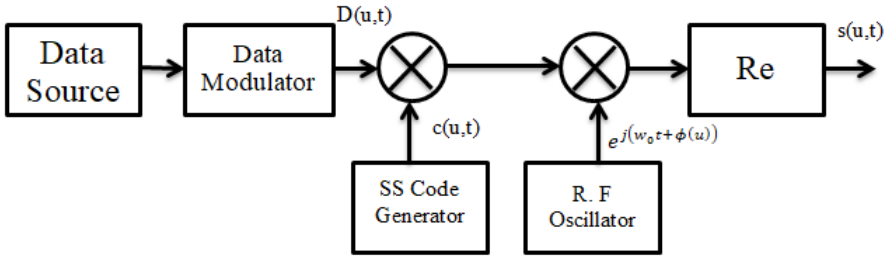

Figure 3: A spread spectrum transmitter described with a block diagram

Although Figure 3 is far from the only way to design a spread spectrum transmitter it helps to clarify the point that the outgoing signal (marked as $s(u,t)$ in the figure) will be affected by the input data, the code generator of the spread spectrum and the RF oscillator. By taking care when choosing how to generate the spread spectrum signal one can make a system very hard to decode for a user not familiar with the spread spectrum code of the system [16].

Figure 4 can be found in [18] and clearly shows the idea behind a spread spectrum technique. Note that when combining the input data with the code sequence the signal is intentionally obtaining a wider bandwidth. This results in one of the benefits with the spread spectrum, namely that it becomes much harder to interfere or jam the signal. Further, as shown in Equation 14, a degradation of the signal-to-noise ratio could be compensated by an increase in bandwidth. Also, if one is able to utilize orthogonal coding sequences the added benefit is also that multiple users can transmit at the same time without disturbing each other. The left part of Figure 4 shows how the input data (1 0) is translated using the code sequence (1 0 1 1 0 1 0 0 0 1 0 1 1 0 1 1). The resulting TX Baseband Signal will be the mixed signal version of these two signals. The standard mixing process will directly translate the code sequence in the time domain where the input data is represented by a 1 and invert the code signal when the input data is 0. The resulting TX Baseband Signal will hence become 1 0 1 1 0 1 0 0 1 0 1 0 0 1 0 0 and it can then be sent to the

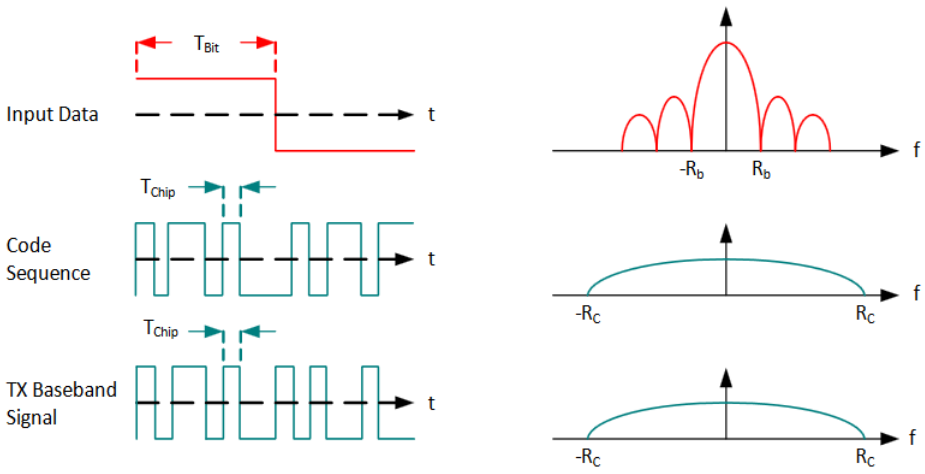

Figure 4: The modulation process of a typical DSSS

receiver. It is however necessary for a receiver to correctly decode the signal in order to understand the data. A block diagram is described in Figure 5 [16].

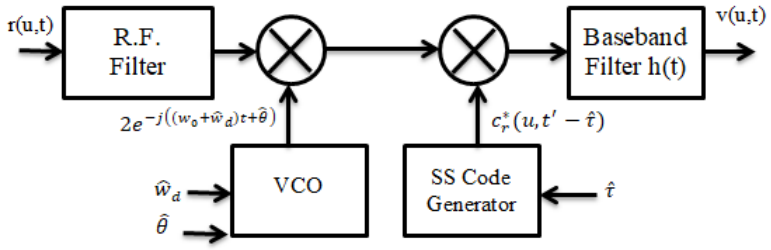

Figure 5: A spread spectrum receiver described with a block diagram

The work will mainly focus on two different types of spread spectrum techniques: Frequency-Hopping Spread Spectrum (FHSS) and Chirp Spread Spectrum (CSS). The main difference is, simply speaking, how one chooses to operate the SS Code generator as described in Figure 3 and 5 [12].

To understand the Frequency-Hopping Spread Spectrum technique one should make a few alterations to the situation shown in Figure 3. A more common approach for the FHSS is to let the SS code generator affect the modulation of the R.F signal and then feed the unaltered data to the R.F modulator. Hence, the case is that for FHSS the spreading signal is used to change the frequency of the R.F modulator. This will cause the typical "hopping" pattern of the FHSS as the data will be modulated on a narrowband carrier signal that changes frequency repeatedly over a wide band of frequencies [10].

As is the case of other types of spread spectrum signals it thus becomes very difficult for a narrowband transmitter to jam the signal. The FHSS is hence a tool to take what might have been a narrowband transmission and spread it out over a larger bandwidth. Any narrowband disturbance on one of the frequencies could however result in the loss of one or more bits depending on how many bits are transmitted within each frequency. Hence, a FHSS transmission is often associated with some type of error correction protocol to try to compensate any missing bits [10].

This however, is typically only true if one or more data bits are transmitted within each frequency. Another solution that might be applied is to increase the stability of the frequency hopping scheme is to divide one bit over several frequencies. A receiver can then make a decision on what this bit has been based on a majority result from different readings of the same bit [12].

Further more, a narrowband receiver used to eavesdrop on the transmission will experience problems due to the frequency hopping nature. As a result it will be problematic for a receiver to distinguish between a bit and a short time impulse noise [10].

Moving on, the FHSS is, as has been stated, not the only spread spectrum technique that can be used. Another one which will be of value to mention for this work is the chirp spread spectrum adapted from its earlier applications in advanced radar systems. The application of CSS is more similar to the situation presented in Figure 3 and the modulation process Direct Sequence Spread Spectrum (DSSS) that is shown in Figure 4 [18].

DSSS is a highly popular solution, but systems used today require highly accurate reference clocks and long synchronization times which have been some of the concerns for adapting DSSS into low-power devices. The idea with CSS is instead to use a chirp, that is to say a signal with a linearly varying frequency when modulating the data. Semtech, a company producing radio chips utilizing CSS, claims the technology address all the issues with DSSS and are suitable for low-power devices [18].

However, every rose has its thorns and it should be said that CSS is not without its own challenges. As will be shown shortly, the data sheet does indeed indicate that CSS is a suitable technique to reach a low-power, long-range and low-cost communication solution. However, with a loss of orthogonality among different chirped waveforms a poor spectral efficiency arises and the modulation rate when using CSS is typically well below the theoretical rate (see Equation 14). As of today (October 2017) there is no known CSS system able to achieve the theoretical rate, mainly due to problems with orthogonality of the chirps [12].

In comparison to FHSS when the bit is transferred over one or several frequencies, the chirps associated with CSS have certain features worth to consider. When analyzing CSS, one often talks about CSS symbols, where a CSS symbol has four important aspects: the spreading factor, the minimal frequency, the maximum frequency and the input bits. It should be noted that in its essence, the spreading factor can be thought of as the number of chirps per symbol. However, by Semtech it is customary to talk about the spreading factor as the

value of the register on their module and this norm will be followed throughout this work when analyzing Semtech's products [14]. Hence, as an example, if a spreading factor in this work is said to be equal to 12 that does not mean that there is 12 chirps per symbol, but simply that the spreading factor register value of a Semtech LoRa module is 12.

For a linearly chirped wave the wave can be described as

$$\psi(t) = \frac{1}{\sqrt{T}} \exp(j\pi\alpha t^2). \tag{15}$$

In this description, α is the chirp rate and T the period. It should be noted that the description is true within the following interval.

$$\frac{-T}{2} \leq t < \frac{T}{2} \tag{16}$$

Using the Fourier transform can be used to obtain the spectrum of the chirp.

$$\psi_\Omega(f) = \mathcal{F}(\psi(t)) = \frac{1}{\sqrt{T}} \int_{-T/2}^{T/2} \exp(j\pi\alpha t^2) \exp(j2\pi f t) dt \tag{17}$$

$$F_\psi(x) = \int_0^x \exp(-j\pi t^2) dt \tag{18}$$

If the Fresnel integral is defined according to Equation 18 then Equation 17 can be rewritten to:

$$\psi_\Omega(f) = \frac{1}{\sqrt{\alpha}} \exp(j\pi f^2/\alpha) \left(F_\psi \left(\frac{f}{\sqrt{\alpha}} + \sqrt{\alpha}\frac{T}{2} \right) - F_\psi \left(\frac{f}{\sqrt{\alpha}} - \sqrt{\alpha}\frac{T}{2} \right) \right) \tag{19}$$

Ouyang et al. have studied the effects of CSS modulation and orthogonality in [12] and they were also able to show that although CSS has its problems, some can be overcome. The LoRa adaption of CSS employs a frequency-shift keying (FSK) to improve the spectral efficiency and it does indeed seem to work. In [12] it is shown that LoRa's CSS has improves the spectral efficiency by a factor of $\log_2(N)$ compared to conventional CSS (see Figure 5 in [12]). However, they can also show that LoRa is far from the most ideal system and it is still far from the theoretical rate. Hence, future development of CSS protocols can be expected but as LoRa is a commercially available system today it can be worth to examine further.

2.2 LoRa

LoRa is a CSS based modulation technique currently implemented in a range of modules produced by Semtech which also offers a variety of commercially available systems that implements this CSS modulation. Hence, it will be of importance for this work and should be explained further. Much of what is presented in this section is based on public information made available by Semtech.

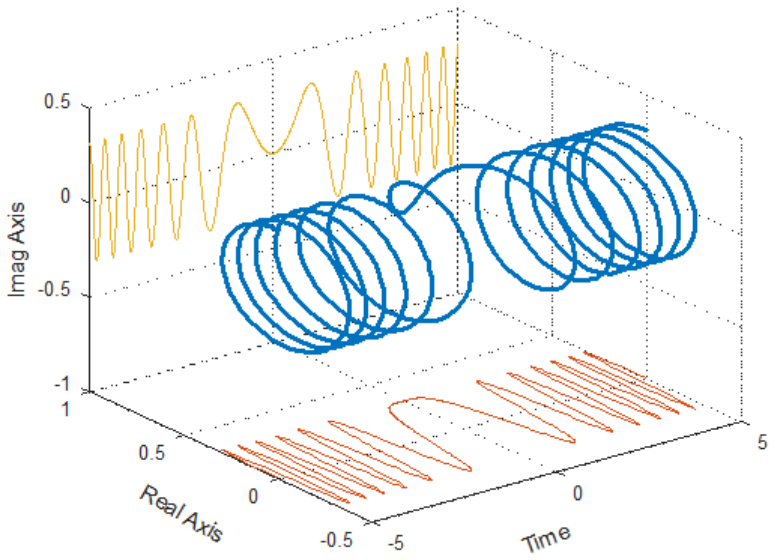

Figure 6: Illustration of Equation 15 with $\alpha = 0.5$ and $T = 10$

The LoRa approach to CSS modulation has several advantages for low-power long distance communication although it has its challenges. One of the inherent practical challenges for the R.F engineer is the bit rate of the system. By Semtech, the modulation bit rate (R_b in bits/s) is described as follows [18].

$$R_b = \mathrm{SF}\frac{W}{2^{\mathrm{SF}}} \tag{20}$$

In Equation 20, W is the bitrate and SF is the spreading factor ranging from 7 to 12. However, LoRa also provides a variable error correction scheme which will somewhat decrease the bit rate of the system.

$$R_b = \mathrm{SF}\frac{W}{2^{\mathrm{SF}}}\frac{4}{4+\mathrm{CR}} \tag{21}$$

In Equation 21, a more realistic bit rate is presented where CR is the register value of the coding rate ranging from 1 to 4 corresponding to 4/5 to 4/8. Equation 21 could also be used to calculate the time it would take to transmit an entire package given that the package size is known. Equation 22 is recommended by Semtech for calculating this for the SX1276-SX1279 modules [19].

$$n = 8 + max\left(ceil\left(\frac{8\mathrm{PL} + 4\mathrm{SF} + 28 + 16\mathrm{CRC} - 20\mathrm{IH}}{4(\mathrm{SF} - 2\mathrm{DE})}\right)(\mathrm{CR}+4), 0\right) \tag{22}$$

In Equation 22, n is the total number of LoRa symbols in a payload structure, PL is the number of bytes in the data message that can range from 1 to 255 per transmission. CRC is 1 or 0 depending on if the redundancy check is turned on and IH indicates if the header is enabled or not. Note that IH is 1 when no header is present. LoRa also have a low data rate optimization option which, if enabled, should cause DE = 1. It is also recommended to use the symbol rate defined as:

$$R_s = \frac{W}{2^{\mathrm{SF}}}. \tag{23}$$

It should be stated that choosing the optimal parameters for the specific use case is of great importance and algorithms are currently being developed [4]. In addition to the actual payload there will be a preamble by default 12 symbols long which will add to the total time of transmission according to the following equation [19].

$$T_{\mathrm{preamble}} = (n_{\mathrm{preamble}} + 4.25) \cdot T_s \tag{24}$$

Also, it should be stated that Equation 22 is not continuous why also the transmission time will not be continuous. SF = 12, CRC = 0, IH = 1, CR = 1, W = 125000 Hz, DE = 1 and $n_{\mathrm{preamble}} = 12$ could be used to calculate the transmission time depending on the package size. The time can be seen in Figure 7.

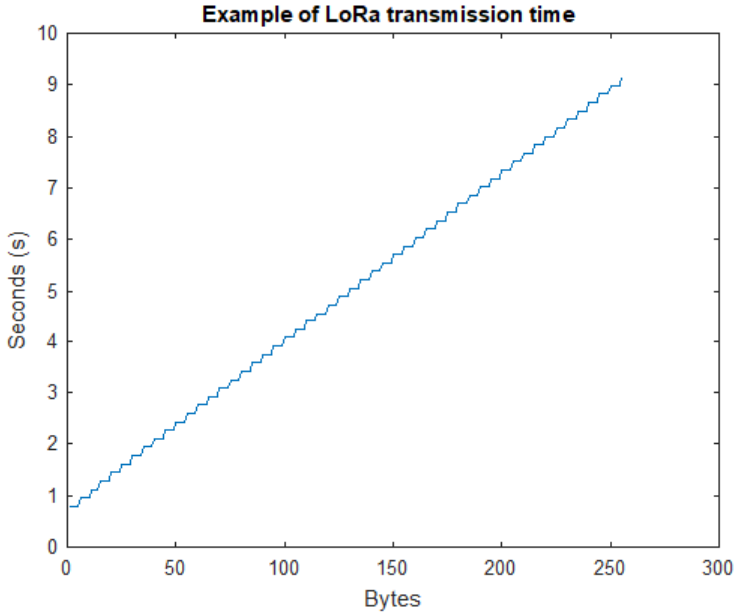

Figure 7: The transmission time of a LoRa signal depending on its size

Note that Figure 7 is not continuous and one should hence understand that less data will not necessarily result in a faster transmission. A detailed section of the transmission time can be seen in Figure 8. As an example, transmitting 15 bytes will take the same time, 1.286 seconds, as transmitting 16, 17, 18 or 19 bytes. Hence, the non-continuous nature of the LoRa transmissions has the effect that less data not necessarily results in a faster transmission. Note that as can be seen in Equation 22, a lower SF will make this effect less pronounced [4].

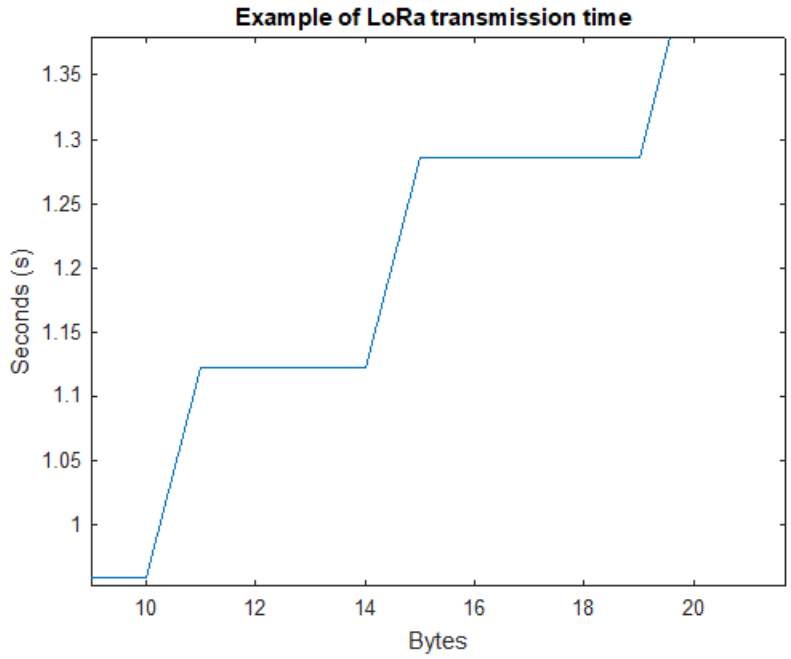

Figure 8: A detailed section of the transmission time

Moving on, in addition to the transmission speed it is important to understand the sensitivity of the receiver and this happens to be a strong suit of LoRa. Semtech's implementation guide offers a formula for calculating the theoretical noise floor of the receiver [18].

$$\text{Noise floor} = 10 \cdot \log_{10}(1000 \cdot kTW) \tag{25}$$

In Equation 25 the factor 1000 is used to scaling to express the answer in dBm. k is Boltzmann's constant and T the temperature in Kelvin. However, as one implementing the LoRa CSS will be quickly aware of is that this theoretical approximation is far from true. Instead, the data sheet of the popular SX1276-SX1279 offers another insight into what one might expect in terms of which signal strength is required. Table 1 consists of the information gathered from the LoRa data sheet [19].

Table 1: Receiver sensitivity at different conditions for band 2 and 3

FDA = 5 kHz, R_b = 1.2 kb/s	−121 dBm
FDA = 5 kHz, R_b = 4.8 kb/s	−117 dBm
FDA = 40 kHz, R_b = 38.4 kb/s	−107 dBm
FDA = 20 kHz, R_b = 38.4 kb/s	−108 dBm
FDA = 62.5 kHz, R_b = 250 kb/s	−95 dBm

Table 1 assumes that the user has shared the Rx and Tx-pins on the LoRa module and FDA is the frequency deviation experienced by the chirps during transmission. If one would not share the Rx and Tx-pins on the module but use separate paths for transmission and reception the sensitivity would be 4 dBm more. Hence, FDA = 5 kHz, R_b = 1.2 kb/s would result in a sensitivity equal to −125 dBm etc. It should also be said that band 2 and 3 is by Semtech defined as 410-525 MHz and 137-175 MHz with exception for certain modules. Band 1, ranging from 862-1020 MHz would instead result in the sensitivity that can be seen in Table 2 [19].

Table 2: Receiver sensitivity at different conditions for band 1

FDA = 5 kHz, R_b = 1.2 kb/s	−119 dBm
FDA = 5 kHz, R_b = 4.8 kb/s	−115 dBm
FDA = 40 kHz, R_b = 38.4 kb/s	−105 dBm
FDA = 20 kHz, R_b = 38.4 kb/s	−105 dBm
FDA = 62.5 kHz, R_b = 250 kb/s	−92 dBm

As before, it is assumed that the Rx and Tx-lines are shared. A slight gain could be achieved by separating the pins, namely 4 dBm, excluding any loss in a potential RF-switch used by the engineer. Even though the theoretical value in Equation 25 was not fully applicable, a 20 dBm transmitter would still have a link budget of around 140 dBm. Further, because of the design of the CSS modulation, a LoRa module would also be capable of understanding signals with a negative SNR.

The current consumption of the module is defined in Table 3 and is based on information from the data sheet. The data in the table is based on usage of bandwidth = 125 kHz, SF= 12, band 3 and a payload length of 64 bytes [19].

As a final note, it should be said that altough the LoRa technology is based on CSS modulation several of its modules does provide a basic FHSS modulation. In the data sheet this is motivated by regulations potentially causing a package to exceed maximum allowed channel dwell time. It is mostly designed for US ISM bands but shows how techniques could be combined to overcome communication challenges, both physical and artificial ones [19].

Table 3: Current consumption for SX1279 at 3.3V

Receive mode, LnaBoost off	11.5 mA
Transmitter mode, PA_BOOST	90 mA
Transmitter mode, 13 dBm	28 mA

2.3 SX Module

Moving, just as Semtech's LoRa has become a commercial alternative for CSS modulated transmissions another company is claiming territory with its mesh technology built around FHSS modulated transmissions. However, this mesh solution holds several built-in features currently not included in the LoRa modules. As an example, as the name indicates, a method to build a mesh network and connect units to each other in order to expand the network is inherent to the system. An illustration of this is shown in Figure 9.[1]

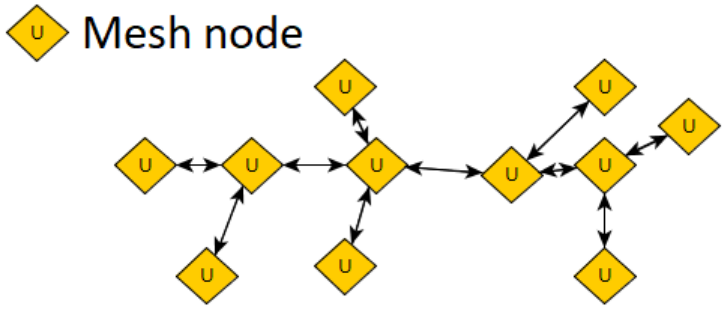

Figure 9: The structure of the mesh network provided by the SX Module

Implementing a similar structure for the LoRa modules is not unthinkable but would require work beyond the scope of this paper, hence the built-in features of the SX Module offers an advantage for the engineer to quickly setup a communication network. Also, in comparison to the LoRa modules the SX Module uses FHSS as its main modulation technique.

Compared to the LoRa module, not as much information is available for the SX Module which is one of the reasons why the information about this module will be limited at best. Regarding the transmission speeds it is mentioned in the data sheet with the explanation that the module has two mode: a high data rate mode and a low data rate mode. With the high data rate, speeds up to 80 kb/s is claimed to be achievable whilst the low data rate is limited to 10 kb/s.

In reality, the through put of a mesh network it is not as straight forward as was the case with the LoRa module. The complexity of the network structure, depending on the number of hops between a sender and a receiver, is a major

[1] The name of the module is withheld for commercial purposes.

driver for data throughput of the network. The data sheet of the SX Module provides some indication to what should be expected. The results presented in the data sheet were acquired by streaming 10 000 bytes of data from a transmitter to a receiver at a serial baud rate of 115 200 b/s.The results can be seen in Table 4.

Table 4: Data throughput for SX Module

Configuration	**Data throughput**
Point to point, encryption disabled	34.63 kb/s
Point to point, encryption enabled	34.48 kb/s
Mesh unicast, one hop, encryption disabled	27.54 kb/s
Mesh unicast, one hop, encryption enabled	27.3 kb/s
Mesh unicast, three hops, encryption disabled	9.55 kb/s
Mesh unicast, three hops, encryption enabled	9.38 kb/s

The chosen data rate mode will also have an effect on the sensitivity of the receiver. The low data rate mode will allow a sensitivity of -113 dBm whilst the high data rate mode limits this value to -106 dBm. It should be noted however, that this assumes that the modules built in LNA is activated as the module does provide a bypass option. Should the bypass be enabled the sensitivity will be limited to -100 dBm and -94 dBm respectively.

Moving on, the current consumption will vary and is defined as Table 5 according to the data sheet. EIRP is short for Effective Isotropically Radiated Power and is the sum of the device's output power and the antenna gain for a 2.1 dBi antenna.

Table 5: Current consumption for SX Module at 3.3V

Receive current	40 mA
Transmit current	55 mA @ 32 mW EIRP
Transmit current	45 mA @ 16 mW EIRP
Transmit current	40 mA @ 10 mW EIRP
Transmit current	35 mA @ 5 mW EIRP
Transmit current	32 mA @ 2 mW EIRP

Finally, regarding the SX Module it should be noted that a user implementing this module is more limited in terms of frequency choice. As said before, a typical SX LoRa module would offer three bands of communication. 137-175, 410-525 and 862-1020 MHz. The SX Module is available in two different versions: the US version operating on 902-928 MHz and the EU version operating on 863-870 MHz. As with the LoRa module, there are settings to prevent the modulation from using certain frequencies in the band to prevent intruding on reserved frequencies [19] .

2.4 Security

As the final part of this theory section, certain security features will be explained. The SX Module offers built-in AES128 encryption as part of a symmetric-key encryption whilst the SX1276-SX1279 LoRa modules does not [19]. AES is short for Advanced Encryption Standard and is, as the name implies, a well used encryption standard. As is the case with many encryption techniques the principle of the AES128 would be according the Figure 10 [9].

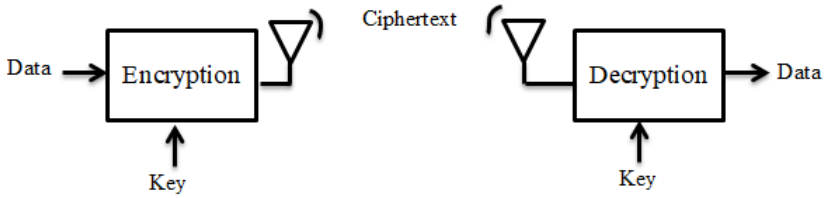

Figure 10: The principle behind the AES128 encryption

In the AES128 encryption a 128 bit encryption key is used to perform the encryption and the technique is considered safe and efficient although weaknesses are actively being searched for [13]. Though the LoRa module does not offer a built in AES encryption is should be said that the situation in Figure 10 is adaptable. As an example, it is thinkable that a user would encrypt the message on a MCU before feeding the information to the LoRa module and hence get the same security value as with the SX Module. It should be noted that the key must still be known both by the sender and the receiver in order for a correct decryption process to be possible.

3 Purpose and research question

The purpose of this work is to evaluate secure long distance communication solutions in non-urban environments for wearable devices. A non-urban environment is defined as an environment where stationary infrastructure, such as cell phone towers, can not be expected to exist. The technologies will be evaluated from the suitability of usage as a communication link in a real-time positioning system. Hence, the research question is:

> What is a suitable technology for secure long distance communication in a non-urban environment for creating a communication link in a real-time positioning system?

3.1 Delimitation

This work will be limited to only examine the LoRa SX1279 module as a representation for CSS modulation and the SX Module as a representation for FHSS modulation. The suitability of the technology will be examined with respect to maximum range (both line-of-sight and a more varied environment), encryption, power consumption, update frequency in a TDMA system and cost. The applicability of a system based on these techniques will then be discussed based on the results from the point of view on a real-time positioning system.

4 Setup

In order to fulfill the purpose of this paper two different hardware designs are created to test the suitability of the different approaches to secure long distance communication in non-urban environments. The different communication modules will be connected to Texas Instruments' MSP432P401M processor and a GPS module used to generate the data. Figure 11 describes the basic setup of the system.

Figure 11: The basic setup of the system

In addition to what can be seen in Figure 11 additional components are also connected to the processor to allow for UART communication with the computer, battery charging etc. The produced hardware consists of the following major sections:

- Processor
- GPS module
- Radio module
- Accelerometer
- UART to USB
- Circuit for measuring state of the battery
- Circuit for charging the battery
- LDO regulator
- Programming contact

The main difference between the two designs will, as stated in the purpose of this paper, be in the usage of two different radio modules. This will also include differences in the hardware layout as the modules are of different size and shape. It should also be noted that the impedance matching is to a large extend done outside the module for the SX1279 module whilst the SX Module has this included in the module. The following parts will describe the implementation for each of the modules.

4.1 SX1279

The SX1279 is a LoRa module and relies on CSS modulation when transmitting the data. The SX1279 is available as a 28-lead QFN package of size 6x6 mm [19]. When implementing the SX1279 module an external impedance matching network was designed in order to guarantee an efficient signal reaching the antenna. The design of this network follows the recommendations from Semtech on implementing the module [20].

The final design can be seen in Figure 12.

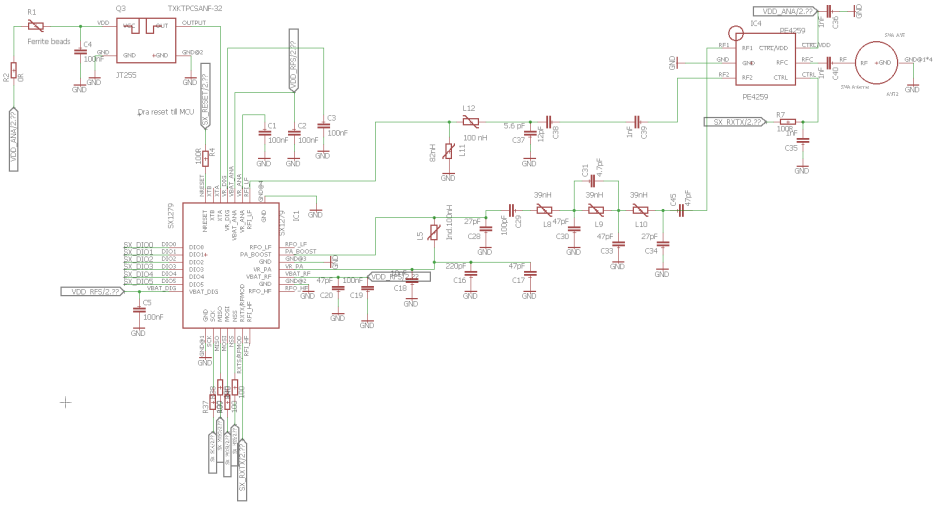

Figure 12: The schematics of the implementation of SX1279

The schematics was then printed on a 2-layer 1 mm thick PCB. The total component cost for 1 complete setup was 175.52 SEK with the money value of 2017-10-04.

4.2 SX Module

Moving on, implementing the SX Module requires few external parts as the module, with its larger size of 33.8x22.1 mm, incorporates many of the components that needed to be added separately to the SX1279.

The total cost for this setup was 206.16 SEK with the money value of 2017-10-04. The main bulk of this cost is the cost for the module. This can be compared to the setup of the SX1279 where the SX1279 module made up only 42 % of the total price. It is also worth to mention that a higher quantity of components tends to lower the price per setup.

5 Results

This section summarizes the results from the experiments with the different modules.

5.1 Distances - Peer to peer communication

The maximum distances achieved by the modules was tested by having one module communicating to another one and gradually increasing the distance between them until the transmission failure was higher than 50 %. The message that was sent was 15 bytes large excluding the headers and house keeping data. Table 6 summarizes the maximum distances achieved with the different modules both line of sight and in the varied conditions described in Appendix A. 1.6 dBi antennas were used during the test. The stationary module was placed at different heights above the ground.

Table 6: Maximum distances in a peer to peer network

	Height above ground	**SX1279**	**SX Module**
Line of sight	10 m	>250 m	>250 m
Line of sight	1 m	>250 m	>250 m
Varied terrain	10 m	938 m	843 m
Varied terrain	1 m	666 m	282 m

5.2 SX1279 signal reception

Two SX1279 systems was placed 20 cm apart and a message of varying size was sent from one module to the other. The built in feature of the SX1279 to determine the signal strength of the received message was then used to create Table 7 and Figure 13 where an average of four messages was used to create the graph. The settings used was SF = 12, CRC = 0, IH = 1, CR = 1, W = 125000 Hz and DE = 1.

5.3 SX1279 outgoing signal strength

A SX1279 system was connected to an oscilloscope via a 50 Ohm RF coaxial cable from the antenna SMA connector and the peak-to-peak voltage was measured for messages with different data sizes. The settings used was SF = 12, CRC = 0, IH = 1, CR = 1, W = 125000 Hz and DE = 1. The results can be seen in Table 8. A graph of the data can also be seen in Figure 14.

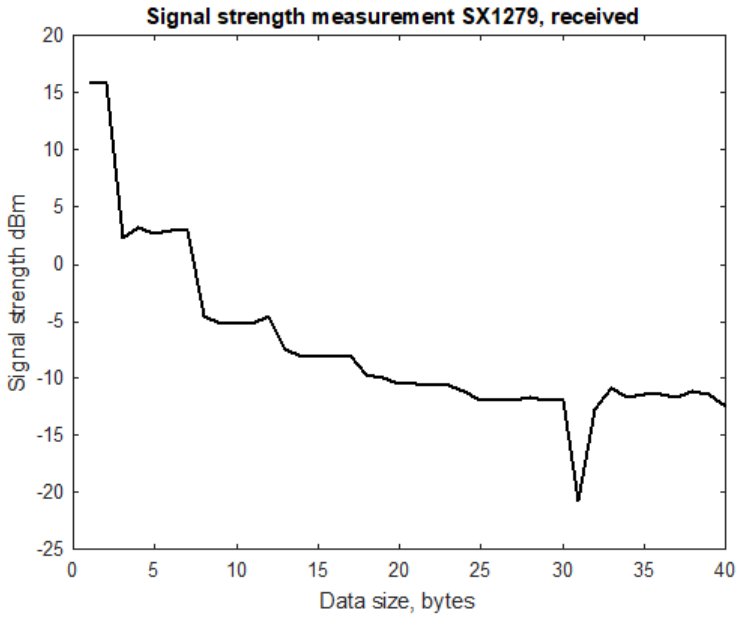

Figure 13: A graph of the average values from the data in Table 7

5.4 Signal strength with different SF, SX1279

The received signal strength of the SX1279 can also be evaluated for different SF. The results are summarized in Table 9 and Figure 15. The other settings used was CRC = 0, IH = 1, CR = 1, W = 125000 Hz and DE = 1.

5.5 LoRa voltage evaluation

Whilst transmitting, a 200 MHz oscilloscope was used to measure the voltage drop on the C2 capacitor as seen in Figure 12. Based on these measurements a voltage drop could be observed when transmitting. The module was powered by a Keithley 2450 SourceMeter. The results can be seen in Table 10.

During the test, the sender's and the receiver's antenna connectors was connected to each other via a coaxial cable. It should also be said that the period of the drop varied between 10-80 ms for all data sizes with no apparent pattern.

5.6 Alternative design for matching network of SX1279

The performance of the SX1279 module was also examined after some changes had been made to the setup seen in Figure 12. The alternative design is seen in Figure 16. With this setup, the results seen in Table 11 was obtained when two boards were connected with a coaxial RF cable.

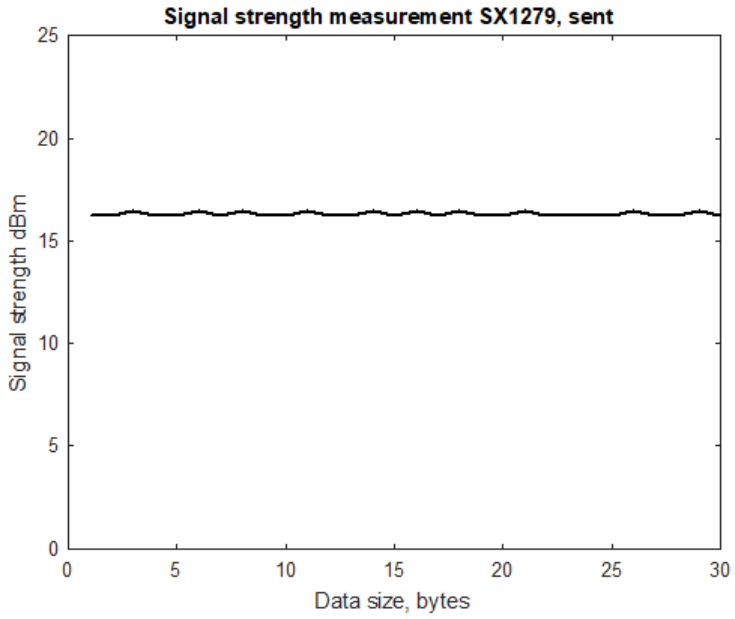

Figure 14: A graph of the values from the data in Table 8

Further increasing the C2 capacitor to 100 μF made the voltage drop disappear.

5.7 Transmission time, SX Module

The transmission times of the SX Module was explained in Table 4. However, from the tests is was noted that the SX Module does not support direct access to the registers. Instead, in order to transmit a package, AT commands have to be used which makes the module internally perform changes to the registers. The process used to make these changes was:

- Wait 1000 ms guard time
- Enter command mode
- Wait 1000 ms guard time
- Set high MAC address to receiver
- Set low MAC address to receiver
- Apply changes
- Exit command mode
- Send data

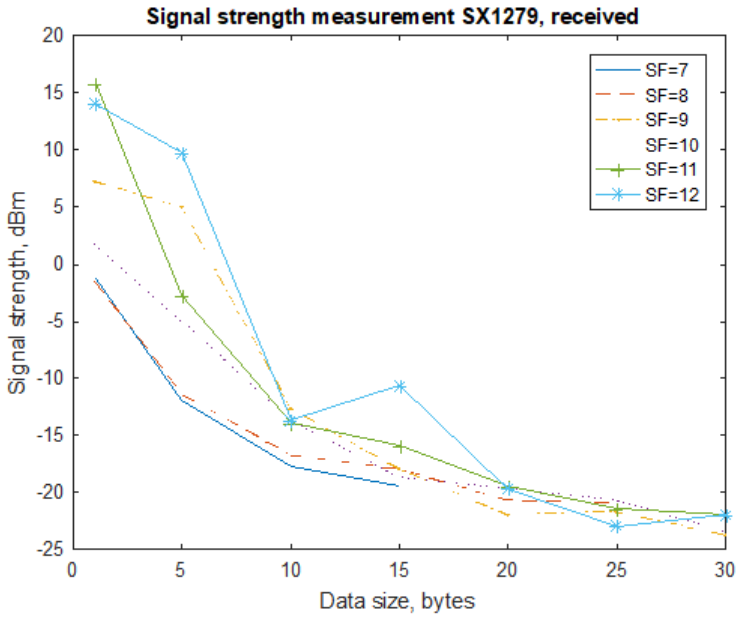

Figure 15: Signal received strength for different SF

The guard time can be changed according to the user's needs.

5.8 Current consumption

The current consumption of the SX1279 system was an average of 26 mA when the system was in listening mode waiting for packets. The increase when transmitting on PA_BOOST was as expected.

The current consumption of the SX Module system in standby mode with the radio listening for packets was an average 31 mA. When transmitting the radio module required an average of 58 mA when sending at 32 mW EIRP.

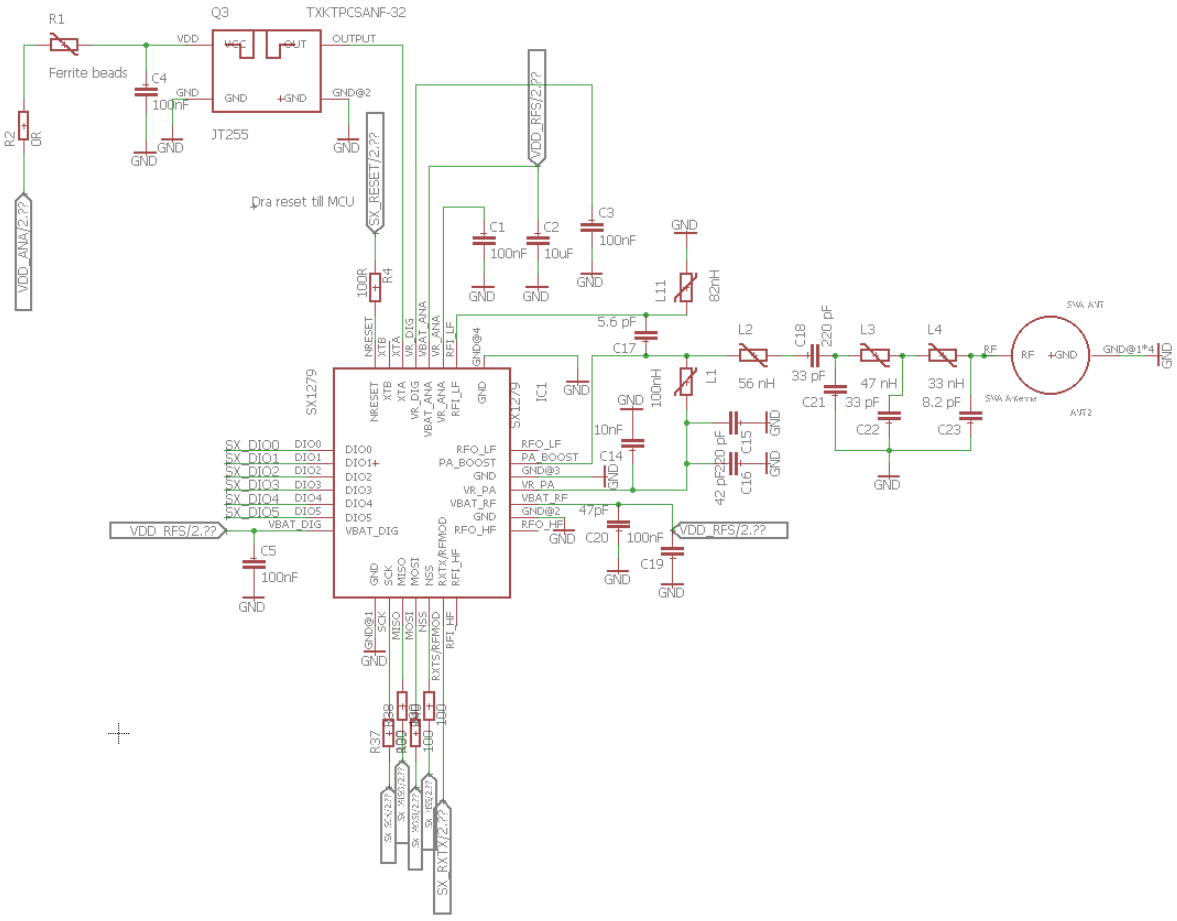

Figure 16: Alternative design for the SX1279 implementation

Table 7: Signal reception strength with different data sizes

Bytes	**Msg1, dBm**	**Msg2,dBm**	**Msg3, dBm**	**Msg4, dBm**
1	16	16	16	16
2	16	15	16	16
3	15	-2	-2	-2
4	-1	16	-1	-1
5	-1	15	-2	-1
6	15	-1	-1	-1
7	-1	15	-1	-1
8	15	-11	-11	-11
9	15	-12	-12	-12
10	15	-12	-12	-12
11	-12	15	-12	-12
12	16	-11	-11	-12
13	15	-15	-15	-15
14	15	-16	-16	-16
15	15	-16	-16	-16
16	15	-16	-16	-16
17	15	-16	-16	-16
18	15	-18	-18	-18
19	16	-18	-19	-19
20	15	-19	-19	-19
21	15	-19	-19	-19
22	15	-19	-19	-20
23	-19	15	-20	-19
24	-20	15	-20	-20
25	15	-21	-21	-21
26	15	-21	-21	-21
27	-21	15	-21	-21
28	15	-21	-20	-21
29	-21	15	-21	-21
30	15	-21	-21	-21
31	-21	-20	-21	-21
32	15	-22	-22	-22
33	16	-20	-20	-20
34	15	-21	-21	-20
35	15	-20	-21	-20
36	15	-20	-21	-20
37	-21	15	-20	-21
38	-20	15	-20	-20
39	15	-20	-20	-21
40	15	-22	-21	-22

Table 8: Signal voltage with different data sizes

Bytes	**P-to-P voltage (V)**
1	4.1
2	4.1
3	4.2
4	4.1
5	4.1
6	4.2
7	4.1
8	4.2
9	4.1
10	4.1
11	4.2
12	4.1
13	4.1
14	4.2
15	4.1
16	4.2
17	4.1
18	4.2
19	4.1
20	4.1
21	4.2
22	4.1
23	4.1
24	4.1
25	4.1
26	4.2
27	4.1
28	4.1
29	4.2
30	4.1

Table 9: Received signal strength. x indicates no received signal

SF	**Bytes**	**Signal strength (dBm)**			
	1	x	x	x	x
	1	-2	-1	-1	-1
	5	-14	-12	-10	-12
6	10	-18	-18	-18	-17
7	15	-21	-19	-20	-18
	20	x	x	x	x
	1	-2	-1	-2	-1
	5	-12	-12	-10	-12
	10	-17	-17	-16	-17
8	15	-18	-18	-18	-18
	20	-20	-21	-21	-21
	25	-21	-21	-21	-21
	30	x	x	x	x
	1	-2	16	-1	16
	5	-5	-4	-6	-5
	10	-13	-12	-12	-12
9	15	-18	-18	-18	-18
	20	-22	-22	-22	-22
	25	-22	-21	-22	-22
	30	-22	-25	-25	-23
	1	-2	-3	15	-3
	5	-2	-6	-6	-6
	10	-14	-14	-13	-14
10	15	-18	-19	-19	-19
	20	-19	-19	-19	-20
	25	-21	-21	-20	-21
	30	-23	-24	-23	-24
	1	16	16	15	16
	5	-4	-3	-2	-2
	10	-14	-14	-13	-14
11	15	-18	-15	-15	-16
	20	-19	-20	-19	-20
	25	-20	-22	-22	-22
	30	-23	-24	-23	-24
	1	14	14	14	14
	5	14	14	-3	13
	10	-14	-13	-13	-13
12	15	-19	-19	14	-19
	20	-19	-20	-20	-20
	25	-23	-23	-23	-23
	30	-22	-22	-22	-22

Table 10: Voltage drop for SX1279 during transmission

Bytes transmitted	**Lowest voltage registered**	**Received signal strength**
1	2.24 V	26 dBm
15	2.24 V	1 dBm
30	2.24 V	-2 dBm

Table 11: Results from the alternative design of the SX1279 implementation

Bytes transmitted	**Lowest voltage registered**	**Received signal strength**
1	2.8 V	-117 dBm
2	2.8 V	-117 dBm
15	2.8 V	-87 dBm
30	2.8 V	-88 dBm

6 Discussion

This section will discuss and analyze the results of the systems. To begin with, it should be noted that based on the theory of the systems the LoRa module had a very optimized link budget which should be expected to give the module a long range. As seen in section 5.2-5.6 there was initially some confusion regarding the performance of the system whilst situated in a lab environment.

6.1 SX1279 lab performance

Figure 13 shows an unexpected problem that was not indicated by the literature analysis. Figure 13 seems to indicate that an increase of the transmitted data size decrease the received signal strength. However, as seen in the data in Table 7, taking an average of all the measurements to produce Figure 13 might be misleading as there always tends to be one high value in the beginning. Taking the average value of the two last measurements produce Figure 17 which gives a new insight in to the behaviour of the system.

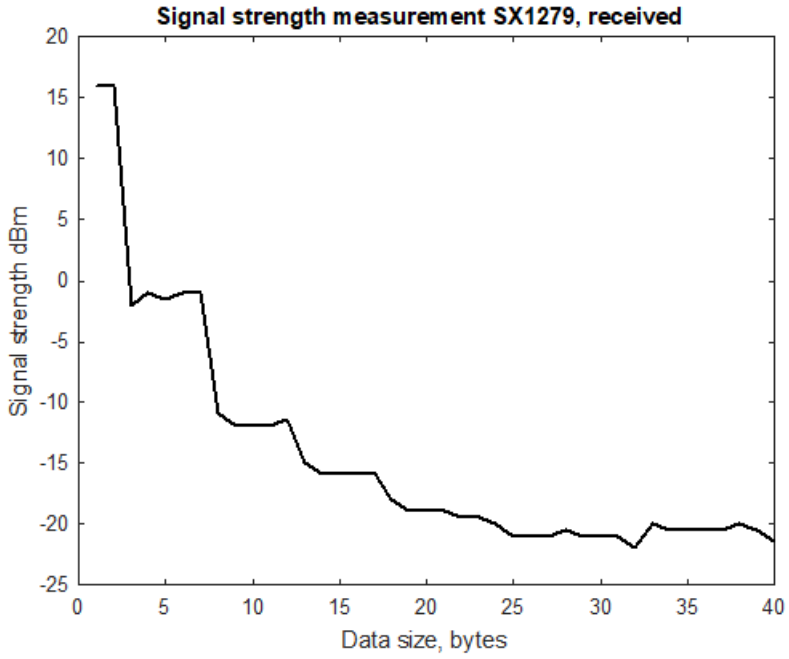

Figure 17: The average of the last two values from the data in Table 7

According to Figure 17 the behaviour seems to be discontinuous with a clear decrease at 3 bytes, then at 8 bytes and later at 13 bytes etc. In the beginning it was expected that this was the result of a voltage drop in the system. A voltage drop was indeed identified, although it did not solve the problem of the

decrease in received signal strength when this voltage drop was counteracted. This might have a number of probable explanations. First, it should be noted that the modules were placed as is shown in Figure 18. Because of this the desktop would have blocked a substantial part of the Fresnel zone.

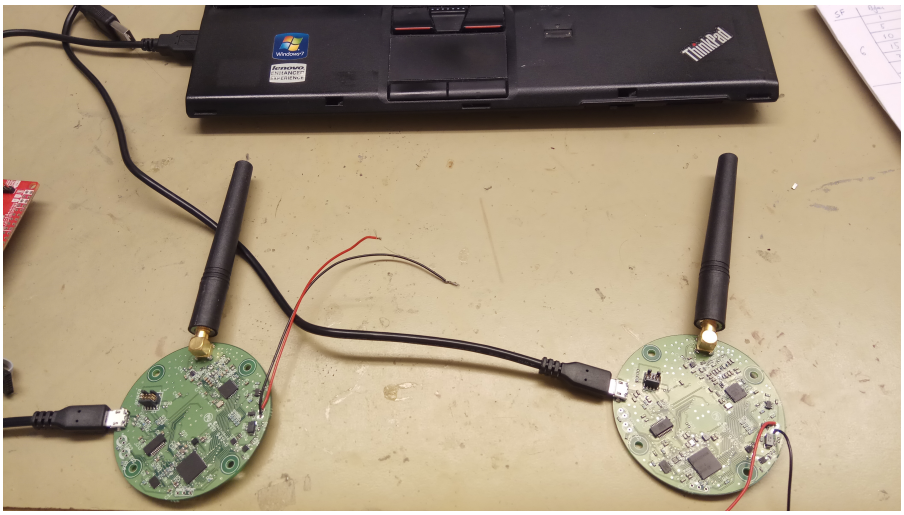

Figure 18: The two modules were placed 20 cm apart

In addition, it is thinkable that the proximity of the modules and the high transmission power resulted in the maximum allowed receiving power of the module to be exceeded. This should especially have been the case when the two modules were connected via a coaxial RF-cable when researching this phenomenon. By connecting the transmitting module straight into the oscilloscope via a coaxial cable it could also be observed that a high power signal reached the antenna for the various data sizes as observed in Figure 14.

When changing the SF, as seen in Figure 15, the results was in line with what had previously been noticed. Based on the documentation of the SX1279 it was known that the SF could be used as a way of increasing the data throughput of the system with a cost on the link budget. Hence, the behaviour observed in Figure 15 is as expected with a higher received signal strength for a higher SF. What remains strange is the overall low value of the signal strength, but again that could be explained by the experimental setup in the lab environment. In the external setting this should not have been observed. It should also be noted that Figure 15 is probably appearing to be more continuous than what is the actual case. More data points would probably have resulted in the same discontinuous appearance as Figure 17.

Based on Figure 14 which shows that the outgoing signal is not decreasing in intensity one should expect the problems to arise on the receiver side. It was also of interest to research if a change in the design of the impedance matching circuit would cause any notable differences. When the entire design was changed

to Figure 16 the results was below expectations which might again be attributed the experimental setup.

In Figure 16 the input and output of the radio signal is connected to each other and there is no longer a need for a RF-switch. As mentioned in the theory section, the data sheet of the SX1279 module describes this as an alternative approach to simplify the implementation of the module. As described in association with Table 1, connecting the Rx and Tx-pins will decrease the link budget.

The explanation that the proximity of the modules exceeded the maximum allowed power receivable by the modules helps to explain why the low value of the signal strength was observed. It is thinkable that this is a mechanism to help protect the circuits of the module. However, the module did perform substantially better outside the lab.

6.2 SX1279 performance in an outside environment

Table 6 shows the SX1279 to work much more reliably outside the lab environment with a very satisfying result. First, it should be said that the line of sight measurements were not able to be done at the full distance first imagined during the design of this experiment. It was first thought that the ice stretching out from the bird watching tower used during the experiment would be strong enough to walk on. However, because of the weather it was not deemed safe and the longest line of site measurement able to be done was approximately 200 meters which all the setups managed to do.

The maximum distance of the SX1279 was approximately 940 meters although as the map in Appendix A shows the topography took a drastic change after that when following the path in the forest. There was both a decrease in altitude and movement behind a mountain. Hence, one could expect another environment to produce more beneficial results for the SX1279. Indeed, this is made probable since the signal reception was around -95 dBm before the signal was cut off. The module has the capability of receiving much weaker signals then that which means the mountain likely absorbed a lot of the signal when continued movement was made of the path.

Based on the results in Table 6 it is also clear how the possible communication distance is affected by how high the module is placed. Based on the theory known about the Fresnel zone this could be expected. However, this should be compared to the results of the SX Module.

6.3 SX Module performance in an outside environment

The SX Module was able to communicate almost the same distance as the SX1279 when the stationary module was placed at a height of 10 meters above the ground. However, when the stationary modules were lowered to 1 meter the maximum communication distance decreased 67 % for the SX Module, whilst only decreasing 29 % for the SX1279. This can not only be explained with the Fresnel zone being more disturbed by the ground since this should have a

larger effect on the SX1279 module with the lower frequency as is apparent from Figure 2.

One explanation for this phenomenon could however be in the different frequencies. It is thinkable that the disturbance experienced by the signal when it has the travel through the biomass close to the ground is more pronounced for the higher frequency used by the SX Module. Future work could do a more thorough study on the choice of frequency, especially as the SX1279 module has the ability to communicate in three distinct frequency bands.

6.4 Secure transmission of data

A purpose with this work has been to identify and evaluate a suitable technology for secure long distance communication. Several security features was identified in the theory section whilst additional precautions (such as a MCU based encryption) was mentioned. The SX Module's built-in AES128 was not matched by the SX1279, but had to be done externally. In addition, it should be repeated that for a user not familiar with the changing behaviour of the transmission signal, an interception could be very problematic. Hence, the spread spectrum technique has an inherent degree of security. Though, the more commercially available these systems are, the less safety will be associated with it.

Further, without proper care the encryption could have a negative impact on the maximum allowed update frequency of the network. As seen in Table 4 the data throughput of the network decrease by 0.43 % for point to point communication. The high transmission speeds, in comparison to the SX1279, makes this negligible for most systems although an external encryption process could help to overcome this problem. With a system based on the SX1279, this solution with an external encryption system is not optional.

6.5 Transmission speeds and update frequency

A system communicating a 15 byte data string in a point to point configuration on the SX Module would have a maximum update frequency of 2309 Hz with encryption disabled. With encryption enabled this value is decreased to 2299 Hz. This should be compared to the SX1279 with substantially lower transmission speeds. For a 15 byte data string, one transmission with SF = 12, CRC = 0, IH = 1, CR = 1, W = 125000 Hz, DE = 1 and $n_{preamble}$ =12 the transmission time would be 1.286 s. Hence, the maximum update frequency would be 0.778 Hz.

Assuming that a real-time positioning system is based on the SX1279 chip and that it would require position updates at least once every 10 seconds would limit the number of active users to a maximum of seven users. The position would then be updated once every 9 seconds in a perfectly synced system. For a SX1279 based system with SF= 11 the maximum number of users would be 15 users.

The maximum update frequency of the LoRa based system could be further increased by decreasing the value of SF. However, as was shown in Figure 15

this would result in a decreased range. The SX1279 is hence clearly showing a drawback of a CSS based system that needs to rely on a high update frequency. However, as was said for the SX Module system in the result section of this work, it does not support direct access to the registers which could impact communication speeds.

It is fully thinkable that another FHSS based system would allow direct access to the registers, but the SX Module required a tedious process to be made using AT commands. Especially the high guard time used as a standard by the system, 1000 ms, is problematic as that would clearly decrease the maximum update frequency for a system that needs to make changes to the registers between transmissions. However, as the guard time is changeable it should not be an insurmountable problem for a system requiring a high update frequency.

6.6 Current consumption

The current consumption for the SX1279 was almost twice what was expected. Some of this could be attributed to losses in the circuit used to test the system, but this result helps to clarify a problem with the theory section. When discussing the specific implementations of the SX1279 or SX Module it is heavily reliable on the documentation provided by the company producing the modules. It could be argued that it is the companies interest to guarantee its users an accurate a well crafted documentation. However, the risk for inaccuracies should always be considered.

Further, it is also possible that the higher than expected current consumption is an indication of the reception problems that was experienced during the testing. It would hence be recommended for future work to examine this further to determine the cause of this value.

Regarding the general current consumption it could be observed that the SX1279 is indeed a power efficient module with the SX Module close behind. One thing to keep in mind is that, although the PA_BOOST setting on the SX1279 module will increase range by sending at 17 dBm compared to maximum 13 dBm with PA_BOOST off, it requires a high current whilst it should be remembered that the CSS protocol used by the SX1279 requires substantial time during transmission.

In terms of applicability for a real-time positioning system the lower current consumption of the SX1279 is definitely desirable. If the current consumed in listening mode could be decreased to the expected 11.5 mA, it would be a highly efficient system. Again, the drawback of the system in terms of current consumption would be the high amount of energy consumed during a PA_BOOST transmission. For a real-time positioning system, which is the application studied by this work, PA_BOOST's 17 dBm transmission would most likely be the system of choice in comparison to the 13 dBm transmission if the maximum distance between two nodes could not be limited. Hence, regular updates, as would be expected for real-time positioning, would require a high amount of energy.

In comparison, it was observed that the standby current consumption of

the SX Module was around 19 % higher than the SX1279, but the maximum transmission current lower than the PA_BOOST mode of the SX1279. However, even with the 13 dBm transmission of the SX1279, the link budget of the SX1279 module would still be higher compared to the SX Module.

Though, the SX1279's implementation of CSS modulation is very efficient the inherent problem of long transmission times will have a negative impact on a battery based positioning system. It is known that a PA_BOOST transmission of 15 bytes would take 1.286 seconds resulting in:

$$90 \text{ mA} \cdot 1.286 \text{ s} = 115.74 \text{ mAs}. \tag{26}$$

Following the same procedure a 13 dBm transmission would require 36 mAs which will be substantially higher than the SX Module system. In terms of current, the engineer should hence consider the transmission time of the string the needs to be sent and the impact the will have on the life time of the system. In addition, the requirements regarding update frequency needs to be considered as seldom transmitting systems based on the SX1279 will have a benefit with the low current consumption in standby mode.

For a real-time positioning system based on the SX1279 with seven users the lifetime of the units can be estimated. Assuming that the transmissions are made with PA_BOOST and that the current used is 90 mA and the current in listening mode between the transmissions is the measured 26 mA. Then the SX1279, powered by a standard 1200 mAh battery, would have have a lifetime of approximately 34 hours excluding the power consumed by the peripheral devices.

6.7 Implementation

Moving on, certain implementation aspects should be mentioned. Regarding the microstrip impedance of the two designs the final product was not exactly 50 Ω as was desired. Equation 6 can be worth to restate.

$$Z_0 = \frac{87.0}{(\epsilon_r + 1.41)^{1/2}} \ln\left(\frac{5.98h}{0.8w + t}\right) \tag{27}$$

As previously said, because of standards in PCB production certain variables here are seldom changed. As a result of this, the equation can be simplified to the following.

$$Z_0 = 36.73 \ln\left(\frac{5.98h}{0.8w + 35 \cdot 10^{-6}}\right) \tag{28}$$

The produced PCBs had a height of 1 mm and the width of the microstrip tracing on the board was 1.5 mm. Based on these values the microstrip impedance would hence have been 58.89 Ω, that is to say 18 % higher than what would have been ideal. Future work could improve this further by increasing the width of the data lines to 1.9 mm instead which would have resulted in an impedance of 50.22 Ω.

Further, it should be stated that the standard components used during the assembly of the two designs, such as resistors and capacitors, had an accuracy of 5 % following the recommended implementation guidelines. It is thinkable that more accurate components could have increased the performance of, especially, the SX1279 module and should be worth to consider further.

Finally, it should be stated that the software implementation of the SX Module was far more unstable compared to the SX1279. Partly because the SX Module did not allow for direct access to its registers but depended on communication using AT commands. Several times it was observed that the response from the AT command was not sent when and as expected which required the software on the local MCU to have more complex design than the SX1279.

Future software updates to the SX Module should hopefully decrease the need for this but the revision 1 of the module used during this work had several software implementation problems that needs to be considered by the engineer.

Moving on, before analyzing and discussion the applicability of these two systems in a real-time positioning system, it is of value to analyze the results from the SX Module further. The data sheet of the SX Module said a line-of-sight range for the system was 14.8 km with a 2.1 dBi antenna. As said before, during the test a 1.6 dBi antenna was used which, as we know from the theory section, should give a slightly lower range.

The theoretical line-of-sight can be calculated using the knowledge of the Free-Space Path Loss as described in Equation 10. This can then be be used to understand the usage of the system's link budget. Before that can be done however, one should write Equation 10 in dB to simplify the comparison to other values.

$$\text{FSPL} = \left(\frac{4\pi r}{\lambda}\right)^2 \tag{29}$$

$$\text{FSPL}_{dB} = 10\log_{10}(\text{FSPL}) \tag{30}$$

$$\text{FSPL}_{dB} = 20\log_{10}(r) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) \tag{31}$$

$$\text{FSPL}_{dB} = 20\log_{10}(r) + 20\log_{10}(f) - 147.5522 \tag{32}$$

With Equation 32 one can then combine knowledge with the link budget to get an estimate of the range parameter, r. In this case the received power, P_r could be expressed as:

$$P_r = P_t + G_t - L_t - L_{fs} - L_m + G_r - L_r. \tag{33}$$

In this case, P_t is the transmitted power, G_t the antenna gain for the transmitter, L_t the losses in the transmitter, L_{fs} the Free-Space Parth Loss, L_m other miscellaneous losses, G_r the gain of receiver's antenna and L_r the loss of the receiver. Unfortunately, the values L_t and L_r is not made public by the

manufacturer and for this reason they will be ignored. For an ideal line-of-sight transmission it will be assumed that the miscellaneous losses are zero, although one should be aware that in a non-ideal environment this is usually far from the case.

Hence, the situation becomes:

$$P_r = P_t + G_t - L_{fs} + G_r. \tag{34}$$

Based on Equation 34 one can then understand that the maximum range is achieved when the P_r is at the minimum value detectable by the receiver. Based on the information presented in the theory section it is understood that this value is -113 dBm in a low data mode and -106 dBm in a high data mode. As a result, the only unknown parameter left is the range. Some restructuring of the equation above would give.

$$\log_{10}(r) = \frac{P_t + G_t + G_r - P_r + 147.5522 - 20\log_{10}(f)}{20} \tag{35}$$

For the high data rate mode, the range would be limited to around 45 km which is far longer than what could realistically be achieved meaning that the system is associated with a range of different disturbance parameters. However, the results achieved during this work is realistically and the, in comparison, large link budget shows the strength of the spread spectrum techniques.

Again, the line of sight measurements were not able to be done to the extent imagined but the results in the varied terrain could be tested extensively. Just as with the SX1279 the terrain used can be seen in Appendix A. It is a dense forest with slight topographic variations. As expected with respect to the Fresnel zones the distance able to communicate decreased quickly once the stationary module was brought closer to ground level. However, as was stated previously. The decrease in the range of the SX Module is larger than what could be attributed only to the Fresnel zone and future work could analyze other explanations further.

6.8 Applicability in a real-time positioning system

The purpose of this work has been to examine the techniques from the point of view that it should be applicable in a real-time positioning system and hence certain features have been identified as important factors for the network performance of the different modules. To begin with, the variations in transmission time and hence data throughput of the systems are worth to discuss further.

During the tests a 15 byte string was used to indicate uncompressed positioning data thought to contain the ID of the unit, latitude, longitude and the time it was updated. Future work could examine the possibility of compressing this data to allow for a shorter transmission time. However, based on the inherent nature of the LoRa transmission it is deemed unlikely to reach a transmission time much less than one second.

As previously explained, this transmission time is extremely high, especially in comparison to the SX Module system. Hence, the LoRa as a basis for a

TDMA based real-time positioning system would be highly limited in terms of possible users before the "real-time" criteria breaks down. For the engineer, it would be a possibility of using another multiplexing technique based on the orthogonal spreading patterns of LoRa if the decrease in link budget would be acceptable. However, as the SX1279 module does not support receiving multiple signals in parallel the receiver unit would have to increase in complexity.

The resilient nature of the LoRa transmissions does however hold an appeal for the person requiring extremely long distance communication. The LoRa transmissions have a maximum link budget of 168 dBm, which is larger than SX Module's 128 dBm. Further, with the LoRa protocol the users have the possibility of recognizing signals with a negative signal to noise ratio. That is to say, the SX1279 have the possibility of receiving and correctly interpreting signals with a strength less the the noise level.

The ability to understand transmissions with a negative SNR was confirmed during this work, although it would have been interesting to also have the possibility to also understand the maximum LOS distance one could achieve with the SX1279.

It is known that many professional radio transmitters used in a forest environment operates at a frequency around 150 MHz. Hence, it is thinkable that the SX1279 would have been more optimal in terms of minimizing signal degradation when operating in the 150 MHz-mode which could explain parts of the results. Further, the SX1279's wide span of available frequencies definitely counts as a benefit for the the module since it can easily be implemented with using a range of different frequencies best suitable to the engineer.

For a system with a limited user base that is able to handle the current consumption and needs to transmit long distances the SX1279 would appear to be a very suitable choice for a radio engineer designing a real-time positioning system. However, the long transmission times resulting in a low update frequency for a system with many users and a high current consumption indicates that the SX Module have certain advantages. The SX Module has a more limited link budget, but could through its built-in support of a mesh network compensate this for a system where the users are spread out beneficially.

This situation can be more generally expressed. Imagining a real-time positioning system where a TDMA scheme is active and the information sent is 15 bytes, the situation becomes as Figure 19 for the SX1279 module.

During the tests of this work it could also be confirmed that a system based on this principle quickly becomes unstable and out of sync if there is no synchronized clock. A quick solution to this problem would be to have a scheme where the hub in the positioning system requests information from nodes based on a predefined ID for each unit. In that case however, the update frequency would decrease further although the system would be more robust to a changing number of users. The situation can be seen in Figure 20 where it has been assumed that a 2 byte signal is transmitted from the hub with the ID of the node that is supposed to answer and provide the position.

The SX1279 could however, with a link budget cost, have an increase in the possible update frequency most notably through a change in the spreading

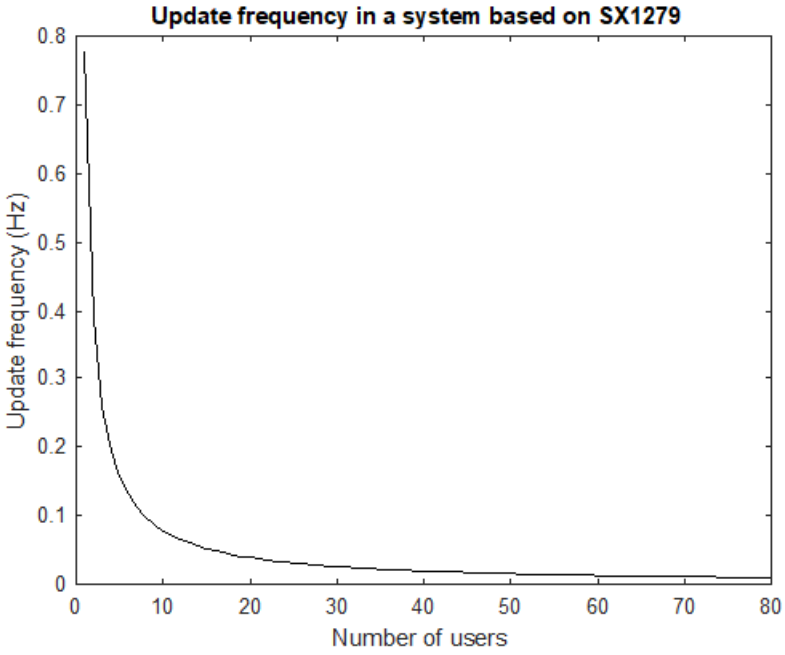

Figure 19: Update frequency for a multiple user TDMA system based on the SX1279

factor. Keeping CRC = 0, IH = 1, CR = 1, W = 125000 Hz, DE = 1 and $n_{preamble}$ =12, the spreading factor can be changed to allow for a faster update frequency. In Figure 21 the update frequency depending on different spreading factors can be seen. It is assumed that a hub is synchronizing the system with a 2 byte ID transmission as was the case previously discussed.

The lower the value on the spreading factor is, the lower the link budget will be. Based on the information available in the data sheet for the SX1279 module one can conclude that the link budget will decrease as follows in Table 12.

It should be noted that the maximum link budget achieved with the SX Module is limited to 128 dBm, although the possible update frequency is completely different. Even with the low data rate, the system would be able to handle 100 users in a positioning system before the SX1279 had completed with one person assuming peer to peer communication for the SX Module system. And the built-in support for an advanced mesh network structure also works to compensate the link budget for a system were the users are spread out.

Moving on, not only update frequencies and link budget considerations have been of importance during this discussion. Also battery consumption should be considered when applying these techniques to a battery based positioning system. It is assumed that the system is powered by a 1200 mAh battery and that the peripheral components such as MCU, GPS etc. will consume a constant

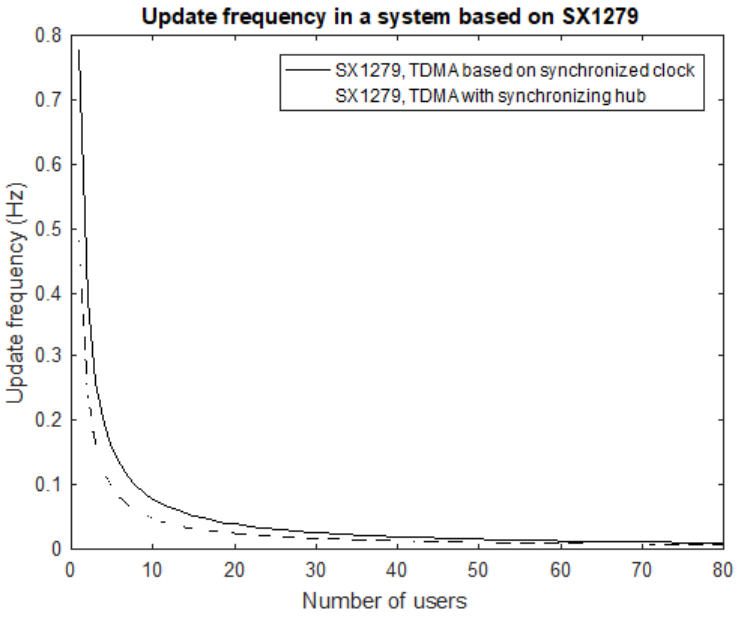

Figure 20: A more robust design of the system will further slow it down

of 30 mA.

For the SX1279 it is assumed that the PA_BOOST is used and that the module is in sleep mode when not in use. Regarding the SX Module it is assumed to use the highest possible transmission power and be in sleep mode when not in use. Figure 22 shows the life time of a system according to these assumptions.

As one can see in Figure 22, the life time will as expected increase if the module is allowed to sleep for a longer period of time between transmissions. That is to say if the update frequency of the system is lower. The SX1279 module in SF = 12 mode is obviously different for the other settings, the reason being the long transmission times. The SX1279 module requires a substantial current during transmission and, as is obvious with Figure 22, it does not bode well for a battery driven system when combined with the long transmission time.

Although the SX1279 has an impressive link budget, other aspects should be considered before implementing the system. Especially the long transmission times could be problematic for a system relying on a high update frequency. Both the SX1279 and the SX Module does however show how the spread spectrum technique could be applied with great benefit. As said in the theory section of this work, the SX1279 is based on the CSS modulation compared to the FHSS modulation of the SX Module. The SX1279 does however have a setting to combine the CSS with the FHSS and maybe similar solutions are what should be expected in future systems.

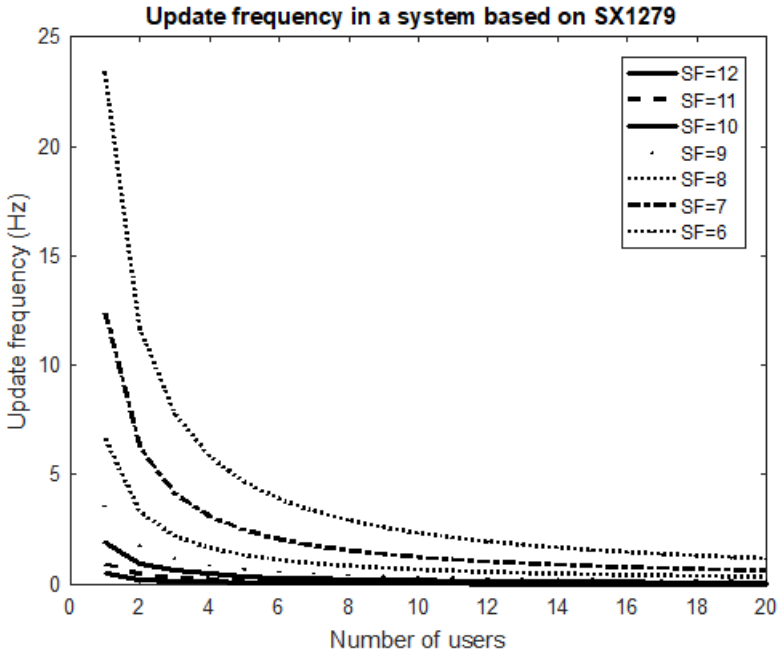

Figure 21: The spreading factor has a notable impact on the update frequency of the system

6.9 Future work and improvements

The purpose of this work has been to examine different technique's suitability to a real-time positioning system. The results obtained from this work creates a stable foundation for a future implementation of a spread spectrum technique in a real-time positioning system. This part of the work will focus on where future work and improvements could be made to further improve the empirical ground for decisions when designing a real-time positioning system.

As part of the hardware design, future work could examine the effect of using more expensive but also more accurate components. As said before, this implementation used components with a 5 % margin of error. The effects of changing this to 1 % would be of interest to determine.

As also noted before, future designs should change the width of the RF micro strips to allow for a more accurate impedance. It would also be of interest to expand the different environments used to test the module to get a better understand about how different environments impacts the usability of the system.

Regarding the SX1279 it would be of interest to examine how the range in a real-life scenario would be affected by decreasing the spreading factor. Decreasing the spreading factor allowed for a higher update frequency which

Table 12: Link budget for a 125 kHz bandwidth, split RX/TX paths, long-range mode with PA_BOOST

SF	Link budget
12	153 dBm
11	150 dBm
10	149 dBm
9	146 dBm
8	143 dBm
7	140 dBm
6	135 dBm

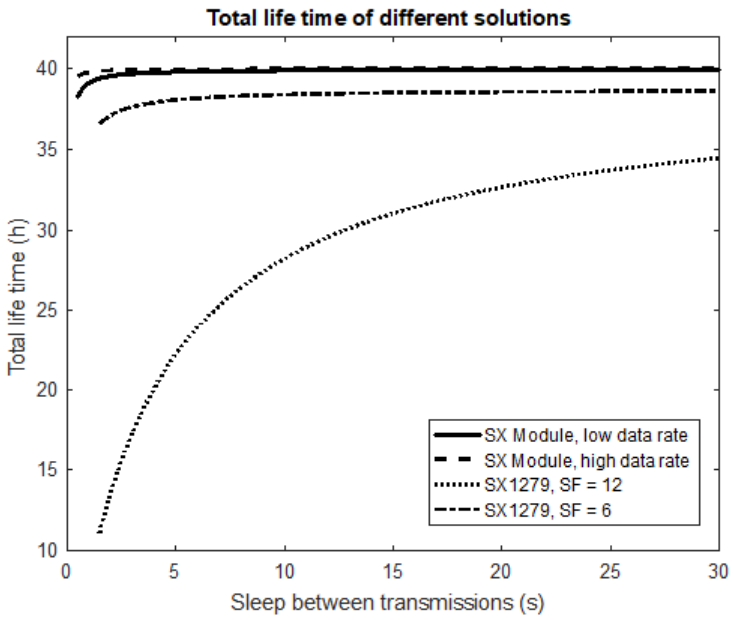

Figure 22: Various life times of a system with a 1200 mAh battery using certain assumptions

would be suitable for applications where real-time applications are of interest.

Should one choose to use a LoRa based system, optimizing the data transmitted becomes of utmost importance. Hence, future work would wisely choose to examine the optimization possibilities further to determine the possible benefits. Especially in a real-time positioning system the data should be able to be compressed substantially as one can assume the transmitters to be located in transmit range.

7 Conclusion

In this work the applicability of two implementations of the spread spectrum technique has been examined through the possibility of adapting it in a real-time positioning system. The spread spectrum technique has potential advantages in terms of low frequency dwell time, low risk for jamming and inherent security features. Both CSS and FHSS was examined as potential techniques and they both showed the advantage of spread spectrum for secure long distance transmissions in non-urban environments.

The LoRa chip was shown to provide a long range transmission which should be beneficial for a real-time positioning system where the users are spread out over a large area. However, as was discussed, the long transmission time results in a very limited number of possible users. An example scenario for the requirements of the Fire and Rescue Service limited the number of active users to seven with the lifetime for a battery driven system approximated to 34 hours. Considering the measured range and the lifetime of the LoRa chip it could be a solution of interest to the Fire and Rescue Service. The low number of users is a problem however and future work should examine the impact of decreasing the spreading factor on the range of the system.

For systems with a low update frequency, great need for a long transmission and few users LoRa's CSS implementation has been shown to be a suitable choice. In conclusion, both of the examined modules showed the benefits of the spread spectrum technique and understanding its benefits and drawbacks will guarantee the right solution being implemented for the right application.

References

[1] LoRa Alliance. Lora alliance, `https://www.lora-alliance.org/` *accesssed:* 2017-09.

[2] Burkhardt Andrew J., Gregg Christopher S., and Staniforth J. Alan. Calculation of pcb track impedance. *Circuit World*, 2000.

[3] J. P. Bardyn, T. Melly, O. Seller, and N. Sornin. Iot: The era of lpwan is starting now. In *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, pages 25–30, Sept 2016.

[4] M. Bor and U. Roedig. Lora transmission parameter selection. In *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 27–34, June 2017.

[5] The Institue for Interconnecting and Packaging Electronic Circuits. Ipc-2141 controlled impedance circuit boards and high speed logic design. 1996.

[6] Roger L. Freeman. *Telecommunication System Engineering.* John Wiley & Sons, Inc., New York, NY, USA, 3rd edition, 1996.

[7] Andrea Goldsmith. *Wireless Communications.* Cambridge University Press, NY, USA, 1st edition, 2005.

[8] N. Hayati and M. Suryanegara. The iot lora system design for tracking and monitoring patient with mental disorder. In *2017 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, pages 135–139, Oct 2017.

[9] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography.* Chapman & Hall/CRC, Boca Raton, 2008.

[10] Earl McCune. Dsss, vs. fhss narrowband interference performance issues. *RF signal Processing*, pages 90–98, September 2000.

[11] MSB. Rakel, `https://www.msb.se/sv/Produkter--tjanster/Rakel/Om-Rakel/`. Accessed December 2017.

[12] X. Ouyang, O. A. Dobre, Y. L. Guan, and J. Zhao. Chirp spread spectrum toward the nyquist signaling rate 8212;orthogonality condition and applications. *IEEE Signal Processing Letters*, 24(10):1488–1492, Oct 2017.

[13] A. A. Pammu, K. S. Chong, W. G. Ho, and B. H. Gwee. Interceptive side channel attack on aes-128 wireless communications for iot applications. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pages 650–653, Oct 2016.

[14] B. Reynders and S. Pollin. Chirp spread spectrum as a modulation technique for long range communication. In *2016 Symposium on Communications and Vehicular Technologies (SCVT)*, pages 1–5, Nov 2016.

[15] W. San-Um, P. Lekbunyasin, M. Kodyoo, W. Wongsuwan, J. Makfak, and J. Kerdsri. A long-range low-power wireless sensor network based on u-lora technology for tactical troops tracking systems. In *2017 Third Asian Conference on Defence Technology (ACDT)*, pages 32–35, Jan 2017.

[16] R. Scholtz. The spread spectrum concept. *IEEE Transactions on Communications*, 25(8):748–755, Aug 1977.

[17] Semco. Semco oil and gas, `https://www.semcomaritime.com/en-en/industries/oil-and-gas`. Accessed October 2017.

[18] Semtech. An1200.22 lora modulation basics, 2015-05.

[19] Semtech. Sx1276/77/78/79 datasheet, Rev 4. 2015-03.

[20] Semtech. Sx127x reference design overview, `http://www.semtech.com/images/datasheet/AN1200.19_SX127x_RefDesign_STD.pdf`. Accessed October 2017.

[21] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, July 1948.

[22] Sigfox. Sigfox, `https://www.sigfox.com/en` *accesssed:* 2017-09.

[23] X. Xie, Z. Xu, and H. Xie. Channel capacity analysis of spread spectrum watermarking in radio frequency signals. *IEEE Access*, 5:14749–14756, 2017.

Appendix A

This appendix shows a map of the area used to measure the maximum distance of the transmissions. The measurements where made during winter and the area was thus covered in snow. Apart from that the weather was clear and there was no precipitation.

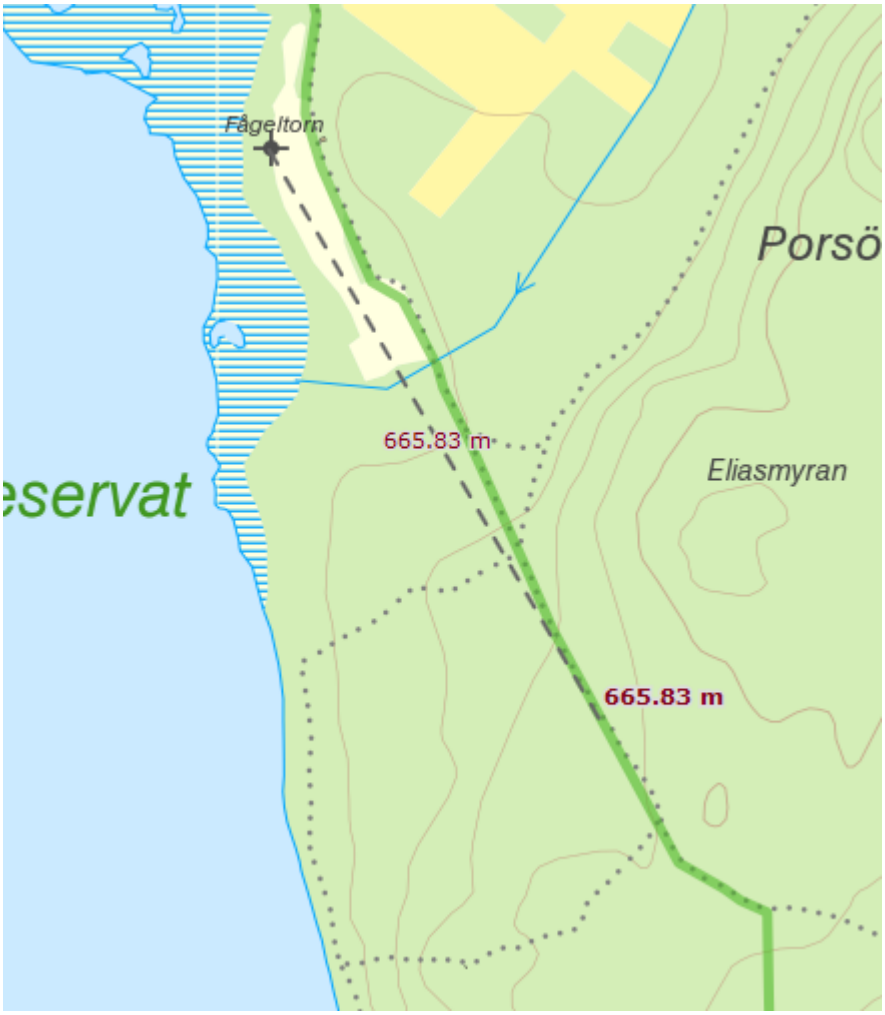

Figure 23: SX1279 placed 1 meter above ground

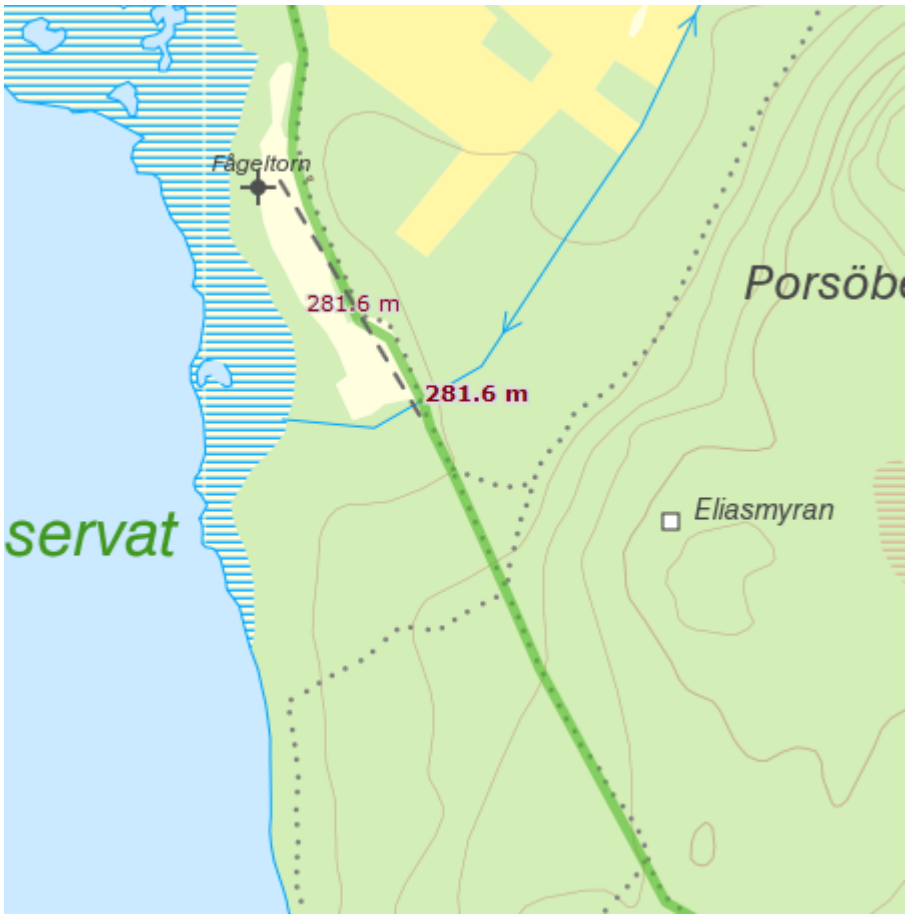

Figure 24: SX Module placed 1 meter above ground

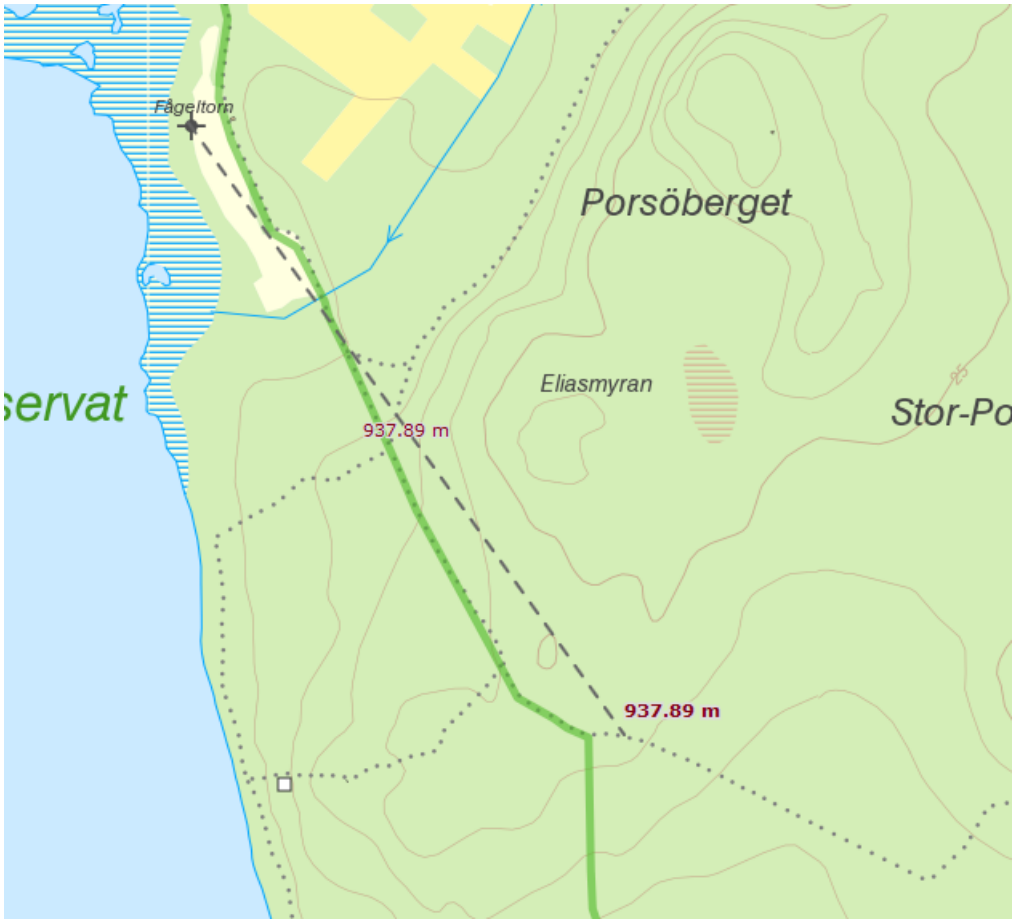

Figure 25: SX1279 placed 10 meter above ground

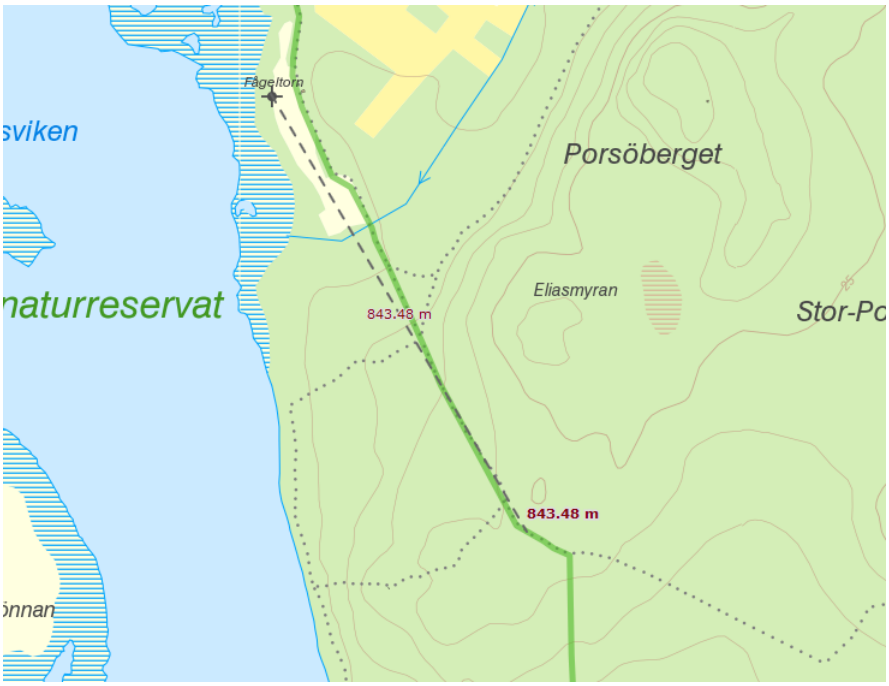

Figure 26: SX Module placed 10 meter above ground