CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Radio signal detection and localisation for uncovering unauthorised signals in an examination environment

Bachelor's thesis in Computer Science and Engineering

Marcus Adler
Otto Lundin
Lam Nguyen
Nour Alddin Taki

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2021

Bachelor's thesis 2021

Radio signal detection and localisation for uncovering unauthorised signals in an examination environment

Marcus Adler
Otto Lundin
Lam Nguyen
Nour Alddin Taki

UNIVERSITY OF
GOTHENBURG

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2021

Radio signal detection and localisation for uncovering unauthorised signals in an examination environment

Marcus Adler Otto Lundin Lam Nguyen Nour Alddin Taki

Supervisor: Arne Linde, Computer- and Information Technology
Examiner: Torbjörn Tjelldén, Computer- and Information Technology

Bachelor's Thesis 2021
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Typeset in LaTeX
Gothenburg, Sweden 2021

Abstract

Examination is a fundamental part of education, both for students and institutions. Cheating on exams is something educational institutions are trying to reduce. One form of cheating is the use of a mobile phone to live-stream the exam to pass the test. The goal of this project is to explore the possibility to detect unauthorised communication and locate the signal source. This is done by constructing a system consisting of three Software-defined radios, ADALM-PLUTO, as anchors. A host computer then utilises the signal strength of incoming signals to estimate the distance to its source, and eventually locate the source using a multilateration algorithm. The combined system resulted in the detection of wireless activity on the 2.4 GHz Wi-Fi band, and it could successfully locate the signal source. However, the localisation could not consistently be repeated. We believe that through further development of the system, there are enormous potential benefits for users, that many interested parties can take advantage of.

Keywords: Cheating, Anti-cheat, Cheat-detection, Radio signal detection, Multilateration, SDR, ADALM-PLUTO, Signal localisation

Sammandrag

Examinering är en grundläggande del av en utbildning, både för studenter och institutioner. Fuskande på tentor är något som utbildningsinstitutioner försöker minimera. Ett sätt att fuska är genom att använda mobiltelefoner för att livestreama provet och på så vis klara av tentan. Målet med projektet är att undersöka möjlighetena att upptäcka obehörig kommunikation och lokalisera signalkällan. Detta görs genom att konstruera ett system som består av tre mjukvarudefinierade radior, ADALM-PLUTO, som ankare. En huvuddator använder sedan signalstyrkan från inkommande signaler för att uppskatta avståndet till källan och för att så småningom lokalisera källan med hjälp av en multilaterationalgoritm. Det kombinerade systemet kunde detektera trådlös aktivitet på 2,4GHz Wi-Fi bandet och kunde framgångsrikt lokalisera signalkällan. Lokaliseringen kunde dock inte upprepas framgångsfullt. Vi tror att genom vidareutveckling av systemet så finns det enorma potentiella fördelar för användare som många intresserade parter kan dra nytta av.

Nyckelord: Fusk, Antifusk, Fuskdetektering, Radiosignaldetektering, Multilateration, SDR, ADALM-PLUTO, Signallokalisering

Acknowledgements

We would like to give thanks to our supervisor Arne Linde for guidance and support during the development of this project. We would also like to thank Prof. Erik Ström, head of the Division of Communications, Antennas, and Optical Networks at Chalmers for his great insight and advice at the beginning of the project.

Contents

List of Figures

List of Tables

Glossary

Anchor ..... Signal receiver with a known position.

BS ..... Base Station is a radio receiver or transmitter that serves as the hub of the local wireless network.

dBm ..... decibel-milliwatts is a unit of level used to indicate that a power level is expressed in decibels (dB) with reference to one milliwatt (mW).

GHz ..... Gigahertz is a measure of a signal frequency.

GNU Radio .. Software toolkit provides signal processing blocks used to implement software-defined radios.

GUI ..... Graphical User Interface for the user to interact with the program.

IMSI ..... The international mobile subscriber identity is a number that uniquely identifies every user of a cellular network. It is stored as a 64-bit field and is sent by the mobile device to the network.

Noise floor ... Noise floor is the measure of the signal created from the sum of all the noise sources and unwanted signals within a measurement system.

Python ..... Computer programming language.

RSSI ..... Received Signal Strength Indicator is a measurement of the power present in a received radio signal.

SDR ..... Software Defined Radio is a radio communication system where components are implemented by software.

1

Introduction

Wireless communication and its uses surround us in today's world and have allowed us to use technology in incredible ways. From using GPS to navigating your way through a country to connecting to the internet through Wi-Fi. However, every rose has its thorn and with wireless technology, new methods of cheating during exams have emerged.

1.1 Background

During exams, online information gathering or communication with others is generally disallowed, and cheaters can oftentimes cheat by using cheat sheets or looking over another participants shoulder. But with wireless communication technology advancing, new ways of cheating are emerging. Some real-life examples of cheating include using a phone to look up answers during the examination, using in-ear headphones [1], or a secret camera that takes photos/record the exam and transmits it somewhere else. Fortunately, there are many ways to detect cheating, like walking around the exam room and checking the students, analysing answers against plagiarism detecting software [2], or investigating unauthorised wireless communication inside the exam room.

1.2 Purpose

This project aims to explore the possibility of detecting and locating unauthorised signal transmitters in an indoor environment and examine whether this could be used for cheat detection purpose. Therefore, the end goal is not a complete product, but rather a proof of concept. This will be done by constructing a system that can detect when someone transmits a signal in a room, and eventually, the system should be able to locate where in the room the sender is.

The result will be presented through a graphical user interface, which will for instance allow an invigilator to do further investigation and respond with appropriate disciplinary actions.

1.3 Delimitation

For this project, the system will only detect 2.4 GHz Wi-Fi signals. There are several reasons for only examining one wireless technology. One of the reasons is to help narrow down the scope of this project to facilitate the development process. Another reason is that a working prototype operating on Wi-Fi 2.4 GHz will lay the groundwork for future iterations of the project to extend upon with more technologies like 5GHz Wi-Fi, 4G, or Bluetooth.

The project has its focus on detecting unauthorised transmitter in an open-space indoor facility since the majority of written exams are held in such facility.

The system will be stationary, meaning that the receivers will be placed around the room at predetermined locations before usage, as opposed to a mobile device that is moved around inside the room during usage. This is due to the significantly higher ease of use and convenience of such a system compared to a mobile one since the system's user does not need to move around to detect a cheater.

The transmitter is assumed to be stationary in the room. This delimitation is partly since all participants are assumed to be stationary and not moving around the room during an exam. Moreover, by assuming that the transmitter is stationary the system does not need to implement a real-time tracking feature.

The transmitter will be sending signals by performing a continuous video call. By using a continuous video call, it mimics a real-world scenario [1], where a cheater uses a hidden camera and stream a video feed to an outside party that gives the cheater correct answers through an in-ear headphone.

Both environmental factors and the inherent behaviour of wireless signal affect the accuracy of the systems [3]. Environmental factors such as noise floor, wall structure and signal behaviours such as echoing, varying signal strength and wall penetration ability make it complicated to detect and locate transmitters. Therefore calibration before usage is required to help mitigate these factors.

Considering this project's aim, only location data of unauthorised transmitters are of interest. The content of the transmitted data, on the other hand, is not relevant, since it is not used in the process of location determination. Therefore this prototype will not be able to and is not going to collect, decode or read transmitted data. Besides, doing this could be considered wiretapping, which is illegal and heavily discouraged in Sweden [4]. To further prevent unwanted data collection, signals that are determined to be from outside of the examination room will be discarded immediately. This is done to avoid unwanted and unnecessary data and preserve the privacy of other people's data.

Developing a surveillance system requires high attention to security details. If an attacker successfully gains access to the system, they can potentially either erase evidence of their cheating or, perhaps more alarming, use the system to implicate

someone else cheating. Common security measures such as encryption and input sanitation should be implemented. Since this is a prototype, security is not prioritised. However, in an actual product, security should be one of the main concerns.

1.4 Method

This section will present different tools and approaches that have been used to develop this project, as well as explaining the intended goals behind using each of them.

1.4.1 Literature review

This thesis is based on different scientific papers and articles that discuss the main topic of the project, which is detecting signals indoors. The search for information about the topic has been done through reliable websites such as the IEEE Xplore digital library [5]. The keywords that have been used for the search were for example ”signal detection”, ”Wi-Fi detection”, ”indoor Wi-Fi detection algorithms”. Furthermore, other projects that utilise the same tools as this project does was also studied. A lot of the articles that have been referred to in this project were found and studied during this literature review phase.

1.4.2 Development process

The development of this project consisted of multiple steps. The first step was to research and collect information that is relevant to the subject of signal detection to build a good knowledge-base regarding the topic. Thereafter, the tools on which the system would be built on were chosen. Due to the availability of the hardware in the early stages of development, the decision of choosing other tools to develop the system depended greatly on the chosen hardware. The next step was to develop and then assemble the different parts of the system for testing, evaluating and improving the system.

1.4.3 Testing setup

Most of the test sessions were conducted in exam rooms in the Johanneberg Campus at the Chalmers University of Technology. However, a few testing sessions have been performed outside the city, in a calmer environment with less interference to test the functionality of the system in a completely different testing setup. Each testing session has been a part of the development process of the system. Furthermore, having different results in each testing session has created the opportunity to improve different part of the system. For instance, improving the signal processing by adding different filters to interpret the signal more accurately.

1.5 Ethics

When technology is developing at an incredibly fast pace, sometimes ethics and sustainability are overlooked by both developers and users. A surveillance system, such as the one that this project is developing, can be of good or malicious use. Many ethical problems emerge along with the development of a surveillance system. Concerns like who is watched, who is watching, what is collected and so on should be taken seriously.

The intended usage for this system is to prevent cheating in the exam. From a sustainability standpoint, this system, if successfully developed and deployed, will increase fairness between exam attendees. If cheaters know that their phone signals are being detected, then this might increases the threshold for cheating, meaning that the cheater finds a quick opportunity to cheat during an exam with their phone.

If this prototype becomes a product, it should only be used as a complement when prosecuting someone for academic dishonesty. Since there is no guarantee that the system will always give correct results. Other evidence should also be used during a prosecution, considering that the consequences of being sentenced to cheating can result in expulsion or a prison sentence [6].

Integrity and privacy violation have been a real concern in the last decade. It is relatively easy to stalk, eavesdrop and spy on people [7]. New laws, that regulate the collection of data like the General Data Protection Regulation (GDPR) [8], are trying to increase personal data protection. Since no one in the group are experts in privacy law, and if the system will be put into real use, then the test administrators are recommended to do some research on how they can legally use the system. One possible solution could be that test administrators inform and ask for attendees consent to the exam so that laws are not inadvertently violated when using the system. Without consenting to these requirements, attendees could be denied from doing the exam. This will prevent possible integrity violation disputes later on. The existence of a transmitting device per se is trivial under the assumption that the institution uses this system for its intended purposes.

So, the answer to the question of who is responsible in case of wrongdoing with this system is both the user and the developer. The developer has the responsibility to build a safe and secure system for its intended usage. The system should only be capable of detecting and locating potential unlawful communication in the exam room for further investigation and not anything else. On the other hand, the user must be authorised and only use the system in the realm of its intended purposes.

2

Theory

This chapter introduces the different theories and literature that have been studied under the process of the project, in order to gain knowledge of different aspects in the topic of detecting signals.

2.1 Radio Wave

This section will lay out some fundamental physical theories behind radio waves and their use for communications. This is a complex field of study, and thus only a brief introduction to relevant topics to this project will be touched on. These include basic radio wave propagation, multipath, and antenna theory.

2.1.1 Radio Wave Propagation

As radio waves travel in the atmosphere of the earth they are affected by several different physical phenomena, all of which results in complex patterns of propagation. The waves attenuate, reflect, interfere, diffract and more [3]. In the most simple case, where a signal travels through a homogeneous medium without obstacles, the strength of the signal at any point will be decided by the frequency of the signal, the strength of the signal at the emission point, and the distance from the measured point to the emission point. When encountering an obstacle, a radio signal will both reflect off of it and attenuate through it, causing the path of the wave to split up. Various materials will also attenuate and reflect radio waves differently. The geometry of the obstacle will also play a major role in how the signal is affected. A radio wave will also interfere with itself, constructively and destructively, causing this splitting up of the wave to add another layer of complexity to the propagation pattern.

2.1.2 Multipath Propagation

Multipath propagation occurs when a signal takes several different paths from a transmitter to a receiver. This may be the case when an object or terrain causes the signal to be reflected. This may also cause the signal to arrive at the receiver at different times and with different strength relative to each other. Since the length of the various paths is probably different from each other, interference may occur.

In the field of radio communications, this is a major concern as this makes it much more difficult to decode received signals when multipath is an issue.

2.1.3 Log-distance Path Loss Model

Path loss is the phenomenon of radio waves, as it propagates through space, gradually loses its power density due to many effects such as free-space loss, diffraction, reflection and so on. Besides, path loss depends on other factors for example distance between the transmitter and receiver, propagation medium and terrain.

The log-distance path loss model is a radio signal propagation model which predicts the path loss that signals encounter over distance. The model is expressed as [9]:

$$PL(d) = PL_0 + 10nlog_{10}\frac{d}{d_0} + X \tag{2.1}$$

$PL(d)$ respectively $PL(d)$ is the path loss at distance d respectively d_0 from the transmitter.
n is the path loss exponent. n varies depending on the environment.
X is the zero-mean Gaussian distributed random variable expressed in decibels (dB), reflecting attenuation of a signal caused by fading in wireless communication.

2.1.4 Antennas

Antennas are of huge importance for any radio application as they are the link between the transmitter or receiver and the free space the signal is to travel through. There are many aspects of antennas that need to be carefully considered when constructing a system so that the signal quality is not unnecessarily worsened [10]. For the antenna to be able to receive the intended signals in the first place, the tuned frequency of the antenna must be known and in the vicinity of the signal frequency. This is most often done by altering the geometry of the antenna itself. A very common type of antenna where this is easily noticeable is the half-wave dipole antenna. The total span of the two antenna elements is one half the length of the tuned wavelength of the signal. The wavelength λ is a direct function of the frequency f according to $\lambda = \frac{c}{f}$ where c is the speed of light.

Directionality is also an important consideration when choosing an antenna. Antenna directionality is a measure of how the radiation density changes over the geometry of the antenna. The directionality of an antenna is referenced to a theoretical antenna called the isotropic radiator. The isotropic radiator is a theoretical antenna that emits a perfectly symmetric radiation pattern. The isotropic radiator is not a physically possible antenna but it is used as a reference point for evaluating other designs. By defining the gain of the isotropic radiator in any direction to be 1 dBi, the gain of other antennas can be defined relative to this. Figure 2.1 shows the radiation pattern of the default antenna that comes with ADALM-PLUTO. Usually, these measurements are presented in two planes and using polar coordinates to allow for easier visualisation. Directional antennas are specifically designed so that the gain is larger in certain directions, and smaller in others, in relation to

the orientation of the antenna. This can help in situations when the direction from where the signal is originating is known beforehand.

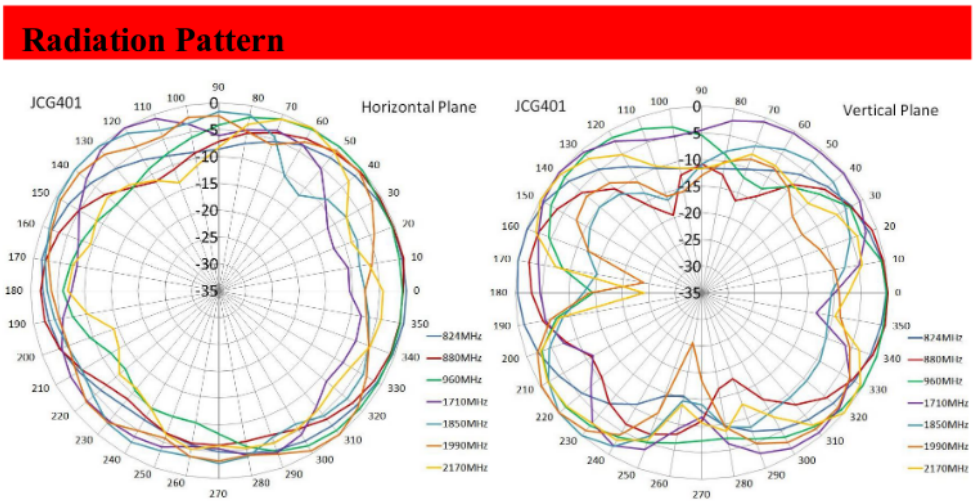

Figure 2.1: Radiation pattern of antenna JCG401 that comes with ADALM-PLUTO [11].

2.1.5 Received Signal Strength Indicator

Received signal strength indicator (RSSI) is an estimated measurement of the strength of a signal at the receiver. RSSI is however not a direct measurement of the power level but rather an estimation of the quality of the signal, where the strength is a major factor. Other factors such as interference from noise and other networks also affect the RSSI. The RSSI is reported as an index ranging from 0 to whatever max value the manufacturer of the hardware has decided. Since radio signals attenuate when transmitted through air, the received signal strength at the receiver will be lower than the transmitted signal strength emitted from the transmitter. Since oftentimes the transmitted strength is not known at every instant, the RSSI value can not on its own be used for determining the length the signal has travelled. Although, if the RSSI at several different points in the same instant and the points relative positions are known, an estimate of position can be derived using multilateration.

2.2 Software-defined Radio

A Software-defined radio (SDR) is a radio device that handles the majority of the signal processing using software rather than hardware. The radio hardware in an SDR is only aimed at gathering and encoding the incoming signals into a format that the software can handle. Afterwards, the software handles filtering and decoding of the signals of interest. This allows for much greater flexibility since the device can accommodate many different applications by changing the software, as opposed to a hardware-based device where the function is predefined and static.

2.3 Wi-Fi

Wi-Fi is a communications protocol used for wireless network connectivity. Wi-Fi is a collection of different standards officially know as IEEE 802.11, which is governed by the Institute of Electrical and Electronics Engineers (IEEE) [12].

The frequency bands used by these standards are also several and depend on the standard in use and its configurations, but the most common operating frequencies for these are 2.4GHz and 5GHz. Wi-Fi is further divided up into channels to allow neighbouring networks to interfere less with each other. For 2.4GHz Wi-Fi networks, there are 14 channels, each occupying a different frequency band [13]. The 2.4GHz spectrum starts at 2401 MHz at channel 1 and ends at 2495 MHz at channel 14. Practically, only channels 1, 6, and 11 are used since these channels allow for the least amount of interference across different channels. This is since adjacent channels overlap with each other which causes noise and in turn congestion. For minimising congestion it is better to use separated channels with several users each than to spread those users out over different but overlapping channels [14].

2.4 Signal Processing

Raw data - data that has not been subjected to manipulation by a software program or human researcher - captured by a software-defined radio contains a lot of information as well as noise. Extracting useful information from the captured data is hard and requires careful analysis of raw data to not misinterpret the information interested. A noise floor filter can be used to pick out RSSI measurements from a transmitter and discard unwanted noise. Thereafter, a Kalman filter is used to reduce fluctuation in the amplitude of RSSI. This section gives a brief introduction and the purpose of those filters.

2.4.1 Noise Floor Filter

Monitoring malicious activity through a wireless connection in an exam requires a substantial amount of RSSI measurements to be collected. With the assumption that only a few students cheat during an exam, a majority of the collected data is noise and trivial to the detection process.

In signal theory, noise is an unwanted and in general unknown signal that carries no useful information. Noise is present and received by radio even without the existence of a signal. The noise floor is defined as the measurement of signals created from the sum of all noise sources and unwanted signals within the system [15]. If the interested signal has a lower RSSI value than the noise floor, then it cannot be detected. Since radio signals attenuate with distance, noise floor limits the maximum distance between an anchor and a sender. Therefore the determination of noise floor is essential to the deployment and calibration of the cheat detection system.

2.4.2 Kalman Filter

As mentioned before, RSSI is noisy due to its environmental dependency. Each sample of RSSI is different from the other in amplitude despite the same system configuration. Depending on constructive or destructive interference of incoming signal, RSSI reading fluctuations manifest as peaks and dips in an amplitude-time graph [16]. If these variances are big enough, it will throw off the location calculation and results in a big error margin. To combat this issue, a Kalman filter is applied to a series of RSSI measurements to generate a more accurate estimation of the true RSSI value

Kalman filter is an effective recursive algorithm that estimates the state of a dynamic system from uncompleted or noisy measurements. It is named after Rudolf E. Kálmán, a mathematician who is the primary founder of the algorithm [17]. Kalman filter is widely used and has numerous applications in technology such as guidance system, navigation and time analysis in signal processing.

Kalman filtering is a two-step process: prediction and updating [18]. Assuming that the k-th state of the system is a function of the $(k-1)$-th state as followed:

$$x_k = F_k x_{k-1} + B_k u_k + w_k \tag{2.2}$$

Where F_k is a state transition model which is applied to state $k-1$. B_k is the control-input from the system which is applied to the control-vector u_k. w_k is the process noise, which is the noise caused by calculation in the system itself. w_k has a covariance of Q_k. For this application, a constant RSSI measurement is expected because of the assumption that the sender does not move during the exam and no input is taken to regulate signal strength. Equation 2.2 is simplified to:

$$x_k = x_{k-1} + w_k \tag{2.3}$$

In state k an observation of true RSSI value is made according to:

$$z_k = H_k x_k + v_k \tag{2.4}$$

H_k is the observation model which maps the true value of RSSI to the observed value and v_k is the measurement noise with covariance R_k. Since RSSI measurement is directly used and considered to be the observed RSSI without any modification. Equation 2.4 becomes:

$$z_k = x_k + v_k \tag{2.5}$$

- Prediction

$$\bar{x}_k = x_{k-1}$$
$$\bar{P}_k = Z_{k-1} + Q_k$$

- Updating

$$K_k = P_k/(P_k + R_k)$$
$$x_k = \bar{x}_k + K_t(z_k - \bar{x}_k$$
$$P_k = \bar{P}_k(1 - K_t)$$

Notice the difference between x and $\bar{x}$, P and $\bar{P}$. x and P are the estimated value of RSSI and the covariance, while $\bar{x}$ and $\bar{P}$ are the value of RSSI and its covariance after correction.

2.5 Position Determination Algorithms

Position determination algorithm refers to the methods that are used to compute and localise the source of a captured signal. Several algorithms are based on different computations and parameters. For instance, some algorithms can determine the position of a signal through a database of fingerprints of the signal, and some algorithms rely on computing the signal strength to localise the source [19]. Some algorithms rely on the direction from which the signal is coming from to determine the source of that signal. In this section, two algorithms that have been considered during the process of the project will be talked about.

2.5.1 Multilateration

Multilateration is an algorithm that can estimate the location of the source of the signal using the location of at least three base stations (BS) and their distance to that source as shown in figure 2.2. It relies on computing the intersection between the circles that have the distance between the BSs and the source node as their radius. By using the noise floor filter and Kalman filter, the performance and the accuracy of the multilateration algorithm can be enhanced and improved for instance by alleviating the impact of the environment-related errors such as noise and physical obstructions between the BSs and the source sender [20].

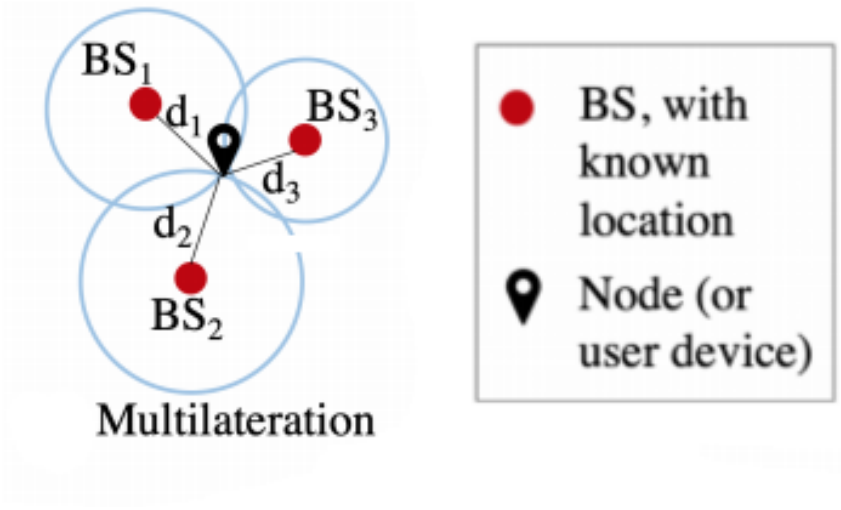

Figure 2.2: A positioning system based on Multilateration algorithm, [21].

2.5.2 Multiangulation

Multiangulation is an algorithm for computing the position of the source of a signal by measuring the angle between the source and at least two base stations as shown in figure 2.3. This algorithm uses position information that is derived from several other methods such as Angle of Arrival, Time of Arrival, signal strength, or Time Difference of Arrival to localise the intended signal [22]. This method has been widely used in wireless Ad-hoc networks due to the accuracy it provides for positioning in the network [23].

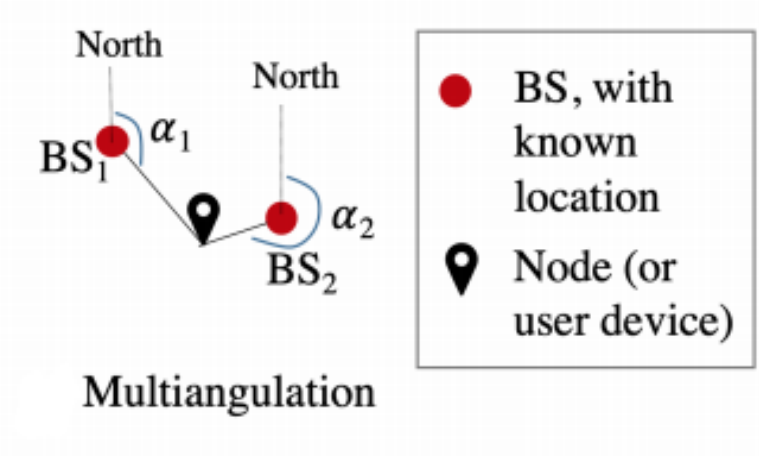

Figure 2.3: A positioning system based on Multiangulation algorithm, [21].

3

System

This chapter gives a briefing about different software applications, hardware and tools that are used to build the prototype. For the second part, an overview of the system is operated including how the system is setup, calibrated and used.

3.1 A top-down approach analysis

The system needs to do two things: detecting and locating the signal source. Detecting the wireless activity can be done by analysing the RSSI spiking frequency in signal strength recorded by the system. When a network package is sent, the RSSI will spike over the noise floor level unless there is too much noise. If the system records a lot of those spikes in RSSI under a short period of time then there is a probability that someone is using that Wi-Fi channel.

Locating the signal source is more problematic. The chosen location detection algorithm is multilateration, which means that an estimated distance between each anchor to the signal source is required. This is where the log-distance path loss model comes into play. If a model of RSSI attenuation over distance is created, which can be done by calibrating the system, then distance can be estimated through the RSSI reading. Now with distances from the signal source to each ADALM-PLUTO calculated, the estimated coordinates of the signal source inside the room can be determined.

One of the disadvantages of this approach is that it is acceptable to noise. The noise floor can jump up to a higher level if there are ongoing wireless activities in nearby Wi-Fi channels, which overlaps the observed channel. Since these noises are stronger than the set noise floor during calibration, they will be registered as real wireless activities and not noise. This will potentially through off the system. Luckily, non-overlapping channels 1, 6 and 11 are most commonly used as mention in section 2.3, the risk of interference from overlapping channels is mostly avoided.

3.2 System Specification

The system can be divided into two parts, hardware and software. On the hardware side, the system is constructed using a host computer, three anchors which

are software-defined radios with their respective antenna and a network switch for communication between the host and the anchors. The software that the system runs on was developed in python with help of GNU Radio. Location detection is based on the multilateration algorithm.

3.2.1 Software-defined Radio

There are many software-defined radios available for commercial use on the market with significant variation in capability and price range such as ADALM-PLUTO, HackRF One, RTL-SDR and so on. The most important requirement for choosing an SDR for this project is that the SDR covers the spectrum from 2.4 GHz to 2.5 GHz, where Wi-Fi 2.4 operates. For that reason, RLT-SDR which has frequency ranges between 500 MHz to 1.7 GHz is not an option.

Both ADALM-PLUTO and HackRF cover the desired spectrum. HackRF One is one of the better alternative considering its higher sampling rate and broader operating frequency out of the box. With a firmware update, ADALM-PLUTO could cover the same spectrum as HackRF [24]. The choice between these two SDR boils down to price and availability and ADALM-PLUTO was chosen due to just that.

ADALM-PLUTO Active learning module, also known as PlutoSDR, is used as a radio signal receiver for this project [25]. This was selected due to the highly versatile nature of SDRs, as well as the consideration for ease of use and availability. The device is capable of receiving signals between 325 MHz up to 3.8 GHz, which is well within the desired range for the project. The sample rate of ADALM-PLUTO is over 64 Mega samples per second with a 20 MHz bandwidth. With these specifications, ADALM-PLUTO can almost cover a whole Wi-Fi channel. Since the device is designed for educational purposes there is a good amount of documentation, allowing for more rapid development. There are two ways to connect an ADALM-PLUTO to a host computer. The first and easiest way is to directly connect the ADALM-PLUTO to a host computer via USB 2.0, which simultaneously supplies power to the ADALM-PLUTO and captures radio signals from it. For this project, however, ADALM-PLUTO is connected to a host computer via Ethernet cable. A Micro USB to Ethernet adapter is plugged into the ADALM-PLUTO to transfer captured signals to the computer, while power is supplied through a specific power port. This was done to more easily connect multiple ADALM-PLUTO devices to a host computer without long USB cables which may cause stability issues. Besides, a long Ethernet cable, up to 10 meters, is more accessible than 10 meters micro USB to USB cable.

3.2.2 Antenna

The antenna that has been used during this project is a Global System for Mobile (GSM) antenna. Those antennas came with the SDR that was used during this project, ADALM-PLUTO, and they can cover 824-894 MHz and 1710-2170 MHz [26]. According to the specifications the antennas are mostly omnidirectional in the horizontal plane. GSM antennas are typically used in mobile phones and cell towers.

During the calibration phase, those antennas seemed to be working as intended for the project. Hence they have been used for the rest of the testing sessions.

3.2.3 Python

The programming language used in this project is Python 3.8 [27], as this is a very powerful language for rapid prototyping and testing. Python has a huge library of frameworks that extend the functionality of the language [28]. The Python community is huge and helpful. Besides, GNU Radio is mainly built on Python and C++. [29]. Developing software with Python will mitigate the risk of complication in integration with GNU Radio.

Python was chosen over other programming languages since the development team has already had better knowledge of Python beforehand. Besides, Python facilitates connections between different parts of the system, which were also built in Python.

3.2.4 GNU Radio

GNU Radio, an open-source program, is extensively used for developing an application to perform signal processing in this project [30]. GNU Radio offers different source blocks, which is responsible for connecting and extracting data from an SDR to the host computer. Moreover, it has a graphical interface to easily connect and manage different elements in signal processing, such as filter, decoder, synchronisation, etc. GNU Radio allows for flowcharts to be constructed using pre-programmed blocks that allow for easy development of a radio system. An embedded Python block can be used for easier integration of custom features in GNU Radio. ADALM-PLUTO already has integrated blocks, namely ADALM-PLUTO Source block and IIO Attribute block, which is used for connecting, extracting data and controlling its functionality in GNU Radio [31]. Using GNU Radio will save a lot of time and troubles in the developing process.

GNU Radio was chosen over other signal processing tools, like MATLAB, since it was deemed easier to integrate GNU Radio with the constructed software due to both being implemented in Python.

3.2.5 Algorithm

As mentioned in section 2.5.1, multilateration was the chosen position determination algorithm for this project. The algorithm was implemented in the system using three anchors. This algorithm is one of the most popular ones in the branch of signal localisation due to the ease of use, and the low cost of the equipment needed to implement it into the system. The chosen algorithm was partly made because other algorithms require more complicated implementations than multilateration. Another reason for choosing multilateration was as a result of the simple geometry used to compute the position of the transmitter signal. During the early steps of the project and literature review, different algorithms were considered. However, this

method seemed the most suitable and applicable with the available timeline and equipment to obtain to some extent a good result.

3.3 System Overview

The operation of the system is split up into two distinctive modes. The first mode is the setup stage that handles setting up the system to work in a particular room as well as calibrating the receiving units. The second mode, called the ”running mode”, collects RSSI measurements and runs the location detection algorithm. This mode gathers information from the receiving devices and calculates an estimation of where a cheater might be in the room.

3.3.1 System Setup

Three ADALM-PLUTO devices are placed at predetermined locations inside the exam room. The dimensions of the room are measured and entered into the program during the calibration phase, along with the positions of the ADALM-PLUTO devices. After defining these variables, the receivers are calibrated using a transmitter placed at various locations in the room. At each location, the RSSI at each receiver is noted down by the program, along with the position of the transmitter which is entered by the system's user.

The program will build a list of coordinates and their corresponding RSSI values, which are then fed into the log-distance path loss model to create a function simulating the relation between RSSI and distance to the transmitter. This model will be used later on by the system to locate received signal sources in running mode. All settings entered in setup mode will be saved and can be used again without going through the setup steps again, provided the environment the system is deployed in has not changed significantly.

3.3.2 System Calibration

Calibration of the system after deploying is required due to the unpredictable behaviour of radio signal in an indoor and noisy environment. Only using the path loss model to predict signal strength attenuation leaves a lot to be desired accuracy wise. For example, anchor A is placed near a known noise source outside of the room which constantly transmits a signal. Then A's floor noise level will be different from another anchor B's, which is outside of the noise source's range. Besides, other incoming signals to anchor A's antenna is prone to interference from the noise source and possibly yield different RSSI measurements than B's. Therefore, a well-calibrated system increases the accuracy of true RSSI value prediction, which in turn improves location determination precision.

Every deployed system is calibrated in two steps. The first step is determining the noise floor level. This process is carried out by measuring the RSSI level in the room without any transmitting devices. The result is then filtered and used as a

threshold for noise floor filter. This filter reduces the huge amount of raw data to a manageable size of interesting data for further location determination process.

The second step is RSSI fingerprinting. To simplify the mathematical modelling of radio signal attenuation, the RSSI measurement when a transmitter is 1 m away from each anchor is required. The distance between the transmitter each anchor is manually recorded and put into the system. At each location, a sender continuously transmits signal and RSSI is recorded by all the anchors, filtered and then used as input for its mathematical model of RSSI. This calibration process is repeated at several locations in the room preferably at different distances between anchors and transmitter.

Figure A.1 shows how the calibration mode is implemented in GNU Radio.

3.3.3 Running Mode

The system uses the principle of multilateration to estimate the position of a transmitter in the vicinity of three anchors placed at know locations. The anchors send their estimated RSSI to a host computer over Ethernet on a private network using a network switch. The RSSI measurements are collected by the host computer and are filtered through the Kalman filter and noise floor filter to suppress any unwanted spikes and to get rid of unrelated noise. The data is then compared to the previously generated log-distance path loss model to estimate the distance between the transmitter and each anchor. These distances are then used by the multilateration algorithm to estimate the position of the transmitter in the room. Once the position estimate is calculated the program will display the information onto a simple map of the exam room, so that the system's user may take appropriate action. Figure A.2 shows how the running mode is implemented in GNU Radio.

3.4 User Interface

The graphical user interface is the front end that allows a user to interact with the system. In the beginning, there was a need for a simple graphical interface that could visualise testing results. Using a simple Python library *graphic.py* [32], a simple program was created for testing purposes. The interface was fairly simple, yet it served its purpose well. However, later on, the Tkinter graphic library was used to create a better graphical user interface [33], because it provides a faster and easier way to create GUI applications. The Tkinter application would provide the ability for the user to choose between two different modes: calibration mode or running mode. The calibration mode gives users the ability to adjust the anchor's positions and manually enter the distances between the anchors and the transmitter to calibrate the system. The running modes include different buttons to control the program, such as starting, stopping and pausing the program. This mode also presents the graphical representation of the room and the positioned anchors in the room. To show the estimated distance between each anchor and the transmitter circles are drawn, centred on each respective anchor, with a radius equal to the

estimated distance.

3.5 Theoretical Cheater

An exam participant can cheat in numerous ways, ranging from some more traditional ways [34] to some more modern ways [35]. In the purpose description 1.2, it's explained that the goal is to perform signal detection to find cheaters. Our version of a cheater should consequently use some sort of wireless signals when cheating.

Several aspects need to be considered before creating the theoretical cheater. One aspect is the understanding of how wireless technology can be used to cheat in an exam is critical to determine how a potential cheater cheats. Another aspect is that the system must be able to detect the cheater reliably, for instance, if the cheater is only sending short messages then the system will have trouble detecting these.

Considering these points, we found that similar methods to those used by the cheaters in Trafikverket's driving test [1] are suitable. This means that the cheater will cheat by using a hidden camera that live-streams the test to an outside source. Then the outside party simply says what the cheater should answer through some hidden in-ear headphones. This method of cheating works well for this project since it uses a constant wireless video stream which the system can detect.

4

Results

This section contains a summary of the testing process. The collected data is processed, analysed and presented in different graphs throughout this section.

4.1 RSSI Attenuation Mathematical Modelling

A vital process of this project is to collect RSSI measurements and represent their attenuation in a mathematical model. It is impossible without a mathematical model to correctly estimate the distance between transmitter and anchors with the chosen location determination algorithm. RSSI attenuation modelling is done in the calibration mode of the system. To evaluate the radio signal path loss model, this test was carried out in a calm environment where interference was low and close to the ideal environment. An open field in Alingsås was chosen for this test. The test system was set up as followed:

- A tablet and a smartphone, both of brand Samsung, were used to simulate a transmitter and receiver. Wi-Fi hotspot was enabled on the phone to share an internet connection to the tablet over channel one of Wi-Fi 2.4 GHz. This channel covers a spectrum of 22 MHz from 2.401 GHz to 2.423 GHz.

- An anchor, ADALM-PLUTO SDR, is connected to a laptop. The software was configured to monitor Wi-Fi channel one and automatically collected RSSI measurement with the frequency of 20 Hz.

Continuous transmission between the tablet and the smartphone was achieved with a video call. To prevent the video call application from compressing the video, and thus sending fewer signals, a person next to the smartphone and tablet constantly waved across both the camera's view to achieve a constantly updating video feed. The two devices were placed next to each other at various distances from the anchor. In this test, the distance between the anchor and the senders stretched between one meter to nine eight meters with one meter in between different calibration points. A side note here is that this is the ideal setup to test RSSI attenuation modelling. Otherwise, the same distance between calibration points is not a requirement for calibration to work well. Nevertheless, outspread calibration points are desirable for better regression. The collected measurements are then filtered and presented in

figure 4.1.

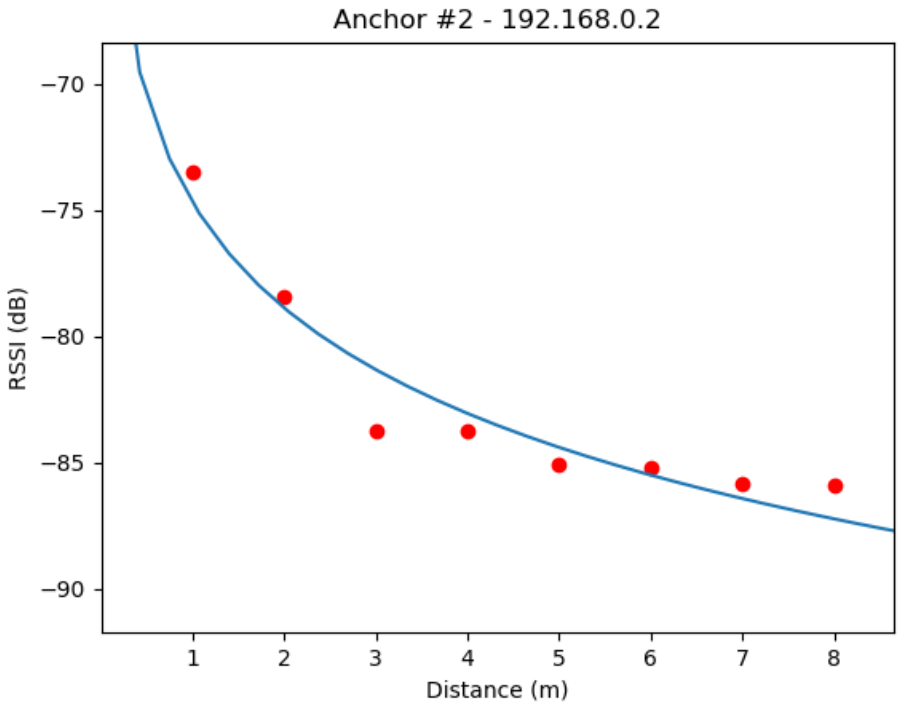

Figure 4.1: Relation between RSSI (dBm) and distance (m) captured by Anchor 2 in a calm environment. The red dots represent an RSSI measurement at a certain distance. The blue curve is the logarithmic function generated by fitting the log-distance path loss model to the data.

4.2 Field-test

A total of three field-tests were performed. The first one was a more primitive test of the system in the early stage of development with fewer calibration points and manual position estimation. The main goal of the first test was to test the functionality of the system. During the second and third test, the system was more or less completed with the exception of a GUI. We tested with even more calibration points and simulated cheater positions.

The first field test was a bit more basic with only 4 calibration points. We tested having the phones outside the exam room to see if we could determine whether the signals came from inside the room or not. And according to the RSSI values gathered we could determine that the source came from outside.

The second field-test was done with a more or less complete system except for the graphical user interface. Calibration and location detection was done through a command-line interface.

All the field-tests are conducted using the same setup of one host computer, Dell Latitude 7300 running Ubuntu 20.04, one Cisco switch and three ADALM-PLUTO devices. The network configuration of the system is shown in table 4.1.

Device	Name	IP-address	Position in the room
ADALM-PLUTO	Anchor 2	192.168.0.2	A
ADALM-PLUTO	Anchor 3	192.168.0.3	C
ADALM-PLUTO	Anchor 4	192.168.0.4	B
Computer (Ubuntu 20.04)	host	192.168.0.5	User's choice

Table 4.1: Table to test captions and labels

The functionality of the prototype was evaluated by testing in one of the smaller sized exam rooms, EA in EDIT-house at Johanneberg Campus. The dimensions of the chosen room are 10.75m x 7.3m as shown in figure 4.2. Three anchors were spread out and set up at positions A, B and C around the room, as seen in figure 4.2 to maximize coverage of the student-sitting area. In the sitting area of room EA, the back row seats are slightly higher elevated than the front row. This means that the anchor's C position is higher than A, and B is elevated higher than both C and A. A Wi-Fi hotspot was set up with a Samsung Galaxy S10 connected to its network. RSSI was measured in eight different spots in the room to calibrate the system. Three of these calibration points were placed one meter from each of the three anchors, one after the other, to collect essential base-RSSI measurements for the RSSI attenuation model of that anchor. The other calibrations points were chosen so that their distances from each anchor spread out between one and eight meters.

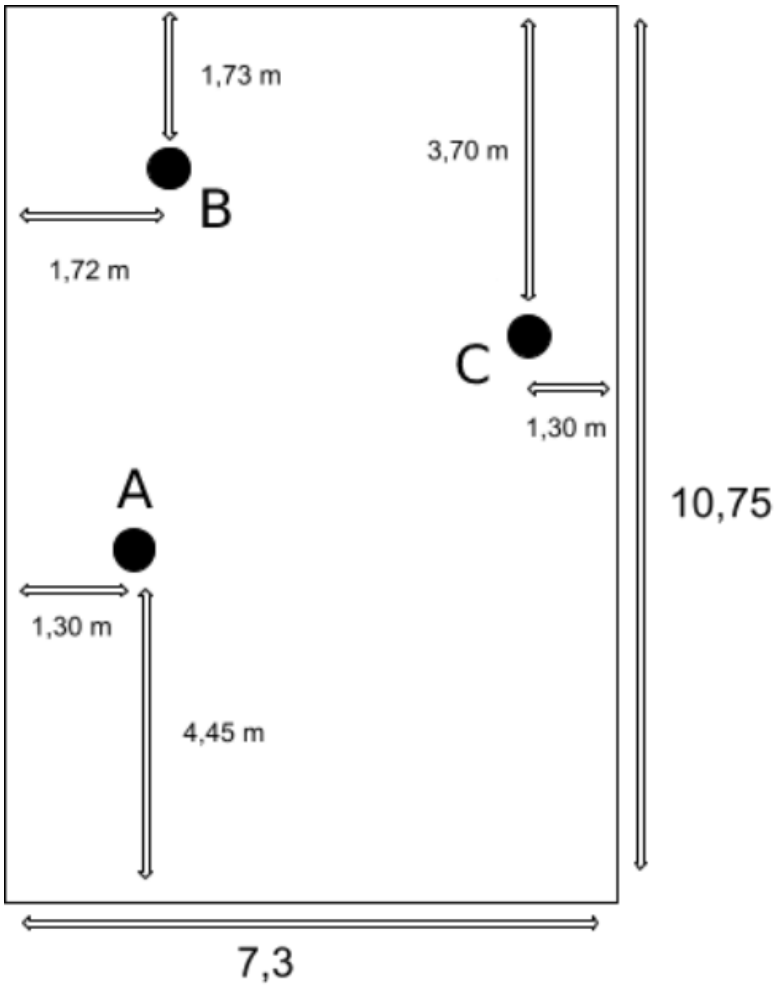

Figure 4.2: Layout of the exam room the test was performed in, and the anchor's positions A, B and C

Calibration of the system was then conducted as described in System calibration 3.3.2. The result was not as expected. Analysis of the collected data shows that a relationship between the RSSI measurements of the anchor at position A and distance exists. As shown in figure 4.3, a decreasing RSSI-distance function can be generated from the collected measurements according to the path loss model with some error margin.

Unfortunately, measured RSSI from the other two anchors at position B respective C do not show any relationship with distance. The graph in figure 4.4 shows RSSI measured of the anchor at position C from various distances. Based on observation, it does not appear to be any relationship between RSSI and distance. The same conclusion can even be drawn from measurements of the anchor at position B.

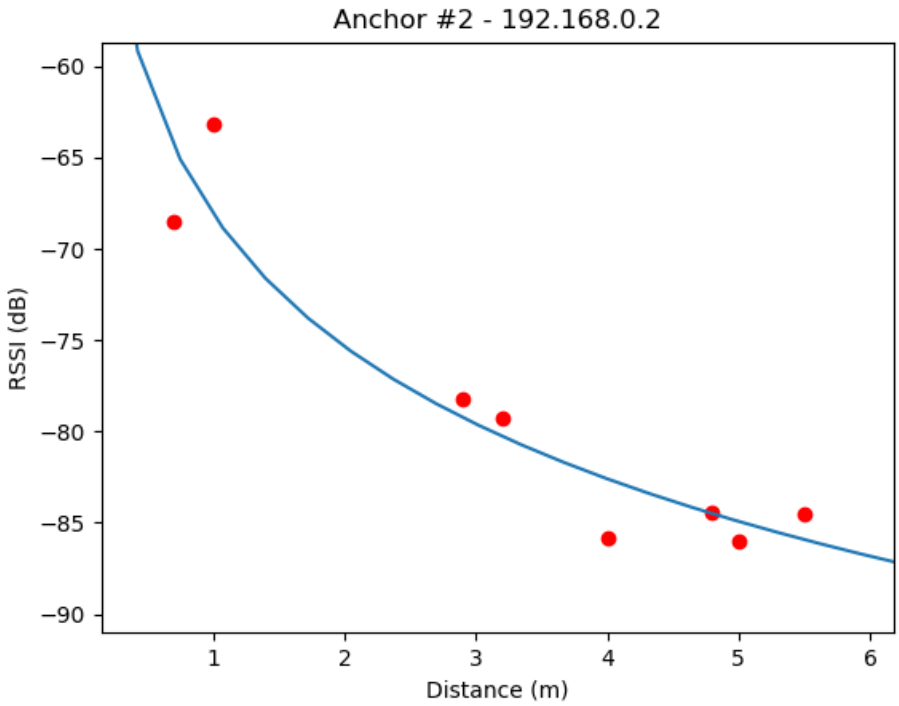

Figure 4.3: Relation between RSSI (dBm) and distance (m) captured by Anchor 2 in EA lecture hall. The red dots represent an RSSI measurement at a certain distance. The blue curve is the logarithmic function generated by fitting the log-distance path loss model to the data.

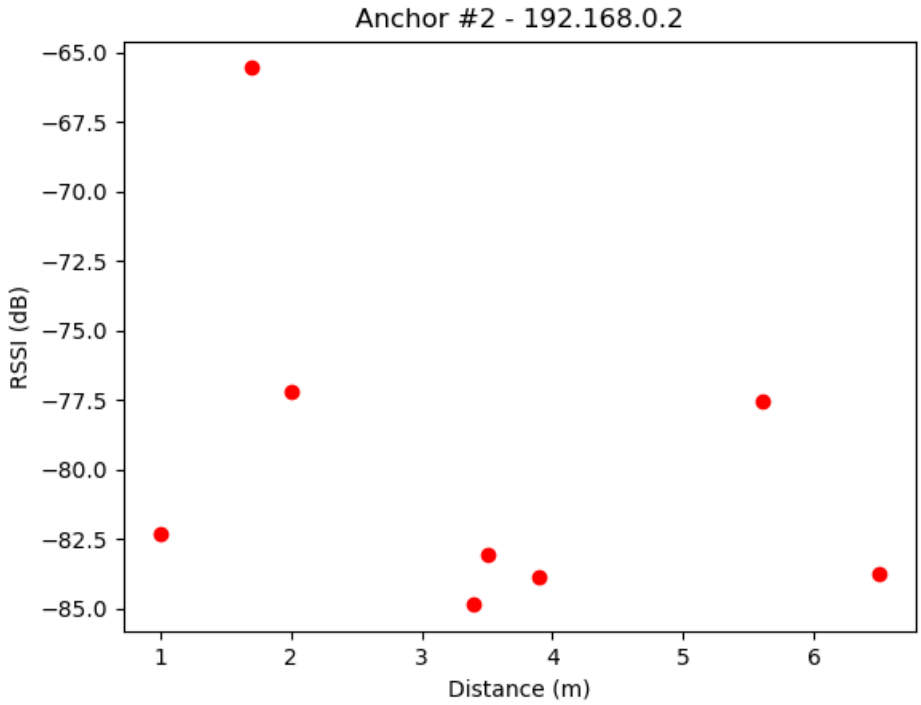

Figure 4.4: Relation between RSSI (dBm) and distance (m) captured by Anchor 2 in EA lecture hall. The red dots represent an RSSI measurement at a certain distance.

Another test, the third field-test, with the same settings as the second one was performed to ensure that the result from the second test result was not just an odd case rather than a systematical error. The result of that test was, to the most part, similar to the first test where the anchor at position A showed some relationship while the anchor at position B respective C did not yield a better result.

To better understand the cause of the randomness in RSSI measurements of the anchor at position B and C, the ADALM-PLUTO at positions A was swapped to position B and vice versa. A quick test where the two anchors simultaneously measured RSSI was performed. The collected data was not conclusive enough for any conclusion to be drawn, even though a big fluctuation in RSSI from anchor at position A could be observed.

Due to the unsuccessful calibration of the system and time constraints, we could not continue with the planned attempt to detect unauthorised transmitters.

5

Discussion

This chapter discusses the outcome of the project as well as some speculation over the reasons why the system did not perform as well as we would have hoped. We will touch on where the process of developing the project worked, where it failed, what went better than expected and what caused unforeseen delays. Motivations for the choice of the hardware, software, and algorithms are also discussed below. Finally, we talk about some potential future work and improvements to the system.

5.1 Test result analysis

Based on the test result presented in section 4, there are some observations and conclusions worth discussing.

The first field-test yielded a good result. However, the good results could not be replicated in later tests. This could depend on the fact that the system was calibrated with only 4 points and we believe that it is too few points and not good enough for a valid calibration. The good result we got from the first field-test could be from pure luck and not because of the systems ability to locate the signal source. Therefore this test can not validate the functionality of the whole system.

A quick observation of the graph in figure 4.1 shows that the transmitted signal loses its strength over distance, hence the attenuation increases with distance. The path loss model is fitted nicely to the collected data and generates an acceptable curve with some error margin. At the distance of 3 meters and 6 meters from the transmitter, the observed measurements drift a little bit longer from the curve compared to measurements at other points, but this could be explained by the instability of RSSI.

In the first four meters, the signal strength drops from around -70 dBm to -83 dBm, which eventually results in a smaller error margin in distance calculation as RSSI fluctuates. It is more troublesome to estimate distance if the RSSI measurements fall between -83 dBm to -87.5 dBm. According to the curve in figure 4.1, the estimated distance would be between 4 meters to 8 meters. Distance estimation in this range has a much bigger error margin since the estimated RSSI fluctuations are much smaller, -4.5 dBm, compared to -13 dBm for the distance between 0 meter

and 4 meters. For example, RSSI is measured at around -86 dBm with little to no difference for all four distances 5 meters, 6 meters, 7 meters and 8 meters from the transmitter and this means an error margin at around 3 meters. Considering the accuracy of the measuring instruments, which in this case is the ADALM-PLUTO SDR devices, a reasonable estimation of distance by RSSI leaves much to be desired.

The test result from the many field-tests that were conducted at Campus Johanneberg, shows that the system is not tolerant to noise despite implemented countermeasures such as a noise floor filter and Kalman filter. RSSI varies more randomly in a noisy environment, which can be observed from figure 4.3. RSSI measurements in 4.3 deviate from the curve more compared to the graph in figure 4.1.

The randomness of RSSI measurements in figure 4.4 could be the result of malfunctioning measuring instruments or a bug in the system software. Despite some attempts to understand and resolve the issue, it still remains. What should have been done differently is to test each ADALM-PLUTO individually instead of assuming that all the ADALM-PLUTO devices works similarly to the tested one.

5.2 Hardware

The hardware turned out to be one of the larger obstacles for this project. Even though we had anticipated some difficulty in getting the grips on the hardware. We initially believed that this would be something we could overcome in the early stages of the project and then be able to fully focus on the software and algorithm aspects of the system. This assumption was however only partly correct. Many of the early problems we had with the ADALM-PLUTO devices were issues relating to connecting them to the host computers and getting them to properly communicate with GNU Radio. Since two of the three devices were previously used in other projects, their settings had been changed and deviated from the factory settings. These settings altered certain attributes central to establishing a link with the host computer, such as the IP address of the device for example. After accessing and configuring these settings, we were successful in connecting several ADALM-PLUTO devices to a host computer through GNU Radio.

In the testing phase, we discovered that the two older ADALM-PLUTO devices were reporting significantly worse readings relative to the newly purchased device. This has caused unreliability in our tests since the two older devices did not receive sufficiently different RSSI measurements when moving the transmitting devices to different distances away from the devices. Because of this, the system could not produce an accurate mapping of RSSI and distance, which negatively affects the accuracy when RSSI readings later used by the system for locating transmitters. The reason for this is not clear to us, but we have a couple of theories as to why this happened.

The devices could have had some setting altered by previous users that we were not aware of and could not find. This is quite likely since we already know there

were some settings relating to IP addresses that had been changed by a previous group [36]. While testing, we also discovered a setting for automatic gain control that would render our readings useless for our purposes. This is because the gain directly affects the RSSI reading, and a fluctuating gain would be indistinguishable from a change in RSSI to our system. Fortunately, this was discovered early in the testing phase before the system was assembled for a full-scale test. The gain was set to manual and adjusted to be the same for all three devices for all future tests.

The antennas that came with the older devices could be different from the antenna of the newer device. These antennas were included with the ADALM-PLUTO when purchasing and were of the type we intended to use for the project, thus we saw no reason to purchase any additional or different antennas. It is possible the new antennas are tuned to a different frequency than the older antennas, or that the gain characteristics are different. We do not however believe that the antennas are causing these issues since the problems encountered were not consistent between tests.

A bug in the software controlling the receivers could also be to blame. If for example, the code controlling the frequency tuning of the ADALM-PLUTO fails this could cause the receivers to be out of tune with the frequencies being transmitted by the test transmitters.

5.3 Software

The software was developed almost exclusively in Python since it is an excellent language for prototyping. GNU Radio is built in Python which enables us to integrate our own python code with relative ease. The problems of developing the software mostly stemmed from not being comfortable with the structure of GNU Radio. Some aspects such as the flow of data caused a lot of delays when developing several parts of the software. This caused us to have to spend many hours debugging our software so that it would work with GNU Radio. On top of this, GNU Radio attempts to validate any custom python code that is written in python blocks, when these blocks are being saved. This behaviour was very unreliable since it would only validate some of the time and there were no clear indications of when the last attempted validation was made, making it unclear if the current code was free of syntax errors. This validation also attempted to run the code in the process of validating it, causing major issues when attempting to integrate a custom GUI into these python blocks, since the GUI would launch with every validation. If the GUI was not implemented properly the GUI would get stuck open, and the only way we found to exit out of it and regain control over GNU Radio was to terminate and reboot the entire program. These two factors, along with our unfamiliarity with GNU Radio made the development process for the software slow and caused us to have to revise the design many times to facilitate easier development.

Additionally, GNU Radio is not immediately compatible with the ADALM-PLUTO hardware. This means that we had to spend some time installing some extensions

to GNU Radio before we could get started with the hardware. This was however only a problem in the very beginning and once it was solved the issue did not hinder the work anymore. It is worth noting however that this forced us to use a specific version of GNU Radio, causing us to be unable to use some features added in newer versions.

The GUI was never finished due to our choice of prioritising our resources on debugging the calibration feature of the system. This was a great setback for the development and made it more difficult to test other parts of the system.

5.4 Algorithm

The algorithm was the major deciding factor in the project. It dictates what hardware needed to be acquired and thus was an important part of the early work. A large amount of time was spent on researching different localisation algorithms since the project could not proceed in a meaningful manner until we had chosen one to focus on. A large part of the difficulty in choosing the algorithm came down to comparing accuracy and features, versus ease of use and ease of implementation. Some algorithms were better suited to long-range implementations, and some required specialised hardware that would be difficult to acquire in a timely manner and difficult to use efficiently since these often targeted experienced radio users. Considering the time constrain of the project, the choice of algorithm is justified.

5.5 Sources of Error

The system has a few aspects that could impact the reliability and accuracy of the results. Most notable is the fact that the location estimation depends on only a single variable, the RSSI value at the receivers. RSSI is also affected by other factors than the distance from the transmitter, such as the propagation of the wave which is also affected by the room's temperature and humidity. Therefore, the RSSI values must be taken with a grain of salt. It is possible that a signal emanating from outside the exam room and travelling through a wall or the ceiling may appear similar in strength to a signal on the far side of a room for a single receiver. This is not a problem in an ideal scenario where there is only a single transmitter in range of the system. In a more realistic scenario, where there might be several transmitters in and around the exam room this could ruin the location estimation. Even when only considering transmitters within the room, the system is only capable to handle a single transmitter. Multiple transmitters at different locations will cause the system to give an incorrect estimate.

Another major possible source of error is the issue of multipath and line-of-sight propagation. The geometry and furnishing of the room may cause the signal to not follow the log-distance path loss model. This is very hard to detect and correct, since the propagation of the signal can be very complex, especially when the exam room is occupied by people. Line-of-sight propagation is a problem since a transmitter

in the pocket of a potential cheater may have line-of-sight to one receiver while being occluded by the body of the person when viewed from another receiver. This can cause the RSSI to be lower for the occluded receiver than for the receiver with line-of-sight, independent of distance. This would also cause the location estimation algorithm to produce a faulty result.

5.6 Test method and facility

All testing of the system in the final stage of development was done thoroughly as if it was a real deployment and using of the system. By doing it this way, the system's functionality and capability were fairly evaluated.

The system was tested in a lecture hall, which is fully capable of hosting an exam. The chosen lecture hall is an open-space room that is smaller than the space that the system could have covered if it had worked properly. This is fine for early testing of the system. But it would have been even better to stress-test a functional system in a bigger facility to gain knowledge about the system specification such as coverage and limitation.

The location of the testing facility is in a multiple-stories building with a lot of Wi-Fi access points and transmitting devices nearby. Even though a real exam location was realistically simulated, it would have been better to first develop and test the system in an ideal environment. An ideal environment for this project is an environment with low wireless activity and therefore less noise, which is an important consideration when developing a wireless system. Testing in this environment would review problems such as hardware's instability and it would be easier to evaluate the plausibility of the solution.

5.7 Future Work

Since cheaters can use technologies like 5GHz Wi-Fi, Bluetooth, 4G, et cetera, the next step in development would be expanding the system to incorporate more frequencies than the 2.4 GHz Wi-Fi that already exists.

The unfinished GUI is something that in the first place could be completed, but also be expanded upon. There is potential in exploring how a proctor could use a tool similar to the system in practice, and more features could be added to help their work. For example a timeline of all detected signals in the room during the exam, or an easier calibration process that could allow the user to drag and drop where the antennas are and change the room size with the help of their mouse.

To develop the system further, isolating the different factors that could impact the performance of the system could be a good idea. For instance, changing the antennas to see if it improves or impairs the ability of the system. Going through the different components of the system and testing variations could highlight what works and what needs further development.

One alternative to detecting cheaters is using an international mobile subscriber identity-catcher (IMSI-catcher), which could be used to intercept the phones in an exam room to perform a man-in-the-middle attack. This means that the IMSI-catcher could gain access to the data being transmitted from the exam room and thus determine who is cheating. However, in Sweden, this technology is currently only allowed as an extreme measure by the Swedish police or Swedish Armed Forces [37].

Another alternative that could help against cheating is to decode Wi-Fi headers, this means that depending on the Wi-Fi protocol it is possible to decrypt some metadata in the Wi-Fi header [38]. Through this, the system can see what the MAC address is connected to the Wi-Fi, and by using the MAC address it should be possible to determine what Wi-Fi packet is coming from what device.

An alternative way of preventing cheating through the use of wireless technology is by using a mobile phone jammer. By transmitting noise on the same frequency that a phone uses it is possible to prevent the phone from communicating at all in that frequency. However, this is highly illegal in Sweden and it has the potential to be dangerous since for example if someone wanted to call emergency services they would not be able to since the call would be jammed [39].

One altogether different approach to the cheating problem is to explore the area through a more psychological or humanities-oriented focus on why cheating happens. Researching if cheating is a symptom of a bigger underlying problem in exams or education [40] and if it is preventable by changing how exams are conducted could be relevant.

6

Conclusion

The original goal of this project is to explore the possibility of detecting and locating an unauthorised wireless transmitter in an indoor environment, as a foundation for building a cheat detection system. Due to time constraint, this project is set to only exploring wireless communication of a single transmitter over Wi-Fi 2.4 GHz. Up to this point in time, a prototype of the system was constructed, deployed and tested. Based on the result, the prototype can not consistently locate the signal source. But it is fully capable of detecting if there is an active transmitting device nearby.

The prototype consists of three ADALM-PLUTO SDR devices, a network switch and a host computer. The three ADALM-PLUTO devices act as three anchors and are placed around the target facility. These anchors, when at work, constantly sweep through three of the most popular Wi-Fi 2.4 GHz channels 1, 6 and 11 to collect the signal strength of the incoming signals if there is any. These RSSI measurements are then sent to the host computer through an Ethernet cable. The network switch handles the communication between three anchors and the host computer. At the host computer, collected RSSI measurements are filtered by a floor noise filter to separate the RSSI measurements of interest from the noise-contaminated ones. A Kalman filter is then used to counter the random fluctuation tendency of RSSI. If there is a device actively transmitting a signal, the three anchors will pick up the jump in RSSI measurement. By doing it this way, a nearby transmitting device can be detected.

The location detection feature of the system is completely implemented but does not work as intended. In theory, a radio signal is subjected to path loss, which means the signal loses its strength over distance. A Log-distance path loss model is used in this project for mapping RSSI measurements, which can be used to estimate the distance between a transmitter and an anchor. By using the multilateration algorithm, an estimated location of the unauthorised transmitter could be calculated. However, to locate the signal source, a more accurate measurement of RSSI is required and this could not be done with our implementation. So location detection feature is left for further development.

For future development, a better software-defined radio could be used to increase the accuracy of RSSI measurements and thus improve the location detection ability of the prototype. The prototype is capable of covering the Wi-Fi 5 GHz spectrum in

theory but this feature has never been implemented or tested by us. Small software tweaks and testing would extend and confirm the capability and functionality of the prototype on the 5 GHz Wi-Fi bands.

Finally, we believe that if the system is further developed, there is an enormous potential benefit for both the students and educational institutions, to increase the fairness of exams. There are also a lot of interested parties that could take advantage of such a product.

Bibliography

[1] TT, *Körkort tas med fusk, mutor och svarta pengar*, sv, Section: nyheter, Mar. 2021. [Online]. Available: https://www.aftonbladet.se/a/OQzkkE (visited on 04/08/2021).

[2] Urkund, *Urkund's anti-plagiarism system*, en, 2020. [Online]. Available: https://www.urkund.com/the-urkund-system/ (visited on 02/02/2021).

[3] Hervé Sizun, *Radio Wave Propagation for Telecommunication Applications*, ser. Signals and Communication Technology. Springer, 2005, ISBN: 978-3-540-40758-4.

[4] *Brottsbalk*, SFS 1962:700, Justitiedepartementet Stockholm, Sverige: Regeringskansliet, Dec. 1962 [Online] Availible: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700.

[5] IEEE Xplore, *IEEE Xplore*. [Online]. Available: https://ieeexplore.ieee.org/ (visited on 05/13/2021).

[6] UHR, *Fusk på högskoleprovet*, sv, Feb. 2020. [Online]. Available: https://www.studera.nu/hogskoleprov/infor-hogskoleprovet/fusk-hogskoleprovet/ (visited on 02/09/2021).

[7] Joseph Cox, *Here's How Easy It Is to Make Your Own IMSI-Catcher*, en, Nov. 2018. [Online]. Available: https://www.vice.com/en/article/gy7qm9/how-i-made-imsi-catcher-cheap-amazon-github (visited on 02/08/2021).

[8] *Regulation (eu) 2016/679 of the european parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)*, EUT L 119. [Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 (visited on 02/08/2021).

[9] Mathuranathan, *Log Distance Path Loss or Log Normal Shadowing Model*, Sep. 2013. [Online]. Available: https://www.gaussianwaves.com/2013/09/log-distance-path-loss-or-log-normal-shadowing-model/ (visited on 03/10/2021).

[10] M. Reckeweg and C. Rohner, "Antenna Basics White Paper," *Rohde Schwarz*, 2015.

[11] Analog Devices, *GSM Antenna JCG401*. [Online]. Available: https://wiki.analog.com/_media/university/tools/pluto/users/jcg401.pdf (visited on 05/14/2021).

[12] Electronics Notes, *WiFi Standards: IEEE 802.11*. [Online]. Available: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/standards.php (visited on 05/14/2021).

[13] ——, *Wi-Fi Channels, Frequencies, Bands & Bandwidths*, 2021. [Online]. Available: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php (visited on 05/14/2021).

[14] MetaGeek, *Adjacent and Co-Channel Interference*. [Online]. Available: https://www.metageek.com/training/resources/adjacent-channel-congestion.html (visited on 06/03/2021).

[15] Electronics Notes, *What is Noise Floor for radio receivers*. [Online]. Available: https://www.electronics-notes.com/articles/radio/radio-receiver-sensitivity/what-is-noise-floor.php (visited on 05/14/2021).

[16] Khan Academy, *Diffraction and constructive and destructive interference*. [Online]. Available: https://www.khanacademy.org/test-prep/mcat/physical-processes/light-and-electromagnetic-radiation-questions/a/diffraction-and-constructive-and-destructive-interference (visited on 04/29/2021).

[17] G. Welch, *The Kalman Filter*, Jul. 2016. [Online]. Available: https://www.cs.unc.edu/~welch/kalman/.

[18] W. Bulten, *Kalman filters explained: Removing noise from RSSI signals*, Oct. 2015. [Online]. Available: https://www.wouterbulten.nl/blog/tech/kalman-filters-explained-removing-noise-from-rssi-signals/ (visited on 04/29/2021).

[19] S. Xia, Y. Liu, G. Yuan, M. Zhu, and Z. Wang, "Indoor Fingerprint Positioning Based on Wi-Fi: An Overview," en, *ISPRS International Journal of Geo-Information*, vol. 6, no. 5, p. 135, May 2017. DOI: 10.3390/ijgi6050135. [Online]. Available: https://www.mdpi.com/2220-9964/6/5/135 (visited on 05/13/2021).

[20] D. Plets, W. Joseph, K. Vanhecke, E. Tanghe, and L. Martens, "Coverage prediction and optimization algorithms for indoor environments," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 123, Mar. 2012, ISSN: 1687-1499. DOI: 10.1186/1687-1499-2012-123. [Online]. Available: https://doi.org/10.1186/1687-1499-2012-123 (visited on 04/29/2021).

[21] Y. Li, Y. Zhuang, X. Hu, Z. Gao, J. Hu, L. Chen, Z. He, L. Pei, K. Chen, M. Wang, X. Niu, R. Chen, J. Thompson, F. M. Ghannouchi, and N. El-Sheimy, "Toward Location-Enabled IoT (LE-IoT): IoT Positioning Techniques, Error Sources, and Error Mitigation," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4035–4062, Mar. 2021, ISSN: 2327-4662. DOI: 10.1109/JIOT.2020.3019199.

[22] A. S. Yaro, S. Salisu, A. Umar, and M. J. Musa, "Multiangulation position estimation performance analysis using a Bartlett's Beamforming Method," en, *Nigerian Journal of Technology*, vol. 36, no. 4, pp. 1155–1161, 2017, ISSN: 2467-8821. DOI: 10.4314/njt.v36i4.23. [Online]. Available: https://www.ajol.info/index.php/njt/article/view/164977 (visited on 04/29/2021).

[23] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AOA," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, ISSN: 0743-166X, vol. 3, Mar. 2003, 1734–1743 vol.3. DOI: 10.1109/INFCOM.2003.1209196.

[24] GREAT SCOTT GADGETS, *Great Scott Gadgets - HackRF One*. [Online]. Available: https://greatscottgadgets.com/hackrf/one/ (visited on 05/14/2021).

[25] Analog Devices, *ADALM-PLUTO Overview*, Jan. 2021. [Online]. Available: https://wiki.analog.com/university/tools/pluto (visited on 04/29/2021).

[26] ——, *ADALM-PLUTO Antennas*, Feb. 2021. [Online]. Available: https://wiki.analog.com/university/tools/pluto/users/antennas (visited on 05/14/2021).

[27] Python, *Python Release Python 3.8.3*, May 2020. [Online]. Available: https://www.python.org/downloads/release/python-383/ (visited on 05/14/2021).

[28] Lance Whitney, *Why Python is considered the top programming language ahead of JavaScript and C++*, Oct. 2019. [Online]. Available: https://www.techrepublic.com/article/why-python-is-considered-the-top-programming-language-ahead-of-javascript-and-c/ (visited on 04/29/2021).

[29] *GNU Radio*, en, Page Version ID: 1014905974, Mar. 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=GNU_Radio&oldid=1014905974 (visited on 04/29/2021).

[30] GNU Radio, *GNU Radio - The Free & Open Source Radio Ecosystem*. [Online]. Available: https://www.gnuradio.org/ (visited on 04/29/2021).

[31] GNU Radio Wiki, *Main Page*. [Online]. Available: https://wiki.gnuradio.org/index.php/Main_Page (visited on 04/29/2021).

[32] John M. Zelle, *Python Programming: An Introduction to Computer Science*. [Online]. Available: https://mcsp.wartburg.edu/zelle/python/ (visited on 05/13/2021).

[33] Python, *Tkinter — Python interface to Tcl/Tk*. [Online]. Available: https://docs.python.org/3/library/tkinter.html (visited on 05/13/2021).

[34] P. C. Shon, *How college students cheat on in-class examinations: Creativity, strain, and techniques of innovation*. Ann Arbor, MI: MPublishing, University of Michigan Library, 2006.

[35] L. Z. Bain, "How students use technology to cheat and what faculty can do about it," *Information Systems Education Journal*, vol. 13, no. 5, p. 92, 2015.

[36] J. Binde, E. Frennborn, L. Glimfjord, G. Henriksson, D. Nguyen, and J. T. Pedersen, "Ett prototypsystem för detektion och lokalisering av fusk under tentamina genom signalspaning av WiFi-frekvenser," Department of Computer Science and Engineering, Tech. Rep., 2020.

[37] Riksdagsförvaltningen, *Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet Svensk författningssamling 2008:2008:717 t.o.m. SFS 2018:1918 - Riksdagen*, sv, Last Modified: 2014-12-12 15:00:54. [Online]. Available: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717.

[38] IEEE, "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, Dec. 2016. DOI: 10.1109/IEEESTD.2016.7786995.

[39] Post- och telestyrelsen, *Förbud mot störsändare | PTS*, sv, Oct. 2016. [Online]. Available: Pts.se (visited on 05/13/2021).

[40] D. Lederman, *Best Way to Stop Cheating in Online Courses? 'Teach Better'*, en, Jul. 2020. [Online]. Available: https://www.insidehighered.com/digital-learning/article/2020/07/22/technology-best-way-stop-online-cheating-no-experts-say-better (visited on 02/08/2021).

A

Appendix 1

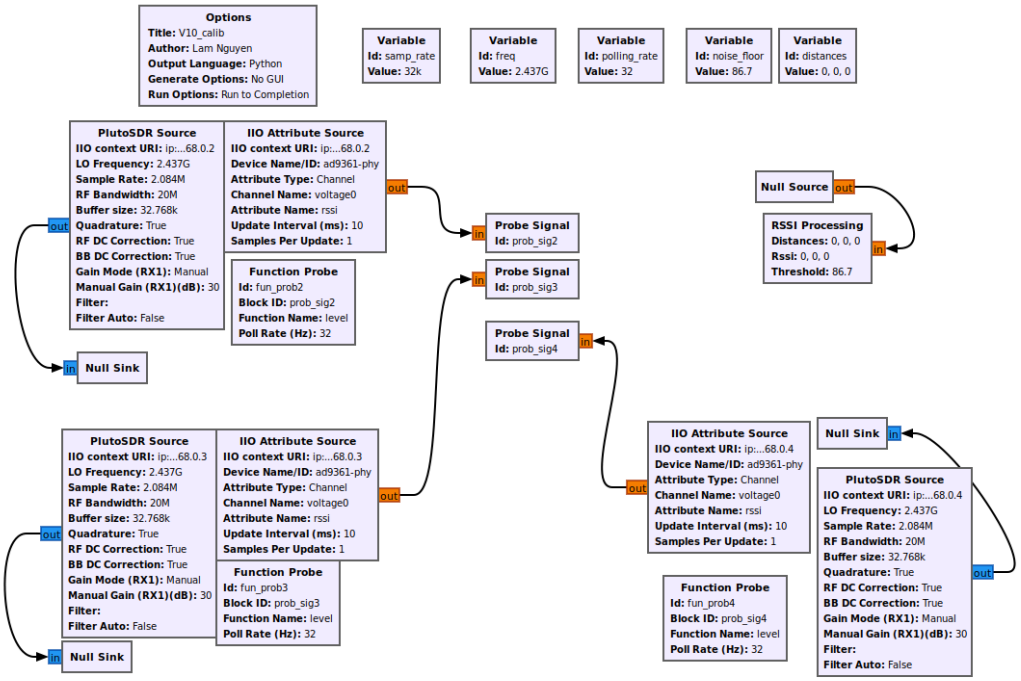

Figure A.1: Flowchart of the calibration mode in GNU Radio.

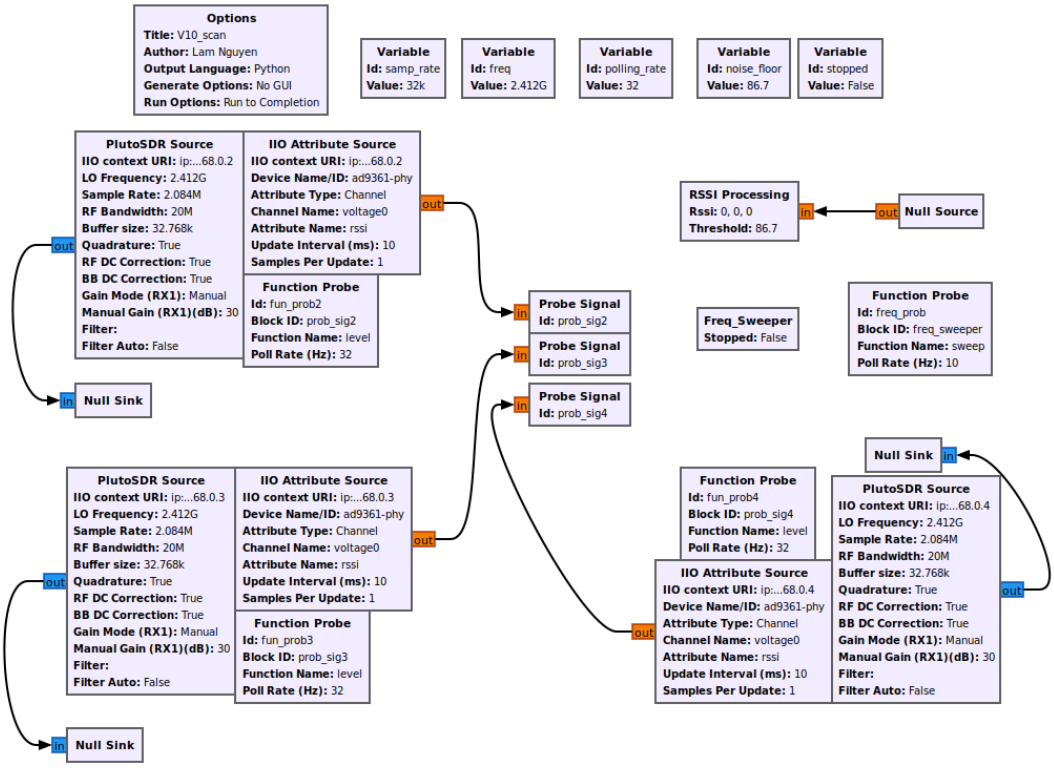

Figure A.2: Flowchart of the running mode in GNU Radio.