Multi-Factor Mobile based Access Control Solution

August Larsson
dat15ala@student.lu.se
Alvin Ohlsson
dat15aoh@student.lu.se

Department of Electrical and Information Technology
Lund University

Supervisor: Maria Kihl
Axis Supervisor: Johan Adolfsson

Examiner: Christian Nyberg

July 8, 2020

Printed in Sweden
Tryckeriet i E-huset, Lund

Abstract

In this thesis, alternatives for replacing an RFID card + PIN based access control solution for office buildings with a mobile applications are evaluated. The proposed solutions are based on a probabilistic fingerprinting approach where distributions of RSSI are approximated and stored in a fingerprint database during an initial offline phase. Unlike traditional fingerprinting applications, the solution utilize the fact that only position relative to the different doors is required by solely creating fingerprints at each doors position as opposed to in a grid of the building. In the following online phase, Maximum Likelihood Classification is applied to find the best match between a users RSSI and objects in the database, granting access to the respective door.

Alterations are made to the original solution to counteract a) restrictions imposed on the Android API which slow down Wi-Fi RSSI scanning and b) decreased accuracy with too many doors densely placed. The alternate Wi-Fi solution uses the previously received RSSI sample to create a coarser estimation of location, allowing the user to choose between the three closest doors for instant authentication. For improved accuracy with tightly grouped doors, a geomagnetism based solution is used that use fingerprints similar to the Wi-Fi solution, but that are not subjects to spacial variations in the same manner.

Additionally, behaviour of Wi-Fi signals in an indoor office environment is measured in terms of spatial variations and line of sight obstruction. In turn, different AP setups and how they affect localization performance are evaluated, along with improvements made to the RSSI sampling process to account for human obstruction of AP line of sight during use.

Finally, results from testing in a dedicated test environment show that all of the solutions can be suitable for real use in different scenarios. The thesis provides concrete conclusions of how each solution can be applicable for different use cases, or improved upon further with other hardware or technologies.

Popular Science Summary

The most common way of providing access control to buildings is the combination of an RFID card and a PIN code. However, carrying around a card and briefly interacting with the door unit is not very convenient for the frequent user. This work has produced several mobile solution alternatives that, using Wi-Fi and the earths geomagnetic field, determines user proximity to the doors to grant or deny access.

Since many companies employ an RFID + PIN based solution as a safety measure, it is reasonable to assume that many would desire a more convenient option, provided that safety aspects are not compromised. As most individuals carry a mobile phone with them daily, a logical approach is to move the functionality to a mobile application. Assuming that the application is only distributed to authorized users, similar to the RFID card, the remaining challenge can be equated with detecting which door such a user is located at when desiring access.

This thesis has resulted in three variations of a mobile application aimed at this task, that are applicable in different scenarios. The initial solution uses the common indoor localization algorithm of Wi-Fi fingerprinting, where a database of different locations is built by sampling Wi-Fi signal strength at the doors locations. Locating the user is then a simple problem of matching the measurements received live with the database ones, the closes match is the closest door to the user. The accuracy is adequate but restrictions in Android makes it slow and inconvenient to use in practice since the user has to wait too long for the Wi-Fi scan results.

To provide a faster solution, an alteration was made to instead show the three closest doors, allowing the user to open a door by pressing the corresponding button on the application. The reasoning behind this is that the system now can use the previous scan, which still provides sufficient accuracy for having the correct door among the top 3. The accuracy is more than sufficient for localization as long as doors are not placed too densely.

For use cases where many doors are required to be placed within close proximity of each other, the last solution combines Wi-Fi positioning with a geomagnetic

component. Modern mobile phones are equipped with inertial sensors that can sense the geomagnetic field intensity. Since the magnetic field is incredibly stable within a set position, it is perfect for labeling different positions similar to Wi-Fi by building up a database. The accuracy with this solution is excellent but the main problem is that it is difficult to produce enough unique fingerprints for an entire building. The solution was then to combine with the Wi-Fi solution to let the Wi-Fi determine a rough estimation of the position while the geomagnetism determines the finer position in this general area.

Table of Contents

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Background

As the world is becoming more security aware there is an increased demand on secure solutions for authentication and authorization, both from a purely network based perspective but also from a physical perspective. A common way of addressing the issue today is by using an RFID card + PIN combination. This solution might not always be the most convenient, as you always must carry your card with you and carry out a brief interaction with the unit. An alternative is to use your mobile phone, which you most likely already always have in your pocket. A modern mobile phone contains many different technologies and sensors such as NFC, BLE, Wi-Fi, Location, etc., and many buildings have smart readers on their doors that could communicate with said mobile technologies. As the basis for this project, mobile based applications, where emphasis is put on higher ease of use rather than improved security, will be evaluated. Using the RFID + PIN solution as comparison, the mobile based solution should provide quicker and more convenient access without compromising the security aspect.

Multi-factor authentication is an authentication process which combines several authentication factors to make the system more secure than just using a single factor. One factor being compromised will not give an intruder access to the system but rather all factors must be present. There are four factors that are the most common [16]:

- What the user knows - passwords,pin code etc.
- What the user has - smart cards, smartphone etc.
- What the user is - face, voice, fingerprint etc.
- Where the user is - GPS, IP address etc.

C. Wang et al. [17] argues that including more factors - while making the system more secure - can also make the system too complicated or tedious to use. The example of taking a front photo for face ID, pressing a thumb for fingerprint and enter a password each time you wish to unlock your phone makes the statement clear. The system might be secure but the efforts are too cumbersome for a regular user that interacts frequently with the system. A. Dmitrienko et al.[6] brings

up how mobile two-factor authentication solutions - which require no additional hardware such as smartcards - are a good trade-off between security, usability and cost. This thesis - similar to C. Wang et al. - aims to combine several factors in a way that is organic and does not take unnecessary effort from the user, while also not introducing additional hardware.

1.1.1 Problem Definition

Based on the classic authentication factor categories object-based, knowledge-based, biometrics-based and location-based, the aim of this project is to combine several authentication factors to scale down the user effort required as far as possible while remaining within acceptable levels of security. As a constraint of this project, no emphasis is put on security aspects beyond ensuring that the new solutions are comparable to the original solution in terms of number and quality of authentication factors.

The problem of improving the solution in terms of effort required can be split into two parts:

• Providing a faster way of identifying which door is to be opened and that the user is in its vicinity, thus limiting the manual interaction with the door or attached readers.

• Automatically or more rapidly identifying that the user is authorized to enter the door, reducing the need of interaction with the application (e.g. password input/fingerprint scanning).

In practice, the first issue is equivalent to providing a way of localizing the phone relative to the doors, or in other ways sensing its vicinity.

1.1.2 Related Work

In this section, studies that have addressed problems similar to this thesis are presented. Furthermore, papers that address either of the aforementioned sub problems are discussed.

In related projects, solutions typically included few but technical authentication factors to either achieve high security at the cost of convenience, or low to no effort solutions with lacking evidence of security. Additionally, many of the solutions only aim to authenticate the user to a single client (e.g. a computer), while this project involves the extra step of identifying which door is being requested access to.

Mobile Authentication Solutions

SoundAuth is a solution that utilizes ambient sound to authenticate users with minimal effort [3]. SoundAuth can reliably detect whether two devices are co-located and uses this as the second authentication factor that requires zero effort. However, this thesis aims to authenticate towards several doors that can all be in

the same macro location. Separating these with sound would prove difficult and counter-intuitive.

ZEMFA is another solution that uses both a smartwatch and a smartphone to capture the mid/lower body's and the wrist/arm's so-called gait patterns in order to authenticate users. [4] This allows the system to authenticate users with zero effort from the user. However, additional hardware in terms of a smartwatch is needed.

Sound-Proximity uses RF (radio frequency) signals to communicate and authenticate with a challenge-response protocol when you are in close proximity to your car. It is an improvement to the Keyless-go system innovated by Mercedes-Benz in the 90s and it allows the user to reduce needed interaction with the car. [5] A system like this could be utilized with a car being the door station and the key being your phone. The problem that needs addressing is that for the car system there is one key for one car but to be able to open all doors in a building, the key must work on all doors.

OWC (Optical Wireless Communication) is a complementary or alternative to the radio frequency communication, like RFID for example. It can be divided into four categories: free space optical (FSO) communications, visible light communications (VLC), light-fidelity (Li-Fi), and optical camera communications (OCC). [14]

VLC (Visual Light Communication) is a technique where the fast switching possible with LED lights are being utilized for wireless communication. L. Fan et al [11] use this technology for a mobile access control solution by modulating the LED signal coming from a smartphone's flash light. However, VLC has the requirement of having a photodiode receiver which is also true for FSO and Li-Fi.
The most interesting OWC technology for this thesis - since it does not require additional hardware - is OCC which is compatible with regular cameras. [14] OCC can be used similar to VLC with fast light switching to avoid flickering but commercial cameras with 25-50 fps are only suitable for video recording. This can be solved by modulating the signal the receiver side. [15] This would allow for wireless communication with the door-station and reduce interaction. For example, each user could have a unique flash sequence to identify themselves with.

UWB (Ultra-wideband) is a technology that provides higher positioning precision than Wi-Fi (down to 10cm), however it requires additional hardware. [44]. Additionally, most smartphones do not support UWB. It was however added into iPhone 11 [45], which might be a sign of what is to come. UWB is based on sending short pulses which operate over several frequencies simultaneously. This makes UWB less impacted by other radio frequency interference and the short pulses make it easy to filter out multipath effects. Additionally, UWB does not suffer from line-of-sight problems and can easily penetrate walls, equipment and clothing. [46]

Wi-Fi Based Solutions

The RSSI (Received Signal Strength Indication) of different Wi-Fi access points can be utilized together with different localization techniques in order to estimate the position of Wi-Fi enabled devices such as smartphones.[1][2] In [1], the common localization techniques of trilateration and fingerprinting are compared in terms of accuracy, computational complexity and resource limitations. Additionally, the experiments investigate the optimal number of access points, and achieve optimal results when using the 3 or 4 APs with strongest RSSI. [2] Combines the received RSSI with corresponding BSSI (MAC address) of each AP in order to create fingerprints - i.e. measurements of what the RSSI looked like at a certain time, not to be confused with biometric fingerprints - that will not get confused with other locations with similar signal strength.

1.2 Restrictions

Figure 1.1: Axis Network Door Station A8207-VE.

The aim of this thesis was to develop a mobile multi-factor authentication solution either towards the Axis A8207-VE network door station unit, see Figure 1.1, or a solution that works independently without a door station unit. The door station has an ultra wide-angle lens 6MP IP camera, an integrated RFID reader with keypad, a microphone and speaker with acoustic echo cancellation and noise reduction. There is also additional hardware such as relays, HDMI output and RS485.[7] Early on in the project discussions it was decided to not introduce new hardware but to work only with what is available in the unit and in the building.

As stated in the problem definition, security issues beyond the baseline are out of the scope for this project. Similarly, all forms of usability, user experience and other design related aspects are omitted. Thus, the design and layout of the system and application itself is focused solely on ease of testing and evaluation.

Chapter 2

Approach

2.1 Method

To find a good solution for the problem, four different solutions have been evaluated and iterated upon to solve existing known problems or unknown arisen problems. All of the solutions aims to fulfill the original request for reduced interaction.

2.1.1 QR Scanner with Fingerprint Authentication

To provide a basis for comparison and a fallback solution to use in case other authentication functionality malfunctions, the first solution utilizes fingerprint scanning functionality (biometrics) of the mobile phone to generate a QR code that is then shown to the door station unit to gain access.

This combination can be directly compared to the original RFID + PIN solution in terms of security, where possession of the phone corresponds to possession of the card ("something you have"), bio-metric authentication corresponds to proving your identity with the photo on the card("who you are"), and a third factor is provided by proximity to the door ("where you are").

As the application can be created with existing and available technology, using the Axis Visitor Access [8] for QR generation and recognition as well as Androids API for fingerprint authentication, [9] it was chosen as the minimum viable way of fulfilling the original requirements.

Performance is measured in terms of total interaction time, interaction time with the door station unit, authorization range and rate of failure, and this data is used as a benchmark for comparison with other solutions and improvements. Lastly, the application itself will work as a platform for building the improved solutions on, containing all functionality in one place to facilitate testing and evaluation.

2.1.2 Wi-Fi Location with Fingerprint Authentication

The second solution will focus on the fourth factor mentioned in Section 3.1, location, or "where you are". The idea is that through Wi-Fi localization it can be determined which door the user is closest to without any interaction with the actual door-station.

Every user has a smartphone with the mobile application on it ("something you have") which they authenticate toward. First, in order to access the app you need to provide a fingerprint ("who you are"). Secondly, once you have accessed the application and are standing outside the door, the user can click an "OPEN VIA WIFI" button which will send the current Wi-Fi data to the server that in turn determines which door the user is closest to ("where you are") and open it.

Performance is measured in terms of accuracy, i.e. how often is the algorithm correct in which door you are closest to. Being "closest" to a door in this instance means being within the threshold distance within which no adjacent door should be chosen by the localization algorithm.

2.1.3 Three Doors Solution

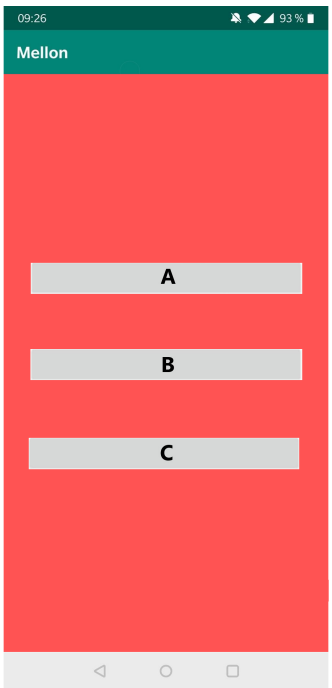


Figure 2.1: Illustration of three door idea.

As an alternative solution to the Wi-FI scan, a solution is provided that simply displays the three closest doors at the time, as seen in Figure 2.1. The displayed doors continuously update as new scans are being completed. This solution is based upon the fact that it is not reliant on rapid RSSI scan completions. Since "old" data - up to six seconds - is sufficient enough to determine the general area, which should not contain more than three doors placed densely enough to risk being displayed.

To evaluate this solution, it is established how quickly after moving to a new door the correct door option shows up in the application. Since the solution uses the latest signal strength data available, it may take a certain amount of time to display the correct door immediately after moving there, depending on the layout of fingerprints. This average time is measured for a given fingerprint configuration as a performance metric as well as how often no waiting is required.

2.1.4 Wi-Fi Combined with Geomagnetism

To improve the original Wi-Fi solution in subsection 2.1.3, a geomagnetic component is combined with the Wi-Fi data for faster localization. In this solution, the Wi-Fi localization is used to determine macro location, i.e. proximity while geomagnetic fingerprints are used to determine micro location. Similar to the Wi-Fi solution the user will use the mobile application ("something you have"), access it with a fingerprint ("who you are") and then click "OPEN VIA GEO" which will determine which door you are closest to and open it ("where you are"). However, for this solution there will be a marker on the door where you are supposed to place the phone before pressing open.

In subsection 2.2.6 geomagnetism is discussed further and found to have spatial discrimination problems since there is a high risk of finding the same values at several positions in a building. This is what prompted the combination of Wi-Fi with geomagnetism since Wi-Fi can provide the macro location i.e. which building/floor/corridor while geomagnetism then can provide micro location i.e. which door is the best match in this macro location.

To evaluate the solution, tests are performed to estimate how much the geomagnetic fingerprint changes in a set location to determine the range for a unique fingerprint. Subsequently, tests at different doors were carried out to measure the range of the geomagnetic values in the area. With both of these tests, it is possible to determine the amount of possible fingerprints at a door. If there are a lot of unique fingerprints at each door then the risk for overlap in the x closest doors given from the Wi-Fi solution is minimized. If the overlap is small then more fingerprints can be considered from the Wi-Fi solution and this will improve the accuracy since the magnetic fingerprints are very stable. The only time this solution is wrong is when the right fingerprint is not included within the possible matches.

2.2 Theory

In this section a majority of the underlying theory and terminology needed to understand the rest of the paper is introduced. Moreover, some possible problems are mentioned that are later investigated in section 3.2 and further discussed in chapter 4.

2.2.1 Micro and Macro Localization

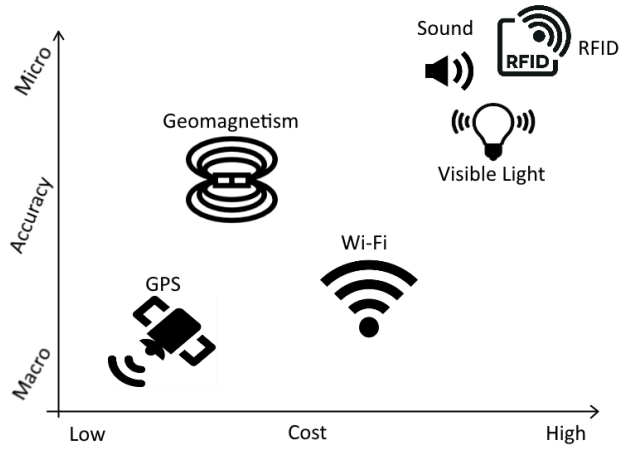


Figure 2.2: Cost and performance for smartphone-based indoor localization. [37]

Positioning systems are naturally divided into categories based on their strengths and weaknesses, Figure 2.2 shows such a comparison. The cost usually rises with the need for additional hardware which is something this thesis aims to avoid, see section 1.2.

This thesis will continuously refer to the terms micro and macro localization which are terms that are contextualized a little bit in Figure 2.2. GPS is a good example of a macro localization technology that does a good job of determining in which area you are but does not offer any fine grained localization such as which room inside that building. RFID, sound and visible light are all micro technologies since they are short ranged and therefore can only determine exact location while larger areas get blurred together. Wi-Fi and geomagnetism are somewhere in between although Wi-Fi and geomagnetism lingers more towards macro and micro respectively.

2.2.2 Received Signal Strength Indication

In the context of Wi-Fi networking, Received Signal Strength Indication, or RSSI, is a measurement of the relative power of a received radio signal in a client device. RSSI is typically measured in decibels relative to milliwatt (dBm) and ranges between around -30 dBm for excellent reception and -90 dBm on the border of visibility. [12] As decibels are measured on a logarithmic scale, this means that an RSSI drop of 3 dB corresponds to a halving of signal strength.

The signal strength in an indoor environment can vary substantially depending on the layout. FCC regulations require Wi-Fi signals to operate at very low power levels which means that a concrete wall is enough to degrade the accuracy. Furthermore, users holding a mobile device can block the signal to an access point, resulting in a 10-15 dBm signal drop.[20] This is because water's resonance frequency is 2.4 GHz and humans consists of 70% water.[47] Taking into account the previous paragraph regarding logarithmic scale, a drop of this magnitude is devastating.

Moreover, RSSI values are shown to vary significantly between different brands of smartphones. Crucially, if one phone does the offline fingerprinting then another brand might mismatch the fingerprints in the online localization phase.[21] Signal differences all the way up to 25 dB have been measured in the same location, rendering some algorithms useless. However, a way to counteract this is to utilize signal strength ratios instead of the absolute values. [22]

Hardware such as the router and access point can also make RSSI readings vary greatly, even between chipsets of the same brand. G. Lui et al. also present some interesting behaviour of hardware where certain signals drop greatly and then recover, oscillations in the signal and even some chipsets that seem to cache the RSSI data. It is also concluded that 2.4 GHz suffers from increased interference which gives the signal readings higher variance. [32]

The RSSI typically changes on large distances due to so called large scale variations. This allows RSSI fingerprinting to be utilized for positioning since it makes the signal signature change when a user moves to different parts of the room, i.e. different distances from the access points.[23] The way RSSI changes with distance can be described by a path loss model, see Equation 2.1. d is the distance from a node, n is specific for an environment and C is a constant. [48]

$$RSSI = -10 \cdot n \cdot log_{10}(d) + C \tag{2.1}$$

However, there are also small scale variations that are harder to deal with. Within centimeters range the signal can change in the size of 10 dB. [23]

2.2.3 Fingerprinting Localization Technique

Fingerprinting is a widely used localization technique that consists of two different phases.

In the first phase, commonly referred to as the "offline phase", some geographically unique data is collected and stored as a fingerprint in a database. As it is impossible to sample at every possible physical location, fingerprints are typically combined into a radio map grid with a set distance between cells.[13] The granularity of the fingerprints - see Figure 2.3 - depend on the desired level of accuracy, where a coarse grid of fewer, large fingerprints can be sufficient to achieve a very rough estimate of position, but where a detailed grid of many small fingerprints are required for greater accuracy.

In the second phase, the "online phase", the tracked client device captures the same type of data in real-time for comparison with the values in the database, determining the most similar fingerprint and thus also an estimate of position.

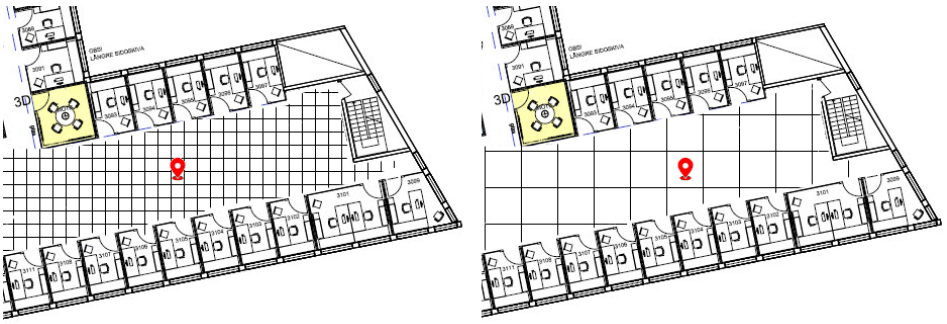


Figure 2.3: Coarse vs. fine grained fingerprint maps.

Due to the fact that RSSI can be easily accessed with little to no hardware modification of modern mobile phones and other portable devices, and that Wi-Fi networks already are available in many indoor environments, Wi-Fi RSSI is the by far the most commonly used fingerprinting measurement in recent papers and studies. In theory however, any data that can be measured and varies geographically in a similar manner could be used for the same purpose, and other measurement examples that are used on their own or proposed in research papers include bluetooth RSSI, magnetometer data and landmark features (locational characteristics observable e.g by camera).

2.2.4 Deterministic Fingerprinting

To determine the closest match between a real-time sample and a fingerprint in the database, systems typically utilize one of two different algorithm types; either

a deterministic or a probabilistic approach. Deterministic algorithms minimize the distance between a detected signal vector and those of the database to get the closest match corresponding to the estimated position. The distance metric may or may not be relative to the actual physical distance, and some common deterministic algorithms include k Nearest Neighbour (kNN) utilizing the euclidean distance between vectors, the Centroid method calculating the average of distances to single access points in the database, and more advanced methods such as the support vector machine (SVM) and artificial neural networks (ANN).[24][26].

$$\sqrt{\sum(\bar{x}_i' - \bar{x}_i)^2} \tag{2.2}$$

Equation 2.2 shows the Nearest Neighbour formula utilized in kNN.

2.2.5 Probabilistic Fingerprinting

In deterministic algorithms, the fingerprints consist of the average RSSI value that was sampled over the duration of the offline phase. This leads to lost information, as the mean says nothing about the underlying distribution of signal strength. Probabilistic algorithms address this by instead storing the RSSI probability distribution of each access point as fingerprints. Some studies suggest that the signal strength distribution can be assumed to be Gaussian[23][28] while others conclude that this is not always the case and that the distribution might be negatively skewed or even bi-modal.[30][31] In the online-phase, probabilistic algorithms are used to retrieve the location that maximizes the posterior probability of each location in the fingerprint database, given the real time sample data. This is done through a combination of Bayes theorem and Maximum A Posteriori estimation[26]

Bayes' Theorem

Bayes' theorem, (also known as Bayes' rule, Bayes' law) as described in Equation 2.3 describes the probability of event A occurring, given occurrence of event B.

$$P(\mathbf{A}|\mathbf{B}) = \frac{P(\mathbf{B}|\mathbf{A})P(\mathbf{A})}{P(\mathbf{B})} \tag{2.3}$$

In probabilistic fingerprinting, this can be used to describe the problem as:

$$P(\mathbf{FP}|\mathbf{AP\_RSSI}) = \frac{P(\mathbf{AP\_RSSI}|\mathbf{FP})P(\mathbf{FP})}{P(\mathbf{AP\_RSSI})} \quad , \tag{2.4}$$

where $\mathbf{AP\_RSSI} = (RSSI_1, RSSI_2, ...RSSI_n)$ is the vector of observed signal strength to corresponding n access point points in the online phase, and **FP** is a location fingerprint in the database.

When using Bayes' theorem in fingerprinting, the goal is to acquire the most likely position **FP** given an RSSI vector **AP_RSSI** [40] i.e.

$$argmax_{FP}[P(\mathbf{FP}|\mathbf{AP\_RSSI})] \tag{2.5}$$

Using Equation 2.4, Equation 2.5 can be rewritten as following:

$$argmax_{FP}[\frac{P(\mathbf{AP\_RSSI}|\mathbf{FP})P(\mathbf{FP})}{P(\mathbf{AP\_RSSI})}] \tag{2.6}$$

Since $P(\mathbf{AP\_RSSI})$ is a constant and the same for everyone [40], i.e. the probability to get a certain observation vector $\mathbf{AP\_RSSI}$ will not change with which $\mathbf{FP}$ that is considered, this means that it can be removed. Moreover, since the previous location is not taken into account in the algorithm, the probability to be at a certain position can be seen as a uniform distribution [26]. This means that also $P(\mathbf{FP})$ does not have to be considered in the maximization, leaving the final formula as:

$$argmax_{FP}[P(\mathbf{AP\_RSSI}|\mathbf{FP})] \tag{2.7}$$

The conditional probability $P(\mathbf{AP\_RSSI}|\mathbf{FP})$ can be estimated in several ways [26], one of them being estimating the distribution from normalized histograms which is the chosen method for this thesis, as further described in subsection 3.2.2.

Maximum Likelihood Classification

Deterministic algorithms discussed in subsection 2.2.4 such as Nearest Neighbour work relatively well but they do not take into account standard deviation [33]. As N. Pritt [33] has concluded, the distributions to different APs can vary greatly. Signals that are not in line-of-sight (NLOS) have a much wider distribution and this needs to be reflected in the AP scoring.

As mentioned in the previous paragraph, the prior probability is uniform and does not have to be included in the maximization. This makes Maximum A Posteriori equal to Maximum Likelihood and allows us to incorporate the theory of the previous section. The standard normal distribution probability density function looks as following:

$$P(\mathbf{AP\_RSSI}|\mathbf{FP}) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-\mu}{\sigma})^2} \tag{2.8}$$

However, the signals from different APs can be considered independent, which means Equation 2.8 can be rewritten. With S_i being standard deviation of AP_i, $\bar{x}_i$ is mean of AP_i and x' is the current RSSI at unknown position. [33]

$$P(\mathbf{AP\_RSSI}|\mathbf{FP}) = \frac{1}{(\prod s_i)(2\pi)^{n/2}} e^{-\frac{1}{2}\left(\Sigma\frac{\bar{x}_i' - \bar{x}_i}{s_i}\right)^2} \tag{2.9}$$

By taking the natural log and multiplying with -1 and removing constants the result is: [33]

$$g(\bar{x}') = \ln(\prod s_i) + \frac{1}{2}\sum\left(\frac{x_i' - \bar{x}_i}{s_i}\right)^2 \tag{2.10}$$

Which is the function that is minimized in order to acquire the maximum likelihood estimation. Multiplication with -1 to simplify is what makes the function be minimized instead of maximized as one would expect when trying to maximize a probability.

2.2.6 Geomagnetism

Earth's magnetic field, also referred to as geomagnetism, is a signal that can be utilized for indoor localization. It is more cost effective than Wi-Fi since it requires no additional hardware except for the smartphone itself. Additionally, geomagnetism supposedly outperforms Wi-Fi in differentiating locations. [37]

The earth's magnetic field consists of several parameters but are usually expressed in x,y and z coordinates.[34] The geomagnetic field intensity (GFI) is very stable on the same place on the earth. However, a lot of local anomalies and distortions are caused by ferromagnetic materials such as pipes and rebar as well as by the steel construction of most buildings. [34][35] This is what makes it plausible to use for indoor localization.

GFI is stable in theory but in practice it is not so easy to use effectively because the GFI values change with the phone's attitude.[35] Figure 2.4 shows the coordinate system for an Android smartphone that is used with the Sensor API. Obviously, rotating the phone or tilting it will change the axis values and in turn change the GFI value.

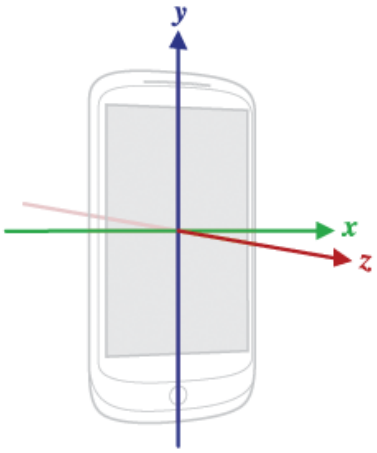


Figure 2.4: Coordinate system (relative to a device) that's used by the Sensor API. [36]

This attitude problem can be solved in two ways; either by transforming the magnetometer readings from local coordinate system - the phone's coordinates from Android Sensor API - to global coordinate system or using the magnitude of the magnetometer vector. However, simply using the magnitude brings a spatial discrimination problem since there is only one dimension and high risk of similar values at several positions. [35] [51]

Transformation of 3D magnetometer readings

The relationship between the local coordinate system and the global coordinate system can be described by three angles called pitch (x-axis), roll (y-axis) and yaw (z-axis). These angles can be calculated from any Android phone's gyroscope with a simple API call. However, the gyroscopes inside smartphones are low-cost and can not reach sufficient accuracy, often displaying 40 degrees error or more. [38] On the other hand, the direction of gravity in smartphones is stable and can therefore be used for fingerprinting. [39]

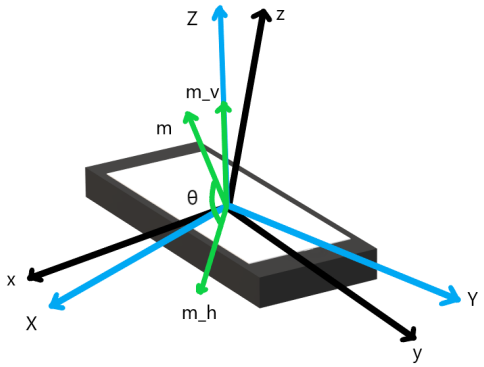


Figure 2.5: World coordinate system (blue), Local coordinate system (black).

Transformation is done by decomposing the three-axis magnetometer m into a vertical and horizontal component, m_v and m_h. [34] The direction of the gravity vector is the opposite as the global coordinate system's Z-axis. Which means that the magnetometer reading in the local coordinate system can be projected onto the gravity vector to acquire the vertical - as well as the horizontal - component in the global coordinate system. If the angle between m and m_v is assumed to be $cos(\frac{\pi}{2} - \theta)$ then the vertical projection can be described by: [35]

$$m_v = \|m\| \cos(\frac{\pi}{2} - \theta) \tag{2.11}$$

Finally, knowing m_v and m it is trivial to acquire m_h through the Pythagorean theorem:

$$m_h = \sqrt{\|m\|^2 - m_v^2} \tag{2.12}$$

Calibration

The magnetometer inside smartphones is prone to be disrupted by noise produced by ferrous materials, such as keys in your pocket. This causes the magnetometer readings to be off and manual re-calibration might be needed to achieve expected results. [51]

2.2.7 Environment

For the purpose of this thesis, a custom environment has been set up with four access points that are always visible in the testing area. However, in most realistic applications the environment is noisy and it is not always known where APs are located. Furthermore, they are not set up in a way that is advantageous for location of mobile devices.

Due to the ubiquitous nature of Wi-Fi signals it is realistic to have up to 20-40 audible APs in a building. [41] If all audible signals are considered then a few that are just on the edge of audibility are going to be weak in signal strength. This in turn will mean that every scan a set amount of APs will likely be missing from the result list. [42]

Most works counteract this by choosing a set of important APs that are to be used in the offline fingerprint database. LocAuth [43] ranks the network nodes according to highest average signal strength, highest correlation rating as well as amount of appearances out of a set amount of scans. However, in a noisy environment this might mean missing out on important information. If a signal from AP B is missing in the online fingerprint and fingerprint A has AP B then there is a low chance that fingerprint A is the right location. Furthermore, adjacent positions share a lot of similar visible APs where the low signal and low visibility APs provide valuable information to differentiate APs. [42]

One problem that arises in a noisy environment is that APs which have sufficient signal strength sometimes do not show up in the readings. According to M. K. Hoang et al. there is a correlation between the amount of APs and the drop-out rate where increasing the amount of audible APs will also increase the drop-out rate. [41] Y. Li et al. [42] found that around 60% of APs have less than 50% visibility and around 20% have less than 10% visibility. To clarify, in a noisy environment these drop-out APs are not necessarily on the edge of visibility but can have quite good signal strength when they show up.

This leads to a problem of missing data and it needs to be solved before it is possible to estimate the probability distributions. The common solution is to replace the missing data with a low value reading such as -110 dBm. For a deterministic approach this is fine but in a probabilistic model this will ruin the distribution estimation. [42] Additionally, even for a deterministic approach this would be sub-optimal for the drop-out problem stated above, where strong signals seamlessly disappear. The low strength constant -110 dBm is based on the assumption that the signals that disappear are weak signals.

Y. Li et al. [42] proposes a solution which takes into account these unseen APs by calculating the probability to fail to see the AP after M scans. In other words, when finding an AP that has not been found in the offline fingerprint phase the probability is calculated as the probability to fail to discover it M times and then

finding it the next time.

$$f(M) = (1-p)^M \cdot p, \text{where } p = \frac{1}{M+1} \tag{2.13}$$

Equation 2.13 shows the probability $f(M)$ to fail to see an AP after M scans.

2.3 Implementation

In this section, description of - and reasoning behind - important implementation choices for all the solutions are presented.

2.3.1 Client/Server-model

For the purpose of this thesis, a Client/Server-model was built in order to carry out our experiments and evaluation. The client is written as an Android application in Java and it communicates with the server through Java's Socket class [18]. The client either sends it's location when the user wants to open a door or it sends fingerprint data which will be stored in the database together with corresponding door ID.

The server is also written in Java and utilizes the Java class ServerSocket [19] to listen to incoming connections. First a ServerSocket instance is created on the right port and then the program waits for a connection to connect and then returns the Socket which communication will be carried out over.

For the sake of evaluating the proposed solutions of this thesis and to limit implementation time unrelated to the core problem, the server is hosted on a dedicated PC on a local network. Furthermore, a mock database system is used that simply stores and manages data in text files on the dedicated server PC.

2.3.2 QR Solution

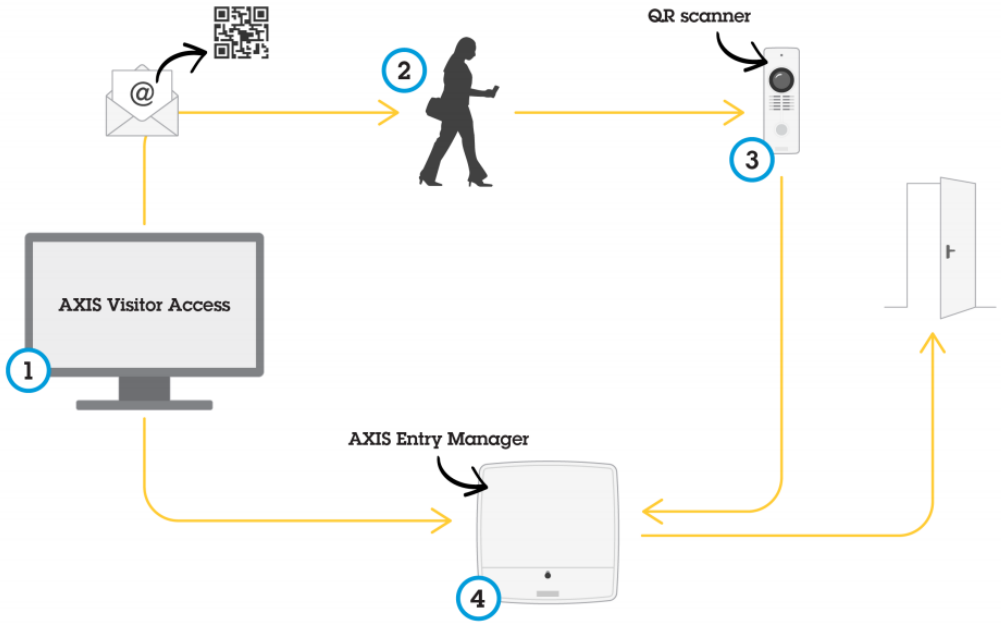


Figure 2.6: Axis Visitor Access.

Figure 2.6 shows how Axis Visitor Access is used as a commercial product. In the first step, a QR code is generated from a PC application containing credentials (full name + temporary card number) of a guest and is then distributed to them via email. The software also enrolls the user as an authorized guest in the specified entry manager hardware. In this solution, a QR code is created in the same manner and hard coded in the application for testing and evaluation purposes. In step two, the user opens the mobile application and scans his/her finger in order to display the QR image. The mobile application is written in Java using Android Studio, and the bio-metric authentication is performed using the android.hardware.fingerprint [9] package to query whether the scanned finger matches the fingerprint enrolled on the mobile phone.

2.3.3 Wi-Fi Solution

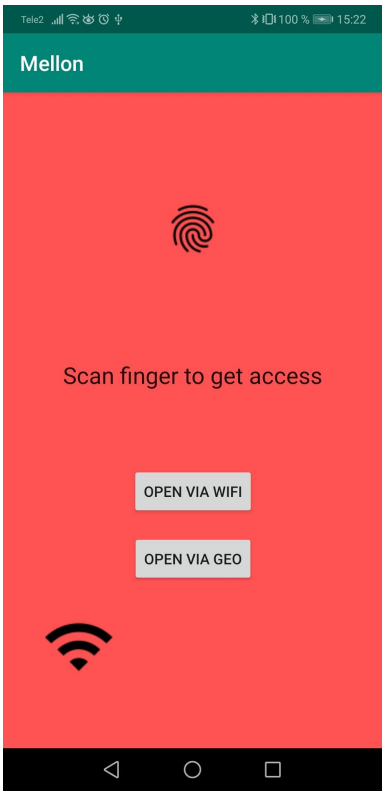


Figure 2.7: Image of the start screen of the application.

When access through a door is requested and "OPEN VIA WIFI" is pressed (see Figure 2.7), the client initiates a scan for available Wi-Fi access points through the android API class 'WifiManager' [27]. More concretely, this is done through the 'startScan' method, which passively scans for nearby access points and returns information such as RSSI, BSSID (mac address), SSID (network name) etc. for each of them. Simultaneously, a callback is registered though the use of the Java class BroadcastReceiver[10] that waits for the asynchronous event that the 'startScan' method returns. Upon arrival, an instance of the class SendThread is created on a new thread, which establishes a WebSocket connection to the server on the given port. The thread then sends the BSSID + RSSI for all access points detected to the served, before finally terminating.

The server either receives a location which is supposed to be used to generate a new fingerprint or it is sent a request to find a best match. In both cases the data received is a list of RSSI values combined with their respective BSSI, i.e. mac address. However, if the first case happens and the server wants to generate a new fingerprint then the server also receives the DOOR ID which the data belongs to.

The server then continues to listen on the socket while storing the received data in a separate text file, see Figure 2.8. D in this case is the DOOR ID, follow by the mac address and then the RSSI value. The final value is just a timestamp. Every time the server is started it will read this text file to calculate the mean RSSI value to each mac address for each DOOR ID as well as the standard deviation for each mac address.

```
D 74:da:88:d3:48:3e -39 316752
D 74:da:88:d3:43:58 -47 316753
D 74:da:88:d3:3c:c5 -49 316753
D 74:da:88:e3:d9:cd -60 316753
```

Figure 2.8: One fingerprint data sample in text file.

On the other hand, if the received data is a request for a best match then the DOOR ID is replaced with "loc" see Figure 2.9. The server will not continue listening but will handle the received data instead. Handling the data means determining a best match with the fingerprints that are available in the text file.

```
loc 74:da:88:d3:48:3e -42 309724
loc 74:da:88:d3:43:58 -43 309725
loc 74:da:88:e3:d9:cd -49 309726
loc 74:da:88:d3:3c:c5 -54 309726
```

Figure 2.9: Data sent in an OPEN VIA WIFI request.

The algorithm used is the Maximum Likelihood Classification discussed in section 2.2.5, more concretely Equation 2.10. Since all standard deviations s_i in Equation 2.10 as well as all mean values x_i are loaded when starting the server. $x_i^{'}$ is inserted into the formula which are the RSSI values that are received from the client. In the Figure 2.9 example these $x_i^{'}$ values correspond to -42, -43, -49 and -54. The DOOR ID that minimize this function is then determined the best match. For the alternate Wi-Fi solution in subsection 2.1.3 the 3 best results are instead saved and sent back to the client so that it can display the results.

2.3.4 Wi-Fi Combined with Geomagnetism

In the geomagnetism solution a lot of the underlying structure is the same as the alternate Wi-Fi solution except that the 3 doors are not sent back to the client but rather used internally in the server to determine a geomagnetic best match. Moreover, the solution can be scaled up to not just consider 3 closest door but however many that is optimal for the local setup. This is further discussed in section 4.3.

```
mag loc -40.28032372118946,14.902405594541674
```

Figure 2.10: One of 50 consecutive samples sent in a OPEN VIA GEO request.

When "OPEN VIA GEO" is pressed, both the Wi-Fi location data, as displayed by Figure 2.8, as well as 50 geomagnetic samples - see Figure 2.10 - are sent. The first value is the vertical projection of the GFI mentioned in subsection 2.2.6, followed by the horizontal component.

Similar to the Wi-Fi solution this magnetic fingerprint data is collected and stored in a text file. This text file is read when the server is started and then the mean for both components are calculated for each DOOR ID. In this solution the algorithm is a traditional nearest neighbour algorithm as mentioned in Equation 2.2. $\bar{x}_i'$ is the magnetic horizontal component in the database read from the text file and the $\bar{x}_i$ is the corresponding magnetic component received from the client, see Figure 2.10. The same is done for the vertical component. The best magnetic match is the DOOR ID which minimizes the sum of this equation for both components.

Chapter 3

Evaluation

3.1 Experimental Setup

This section focuses on the setup used in the experiments presented in the Result section. The custom AP setup in Figure 3.1 with dynamic scanning is used if nothing else is mentioned.

3.1.1 QR Scan Time

QR scanning can not fail in the same way as a location estimation since it is more binary, it simply works or not. Therefore, the time for it to work is the more interesting metric. A user does not want to be stuck trying to scan the QR code forever because it is hard to figure out how to hold the phone. It seemed relevant to not only test by ourselves but also by someone who does not know how the system works or the optimal way to scan with the door stations particular camera. Since it is a wide-angle lens as mentioned in section 1.2, it is not obvious how to hold the phone optimally. The results are provided in Table 3.1.

The results were gathered by measuring the time it takes for the system to accept a QR code presented to the camera. The screen was at 50% brightness and already unlocked from the start of the time measurement.

3.1.2 Wi-Fi Signal Behaviour

To examine the behavior of Wi-Fi signals in a typical office environment, a local network consisting of four TP-link RE305 AC1200 Wi-Fi repeaters are mounted as shown in Figure 3.1. The number of access points are chosen in accordance to [25] which states three to four APs as the optimal number in certain scenarios where APs are scarcely located.

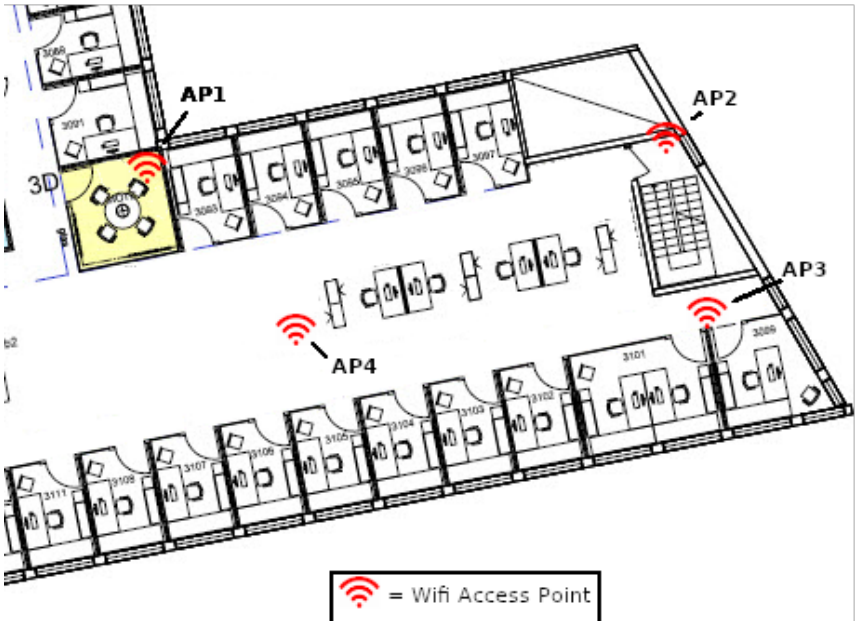


Figure 3.1: Custom AP setup.

Large Scale Variations

To determine the variations in received signal strength across the office and thus the feasibility of creating unique yet densely placed fingerprints, the RSSI loss over distance needs to be examined. To investigate these large scale variations, a sampling device is placed in a static position one metre from AP2 with clear line of sight. The device then samples the RSSI from AP2 once every seventh second for ten minutes. The process is repeated with increments of one metre up to a distance of ten metres. Lastly, the received values are averaged out at each measure point, taking into account the movement of employees in the area and other noise.

RSSI Probability Distribution

In order to counteract the RSSI small scale variations mentioned in the theory subsection 2.2.2 and utilize the generally more accurate probabilistic algorithms in Wi-Fi localization, some knowledge of the underlying RSSI distribution is required. To estimate the distribution of signal strength, a sampling device is placed in the center of the room to sample the RSSI from every access point once every seventh second for one hour. The frequency of measured RSSI values to each access point is combined into normalized histograms using Microsoft Excel, as is presented in the Results section. This data is then used to calculate mean and standard deviance, to be used in the probabilistic localization algorithm as further described in subsection 2.2.5. The same test is carried out when the sampling device is not in line-of-sight of the APs to see the effect on the distribution.

Non-line-of-sight Propagation

To establish how dropping line of sight towards an access point affects the RSSI level and thus also the fingerprint placement options, the sampling device is placed on each side of a nine centimeter thick wall with otherwise clear line of sight to AP4, where it samples the RSSI values of said AP for one hour each. The observed signal strength values and distributions are presented in the Results section.

3.1.3 Wi-Fi Performance Evaluation

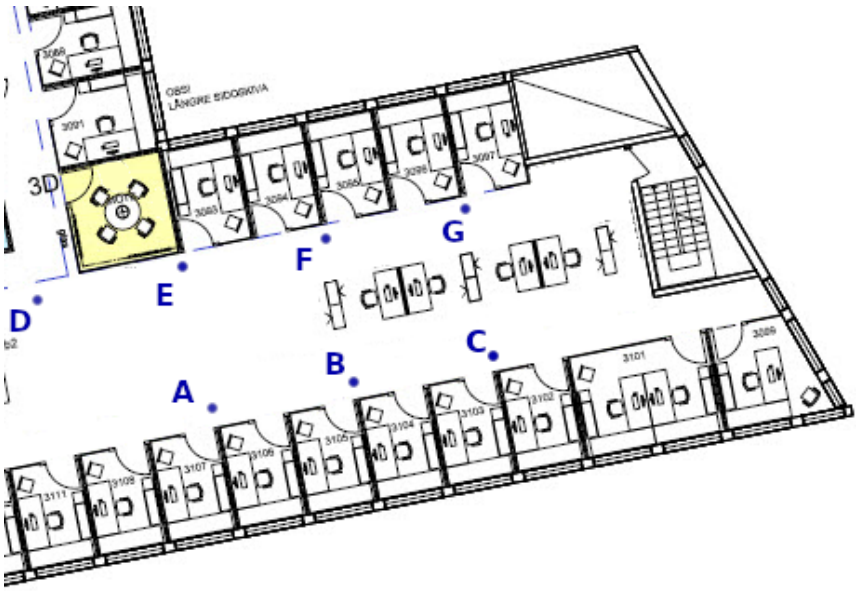


Figure 3.2: Fingerprints 4,5 metres.

To evaluate the performance of the Wi-Fi based solution, fingerprints are placed as shown in Figure 3.2 with a minimal distance of 4.5 metres separating them. To create the fingerprints, the sampling device is held manually with the test person facing down the corridor. The RSSI value from access points in the chosen network(s) are then sampled for five minutes, while rotating the device within 180 degrees from the starting position. The averages of the values to each AP are then combined to a fingerprint for each location.

As an initial step of evaluation of the online phase, a test person is placed immediately on top of every fingerprint in Figure 3.2. The test person then requests access to the closest hypothetical door via the mobile application. After that, the server calculates the best fingerprint match in the database and prints it to the terminal. The process is repeated for 50 iterations and the success rate for each fingerprint is presented in Table 3.2.

In a realistic scenario, the user will obviously rarely be positioned exactly on top of the fingerprint location. Therefore, it is important to examine the amount of leeway existing in terms of distance to the fingerprint while maintaining a sufficient level of accuracy. Optimally, walking within 2.25 metres in any direction from a fingerprint should always yield the same result. Due to the small scale variations this is not feasible in reality, and to determine this sensitivity a set of sampling points are set up according to Figure 3.3, one meter from the fingerprints in different directions. The drop-off in accuracy is then tested in the same manner as on the fingerprint itself. Note that the placement of other fingerprints plays a big part in determining the accuracy, as our solution does not use a traditional grid structure as Figure 2.3. In other words, the closer B is placed in relation to A in Figure 3.2 the harder it will be to maintain desired accuracy further from the fingerprint. For example, in the given scenario there is a distance of 4.5 meters between A and B. Moving 2.25 meters toward B from A would mean you are 2.25 meters from both fingerprints and calculating the correct estimate becomes ambiguous.

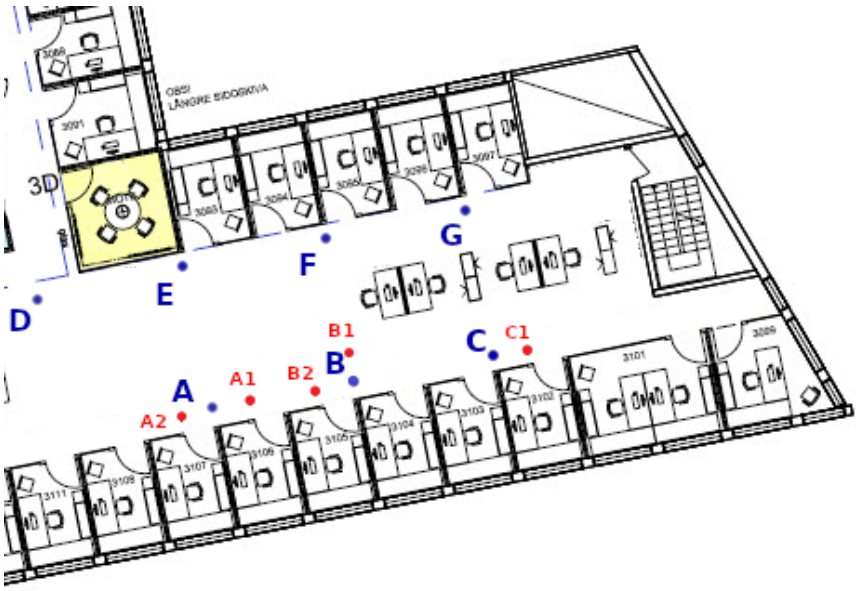


Figure 3.3: Fingerprint offsets of 1 meter.

With the introduction of the three doors solution in subsection 2.1.3 there was also a need to evaluate the effectiveness. Since the main problem with the original Wi-Fi solution was the scan time to complete this solution was evaluated focusing on waiting time. The evaluation was done by - starting from a random location in the room - walking to a fingerprint and then taking the time for the fingerprint to show up as one of the three doors options in the menu, see Figure 2.1. The choice was made to test fingerprint B and E since this would hopefully catch several scenarios. E is a relatively easy estimation with not so many fingerprints in both

directions while B is a harder match because there are three or more fingerprints in either direction. For example, E will usually be a part of top three matches in all of the left part of the room see Figure 3.2. However, B is not always covered in both parts of the room. In the right side you might find only F,G and C as well as on the top there might be D, E and A. Therefore, moving between these zones might produce more bad estimations for B. The results are presented in Table 3.7. The results are divided into how often the estimation was completely correct, how many times the right estimation was in the top 2 and lastly how many times in the top 3. The most important metric is that the right door is in the top 3 since the order does not really matter when the user just has to click one of the 3 buttons.

Sampling Methodology

The offline phase is not trivial to carry out. How long to scan each location and how the scanning is carried out needs to be addressed. Leaving a sampling device in the fingerprint location to scan continuously for a long duration gives a lot of data but perhaps not the most useful. Sampling in this manner might produce a disparity between the online and the offline phase. At the online phase the user is holding the phone and might block certain APs, which changes the signal strength severely.

This thesis has chosen to divide the sampling into two categories, static sampling and dynamic sampling. Static is when the phone is not held by a user when sampling but instead scans for a long duration. Dynamic is when the phone is held by a user and also rotated in a 180 °angle continuously during the sampling. Furthermore, the dynamic sampling duration is significantly shorter.

Performance Impact of Access Point Placement

To minimize the amount of required hardware while maintaining sufficient Wi-Fi coverage, existing access points in the office buildings are typically placed centrally in the ceiling of corridors and open space areas, following a one dimensional path through the building unlike the first custom AP setup in Figure 3.1. To mimic and evaluate how such a configuration affects the performance of the Wi-Fi localization possibilities, a second custom network is mounted as displayed in Figure 3.4.

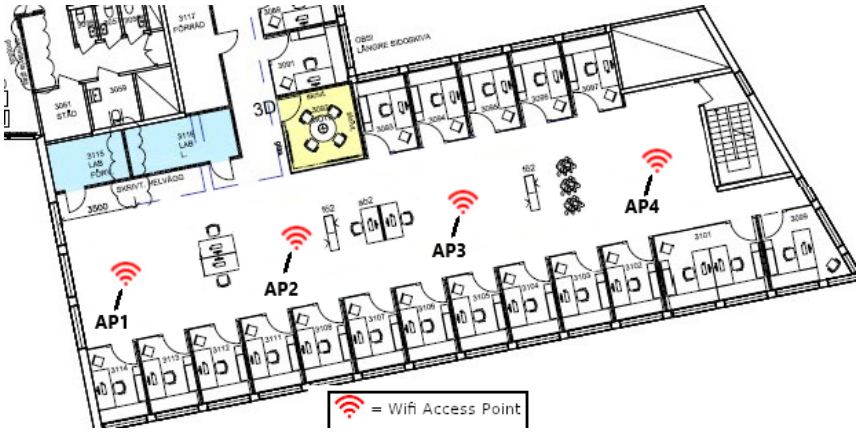


Figure 3.4: One dimensional access point configuration.

The offline phase is carried out in an identical manner as for the first custom network, once again performing so called "dynamic sampling" to record fingerprint A-G of Figure 3.2 by sampling Wi-Fi RSSI while rotating the device over five minutes. The accuracy is then measured over 50 authentication attempts per chosen fingerprint, and the resulting scores are presented in Table 3.3

Moreover, the Wi-Fi solution is also evaluated on a noisy network, see subsection 3.2.5 for details. In this test the solution is evaluated on a network that is not made for localization with unknown AP placements and with a lot of noise from walls and floors. The performance of the position estimation was first measured when only considering a few of the fingerprints, see Table 3.5. In other words, the position estimation could never be fingerprints D, E, F or G, see Figure 3.2. As mentioned in subsection 3.1.3, the placement of the fingerprints as well as the granularity matter greatly which is why this test was performed. The test was then also done when all fingerprints could be considered, results disclosed in Table 3.5.

3.1.4 Magnetic Field Indoor Behavior

To establish what can be regarded as a "unique" fingerprint, the geomagnetic field intensity is measured in the same location for 15 seconds to determine the fluctuations of the readings. The test is performed once with a user holding the sampling device in approximately the same area over the duration, and once with the phone in a completely static position without any user interference. Figure 3.10 and Figure 3.9 shows how the intensity varies over the duration in both of the test cases respectively.

To plan efficient fingerprint placement, knowledge of how many distinct fingerprints are theoretically possible to create in the same location is required. To investigate this, a set location is sampled continuously, noting the highest and lowest value that the geomagnetic field intensity reaches. The sampling is performed by moving the sampling device across the area in different dimensions until an

estimate of all possible values in the zone have been acquired. The location is chosen to be a plane with a width of one metre and a height between 90 and 150 centimetres, intended to be applicable on a door frame with the height of which a user could comfortably reach. The process is repeated for door frames located at fingerprints B, C, and E with resulting values as presented in Table 3.11.

3.2 Results

This section provides the results of experiments carried out in this thesis. The underlying method and setup is described in section 3.1.

3.2.1 Large Scale Variations

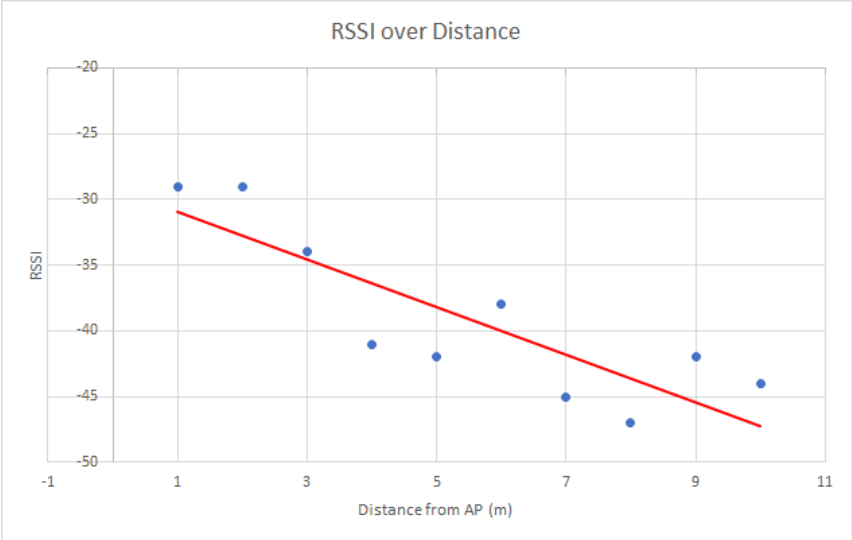


Figure 3.5: RSSI values measured at incremented distances to a single line-of-sight AP.

As the theory suggest, the RSSI values change with distance. A regression line is plotted in the same graph and the RSSI values have a linear decline in the 1-10 meter range.

3.2.2 RSSI Distribution

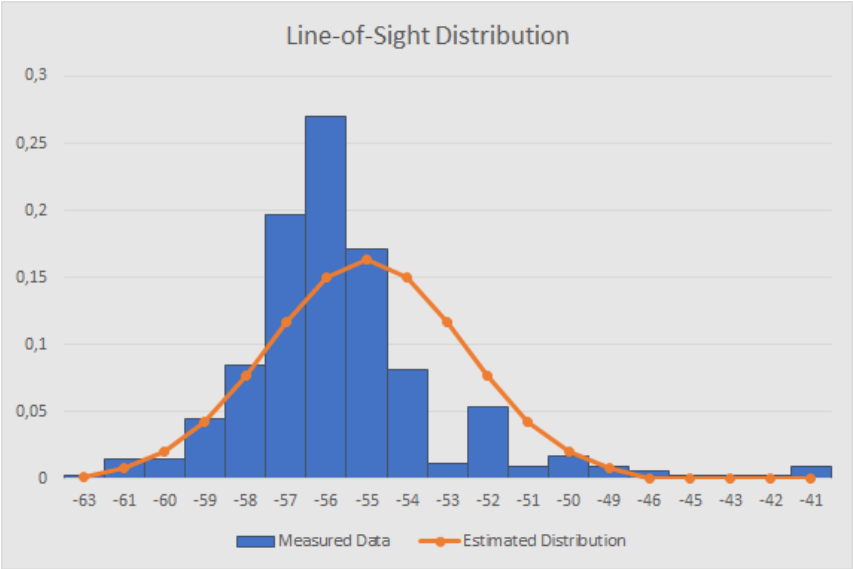


Figure 3.6: AP in line-of-sight RSSI distribution.

When the access point is in line-of-sight of the AP, the distribution is very pointy with a clear maxima in -56.

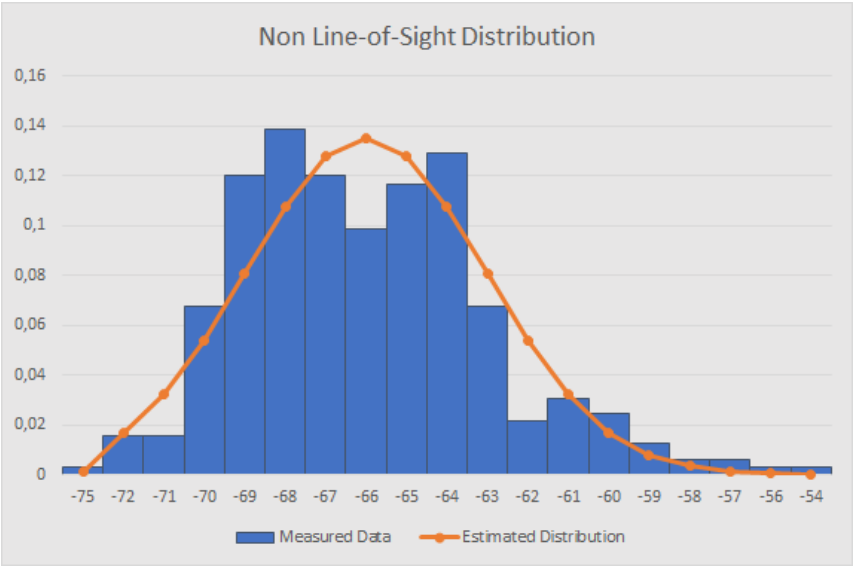


Figure 3.7: AP in non line-of-sight RSSI distribution.

When the AP is not in line-of-sight the distribution is a lot wider, i.e. the

standard deviation is higher. There is no clear maxima-point but instead several points with almost identical probabilities.

3.2.3 QR Solution Performance

Experienced user (s)	Novice user (s)
2.89	5.09

Table 3.1: Average time showing a QR code before scan succeeds.

An experienced user that knows about the system does the scanning in almost half the time of a novice user.

3.2.4 Custom Network Performance

The solution was evaluated for static and dynamic sampling respectively, this choice is motivated in subsection 4.2.5.

Fingerprint	Correct with Dynamic (%)	Correct with Static (%)
A	84	88
B	72	52
C	84	52
E	98	76
F	80	36
G	98	100

Table 3.2: Performance of Wi-Fi localization algorithm on the first custom network with static vs dynamic sampling.

Dynamic sampling is significantly higher on average, never dropping below 72% accuracy. In the following test dynamic sampling was always utilized.

Second Custom Network

To test how placement of access points affects localization performance, a second setup was tested as shown in Figure 3.4.

Fingerprint	Correct (%)
A	84
B	70
C	96
E	48
F	26
G	36

Table 3.3: Localization performance with APs placed in a line.

Interesting with this setup was that it worked quite well on fingerprints A, B and C, all achieving an accuracy similar to the first setup. It was not until the fingerprints on the opposite side were tested that the subpar performance was revealed, with all of E, F and G performing worse than 50%.

Meter Accuracy

Fingerprint	6 meters (%)	4.5 meters (%)
A	100	84
B	88	72
C	98	84

Table 3.4: Accuracy with different distances between fingerprints.

3.2.5 Noisy Network Performance

Fingerprint	Only ABC Fingerprints (%)	All Fingerprints (%)
A	98	62
B	96	54
C	100	16

Table 3.5: Correct position estimation with only fingerprints A, B and C versus all fingerprints.

The amount of fingerprints greatly affect the results, the accuracy on fingerprint C goes from 100% to 16% when introducing fingerprint D, E, F and G.

3.2.6 Combined Network Performance

Fingerprint	Combined (%)	Only Custom (%)	Only Noisy (%)
A	80	84	62
B	86	72	54
C	100	84	16

Table 3.6: Correct position estimation with all fingerprints when utilizing both the noisy network and the first custom network.

Increased accuracy can be achieved by combining networks to maximize coverage. The combined network provides overall higher accuracy and even reaches 100% on fingerprint C up from 84% and 16% respectively.

3.2.7 Three Doors Solution Performance

Fingerprint	Average Wait Time (s)	Zero Wait (%)
B	1.61	72
E	1.35	64

Table 3.7: Waiting times for the right door to show up as one of the three options.

Majority of times the user does not have to wait at all and when it is necessary the waiting times are lower than both the QR solution and the original Wi-Fi solution.

Fingerprint	Correct (%)	Top 2 (%)	Top 3 (%)
A1	68	84	94
A2	76	96	100
B1	82	98	100
B2	46	94	100
C1	98	100	100

Table 3.8: Top 3 performance data on offset locations.

Positions that would struggle to provide the desired accuracy in the original solution have more often than not 100% accuracy of displaying the correct door among the three best options.

3.2.8 Geomagnetic Field Intensity Indoor Behaviour

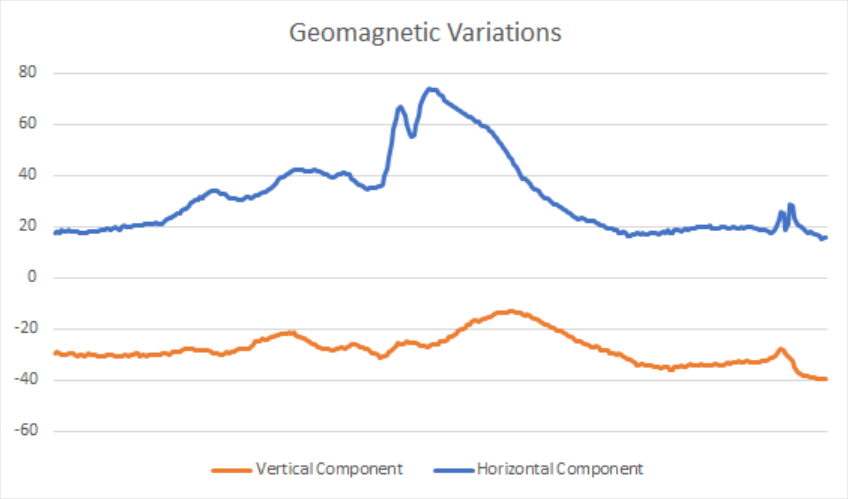
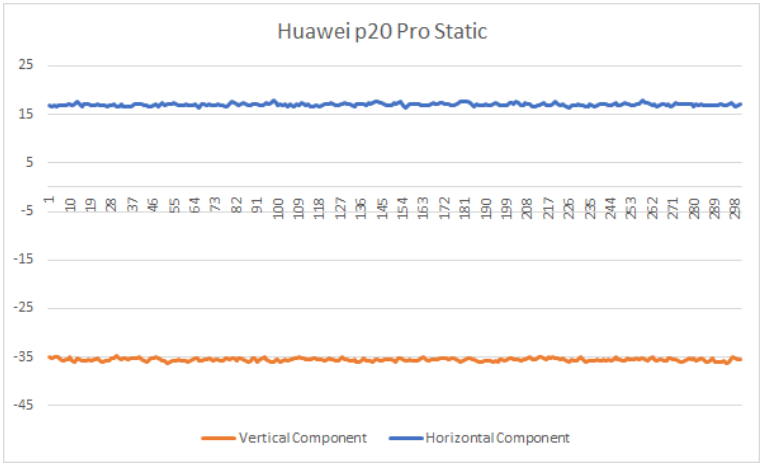
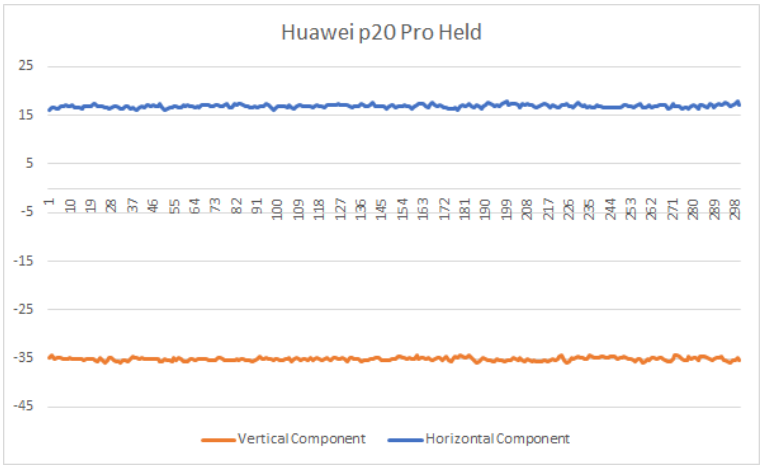


Figure 3.8: The possible variations in the geomagnetic field in 0.5m area around a door

The variations are way too high in a 0.5m area for this solution to be used in the same manor as the Wi-Fi solution were general area is sufficient.

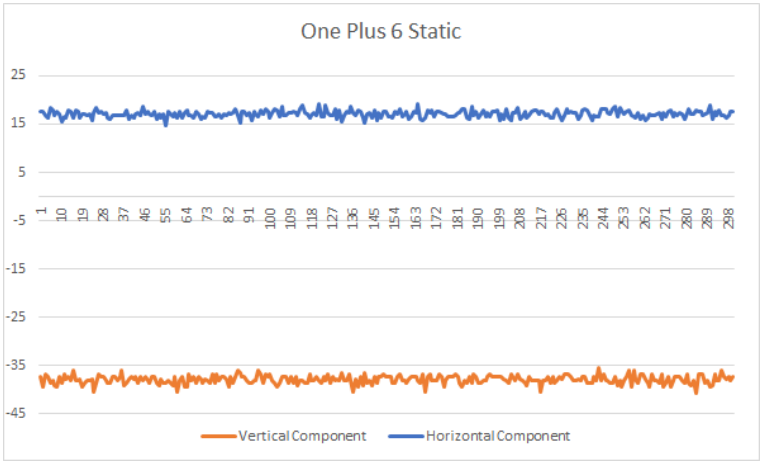


(a) Smartphone is placed statically without any human interaction.

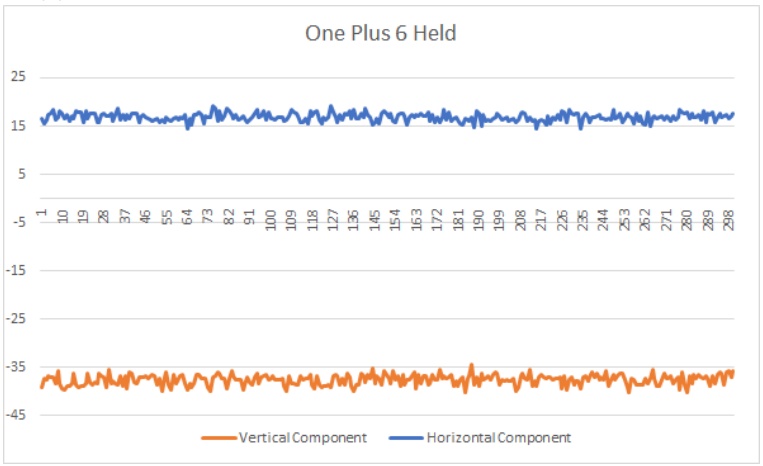


(b) Smartphone is held in the hand of a user.

Figure 3.9: Geomagnetic field intensity transformed into a vertical and horizontal component measured in a static location on a Huawei p20 Pro handset.



(a) Smartphone is placed statically without any human interaction.



(b) Smartphone is held in the hand of a user.

Figure 3.10: Geomagnetic field intensity transformed into a vertical and horizontal component measured in a static location on a One Plus 6 handset.

Smartphone	Vertical Avg. (μT)	Vertical Diff (μT)	Horizontal Avg. (μT)	Horizontal Diff (μT)
Huawei p20 Pro Static	-35.50	1.52	17.03	1.57
Huawei p20 Pro Held	-35.13	2.35	16.91	2.83
One Plus 6 Static	-37.87	5.21	17.08	4.72
One Plus 6 Held	-37.56	6.3	16.87	5.92

Table 3.9: Collection of specific numbers from Figure 3.9 and Figure 3.10. Diff is the difference between maximum and minimum values.

The One Plus 6 shows a more fluctuations in the values, sometimes reaching a difference of more than 6 μT while the Huawei is a lot more stable over time. However, neither phone shows any alarming difference in values between when it is held by a user or placed statically.

Smartphone	Vertical Diff (μT)	Horizontal Diff (μT)
Huawei p20 Pro	0.91	1.59
One Plus 6	2.30	2.18

Table 3.10: The vertical and horizontal difference when considering the average of 50 "OPEN VIA GEO" requests.

As described in subsection 2.3.4, an "OPEN VIA GEO" request sends 50 consecutive samples to the server which calculates the average. When considering this average instead, the differences have dropped from what was previously measured in Table 3.9. Crucially, the difference for the One Plus 6 which was disastrously high seems to balance out when working with averages.

Fingerprint	Vertical value range (μT)	Horizontal value range (μT)
B	16-24	32-40
C	8-25	36-48
E	16-24	31-41

Table 3.11: Geomagnetic field intensity value ranges measured around fingerprints.

It is apparent from Table 3.11 that fingerprint C has a much larger range and possibility to extract a lot more fingerprints. Working with the numbers that was found in Table 3.10, Huawei p20 Pro could optimally produce 32 unique fingerprints on B. Furthermore, for One Plus 6 this number is still a respectable 9. Naturally for C this number is even higher. However, this is the optimal scenario when all combinations are possible, which might not always be the case.

Chapter 4
Discussion

4.1 QR Performance

As mentioned in subsection 2.1.1, QR was mainly pursued to have a simple solution that solves the original problem of replacing the card. Directly comparing with the other solutions is not trivial since for example accuracy with QR is binary, either the scan succeeds or not. Therefore we chose average time to wait for a scan to succeed as the most relevant measurement. Since one of the big problems encountered with the original Wi-Fi solution was time this proved relevant.

An experienced user is in this case not realistic to a normal scenario and it is doubtful that this average time would be achieved by any normal user. When doing the test we were very aware of exactly what height and angle to use which will not be the case usually. However, it provides some sort of lower bound on the time. A more realistic time is the novice user which was done by persons not knowing the system at all.

4.2 Wi-Fi

Our original Wi-Fi solution is in some way involved in all of the different solutions. The solutions have therefore been influenced greatly depending on how well the Wi-Fi localization works.

4.2.1 Scanning Wi-Fi in Android

The initial Wi-Fi solution introduced a delay problem with the Wi-Fi scanning that is done in Android. The idea was to be able to walk up to a door and upon arrival press "OPEN VIA WIFI". However, it became apparent that the scanning is done passively in Android and not actively. This means that to get a new scan result the unit has to wait for APs to broadcast their signal strength and can not make this procedure faster. The result is a wait time of up to 7 seconds before receiving a new scan result. For an application that is supposed to make the system more convenient, this was simply not acceptable. If several seconds was acceptable then the QR solution would be better in this regard.

Moreover, scanning for Wi-Fi in Android has been heavily restricted during the years mainly to improve performance, security and battery life. [49] The only way to get around this throttling is with Android 10 compatible devices that can activate developer mode and thus disable Wi-Fi throttling. This is obviously a practical issue since Android 10 is not available on all devices yet and more of a workaround than a solution. IndoorAtlas is a company that sells different indoor positioning solutions and they also have not found a way around this but are simply stating that devices that run Android 8 or lower - i.e. predate the throttling - as well as Android 10 are compatible with the Wi-Fi solutions. [50] So there does not seem to be any more sophisticated solution as of yet.

4.2.2 Accuracy

The accuracy was always going to depend a lot on the chosen setup. Like mentioned in subsection 2.2.3, the traditional approach is to build a radio map grid and determine accuracy based on how many grids away the estimation is from true position. A dense grid meant increased possible accuracy while a coarser grid would naturally present a more macro location. However, we made a conscious decision to not have a grid structure but rather limit our fingerprints to door locations. Therefore a lot of the accuracy depends on how far apart and positioned the doors are to each other. As expected, placing the doors further away from each other improves the accuracy, see Table 3.4. 4.5 meters was found to be the point were the accuracy is acceptable, going below this threshold will produce results that are not acceptable. Furthermore, as we discovered from Table 3.3 and Table 3.5, the accuracy might be very good in one direction while disappointing in the other. If it is possible to choose AP placements, it can utilized to achieve a desired accuracy.

4.2.3 Improved Scaling

As stated in subsection 2.2.3, the standard fingerprinting technique is to build a grid structure inside the building. This is usually one of the biggest arguments against fingerprinting since it requires a lot of manual labor to generate these hundreds or thousands of fingerprints as well as the computational costs associated with such a huge database. [56] However, for our solution it is only necessary to have fingerprints scarcely placed at the doors themselves which reduces this scaling problem significantly.

4.2.4 Environment Effects

As mentioned in subsection 2.2.7 the environment can pose some problems for the algorithm which have to be addressed. This prompted the tests at subsection 3.2.5 which evaluated the noisy network in the building. We found that the setup of the fingerprints mattered greatly. Table 3.5 shows how the position estimation works with only the A, B and C fingerprints in the system. Almost flawless with close

to a 100% accuracy on all of them. This made us think that the drop-out problem mentioned in subsection 2.2.7 is not the main problem for the noisy network we tested on. The bigger problem seems to be trouble separating between fingerprints. When all of the fingerprints are included then a lot of the time the opposite fingerprints are confused with each other. At A the system often estimates E and at B often F etc. Resulting in the - much worse - results that are also presented in Table 3.5.

When utilizing the noisy network there is only a single AP that is visible through all the scans, the rest come from APs that reach the phone through the floor or through several walls. The spatial discrimination is thus subpar, moving a few meters in either direction might not effect the signal enough compared to the noise of penetrating several walls and/or floors. Consider Figure 3.7, already by just blocking line-of-sight with a wall we can see that the signal strength standard deviation is a lot higher. There are 6 values that occur approximately as often, while in line-of-sight that number is 3. If we follow the regression line in Figure 3.5 we see that moving 5 meter - approximately the difference between fingerprint A and E - the signal should change with 7 dBm. In other words, there might be a lot of situations where these possible offsets nullify each other. Consider if the noise makes the signal change 6 dBm in one direction and the change of distance 7 dBm in the other direction. The mean values are calculated in our offline sampling and if this noise consistently happens - which it does - then on average the offsets could each other out. Remember, this data is just when the signal goes through one wall relatively close to an access point. A lot of the reachable access points are much further away and face more disturbance.

Another explanation would be that its an effect of the placement of the APs in the building. What is apparent from Table 3.5 is that in one direction it is no problem to differentiate the access points. In fact, the accuracy is better than our custom setup. However, since the APs are not set up for indoor localization there are places where the accuracy is poor. Figure 4.1 shows an example of this, access points that seem to be far apart in a particular room or building might still be the same distance away from the access point locations. Especially since access points are usually placed in the middle of rooms to cover as much area as possible, the risk for symmetry is large. This was further tested in our second custom AP setup, as Table 3.3 shows, this setup provided similar symmetry problems. A, B and C all yielded a high level of accuracy, but when testing the other side, E, F and G are all below 50%.

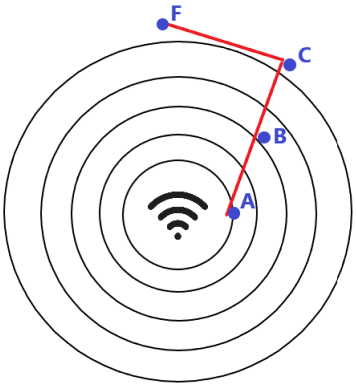


Figure 4.1: Noisy network access point signal spread.

This prompted the testing of a combined network, where the idea was to bring together the best of both the noisy network and the original custom network. The amount of APs available on the noisy network makes it in theory better at discriminating positions and building unique fingerprints but as discussed in the previous paragraph, some locations are too similar. The idea is to then bring in the custom network in these troubling areas to provide that needed discrimination, see Figure 4.2.

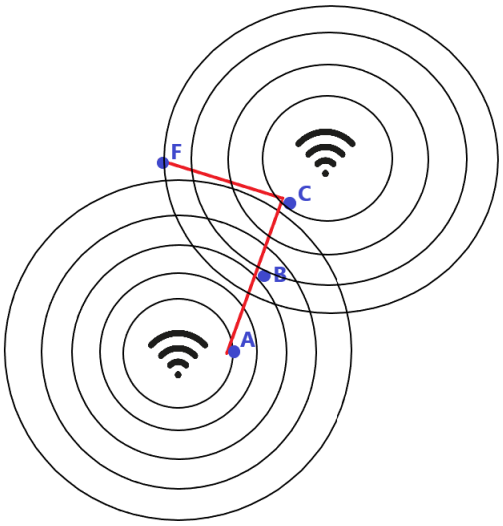


Figure 4.2: Addition of custom network access point to the noisy network.

In theory it will be similar to the macro and micro localization that we discussed in subsection 2.2.1, where the noisy network provides the macro location.

In our example, this macro location would for example be fingerprint C and F since the noisy network has trouble separating these two. Then the custom network can easily separate them. By combining the networks the risk of estimating B with true position C is reduced because of the noisy network being effective in this direction. Table 3.6 shows the result of the combination and we can see that A is still around the same accuracy but there is clear improvement in both B and C where the combined network performs a lot better. For C we achieved a flawless 100% accuracy with this system from a previous 84% on the custom network.

4.2.5 Fingerprint Sampling Methodology

Initially, the idea was to do the offline sampling by placing a phone in the fingerprint location for an hour to capture all possible value possibilities. However, we found that placing the phone statically in a single location was not representative of a realistic scenario. As [47] states and as mentioned briefly in subsection 2.2.2, the body greatly effects the signal. When placing the phone statically as we did initially, we never blocked any signal with our bodies which will happen in most cases when trying to open a door in the localization phase. RADAR was one of the first Wi-Fi localization solutions and they calibrated using four different orientations at each fingerprint to deal with this problem of blocking access points. [52] We addressed the problem by sampling dynamically by holding the phone in the hand and rotate in a 180° angle to capture as many cases as possible. Realistically, this could not be done for as long time as the static sampling where one could simply leave the phone. Even so, sampling for a much shorter time dynamically still provided better results than the static sampling, see Table 3.2.

An interesting outlier is fingerprints A and C where the static sampling actually provides better results. There will most likely always be positions where the static sampling is the better option, with our first custom setup as Figure 3.1 shows, all the access points are on one side of fingerprint A. We were testing by facing down towards AP2 and AP3. In this orientation none of the APs are likely blocked by the body and static sampling therefore works better. Moreover, if we are facing down towards AP2 at fingerprint G, we are most likely blocking AP1 and AP4 which makes the algorithm think that the position is further away. Since G is the fingerprint furthest away it works quite well. If there would be a fingerprint H that is beyond G then we could expect worse results on G with the static sampling. In general, we found that doing the dynamic sampling helps the worst case a lot, as we can see in Table 3.2 we don't have any 50% performance anywhere. But this is because we are diluting the values by rotating and purposely blocking APs. By doing this we are allowing more leeway in the signal but we will not achieve the perfect accuracy if there never is any blocking of the signal, as is the case at fingerprint A when facing down towards AP3. Furthermore, the dynamic sampling is a better fit for the three doors solution presented in subsection 2.1.3. Since this solution utilizes continuous scanning while the user is walking, there is no guarantee for orientation or location of the user at the time of scanning. Therefore coarser average values are more representative of an area than an exact orientation measurement.

4.2.6 Wi-Fi for Macro Location

As an effect of the scanning throttling mentioned earlier in this section, we had to find a solution that is faster and still works well without too much interaction. We realized that expecting to be able to just press "OPEN VIA WIFI" when you reach the door would not be possible. If we would be scanning continuously and send the latest scan result to the server the data would be old and not representative of the current location. On the other hand, if we instead initiate a scan when reaching the door as the initial idea was, then there is the wait time problem with the passive scanning in Android. The idea was then to instead use Wi-Fi for macro location and let the user decide which door they want to open from the 3 best matches. Undoubtedly, making the user have to choose increases the interaction somewhat from what we initially expected but it delivers good results. Since the signal strength is linear with distance as we see from Figure 3.5, scanning between fingerprint locations still gives good results. Table 3.8 shows how the result varies in these offset locations. We wanted to see how accurate it is when the scan does not occur right on top of the fingerprint as it will rarely be the case when moving to a door. As presented by the results we achieve almost 100% accuracy of displaying the right door in the top 3. Furthermore, as the primary motivator was to reduce wait time at the door we tested the average wait time at a few fingerprints, see Table 3.7. From having to wait a whole scan in our initial solution - which takes around 4-7 seconds - the wait time is instead under 2 seconds on average and there are also a majority of times where there is no wait time at all.

4.3 Magnetic Field Solution

The original idea was to use geomagnetic fingerprinting in the same manner as Wi-Fi fingerprints, i.e. by saving the values at a door location and then the algorithm can calculate the nearest neighbour match when you are in this vicinity. However, as Figure 3.8 shows, the geomagnetic value fluctuates unpredictably in small areas. Essentially, geomagnetism suffers from small scale variations but with no large scale variations. Moving 1m in one direction away from the current value and it is impossible to guess what the value will be. There is no path loss as Wi-Fi has, see Equation 2.1. This meant that if the "OPEN VIA GEO" button is not pressed in exactly the same height and in the same location, there was no guarantee that the fingerprint would be similar. However, what was found is that the signal is extremely stable in the same location. Therefore the solution instead became a set scanning location to open the door as Figure 4.4 depicts.

4.3.1 Geomagnetic Fingerprints

As the variations shown in Figure 3.10 and Figure 3.9 of a completely stationary device, different smartphones show very different stability in the same location with negligible impact of user presence. Fortunately, when averaging the values over 50 samples - which is what is done at the online phase of the geomagnetic solution - the difference is not as severe, see Table 3.10. Especially for the more unstable handset - in this case the One Plus 6 - the decrease is by a factor of 2.73

and 2.71 for the vertical and horizontal component respectively. The findings of Table 3.10 are used to set the required spacing between field intensity values in order to ensure uniqueness. As the intensity varies by up to 2.30μT and 2.18μT, this fact gives ground to a recommendation of placing the fingerprints at least 2.3μT and 2.18μT apart in the vertical and horizontal direction respectively in order to avoid overlapping.
Worth noting is that the example of optimal amount of extracted fingerprints from Table 3.11 discussed in subsection 3.2.8 is rarely a possibility but rather a contextualization to give the numbers some practical weight. This is because all combinations can usually not be achieved practically. To use the numbers in Table 3.11 as an example, 16μT in the vertical component of B might just appear with 35-40μT in the horizontal range, thus limiting a lot of combinations.
It is especially important to have uniqueness of the magnetic fingerprints in scenarios where the two doors are in the same macro location and therefore risk getting included in the results from the Wi-Fi scan. In scenarios where two doors never risk being seen at the same time, e.g. by being placed in different buildings and thus having fingerprints based on completely different APs, this guideline can be completely disregarded and the magnetic fingerprints could theoretically have the exact same value. In Table 3.11 we see this problem of two doors having similar value ranges in quite close locations. There is definitely the possibility that B will be included in a scan at E. Here it is important to avoid the overlapping mentioned in the previous paragraph and place the fingerprint - see Figure 4.3 - in a way that uniqueness is provided.

Despite the sensitivity to positional variations, Figure 3.10 and Figure 3.9 shows the geomagnetic field intensity to be very stable within a fixed location. This is validated in [34] [39] where field intensity over the same trajectories are compared over several days up to three months, as well as measurements performed over the course of this project yielding the same values over several months. This is what allowed the compromise solution of having a dedicated small area where the user would hold her/his phone while opening the door. The physical design and layout of this area can be chosen as desired, for example by a line with an associated icon on the wall adjacent to the door, such as demonstrated in Figure 4.3 and Figure 4.4.

Figure 4.3: Magnetic field fingerprint mobile zone example.

Figure 4.4: Magnetic field fingerprint mobile zone example with phone.

4.3.2 Geomagnetic Solution Compared to Three Doors

At first glance - and in what holds true for certain scenarios - the magnetic field solution is indeed very similar to the solution of displaying the three closest doors. If the three best matches can be determined, is it not better to simply press the door that you want to open, rather than installing a second system and relying on a second algorithm to decide? The answer depends heavily on the environment in which the system would be utilized. In a scenario such as in figure Figure 3.2, the

evaluations show that the three door solution performs well, with only 1.35 seconds of average wait time and 64% attempts with instant success even in the worst case. The absolute worst case scenario here means receiving a Wi-Fi scan just before walking into the zone that would correctly estimate the position, thus having to wait the better part of a new scan (around 6 seconds). The worst case scenario of the magnetic field solution is more common and can be quite hazardous, as it will open a door no matter what. This means that even if the magnetic field fingerprint is a perfect match, if the door is not among the top three results, another door will be opened in its place based on the closest match to the magnetic fingerprint. This would occur every time the three door solution does not result in "zero wait".

Fortunately, the magnetic field solution can be remedied in ways not applicable to the three doors solution. The number of closest doors taken into account can easily be modified, so in theory every single door can be considered in the calculations, although the algorithm obviously imposes a requirement of having magnetic fingerprints that are sufficiently unique, as discussed earlier. This becomes a more scalable option than displaying the closest doors, as such a list quickly becomes inconvenient to use, further aggravated by displayed doors changing order every time a new Wi-Fi scan is completed. For example, an office building where each wing contains up to five separate doors used in the access control system and no other such doors in the area, the program can be modified to consider the five closest doors and thus receive an accuracy of 100% provided the unique fingerprint criteria are met.

4.3.3 Accuracy

To achieve optimal accuracy with the magnetic field solution, a certain amount of domain knowledge is required from the installer, both in terms of layout of the building and regarding limitations and workings of the application. The current geomagnetic field intensity can be displayed in real time on the client phone, allowing the installer to know and decide what values are chosen as fingerprints. The installer needs to match these values with the number of doors in close proximity to each other. Assuming a double sided corridor setup with densely placed doors such as in figure Figure 3.2, each door has five adjacent doors, thus requiring six unique fingerprints. Moving further along the corridor in either direction, the fingerprint values from the opposite side can be freely reused provided they are available.

The largest advantage of the magnetic field solution is the fact that it is able to maintain its accuracy even with doors placed directly next to each other. As table Table 3.2 displays, performance of a purely Wi-Fi based system dwindles with doors placed 4,5 meters in several directions, and with regards to how RSSI values change over distance it is safe to assume that the system would quickly become too unreliable for use with further decreasing door spacing. However, the unpredictability of the magnetic field that poses problems when trying to do general fingerprints works in our advantage when trying to increase accuracy. Since the signal does not change reliably with distance, there is nothing that stops us

from having sub one meter accuracy.

Chapter 5
Future Work

5.0.1 Phone Models and Operating Systems

An important aspect to consider before implementing the system in a real environment is to evaluate how the solutions perform on different operating systems, such as iOS. Furthermore, the Wi-Fi based solution was only tested on a single phone model (OnePlus 6), and the geomagnetic solution tested on two models (OnePlus 6 and Huawei P20 Pro). Issues relating to Wi-Fi might not only include a scan cap as seen in Android 9, but also a variance in received RSSI in the same area depending on the network card of the phone. With the geomagnetism based solution, Table 3.9 demonstrates how the field intensity can vary between phone models and, albeit not warranting a need for improvements or alternate solutions in this case, might do so for other models.

Despite not being explicitly tested, availability on iOS was consciously taken into consideration for the different solutions, and Wi-Fi scanning is available e.g as in Apples own application AirPort Utility[53]. Porting the application to iOS, geomagnetic data can be obtained with the Core Motion framework and the CMDeviceMotion class.[54][55]

5.0.2 Extensive Evaluations

Due to many factors such as limited available suitable test space, Wi-Fi hardware and pure labour cost of carrying out experiments, covering every use case and even establishing an accurate measurement of performance is a difficult task to achieve. The results presented in this thesis give a good indication of how the solutions might perform in different scenarios and provide strong guidelines for what needs to be considered in different situations. However, the sample size of both access point layouts and fingerprint is quite limited, and similar performance in other environments is not guaranteed. An indication of performance can be obtained quite easily by a potential adopter, using the application to create fingerprints as desired within the current network and thereby deciding on which solution is most suitable in the environment, such as magnetic fingerprints if the doors are too densely placed, erecting additional access points if accuracy is poor and so on. If this system is to be implemented in a further extent, it is advisable to validate accuracy in additional office environments.

5.0.3 Improved Algorithms

In this thesis, several relatively simple implementations of different algorithms were combined to achieve the end result. The entire approach was based around producing decent results with an existing technology, and when deemed sufficient, mainly improving it further by adding additional factors rather than refining the single factor solution. For example, when Wi-Fi accuracy worked with sufficient accuracy focus was put on solving the slow scanning rather than improving the algorithm.

One such improvement would be in the probabilistic fingerprinting. The curve is estimated with a normalized gaussian. However, some information could be lost by doing this. M. Lin et al. [58] propose using a polynomial fitting curve instead which might produce a more accurate curve estimation of the data. Another improvement would be to reduce the effects of different phones. Both with the Wi-Fi solution and the geomagnetism, different phones can give different values or accuracy. Utilizing ratios as previously discussed in subsection 2.2.2 is a possibility to counteract different phone models implications. The brute force solution would of course be to have a set of fingerprints for all the popular phone models, the practical feasibility of such a system is up for discussion. Another proposed solution to the problem could be that individual phones stores local fingerprints, if an area is different for a specific phone there could be the possibility to overwrite this position with a local value that is phone specific. How this would work practically is not trivial and needs to be further pursued.

5.0.4 Security Aspects

As mentioned already in the introduction of this thesis, the security aspect was never a focus. We do acknowledge however that for a potential adopter of the system this is obviously a concern. Here we present some implementations that can make the system more secure.
One very real concern is a man-in-the-middle attack where someone would listen on the network and act as either client or server to disturb the system. One way to counteract this could be to introduce full-duplex communication, some handshake that makes sure that the two communicators are who they say. Most commonly this is done by public key exchanges and would be advisable to apply if the system is used in a real application area.
Secondly, a timestamp in the data sent could be used to prevent spoofing done by unauthorized parties. This would limit, for example, unauthorized parties to eavesdrop and reuse correct data sent by valid users.
Using a medium such as Wi-Fi elevates the risks of these attacks since a lot of Wi-Fi networks are public. If possible, limiting the Wi-Fi to private users will also add another layer of security.

There is also the possibility to add more factors to the authentication but then there is a risk that the system loses its simplicity for the user. However, if one was to introduce more factors, a good option would be face detection. These factors could easily be combined if there is a camera at the door, simply done by checking

if the face at the door matches the user that wants to open.
An interesting compromise between convenience and security that is used in a lot of systems is to introduce more factors on different times. For example, an office building could introduce a PIN code outside of office hours on top of the presented solutions.

5.0.5 Alternative Hardware

If the constraint of not adding additional hardware no longer needs to be considered, or if the consumer is installing the system in a brand new location, there are two approaches that stand out in terms of promising performance improvements. These technologies are Round Trip Time (RTT) supported WiFi and Ultra Wide Band (UWB), both of which could employ a similar algorithm to what was used in the WiFi solution.

RTT

WiFi Round Trip Time is a technique that measures the time it takes for a signal to travel between two WiFi enabled devices and back, thus obtaining a measurement of distance between the units. It is stated that a measurement between a client device and 3+ access points likely yields an accuracy of 1-2 meters [57], which would improve the accuracy of the fingerprinting algorithm. The largest advantage however is the possibility to instantly receive the scan results, circumventing the restrictions imposed on the WifiManager API. These scanning restrictions on Android 9, despite the cumbersome workarounds introduced in Android 10, combined with WiFi-RTT being introduced in Android 9 make it seem probable that there is a technological push towards a new standard for Wi-Fi localization. The new standard is called the IEEE 802.11mc standard, which allows for measuring of Round-trip-time (RTT) in Wi-Fi enabled devices.

The downside of this technology is that it is only supported by a handful of devices and even less access points. It is going to take a few years before a lot of buildings support this kind of technology in their access points even if smartphones will have it soon. However, it seems likely to be the more future proof solution as the only step required would in theory be to replace current Wi-Fi access point with RTT enabled hardware, and still being able to use the old scanning methodology until enough clients support the system. As proximity to the office doors still needs to be determined, distance to the relevant access points can the be stored in the same manner as RSSI fingerprints, and the closest match calculated with the same algorithm. With RTT, a deterministic approach with interval values such as $1.5 < x < 2.5$ stored in place of the RSSI value could reach very high accuracy, but further testing would need to ensure that the distance always falls within said interval and in turn that no overlapping occurs.

Ultra-wideband

Another emerging technology for indoor localization than in fact provides even greater accuracy than RTT is the Ultra-wideband (UWB) radio technology. As

described in subsection 1.1.2, UWB is a short range transmission protocol that utilize a broad spectrum of frequencies (>500MHz) to send short pulses that can achieve a localization accuracy as small as 10 cm [44].

For the access control purpose investigated in this thesis, an improved localization accuracy does not always imply a more accurate final product, and precision better than one meter would become superfluous as this level of accuracy would realistically never be needed to discriminate between two door locations. This means that the decision between potential implementation of an RTT or UWB based system mainly becomes a cost related issue, and an evaluation comparing the two options in terms of hardware cost and implementation capabilities would be required beforehand.

Another option provided both by RTT and UWB is to use an access point as a proximity sensor for each door, simply giving access to a user if he/she has pressed the "open" button in the application while being within a set distance of a single AP representing a single door. This would obviously require a much larger amount of hardware to achieve the exact same goal, but is still worth mentioning as the implementation would be the by far most simple, and could be the most lucrative solution if the intended area of use only has a handful of doors to monitor.

Chapter 6
Conclusions

The goal of this thesis was to investigate possible mobile solutions to replace the common RFID + PIN solution for access control. In this endeavor, several solutions have been proposed and evaluated which have proved effective in different aspects.

One of the areas this thesis aimed to explore was if the fingerprinting methodology is applicable without using the traditional grid structure of fingerprints and instead utilize fingerprints only at the doors in question. Since utilizing a grid is mainly for tracking an object, the labor intense process this brings with no guarantee of increased accuracy is superfluous. Placing the fingerprints in the important locations both decreases the manual work and the computational costs while still producing good accuracy.

The accuracy of the Wi-Fi localization is deemed sufficient for the purpose described in this thesis. However, the limitations introduced by Google on the Android API which makes scanning for Wi-Fi slow leaves the original Wi-Fi solution cumbersome. One way to work around these limitations in the API is by scanning continuously and letting the user choose between the three best matches. Another way is to incorporate the inertial sensors in the phone - such as the magnetometer and the gravity sensor - with the Wi-Fi solution to faster and more accurately estimate position.

The placement of the access points matter greatly for the accuracy. The system applied to an existing network has no guarantee to work well. However, by setting up custom access points combined with the existing network, increased accuracy can be achieved. Breaking symmetry with the access point placements is important.

Lastly, the Wi-Fi based solution has room for smooth integration with newer hardware if new buildings are planned or if even finer localization is required in certain locations.

References

[1] S. Boonsriwai and A. Apavatjrut, "Indoor WIFI localization on mobile devices," 2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Krabi, 2013.

[2] Lee, S., Kim, J. and Moon, N. Random forest and WiFi fingerprint-based indoor location recognition system using smart watch. Hum. Cent. Comput. Inf. Sci. 9, 6 (2019). https://doi.org/10.1186/s13673-019-0168-7

[3] M. Wang, W. Zhu, S. Yan and Q. Wang, "SoundAuth: Secure Zero-Effort Two-Factor Authentication Based on Audio Signals", 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, 2018.

[4] B. Shrestha, M. Mohamed and N. Saxena, "ZEMFA: Zero-Effort Multi-Factor Authentication based on Multi-Modal Gait Biometrics", 2019 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 2019.

[5] W. Choi, M. Seo and D. H. Lee, "Sound-Proximity: 2-Factor Authentication against Relay Attack on Passive Keyless Entry and Start System", Journal of Advanced Transportation, 2018.

[6] Dmitrienko A., Liebchen C., Rossow C., Sadeghi AR. (2014) On the (In)Security of Mobile Two-Factor Authentication. In: Christin N., Safavi-Naini R. (eds) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science, vol 8437. Springer, Berlin, Heidelberg

[7] Axis Communications. (2020). Axis A8207-VE. [online] Available at: https://www.axis.com/sv-se/products/axis-a8207-ve/ [Accessed 3 Mar. 2020].

[8] Axis Communications. (2020). AXIS Visitor Access. [online] Available at: https://www.axis.com/sv-se/products/axis-visitor-access/ [Accessed 3 Mar. 2020].

[9] Android Developers. (2020). android.hardware.fingerprint | Android Developers. [online] Available at: <https://developer.android.com/reference/android/hardware/fingerprint/package-summary> [Accessed 3 Mar. 2020].

[10] Android Developers. (2020). android.content.BroadcastReceiver | Android Developers. [online] Available at: <https://developer.android.com/reference/android/content/BroadcastReceiver> [Accessed 22 Apr. 2020].

[11] L. Fan et al., "Visible light communication using the flash light LED of the smart phone as a light source and its application in the access control system," 2016 IEEE MTT-S International Wireless Symposium (IWS), Shanghai, 2016, pp. 1-4.

[12] Metageek.com. 2020. Wifi Signal Strength Basics | Metageek. [online] Available at: <https://www.metageek.com/training/resources/wifi-signal-strength-basics.html> [Accessed 23 March 2020].

[13] S. Boonsriwai and A. Apavatjrut, "Indoor WIFI localization on mobile devices," 2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Krabi, 2013, pp. 2-3.

[14] N. Saeed, S. Guo, K-H. Park, T. Y. Al-Naffouri, M-S. Alouini, "Optical camera communications: Survey, use cases, challenges, and future trends", Physical Communication, Vol. 37, Dec 2019.

[15] Z. Ghassemlooy, P. Luo, S. Zvanovec, "Optical Camera Communications" in Optical Wireless Communications, Springer, pp. 547-568, 2016.

[16] D. Dasgupta, A. Roy, A. Nag, Multi-factor authentication, in Advances in User Authentication (Springer, New York, 2017), pp. 185–233

[17] C. Wang, Y. Wang, Y. Chen, H. Liu and J. Liu, "User authentication on mobile devices: Approaches, threats and trends", Computer Networks, Vol. 170, April 2020.

[18] Docs.oracle.com. 2020. Socket (Java Platform SE 7). [online] Available at: <https://docs.oracle.com/javase/7/docs/api/java/net/Socket.html> [Accessed 25 March 2020].

[19] Docs.oracle.com. 2020. Socket (Java Platform SE 7). [online] Available at: <https://docs.oracle.com/javase/7/docs/api/java/net/ServerSocket.html> [Accessed 25 March 2020].

[20] Sakib, Md & Quyum, Md & Andersson, Karl & Synnes, Kåre & Korner, Ulf. (2014). Improving Wi-Fi based indoor positioning using Particle Filter based on signal strength. 1-6. 10.1109/ISSNIP.2014.6827597.

[21] Shang, J., Hu, X., Gu, F., Wang, D. and Yu, S., 2015. Improvement Schemes for Indoor Mobile Location Estimation: A Survey. Mathematical Problems in Engineering, 2015, pp.1-32.

[22] M. B. Kjærgaard and C. V. Munk, "Hyperbolic Location Fingerprinting: A Calibration-Free Solution for Handling Differences in Signal Strength (concise contribution)," 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), Hong Kong, 2008, pp. 110-116.

[23] Youssef, M. and Agrawala, A., 2007. The Horus location determination system. Wireless Networks, 14(3), pp.357-374.

[24] Bagosi, Timea & Baruch, Zoltan. (2011). Indoor localization by WiFi. 10.1109/ICCP.2011.6047914.

[25] S. Boonsriwai and A. Apavatjrut, "Indoor WIFI localization on mobile devices," 2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Krabi, 2013, pp. 1-5.

[26] Li, Y. (2019). A Probabilistic Approach for Wi-Fi based Indoor Localization.

[27] Android Developers. 2020. Wifimanager | Android Developers. [online] Available at: <https://developer.android.com/reference/android/net/wifi/WifiManager> [Accessed 25 March 2020].

[28] J. Yim, C. Park, J. Joo, and S. Jeong, "Extended kalman filter for wireless lan based indoor positioning," Decision support systems, vol. 45, no. 4, pp. 960–971, 2008.

[29] Docs.oracle.com. 2020. Hashmap (Java Platform SE 8). [online] Available at: <https://docs.oracle.com/javase/8/docs/api/java/util/HashMap.html> [Accessed 25 March 2020].

[30] P. Mirowski, H. Steck, P. Whiting, R. Palaniappan, M. MacDonald, and T. K. Ho, "Kl-divergence kernel regression for non-gaussian fingerprint based localization," in 2011 International Conference on Indoor Positioning and Indoor Navigation. IEEE, 2011, pp. 1–10.

[31] L. Chen, B. Li, K. Zhao, C. Rizos, and Z. Zheng, "An improved algorithm to generate a wi-fi fingerprint database for indoor positioning," Sensors, vol. 13, no. 8, pp.11 085–11 096, 2013

[32] G. Lui, T. Gallagher, B. Li, A. G. Dempster and C. Rizos, "Differences in RSSI readings made by different Wi-Fi chipsets: A limitation of WLAN localization," 2011 International Conference on Localization and GNSS (ICL-GNSS), Tampere, 2011, pp. 53-57.

[33] N. Pritt, "Indoor positioning with maximum likelihood classification of Wi-Fi signals," SENSORS, 2013 IEEE, Baltimore, MD, 2013, pp. 1-4.

[34] B. Li, T. Gallagher, A. G. Dempster and C. Rizos, "How feasible is the use of magnetic field alone for indoor positioning?," 2012 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Sydney, NSW, 2012, pp. 1-9.

[35] H. Yuan, J. Wang, Z. Zhao, J. Cui, M. Yan and S. Wei, "MagWi: Practical Indoor Localization with Smartphone Magnetic and WiFi Sensors," 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, 2019, pp. 814-821.

[36] Android Developers. 2020. Wifimanager | Android Developers. [online] Available at: <https://developer.android.com/guide/topics/sensors/sensors_overview> [Accessed 21 April 2020].

[37] HE, S. and SHIN, K. G. (2017) 'Geomagnetism for Smartphone-Based Indoor Localization: Challenges, Advances, and Comparisons', ACM Computing Surveys, 50(6), pp. 1–37. doi: 10.1145/3139222.

[38] P. Zhou, M. Li, and G. Shen. 2014. Use it free: Instantly knowing your phone attitude. In Proceedings ofthe 20th Annual International Conference on Mobile Computing and Networking. ACM, 605–616.

[39] Wu, H., Mo, Z., Tan, J., He, S. and Chan, S., 2019. Efficient Indoor Localization Based on Geomagnetism. ACM Transactions on Sensor Networks, 15(4), pp.1-25.

[40] Youssef, Moustafa and Agrawala, Ashok and Shankar, A.. (2003). WLAN location determination via clustering and probability distributions. Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications, PerCom 2003. 143- 150. 10.1109/PERCOM.2003.1192736..

[41] M. K. Hoang, J. Schmalenstroeer and R. Haeb-Umbach, "Aligning training modelswith smartphone properties in WiFi fingerprinting based indoor localization," 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brisbane, QLD, 2015, pp. 1981-1985.

[42] Y. Li, S. Williams, B. Moran and A. Kealy, "A Probabilistic Indoor Localization System for Heterogeneous Devices," in IEEE Sensors Journal, vol. 19, no. 16, pp. 6822-6832, 15 Aug.15, 2019.

[43] Alawami, M. and Kim, H., 2020. LocAuth: A fine-grained indoor location-based authentication system using wireless networks characteristics. Computers & Security, 89, p.101683.

[44] J. Blazek, J. Jiranek and J. Bajer, "Indoor Passive Positioning Technique using Ultra Wide Band Modules," 2019 International Conference on Military Technologies (ICMT), Brno, Czech Republic, 2019, pp. 1-5, doi: 10.1109/MILTECHS.2019.8870099.

[45] Apple Support. 2020. Ultra Wideband Information. [online] Available at: <https://support.apple.com/en-ae/guide/iphone/iph771fd0aad/ios> [Accessed 6 May 2020].

[46] H. Liu, H. Darabi, P. Banerjee and J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 37, no. 6, pp. 1067-1080, Nov. 2007, doi: 10.1109/TSMCC.2007.905750.

[47] K. Kaemarungsi and P. Krishnamurthy, "Properties of indoor received signal strength for WLAN location fingerprinting," The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004., Boston, MA, USA, 2004, pp. 14-23, doi: 10.1109/MOBIQ.2004.1331706.

[48] S. Sadowski and P. Spachos, "RSSI-Based Indoor Localization With the Internet of Things," in IEEE Access, vol. 6, pp. 30149-30161, 2018, doi: 10.1109/ACCESS.2018.2843325.

[49] Android Developers | 2020. [online] Available at: <https://developer.android.com/guide/topics/connectivity/wifi-scan> [Accessed 13 May 2020].

[50] Support. 2020. Devices Compatible With Fingerprinting. [online] Available at: <https://indooratlas.freshdesk.com/support/solutions/articles/36000054947-devices-compatible-with-fingerprinting> [Accessed 13 May 2020].

[51] Chao Gao and R. Harle, "Sequence-based magnetic loop closures for automated signal surveying," 2015 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Banff, AB, 2015, pp. 1-12, doi: 10.1109/IPIN.2015.7346765.

[52] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064), Tel Aviv, Israel, 2000, pp. 775-784 vol.2, doi: 10.1109/INFCOM.2000.832252.

[53] Apple Support. 2020. About Wireless Roaming For Enterprise. [online] Available at: <https://support.apple.com/en-us/HT203068> [Accessed 27 May 2020].

[54] Developer.apple.com. 2020. Core Motion | Apple Developer Documentation. [online] Available at: <https://developer.apple.com/documentation/coremotion> [Accessed 28 May 2020].

[55] Developer.apple.com. 2020. Cmdevicemotion - Core Motion | Apple Developer Documentation. [online] Available at: <https://developer.apple.com/documentation/coremotion/cmdevicemotion#//apple_ref/doc/c_ref/CMDeviceMotion> [Accessed 28 May 2020].

[56] Sakpere, W., Adeyeye Oshin, M. and Mlitwa, N., 2017. A State-of-the-Art Survey of Indoor Positioning and Navigation Systems and Technologies. South African Computer Journal, 29(3).

[57] Android Developers. 2020. Wi-Fi Location: Ranging With RTT | Android Developers. [online] Available at: <https://developer.android.com/guide/topics/connectivity/wifi-rtt> [Accessed 28 May 2020].

[58] M. Lin, X. Yubin and Z. Mu, "Accuracy Enhancement for Fingerprint-Based WLAN Indoor Probability Positioning Algorithm," 2010 First International Conference on Pervasive Computing, Signal Processing and Applications, Harbin, 2010, pp. 167-170, doi: 10.1109/PCSPA.2010.49.