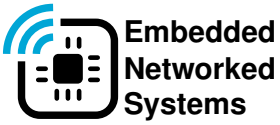
Delft University of Technology
Master's Thesis in Embedded Systems

Novel Interaction Method for UHF RFID Tags

Yaèl Machiel Thijmen Ketel



TU Delft Delft University of Technology

Novel Interaction Method for UHF RFID Tags

Master's Thesis in Embedded Systems

Embedded & Networked Systems Section
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
Mekelweg 4, 2628 CD Delft, The Netherlands

Yaèl Machiel Thijmen Ketel
y.m.t.ketel@student.tudelft.nl
thijmenketel@gmail.com

Thursday 4th July, 2019

Author

Yaèl Machiel Thijmen Ketel

Title

Novel Interaction Method for UHF RFID Tags

MSc presentation

Monday 15th July, 2019

Graduation Committee

Prof. Dr. Koen Langendoen	Delft University of Technology
Dr. ir. Alessandro Bozzon	Delft University of Technology
Dr. ir. Przemysław Pawełczak	Delft University of Technology
Dr. ir. Marco Zúñiga	Delft University of Technology

Abstract

RFID technology is slowly replacing traditional bar codes as a way to identify and track objects and individuals. However, consumer-oriented market penetration has been limited as dedicated RFID readers carry a high start-up cost. Furthermore, *interactions* with the individual tags require special-purpose, handheld RFID readers, instead of ubiquitous devices like smartphones. Simply, traditional smartphones do not have the ability to communicate with the RFID tags off the shelf.

To address this, we propose an interaction system design that utilises fixed positioned RFID readers and common smartphones. This system removes the need for expensive handheld RFID readers to interact with a single tag and in its place uses a small, inexpensive smartphone attachment. The system exploits RF phase measurements in the backscatter communication that is used by RFID systems. By inducing a magnetic field near the RFID tag, the RF phase rotation measured by the RFID reader can be changed and turned into a communication channel.

We implemented a proof of concept of this interaction system consisting of a fixed positioned RFID reader and RF phase modulator, and we evaluate the created communication channel. We reach an average *goodput* of 15 bits/s with a *packet reception rate* of 96 % and an average goodput of 47 bits/s with a packet reception rate of 59 %. However, a raise in the packet reception rate should be possible with a different fixed positioned RFID reader.

Preface

This thesis is the finalisation of my Master's degree in Embedded Systems at Delft University of Technology and was completed at the Embedded and Networked Systems group under the supervision of Dr. Przemysław Pawełczak and Dr. Marco Zúñiga.

The field of RFID and its possibilities is of interest for this group, specifically into batteryless computing. However, exploiting aspects of commercially available RFID systems is a completely new direction. The high cost of conventional RFID readers makes such systems difficult to obtain for small businesses. This inspired me to find less expensive solution. This work presents a proof of concept to demonstrate the functionality of the such system.

I would like to thank Dr. Przemysław Pawełczak and Dr. Marco Zúñiga for their support and guidance during the project, be it technical or personal. I would also like to thank Dr. Yuxiou Hou for his input during the brainstorming sessions and discussions. Further, I would like to extend my thanks to the master and PhD students at the Embedded and Networked Systems group for their input and company during my time there. My words of acknowledgement to the other two members of the graduation committee, Prof. Koen Langendoen and Dr. Alessandro Bozzon, for accepting to attend and judge my work.

I would like to thank my mother and father for their support during the previous years of my education. And finally, Siske Zwiers, for her constant support and care, without which I could not have completed this project and degree.

Thijmen Ketel

Delft, The Netherlands
Thursday 4th July, 2019

Contents

Chapter 1

Introduction

Wireless communication in small embedded devices is usually facilitated by a dedicated infrastructure, e.g. Low Power WiFi [45] or Bluetooth [8]. The most widespread method to implement such a dedicated infrastructure is by using *active* transmitting and receiving radios. A significant problem with systems that use active radios is that they need power hungry components that require batteries or dedicated power sources to operate, which in turn limits the placement and flexibility of deployment (batteries need to be recharged or cables need installation). Furthermore, any required batteries are usually expensive, bulky, unreliable and will require maintenance on a regular basis [23]. To avoid the power hungry components, a form of *passive* communication can be used: radio frequency (RF) *backscatter* [7]. Backscatter devices are usually powered by an RF source and can thus operate without a battery. A backscatter device can change the reflection coefficient of its antenna, which can then be used to send data through the reflected RF waves.

The most well known technology using backscatter communication is *RFID* (Radio Frequency Identification). A typical RFID system operates in the 860–960 MHz frequency band [10] and consist of one or more RFID readers combined with many batteryless tags that harvest energy from radio waves emitted by the reader. The low cost, e.g. 10 cents per tag [39], and batteryless nature of the tags allows for integration in everyday scenarios such as indoor localisation [46] and tracking of objects [50], vibration sensing [51], health care applications such as respiration monitoring [13] and retail inventory tracking [29].

Despite the wide portfolio of industrial scenarios, integration into the consumer-oriented, retail market seems to stay behind. The slow growth can be attributed to any number of reasons. For instance, the price of adoption and replacement of current systems (bar code or other) is high, which makes RFID less attractive for small scale businesses [28]. Another reason is the lack of simple, inexpensive integration with existing consumer

devices used by retail employees such as smartphones, whereas bar codes can be used with low cost scanners and smartphone cameras, RFID tags require an expensive, specialised RFID reader. For instance, a common handheld RFID reader can cost as much as €1700 [34].

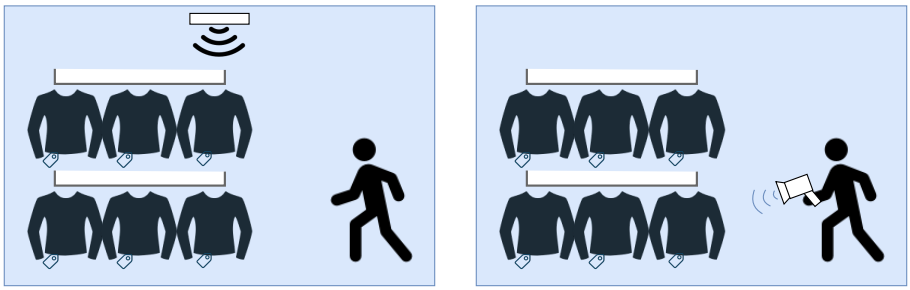
Nonetheless, both the industry and the research community created solutions to integrate existing consumer devices (smartphones in particular) into RFID infrastructure, each with a different approach. For example, many RFID hardware manufacturers, e.g. Alien, Impinj, sell RFID readers that are connected to smartphones via Bluetooth, e.g. Alien ALR-S350 [35], or can be plugged into the headphone jack, e.g. Turck Reader [40], whereas these RFID readers allow the use of smartphones, they also carry high investment and replacement cost with them (€250–€2000).

The research community presented solutions to interact with RFID systems using legacy smartphones. A method communicate with RFID tags through WiFi has been demonstrated by utilising frequency harmonics, which makes tags transmit their ID as a WiFi access point (TiFi) [2]. However this solution is far from functional as it requires operation outside the UHF RFID frequency band. Therefore, there is still a long way ahead in enabling RFID technology ubiquitously.

1.1 Challenges of RFID Infrastructures

The cost of RFID systems for the end user is a function of the size of the area that needs to be monitored. As the area increases, so does the number of RFID readers. RFID systems are implemented in a number of different ways, depending on scenario and application. For example, in a retail scenario, e.g. clothing store, bookshop, every product is tagged and documented in a database (i.e. every item with a tag is connected to an ID number in the memory of the tag). This way the retailer can keep track of the inventory. The retailer has the choice to either use multiple handheld RFID readers, e.g. Alien ALR-S350 [35], or use a fixed RFID reader, e.g. Impinj R420 [16], to manage the inventory, with each its own trade offs:

- **Multiple handheld RFID readers:** A handheld reader has the ability to query tags which are in close proximity, which allows the user to interact with individual products in a somewhat fine-grained way (see Figure 1.1b). The user simply moves the RFID reader close to the tag and the tag can be queried. However, to keep track of items in the inventory (in case of a sell or return for example), the retailer is required to perform regular, manual inventory counts by walking through the shop and scanning each tag. Furthermore, if the retailer has a many employees, the cost and maintenance of many handheld readers is high. For example, with a popular RFID reader such as the



(a) *Fixed reader* ***(b)*** *Handheld reader*

Figure 1.1: *Two possible scenarios for retail RFID integration, each with their own trade-offs. A fixed reader (Figure 1.1a) is enabling continuous inventory management but not able to query a single tag without knowing its ID. Handheld readers (Figure 1.1b) can query single tags with precision but cannot perform continuous inventory management.*

Alien ALR-S350, the cost of five devices (for five employees [1]) is over €7000 [35].

- **Fixed-positioned RFID readers:** When a retailer decides to use a fixed-positioned RFID reader, regular inventory counts are not necessary as fixed RFID readers can keep track of an inventory at all times (see Figure 1.1a). However, interactions with individual products will not be possible with a fixed RFID reader as the reader is unable to be moved. To perform an interaction with individual products, a tag has to be taken away to isolate it or a single handheld RFID reader might be needed, which is another expense that grows with the amount of employees. For example, the cost of jointly using a popular fixed RFID reader such as the Impinj R420 with a popular handheld reader, exceeds €2800 [35, 38].

The factors mentioned above lead us to the following research goal.

1.2 Research Goal

Our goal is to enable interaction with *existing* RFID infrastructure (readers and tags) via legacy smartphones. We want to replace the handheld RFID readers (some attachable to smartphones) with a device that is orders of magnitude cheaper. We are able to do that thanks to the observation that information can be *embedded* in existing RFID reader to RFID tag communication. If we could *modulate* this information (by means of perturbing the phase of amplitude of the RFID reader signal) our goal would be achieved.

1.3 Contributions

This has lead to the following key contributions:

- Development and hardware implementation of a transmitter circuit that can influence the measured RF phase rotation in RFID systems. The circuit is simple in its design and uses low cost components to enable customisability and easy integration.
- New protocol based on the use of the designed transmitter. The design includes packet structure, encoding and error detection and correction.
- Development and implementation of RFID software that is able to decode and interpret the modulated RF phase rotation samples. The signal processing chain and data interpreter are integrated with the RFID interface software.
- Evaluation of the effect that the transmitter has on the RF phase rotation and an evaluation of the system's effectiveness and goodput at different bit periods. We demonstrate an average goodput up to 15 bits/s with a packet reception rate of 96 % and an average goodput up to 47 bits/s with an packet reception rate of 59 %.

1.4 Thesis Outline

This thesis is organised as follows: Chapter 2 presents related work that tackles similar problems and topics that inspired this work and Chapter 3 covers the basic concepts and topics related to RFID systems and backscattering. The design choices and implementation details are described in Chapter 4 which is followed by the evaluation of the system in Chapter 5. In Chapter 6 the limitations that presented themselves during the project as well as possible future directions for the project are discussed. Finally, the conclusions drawn from the thesis are presented in Chapter 7.

Chapter 2

Related Work

To place this work in context, this chapter gives a summary of known state of the art research and papers. Alternative applications for established technology and infrastructures is covered extensively in literature. Systems that interact with RFID specifically are presented in Section 2.1, systems that enable alternative communication through an existing platform like smartphones or displays, are covered in Section 2.2 and systems that use RFID specifically in a novel way are Section 2.3.

2.1 RFID Tag Interaction

Interaction with RFID systems is extensively researched by the industry as well as the academic community. As mentioned in Chapter 1, the approach taken by the industry is to develop dedicated, RFID protocol specific, e.g. EPC Class 1 Gen 2 [10], handheld readers at high cost [37]. However, the approach that is taken by the academic community is based on exploiting the existing hardware and infrastructure to interact with RFID tags (possibly without use of handheld readers). We will now review the most relevant contributions.

2.1.1 Location Based Systems

A method to interact with an RFID tag *without* the need for handheld RFID readers, is to locate it relatively to a *fixed* reader. When the fixed RFID reader has determined the position of the tag, a person can then locate a specific tag and interact with it.

A method to locate a single or multiple tags has been explored in several different papers, notably LANDMARC [22], PinIt [47] and Tagoram [50]. These papers can be divided into two separate methods of localisation: RSS-based (LANDMARC, PinIt) and RF Phase-based (Tagoram). LANDMARC is able to determine the position of a tag based on the location of reference

tags that are nearby. By comparing RSS (received signal strength) of the tags, neighbouring tags can be located. However, the method is accurate up to 600 mm and suffers from variation between tags, antenna gain and orientation. PinIt improves on LANDMARC by using a special antenna to emulate an antenna array and comparing a multipath profile to reference tags placed in the space. This method increases accuracy to 11 cm and impoves non-line of sight performance, but requires a special antenna and a priori placed reference tags to achieve it's goal. Tagoram presents a system that utilises the phase values of the backscattered signal that is provided by the RFID reader. The tracking of mobile tags has shown to be possible within a 5–8 mm median location error.

While location-based systems allow users to locate a specific tag based on its ID number, interaction with, to the user, unknown tags is not possible this way. Our work aims to allow interaction with tags without the needs for the user to know the ID number of that specific tag.

2.1.2 Touch-Based Systems

If a central RFID reader can detect when an RFID tag is touched, more granular interaction is possible. This way a user can select a single tag and signal to the central RFID reader which one, without knowing the touched tag ID number.

Methods that allow RFID readers to detect a touch interaction are presented in IDSense [18] and RIO [26]. IDSense presents a method to detect when a tag is touched based on an RF phase change in the backscattered signal. The system uses a Support Vector Machine (SVM) to detect and classify several different tag touch interactions. The SVM is trained by 600 labelled touch interaction instances and achieves a 97 % accuracy. RIO presents a system that allows users to create a touch interface out of RFID tags which is able to detect touches and swipes. The system is able to achieve this without extensive training of a model, but a simple four swipe calibration. By comparing RF phase values to calibrated data through Dynamic Time Warping (DTW), the position of a finger on a tag can be determined. The system is able to detect a touch on a single tag with up to 100 % accuracy and tracking the position of a finger on a tag with a median error of 3.8 %.

While both presented systems allow for accurate detection of touch, a touch is still a simple, analogue interaction. Our work aims to extend the interaction to actual digital data transmission opposed to an inaccurate, analogue solution.

2.1.3 Cross-Technology Communication

The problem with most systems that try to interact with RFID tags is that they usually require additional hardware or only allow simple interaction. A

solution might be to use ubiquitous devices such as smartphones. However, to make such an idea feasible, technology boundaries have to be crossed.

The system presented in TiFi [2] allows RFID tags to broadcast their EPC ID as a WiFi access point, which can be detected by modern smartphones. By exploiting harmonics of the carrier wave of RFID, tags can broadcast their tag ID as an SSID (access point name) on the 2.4 GHz band that is used by WiFi. The tags broadcast their SSID name only in a near field (within 2 m), which provides local interaction with tags without the need for expensive handheld RFID readers. While TiFi seems to offer a robust solution, the system has its flaws. Firstly, the maximum frequency at which the harmonic effect can be exploited is 828 MHz, which is well below the standardised frequency band of 860–960 MHz [10] that RFID uses. The robustness of the RFID tags allows them to still operate in such a low frequency range, but is not allowed for RFID readers. Secondly, as all near field tags are detected by the smartphone, single selection of an RFID tag might not be possible which limits the interaction possibilities.

2.2 Alternative Applications for Established Systems

The meaning of *alternative applications* in this context can be defined as any way to interact with or build on an existing platform, i.e. device or system, to allow additional functionality.

2.2.1 Interactions

An example of interaction extension that allows additional functionality is VSkin [41], which demonstrates touch gesture sensing on all surfaces of a mobile device. This is achieved through sensing based on acoustic signals inside and outside of the device. By measuring both the amplitude and phase of each path of sound, the system is able to detect tapping events with 99.65 % accuracy and finger movement with an accuracy of 3.59 mm. As mentioned above, IDSense [18] and RIO [26] also enable interaction based on existing platforms.

As the systems mentioned here only allow basic interaction, e.g. a single touch or gesture, it limits the functionality by not allowing to transmit digital data.

2.2.2 Digital Communication

A more complete extension to existing platforms would be an enabling of actual data transmission. Systems like Bioamp [12], Touch-And-Guard [48], Ripple [31], Ripple II [30] and Shadow [52] all utilise a feature of an existing

platform to transmit data. Each of the mentioned systems exploit an existing platform in a novel way to facilitate data transmission:

- Bioamp [12] modulates the natural capacitance of the human body through a wristband to create a communication channel from a finger to a touchscreen. The touchscreen device can sense the change in capacitance on the finger which is used to transmit authentication data. Through this system a user can be continuously authenticated to make sure no unauthorised persons are using the touch device. Achieved data rates through the touchscreen itself are 12 bits per second but can be increased to 2 kilobits per second if an external ECG electrode connected to the headphone jack is used.

- Touch-And-Guard [48] attempts to established a secure connections between a wristband and a touched device through hand resonant properties. By using vibration motors and accelerometers secret bits can be exchanged between a user wearing a wristband and a device with an accelerometer. This system achieves a data rate of 7.84 bits per second, which is faster than putting in a regular pin code and more robust to eavesdropping.

- Ripple [31] is a system that, like Touch-And-Guard, exploits the vibration motors and accelerometers in mobile devices to create a communication channel. However, Ripple allows for two way communication as two phones have vibration motors and accelerometers. The system can reach up to 80 bits per second with regular phones and up to 200 bits per second on of the shelf vibration motor chips. Ripple II [30] improves on Ripple by exploiting the microphone as a receiver instead of the accelerometer. Furthermore, by using more dedicated hardware the bit rate is increased to 30 kilobits per second.

- Shadow [52] exploits electromagnetic radiation (EMR) that is emitted by displays to transmit information. By modulating the high-frequency signals in the display interface the emitted EMR falls into the FM band. Phones (that carry an internal FM receiver) can then receive the information. The system achieves a throughput of 1.5 kilobits per second at 20 cm without modifications to the hardware of the display.

The systems mentioned above all exploit existing hardware or infrastructures to create alternative communication channels. As most of them are in a proof of concept state the throughput is well below the throughput of existing systems as WiFi or NFC. However, the created side channels can facilitate unusual and novel applications without modifications to the underlying infrastructure.

2.3 Novel RFID Applications

Aside from the more directly applicable systems proposed in Sections 2.1 and 2.2, some state of the art papers explore the possibilities that RFID systems may allow in the future. Some examples of novel applications using RFID are:

- Tagbeat [51] presents a system that is able to detect the frequency of a vibrating object that is tagged with an RFID tag. As the read rate of modern RFID systems is not high enough for regular sound sampling, Tagbeat developed a version of compressive sampling which they call compressive sensing. The system can recover a vibration frequency up to 1 kHz with a relative error rate of 0.03 %.

- Tagbreathe [13] exploits the precise movement detection in RF phase rotation of backscattered signals to recover the respiration rate of a person with an RFID tag on its chest. Which it can do with an accuracy of up to 95 % depending on the scenario, orientation and number of users.

- The work presented in Tagyro [49] proposes a system to determine the orientation of an object that is tagged with RFID tags. The system relies on the relative RF phase rotation between tags to determine the orientation and change of orientation of an object. The system reports a small error of 4° on average.

- RF-Mehndi [53] employs multiple RFID tags as a passive personal identifier. A grid of nine tags is connected to a conductor at the exact same point and the exposed area of the conductor can be touched by a fingertip. By relying on the relatively stable and unique internal resistance of the human body, different users might be distinguished by their impedance. Evaluation with 15 individuals achieve promising authentication accuracy of 99 %.

The research presented above are examples of systems that build on existing technology to create novel applications.

2.4 Comparison to State of the Art

To position this work in its context, specifically tag interaction, it is important to compare it with the different solutions that have been introduced. Our system aims to reduce the cost of RFID infrastructure by introducing a novel method to interact with tags (the specifics of the system design can be found in Chapter 4).

	Fine grained	COTS	Digital interaction	Low cost
RFID reader	✓	✓	✓	✗
RIO [26]	✓	✓	✗	✓
IDSense [18]	✓	✓	✗	✓
TiFi [2]	✗	✗	✓	✓
LANDMARC [22]	✗	✓	✗	✓
PinIt [47]	✓	✗	✗	✓
This work	✓	✓	✓	✓

Table 2.1: *Comparison with existing systems that allow interaction with RFID tags.* Fine grained *means that a tag can be selected by the user without the need to know the tag ID,* COTS *means the system is build on commercial hardware and* digital interaction *means that the system can either query or interact meaningful with the tag.*

In Table 2.1 some important properties are compared across different solutions. Some of the interesting ones are *expense* and commercial availability (commercially of the shelf, *COTS*), which make a big impact on adaptability of a solution.

Chapter 3

Background

This chapter gives background information regarding the topics covered this thesis. The fundamentals of RFID and UHF RFID are covered in Section 3.1 and RFID sensing and RF phase measurements are explored in Section 3.2.

3.1 Radio Frequency Identification

While the field of RFID is made up of several different version and standards that use different frequencies, ranges and tag types, the basic building blocks are generally the same. The following sections give an overview of the different RFID versions (Section 3.1.1) and explore the version used in this thesis (Section 3.1.2).

3.1.1 Basics of RFID

The roots of RFID can be found in a listening device from the 1950s: The Thing [21]. This device allowed speech to modulate the impedance of an antenna which in turn influenced the reflection of a carrier wave. By demodulating the reflection of the carrier wave, eavesdropping on conversations could be achieved without a battery powered microphone. This method is considered the basis for the creation of most modern RFID systems as we know it today.

The basic building blocks of an RFID system are an interrogator (or reader) and a transponder (RFID tag, microchip with an antenna). The RFID reader transmits a carrier wave on which the tag will modulate their identification information through *On/Off Keying* (OOK). The tag is able to do this by switching the antenna connection through one of two different resistance routes[1] which will change the reflection characteristics of the tag

[1] In modern tags this is done by shorting the antenna, which leaves the tag without power during this state.

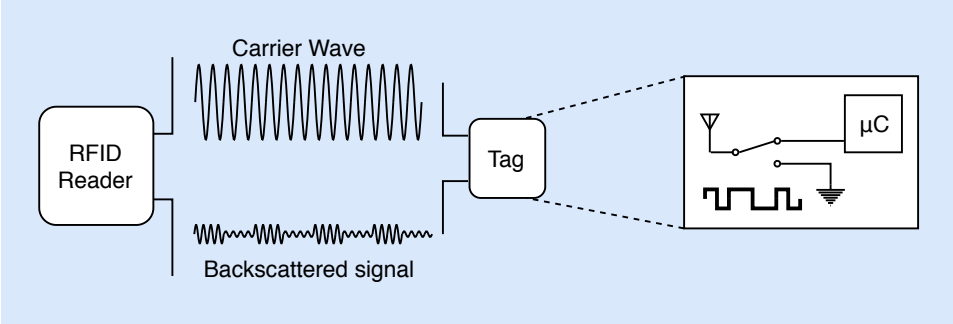


Figure 3.1: *Basic principle of RFID backscatter: on-off keying a shorted connection at the antenna to change the reflection of the tag.*

(see Figure 3.1). The reader is able to recover the modulated reflection of the carrier wave and extract the information that the tag transmitted.

While the basic concept behind RFID is the same for most versions, the specific implementation can vary widely. The most common versions that are used are differentiated from each other by the frequency range that is used: LF (Low Frequency), HF (High Frequency) and UHF (Ultra High Frequency). Roughly all modern RFID systems operate in either of these three frequency bands. The lowest band (LF) has its center frequency at 125 kHz and has a maximum range of around 50 cm. These RFID systems are generally used for building access control and animal tagging. The HF version has its center frequency at 13.56 MHz and has a maximum range of about 1 m. These tags allow for higher data rate and extended functionality such as NFC (which enabled contactless payment cards) [5, 9].

All the mentioned RFID systems support either passive or active tags. When a tag is passive it will be powered by the carrier wave from the reader and is thus *batteryless*. An active tag usually has a transmitting antenna and a battery which allows it to transmit its information without the presence of a carrier wave.

3.1.2 Ultra High Frequency RFID

For this thesis the UHF RFID system is used, which operates in the 860–960 MHz frequency band and has a range of around 10 m [10]. The range, small size and low price make UHF RFID tags the go-to standard for large scale industry, healthcare monitoring application and managing retail inventory [17].

EPC Class 1 Gen 2

The main application envisioned for UHF RFID was supply chain management. Low cost and high range make the tags ideal to tag a product by

the manufacturer and be tracked throughout a supply chain. Compared to old style barcodes, which require line of sight, RFID tags represent a more robust and flexible solution. To reach such a goal, manufacturers realised that interoperability between different brands of RFID tag was essential. Therefore an organisation was created to standardise UHF RFID systems: EPCglobal. The most popular version of the UHF RFID standards is the EPCglobal Class 1 Generation 2 protocol (EPC C1G2) [10]. The protocol is based around the *Electronic Product Code*, which is meant as an identification code for individual products and can be stored on RFID tags or represented as a barcode.

The EPC C1G2 protocol describes the use of the UHF band to communicate with the tags and which communication standards the readers and tags should use. The specific frequencies that RFID readers will use is dependent on location, which can essentially be either one of two frequency bands: the 865.6–867.6 MHz range (ETSI regulations, European territory) and the 902–928 MHz range (FCC regulations, USA territory). However, unlike the regional regulations for RFID readers, the RFID tags are usually able to operate in any of the regions.

Anti Collision Protocol

An RFID system has two methods to prevent interference: *spread spectrum frequency hopping* and the *slotted ALOHA* protocol.

The former is aimed at reducing the probability that two RFID readers interfere with each other on the same frequency. By randomly hopping through different frequencies, the probability that two RFID readers transmit on the same frequency at the same time is drastically reduced. The frequencies depend on the operation regions' regulations.

Due to the batteryless nature of the RFID tags, no synchronisation is possible between tags, which means tags will respond whenever they can (ALOHA protocol). The problems arise with a large number of tags, which will cause many collisions because data frames have a larger change to overlap. When data frames overlap and collide the data is lost. To reduce the probability of collision, the slotted ALOHA protocol is used. Slotted ALOHA divides the time into discrete time slots where the size corresponds to the length of a data frame. Tags then wait for the start of a time slot to transmit their data. This system reduces the change that a collision between tags occur, however it does not completely eliminate interference as tags can still respond in the same time slot.

3.2 RFID Sensing

Modern RFID readers have the capability to report more than just the tag ID of RFID tags. Information about the signal strength (RSSI), RF phase

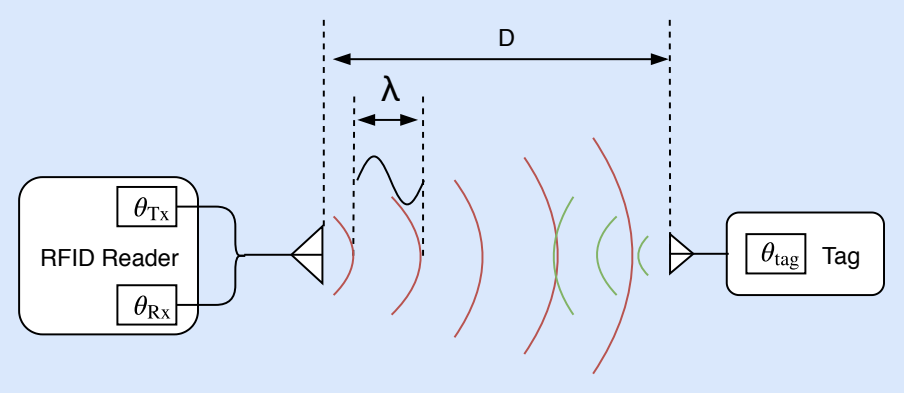


Figure 3.2: *Radio wave propagation between RFID reader and RFID tag*

rotation of the reflected carrier wave and Doppler shift of the carrier wave are some examples. The related work presented in Chapter 2 as well as the work presented in this thesis, exploit this information in their innovations. This section will focus on the RF phase rotation measurement that the RFID reader reports.

3.2.1 RF Phase Measurement

The RF phase rotation measurement that the RFID reader reports is calculated from the reflected carrier wave, which is visualised in Figure 3.2. Suppose the distance between the RFID reader antenna and the RFID tag is represented by D, the total distance that the carrier wave traversed will be $2D$ and the phase rotation can then be defined as

$$\theta = \left(2\pi \times \frac{2D}{\lambda} + \theta_{\text{tag}} + \theta_{\text{Tx}} + \theta_{\text{Rx}}\right) \mod 2\pi \tag{3.1}$$

where λ is the wavelength of the carrier wave, and θ_{tag}, θ_{Tx} and θ_{Rx} represent the additional phase rotation induced by the circuitry of the tag and the transmitting and receiving circuits of the reader. The measured RF phase rotation repeats with a period of 2π every $\frac{\lambda}{2}$ in the direction of the backscatter communication. RF phase rotation is also influenced by a lot of environmental factors such as movement of the tag itself, movement around the tag and touching the tag.

3.2.2 Impinj RF Phase Reporting

The Impinj Speedway R420 UHF RFID reader that is used in this work has the capability to report RF phase measurement with 12 bit accuracy [15]. This means that the maximum value of 4096 equals 2π and the accuracy in radians is $\frac{2\pi}{4096} = 0.0015$. This gives a theoretical accuracy in detecting

movement of 39.9 µm (at a frequency of 915 MHz). However, Impinj notes a standard deviation of ±0.1 radians [15], which translates to ±2.6 mm. While this reduces the accuracy of the RF phase reporting slightly, this reduction does not reduce the effectiveness of the system presented in this work. Experiments going into the accuracy of the RF phase reporting have been performed for this work and can be found in Appendix A.

Chapter 4

Design and Implementation

As covered in Chapters 1 and 2, current solutions to interact with RFID tags are either expensive or limited, which requires the development for a new system. In this chapter the design choices and implementation details are covered for the different components in the system.

4.1 System Overview

The system architecture, as presented in Figure 4.1, envisions a completed infrastructure that requires components that are not included in this work, as these require a significant engineering effort to develop without adding to the scientific contribution. However, the components that this thesis cover are the following: RF phase signal processing and data decoder (controller program or receiver) and the RF phase modulator and data encoder (Arduino and inductor). The server backend and smartphone application are not in the scope of this work, these were developed as a parallel project to this work and has been reported in [3]. Later on in this project we will refer to some results from that implementation.

4.1.1 Interaction Design

The design of the system has been made with a certain progression of actions in mind.

When looking from the perspective of a user, all interaction will be performed through a smartphone with an inexpensive attachment. This is visualised in Figure 4.2 as a series of actions on the smartphone. When a user wants to interact with a tag he holds the attachment near (within 2 cm) of the tag and presses a button in the smartphone application. When this happens a notification gets send to the server to expect a transmission. The smartphone will then initiate the attachment (transmitter) to send the selected data. The data can be anything the application requires, such as

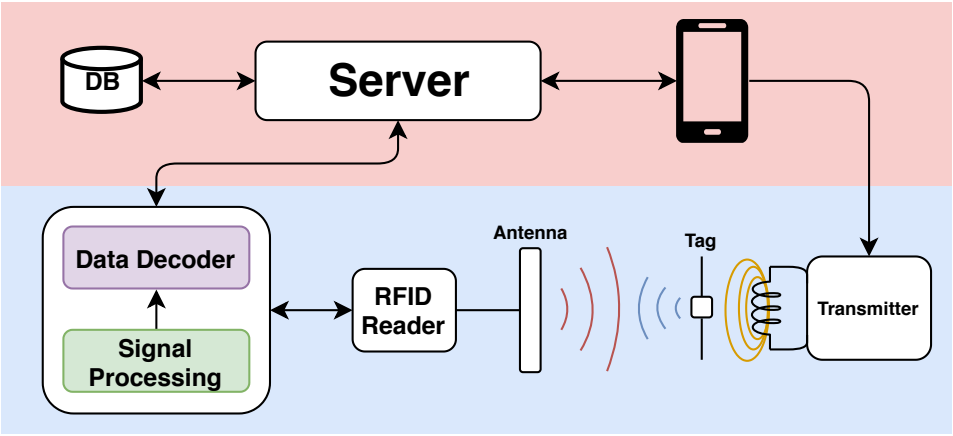


Figure 4.1: *Overview of the system. The section in red (top part) is not implemented in this work, the section in blue (bottom part) is implemented. The circular lines near the transmitter represent an induced magnetic field.*

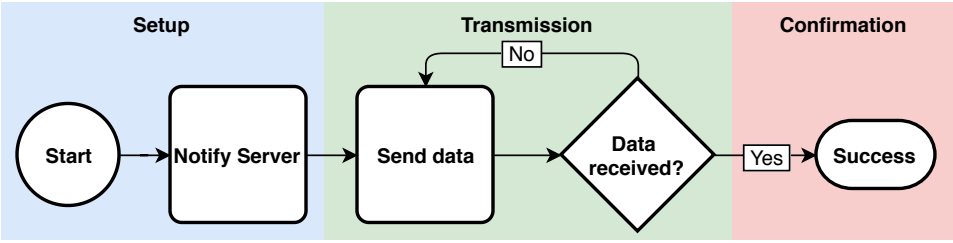


Figure 4.2: *Interaction progression as seen from the perspective of the smartphone.*

the ID of the smartphone's owner or a certain predefined command. The transmitter then modulates the data on top of the regular communication between the reader and the tag. The software behind the reader then decodes the modulated data from the RF phase values and sends it to the server. When the server receives data from the RFID reader, it notifies the smartphone with a confirmation that the intended data has been received. When data is not received, the server will request the smartphone to send the data again.

4.1.2 System Components

The system is primarily designed for digital communication, this means it consists of a *transmitter* and *receiver*. The implementation of the transmitter and receiver on top of the existing RFID infrastructure can be divided into several separate components:

- *Transmitter* (Section 4.2): this part consists of a circuit design and

data encoder to digitally influence the RF phase measurement.

- *Signal processing chain* (Section 4.4): this part processes the raw RF phase values before they can be interpret to extract the encoded data.
- *Data decoder* (Section 4.5): this part takes the processed RF phase values to extract the encoded data.

4.2 Transmitter

In Section 2.1 the related works only allow analogue interaction with RFID tags. To make the interaction controlled and digital, modulation of the RF phase needs to be more controllable. This section will explore the effects on RF phase and presents a method and *transmitter* circuit design to modulate RF phase values.

4.2.1 Effects on RF Phase

The first step in controlling the RF phase change is to determine what affects the actual phase values. As mentioned in Section 3.2.1 the RF phase parameter is dependent on several factors in the system: distance from the antenna to the tag (D), wavelength (λ), phase rotation induced by the reader transmit and receive circuitry (θ_{Tx} and θ_{Rx}), and the tag circuitry (θ_{tag}). In a regular RFID system set up, θ_{Tx}, θ_{Rx}, θ_{tag} and λ are constant (aside from the frequency hopping effect), however D will fluctuate. Usually tags are moved around which will change the value of D. However, the overall phase can also be influenced by activity around and position of the RFID tag itself. Multipath fading has a strong influence on the measured phase values. Fortunately, changes of D and influences by multipath fading are relatively slow compared to the effect of the transmitter (in Figure 4.1), which means they are easy to ignore. The changes in D can be used for applications such as localisation, examples of which are presented in Section 2.1.1.

Effects on RFID Tag

Many examples of state of the art work exploit the D value in the phase measurement for localisation or motion tracking (see Section 2.1.1), however the phase rotation induced by the RFID tag (θ_{tag}) can also be changed. This is shown by RIO [26] where the impedance of the RFID tag antenna is changed by human touch. The impedance which is inherent to the human body will add to the impedance of the tag antenna itself, which will change the current running through the antenna. When the current changes in the tag antenna, the reported RF phase will change as well. This current can be expressed as [4]:

$$I_{\mathrm{m}} = -\frac{E_{\mathrm{inc}}}{(Z_{\mathrm{L}} + Z_{\mathrm{A}})\beta \cos^2\left(\frac{\beta L}{4}\right)} \tag{4.1}$$

where I_{m} is the maximum current along the antenna, E_{inc} is the incoming electric field, Z_{L} and Z_{A} are the IC's and antenna's impedances respectively, β the free-space constant and L the length of the tag's antenna. When the antenna is touched, the effective impedance Z_{A} is changed, which changes the current I_{m} and in turn the reflected electric field. This means that the effective change in phase of I_{m} will result in a change in the measured RF phase at the RFID reader's side.

4.2.2 Enabling Digital Interaction

While touching a tag will result in a very consistent reaction in RF phase measurement, the interaction itself is analogue. No more meaningful information can be transmitted through touching a tag other than a single binary interaction. To extend interaction to more reliable, *digital* interaction requires a different method to change the measured RF phase.

Controlled Modulation

To achieve a digital interaction with the RFID tag, we propose to directly influence the current in the tag's antenna (I_{m}) as opposed to the impedance of the antenna (Z_{A}). By creating a changing magnetic field near the tag's antenna a current can be induced that adds to the existing current in the antenna. As determined in RIO [26], when the phase of the current in the tag's antenna (I_{m}) changes, a corresponding change in the RF phase occurs.

To test the hypothesis stated in Section 4.2.1 and see if a magnetic field near a tag has an effect on the RF phase measurements, a circuit needs to be designed. In the interest of keeping the system simple and low cost, the circuit only contains cheap components and does not require a complex microcontroller. In Figure 4.3 the basic design is shown.

Modulation Circuit

For the actual implementation an Arduino Nano takes the place of the simple microcontroller. The RFID tag that is used is an Avery-Dennison AD-236u7 [6] commercial RFID tag with a NXP UCODE 7 [32] IC. As there is no extensive electromagnetic radiation (EMR) investigation done in this work, no specific coil design is chosen. For the final implementation a tightly winded coil is used as the inductor L. This inductor is made from copper wire (0.5 mm thick) with approximately 40 windings and is circularly shapen with an inner diameter of 30 mm and an outer diameter of 38 mm (this is shown in Figure 5.2). By pulsing a current through the coil via simple

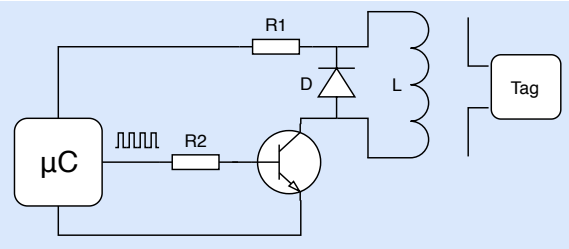


Figure 4.3: *Circuit to influence the current running trough the tag antenna. The µC (microcontroller) is connected through a current limiting resistor R2 (120 Ω) to the base of the NPN-transistor (BC547). The source is connected to an inductor (L) with a flyback diode D (1N4001 diode) to prevent voltage spikes. The overall current through L is limited by R1 (22 Ω).*

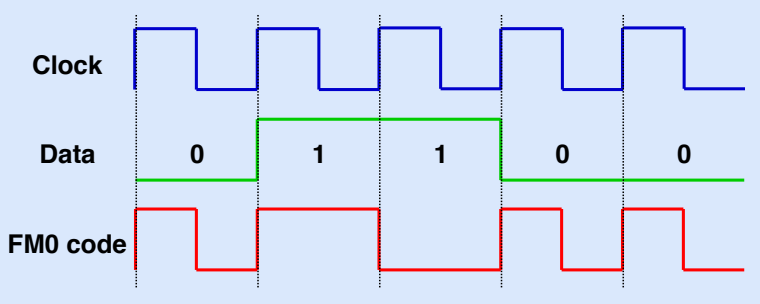


Figure 4.4: *Biphase-S (FM0) encoding of a sequence of bits.*

on/off-keying (OOK), the measured RF phase is modulated. The effect can be seen in Figure 4.8: the shift is small (< 0.5 radians) but large enough to be detected.

4.3 Packet Structure and Encoding

To make the transmitter designed in Section 4.2 actually work, it requires a robust encoding schema (Section 4.3.1) and packet design (Section 4.3.2).

4.3.1 Data Encoding

To encode the data the system utilises simple OOK to influence the measured RF phase and create a line code. Due to the nature of the system the value of the RF phase can drift over time due to factors around the tag (see Section 4.2.1), which makes differentiating between a digital "low" and digital "high" state difficult. To deal with these drifts a line encoding schema needs to be used that can clearly differentiate between bits.

Taking inspiration from the encoding schemas used in the actual EPC

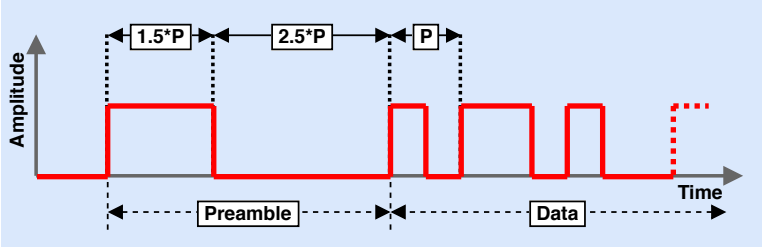


Figure 4.5: *Structure of the preamble, P represents the length of one bit. The length of the preamble parts is designed to be distinguishable from regular bits.*

C1G2 protocol, we chose *Biphase-S* (also known as FM0) encoding [25]. This encoding scheme always has a transition between each bit and an extra transition in the middle of a "zero" bit. This is visualised in Figure 4.4. This encoding schema ensures that there will always be a transition between bits and thus allows decoding by just looking at transitions, regardless of the polarity of the signal.

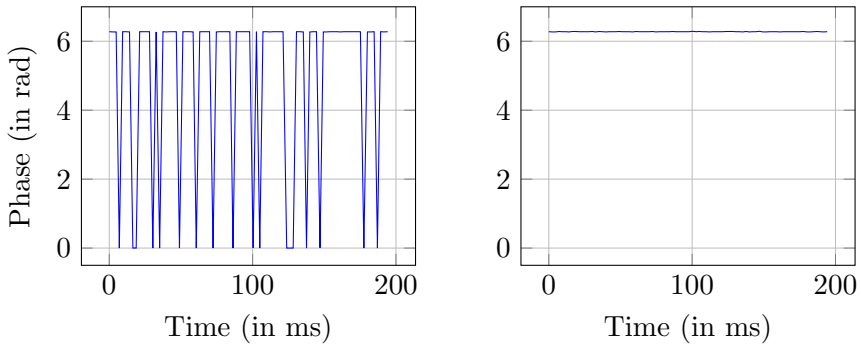
4.3.2 Preamble Design

To make data frames detectable in a sequence of RF phase values that can be noisy, a clearly distinguishable preamble has to be used. Furthermore, unlike some systems that use regular predetermined bit streams as a preamble, the design here should be easy to differentiate from regular data bits. This condition is to make sure the preamble is not mistaken for bits and bits are not mistaken for the preamble.

The choice made here is to make a short but recognisable shape with pulses that are longer than a bit period. Furthermore, the shapes have to be distinguishable enough so that noisy in the RF phase signal is not mistaken for them. This lead to the design shown in Figure 4.5, where P is the period of a single bit for reference. The two parts of the preamble are both distinguishable from a regular data bit and by placing the larger part ($2.5 \times P$) after the shorter part ($1.5 \times P$), there will be a clear border between the preamble and the data. Furthermore, due to length of the two parts, they are easy to distinguish from each other and cannot be mistaken for each other.

4.3.3 Error Correction and Detection

To detect and possibly correct the inevitable errors that will occur in the communication channel, some error correction and detection should be implemented. As the projected bit rate is quite low, a simple code should be sufficient enough without adding much overhead. With simplicity in mind



(a) *RF phase before unwrapping.* ***(b)*** *RF phase after unwrapping.*

Figure 4.6: *Unwrapping RF phase values to remove inconsistencies created by the periodical nature of the RF phase.*

we chose to implement *Hamming Error Correction* coding with additional parity bit (also known as *SECDED* (Single Error Correction, Double Error Detection)) [11]. As the name says this code can correct single bit errors and detect double bit errors.

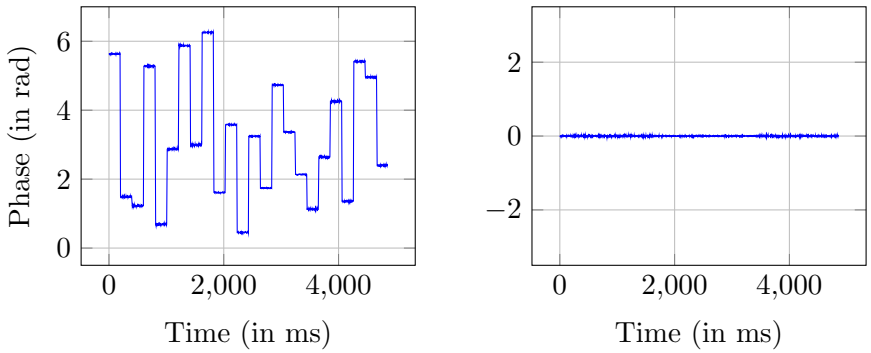
4.4 Signal Processing

The RFID reader that is used in this work is the Impinj Speedway Revolution R420 [16], a modern, high-end RFID reader that supports over 1100 tag reads per second. The raw phase values that the RFID reader reports require several stages of signal processing before they can be interpreted. Aspects like phase wrapping, frequency hopping and general noise need to be addressed to make the data useful.

4.4.1 Phase Unwrapping

As mentioned in Section 3.2.1 the RF phase values are periodical with a period of 2π, which means at the edge cases when the values are close to 0 or 2π it wraps around. This is shown in Figure 4.6a, which shows the wraparound effect. To correct the behaviour around the 0 and 2π points, the phase values need to be *unwrapped*.

To unwrap the RF phase values and remove the discontinuities, a phase wraparound has to be detected first. This is done by looking at two successive phase values and determining the difference. If the difference is larger than π in either direction, an unwrap action is needed. The exact conditions are:



(a) *RF phase before normalisation.* ***(b)*** *RF phase after normalisation.*

Figure 4.7: *RF phase values are normalised to remove unwanted shifts caused by spread spectrum frequency hopping.*

$$\theta_{\mathrm{i}} = \begin{cases} \theta_{\mathrm{i}} - 2\pi, & \text{if} \quad \theta_{\mathrm{i}} - \theta_{i-1} \leq \pi, \\ \theta_{\mathrm{i}} + 2\pi, & \text{if} \quad \theta_{\mathrm{i}} - \theta_{i-1} \geq \pi, \\ \theta_{\mathrm{i}}, & \text{if} \quad |\theta_{\mathrm{i}} - \theta_{i-1}| < \pi. \end{cases} \tag{4.2}$$

By applying the unwrapping conditions on the raw phase values the discontinuations can be removed. In Figure 4.6b the resulted phase values are plot and as shown, the unwrapping action results in a plot without the discontinuities.

4.4.2 Frequency Hopping

In Section 3.1.2 it is mentioned that there are different regulations per region of the world for UHF RFID readers. In the case of this thesis, the RFID reader falls under FCC regulations and has to operate in the 902–928 MHz frequency band. This means that the reader will hop through the frequencies in a random order to reduce interference between multiple RFID readers.

An unwanted side effect that comes with hopping through frequencies is a shift in the measured RF phase. The shift is caused by the change of the wavelength in (3.1) which in turn is determined by the change in frequency as

$$\lambda = \frac{c}{f} \tag{4.3}$$

where f is the frequency and c is the speed of light). The effect of the frequency hopping is shown in Figure 4.7a.

The shift that is caused by the frequency hopping is unwanted as it disrupts any continuous measurements. There are a couple of methods to

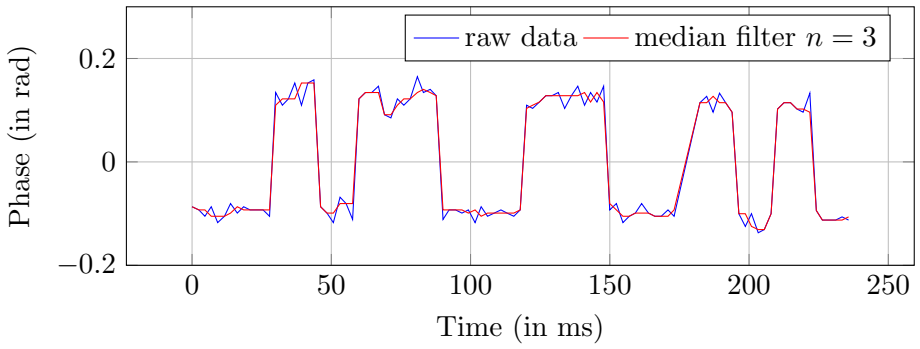


Figure 4.8: *Effect of a moving median filter on noise in phase values.*

manage the shift in phase values, however a complete removal of or compensation to the shift is not possible. For the purpose of this work it is only necessary to observe the phase values from a single channel. By calculating the average value per channel and subtracting the average from each value of the same channel index the phase looks flat (see Figure 4.7b).

However, the shift in phase values when a frequency hop occurs is not the only unwanted effect. Every time the reader changes the frequency, the reader needs between 7.5 and 12 ms to restart operations (see Figure 4.11a), during which there will be no data. This unwanted discontinuation can not be removed by any method. This issue is expanded on in Section 4.5.3.

4.4.3 Noise Filtering

The raw RF phase values (after unwrapping) might be very noisy, which is unwanted if the modulated phase has large peaks from noise. Filtering noise can be done with all kind of different filters, however in this case a simple filter like a *moving median* filter is enough.

A moving median filter is simple to implement and does not require many resources to run for single dimension data. A window size n is selected (needs to be odd size to find the middle value) which is moved over the data. The window is sorted and the median value is chosen as the filtered value. The median filter filters noisy data without averaging edges in the process, this is a preferable property for digital data transmission.

Figure 4.8 shows the effect of a median filter with window size $n = 3$ on a sample of modulated phase values. Larger noise peaks are filtered out without affecting the important edges in the modulated phase values.

4.5 Data Decoder

The final block of the system is the *data decoder*, which is responsible to interpret the processed RF phase values. To decode the encoded bits from

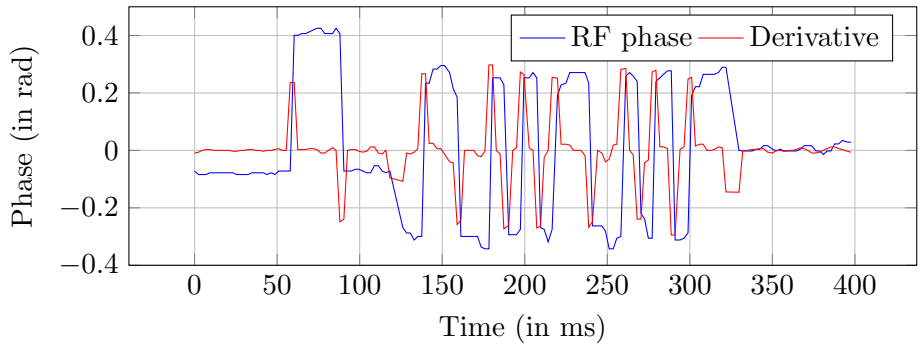


Figure 4.9: *Derivative approximation of central differences on an RF phase modulated signal.*

the RF phase values, the data is processed further in three steps: first the edges need to be detected (Section 4.5.1), then the start of the packet has to be found (Section 4.5.2) and lastly the single bits need to be recovered (Section 4.5.3).

4.5.1 Edge Detection

The most essential part in finding packets in the RF phase values is *edge detection*. This can be done simply through determining the derivative of the RF phase values. However, as shown in:

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \tag{4.4}$$

the definition of the derivative of a function f at point x only holds for continuous functions, which the RF phase is not. Because the RF phase is not a continuous function but a discrete set of samples, the exact derivative cannot be found. However, a derivative approximation by central differences can be made:

$$f'(x) \approx \frac{f(x+h) - f(x-h)}{2h}. \tag{4.5}$$

This is a fast approximation of the derivative of the RF phase at point x and accurate enough to detect the important edges in the signal. The actual edges are determined by a fixed threshold, which in this work is chosen by looking at the peaks of the derivative of a test run. For example, the threshold for the sample in Figure 4.9 would be 0.2. A future improvement on this would be an adaptable threshold, dependent on the preamble.

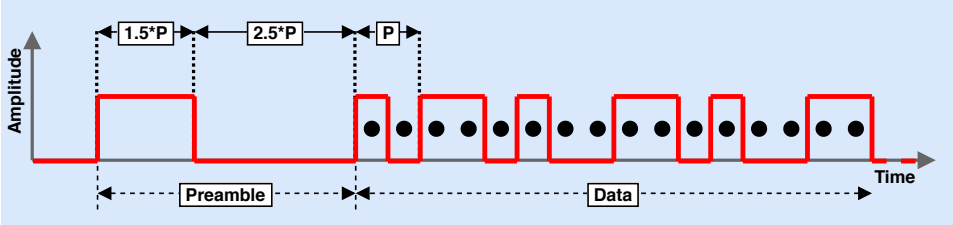


Figure 4.10: *Position markers for expected bits to determine bit value.*

4.5.2 Preamble Detection

Once the edges of the data signal are detected, the next step will be searching for a preamble. We performed this by measuring the length of intervals between edges. The preamble can then be detected by the following steps:

1. Measure length of interval Int_i
   - If $1P < \text{Int}_i < 2p$: move forward to step 2, $i + 1$
   - Else: start over at step 1, $i + 1$
2. Measure length of interval Int_{i+1}
   - If $2P < \text{Int}_{i+1} < 3p$: move forward to step 3
   - Else, if: $1P < \text{Int}_{i+1} < 2p$: stay on step 2, $(i + 2$
3. Preamble detected!

4.5.3 Bit Recovery

Once the preamble has been detected, the system can then try to recover the encoded bits on the phase channel. The first problem that makes bit recovery hard is that, as described in Section 3.1.2, the RFID system uses slotted ALOHA as a MAC protocol. This means that the RFID tag does not respond with uniform time periods between each response, which essentially means that sampling is non-uniform. When the pulsewidth is short, the non-uniform sampling causes the length of the actual bits to vary.

To remove a dependency on measuring the length of intervals between edges, we instead determine where bits should be. By placing markers in certain expected time points of the signal and counting how many markers there are between each edge, the different bits can be determined. This is visualised in Figure 4.10, where the data pulses have black markers in them. The position of these markers are determined by:

$$\text{DOT}_n = (T_{\text{preamble}} + 0.25P) + 0.5P \times n \tag{4.6}$$

where DOT_n is the time point for marker number n, T_{preamble} the time where the preamble ends and P the pulsewidth of the data bits. This means that every full bit will have two markers in it, which makes differentiating between bits easier. This is because a "one" bit is represented by a single interval with two markers in it and a "zero" bit is represented by two intervals after each other, each with one marker in it.

Missed Edges

In a conventional data channel, such as serial communication, some bits will be flipped due to interference. However, due to missed edges from frequency hopping or general noise, the RF phase channel will have bits erased. To maintain the number of transmitted bits at the receiver end and try to correct the erased ones, the number of markers between each edge can give an indication to where and how many edges are lost. To determine where and how many bits need to be inserted, the following steps are taken:

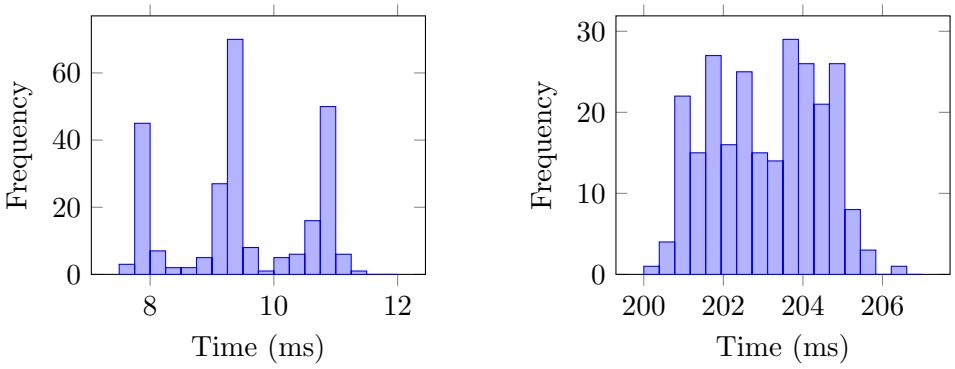
1. Check the number of markers between the edges: if its lower than 3, no edge is missed.
2. If the number of markers is equal or higher than three, it means that there are edges missed. Within this case:
   - If the number of markers is even, calculate the number of missing bits by: num of bits $= \lceil \frac{\text{num of markers}}{2} \rceil$.
   - If the number of markers is odd, calculate the number of missing bits by: num of bits $= \lfloor \frac{\text{num of markers}}{2} \rfloor$.
3. Pad the number of bits with randomised values in the space where bits are is missing.

With this method the number of bits in the data frames are maintained and the chance of successful transmission is increased.

Effect of Frequency Hopping on Packet Reception

The reason this type of bit recovery is needed is because the RFID reader, as described in Sections 3.1.2 and 4.4.2, hops between different frequencies to reduce interference. This hopping has a profound effect on the operation of this system as it requires the reader to halt operations for a short period of time to change the frequency. The discontinuations vary in their length, the distribution of which is shown in Figure 4.11.

As shown in Figure 4.11a, the time that the reader needs to switch to another frequency is between 7.5–12 ms. If this switch happens in the middle of a data frame or the preamble, an edge might be delayed, disappear completely or the preamble might not be detected. The chance that this



(a) *Hopping time* ***(b)*** *Channel time*

Figure 4.11: *Distribution of the time spent in between switching channels (Figure 4.11a) where no RF phase data is reported and distribution of the length of a single channel in milliseconds (Figure 4.11b) where RF phase data is reported.*

happens is higher, the longer the pulse width is. The reason the chance is higher, is because the time the reader spends on a single channel is between 200–207 ms (see Figure 4.11b). For example: if we take a packet with 8 bits of data (including error correction and detection), the packet length (in ms) T_{packet} is then determined by the length of the data bits plus the length of the preamble, which are both determined by the pulse width P. This makes $T_{\text{packet}} = 12 \times P$ ($T_{\text{preamble}} = 4 \times P$ and $T_{\text{data}} = 8 \times P$). The total time for T_{packet} grows linearly with the pulse width, which cannot be too low as the sampling rate of the RF phase values varies between 400 and 550 samples per second. This means that if we want to prevent an intersection by a frequency hop the pulse width needs to be smaller, which might cause bits no longer be detected due to the sampling rate. By using the bit recovery technique described here, bits have a higher chance to be recovered if a frequency hop intersects the packet. However, it cannot prevent a packet being lost if the preamble is intersected.

Chapter 5

Evaluation

This chapter will present the results of the evaluation of the effectiveness and the limits of the design presented in Chapter 4. To do this, an experimental setup has been created in a controlled environment. The specifics of this setup are explained in Section 5.1 and the results of the evaluation are presented in Sections 5.2 and 5.3.

5.1 Experimental Setup

The experiments are done in a small scale, static setup and environment. The RFID reader and antenna are fixed and the position of the RFID tag is within 1 m of the antenna. The system is implemented to work "live", which means that the RF phase data is processed and interpret at runtime and not in post-processing.

5.1.1 Hardware Setup

As mentioned before, the RFID reader of choice in this work is the Impinj Speedway Revolution R420 UHF RFID reader in FCC specification [16]. This reader is paired with an CushCraft S9028PCRJ 8 dBic 902–928 MHz circular polarised antenna, which is 70° directional. The UHF RFID tag that is used in the evaluations is a commercial tag designed for retail inventory management: Avery-Dennison AD-383u7 (see Figure 5.3) [6]. A program was written in Python 3.6 to communicate with reader through the standardised *Low Level Reader Protocol* (LLRP) [14, 27]. The program is run on a Dell Optiplex with an Intel i5 vPro quad-core processor and 16 GB of RAM. The RFID reader transmits at the maximum power of +32.5 dBm and is set to maximum throughput mode (reader mode 0). The transmitter described in Section 4.2 is implemented on a breadboard with an Arduino Nano and simple components (see Figure 5.2).

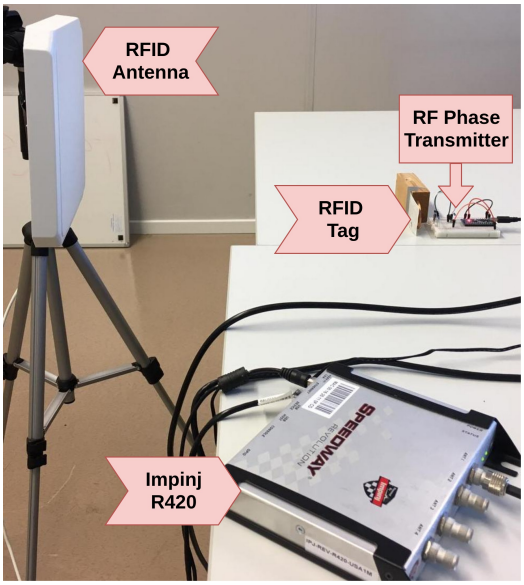


Figure 5.1: *Setup to evaluate the system.*

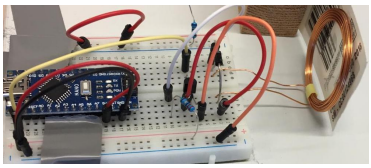


Figure 5.2: *Transmitter circuit build on breadboard with coil and tag on the right.*

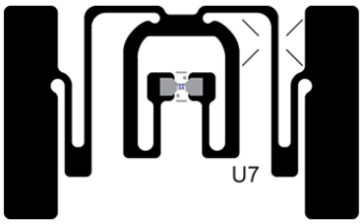


Figure 5.3: *Avery-Dennison AD-383u7 [6].*

5.1.2 Software Setup

Control of the system is migrated to the desktop PC running LLRP software. The software creates a serial connection to the Arduino and a TCP connection to the RFID reader. To make operation and monitoring easy and more flexible, a graphical user environment is written in PyQt.

The software that is created for the project does all the signal and data processing on the fly. The system has been demonstrated to work on a less powerful laptop (XPS 13-9360, Intel i5-7500u, 8GB or RAM). This means no especially demanding processing hardware is needed for the system.

5.2 Effect of Position Reader and Transmitter on RF Phase Shift

To get a sense of the effect that position of the coil and antenna relative to the tag have on the magnitude of the measured RF phase shift, we perform the following experiments. The first experiment (Section 5.2.1) tests the effect of the distance between the transmitter coil and the tag, which is represented as R in Figure 5.4. The second experiment Section 5.2.2 tests the effect the distance between the antenna of the RFID reader and the tag, which is represented as D in Figure 5.4. In both tests the transmitter will modulate a magnetic field near the tag 10 times via OOK with an interval of 100 ms. We then measure the delta of the RF phase shift for all 10 edges

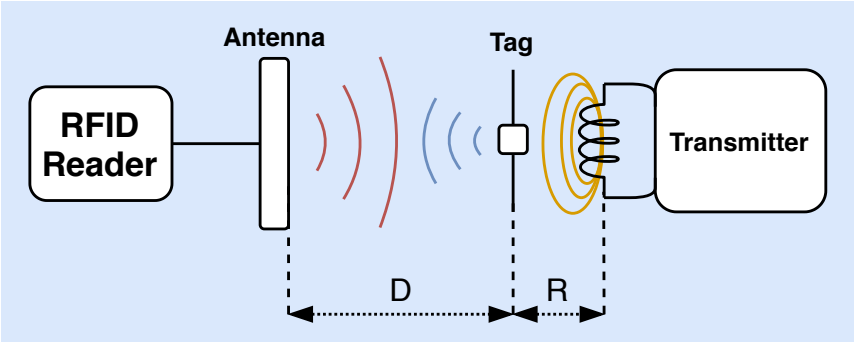


Figure 5.4: *Setup to evaluate the effect of the position of the reader and tranmitter on the measured RF phase shift.*

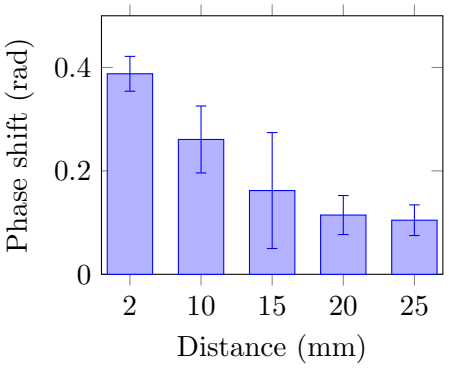


Figure 5.5: *Average induced RF phase shift in radian per distance between transmitter coil and RFID tag.*

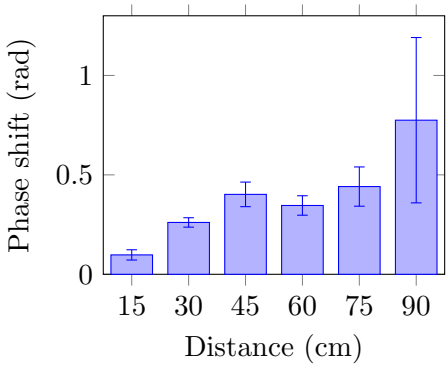


Figure 5.6: *Average induced RF phase shift in radian per distance between RFID antenna and RFID tag.*

that are produced by the transmitter in the RF phase values and average them.

5.2.1 Distance Between Transmitter and Tag

To determine the RF phase shift effect induced by the transmitter at different distances from the tag, we vary the distance R in Figure 5.4. The different distances are: 2,10,15,20,25 mm. The RFID reader antenna is placed at approximately 40 cm from the tag as this gave little noise and sufficient RF phase shift (see Section 5.2.2).

The result of this test is visualised in Figure 5.5. As is shown in the bar chart, the effect of the transmitter decreases as the distance R increases. This is expected as the magnetic field is weaker further from the coil and the induced current in the tag's antenna is lower.

5.2.2 Distance Between Reader Antenna and Tag

To determine the effect of the distance between the RFID antenna and the RFID tag on the induced RF phase shift, we vary the distance D in Figure 5.4. The different distances are: 15,30,45,60,75,90 cm. The distance R between the RFID tag and the transmitter coil is 2 mm as it gave the largest induced RF phase shift (see Section 5.2.1).

The results are visualised in Figure 5.6. As is shown in the bar chart an increase of the distance D also increases the induced effect on the RF phase by the transmitter, which seems counter intuitive. However, if we look at (4.1) it is clear that the current in the tag's antenna (I_{m}) is strongly dependent on the incoming electric field (E_{inc}). Furthermore, from Coulomb's law we can derive the strength of an electric field as [43]:

$$E = \frac{k \times Q}{d^2} \tag{5.1}$$

where E is the electric field strength, k is Coulomb's constant, Q the source charge and d the distance separation from the source charge. Which means that the strength of the electric field decreases with square of the distance from the source. In (5.1) d is equivalent to D in Figure 5.4, which means that when the distance between the RFID antenna and the tag increases, the strength of the incoming electric field decreases, which means the current in the tag antenna also decreases (which we know from (4.1)). However, as R stays the same, the strength of the induced magnetic field, and in turn the induced current, does not change. So when the distance D increases, the induced current from the transmitter coil becomes relatively larger than the current induced by the electric field E_{inc}, which in turn results in a larger induced shift in RF phase.

This would suggest that the best distance for the RFID antenna would be as far as possible, however when we look at the error bars in Figure 5.6 we see that the standard deviation between consecutive RF phase edges is quite large when D is 90 cm. Therefore a more stable distance would be between 30 cm and 45 cm.

5.3 Packet Detection and Recovery

Sufficiently influencing the RF phase is the first step in creating a communication channel, however to transfer data packets, bits need to be detected and recovered first.

The following experimental setup is used. The distance between the transmitter and the tag is 2 mm and the distance between the RFID antenna and the tag is 45 cm. We transmit a 100 data packets through the RF phase channel. The time between each packet is randomised between 850 ms and 1150 ms so the probability that packets line up with the frequency hopping

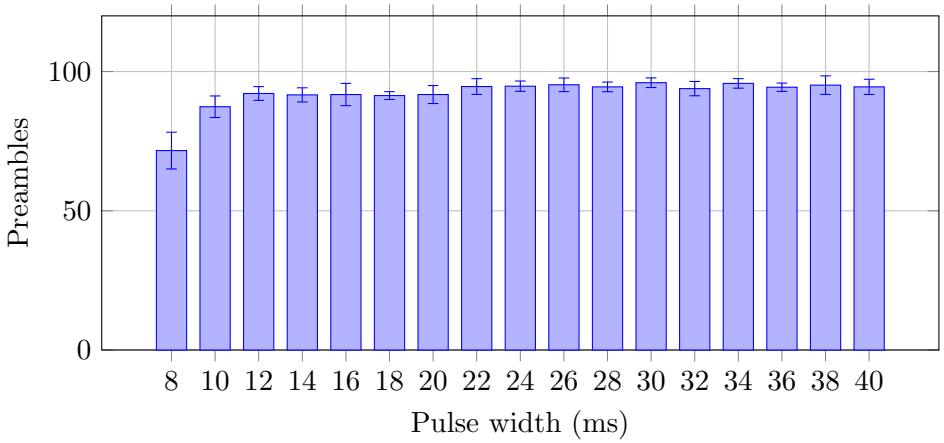


Figure 5.7: *Preambles detected per* 100 *packets transmitted, averaged over eight tests.*

is lower. We then change the pulse width from 8 ms to 40 ms with 2 ms step increments. For redundancy we run the tests 8 times and calculate the *mean* and *standard deviation* from the outcomes.

5.3.1 Preamble Detection

A preamble has been designed in Section 4.3.2. As shown in Figure 4.5 the size of the preamble is dependent on the *pulse width* of the data bits.

In Figure 5.7 the results of the tests are shown. As the pulse width increases, so does the probability for successful detection. However, the detectability of the packets is still only reaching a average of 96 % at most in the best case. This is because the effect of the frequency hopping cannot be completely mitigated. When a hop occurs in the middle of the preamble, there is a high chance that it will not be detected. This is because the RFID reader does not report any data during a hop. However, when the pulse width increases, the impact of the hop time is reduced and packet detection rises.

When we look at Figure 5.7 it is clearly visible that the number of preambles that are being detected flattens off at a pulse width of 12 ms.

5.3.2 Bit Recovery

The next step is to test the effectiveness of bit recovery by the system. The packet has no error correction or detection and is compared on the receiver side to a pre-known byte for validity. The results of the tests are shown in Figure 5.8.

The effect of the longer pulse width is clearly visible as the correctly transmitted packets reach up to 95 % (36 ms pulse width), however for the

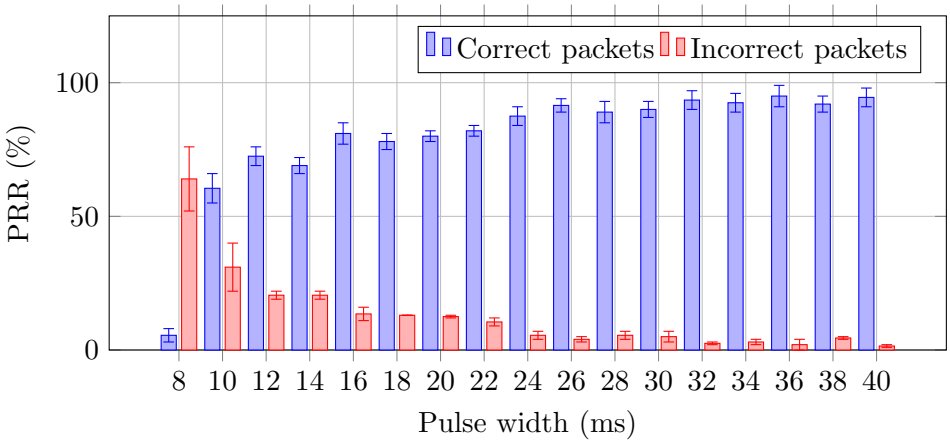


Figure 5.8: *Correct and incorrect recovered packets. The effect of a longer pulse width is clearly visible in the correctly recovered packets.*

lower pulse widths the amount of erroneous bytes is still high. The graph does show an acceptable *packet reception rate* (PRR) ranging from 55 % at 10 ms pulse width up to 95 % at 38 ms pulse width.

5.3.3 Error Correction

As discussed in Section 4.3.3, the data will be encoded to a form of Hamming code called SECDED. This code is able to correct a single bit error and detect a double bit error. This encoding does increase the amount of bits required for the same data, which also increases probability that a frequency hop will happen inside a packet. To test the effectiveness of SECDED on the channel, we use two types of packets: a (8,4) encoding (4 data bits, 8 total bits) and a (13,8) encoding (8 data bits, 13 total bits). For each encoding we run the test four times and average the results.

The results of the tests are shown in Figures 5.9 and 5.10, the graphs show before and after correction is applied to highlight the difference. In both Figures 5.9 and 5.10 the error correction causes a sharp drop in failed packets in the lower pulse widths (10–22 ms) where PRR ranges from 75 % to 94 % for (8,4) encoding and 59 % to 88 % for (13,8) respectively. Above 22 ms pulse width the PRR flattens off around 95 % for (8,4) encoding, but (13,8) encoding only reaches such a PRR at 34 ms pulse width.

Effect of Packet Length

The first thing to notice is that the longer packet (13 bits) has a higher chance to be corrupted, especially in the lower pulse widths (see square lines). This is because the longer packet, due to more bits, has a higher chance to be interrupted by a frequency hop. As described in Section 4.5.3,

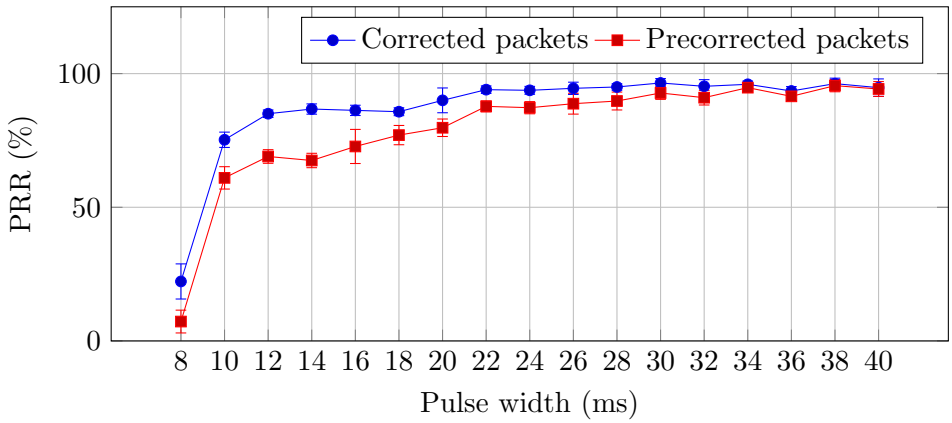


Figure 5.9: *Effect of the error correction on the transmission of (8,4) SECDED encoded data packets. PRR plotted before (precorrected packets) and after (corrected packets).*

the time spend on a single channel is between 200 ms and 207 ms. Thus when the packet length and pulse width grows, it becomes inevitable that a hop will intersect a packet.

For example, an encoded (13,8) packet with a pulsewidth of 16 ms will give a total packet time of: $1.5 \times 16 + 2.5 \times 16 + 13 \times 16 = 272$ ms (preamble and data). This time goes beyond the time spend on a single channel and so every packet will get intersected by a hop. This is visible as the PRR is significantly lower in Figure 5.10 compared to Figure 5.9 at similar pulse widths. However, when the pulsewidth increases, the number of correctly received bytes also increases. This is because the pulsewidth becomes relatively large compared to the hopping time (time spend between channels where the reader does not report RF phase data).

Comparing this to the shorter packet (8 bits) we observe structurally better performance in the same ranges. When we look at the same pulsewidth (16 ms) the packet length is $1.5 \times 16 + 2.5 \times 16 + 8 \times 16 = 192$ ms (preamble and data), which has the possibility to fit within a single channel. When we look at the difference between the pre-corrected and corrected lines, it shows that there is a lot of single bit corrections in the lower pulse widths.

Another observation can be made on the effect of the error correction on the goodput of the system. In the lower pulse widths (10–28 ms) the number of packets that are corrected is quite high. Beyond the lower pulse widths (30–40 ms), the effect is less pronounced but still observable.

5.3.4 Goodput versus Packet Reception Rate

We also looked at determining the goodput versus the chance a packet will successfully arrive. The goodput is defined as the number of useful bits

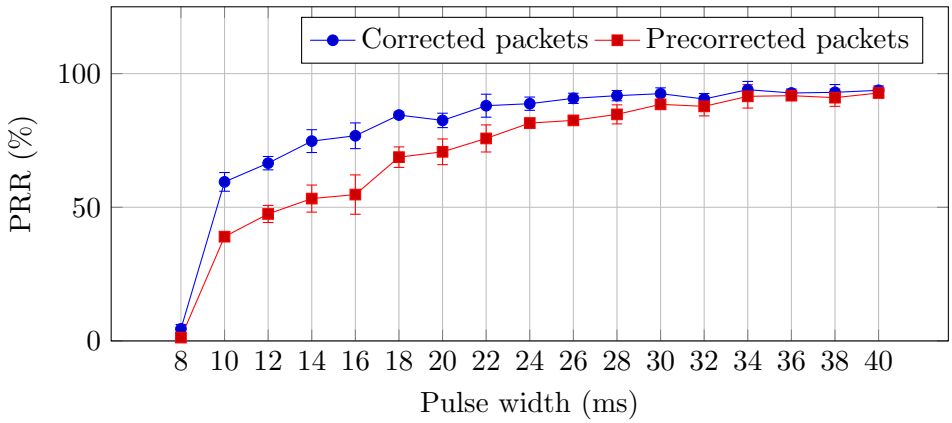


Figure 5.10: *Effect of the error correction on the transmission of (13,8) SECDED encoded data packets. PRR plotted before (precorrected packets) and after (corrected packets).*

delivered by the system per unit of time.

For example, the goodput for a single (8,4) encoded data packet with a pulsewidth of 10 ms can be determined as follows: the full packet has an overhead of 80 ms (i.e. the lendth of the preamble plus encoding overhead). This means of the full packet, only one third is devoted to useful data. This means that although the theoretical throughput at 10 ms is 100 bits/s, the goodput is lower: $(4/12) * 100 = 33.33$ bits/s. When we compare the theoretical goodput (Figure 5.11) to the PRR (Figures 5.9 and 5.10), we can get a sense of the trade-offs of the designed system.

If we look at the goodput of the system, it is clearly visible that the data rate decreases rapidly as the pulsewidth increases. This is an unwanted property, however when we compare this to the PRR of the system it is visible that a higher probability of reception requires a larger pulse width. When we look at the goodput of 13 bit packets in Figure 5.11, it shows a higher goodput than 8 bit packets. However, when we compare the PRR for both, we see that for the 13 bit packets to get the same high PRR of 94 % as the 8 bit packets, the goodput has to drop to 13 bits/s compared to 15 bits/s. However, when comparing the maximum goodput with a PRR higher than 50 %, the longer packets do prove superior: 47 bits/s at 59 % versus 33 bits/s at 75 %.

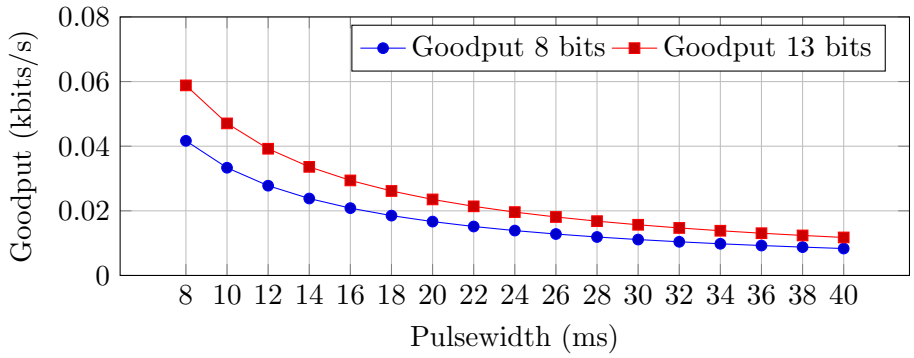


Figure 5.11: *Theoretical goodput plotted. While the lower pulsewidths carry a higher goodput, the chance that a packet will successfully arrive is a lower.*

Chapter 6

Discussion

While the presented work can potentially allow users to interact with RFID systems in a new and less expensive way, the technology is still in its very early stages. To help successful future development its is important that the current limitations and possible next steps are discussed.

6.1 Current Limitations

As shown in Chapters 4 and 5 limitations in the work are taken into the design but have also resulted from the evaluation. To provide transparency for the reader and possible future project we list the following limitations to be taken into consideration:

- **Frequency hopping:** the mayor limitation in this work is caused by the spread spectrum frequency hopping in the RFID system. The hopping causes mayor discontinuations in the RF phase values that cannot be compensated for. This means the maximum size of the data packets is very limited, however as there is still room to compress or encode meaningful information this issue can be dealt with. Furthermore, as shown in Section 5.3.4 we show that a goodput of 47 bits/s can be achieved with a PRR of 59 %. If the frequency hopping is eliminated, the PRR could raise to a more acceptable rate.

- **Antenna–tag distance:** the distance between the tag and the RFID reader's antenna is a big influence on the effectiveness of the system (as described in Section 5.2.2).

- **Coil–tag orientation:** the effect of the position of the coil relative to the tag has been explored (Section 5.2.1), however the orientation has not. The orientation has a significant effect on the functionality of the system.

- **Single tag operation:** the system has only been tested while the reader focussed on a single tag, so performance while inventorying might be different.

6.2 Future Work

Exploiting existing RFID infrastructures is considered a popular topic in the research community (as shown by the novel explorations described in Section 2.3) and although this work is the first to presents *digital communication* through RF phase measurement, there is still much room for future projects and improvements.

First of which would be to build the system with an RFID reader from the ETSI regulatory region as those are not required to frequency hop. This would remove the RF phase measurement discontinuations imposed on the system by the FCC RFID reader. However, to be able to integrate the system world wide, a more robust encoding schema might be needed. By looking into *rateless* or *erasure* coding [24], the channel might be made more robust to bit erasures and discontinuations.

Furthermore, it would be interesting to see the effect of differently shaped tags and coils on the effectiveness of the system. Which would also lead to an investigation into the electromagnetic cause and effect of the transmitter on the tag. Lastly it would be great to realise an attachment for a smartphone on an actual PCB to test the real world performance of the system.

Chapter 7

Conclusions

In this thesis we addressed the problem of RFID integration by looking at a different way to interact with RFID tags. We explored a basic influence on RF phase rotation in RFID systems, designed a system for RFID interaction based on that and consequently build a working prototype of the transmitter and the receiver. By creating and modulating (through OOK) a magnetic field near the RFID tag, the RF phase can be exploited for digital communication. Based on low cost, simple and small components, we were able to create this system at a vastly lower expense than conventional handheld RFID readers and with more functionality than State of the Art research.

The digital communication channel designed in our system achieves an average *packet reception ratio* (PRR) up to 96 % with a goodput of 15 bits/s. However, a goodput up to 47 bits/s can be achieved with a PRR of 59 %. In combination with the server part described in [3], we were actually able to complete an interaction according to Figure 4.2. With these results we demonstrate a novel method to interact with RFID tags that can drastically reduce the expense compared to similar solutions.

We found that the limiting factor in raising the PRR is the effect of frequency hopping on the RF phase measurements. The hopping causes discontinuations in the communication channel that can prevent packets from being detected. In Section 6.2 we propose to implement the designed system on an RFID readers that can disable the frequency hopping, which should raise the PRR in the system.

Bibliography

[1] ABN-AMRO. Kledingzaken: Branchebeschrijving (Dutch). https://www.abnamro.nl/nl/images/Generiek/PDFs/020_Zakelijk/02_Sectoren/Retail/retail-branche-kledingzaken.pdf. Accessed: 2019-06-21.

[2] Zhenlin An, Qiongzheng Lin, and Lei Yang. Cross-Frequency Communication: Near-Field Identification of UHF RFIDs with WiFi! In *Proc. MOBICOM*, pages 623–638. ACM, 2018.

[3] Mike Beijen, Kevin Chong, Callum Robert Holland, and Glenn Keller. Server Program for Retail RFID System with Advanced Message Handling. Bachelor thesis, Delft University of Technology, Delft, The Netherlands. http://resolver.tudelft.nl/uuid:041533eb-6010-418e-b3d1-80ff7cc4996b, 2019.

[4] Benjamin D Braaten, Gregory J Owen, and Robert M Nelson. Design of space-filling antennas for passive uhf rfid tags. In *Radio Frequency Identification Fundamentals and Applications Design Methods and Solutions*. IntechOpen, 2010.

[5] Vipul Chawla and Dong Sam Ha. An overview of passive RFID. *IEEE Communications Magazine*, 45(9):11–17, 2007.

[6] Avery Dennison. AD-383u7. https://rfid.averydennison.com/en/home/innovation/rfid-inlay-designs/AD-383u7.html. Accessed: 2019-06-06.

[7] Daniel M Dobkin. *The rf in RFID: uhf RFID in practice*. Newnes, 2012.

[8] Nilima A Dudhane and Sanjeevkumar T Pitambare. Location based and contextual services using Bluetooth beacons: New way to enhance customer experience. *Lecture Notes on Information Theory*, 3(1), 2015.

[9] International Organization for Standardization. ISO/IEC 18000-3:2010. https://www.iso.org/standard/53424.html. Accessed: 2019-04-10.

[10] International Organization for Standardization. ISO/IEC 18000-63:2015. https://www.iso.org/standard/63675.html. Accessed: 2018-12-03.

[11] Richard W Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, 1950.

[12] Christian Holz and Marius Knaust. Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication. In *Proc. UIST*, pages 303–312. ACM, 2015.

[13] Yuxiao Hou, Yanwen Wang, and Yuanqing Zheng. Tagbreathe: Monitor breathing with commodity rfid systems. In *Proc. ICDCS*, pages 404–413. IEEE, 2017.

[14] EPCglobal Inc. Low Level Reader Protocol (LLRP). https://www.gs1.org/sites/default/files/docs/epc/llrp_1_1-standard-20101013.pdf. Accessed: 2019-04-13.

[15] Impinj Inc. Low Level User Data Support. https://support.impinj.com/hc/en-us/article_attachments/200774268/SR_AN_IPJ_Speedway_Rev_Low_Level_Data_Support_20130911.pdf. Accessed: 2019-05-15.
[16] Impinj Inc. SPEEDWAY R420 RAIN RFID READER. https://www.impinj.com/platform/connectivity/speedway-r420/. Accessed: 2019-05-15.
[17] RFID Journal. Eight More Surprising Uses of RFID. https://www.rfidjournal.com/articles/view?17274. Accessed: 2019-04-10.
[18] Hanchuan Li, Can Ye, and Alanson P Sample. IDSense: A human object interaction detection system based on passive UHF RFID. In *Proc. CHI*, pages 2555–2564. ACM, 2015.
[19] Hans Dieter Luke. The origins of the sampling theorem. *IEEE Communications magazine*, 37(4):106–108, 1999.
[20] Sky McKinley and Megan Levine. Cubic spline interpolation. *College of the Redwoods*, 45(1):1049–1060, 1998.
[21] Crypto Museum. The Thing - Great Seal Bug. https://www.cryptomuseum.com/covert/bugs/thing/index.htm. Accessed: 2019-04-10.
[22] Lionel M Ni, Yunhao Liu, Yiu Cho Lau, and Abhishek P Patil. LANDMARC: indoor location sensing using active RFID. In *Proc. PerCom*, pages 407–415. IEEE, 2003.
[23] M Rosa Palacín and Anne de Guibert. Why do batteries fail? *Science*, 351(6273), 2016.
[24] Ravi Palanki and Jonathan S Yedidia. Rateless codes on noisy channels. In *Proc. ISIT*, pages 37–37. IEEE, 2004.
[25] Connectivity Knowledge Platform. Encoding Schemes. http://ckp.made-it.com/encodingschemes.html. Accessed: 2019-06-23.
[26] Swadhin Pradhan, Eugene Chai, Karthikeyan Sundaresan, Lili Qiu, Mohammad A Khojastepour, and Sampath Rangarajan. RIO: A pervasive rfid-based touch gesture interface. In *Proc. MOBICOM*, pages 261–274. ACM, 2017.
[27] Ben Ransford. Python client for LLRP-based RFID readers. https://github.com/ransford/sllurp. Accessed: 2019-06-06.
[28] Jack Romaine. Disappointed in RFID Adoption? https://www.rfidjournal.com/articles/view?13227/. Accessed: 2019-01-07.
[29] George Roussos. Enabling RFID in retail. *Computer*, 39(3):25–30, 2006.
[30] Nirupam Roy and Romit Roy Choudhury. Ripple {II}: Faster Communication through Physical Vibration. In *Proc. NSDI*, pages 671–684. USENIX, 2016.
[31] Nirupam Roy, Mahanth Gowda, and Romit Roy Choudhury. Ripple: Communicating through physical vibration. In *Proc. NSDI*, pages 265–278. USENIX, 2015.
[32] NXP Semiconductors. UCODE 7/7m. https://www.nxp.com/products/identification-security/rfid/ucode-uhf/ucode-7-7m:SL3S1204. Accessed: 2019-06-23.
[33] Claude Elwood Shannon. Communication in the presence of noise. *Proceedings of the IEEE*, 86(2):447–457, 1998.
[34] Atlas RFID store. ALIEN ALR-H450 HANDHELD RFID READER. https://www.atlasrfidstore.com/alien-alr-h450-handheld-rfid-reader/. Accessed: 2019-06-25.
[35] Atlas RFID store. ALIEN ALR-S350 SLED HANDHELD RFID READER. https://www.atlasrfidstore.com/alien-alr-s350-sled-handheld-rfid-reader/. Accessed: 2019-01-18.

[36] Atlas RFID store. ALIEN SQUIGGLE RFID WHITE WET INLAY (ALN-9840, HIGGS-EC). https://www.atlasrfidstore.com/alien-squiggle-rfid-white-wet-inlay-aln-9840-higgs-ec/. Accessed: 2019-06-21.

[37] Atlas RFID store. Handheld RFID readers. https://www.atlasrfidstore.com/handheld-rfid-readers/. Accessed: 2018-12-11.

[38] Atlas RFID store. IMPINJ SPEEDWAY REVOLUTION R420 UHF RFID READER (4 PORT). https://www.atlasrfidstore.com/impinj-speedway-revolution-r420-uhf-rfid-reader-4-port/. Accessed: 2019-06-20.

[39] Atlas RFID store. Monza 5 Smartrac dipole tag. https://www.atlasrfidstore.com/smartrac-shortdipole-rfid-wet-inlay-monza-5/. Accessed: 2019-01-21.

[40] Atlas RFID store. TURCK (U GROK IT) UHF RFID READER FOR SMARTPHONES. https://www.atlasrfidstore.com/turck-u-grok-it-uhf-rfid-reader-for-smartphones/. Accessed: 2019-01-21.

[41] Ke Sun, Ting Zhao, Wei Wang, and Lei Xie. Vskin: Sensing touch gestures on surfaces of mobile devices using acoustic signals. In *Proc. MOBICOM*, pages 591–605. ACM, 2018.

[42] Alien Technologies. ALN-9840 Squiggle. http://www.alientechnology.com/wp-content/uploads/ALN-9840%20Squiggle%20Higgs-EC%20(2016-04-19).pdf. Accessed: 2019-06-09.

[43] the Physics Classroom. Electric Field Intensity. https://www.physicsclassroom.com/class/estatics/Lesson-4/Electric-Field-Intensity. Accessed: 2019-06-24.

[44] Ingo R Titze and Daniel W Martin. Principles of Voice Production. *Acoustical Society of America Journal*, 104:1148, 1998.

[45] Hoi Yan Tung, Kim Fung Tsang, Kwok Tai Chui, Hoi Ching Tung, Hao Ran Chi, Gerhard P Hancke, and Kim Fung Man. The generic design of a high-traffic advanced metering infrastructure using ZigBee. In *Proc. WoT*, pages 836–844. ACM, 2014.

[46] Benjamin Wagner and Dirk Timmermann. Adaptive clustering for device free user positioning utilizing passive RFID. In *Proc. MOBICOM*, pages 499–508. ACM, 2013.

[47] Jue Wang and Dina Katabi. Dude, where's my card?: RFID positioning that works with multipath and non-line of sight. In *Proc. SIGCOMM*, pages 51–62. ACM, 2013.

[48] Wei Wang, Lin Yang, and Qian Zhang. Touch-and-guard: secure pairing through hand resonance. In *Proc. UbiComp*, pages 670–681. ACM, 2016.

[49] Teng Wei and Xinyu Zhang. Gyro in the air: tracking 3D orientation of batteryless internet-of-things. In *Proc. MOBICOM*, pages 55–68. ACM, 2016.

[50] Lei Yang, Yekui Chen, Xiang-Yang Li, Chaowei Xiao, Mo Li, and Yunhao Liu. Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices. In *Proc. MOBICOM*, pages 237–248. ACM, 2014.

[51] Lei Yang, Yao Li, Qiongzheng Lin, Huanyu Jia, Xiang-Yang Li, and Yunhao Liu. Tagbeat: Sensing mechanical vibration period with COTS RFID systems. *IEEE/ACM Transactions on Networking*, 25(6):3823–3835, 2017.

[52] Zhice Yang, Jiansong Zhang, Zeyu Wang, and Qian Zhang. Lightweight Display-to-device Communication Using Electromagnetic Radiation and FM Radio. In *Proc. IMWUT*, page 49. ACM, 2018.

[53] Cui Zhao, Zhenjiang Li, Han Ding, Jinsong Han, Wei Xi, Ting Liu, and Ruowei Gui. RF-Mehndi: A Fingertip Profiled RF Identifier. In *Proc. INFOCOM*, pages 1513–1521. IEEE, 2019.

Appendix A

Sound Recovery with RFID Tags

To determine the precision that the Impinj Speedway Revolution r420 UHF RFID reader [16] offers in terms of the RF phase rotation reporting, a set of experiments have been performed. The overreaching goal was to find whether it is possible to extract sound with the help of RFID tags placed on the sound source.

A.1 Theoretical Precision

As described in Section 3.2.2 the theoretical precision of the RF phase measurement comes down to 39.9 µm at a center frequency of 915 MHz. However, Impinj lists a standard deviation of ±0.1 radians [14], which comes down to ±2.6 mm. While the standard deviation seems large compared to the absolute precision, it is a calculated, theoretical deviation and might not be the same in a practical system.

A.2 Sound Recovery

Sound recovery through RF backscatter was actually one of the fundamental applications that led to modern day RFID systems [21]. However, since the standardisation of the EPC C1G2 protocol in 2004 there has not been much research in the area of sound recovery with UHF RFID.

One notable paper that touches on sound recovery is Tagbeat [51] (also described in Section 2.3), which exploits the movement detection in RF phase measurements to detect the period of vibrations. This is done through a method called *compressive sensing*, which can detect the period of a signal even if its sampled below the Nyquist-Shannon sampling-rate. However, the signal to be sampled has to be sparse in its nature, meaning no complex combinations of frequencies can be detected. Furthermore, Tagbeat is

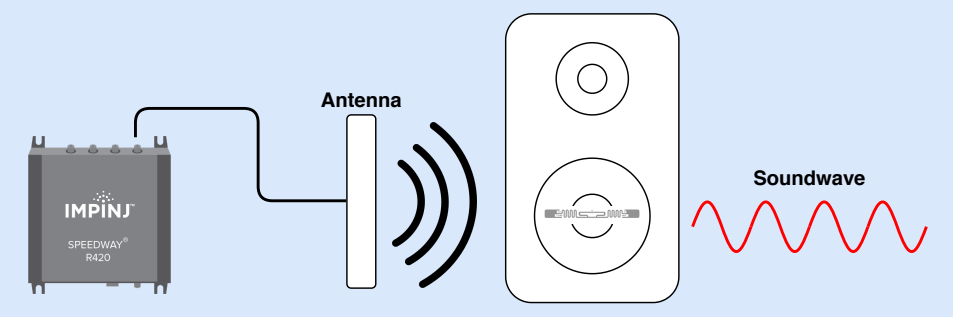


Figure A.1: *Experimental setup to test RF phase precision through sound recovery [16, 36].*

evaluated on relatively large moving systems. A centrifuge, fan and engine displace a lot more (order of cm) than a speaker dome for example (order of mm).

A.2.1 The Sampling Theory

Implied in 1928 by Harry Nyquist and proved in 1933 by Claude Shannon (and independently discovered by Edmund Whittaker and Vladimir Kotelnikov [19]), the sampling theory determines the bridge between the continuous-time signals and discrete-time signals. The theorem determines if a function $x(t)$ contains no frequencies higher than B Hz and if it is sampled at a frequency $f_s > 2B$, perfect reconstruction of $x(t)$ is guaranteed [33].

What this essentially means is that to recover sound of a certain frequency, the sampling frequency needs to be twice as high. The Impinj r420 RFID reader lists a maximum throughput of 1100 tag reads per second, however this is an aggregated number of reads with multiple tags. The single tag throughput is measured to lie between 400 and 550 tag reads per second, depending on the tag that is used. This would mean that realistically the maximum frequency that can be recovered is 275 Hz. This seems limited, however the fundamental frequencies of the human voice fall within the 85–180 Hz range for males and 166–255 Hz range for females [44], which should be detectable with the projected sample frequency.

A.2.2 Experimental Setup

To test the precision that is possible in RF phase measurement we created an experimental setup. As seen in Figure A.1 an RFID tag is taped onto the dome of a speaker, the antenna of the RFID reader is aimed at the speaker and a sound is then played. As a tag we used the Alien ALN-9840 Squiggle RFID tag [42]. Some basic processing of the RF phase values is

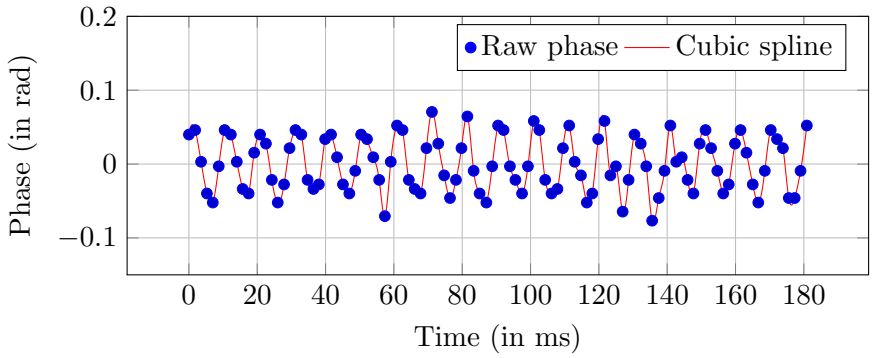


Figure A.2: *Sine wave samples and interpolated. Note the distinct wave pattern visible in the samples.*

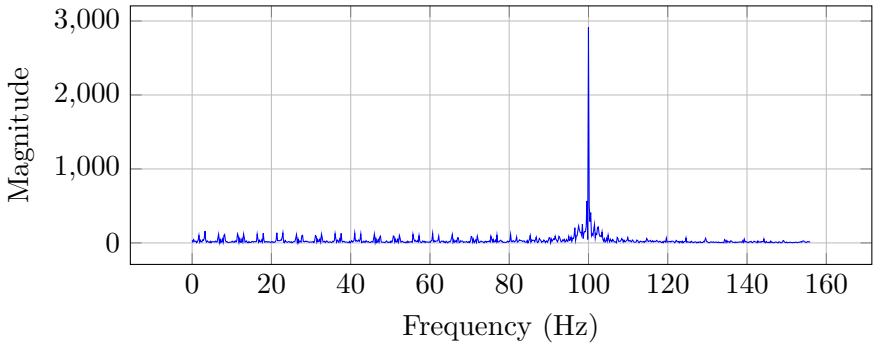


Figure A.3: *Fast Fourier Transform of the interpolated sine wave. Note the large peak at* 100 Hz*.*

done, this is the same as in Sections 4.4.1 and 4.4.2 which mostly removes the discontinuations caused by frequency hopping. As the samples are non-uniformly spaced we apply cubic spline interpolation [20] to create a smooth line between the samples.

The speaker that is used in this experiment is a JBL Northridge E80, this specific speaker dome has a cross-over frequency of 300 Hz. The speaker is connected to a Pioneer VSX-917v 110 W AC-receiver. The audio source is a tone generator and recorded voice audio file on an Apple iPhone 6S connected via the headphone jack to the receiver.

Sine wave

The first experiment is to play a sine wave at 100 Hz through the speaker and plot the resulting RF phase values. The dots in Figure A.2 are the raw RF phase values and the red line represents the cubic spline interpolation. A clear waveform is visible in this sample, which is logical as 100 Hz is low frequency, so the speaker dome has a lot of movement. When a *Fast Fourier*

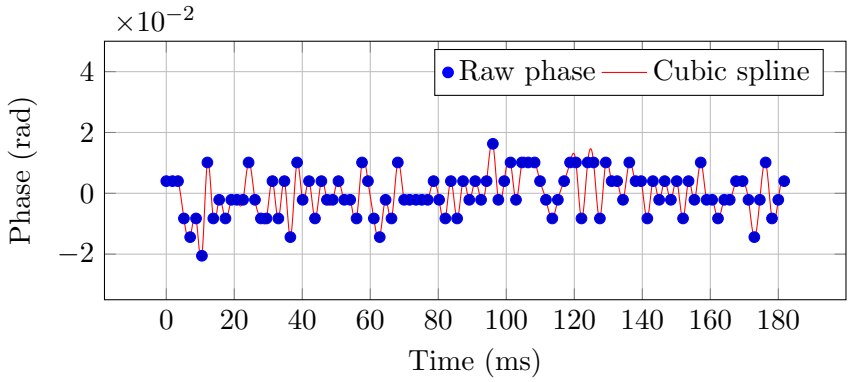


Figure A.4: *Voice samples samples and interpolated. The magnitude is a lot lower compared to Figure A.2.*

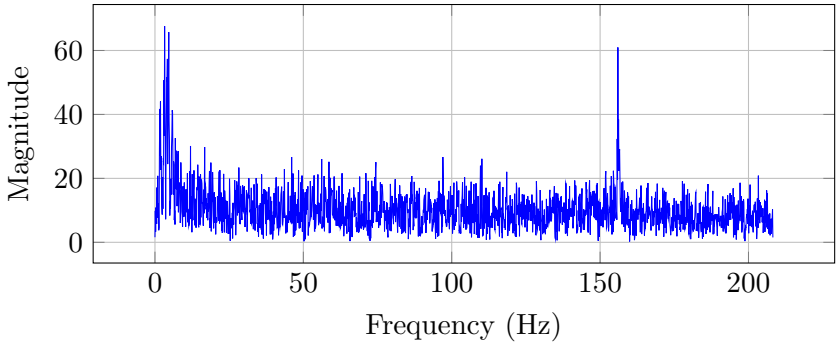


Figure A.5: *Fast Fourier Transform of the interpolated voice signal. Note the large peak at* 156 Hz*, which suggests a fundamental voice frequency.*

Transform (FFT) is performed on the waveform (see Figure A.3), a clear peak is visible at the 100 Hz point.

Human Voice

The second experiment is to play a sample of human voice. This recording is of the author making the sound of the letter *M*. The speaker dome has trouble in reproducing all the frequencies, as this is no longer a single low frequency tone but a composition of low and high frequencies. Most speakers have a cross-over frequency to separate low, mid and high frequencies for the respective specialised domes. The volume of the sound from the dome decreases the closer the frequency gets to the cut-off. This is visible in Figures A.4 and A.5 as the magnitude of the RF phase sample change and the FFT is a lot lower compared to Figures A.2 and A.3. However, a waveform is still visible in Figure A.4 and Figure A.5 clearly shows a peak at 156 Hz, which suggest that for the letter *M*, the fundamental frequency of the author is 156 Hz.

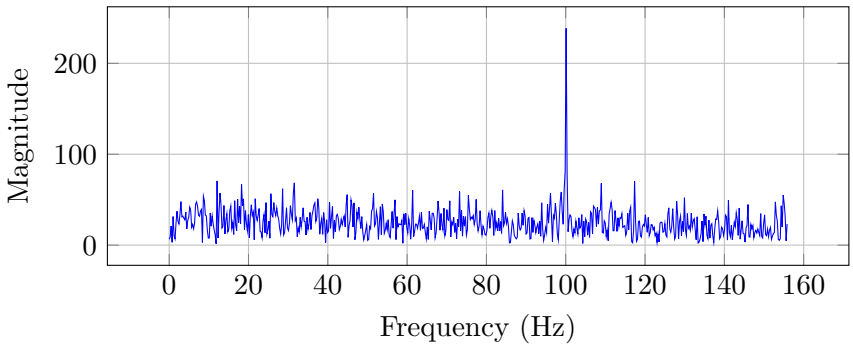


Figure A.6: *Fast Fourier Transform of the interpolated sine waveform recovered from the aluminium foil experiment. Note the* 100 Hz *peak in the spectrum.*

A.2.3 Aluminium Foil

A final experiment is done to demonstrate the sensitivity of the RF phase measurements. In place of the tag being stuck on the speaker dome, a small piece of aluminium foil is taped onto the speaker dome. The tag is then placed near (in the proximity of around 30–50 cm) the speaker, in this case behind. A sine waveform of 100 Hz is then played through the speaker and the samples analysed in the same way as described in Appendix A.2.2. The FFT spectrum plot is shown in Figure A.6 where a distinct peak is visible at the 100 Hz mark. Note that the magnitude is significantly lower than in Figure A.3 but still very distinctive.

A.3 Conclusions

The conclusion that can be drawn from these experiments is that the precision of the RF phase measurements is very high. Large speaker movement is clearly visible even though the RF phase change is lower than the specified standard deviation of 0.1 radians. Furthermore, smaller movement through a voice sample is also measurable, where the change in RF phase is much lower (< 0.002 radians). The sensitivity of the RF phase is also demonstrated through the aluminium foil experiment. If the setup and RFID reader are improved on, the area of sound recovery through RFID might turn out to be an interesting one.