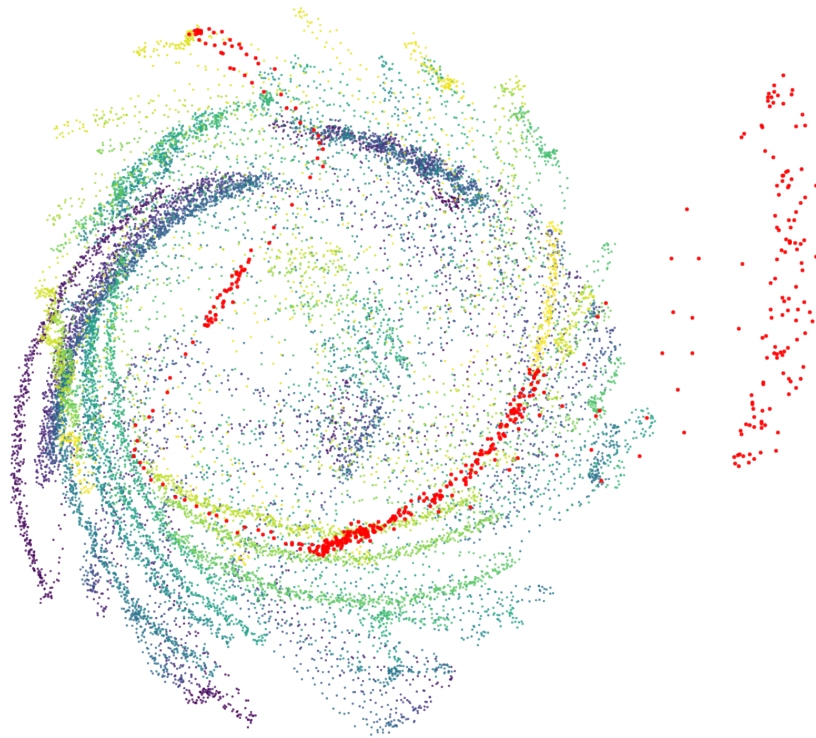




CHALMERS
UNIVERSITY OF TECHNOLOGY



Development of an SDR-Based System for UHF RFID Signal Analysis

Gustav Bardun

DEPARTMENT OF ELECTRICAL ENGINEERING

CHALMERS UNIVERSITY OF TECHNOLOGY

Gothenburg, Sweden 2026

www.chalmers.se

MASTER'S THESIS 2026

Development of an SDR-Based System for UHF RFID Signal Analysis

Gustav Bardun



CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Electrical Engineering
Division of Signal Processing and Biomedical Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2026

Development of an SDR-Based System for UHF RFID Signal Analysis
Gustav Bardun

© Gustav Bardun, 2026.

Supervisor and Examiner: Xuezhi Zeng, Electrical Engineering, Chalmers

Master's Thesis 2026
Department of Electrical Engineering
Division of Signal Processing and Biomedical Engineering Chalmers University of
Technology
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: An I/Q plot of a captured signal, with backscatter marked in red.

Typeset in L^AT_EX
Gothenburg, Sweden 2026

Abstract

This thesis presents the development of a Software-Defined Radio based system for capturing and analyzing Ultra High Frequency (UHF) RFID signals. While UHF RFID has been explored as a sensing modality, commercial readers lack the transparency required to analyze the underlying signal and any interference taking place. A custom Software-Defined Radio based system was implemented to capture, detect, and decode RFID backscatter while providing access to the raw In-phase/Quadrature data. The system utilizes a derivative-based metric to detect RFID backscatter and support tag decoding.

The system was used to analyze RFID signals in scenarios involving multiple nearby tags, including cases where one tag was undergoing controlled motion. The results indicate significant interference between nearby tags. Stationary tags were observed to exhibit "motion-like" periodic variations in phase and RSSI when in close proximity to a moving tag. This often appeared as an inverted reflection of the actual motion, creating ambiguity that makes it difficult to interpret tag behavior on a per-tag basis. This suggests that RFID systems designed for motion sensing may require fundamentally different signal processing chains than commercial systems designed for rapid retrieval of tag information.

Keywords: RFID, SDR, motion sensing, respiratory monitoring, UHF RFID, tag interference, multipath.

Acknowledgements

During this project, I've had to spend a notable amount of time working alone on a singular task, and during this process it is tremendously easy to get tunnel vision when handling problems or simply losing motivation when results are running dry. I've had the great benefit of having my friends, especially those at the C.A.S.E Lab, act as involuntary sounding boards for this project. Although being able to discuss the project at a surface level has been useful, it has been the guidance and expertise of my supervisor and examiner, Xuezhi Zeng, that has made this project feasible and executable. I cannot thank you all enough for your enthusiasm and support.

Appropriate thanks go to the coffee shops around Chalmers for the caffeine-based moral support.

Gustav Bardun, Gothenburg, September 2026.

List of Acronyms

Below is the list of acronyms that have been used throughout this thesis listed in order of topic.

RFID	Radio Frequency Identification
UHF RFID	Ultra High Frequency Radio Frequency Identification
SDR	Software Defined Radio
LO	Local Oscillator
I/Q Signal	In-phase Quadrature Signal
SNR	Signal to Noise Ratio
RSSI	Received Signal Strength Indicator
EPC	Electronic Product Code

Nomenclature

Below is the nomenclature of indices, sets, parameters, and variables that have been used in this thesis.

n	Discrete-time sample index
k	Discrete summation index for convolution
$x[n]$	Discrete input signal
$h[n]$	Discrete impulse response of a system
$y[n]$	Discrete output signal resulting from a convolution
$I[n]$	In-phase amplitude component of the digital baseband signal
$Q[n]$	Quadrature amplitude component of the digital baseband signal
j	Imaginary unit ($j^2 = -1$)
$x'[n]$	First-difference complex signal vector
N	Total number of discrete samples within an evaluation window
RSSI_{dB}	Received Signal Strength Indicator expressed in decibels

Contents

List of Acronyms	ix
Nomenclature	xi
List of Figures	xv
1 Introduction	1
1.1 The use for RFID in motion sensing	1
1.2 The need for a custom solution	2
1.3 Objectives and scope	3
2 Theory	5
2.1 Basics of UHF RFID communication	5
2.1.1 The captured signal	6
2.2 Previous research	8
2.2.1 Hardware setups	8
2.2.2 Detecting tag backscatter	8
2.2.3 Extracting metrics	9
3 Development and implementation	11
3.1 Hardware setup	11
3.2 Detecting tag backscatter	13
3.3 Identifying and decoding tags	14
3.3.1 Backscatter detection and classification	15
3.3.2 Decoding the tag's identity	15
3.4 Extracting metrics	16
3.4.1 Extracting RSSI	16
3.4.2 Extracting phase	16
3.4.3 Pairing data-points with tags	17
3.5 Experiment design	18
3.5.1 Controlled variables	18
3.5.2 Metrics	19
4 Results	21
4.1 Single Tag experiments	21
4.1.1 Different sizes of tags	21
4.1.2 Different distances between SDR and tags	24

4.1.3	Single moving tag	24
4.2	Experiments with multiple tags	28
4.2.1	Mute tag besides a moving tag	28
4.2.2	Two active tags in close proximity	28
4.2.2.1	Different orientation of tags	28
4.2.2.2	Sequential and alternating reading of tags	28
5	Discussion	35
5.1	Interference between tags	35
5.2	The state of the hardware and how it limits experiments	36
5.3	Software and future development	37
6	Conclusion	39
	Bibliography	41
A	Appendix	I
A.1	Boundary detection	I

List of Figures

2.1	A diagram showing a series of EPC GEN2 commands.	6
2.2	Different zoom levels on a typical captured signal.	7
3.1	A diagram of the experimental setup.	12
3.2	Two tags in front of the patch antenna. One tag is placed on the tag-moving rig.	12
3.3	The complex I/Q signal representation of the received signal. The samples acquired during the backscatter interval are marked in red. .	13
3.4	A block diagram of the signal processing chain used.	17
4.1	Single tag read of a smaller tag at a distance of 10 cm from the SDR antenna, and 220 cm from the reader antenna. Green and red lines mark the RN16 and EPC respectively.	22
4.2	Single tag read larger tag at a distance of 15 cm from the SDR antenna, and 220 cm from the reader antenna. Red dotted lines mark the RN16, solid red lines mark the EPC.	22
4.3	SDR measurements from captured signal for a single static tag. . . .	23
4.4	Reader reported RSSI and phase for a single static tag.	23
4.5	Signal of a single tag moving 2 cm back and forth. The tag was at most 12 cm away from the antenna.	25
4.6	Signal of a single tag moving 2 cm back and forth. The tag was at most 12 cm away from the antenna. The movement can not be seen by looking only at the amplitude.	26
4.7	Signal of a moving tag with 1 cm displacement. The movement can not be seen by looking only at the amplitude.	27
4.8	Signal of a moving tag with 2 cm displacement. The movement can not be seen by looking only at the amplitude. A mute tag was placed next to the tag that is being read.	29
4.9	Signal of two tags, one of which is moving in a sinusoidal pattern with period 3 s and a displacement of 2 cm. The still tag (blue) shows a sinusoidal pattern in phase and RSSI even though it is fixed in place. The tags were placed 8 cm apart.	30
4.10	Signal of two tags, one of which is moving in a sinusoidal pattern with period 3 s and a displacement of 2 cm. The still tag (blue) shows a sinusoidal pattern in phase and RSSI even though it is fixed in place. The tags were placed 5 cm apart.	31

4.11	Signal of two tags, one of which is moving in a sinusoidal pattern with period 3 s and a displacement of 2 cm. The still tag (blue) was placed in a vertical orientation and the moving tag (red) was placed in a horizontal orientation.	32
4.12	Signal of two tags read sequentially, one of which is moving in a sinusoidal pattern with period 3 s and a displacement of 2 cm. The still tag (blue) was placed in a vertical orientation and the moving tag (red) was placed in a horizontal orientation.	33

1

Introduction

Radio Frequency Identification (RFID) is a wireless technology used to identify and exchange information with physical objects through radio waves. An RFID system typically consists of a reader and one or more tags that the reader can communicate with. The information exchanged is typically a unique identifier, although tags may also store additional data depending on the application. RFID is ubiquitous in many industrial applications, such as inventory tracking, electronic toll payments, contactless keys, and credit cards. RFID has become the de facto standard when needing to transmit and store small amounts of data that ought to be associated with a specific physical object.

Ultra High Frequency RFID (UHF RFID) is a branch of RFID technology that allows for communication over significantly longer distances than inductively coupled RFID systems. Unlike traditional RFID systems, where tags are energized through near-field electromagnetic coupling, UHF RFID operates in the far field and is instead energized by radio frequency signals transmitted by the reader. The tags modulate and backscatter this signal to transmit information, such as their ID [1].

Although RFID systems are primarily designed for identification and tracking applications, the physical-layer information available during communication can also be utilized for sensing purposes. Measurements such as signal strength and phase are influenced by the position and surroundings of a tag, making it possible to infer aspects of its spatial behavior.

1.1 The use for RFID in motion sensing

UHF RFID systems are highly sensitive to spatial and environmental changes. Variations in tag position, nearby materials, and other nearby tags all influence the backscattered signal [2]. As a result, measurements such as phase and RSSI change in response to movement and environmental factors. This has motivated the use of RFID in sensing-oriented applications, where the signal is analyzed to infer the spatial behavior of a tag.

One particular area in which both motion sensing and the ability to distinguish between multiple signal sources is important is respiratory monitoring. By attaching tags to different regions of the chest, it becomes possible to observe the periodic motion associated with breathing while maintaining separate measurements for each

tag [3]. This potential for detailed non-invasive respiratory monitoring is the primary motivation for this work presented in this thesis.

The widespread use of UHF RFID systems and their ability to uniquely identify multiple nearby tags make them attractive candidates for sensing-oriented applications. However, previous studies have also highlighted limitations when using commercial RFID readers for this purpose. While commercial systems are designed for tasks such as inventory tracking and object identification, sensing applications require continuous and detailed measurements of signal behavior. The metrics provided by commercial readers are often limited in both granularity and transparency, which is an obstacle when trying to analyze causes of interference or develop custom signal processing chains for motion sensing.

1.2 The need for a custom solution

The potential of using UHF RFID for respiratory monitoring has previously been demonstrated using commercial readers [3]. However, the study also identified situations in which sensing performance deteriorated significantly, motivating further investigation into the underlying signal behavior.

It was discovered that under some conditions, performance significantly worsened. The authors theorize that this is due to multi-path interference of the backscattered signal. However, although the reader reports which tags it has read, phase and RSSI, it does not make the In-phase/Quadrature signal from the antenna available to the user. This presents an obstacle when trying to determine exactly what specific phenomena constitutes this "multipath interference". Furthermore, commercial RFID readers often offer little transparency or modularity in their signal processing pipelines. Without the ability to implement custom signal processing chains, it is not possible to optimize the system for the specific challenges of motion sensing or multi-path mitigation, since the onboard processing is adapted to high speed inventory retrieval rather than high fidelity signal analysis.

Several studies corroborate the experience of tags being interfered with by the environment or other tags [4] [2]. Measurement reliability has been observed to become an issue at as little as 90 cm of distance between reader and tag [3]. Placing tags on or in close proximity to certain materials can alter the tags signal [2], sometimes to the extent that no signal can be detected by the reader [5]. Tag interference is not unique to motion sensing applications either. In industry, terms such as "tag shadowing" are used to describe tags being unable to respond when covered by another [6]. So although the motivation for this work is respiratory monitoring, it is not exclusive to that application. Access to raw backscattered may be valuable in a wide range of applications where motion or environmental interactions need to be studied. The goal is to develop a system that enables investigation into the underlying mechanisms of multipath interference and signal degradation, thus helping guide future development of application-specific sensing systems.

1.3 Objectives and scope

The goal of this project is the development and testing of a system that makes the raw signal data of RFID communication available to the user. In addition, the system should be used to analyze this signal in order to make some assertions regarding if and when multipath interference takes place, and whether this is likely to present an obstacle in practice. The observations made here will be limited to determining if interference is taking place, and in what scenarios, rather than its exact nature.

The system should also be able to separate tag backscatter from the signal sent by the reader, as well as separate tags from one another in order to allow experiments with multiple tags. The system should be able to extract phase and RSSI from tag readings so that changes in these metrics during experiments can be analyzed and use to investigate interference between during different experimental conditions.

2

Theory

Trying to *sniff* UHF RFID communication is not a novel pursuit. Sensing the spatial behavior of tags, or simply hijacking the communication has been the motivation for several previous works. Thus, there is already precedent for using either wireless or wired setups in order to detect and analyze UHF RFID communication. This chapter will go over the basics of UHF RFID that have been utilized during this project, as well as a portion of previous research and how it relates to the work done in this project.

2.1 Basics of UHF RFID communication

Considering the project's use of UHF RFID technology, it is worthwhile to describe its most essential elements. In typical RFID systems, the tag or chip is energized via electromagnetic coupling to a reader. This induces current in the chips internal circuitry, allowing it to actively transmit its own signal back to the reader. In UHF RFID systems, tags are energized via radio waves sent by the reader which allows for communication over longer ranges, constituting the main benefit of UHF RFID systems. Instead of the tag generating its own signal to transmit, it instead modulates the waves sent to it by the reader. It does this by modulating its internal load impedance, thus changing how much of the signal it reflects. In one state, the antenna absorbs the energy to power the onboard chip, and in the other the tag reflects signal back [1].

When beginning an *inventory round*, a reader will start transmitting the carrier wave signal, which energizes the tags, and then transmit a query message. This query message can include, among other things, information about which tags should respond to the message, and how many available time slots there are for responding. Tags matching the query now respond by choosing a time slot and a random 16-bit number, called an RN16. Every tag has an internal counter to keep track of when they should reply. The tags select a random number within the available amount of time slots. The reader will then send out a *queryRep* command. The command makes all tags decrease this internal counter by one. The tags then backscatter their chosen RN16 number when their time slot arrives, which is when their counter reaches zero. If multiple tags reply at the same time, the reader will detect this and adjust the amount of time slots based on the number of collisions detected. When an RN16 is successfully decoded, the reader will *acknowledge* that specific tag [7].

The tag then replies with, among other things, its EPC number, which is its unique identifier. After transmitting its EPC, it will no longer respond to any messages during the current inventory round in order to reduce collisions.

The protocol allows the reader to be selective regarding which tags should respond during an inventory round. The protocol has the option of using a filter which allows the user to select which tags should respond depending on their EPC [7].

The commands explained in this section are not a complete description of the EPC GEN2 protocol. The protocol includes many more features that are not relevant to understanding this project. An example of simple series of commands can be seen in Figure 2.1.

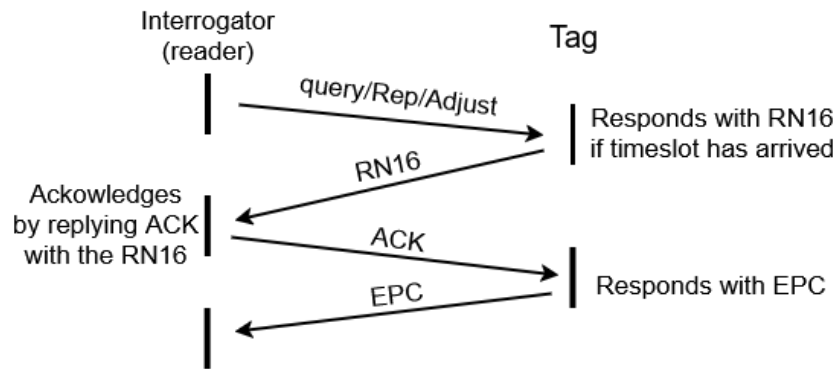
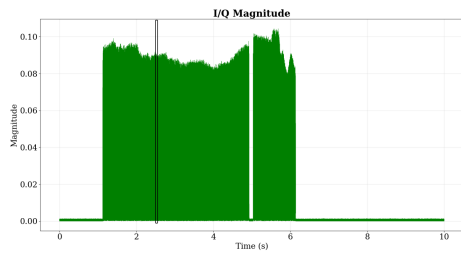


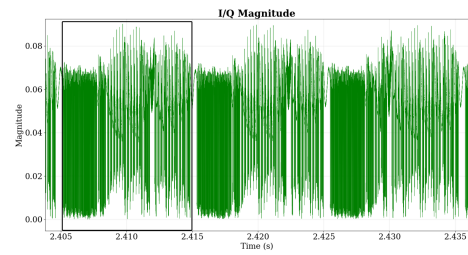
Figure 2.1: A diagram showing a series of EPC GEN2 commands.

2.1.1 The captured signal

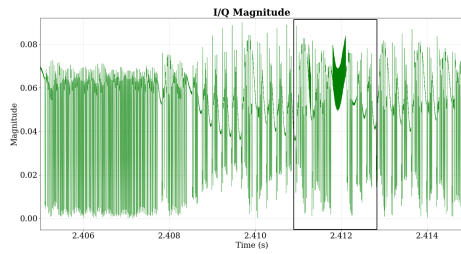
An example of a signal is provided to help garner intuition regarding what the actual communication sequences look like in the captured signal. A step by step zoom-in on captured signal is shown in Figure 2.2. The marked segments in Figure 2.2d show the RN16 and EPC respectively. It is important to note that in the current operating mode, the RN16 right before EPC will always belong to the same tag.



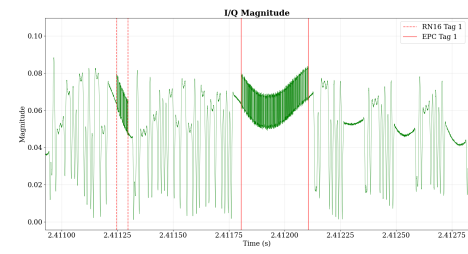
(a) The full captured signal



(b) The captured signal zoomed in to show three repeating inventory rounds



(c) The captured signal zoomed in to show one inventory round



(d) The captured signal zoomed into a single RN16 and EPC pair

Figure 2.2: Different zoom levels on a typical captured signal.

2.2 Previous research

This section will cover some previous research in the area, and how it relates to this project.

2.2.1 Hardware setups

Using a separate device such as an SDR for capturing tag communication has been explored in several previous works. Some studies have resorted to developing completely custom readers [8] [9], but this requires in-depth protocol knowledge, as well as the permission to send powerful signals over the 868 MHz band (in the EU), both resources currently lacking. As a result of the complexity of the protocol, the resulting systems also lack the level of reliability that might be desired for projects of this nature.

More commonly, authors resort to using an Impinj R420 or similar in combination with an SDR to capture the data. Different methods have been used to direct the signal to the SDR. One explored method has been to use a so-called "directional coupler" to split the signal [4]. A directional coupler is a passive RF component that allows signal to pass through it almost unimpeded in both directions, but also couples a bit of the signal flowing in one direction, allowing reading the signal flowing in one direction while attenuating the signal flowing in the other. This would mean being able to sample the signal received by the reader antenna, while receiving comparatively little of the signal sent by the reader.

A benefit of this approach is that the phase and RSSI readings should be the same or very closely match those reported by the reader, making verification of functionality simpler. It also reduces the amount of variables that can affect results. This, however, requires a directional coupler of certain specification. It cannot attenuate the coupled signal too much, since then it becomes difficult to read the already weak back scatter, while at the same time attenuating the signal from the reader unit to the antenna as to not destroy a sensitive SDR. The couplers that were easily available for this project were not of a specification compatible with this task. It was decided to use an antenna instead.

Studies have used different methods for moving a tag in space, ranging from placing the tag on a small robot [4] and elaborate constructions allowing arbitrary translation in a volume [2]. None of these are highly relevant to this project, since the desire is to have highly stable, small, and predictable movement in a single axis.

2.2.2 Detecting tag backscatter

In setups where an SDR is used, it is necessary to be able to separate tag backscatter from the rest of the signal environment. One previously explored method for detecting backscatter is the use of a matched filter. A matched filter convolutes a known signal template with the signal to be analyzed, and the resulting magni-

tude is a function of how strong of a match there is between the signals, as well as their amplitude. A matched filter involves convoluting a signal with a template of a known signal, seen in Eq 2.1 where h is the known template.

$$y[n] = \sum_{k=-\infty}^{\infty} h[n-k]x[k] \quad (2.1)$$

This approach can be exploited due to the fact that all sequences of data sent by a tag starts with a certain pattern called a "preamble". If backscatter is strong enough compared to the rest of the signal, it could be trivial to detect tag backscatter. This, however, requires that the signal behaves similarly to the idealized template, and that the backscatter has a strong enough amplitude compared to the rest of the signal. The captured backscatter is frequently too weak to easily differentiate from the rest of the signal with this method.

Some authors have developed custom metrics [2] for identifying tag responses. A spectrogram is restricted to the band around the expected frequency of the backscatter subcarrier. Then, the ratio between the peak and RMS power within that band is used as an indicator for whether a tag response has been detected or not. This metric works in cases where the reader itself fails to decode the response, since it is not reliant on decoding the tags. This is a reliable technique in environments where backscatter is occasionally weak, since it will still exhibit characteristics that are unique in its environment. This will inform the approach taken in this project.

2.2.3 Extracting metrics

Phase and RSSI are the most commonly used metrics for analyzing the spatial behavior of tags both in custom and commercial hardware setups. Both phase and RSSI are affected in predictable ways when a tag moves. When distance increases between a reflector and antenna, the received signal strength will decrease. In our case, strength of the received signal will decrease by the square of the distance. The closer a tag is to a receiving antenna, the larger the difference in signal strength for a distance moved since it presents a larger relative increase in distance.

Extracting RSSI is a straightforward endeavor as it is obtained using Equation 2.2, but the phase requires more processing to make it a valuable metric. The phase of the backscatter is relative to the carrier wave so one needs to predict the phase of the carrier wave at the point where backscatter occurs. Previously this has been done using linear fit to the carrier wave segments that precede the backscatter, which is what will be done in this project.

$$\text{RSSI}_{\text{dB}} = 10 \log_{10} \left(\frac{1}{N} \sum_{n=0}^{N-1} (I[n]^2 + Q[n]^2) \right) \quad (2.2)$$

The signal processing done on in the reader's firmware introduces a 180° phase ambiguity according to the manufacturer [10]. The absolute phase of a signal does

not matter for decoding it, so it is not reported. Phase also has inherent discontinuity since it wraps around every 360° . Previous studies have utilized different methods for handling this ambiguity. One method is to use the sign of the backscattered signal relative to the reader's carrier wave if the signal quality allows for it. In case that the reader's reported phase is used, it can be unwrapped using the following algorithm [3]:

1. If the difference between two consecutive phase measurements is between 90° and 270° , apply a $\pm 180^\circ$ correction depending on sign.
2. If the difference between two consecutive measurements is greater than 270° , apply a $\pm 360^\circ$ correction depending on sign.

Note that this does not have to be applied on phase measurements made by an SDR, since it does not pass through the reader's processing chain, which is what introduces the ambiguity. The algorithm is only used on the phase reported by the reader.

3

Development and implementation

In order to capture the signal and analyze the relevant parts of it, software needs to be developed in order to process the signal and automatically extract the desired information. This chapter will cover the methods used to extract this information as well as the hardware needed to acquire it. The entire signal processing chain can be seen in Figure 3.4.

3.1 Hardware setup

The approaches for gaining access to the IQ signal has differed between studies. Most commonly, an SDR has been used to capture the signal. This project will utilize a National Instruments USRP 2901. For an SDR to capture signal, an appropriate antenna needs to be used. A patch antenna was chosen since these were easily available and exhibit relatively high directionality. An Impinj R420 UHF RFID reader was used in combination with an Alien Technologies high gain antenna, henceforth referred to as the reader and reader antenna respectively. A diagram of the entire setup can be seen in Figure 3.1.

This setup allows the user to change multiple parameters in the system that would otherwise be constant. The antenna can be moved closer to the tag, increasing its signal strength relative to the signal from the reader. It is beneficial to use a directional antenna in order to reduce interference by the reader signal. This is done by pointing the antenna towards the tag so that the tag and the antenna have their biggest lobes pointed facing each other. There are multiple options for making a tag move in space. It is important that this movement, for the sake of replicability, is predictable and constant. Placing the tag on the chest of a human or a medical simulation mannequin may affect the impedance of the tag [5], and thus how reliable its readings are. The hardware setup used is already sensitive to variations in distance, so it is necessary to eliminate as many sources of error as possible in order to not introduce unpredictable variables to the system. Instead, a simple machine was constructed to move tags back and forth. The machine allows the user to set a motor speed, and a period time for sinusoidal motion. The device lacks the ability to detect how far the tag has moved. The distance the tag moves has to be measured manually. The machine and an example tag placement can be seen in Figure 3.2.

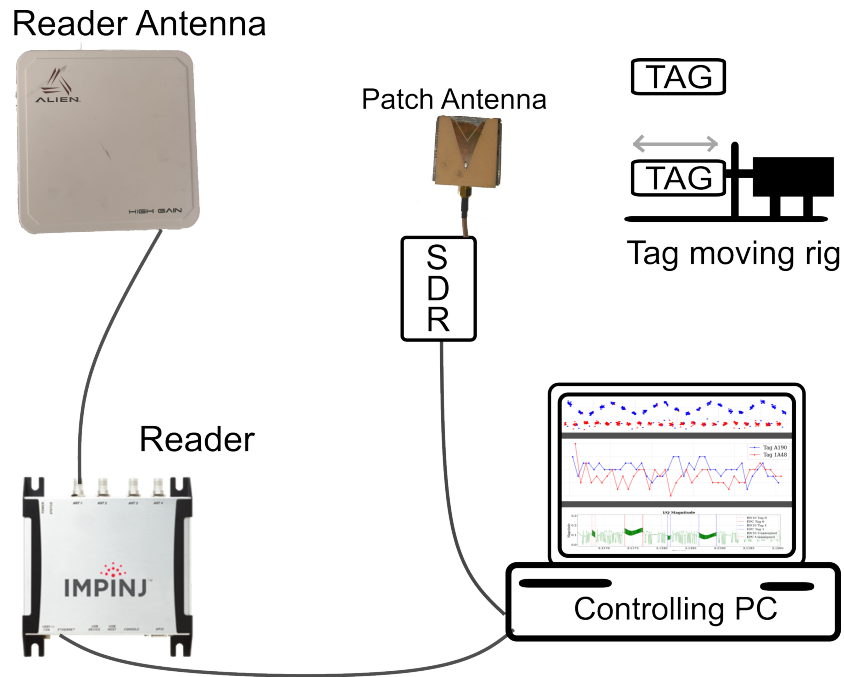


Figure 3.1: A diagram of the experimental setup.

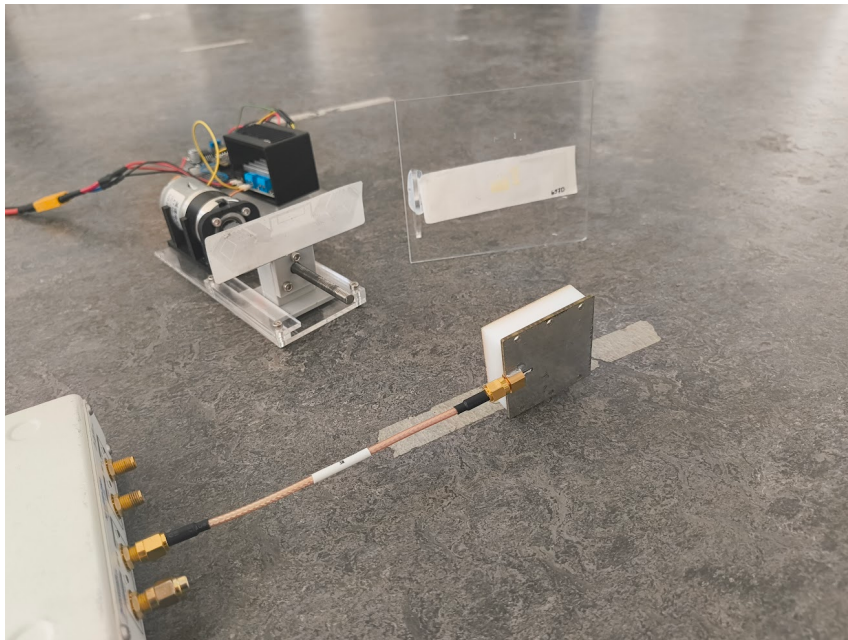


Figure 3.2: Two tags in front of the patch antenna. One tag is placed on the tag-moving rig.

3.2 Detecting tag backscatter

The backscatter from tags exhibits properties that are unique to data sent by tags. One property that differentiates the back scattered signal from the reader is the speed at which it delivers data, both in symbol rate and bandwidth. From looking at the signal, it is apparent that the internal switching times for the tag are a lot faster than those of the reader. The EPC GEN2 protocol only requires the reader to adhere to certain rise and fall times maximums, it does not require the tag to adhere to any specific switching speeds [7]. The inner workings of a tag, however, allow for, and benefits from, high switching speeds. Field-Effect Transistors in the tags often switch states in the nanosecond range. This is significantly faster than the maximum allowed rise times of an interrogator, which are dictated by the protocol. From testing, it has never been the case that noise has transients as fast as these switching times.

The rapid switching of the tag impedance causes sudden changes in the tag's contribution to the received signal. These transitions appear as jumps between samples in the I/Q plane. Taking the derivative of the complex I/Q signal measures this change between samples, producing large responses while the reader signal, which varies quite little sample to sample, is suppressed. This behavior can be seen in Figure 3.3. As the tag switches states, the received signal oscillates closer and further away from the origin in the I/Q plane.

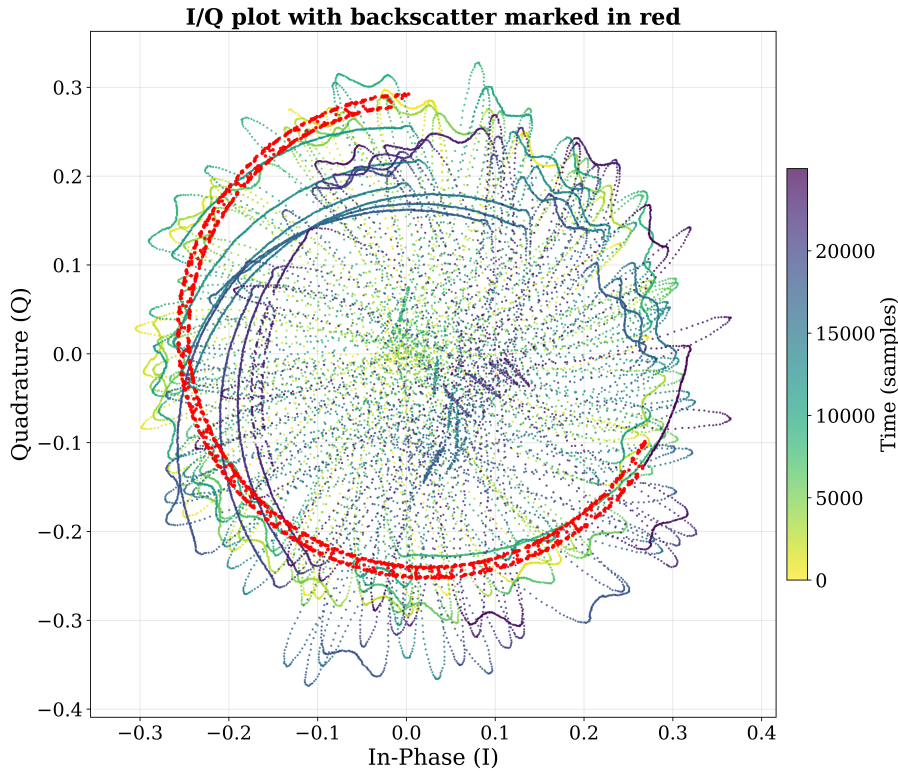


Figure 3.3: The complex I/Q signal representation of the received signal. The samples acquired during the backscatter interval are marked in red.

The implementation of the derivative can be seen in Equation 3.1. Taking a k -th order derivative just involves repeating this operation k times.

$$x'[n] = x[n + 1] - x[n] \quad (3.1)$$

Applying the difference operator a second time yields the second-order finite difference:

$$x''[n] = x'[n + 1] - x'[n] = x[n + 2] - 2x[n + 1] + x[n] \quad (3.2)$$

Since the I/Q samples are complex-valued, $x[n] = I[n] + jQ[n]$, this operation acts component-wise on the in-phase and quadrature components:

$$x''[n] = (I[n + 2] - 2I[n + 1] + I[n]) + j(Q[n + 2] - 2Q[n + 1] + Q[n]) \quad (3.3)$$

Taking the absolute value of this expression finalizes the operation.

Using a simple threshold on the amplitude of the second derivative is a reliable way to detect tag backscatter in this signal environment. Using the second derivative here is arbitrary. One can increase the derivatives indefinitely (within reason). This project will use the second derivative since higher orders has not presented itself with any benefit. It is important to note that this operation is performed on the complex I/Q signal, and not on the signal magnitude envelope.

3.3 Identifying and decoding tags

Since the goal of the project is to be able to analyze how tags interfere with each other and the environment, it is important to be able to both determine which tag the backscatter belongs to, and be able to extract key metrics about the signal, such as phase and RSSI.

The most apparent solution would be to use the information provided by the reader via its SDK. The SDK allows the user to program the reader. The reader reports which tags it has read, their phase and RSSI, and when it has read them. However, it can be seen that these reports do not perfectly align with the EPCs. It is also apparent that the tags actually backscatter their EPCs more frequently than the reader reports one being read. It can also be noted that tags reads, due to the nature of the protocol, do not always happen in the same order the reader reports. It is also the case that the reader reports multiple reads as happening at the same time, which is not possible.

One way to remedy this would be to utilize the filtering functionality present in EPC GEN2 protocol. Ideally, the filter could be changed in the middle of an experiment in order select which tags respond to the message. Then it would be certain that any backscatter within that period belongs to a certain tag. However, the reader cannot be actively transmitting signal when this filter is changed. This does not appear to

be a limitation of the protocol, but of manufacturer implementation. When changing the tag filter, the reader must be powered off and then on again. This process takes around 100 ms and drastically limits the amount of tag reads that can be made within a certain time period if one desires to switch which tag is read frequently. In order to get as many data points as possible whilst handling multiple tags in the tag space, it is apparent that the decoding of tags needs to be done using a custom solution.

3.3.1 Backscatter detection and classification

First, the tag backscatter needs to be classified into what type of reply it is (EPC or RN16). The RN16 does not contain any unique data, so it does not need to be decoded. The most clear way to tell the different types of replies apart is the amount of time that they occupy since RN16 messages are much shorter. By finding the beginning and end of these signals, their type can be determined before trying to decode them.

Although the second derivative has been used to detect the tag backscatter occurring, it is not specific in what part of the backscatter it captures. The algorithm merely finds the first peak above a certain threshold, and if it does, ignores any peaks within a following short time period as to not give more than one detection per backscatter. In order to find the edges of the signal, an algorithm was made to "walk" along the signal. This involves using the second derivative of the signal, traversing along it in a chosen direction, and finding when the second derivative stops oscillating. This algorithm can be found in Appendix A.1. When there has been no significant peak in the second derivative within a reasonable time frame, the last detected peak is set as the beginning or end of the backscattered signal.

3.3.2 Decoding the tag's identity

Once the boundaries of the backscatter have been established, tags can now be decoded. One way to achieve this is to remove low frequency and DC components of the signal to make it oscillate around zero. When the signal flips sign, it is likely that it has flipped state, if this processing is done correctly. This is done by discarding all frequency components below 100 kHz. This number is somewhat arbitrary, but has worked well for the purposes of this project.

Tags can utilize several different methods of encoding data, but for this project, the tags are set to use FM0 encoding. This is configured via the reader, and the required protocol is then transmitted during the start of an inventory round. The FM0 encoding works via these three rules:

1. The signal always changes state at the start of a bit window
2. A logic 0 includes an extra change of state in the middle of the bit window
3. A logic 1 includes no change of state.

It is via this logic that the signal can be decoded into bits, and then into a more

human-readable representation. For this to work reliably, the code needs to take into account the fact that bits will not align perfectly due to imperfect detection of the beginning of the signal, meaning that some margin of error is required. FM0 is a timing-based protocol, and requires a state change at set intervals. The relative weakness of the backscatter, as well as an imperfect method of handling the decoding means that the system is highly sensitive to when it is able to decode the tags. When given a high SNR signal, the system will decode the same identity for a single tag reliably. This is different, of course, from reliably decoding the *actual* identity of a tag. The system does not currently provide the user with a decoded EPC, but rather a decoded version of all the bits sent during the same backscattered segment as the EPC. For the purposes of this project, this yields the same benefits since tags can still be uniquely identified. Since the system extracts and decodes a raw bit-stream rather than protocol-compliant EPCs, the user is required to associate these decoded patterns with specific physical tags. During setup, the user isolates a target tag using the commercial reader's firmware filter (a configurable internal filter) and records the resulting identity decoded by the system. This sequence is then added to a reference library, allowing the system to uniquely identify the tags in the subsequent experiments by matching real-time captures against these known signatures.

3.4 Extracting metrics

Along with a tags EPC, the commercial reader also reports the phase and RSSI of each tag read. These are therefore the most interesting metrics to capture since they can be compared to an reliable control. These metrics also happen to be useful when determining a tags spatial behavior. Thus, these were the main metrics used during this project.

3.4.1 Extracting RSSI

The RSSI is measured by applying eq 2.2 on the backscatter signal. It is worth noting, however, that this signal is not strictly backscatter. The signal measured by our SDR is a combination of both the signal sent by the reader and the signal reflected by the tag. When a tag moves, however, a difference should still be visible since the combined signal will still be weaker.

3.4.2 Extracting phase

Extracting the phase is a slightly more involved procedure. Just plainly extracting the phase according to eq 3.4 will not yield any comprehensible result. Because the tag modulates an existing carrier, the phase captured by the SDR is inherently relative to the readers transmitted signal. Furthermore, the LO in SDR introduces as a frequency offset which manifests as a linear phase drift over time. In order to extract the phase of the backscatter itself, and compensate for potential frequency offsets, the phase contribution of the readers signal needs to be predicted. The EPC

GEN2 protocol requires a carrier wave period of at least ten symbol be transmitted before a tag replies. This period of high SNR signal right before the backscatter makes a good candidate for predicting the phase. A short period of the RN16 is analyzed to obtain this data. The RN16 is shorter than the EPC, and therefore subject to less phase drift due to potential drift in the LO.

During the CW period the instantaneous phase evolves approximately linearly according to:

$$\varphi(t) = 2\pi\Delta f t + \varphi_0$$

Where Δf is the frequency offset between the LO and the received CW. A linear fit to the unwrapped CW phase is used to estimate the drift rate and the initial phase offset. The resulting fit is extrapolated to the start of the RN16 to estimate the phase contribution from the CW at that instant, which is then subtracted from the measured phase of the tag.

$$\varphi = \tan^{-1}\left(\frac{Q}{I}\right) \quad (3.4)$$

3.4.3 Pairing data-points with tags

In order to know which tag a certain extracted data point belongs to, the RN16 which the data is obtained from and an EPC need to be matched together. According to the EPC GEN2 protocol, the RN16 preceding an EPC will always belong to that EPC. It can be seen in the obtained signal that only a single RN16 precedes every EPC, split only by an *Acknowledge* command from the reader. This is not strictly necessary, but it is useful to be able to analyze both RN16s and EPC backscatter segments to see potential differences, if those were to occur. The RN16 is shorter, so measuring it in its entirety leads to less phase drift compared to measuring the entire EPC, as discussed in subsection 3.4.2. One could, of course, avoid this by extracting measurements from just a short segment of the EPC, but this approach is more versatile and follows precedent set by previous studies. This process is independent from the process of extracting metrics, seen in Figure 3.4.

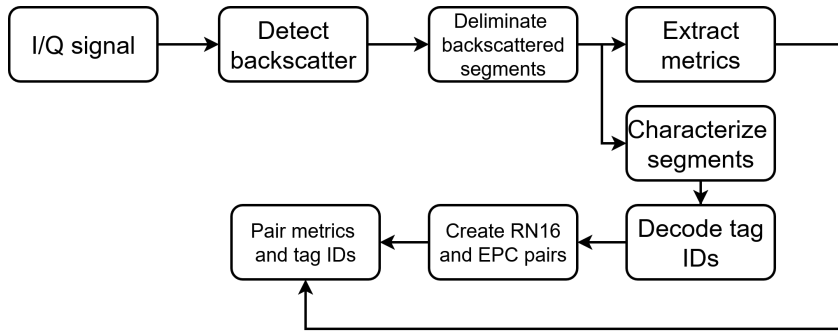


Figure 3.4: A block diagram of the signal processing chain used.

3.5 Experiment design

The experiments performed during this project were designed progressively out of necessity, as new insights given by previous results informs future testing. The initial experiments aim to validate basic signal detection and decoding. These experiments are performed under static conditions in order to establish baseline signal behavior and verify that the extracted measurements do not exhibit systematic patterns that could be mistaken for motion. After this has been established, experiments introducing movement and multiple tags are made. This staged approach helps isolate failure modes and allows individual system components to be evaluated independently before examining more complex environmental interactions.

The experiments are not intended to provide a performance benchmark for what the system is capable of since measurements are highly dependent on hardware configuration and environmental conditions. The experiments are designed to estimate the systems ability to consistently detect, separate, and analyze tags, as well as analyzing potential interference between tags were it to occur.

All experiments were performed multiple times, and the presented examples are chosen because they are representative of the general outcome of the trials.

3.5.1 Controlled variables

During experiments involving motion, both in single tag and multi-tag scenarios, some variables are constant and some are controlled modified depending on the experiment. All modified variables will be described as the results are presented.

The distance between the reader and tags is kept at constant 220 cm, except for when the tag is moving. It is always set so that the tags furthest point from the reader during sinusoidal motion is approximately 220 cm. The signal environment is also kept as constant as practically possible. The experiments are performed in the same room with nothing blocking the direct signal paths except for the antennas themselves.

Any changes made in the setup will be addressed before results are presented. The variables that are occasionally modified are:

1. which tag that is used
2. the distance between the patch antenna and the tag
3. the amplitude and frequency of the sinusoidal motion
4. distance between tags in multi-tag experiments
5. if tags are read simultaneously or sequentially (i.e setting the firmware filter for one tag at a time)

3.5.2 Metrics

Since measurements are swayed by antenna placement and hardware configuration, the experiments will not be evaluated primarily through performance metrics. Instead, the evaluation focuses on the systems ability to consistently detect, characterize, and decode backscatter. In experiments involving moving tags, more qualitative analysis is warranted.

Under static conditions, the results are evaluated based on the successful decoding of tags and reliable measurements absent of periodic patterns. In experiments involving controlled sinusoidal movement, the extracted data is evaluated based on whether it exhibits periodic variations coherent with the motion of the tag. Coherent behavior refers to repeated changes in RSSI, phase, magnitude, or the differentiated signal occurring with approximately the same frequency as the imposed movement.

4

Results

This chapter outlines the different experiments performed and their results. For an interpretation of the results, see chapter 5.

4.1 Single Tag experiments

These experiments are performed with only a single tag in the tag-space. The readers firmware filter was set to only allow for a specific tag, and all other known tags were removed from the room. In order to gather what is shown in the figures, see Figure 2.2 for a step by step zoom in on a signal captured from a single stationary tag.

4.1.1 Different sizes of tags

Multiple types of tags were tested to see which tags provide the best signal for the following experiments that are more error prone since they involve multiple tags. A small tag, roughly $1\text{ cm} \times 5\text{ cm}$ in size, was placed on an acrylic plate, with a distance of 10 and 15 cm to the SDRs antenna, and a distance of 220 cm to the reader antenna. The resulting signal, including processing, can be seen in Figure 4.1. It is worth noting how specific the differentiated signal is to the backscattered signal, as even a weak signal results in a large spike. In this experiment, the tag was successfully decoded 50/139 times.

This test was repeated with other tags of similar size, and it was apparent that tags with a larger surface area had a more easily detectable backscatter. It is for this increase in signal strength that the larger tags are the ones used for the remaining experiments.

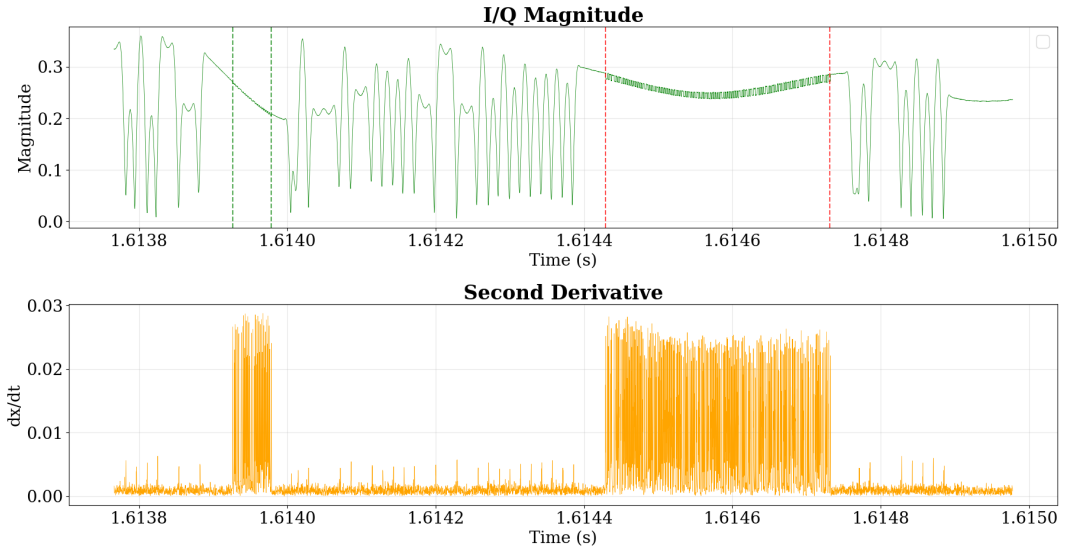


Figure 4.1: Single tag read of a smaller tag at a distance of 10 cm from the SDR antenna, and 220 cm from the reader antenna. Green and red lines mark the RN16 and EPC respectively.

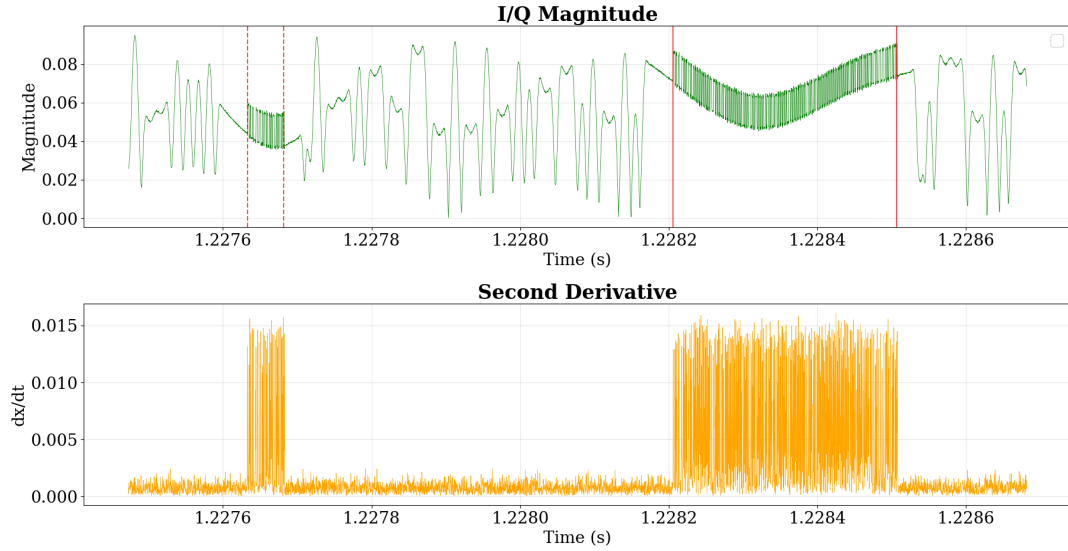


Figure 4.2: Single tag read larger tag at a distance of 15 cm from the SDR antenna, and 220 cm from the reader antenna. Red dotted lines mark the RN16, solid red lines mark the EPC.

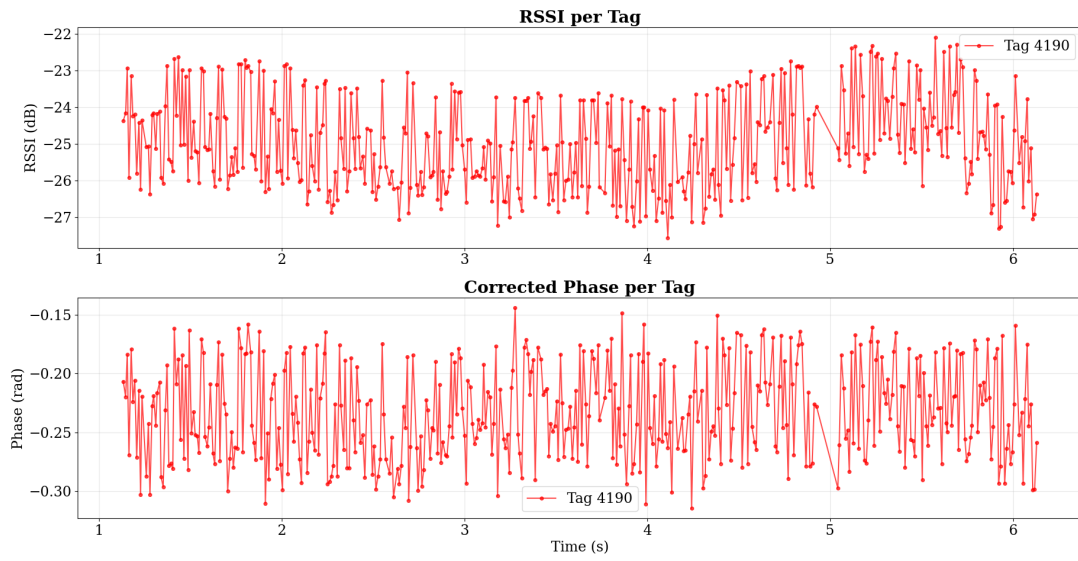


Figure 4.3: SDR measurements from captured signal for a single static tag.

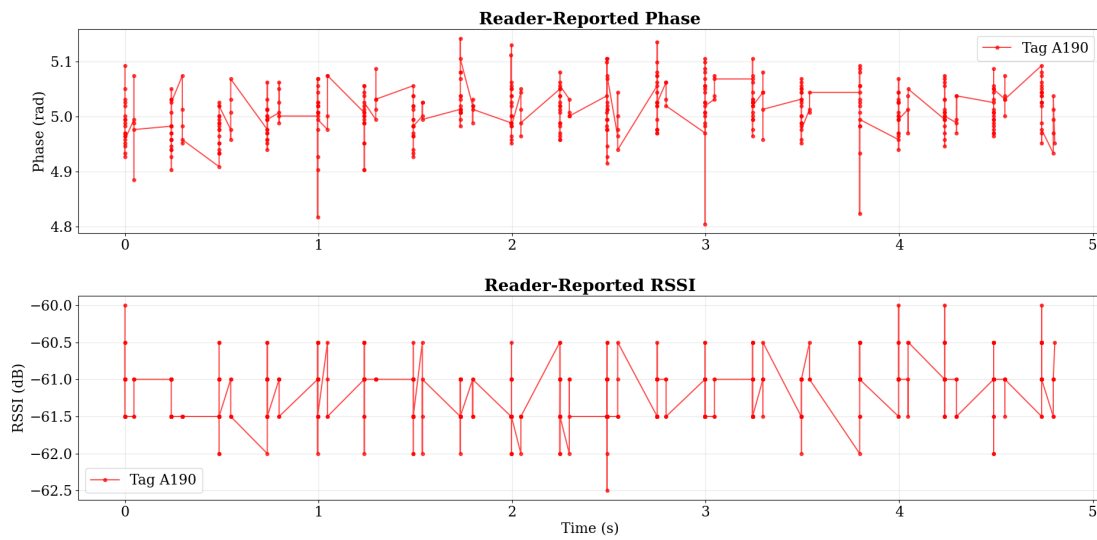


Figure 4.4: Reader reported RSSI and phase for a single static tag.

4.1.2 Different distances between SDR and tags

The system is highly affected by the distance between the reader and the tag. For the sake of experimentation, different distances were tested to see how quickly the performance of the decoding algorithm becomes inadequate to capture enough data points for reliable measurement of movement. When the tag is further away, the decoding success rate decreases.

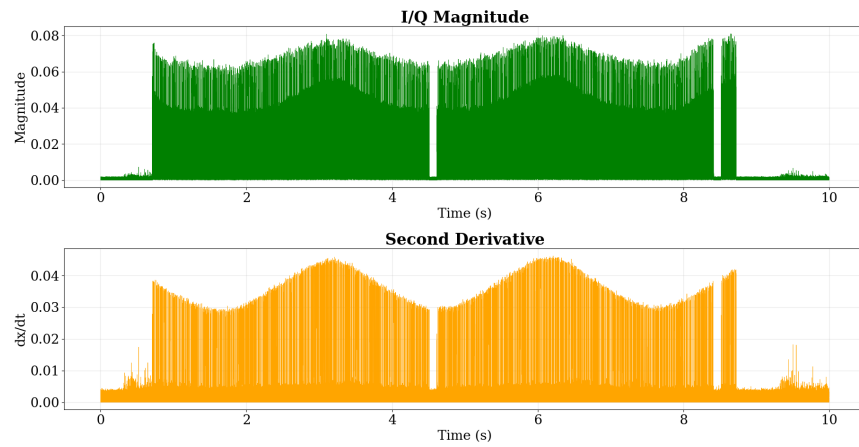
4.1.3 Single moving tag

In order to test the systems ability to capture movement of a tag, it was first tested using a single tag. It has become apparent that the received signal strength is highly dependent on the distance between the SDRs antenna and the tag. With this in mind, the experiments were constructed in such a way that the longest distance from the tag to the reader will still be within a low enough distance for the tag to be decoded reliably.

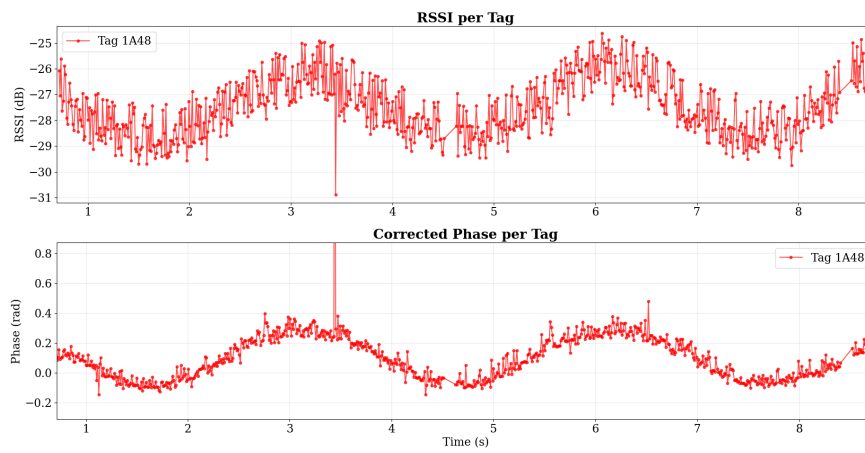
The motorized rig is used to move the tag back and forth. The tag moved in a sinusoidal pattern with an amplitude of 1 cm, resulting in 2 cm maximum displacement and a maximum distance of 12 cm to the SDR antenna. The sinusoidal had a period of 3 seconds. The result of this experiment can be seen in Figure 4.5. The tag was decoded successfully every backscatter. It is apparent that the differentiated signal, seen in the lower half of Sub-figure 4.5a is also capturing movement of the tag. The reader captures a weak pattern, seen in Sub-figure 4.5c. The same pattern can be seen in Figure 4.5b, which shows the data points calculated by the system.

Results varied since it seems the system is very sensitive to movement, and unlike the experiment shown in Figure 4.5, it cannot always be seen on only the magnitude of the signal that the tag is moving. It is, however, captured in the differentiated signal, and if the signal is clear enough it can also be seen in the phase. This is the case in the experiment shown in Figure 4.6. The experiment was performed with the same settings on the motorized rig, and at a maximum distance of 15 cm from the SDR antenna. The reader antenna was kept at a distance of 220 cm away from the tag. The tag was decoded 645/738 times.

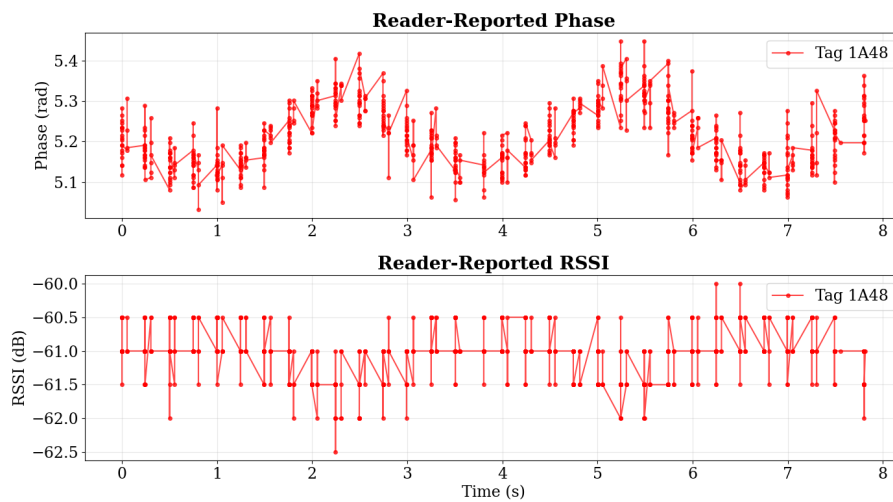
Different amplitudes of sinusoidal movement were tested. In the experiment shown in Figure 4.7, the tags total displacement was 1 cm over a period of 1 second at a maximum distance of 12 cm away from the SDR antenna.



(a) The captured signal of a single tag moving 2 cm back and forth

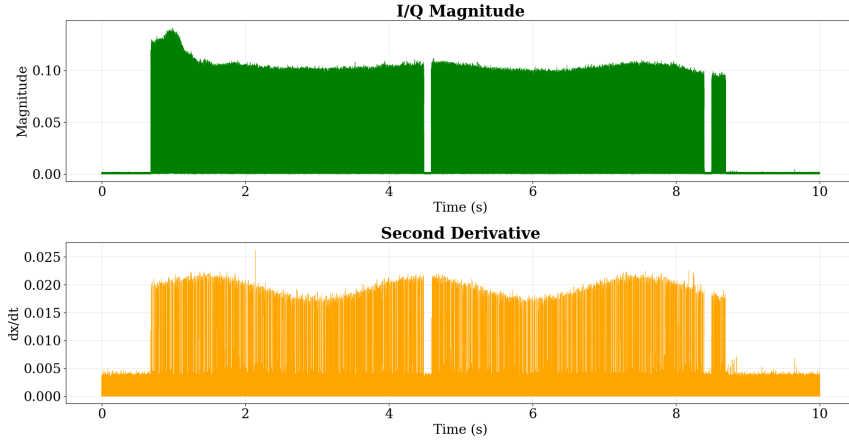


(b) The phase and RSSI measured by the system.

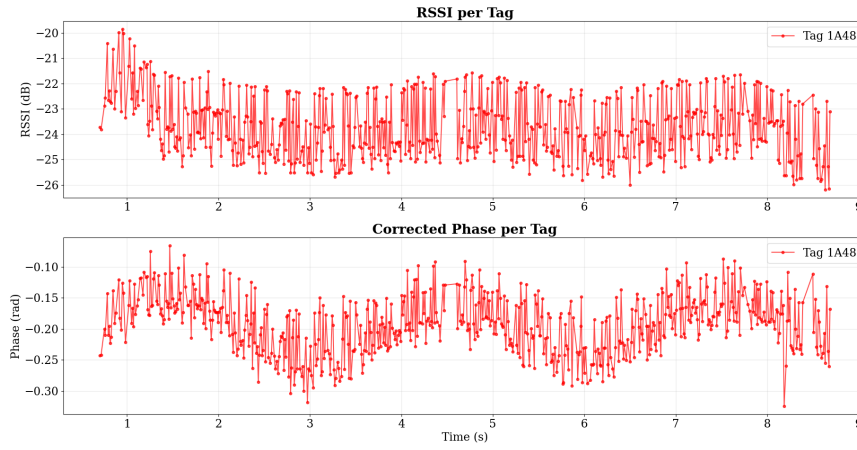


(c) Phase and RSSI reported by the reader.

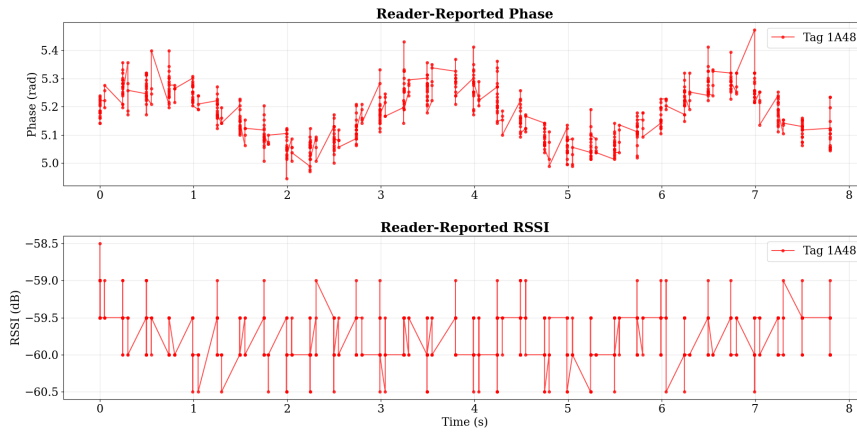
Figure 4.5: Signal of a single tag moving 2 cm back and forth. The tag was at most 12 cm away from the antenna.



(a) The captured signal of a single tag moving. 2 cm back and forth

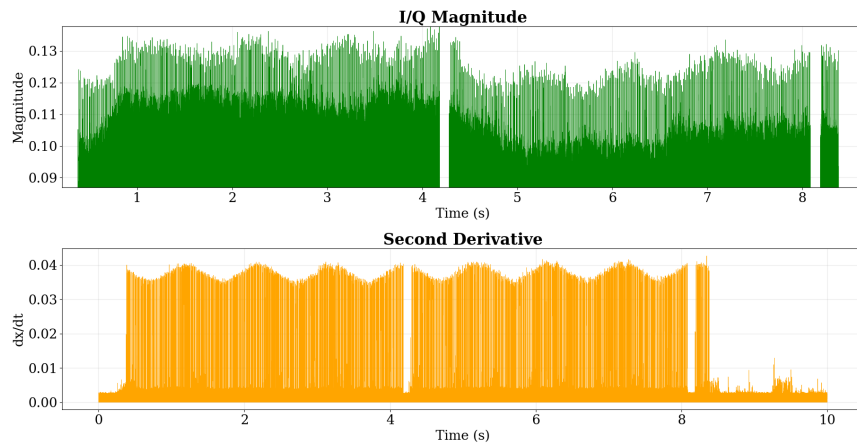


(b) The phase and RSSI measured by the system.

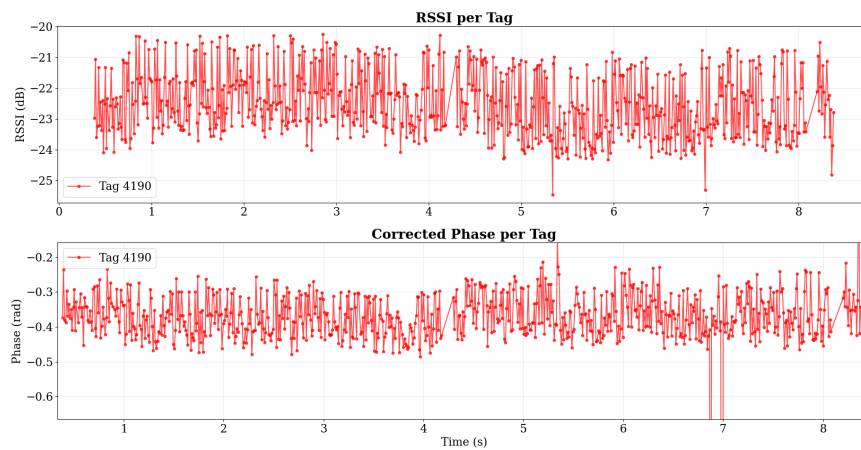


(c) Phase and RSSI reported by the reader.

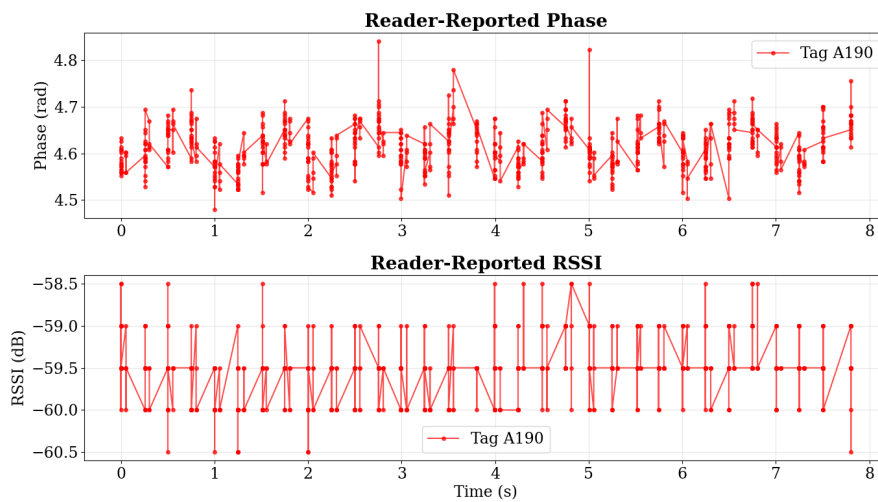
Figure 4.6: Signal of a single tag moving 2 cm back and forth. The tag was at most 12 cm away from the antenna. The movement can not be seen by looking only at the amplitude.



(a) The full captured signal.



(b) The phase and RSSI measured by the system.



(c) Phase and RSSI reported by the reader.

Figure 4.7: Signal of a moving tag with 1 cm displacement. The movement can not be seen by looking only at the amplitude.

4.2 Experiments with multiple tags

The experiments covered in this section all involve having multiple tags within close vicinity of one another. All the experiments involve moving tags.

4.2.1 Mute tag besides a moving tag

To ensure that the mere physical presence of multiple tags does not degrade signal integrity, a control test was conducted. In this experiment, a tag was placed around 8 cm (edge to edge) away from the moving tag, both in a horizontal orientation. This can be seen in Figure 3.2. The tag was 220 cm away from the reader at its furthest point, and the patch antenna was a maximum 12 cm away from the tag. The non-moving tag was placed on an acrylic plate. The moving tag was read in the same way as in previous experiments, and moved with a displacement of 2 cm with a period of 3 seconds. The non-moving tag was set to never backscatter any information by utilizing the readers built-in filter. The results, seen in Figure 4.8 show no discernible impact.

4.2.2 Two active tags in close proximity

The previous experimental setup was kept, as explained in Section 4.2.1. The results can be seen in Figure 4.9. Note that only one tag, the tag ending with ID *1A48* and marked in red is ever moving. It can be seen in Figure 4.9b, 4.9c that some interference is occurring. Although only one tag is moving, the one marked red in both plots, both exhibit changes in phase and RSSI. This behavior is seemingly not as visible in the differentiated signal, seen in the bottom of Figure 4.9a. In this experiment, the tag was successfully decoded 1216/1454 times.

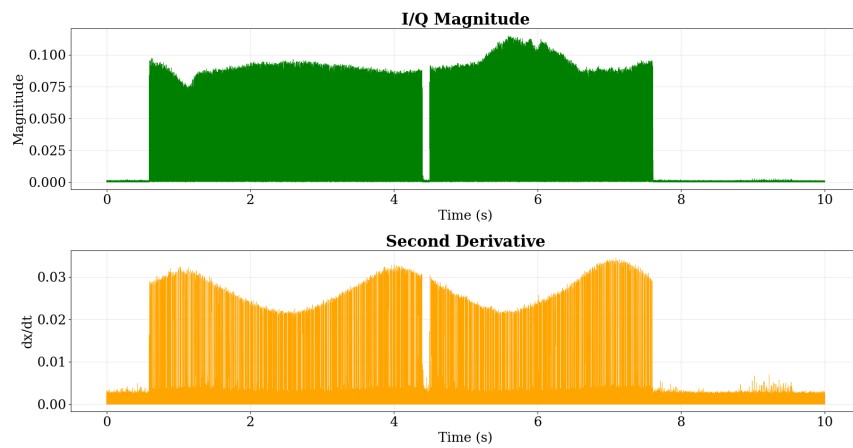
This interference becomes stronger when the tags are located closer to each other. In the experiment shown in Figure 4.10, the two tags were placed 5 cm from each other and in the same orientation. All other parameters were kept the same. The tags were decoded 1340/1372 times.

4.2.2.1 Different orientation of tags

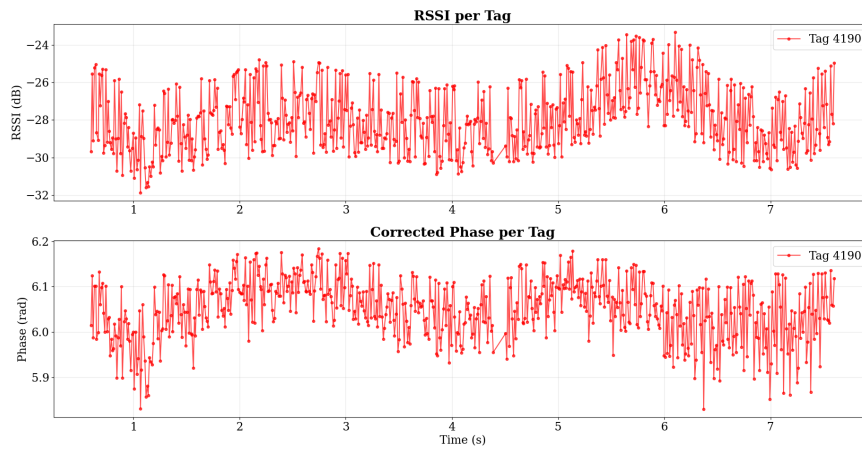
Keeping all other parameters the same, the still tag was now placed in a vertical orientation. The distance between the tags was still 5 cm between their closest points. The resulting captured signal can be seen in Figure 4.11.

4.2.2.2 Sequential and alternating reading of tags

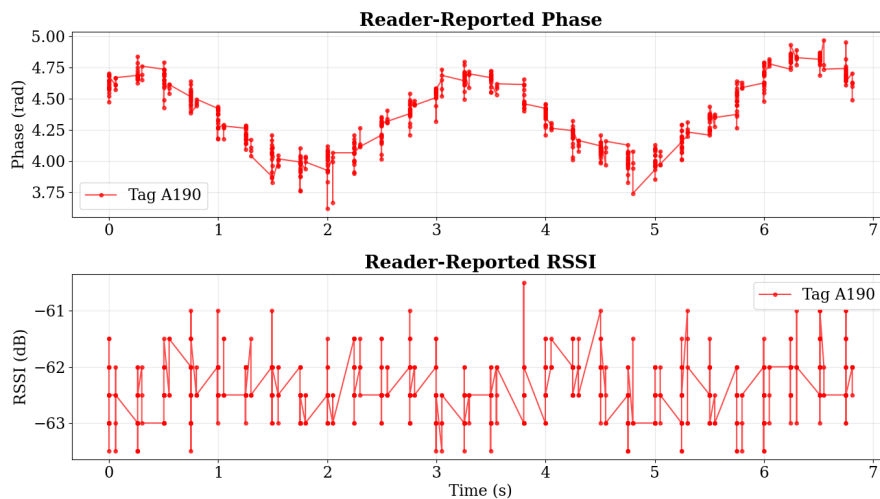
Keeping all variables the same, the reader was set to read each tag one at a time by utilizing the firmware filter. This requires the reader to be turned on and off when switching which tag is read. In the experiment, shown in Figure 4.12, the tags are read alternately. The non-moving tag exhibits sinusoidal pattern opposite that of the moving tag.



(a) The full captured signal of a tag placed next to another.



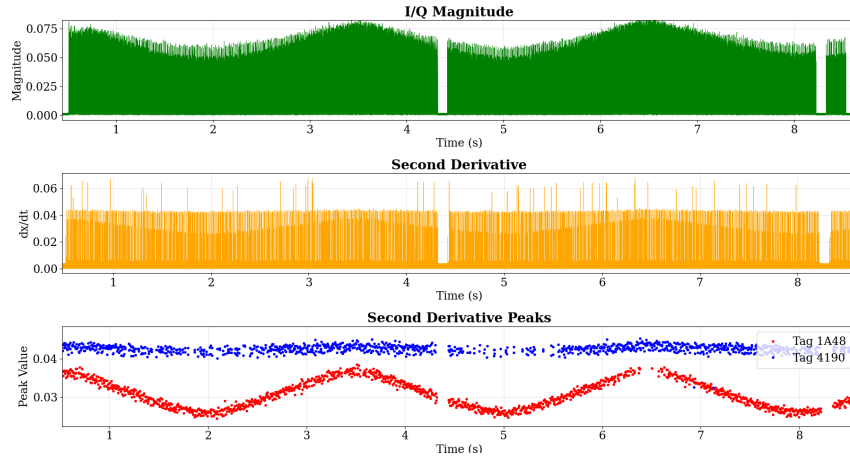
(b) The phase and RSSI measured by the system.



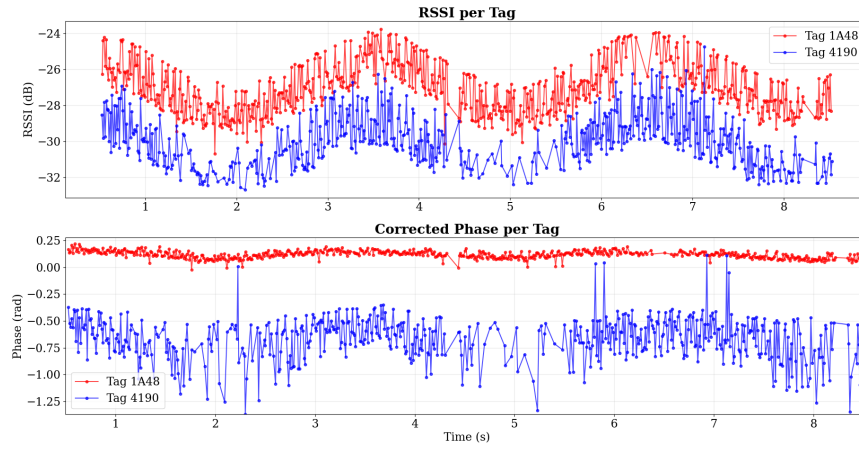
(c) Phase and RSSI reported by the reader.

Figure 4.8: Signal of a moving tag with 2 cm displacement. The movement can not be seen by looking only at the amplitude. A mute tag was placed next to the tag that is being read.

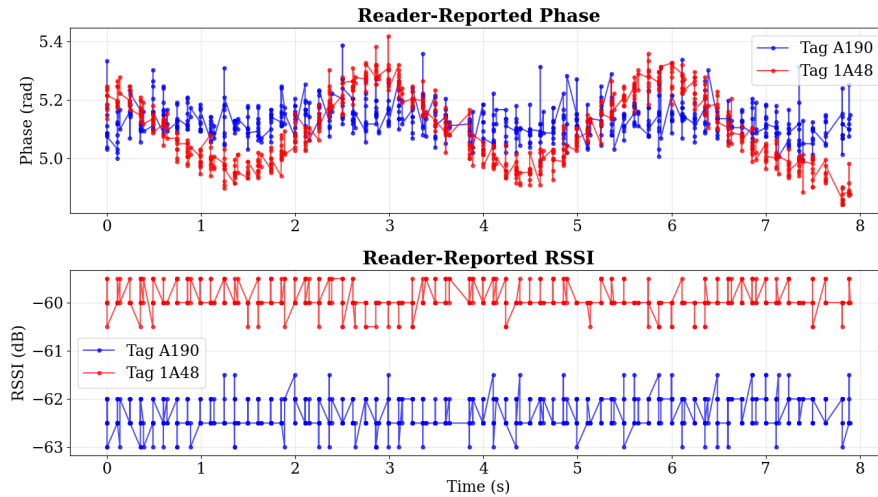
4. Results



(a) The full captured signal of two tags placed 8 cm apart.

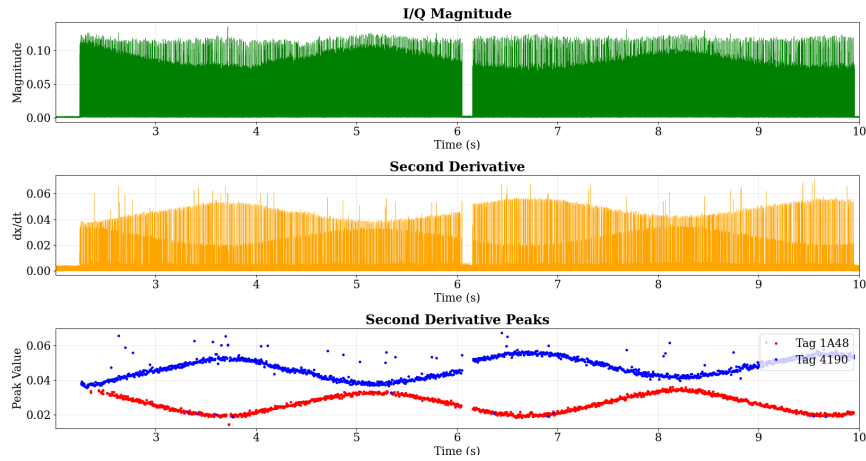


(b) The phase and RSSI measured by the system.

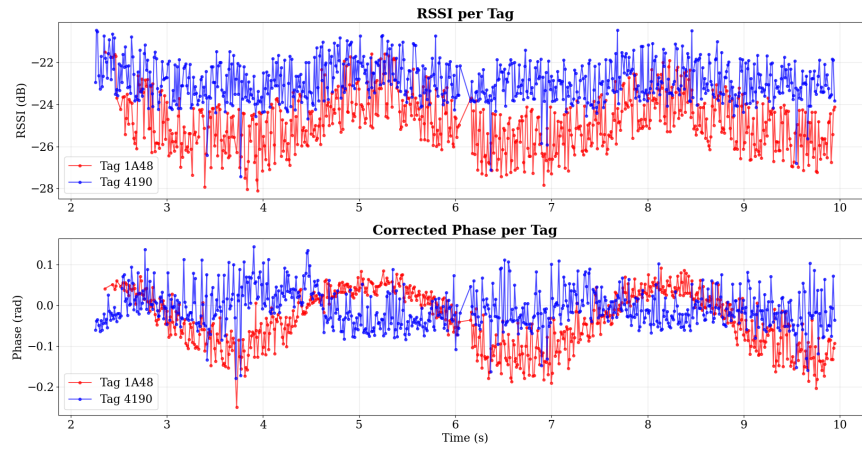


(c) Phase and RSSI reported by the reader.

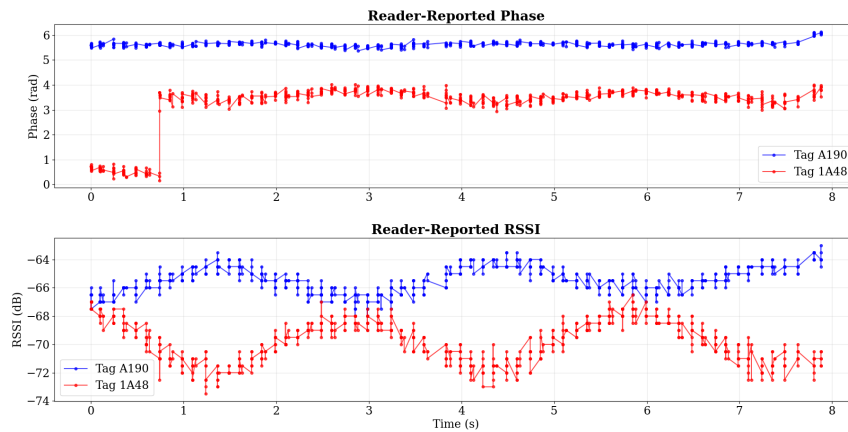
Figure 4.9: Signal of two tags, one of which is moving in a sinusoidal pattern with period 3s and a displacement of 2 cm. The still tag (blue) shows a sinusoidal pattern in phase and RSSI even though it is fixed in place. The tags were placed 8 cm apart.



(a) The full captured signal of two tags placed 5 cm apart.



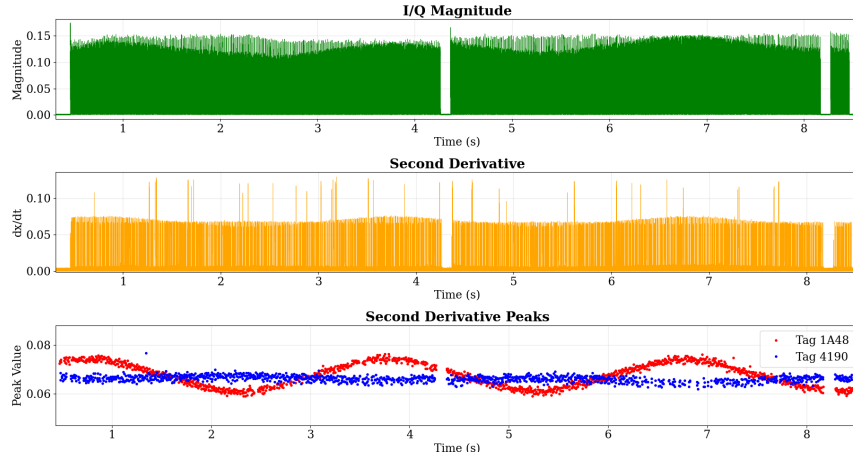
(b) The phase and RSSI measured by the system.



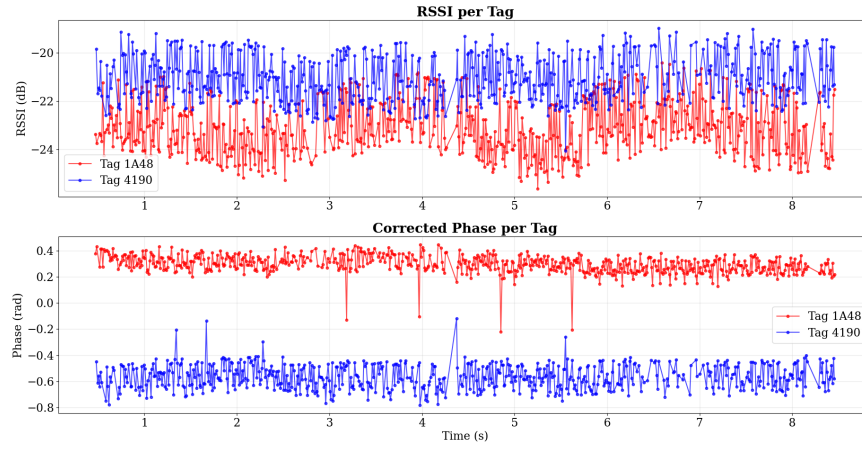
(c) Phase and RSSI reported by the reader.

Figure 4.10: Signal of two tags, one of which is moving in a sinusoidal pattern with period 3s and a displacement of 2 cm. The still tag (blue) shows a sinusoidal pattern in phase and RSSI even though it is fixed in place. The tags were placed 5 cm apart.

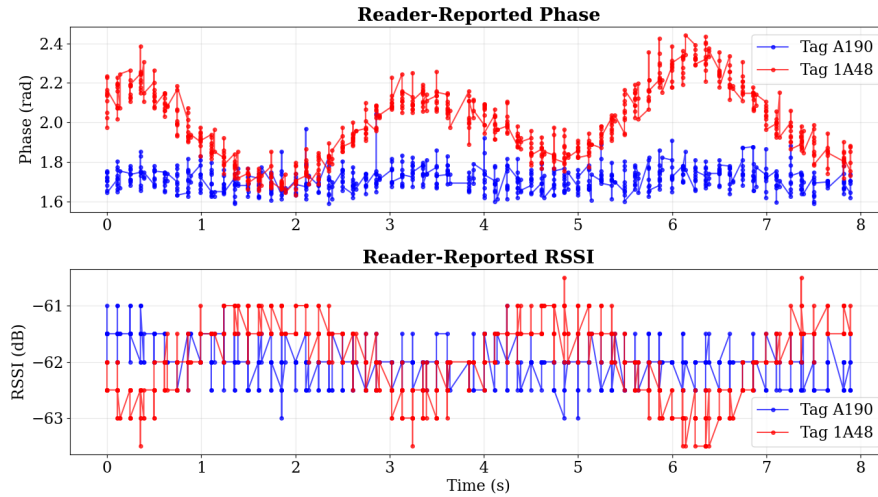
4. Results



(a) The full captured signal of two tags, one of which is vertical.

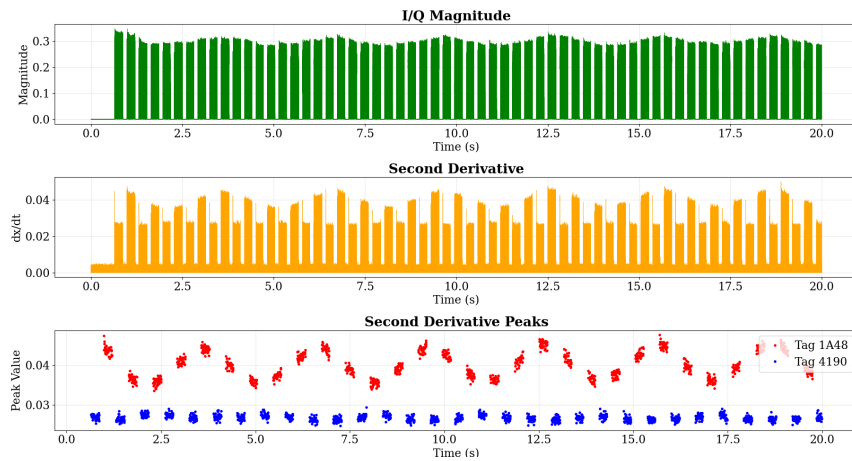


(b) The phase and RSSI measured by the system.

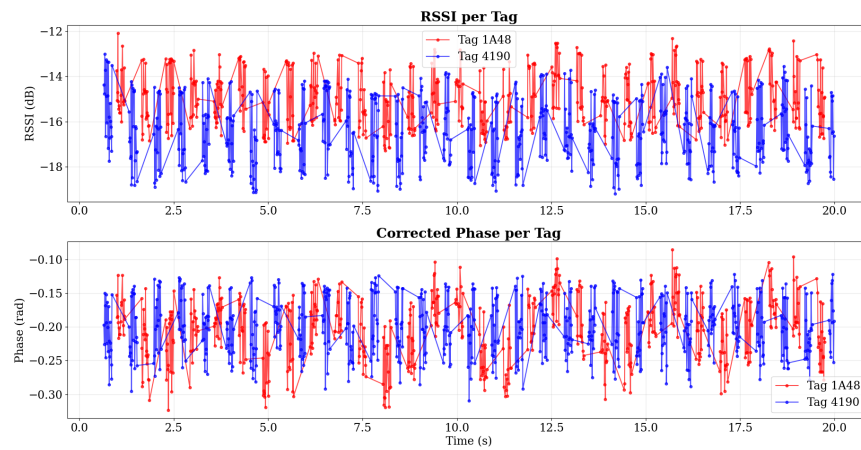


(c) Phase and RSSI reported by the reader.

Figure 4.11: Signal of two tags, one of which is moving in a sinusoidal pattern with period 3s and a displacement of 2cm. The still tag (blue) was placed in a vertical orientation and the moving tag (red) was placed in a horizontal orientation.



(a) The full captured signal.



(b) The phase and RSSI measured by the system.



(c) Phase and RSSI reported by the reader.

Figure 4.12: Signal of two tags read sequentially, one of which is moving in a sinusoidal pattern with period 3 s and a displacement of 2 cm. The still tag (blue) was placed in a vertical orientation and the moving tag (red) was placed in a horizontal orientation.

5

Discussion

This chapter will present some interpretations of the results seen in the previous chapter, as well as discuss some of the projects shortcomings and potential future work.

5.1 Interference between tags

Studies confirm the fact that tags placed close together interfere with each other, so it comes as no surprise that this behavior is observed in this project as well. What is of note, however, is the nature of that interference. When tags are placed around 8 or fewer cm from one another (depending on their size), a notable pattern occurs when some nearby tag is moving. Under these conditions, the measurements of the stationary tag exhibit periodic variations resembling motion despite remaining fixed in place. The behavior appears to be inverted relative to the moving tag with an approximately 180° offset in phase, as seen most notably in Figure 4.10. The RSSI also exhibits this inverted behavior. The RSSI of the moving tag reasonably becomes weaker when it is moved further away, but the RSSI of the fixed tag becomes stronger the further away it is from the moving tag.

This behavior could pose a real obstacle in respiratory monitoring or other applications where it is desirable to have multiple moving tags near one another. It is not easily discernible from phase and RSSI alone which tag is moving and which is still. The most notable difference between them is the amplitude of the sinusoidal and the phase offset. Under these conditions, the measurements alone may become insufficient to distinguish between true physical motion and interference-induced behavior. This interference warrants further investigation, both in how to mitigate it and how to detect it since it is likely that small differences in amplitude could be of great importance in applications like respiratory monitoring. It is possible that application specific insights could help remedy some of this observed behavior. For example, it could be argued unlikely that two tags placed on opposites side of a chest would exhibit inverse behavior, but setting rules for what constitutes reasonable tag behavior becomes more difficult to make in the less constrained environment of general motion sensing. The observed behavior suggests that measurements taken in dense RFID environments cannot necessarily be interpreted tag per tag, since the behavior may be directly influenced by, or influence, the apparent measurements of nearby tags.

Further experiments involving multiple moving tags are warranted since the current setup only allows for a single moving tag at a time. It cannot be excluded that the observed behavior is dependent on the geometry of the setup or the environment. More in depth testing in a more versatile setup is required.

It seems as if the differentiated complex-valued signal shows a larger difference in the amplitude of the sinusoidal between the moving and fixed tag as compared to the RSSI or phase alone. It also appears to be a more stable metric in general, as even small changes in position yield strong outputs. The resulting signal from a 1 cm movement can be seen in Figure 4.7a. The observed response suggests that smaller movements may also be detectable, although this was not investigated. This may suggest that lower-level signal representations retain information that becomes obscured when reduced to reader-reported phase and RSSI measurements alone or that the methods used to extract the measurements from the captured signal are not suited to capture this nuance.

Data points become more sparse and have higher variance when the tags are closer together. This behavior is seen in Figure 4.9b, where the tags are closest together when the moving tag is the furthest away from the antenna. This presents an issue since readings become less reliable where interference becomes stronger, which obviously obfuscates interesting patterns that could otherwise be observable. Any assertions regarding the nature of the interference are hindered by the fact that measurements are less reliable during it, which is itself what constitutes interference.

Rather than just trying to reduce and filter interference, one could attempt to model how the tags interact with each other. This would enable the system to take into account the data from all other tags in order to infer movement. There exists multiple possible solutions to this problem. One is a data-driven approach where a model is trained to identify tag movement using readings from all tags. Another possible method is a physics driven approach where the interactions are modeled explicitly, characterizing how distance and orientation affects interactions between tags. Neither approach has been explored in this work.

5.2 The state of the hardware and how it limits experiments

The current hardware setup, although stable enough for basic development of software, has proven to be too sensitive to environmental factors to be a reliable system during a wider range of experiments. Due to the antenna used, which is both small and directional, the antenna and the tag need to be in close proximity to each other, and placed in a way such that their surfaces are parallel. This limits the types of experiments that can be performed. When analyzing the behavior of multiple tags, the tags must be placed in such a way that they are close enough to parallel with the antenna such that they can still be read. Another caveat is that the moving tag needs to be prioritized when placing the two tags since it otherwise risks moving out of range. This introduces more uncertainty in the measurements. An example of this

can be seen in Figure 4.9b, where the still tag has significantly noisier measurements of phase than the moving tag. Patterns can of course still be discernible, but one can not be as certain of the accuracy of these observations. The problem of losing data points due to failures in decoding are somewhat remedied in experiments where tags are read one at a time, thus allowing the firmware filter to be used. This does not, however, decrease variance in the measured values, since this would require the tags to be placed closer together once again.

Several of the aforementioned issues with decoding tags could be solved completely if the reader could be configured in such a way as to report every single EPC backscatter it detects, as well as its metrics. Alas, the lack of this functionality has made these trade-offs a necessity in this specific hardware configuration. This is not necessarily strictly negative, since this means the system can be adapted for use with multiple types of readers.

Currently, it seems the most meaningful change to the system would be to use a different antenna with a larger surface area and high directionality as to filter out as much of the signal from the reader as possible and allowing greater distances between the antenna and the tags, and as a result allowing more space between the tags themselves to enable simulating the configuration appropriate for the purpose of respiratory monitoring. If one desires to evaluate the potential of sensing distance and not just the presence and frequency of movement, it would be necessary to construct a more sophisticated rig for moving the tags. Using either encoders or motors with inherent knowledge of their movement would make this rather trivial and allow the user to set specific parameters in how movements should be performed. This would allow for repeatable movements of any arbitrary shape as long as it is linear in its path.

5.3 Software and future development

Currently, the software consists of both a program to control the reader, a script to capture data with the SDR, and a script to process, combine, and visualize the data. The software does not have any external synchronization, meaning it needs to be started manually in the *correct* order. The processing script expects the first bit of signal to be a good representation of background noise, so the reader cannot transmit at that time. Having all signal capturing related software be controlled by a common interface would improve usability. The main limitation is that the signal processing can only be done offline, after the data has been captured. There is no real-time functionality, so it is not possible to continuously monitor the signal during experiments. Real-time monitoring would be a necessity for many motion sensing applications, and the signal processing chain would have to be adapted to work on a real time system.

6

Conclusion

Previous research into UHF RFID as a sensing modality has raised multipath interference as an issue worthy of investigation. The nature of the interference has not been able to be analyzed due to the closed nature of commercial UHF RFID readers. This thesis presented the development of an SDR-based system for capturing and analyzing raw UHF RFID communication signals. This allows the user to obtain more detailed metrics than with proprietary UHF RFID systems, which enables the investigation of backscatter behavior and interference.

The system can detect tag replies and decode them, which allows it to differentiate between multiple tags. A derivative-based metric was found to reliably detect backscatter in the conducted experiments. Experiments demonstrated that patterns coherent with motion could be observed in both metrics reported by the reader, and in measurements made on the raw signal.

The experiments revealed significant interference between nearby tags. When multiple tags are close together, stationary tags could exhibit motion-like signal characteristics induced by nearby moving tags, making interpretation of phase and RSSI measurements ambiguous under these conditions.

These observations suggest that measurements used for motion sensing cannot always be interpreted on a per-tag basis, since nearby tags and the environment may significantly alter the apparent behavior of a tag. Although domain-specific insights and constraints may help mitigate some of these effects, this interference could pose an obstacle in scenarios involving nearby independently moving tags, such as in respiratory monitoring. The observed ambiguity in phase, RSSI, and derivative based measurements highlight difficulties in interpreting the behavior of tags using these metrics alone.

It is apparent that RFID systems made for motion sensing may require a fundamentally different signal processing chain than inventory-oriented systems.

Bibliography

- [1] P. V. Nikitin, K. Rao, and S. L. Intermec, “Uhf rfid tag characterization : Overview and state-ofthe-art,” 2012. [Online]. Available: <https://api.semanticscholar.org/CorpusID:912360>
- [2] N. Beuster, A. Ihlow, K. G. Blau, J. F. Trabert, C. Andrich, J. Bauer, and G. D. Galdo, “Uhf rfid tag response measurements using a do-it-yourself platform and components off-the-shelf,” *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 1, pp. 65–72, 2020.
- [3] X. Zeng, J. Wu, A. Thelandersson *et al.*, “Localized measurement of breathing movement using RFID: Proof-of-concept and challenges,” *IEEE Access*, vol. 14, pp. 12 655–12 663, 2026. [Online]. Available: <http://dx.doi.org/10.1109/ACCESS.2026.3654654>
- [4] S. Yang, R. Penty, and M. Crisp, “Wirelessly retrieving phase and rssi of uhf rfid using commodity sdr sniffer,” in *2021 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, 2021, pp. 297–300.
- [5] Z. Ma and J. Wu, “Breathing monitoring with rfid sensing: Tag antenna design and signal processing,” Master’s thesis, Chalmers University of Technology, 2025. [Online]. Available: <https://odr.chalmers.se/items/114453c0-e5eb-44e7-bd02-53fde45e4d9d>
- [6] S. Gotfryd, “RFID tag shadowing - what is it and how do I avoid it?” RFID Insider, Atlas RFID Store, June 2021, [Online; accessed 24-May-2026]. [Online]. Available: <https://www.atlasrfidstore.com/rfid-insider/rfid-tag-shadowing-what-is-it-and-how-do-i-avoid-it/>
- [7] GS1 AISBL, “EPC radio-frequency identity generation-2 UHF RFID standard: Specification for RFID air interface protocol for communications at 860 MHz – 930 MHz,” GS1, Standard, February 2026, ratified Standard. [Online]. Available: <https://ref.gs1.org/standards/gen2/>
- [8] N. Barbot, R. de Amorim, Jr., and P. Nikitin, “Simple low cost open source UHF RFID reader,” *IEEE Journal of Radio Frequency Identification*, vol. 7, pp. 20–26, 2023.
- [9] A. Laurie, “Building a GEN2 UHF RFID reader with SDR,” Presentation at HITBCyberWeek, CommSec Track, January 2020, held on 3-Jan-2020. [Online]. Available: <https://www.youtube.com/watch?v=QKi1OH8Zstk>
- [10] Impinj, Inc., *Application Note - Low Level User Data Support*, Impinj, Inc., [Online; accessed 24-May-2026]. [Online]. Available: <https://support.impinj.com/hc/en-us/articles/202755318-Application-Note-Low-Level-User-Data-Support>

A

Appendix

A.1 Boundary detection

Listing A.1: Burst boundary detection

```
1
2 def find_burst_boundaries(derivative, peak_idx, sample_rate,
3 bit_rate=640e3, search_radius=0.1e-3, max_search=1e-3,
4     threshold_fraction=0.5, max_missing_bits=3):
5     """
6     Find start and end of a backscatter burst by walking away
7     from a peak.
8
9     Args:
10         derivative:      2nd derivative of IQ (abs)
11         peak_idx:        index of detected preamble peak
12         sample_rate:     samples per second
13         bit_rate:        FM0 bit rate (default 640kbps)
14         search_radius:   window around peak to find local max
15         max_search:      max distance to walk in each
16                         direction
17         threshold_fraction: threshold for what is active
18         max_missing_bits: how many consecutive bit periods
19                         below threshold
20                         before burst ended
21
22     Returns:
23         (start_idx, end_idx) or None if detection fails
24     """
25     samples_per_bit = int(sample_rate / bit_rate)
26     radius = int(search_radius * sample_rate)
27     max_samples = int(max_search * sample_rate)
28
29     # Find local maximum around the peak to get reference
30     amplitude
31     local_start = max(0, peak_idx - radius)
32     local_end = min(len(derivative), peak_idx + radius)
33     local_max = np.max(derivative[local_start:local_end])
34     threshold = threshold_fraction * local_max
```

```
31     def walk(start, step):
32         """Walk in one direction, return last valid index"""
33         last_valid = start
34         missing = 0
35         pos = start
36
37         while abs(pos - start) < max_samples:
38             window_start = max(0, pos)
39             window_end = min(len(derivative), pos +
40                             samples_per_bit)
41
42             if window_start >= window_end:
43                 break
44
45             window_max = np.max(derivative[window_start:
46                                     window_end])
47
48             if window_max >= threshold:
49                 last_valid = pos
50                 missing = 0
51             else:
52                 missing += 1
53                 if missing >= max_missing_bits:
54                     break
55
56             pos += step * samples_per_bit
57
58         return last_valid
59
60     start_idx = walk(peak_idx, step=-1)
61     end_idx = walk(peak_idx, step=+1)
62
63     if end_idx <= start_idx:
64         return None
65
66     return start_idx, end_idx
```


DEPARTMENT OF SOME SUBJECT OR TECHNOLOGY
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
www.chalmers.se



CHALMERS
UNIVERSITY OF TECHNOLOGY