Design and Implementation of an Augmented RFID System

by

Alexey Borisenko

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the M.A.Sc. degree in
Electrical and Computer Engineering

School of Electrical Engineering and Computer Science
Faculty of Engineering
University of Ottawa

© Alexey Borisenko, Ottawa, Canada, 2012

Abstract

Ultra high frequency (UHF) radio frequency identification (RFID) systems suffer from issues that limit their widespread deployment and limit the number of applications where they can be used. These limitations are: lack of a well defined read zone, interference, and environment sensitivity. To overcome these limitations a novel receiver device is introduced into the system. The use of such device or devices mitigates the issues by enabling more "anchor points" in the system. Two such devices exist in industry and academia: the Astraion Sensatag and the Gen2 Listener. The drawbacks of the Sensatag is that it offers poor performance in capturing tag signals. The Gen2 Listener is based on the expensive software defined radio hardware.

The purpose of the thesis was to develop a receiver that will enable several new RFID applications that are not available with current RFID systems. The receiver, named ARR (Augmented RFID Receiver), receives tag and reader signals, which are decoded by an FPGA and the results are reported through Ethernet. This device is central to the augmented RFID system. To show the suitability of such an approach, the performance of the implementation was compared to the other two outlined solutions. A comparison of the read rate and range of the implementations were the defining factors. The analysis showed that the ARR is capable of receiving tag signals with a read rate of 50% for passive and 66% for semi-passive tags at a one meter distance and is capable of receiving tag signals at a maximum of 3.25 meters for passive and 5.5 meters for semi-passive tags, with the reader being within 8 meters of the ARR. Two applications were implemented to showcase the ARR: an RFID portal and protocol analyzer.

Acknowledgements

This thesis would not be complete without the help and support of many. I would like to extend my gratitude to Boris Smaryanakis, Victor Xiong, Ovidiu Draghici, and Tzu Hao Li for their comments and suggestions on improving the thesis, Majed Rostamian for his help in the experiments and his comments. I would also like to thank Akshay Athalye from Astraion LLC for providing the Sensatag boards and NSERC for funding the research. I would especially like to thank my supervisor, Dr. Miodrag Bolic, for his wisdom and guidance throughout the years. Last, but not least, my family for always believing in me and always encouraging me on every step of the way.

Alexey Borisenko

Contents

List of Tables

List of Figures

List of Abbreviations

A/D	Analog-to-Digital
ARR	Augmented RFID Receiver
ASK	Amplitude Shift Keying
BB	Baseband
BLF	Backscatter Link Frequency
CW	Continuous Wave
DSB	Double Sideband
EPC	Electronic Product Code
FSK	Frequency Shift Keying
HF	High Frequency
I/Q	In-phase/Quadrature
IC	Integrated Circuit
IF	Intermediate Frequency
LF	Low Frequency
LNA	Low-Noise Amplifier
LO	Local Oscillator
MDS	Minimum Detectable Signal

MeEts	Measurement and Evaluation Test System
NF	Noise Floor
NRZ	Non-return to Zero
OCR	Optical Character Recognition
PA	Power Amplifier
PIE	Pulse Interval Encoding
PR	Phase Reversal
PSK	Phase Shift Keying
PW	Pulse Width
RFID	Radio Frequency Identification
RTcal	Reader-tag calibration
SNR	Signal-to-Noise Ratio
SSB	Single Sideband
TARI	Type A Reference Value
TRcal	Tag-reader calibration
UHF	Ultra High Frequency
UPC	Universal Product Code
USRP	Universal Radio Peripheral
VGA	Variable Gain Amplifier

Chapter 1

Introduction

1.1 Overview of the field

1.1.1 RFID

RFID is a wireless automatic identification technology that uses radio waves to automatically scan and identify individual or bulk items [1]. A complete RFID system typically consists of a reader, one or more tags, and software for controlling the reader and processing the information, as shown in Fig. 1.1. A host PC controls a reader and processes information from it. The reader energizes and provides a clock to the tag in case of a passive tag, or only the clock in case of a semi-passive tag, i.e. a tag with a battery onboard. Data is sent between the reader and tag, and then the reader forwards the data to a host PC.

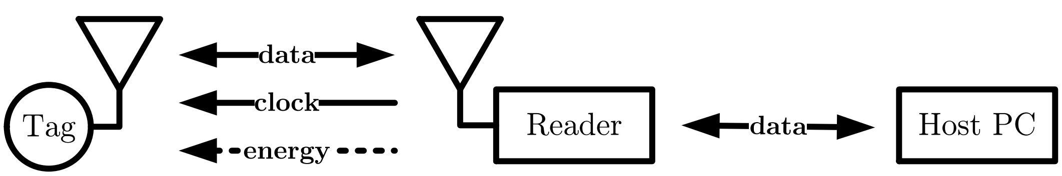


Figure 1.1: High-level RFID system

There are three main types of RFID based on the frequency of operation: low frequency (LF), high frequency (HF), and ultra high frequency (UHF). UHF RFID offers longer read range and lower cost tags compared to LF and HF RFID. UHF RFID tags contain electronic product codes (EPC), used to identify an item. The tags are able to store more bits of information compared to universal product codes (UPC) used in barcodes. Apart from the EPC number, many tags contain additional memory. The memory can store information such as expiration date, manufacturing date, manufacturing location, etc.

RFID tags are composed of small integrated circuits (IC) that store information and perform modulation/demodulation of the reader signal. An additional component of the tag is an antenna attached to the IC. The amount of data processed in an RFID system can be quite large, and so a server architecture is needed to filter and process the large quantities of information as well as perform predefined computations.

RFID is used in various industries including supply-chain management, animal tracking, inventory management and the number of applications is steadily growing [2]. RFID systems suffer from issues that limit their widespread adoption and minimize the number of applications where they can be used. These limitations include: environment sensitivity, interference, and lack of a well defined read zone.

1.2 Problem statement

The objective of this thesis is to design and develop a receiver that overcomes limitations of current RFID systems and enables applications that were not possible with the current state of the art. Existing solutions either do not provide good performance in capturing tag signals or are too expensive to be widely deployed. Central to this system is a UHF RFID receiver. With this receiver and the regular reader-tag RFID system, an augmented system is formed, which can overcome the limitations outlined. With the implementation of such receiver, new applications open up for UHF RFID.

1.3 Existing solutions

The solutions closest to the one presented in this thesis are the Astraion Sensatag [3] and the Gen2 Listener [4]. These designs have different architectures and implementations. The Sensatag uses an envelope detection architecture, suffering from poor sensitivity and selectivity, but has the advantage of simple implementation and low cost. The Gen2 Listener is a software-defined radio, based on the GNU Radio toolkit and running on the expensive USRP hardware. It offers good performance, but the high cost of the hardware prohibits it being widely deployed.

1.4 Motivation and Contributions

The motivation behind the thesis is to enable applications that are not possible or are inefficient with the current state of RFID systems. These applications are: portal receiver, protocol analyzer, sniffer, Internet of Things mote, and proximity-based localization system. Two of these applications, namely protocol analyzer and portal receiver, have been implemented in this thesis.

Existing solutions provide either poor performance, or are too expensive to be implemented in the mentioned applications, such as in proximity-based localization. The design described in the thesis is a low-cost alternative to the Gen2 Listener and offers better performance than the Sensatag. Fig. 1.2 shows the high-level view of the augmented system, with the new receiver component. The ARR receives the reader and tag data signals and also the clock from the reader for synchronization. The results are reported to the host PC through Ethernet. Fig. 1.3 shows the high-level design of the receiver. The RF section consists of an industry UHF RFID reader IC. The signal from the antenna is fed to its RF input port and LO port, for use as a clock. The IC performs the downconversion, filtering, and digitizing of the signal. An FPGA performs the decoding of the bits and commands. This information is then passed to a soft-core CPU, which has a TCP/IP stack. The CPU prepares an Ethernet packet and sends it to the host PC.

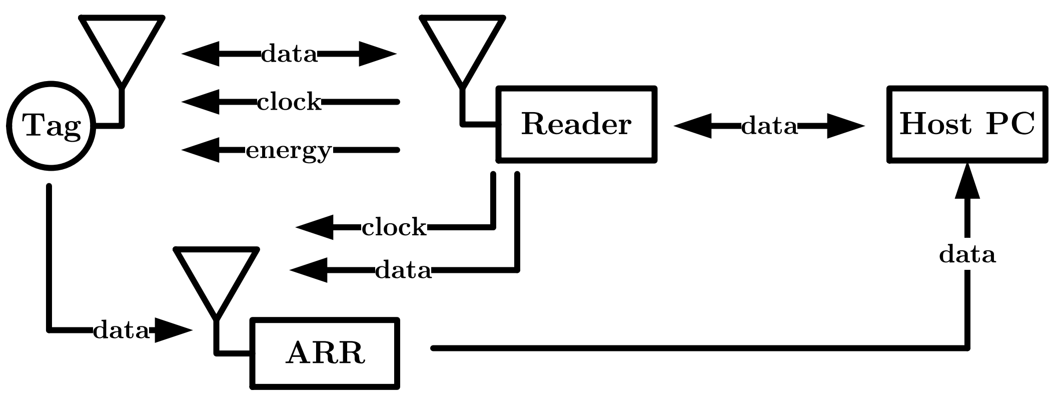


Figure 1.2: High-level augmented system

The contributions of the thesis can be summarized as:

- Survey of devices that augment RFID.
- Design and development of an augmented system.

- Novel way of synchronizing with UHF RFID readers using synchronous detection.
- Implementation of a UHF RFID receiver that needs to detect signals from both the reader and the tags, based on an industry UHF RFID reader IC.
- Measurement of the performance of the system with passive and semi-passive tags.
- Demonstration of the augmented system as a protocol analyzer and RFID portal.

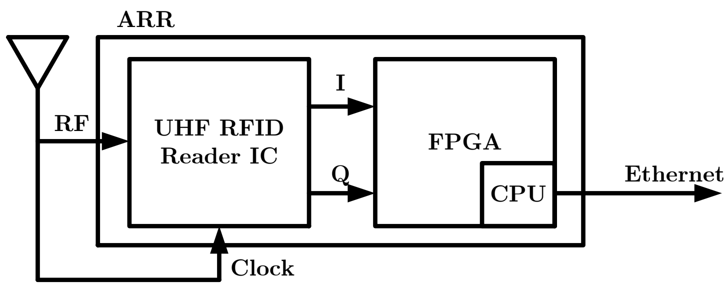


Figure 1.3: High-level design of the ARR

1.5 Analysis

To show the suitability of such an approach, the performance of the implementation was compared to the other two outlined solutions: the Sensatag and Gen2 Listener. A comparison of the read rate and range of the implementations was made. Besides measuring the performance, the system was implemented in two applications, namely: a protocol analyzer and RFID portal.

1.6 Thesis outline

The thesis is organized as follows. Section 2 presents a background on wireless systems and in particular on UHF RFID, with emphasis on the EPC Gen 2 standard. State of the art is presented in Section 3. Section 4 describes the problems current UHF RFID systems face. The solution to these problems and the system-level design of it is presented in Section 5. Section 6 gives the concrete details of the implementation. Experiment test results are presented in Section 7. Section 8 gives an overview of implemented and potential applications where the solution can be used. The thesis concludes with Chapter 9.

Chapter 2

Background

2.1 Radio Systems

2.1.1 Overview

Radios allow communication between devices over some medium. Fig. 2.1 shows a high-level view of a radio system. From the transmitter, a low frequency data stream is first modulated with a high frequency signal provided by the local oscillator. This signal is then amplified and sent through an antenna over a radio link. Finally, the receiver amplifies the received signal and then downconverts it to the original low-frequency signal, with its own local oscillator.

All radio systems have some common traits and properties and can be built from a set of blocks. This section will start with the description of these blocks. When discussing any radio system, parameters, such as sensitivity, selectivity and others, are important in characterizing the system, which will be discussed next. Finally, some popular architectures will be presented. This section builds the necessary background for comparing the implementation details of the radios used in the existing solutions to the implementation in the thesis.

2.1.2 RF building blocks

Table 2.1 shows the high-level basic building blocks of RF systems. Through the combination of these blocks, a radio system can be built.

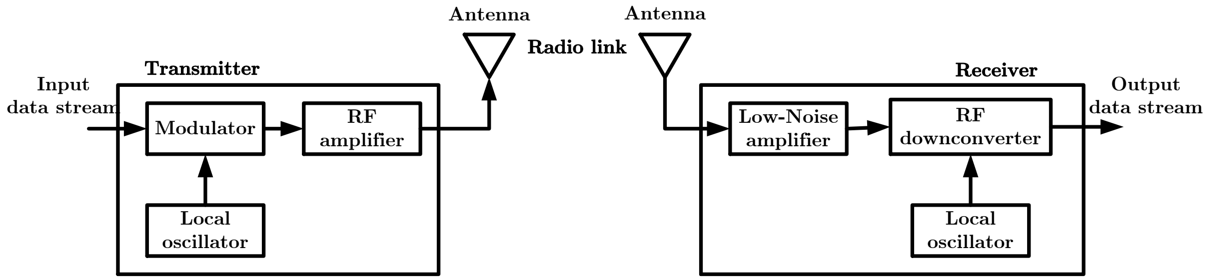


Figure 2.1: Radio system [5]

2.1.3 System Parameters

Wireless receivers have a set of parameters which define their performance. The four main parameters are: *sensitivity*, *selectivity*, *dynamic range*, and *power consumption* [6]. Other system parameters stem from these main ones.

Sensitivity

Sensitivity describes the weakest signal that a radio can successfully decode. It depends on the *Noise Figure* (NF) of the receiver chain, signal-to-noise ratio (SNR) of the encoding used, and bandwidth of the signal [7]. All devices in the receiver chain add noise to the signal. The combination of the added noise by a receiver is called the Noise Figure of the receiver chain.

Noise power at the entrance to the antenna is called the *Noise Floor* and depends on the bandwidth of the signal, Equation 2.1.

$$Noise\ floor = kTB \tag{2.1}$$

where k is Boltzmann's constant, T is the temperature in Kelvin, and B the bandwidth of the signal. Assuming room temperature, 290K, the equation is simplified to $Noise\ floor = -174dBm/Hz + 10log_{10}(B)$.

Thus, from these parameters, the minimum sensitivity can be derived as shown in Equation 2.2. Another term for the minimum sensitivity is the Minimum Detectable Signal (MDS).

$$Sensitivity_{min} = -174dBm/Hz + 10log_{10}(B) + SNR + NF \tag{2.2}$$

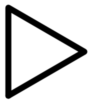
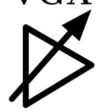
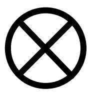
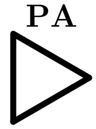
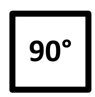
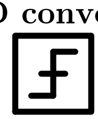
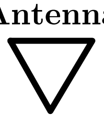
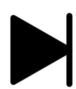
Block	Description	Block	Description
LNA 	(Low-Noise Amplifier) Amplifies weak signals with low distortion	**VGA** 	(Variable Gain Amplifier) Amplifies with programmable gain
Mixer 	A frequency translation device. Multiplies two signals, producing the sum and difference of their frequencies	**PA** 	(Power Amplifier) Amplifies a high-frequency signal with large gain
Filter 	Frequency selective network which attenuates a range of frequencies and passes others	**Phase shifter** 	Shifts the phase of the signal by 90 degrees
LO 	(Local Oscillator) Produces a fixed, high-frequency sine wave	**A/D converter** 	(Analog-to-Digital) Converts an analog signal to digital format
Antenna 	Interface between electromagnetic waves and electrical signals	**Detector** 	An envelope detector used for demodulation

Table 2.1: RF system blocks

Selectivity

Selectivity refers to the tendency of the receiver to respond to adjacent channels [6]. A good selectivity means that the receiver is capable of decoding signals in its channels even in the presence of large signals in adjacent channels. The parameter depends mostly on the types of filters in use and their co-channel rejection rates.

Dynamic range

Dynamic range specifies the range of signal strengths for which the signal can be demodulated and decoded properly. The lower end of the range is the MDS. For the upper range, the $1dB$ compression point is of importance.

The transfer functions of active devices are never perfectly linear. The point at which the observed output is 1dB less than the expected, e.g. an amplifier with a gain of 10dB outputs a signal with a gain of only 9dB, is called the $1dB$ compression point, abbreviated $1dB_{cp}$. Then, the dynamic range can be found:

$$Dynamic\,range = 1dB_{cp} - Sensitivity \tag{2.3}$$

Power consumption

Power consumption is a major factor for mobile receivers, having an impact on the lifetime of the device. The power consumption depends on the number and types of components used. Some systems rely only on passive components in the RF section and can have low power consumption. Using active devices such as mixers and oscillators bring the power consumption up.

2.1.4 Receiver Architectures

Using the blocks described in the section 2.1.2, many receiver architectures can be built, with various performance tradeoffs to be evaluated. The selection of an architecture has an effect on receiver sensitivity, cost of the front-end, size and other important parameters [8]. The most popular architectures are:

- Superheterodyne
- Homodyne
- Envelope detection
- Software-defined radio

What follows is a brief description of these architectures and the rationality of choosing a certain one over the others. A table with advantages and issues is presented at the end of this section.

Superheterodyne

The superheterodyne architecture is the most universally used receiver architecture. A superheterodyne receiver applies a two (or more) stage process for converting an RF signal into baseband. Fig. 2.2 shows the general receiver architecture for a superheterodyne radio [9].

The received signal is first passed through a bandpass RF filter, to reject out-of-band signals. A LNA amplifies the in-band signals. Next, the first frequency downconversion occurs. An intermediate frequency (IF) filter after the mixer selects the channel of interest. The second downconversion stage produces two signal paths: *in-phase (I)* and *quadrature (Q)*, one a 90° phase shifted version of the other. These signal paths are needed for some modulations, such as QAM (quadrature amplitude modulation) [10]. They also deal with phase variations between the received signal and local oscillator, for example, if the received signal is completely out of phase with the local oscillator, the I-channel will be destroyed, but the Q-channel will have an intelligible signal. The signals are then passed through baseband (BB) filters and converted to a digital signal.

A two-step filtering process allows good channel selectivity and sensitivity, because the noise bandwidth can be limited to the channel bandwidth without compromising the receiver's ability to tune across the entire RF band. The dynamic range is good because the combination of filters allows large signals to be present. A disadvantage of this architecture is the presence of an image frequency, located at $f_{RF} - f_{LO}$, if the desired signal is at $f_{RF} + f_{LO}$. If there is a signal at this image frequency, it can potentially distort the desired signal. Another issue is the high cost and large power consumption due to the number of components.

Homodyne

Homodyne receivers, also called zero-IF or direct conversion, have only a one step process in converting the RF signal to baseband. Fig. 2.3 shows the direct conversion receiver architecture [11].

The translation process is similar to superheterodyne receivers, except one stage is used for frequency translation, omitting the IF stage. This saves on components such as

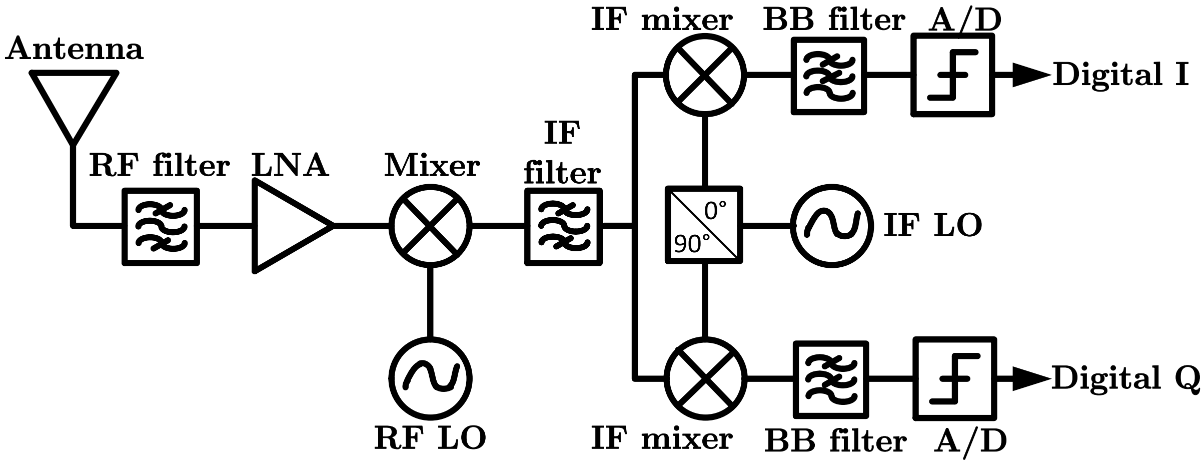


Figure 2.2: Superheterodyne receiver

mixers and LOs, compared to superheterodyne radios. However, the omission of the IF stage causes a new problem: DC offset. The LO is operating at a similar frequency as the RF signal, which causes self-mixing [12], introducing DC offset. Decreasing the number of stages causes more gain requirements in the baseband stage, making amplitude and phase matching of the I/Q paths difficult [13]. The architecture generally has lower power consumption, due to the decrease in the number of components, worse sensitivity and selectivity, due to the DC offset problem, and smaller dynamic range compared to a superheterodyne radio.

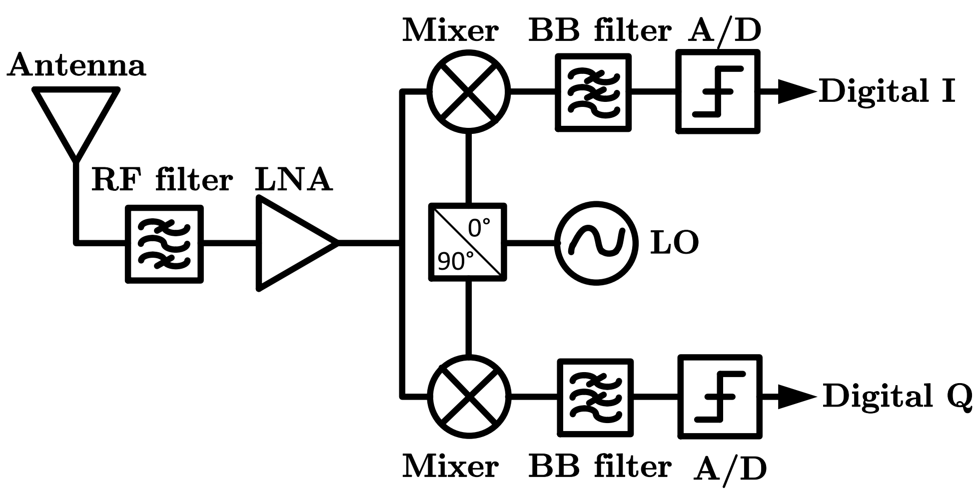


Figure 2.3: Direct conversion receiver

Envelope detection

Envelope detection or tuned radio frequency is the simplest receiver architecture. It consists of a diode, filters and a digitizer, which is a 1-bit A/D converter. Fig. 2.4 shows the architecture [14]. There are no frequency translation steps, rather the RF signal is demodulated at the detector stage. The selectivity of the architecture is not constant and suffers from poor sensitivity [15]. The use of mostly passive components means the cost and power consumption of the architecture is low.

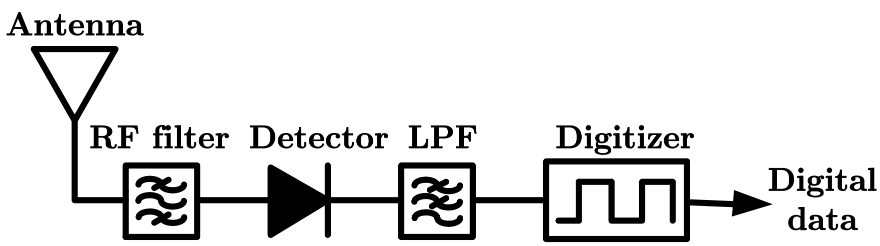


Figure 2.4: Envelope detector

Software Defined Radio

A software defined radio (SDR) is an architecture that tries to bring most components from the analog to the digital domain. This approach allows very flexible radios, since hardware is substituted with software. Fig. 2.5 shows the SDR architecture [16]. The disadvantages of the architecture is the requirement for high-speed and high-performance ADCs, making such radios expensive and having high power consumption. Another issue is the dynamic range of the radio. To be able to tune across a wide range of frequencies, SDRs do not employ narrow band-pass filters before the ADC, like other architectures do. This technique imposes a limitation on the dynamic range of the radio [17].

Comparison of Radio Architectures

Table 2.2 presents a comparison of the discussed radio architectures, with their advantages and issues.

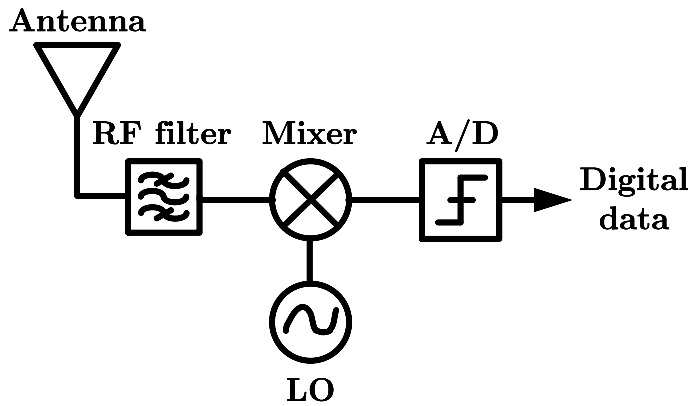


Figure 2.5: Software-defined radio

Architecture	**Advantages**	**Issues**
Superheterodyne	+Provides good electrical performance +Great selectivity and sensitivity	-Expensive -High power consumption
Homodyne	+Good selectivity and sensitivity +Low power consumption attributed to less hardware	-DC Offset -I/Q mismatch
Detector	+Cheapest option +Simplest to build	-Low sensitivity -Variable selectivity
Software defined radio	+Very flexible	-Requires high performance and high-speed ADCs -Expensive -Dynamic range

Table 2.2: Comparison of radio architectures

2.2 Radio Frequency Identification

2.2.1 Overview

RFID technology is a wireless technology that allows for automated data collection and a unique identification of objects. It is an improvement over barcodes and one of many types of automatic identification, including Optical Character Recognition (OCR), biometric (voice, fingerprint), and smart cards. Unlike barcodes, RFID does not require line of sight and supports larger memory. A simple RFID system is shown in Fig. 2.6. A reader, or interrogator, sends data, power, and the clock to tags. The tags respond to the commands of the reader. The RFID system can be classified based on the frequency of operation, how the tags are powered, and coupling. This section starts with describing the applications for RFID, then the main classification classes for RFID and finishes with a discussion on UHF RFID.

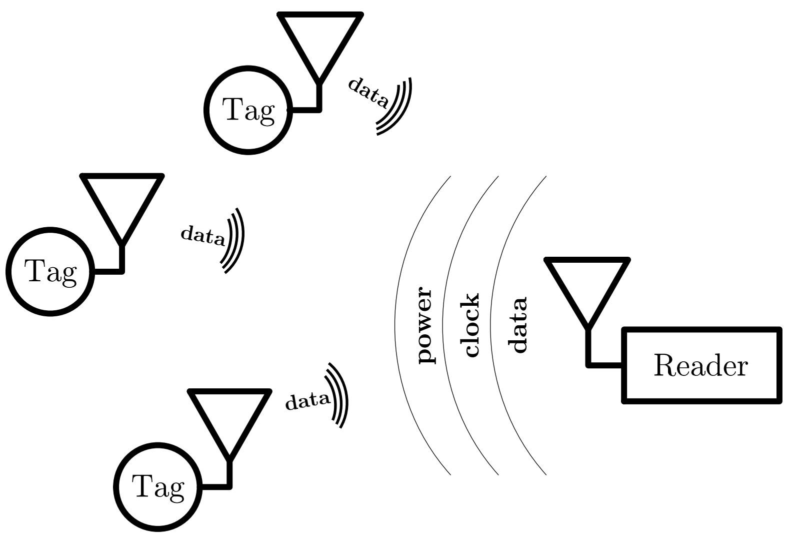


Figure 2.6: RFID system

2.2.2 Applications

RFID can be applied to a vast number of fields. Conceptually, RFID can answer questions such as [18]:

- Where is a certain item located?
- Where is the item going?

- Where has the item been?
- Has the item left a certain place?
- Has the item not been at a certain place?
- How many items are present at this location?
- How long has an item been at this location?

For concrete applications, RFID has been used for baggage tracking [19], evidence collection [20], animal tracking [21], people tracking [22], vehicle tracking [23], and supply management [24]. These are only a small subset of the applications where RFID is used.

2.2.3 RFID classifications

Frequency

The first type of classification relevant to RFID is the frequency range of operation. Fig. 2.7 shows the frequency spectrum with the RFID types displayed, and their main application area. LF has a high penetration rate and can penetrate such material as thin sheets of metal, water, or glass. The disadvantage is that it has a limited range, which is about a meter, and has high cost tags. HF has increased datarate and decreased cost compared to LF. UHF presents longer range and the lowest cost tags, compared to the other frequencies.

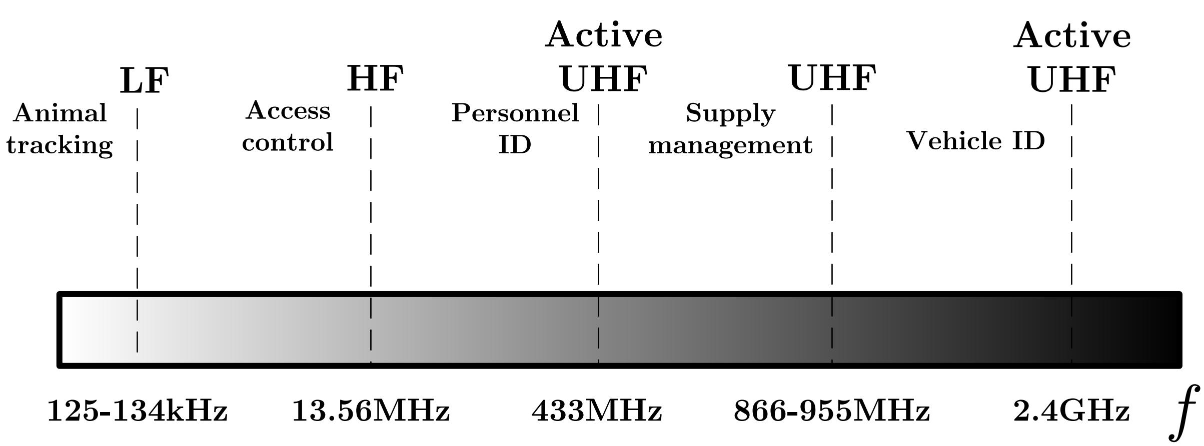


Figure 2.7: Types of RFID [2]

Power

Another type of classification is how the tags in an RFID system are powered. Tags are classified as being either *passive*, *semi-passive*, or *active*. Passive tags receive all of their power from the reader transmission, which results in an unlimited life span. Semi-passive tags have an onboard battery to power the integrated circuit (IC), but use the reader power for the backscattering, their life-times can span two years [25]. Active tags use the onboard battery to power the IC and the communication with the reader. Their life-times vary considerably based on the implementation, but is usually the lowest of the three.

Coupling

In the context of RFID, coupling refers to the way that power is transferred from the reader to the tag. Two types of couplings can be distinguished: inductive (also called near-field) and radiative (far-field) [26].

Near-field operates on the principles of magnetic induction. A large current is passed through a coil on the reader side, while a tag has a smaller coil, where current is induced when within the range of the reader. The tags communicate by *load modulation*, controlling the amount of current induced in the coil, thus transmitting information back to the reader. Inductive coupling is in the range of less than a meter, and is used for LF and HF systems.

Propagating electromagnetic fields are used in the far-field, where the near-field effects are diminished. Tags communicate with the reader through *backscattering*. By controlling the impedance of the antenna, the energy transferred from the reader can be either absorbed, reflected back, or something in-between can be done. These states allow tags to communicate with the reader. Radiative coupling is used in ranges longer than one meter in the UHF range.

2.2.4 UHF RFID

LF and HF ranges have a number of air standards in use, which specify the physical and MAC layers of the network. The UHF range has only one standard currently in use, which is EPCglobal Class 1 Generation 2 [27], EPC Gen 2 for short. In this range, RFID is mostly used for asset-level tracking as well as supply-chain management. EPC Gen 2 was developed with the following goals in mind:

1. Large range
2. High data rate
3. Inexpensive tags
4. Simple tag architecture

2.3 EPCglobal standards

2.3.1 Overview

EPCglobal is an organization set up to promote and standardize EPC (Electronic Product Code), which is an RFID coding scheme, sought to be the successor of barcodes. EPCglobal standards encompass a large variety of fields in UHF RFID, including the *exchange* of information, the *capture* of information, and the *identity* of information. Fig. 2.8 shows the EPCglobal standards hierarchy.

2.3.2 EPCglobal Class 1 Generation 2 standard

Central to the standard is the electronic product code, Fig. 2.9, which is the universal identifier tags use in the EPC Gen 2 standard. The EPC consists of 96 bits, which identify the encoding standard, company information, product type, and unique item identifier. Apart from the EPC number, many tags contain additional memory. The memory can store information such as expiration date, manufacturing date, manufacturing location, etc.

Spectrum requirements

One of the main objectives addressed, when developing the EPC Gen 2 standard, was global compliance. Around the world different regulatory commissions have set their own regulations concerning UHF RFID operations. In North America, the FCC is the regulatory commission, in Europe, ETSI.

In North America a 26 MHz range is allowed for UHF RFID, from 902-928MHz, compared to only 2 MHz in Europe, from 866-868MHz. Finding a way to operate in both frequency ranges created a challenge. Current EPC Gen 2 readers have a number of modes of operation, to encompass the various requirements. The limitation on bandwidth

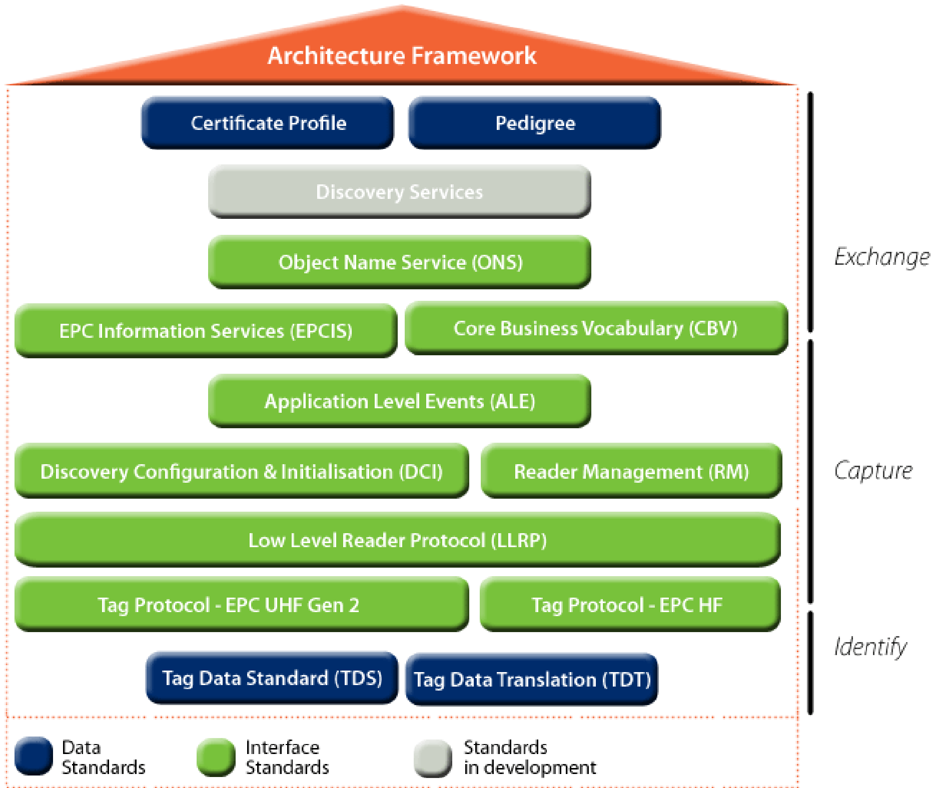


Figure 2.8: EPCglobal framework [28]

Figure 2.9: Electronic product code

has an effect on the speed of operation and read rate. All attention in this thesis will be focused on the North American range.

There are 50 channels allocated, each 500kHz wide in the 902-928MHz Industrial, Scientific, and Medical (ISM) band. Since the ISM band is unlicensed, it is shared with many devices. By FCC regulation, frequency hopping techniques must be used by an

RFID reader and a channel cannot be occupied for more than 0.4 seconds. Another issue is spurious radiation. The readers in an RFID system send a large power signal, with lots of phase noise. Strict spectral requirements are imposed, so that this spectral noise does not interfere with adjacent channels.

Fig. 2.10 shows the output power of an RFID reader and the maximum spectral emissions in neighboring channels for the "dense reader mode" specified in the standard. Readers need to have spurious radiation power in adjacent channels of 30dB less than the transmitting channel. In the ±2 channels, the suprious radiations should be 60dB less than the transmitting channel and -65dB for the ±3 channels.

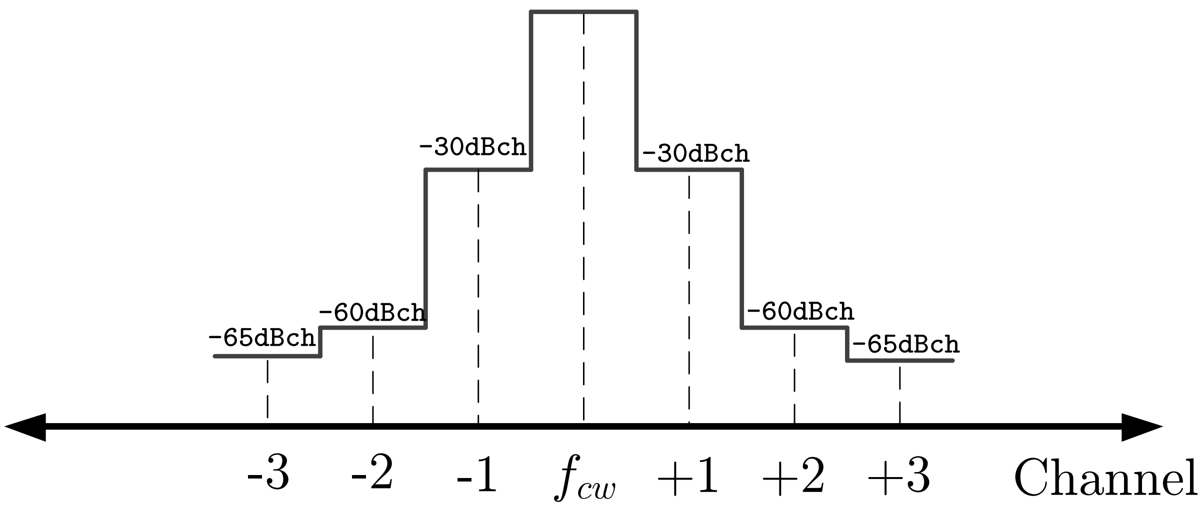


Figure 2.10: Spectral Requirements in Dense Reader Mode

Coding and Modulation

EPC Gen 2 standardizes a number of different modulation and coding schemes. These schemes include the reader-to-tag data link modulation, tag-to-reader data link modulation, reader encoding, and tag encoding.

Sending data in its original format is not always preferable. For example, using the Non-return to Zero (NRZ) encoding, it is difficult to synchronize and impossible to tell the difference between a long sequence of zeroes or the end of transmission [29]. Other times, it is desirable to have the clock encoded within the signal, for simpler synchronization between transmitter and receiver. The selected type of line code can have an effect on the spectrum bandwidth used, the data rate, DC value, and ability for clock recovery.

For the reader-to-tag encoding, the standard specifies Pulse-Interval Encoding (PIE). The main property of PIE is the ability to provide at least 50% of the maximum power even during a stream of zeroes, allowing tags to power themselves up [30]. The encoding used from tag to reader is either FM0 or Miller. Miller can vary the number of cycles within a given symbol, providing more spectral efficiency. Fig. 2.11 shows the line codes with a sample bitstream of "10100". Miller encodings are abbreviated Mx, where x is the number of cycles per symbol. Fig. 2.12 shows the spectral powers of the FM0 and Miller relative to the carrier.

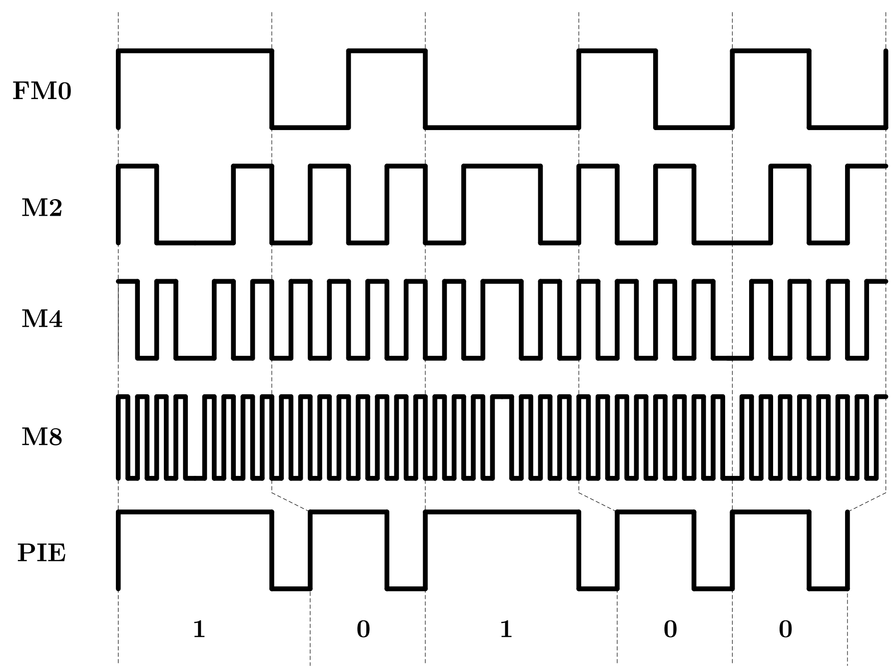


Figure 2.11: Line codes

The standard specifies three modulation methods: single-sideband amplitude shift keying (SSB-ASK), double-sideband amplitude shift keying (DSB-ASK), and phase-reversal amplitude shift keying (PR-ASK). DSB-ASK modulations are the simplest to implement, but are spectrally inefficient. SSB improves on DSB in this respect, by removing one of the sidebands, so the bandwidth and noise are reduced. PR-ASK maximizes spectral efficiency. In the context of RFID systems, DSB-ASK and SSB-ASK modulations would be implemented in systems with simple and low cost transmitters. PR-ASK is suitable for more complex transmitters, with narrowband and longer range requirements [31].

Table 2.3 shows the various modulations in time domain and their corresponding I/Q

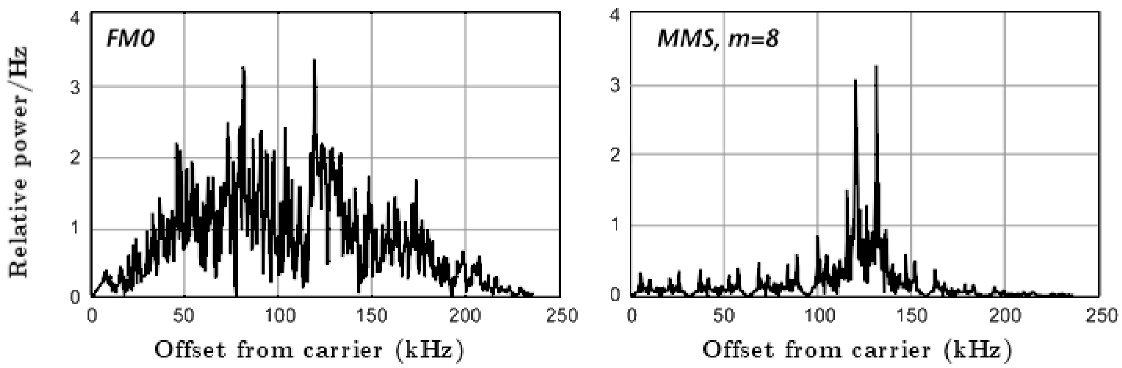


Figure 2.12: Encoding spectral power [30]

constellations. The examples shown are for binary modulations, but the same principles hold for higher order modulations. In ASK modulations, based on either a one or zero, the amplitude is varied both in time domain and on the I/Q constellation. For frequency shift keying (FSK) modulations, the frequency is varied based on the bit value; the phase is varied for phase shift keying (PSK). For both of these modulations, the phase changes 180° on the I/Q constellation. PR-ASK is a combination of the other modulations, with the phase and amplitude changing in the time domain and I/Q constellation.

Packet structure

Packets within the communication between the reader and the tag have special symbols embedded into them which control some of the parameters of the air interface. For example, Fig. 2.13 shows the preamble that is attached to reader packets. A *TARI* (Type A Reference Value) is the length of a data-0 in PIE encoding. The pulse width (PW) depicted on the figure is usually 0.5 of the length of the TARI, but depends on the mode chosen. *RTcal* is the Reader-tag calibration symbol, which defines the length of the data-1 and data-0 symbols of the reader. Upon reception, the tag divides the RTcal by two. Symbols from the reader that are less than half the length of the RTcal are considered data-0 symbols, and longer are data-1 symbols. TRcal (Tag-reader calibration) is a symbol which defines the BLF(Backscatter Link Frequency) , i.e. the speed the tag will respond. The preamble is attached to *Query* commands from the reader, other reader commands are started with a frame-sync. The frame-sync is similar to the reader-tag preamble, but lacks the TRcal symbol.

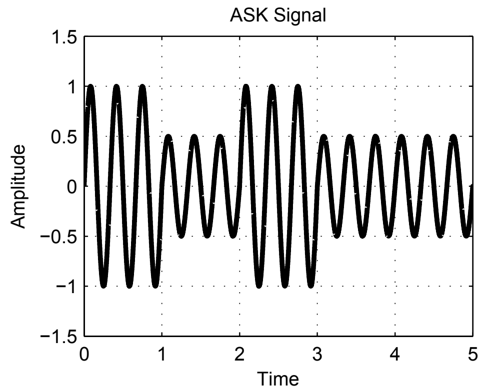
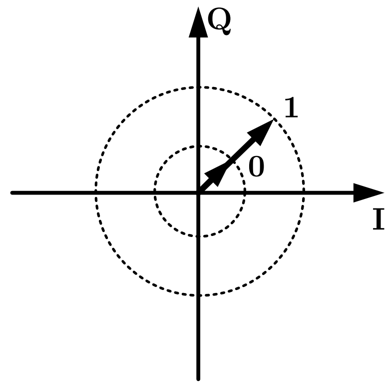
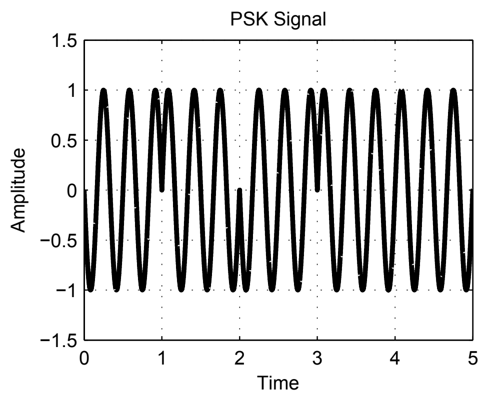
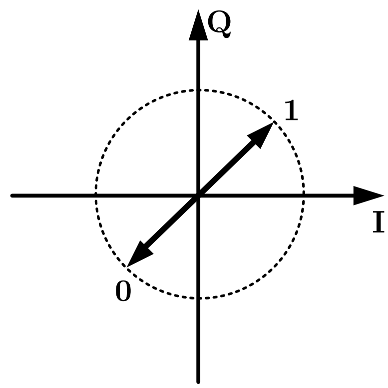
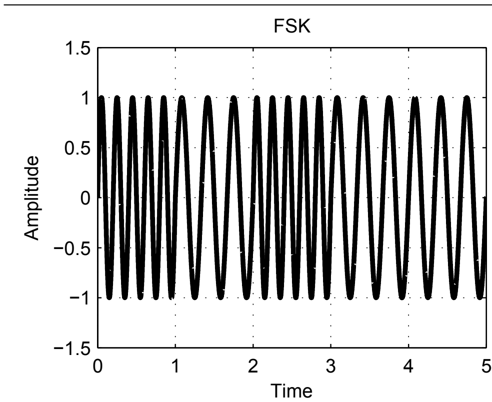
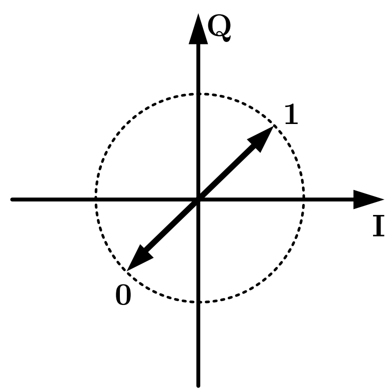
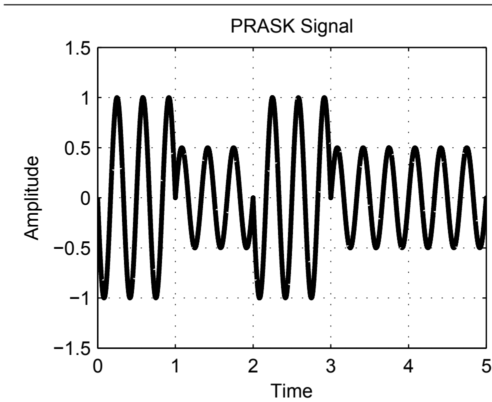
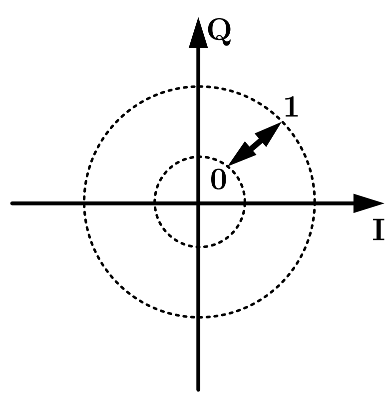
<table>
<tr><th>Time domain</th><th>I/Q constellation</th></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>
</td><td>
</td></tr>
<tr><td>
</td><td>
</td></tr>
</table>

Table 2.3: Various modulations and their I/Q constellations

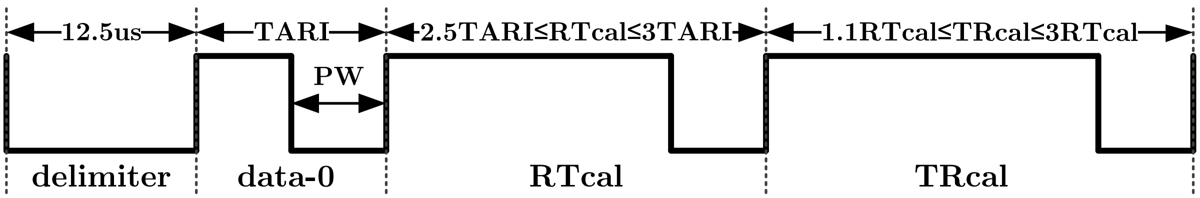


Figure 2.13: Reader-tag preamble

Medium Access Control

When multiple tags are present in the range of the reader, their responses may collide. A process called singulation was formulated as a solution to this problem. EPC Gen 2 adopts a type of Aloha algorithm, called the Q-value algorithm. Upon receiving the Q-value, tags load their slot counters with a random number from the range $\{0, 2^{Q-1}\}$. Commands from the reader can decrement the slot counter of tags. Once a tag's slot counter reaches zero, it responds.

The algorithm for Q-value specified by the standard is presented in Algorithm 1, note that C is some constant. Manufacturers can implement their own version of the Aloha algorithm, and there is extensive research in selecting optimal algorithms for tag singulation [32].

Input: Q_{start}
while *Tags in field* **do**
  Q = round(Q_{start})
  Send *Query* $\{Q\}$;
  if *# of Tag responses = 0* **then**
    Q_{start} = max(0, Q_{start} - C)
  end
  else if *Collision* **then**
    Q_{start} = min(15, Q_{start} + C)
  end
end

Algorithm 1: Q-value algorithm

Commands

The standard specifies a total of 15 commands, with the possibility of extension. The commands can be classified into three types, based on their functions: Inventory, Access, Select. Table 2.4 presents the main commands for the EPC Gen 2 standard.

Command type	**Command**	**Description**
Inventory	Query	Begin inventory round, setting modulation, encoding and other parameters
	QueryAdjust	Increment, decrement, or don't modify the slot counter used for the Aloha protocol
	QueryRep	Decrement the slot counter. If it is 0, then a RN16 is backscattered
	ACK	Acknowledge a single tag, instructing it to send its EPC
Access	Req_RN	Instruct the tag to go into Access state, for further Access commands
	Read	Read a portion of the memory
	Write	Write to a memory location
	Kill	Disable a tag
Select	Select	Select a tag population based on an EPC mask for inventory or access

Table 2.4: EPC Gen2 commands

Link timing

Fig. 2.14 shows the message exchange between the reader and a single tag during a successful read. First, the *Select* command is sent to singulate a population. A *Query* command is sent from the reader to start the inventory round. A tag responds with RN16 (Random number, 16 bits in length). The reader then sends an *ACK* command with the RN16 attached. The tag responds with its EPC. The times *T1, T2, T3,* and *T4* are specified in the protocol and have strict requirements. The values depend on the modulations and encodings used for inventory.

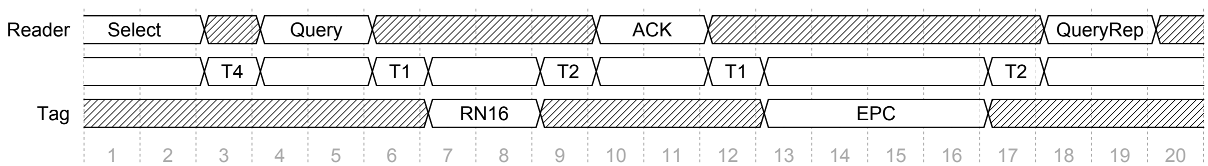


Figure 2.14: Link timing

Fig. 2.15 shows the message exchange between reader and multiple tags. When the *Query* is sent and multiple tags respond, the reader can detect a collision in the RN16. In such case the previously mentioned Q-value algorithm is deployed. A *QueryRep* is sent until a tag's slot counter reaches zero and it responds with an RN16. Next, the same *ACK* → *EPC* exchange follows.

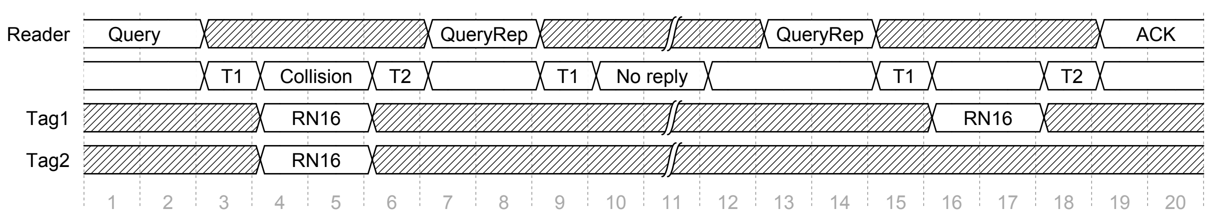


Figure 2.15: Link timing with collision

2.3.3 LLRP

The LLRP (Low-Level Reader Protocol) standard [33] is a specification for the interface between RFID readers and clients, usually in the form of PCs. Many RFID vendors adopted this standard for their reader-client interface [34]. LLRP supports the EPC

Gen 2 standard, as well as allowing the addition of other standards. The protocol allows setting the reader configuration as well as air-protocol configurations, such as: modulation, encoding, frequency range, Q-value, output power level, and sensitivity. These settings can be modified to boost performance or to mitigate interference of RFID systems.

In the LLRP, the data units are called messages and all communication between the reader and the client is performed using these messages. Client-to-Reader messages include getting and setting configuration of the reader, capability discovery, managing inventory, and access operations. Messages from Reader-to-Client include status reports, RF survey reports, inventory results, and access results. LLRP parameters are used to communicate specific settings of LLRP operation in the messages. A parameter contains one or more fields, and in some cases also may nest one or more other parameters.

2.4 Localization

Although outdoor localization techniques have been well studied, and are dominated by GPS technology, the same cannot be said regarding indoor localization. GPS signal are too weak to be used indoors. With this in mind, indoor positioning (IPS) approaches have to be considered.

Mainstream techniques used for indoor positioning include [35]:

- Assisted GPS (A-GPS)
- Inertial navigation
- Infrared positioning
- Radio-based positioning
- Ultrasonic positioning
- Vision-based positioning

Radio-based approaches will be focused on in the thesis. The principle techniques used in Radio-based localization are:

Radio map

Also called ”scene analysis”, signal strength and other parameters are compared to a set of previously measured values in the environment to determine the closest match.

Proximity
A number of receivers with limited range are scattered across a room, when a tag enters the range, the position can be estimated as the position of the receiver.

Triangulation
Based on the direction of arrival of the tag signal to multiple readers or receivers.

Trilateration
Trilateration involves using multiple reference points, i.e. readers or receivers, and using any of the above mentioned localization techniques.

Radio-based IPS approaches can use Bluetooth, RFID, WiFi and other wireless technologies, as well as physical sensors. Most of these technologies were not specifically designed for localization and several workarounds must be made in order for them to localize. They offer localization capabilities with varying accuracies.

Chapter 3

State of the Art

3.1 Overview

This chapter discusses systems that augment, i.e. extend functionally or improve, the ubiquitous reader-tag UHF RFID system. Some goals of these systems include: prototyping, localization, debugging, and research. Special focus is made on receiver systems which have similar functionality to the one outlined in this thesis.

3.2 Prototyping systems for UHF RFID

UHF RFID does not currently have a full-fledged prototyping or development platform. Attempts were made at creating a prototyping or development platform, but they were focused only on a certain aspect of the system, i.e. only the reader or tag side. The following section goes over the prototyping and development platforms in literature and the industry.

3.2.1 Customizable readers

Even with the low-level parameters available in LLRP, control over air-interface parameters is limited. To provide users with more control over the reader, development platforms were created. Angerer, et.al. in [36] describe the implementation of a dual-frequency testbed. Rapid prototyping is achieved by taking a layered approach to the design of the device: a physical layer, a link layer, etc. The device is designed to operate in the 13.56MHz and 868MHz ranges. At the heart of the device is a Virtex II FPGA which focuses on signal processing and a TMS320 DSP processor responsible for the protocol stack with an RF front-end functioning at the HF and UHF ranges. Code for the DSP processor and FPGA is generated by MATLAB and Xilinx System Generator. Modifiable parameters of the RFID air interface are available through registers.

Roy, et.al. in [37] describe the architecture of an FPGA based UHF RFID reader. The focus is more on the FPGA development. The architecture of the FPGA is described as well as potential interfaces that can be used.

GNU Radio, an SDR, was used in developing a customizable reader in [38]. In such an SDR system, all the DSP functionality was done through the host PC, while the acquisition, ADC and DAC through an external device, the Universal Radio Peripheral (USRP). This system suffered from the narrow bandwidth available to the USRP, as well as the timing delays introduced with having all the processing done on the host side.

3.2.2 Development platform tags

The Wireless Identification Sensing Platform (WISP) [39], designed by the Intel Research group [40] is one example of an open source UHF RFID tag development platform. The platform presents a passive tag, consisting of an MSP430 MCU with sensors attached to it. The platform has the disadvantage of being very low-range, in the range of 10 feet as well as not being fully Gen2 compliant, i.e. it does not have all of the required EPC commands implemented. The passive nature of the device limits its extensibility.

Another open source development platform for UHF RFID tags is the semi-passive development tag based on the PIC24F MCU [41]. The semi-passive nature allows the tag to have a better range than WISP. The tag was designed to have extension support for sensors and easily modifiable code for researchers to experiment with. A similar system, but implemented on an FPGA is presented in [42]. The focus is on rapid UHF RFID tag simulation. In [43] a semi-passive FPGA-based tag is developed for eavesdropping the reader signals and relaying the information through a proxy reader.

3.2.3 Protocol analyzers

Protocol analyzers are popular in networking fields, examples being WireShark (for Ethernet) [44], FTS4BT (for BlueTooth) [45], and AirMagnet (for WiFi) [46]. They can be used for debugging the air interface, analyzing performance, and adjusting parameters. In the field of UHF RFID, the National Instruments MeEts (Measurement and Evaluation Test System) system performs that function [47]. It supports all modes of operation in the UHF RFID range of the EPC Gen 2 standard, but has a heavy price tag, making it out of reach for most researchers. Besides debugging the RFID systems, the MeEts can be used for identifying correct tag types for a system, and determining the best position or orientation on a tagged object [48].

3.2.4 Augmented RFID

Augmented systems are systems where a new device is introduced to extend the functionality or improve the performance of the system. Donno, et.al. [17, 4] proposed a RFID receiver system, based on GNU Radio and implemented on a USRP. The receiver had a match filter and a channel selector implemented in digital radio. The applications proposed in the papers were that of localization, by implementing a set of "anchor points", i.e. multilateral RSS-based localization, and protocol analysis. Further research was conducted in [49], where the system was used to evaluate the performance of a UHF RFID system. The use of the USRP makes the device expensive, especially if multiple devices are used to implement the "anchor points".

A similar device is implemented in [3]. There, a special tag acts as a proximity-based localization device. The device can sniff the responses of the tags and embed the sniffed EPCs into the tag's own EPC. The tag is battery-powered and has a FPGA on board. Due to the power-hungry FPGA, the device suffers from low battery life.

A system with additional transmitters was proposed and implemented in [50]. A continuous wave transmitter was used to extend the forward link range of the UHF RFID system. The principle behind it was that the forward link (from reader to tag) is the weakest link in an RFID system [30], i.e. the tag does not have enough power to be on. The continuous wave transmitter would address this issue. This solution can effectively increase the range of passive tags.

An augmented RFID approach is presented in [51]. A combination of RSS-based lateration and image processing is used to identify the 2D coordinates of tags. The requirement of line of sight makes this approach undermine the advantage of RFID technology. A security device for UHF RFID is implemented in [52]. A blocking reader based on the TI CC1101 chip blocks tags from being read in a certain range.

3.2.5 Comparison

Table 3.1 presents a comparison amongst the devices which augment the UHF RFID system.

Paper(s)	Device Functionality	Device applications	Hardware and software
Agerer08 [36]	Dual-frequency prototyping	Prototyping	Virtex II and TSM320s
Roy06 [37]	UHF RFID reader	Prototyping	Virtex-4
Buettner09 [38]	UHF RFID reader	Prototyping	GNU Radio and USRP
Sample08 [39]	Passive tag platform	Prototyping	TI MSP430
Li12 [41]	Semi-passive tag platform	Prototyping	PIC24F
Feldhofer10 [43]	Semi-passive tag platform	Security	Xilinx FPGA
Chen11 [42]	Semi-passive tag platform	Tag simulation	Altera FPGA
Donno10, Donno11 [17, 4]	Receiver	Performance analysis, Localization	GNU Radio and USRP
Park10 [50]	Transmitter	Forward link extension	CC1110
Athalye11 [3]	Tag signal interceptorn	Localization	Custom UHF RFID tag on FPGA
MeETS [47]	Protocol analyzer	Monitor, performance evaluation	Custom
Kenarangui12 [51]	RFID reader with camera and image processing	Localization	RFID and image processing software
Narayanaswamy10 [52]	Blocking reader	Security	CC1101

Table 3.1: Survey of augmented devices

3.3 Receivers

Special focus is put on receivers which augment the RFID system. Solutions closest to the one presented in this thesis are the Astraion Sensatag [3] and the Gen2 Listener

[17, 4, 49]. The solutions have different implementations and applications.

The architectures used in the solutions differ. The Sensatag uses an envelope detection architecture, suffering from poor sensitivity and selectivity, but simple implementation and low cost. The Gen2 Listener is a software defined radio, based on the GNU Radio toolkit, running on the USRP. The hardware for it to run is costly, but is flexible and offers good performance. The solution in this thesis uses a direct conversion architecture.

The Astraion Sensatag is read from a standard EPC Gen 2 reader. The data it receives is encoded into its own EPC, through a technique called piggy-backing [53]. The Gen2 Listener runs directly on a PC, so any kind of IPC (Interprocess Communication) is possible. The implementation in this thesis sends the data through Ethernet.

3.3.1 Receiver comparison

Table 3.2 compares the receivers outlined before to the implementation in this thesis. Note that *Architecture* concerns the radio architecture used, Section 2.1.4. *Interface* refers to the way that data is extracted from the device. *Hardware* refers to the platform that is used. *Middleware* refers to the software component used in the receiver. The last column presents how the device is powered.

Device	**Architecture**	**Interface**	**Hardware**	**Middleware**	**Power**
Gen2 Listener	SDR	USB	USRP	GNU Radio	External connector
Sensatag	Envelope detection	UHF RFID	Custom RF front-end with FPGA	Custom LLRP application	Battery
This thesis	Direct conversion	Ethernet	UHF RFID reader IC with FPGA	Custom LLRP application	External connector

Table 3.2: Receiver comparison

Chapter 4

Performance of UHF RFID systems

4.1 Overview

This chapter presents the problem that the thesis is trying to address. First, the model of an ideal RFID system is described and gradually, section-by-section, problems encountered in the real world are introduced to the model. This chapter serves as a prelude to the next chapter, where the solution to these problems will be discussed in the form of an augmented RFID system. Apart from problems in the regular RFID system, improvements to the RFID system are described which can facilitate more applications.

4.2 Model of a UHF RFID system

The ideal model of a UHF RFID system is shown in Fig. 4.1. Some properties of the model, which are relevant to the thesis, are [54]:

Read zone
: The read zone of the reader is well defined, i.e. the tags exhibit 100% read rate in a certain distance from the reader and are not read outside of this distance.

Environment insensitive
: The reader is insensitive to the surrounding environment, i.e. obstructions.

Interference
: Multiple readers do not interfere with each other.

The chapter continues by introducing problems to this model and pointing out which of these properties will get affected by the problems.

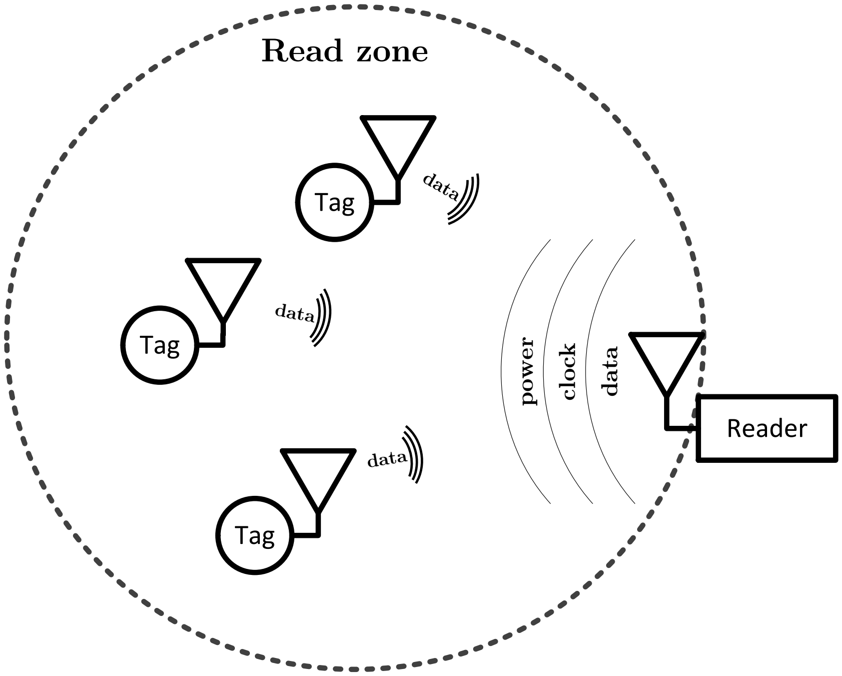


Figure 4.1: Ideal model of RFID system

4.2.1 Read zone

The first issue introduced into the model has to do with the link budget. The link budget defines the power levels of the signal throughout the communication system. The initial signal from the reader can be a maximum of one Watt, or 30dBm [55]. The signal then experiences a gain from the reader antenna, it usually ranges from 1.5dBi to 8dBi, depending on the antenna type. Propagating through free space, from the transmitter to the receiver, the signal experiences free space path loss (FSPL):

$$FSPL(dB) = 20log(d) + 20log(f) - 147.55 \tag{4.1}$$

where d is the distance and f is the frequency. The tag then receives this signal and extracts the power to turn the IC on. New generation tags, such as the Impinj Monza 5 and Alien Technology Higgs 4, require 0.016mW, -17.8dBm [56], and 0.014mW, -18.5dBm [57], respectively. Before powering the chip, the tag antenna, which is in the range of 2dBi, plays a role. Thus, the tag can send a response at around -20dBm. This path compromises the *forward link*.

The signal then traverses back the same distance, experiencing another path loss. The reader antenna catches the signal, and if it is above the MDS of the reader, the signal is decoded. The MDS for the current generation of readers is in the range of -80dBm [58]. This compromises the *reverse link*.

Fig. 4.2 shows the stages of the gains and losses of a signal that goes through a UHF RFID system, as described in the previous paragraphs. The example assumes a reader at a distance of one meter from the tag, line of sight, and a new generation tag with a dipole antenna.

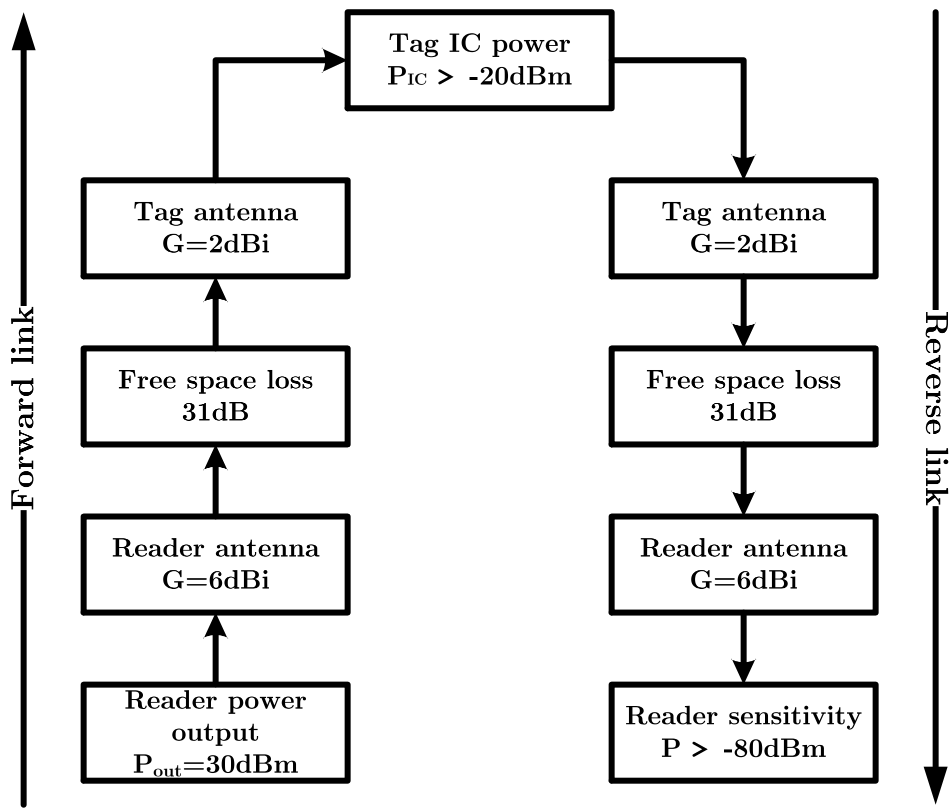


Figure 4.2: Link budget

Most RFID systems are limited by the forward link: as distance increases, the passive tags do not get enough power from the reader to power themselves up [30]. RFID systems with semi-passive tags, or systems with low reader sensitivity are, on the contrary, reverse link limited: the reader sensitivity is not low enough to decode the tag response at some distance.

As tags lower their requirements for IC power, they become reverse link limited. These tags have enough power to power themselves up, but the backscattered signal is not strong enough for the reader to pick up. Fig. 4.3 shows the cases where the forward and reverse links are limited. The passive tag threshold for powering up is at approximately 20 meters, whilst the maximum reader sensitivity allows 36 meters. The threshold for a semi-passive tag can be at -40dBm [59], allowing it to receive enough power to respond at 200 meters. Note that the graph assumes line of sight, no multipath effects, and reader is transmitting at 30dBm.

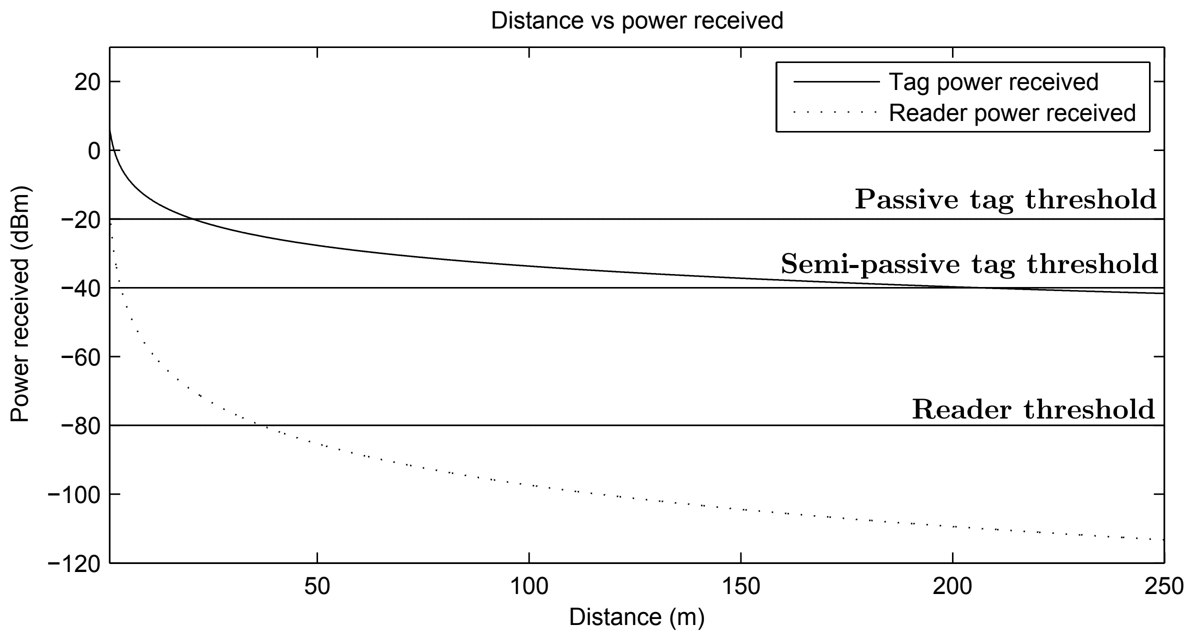


Figure 4.3: Received power

As technology improves, there is a trend towards reverse link limited tags [30], i.e. the reader is not sensitive enough to pick up the tag signal, rather than the tag not having enough power to turn itself on. Currently, semi-passive tags exhibit this problem. The issue stems from the fact that EPC Gen 2 standard was not designed with semi-passive applications in minds. By addressing this issue, more applications can open up for the standard.

4.2.2 Environment sensitivity

The previous section presented a simplistic view of the ranges of UHF RFID systems. In real wireless systems, the effect of fading ruins the model of the link budget. Due to multipath or obstacles, received signals destruct each other at arbitrary distances from the reader. The distance for fading can be quite close to the reader, it all depends on the reflective environment around the system.

Figure 4.4 shows the performance of a dipole tag in a lab environment. The y-axis shows the signal strength of the tag signal that the reader received and the x-axis shows the distance of the tag from the reader. The down-spikes are called *null points*, where the tag cannot be seen by the reader.

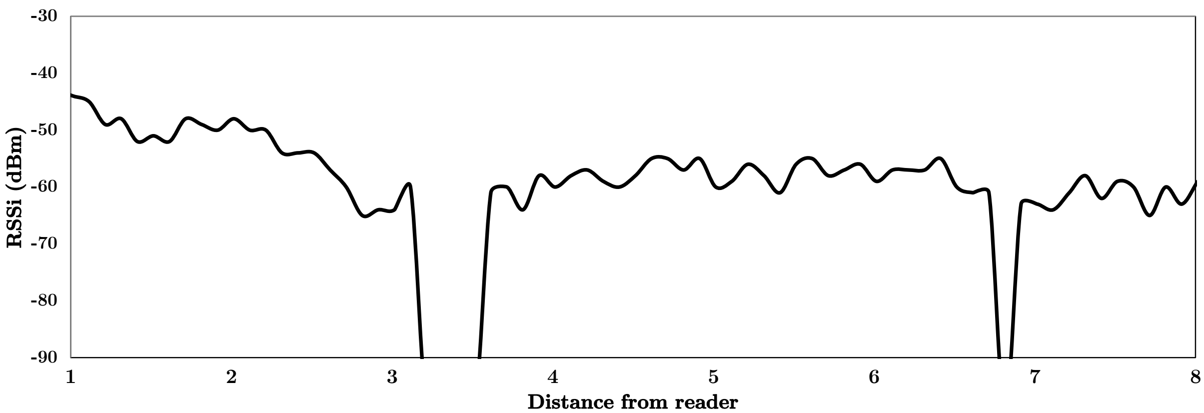


Figure 4.4: Fading effects [60]

4.2.3 Interference

Multiple readers operating in the same environment can interfere with each other. The FCC requires readers to adhere to frequency hopping as a way to mitigate this issue. As discussed in Section 4.2.1, the power ratio between the reader signal and the received tag signal can be in the order of 10^8. The interference can also cause issues in other ISM devices [61].

Figure 4.5 shows an example of the interference. If $reader_1$ is transmitting in channel c_1 and $reader_2$ in channel c_2 while the tag signal is at some offset from the $reader_1$ channel, the signal from $reader_2$ might be stronger than the tag signal, making it incomprehensible to $reader_1$.

The interference problem can affect localization approaches that require multi-reader setups, like trilateration and triangulation. It also causes problems in dense setups, such as in large warehouses, where multiple readers can be located.

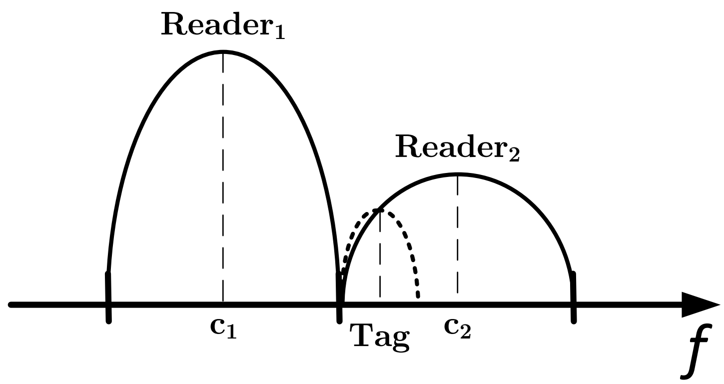


Figure 4.5: Interference from reader

4.3 Improvements

In literature, one of the trends for UHF RFID systems is improving the localization of tags [1]. Localization in a UHF RFID can open up many new applications, such as [62]:

- Tracking people
- Intruder location
- Patient location
- Indoor navigation
- Social interaction monitoring

By itself, a UHF RFID system is limited in its ability to localize tags. Such a system would rely on the received signal strength values of the tags, but due to the effects of multipath and fading, the values received are unreliable. Also, the techniques require calibration. The use of multiple readers for triangulation or trilateration can impose interference problems in the system.

Chapter 5

Receiver System-Level Design

5.1 Overview

This chapter proposes a solution to the problems and improvements described in the previous chapter in the form of an augmented RFID system. Central to this system is a new receiver device, called the ARR, which compliments the regular reader-tag RFID system, Fig. 5.1. The ARR receives the tag and reader signals and reports the collected data to a host PC. The chapter starts with how the augmented system can mitigate the problems introduced in the last chapter. Next, it will discuss unique problems associated with introducing a new actor into the system.

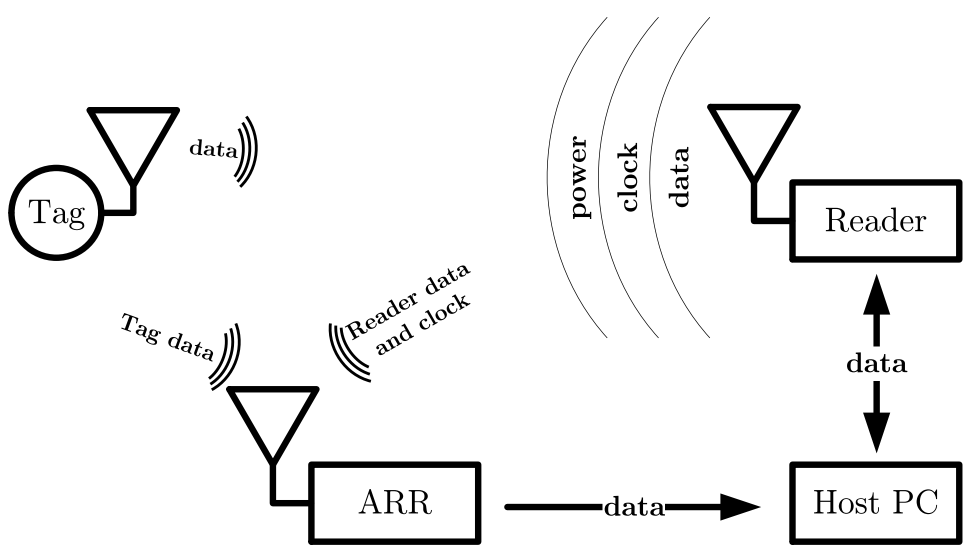


Figure 5.1: Augmented RFID system

5.2 Mitigating RFID problems

Link budget

In the previous chapter, the problem of forward and reverse link limited tags was introduced. A receiver cannot mitigate the issue of forward link limited tags, but can partially solve the reverse link issue. In some cases, the receiver sensitivity of the reader is not high enough to capture the response of a tag, even though the tag received enough power. By introducing receivers, which are scattered across the area, into the system, the chance of that happening is decreased: if the reader does not pickup the signal, the receivers could be able to, thereby improving the read range.

Fading and multipath

The null points introduced in the previous chapter are environment sensitive. By introducing a new receiver into the system, the chance of a tag appearing in a null point decreases. The null point would have to occur for both the reader and the receiver, or for the tag when it does not receive any power, for the tag to be unreadable.

Interference

Having only one transmitter and multiple receivers overcomes the interference issue that multiple readers in an area would have and minimizes interference with other devices in the ISM band.

Localization

Having multiple receivers allows the proximity method to be implemented in a UHF RFID system, as shown in Fig. 5.2. The receivers R_n are fixed at known locations over some area; their receive range is shown by the circle around them. A reader transmits a signal and the tag backscatters a response. Based on which receiver sees the response, the location of the tag is estimated nearby that receiver. This method can be improved using any of the localization methods mentioned in Chapter 2. The methods would have improved performance, due to having multiple anchor points to base their approximations. This approach is followed by the Gen2 Listener [4] and the Sensatag [3].

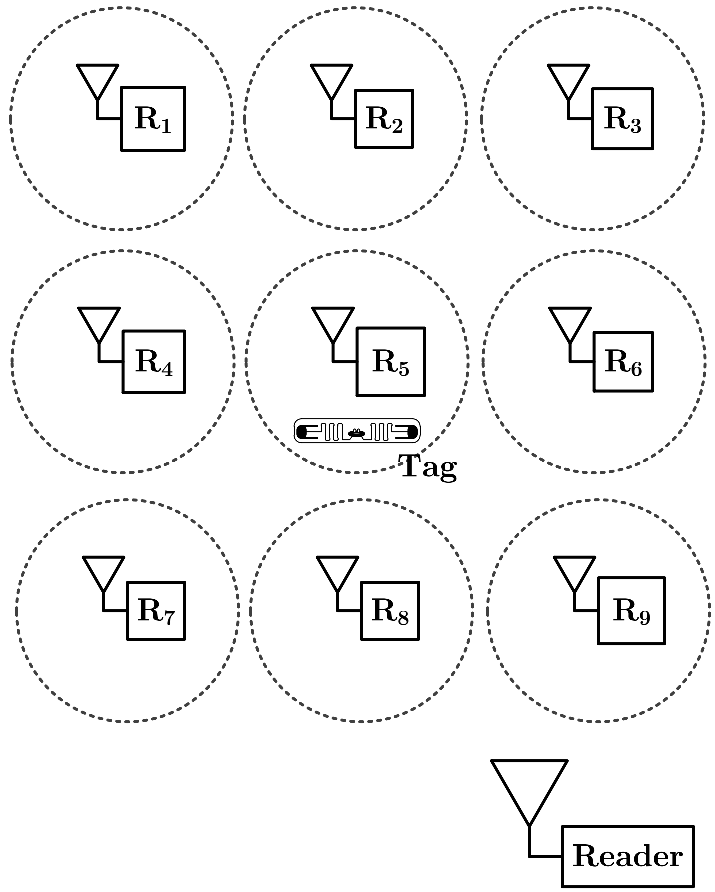


Figure 5.2: Proximity localization

5.3 System-level design

5.3.1 Overview

Fig. 5.3 shows the high-level overview of the receiver implementation, the ARR. It consists of a UHF RFID reader IC acting as the RF front-end and an FPGA with a soft-core CPU performing the digital functionality. Ethernet is used for communication with the host PC. The next sections in the chapter will give the details of the subsystems in use.

5.3.2 RF selection

An important issue with the receiver is the radio architecture used. Choosing a architecture can affect the sensitivity, dynamic range, and other properties, as discussed in Chapter 2. The direct conversion architecture was selected for the receiver because of its

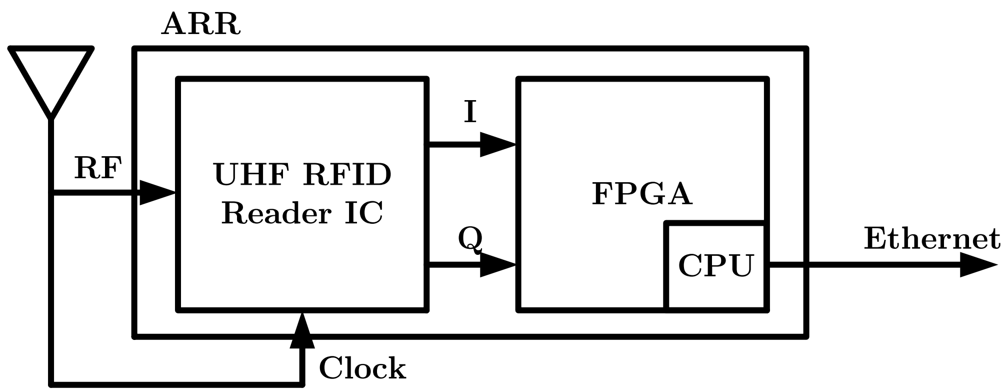


Figure 5.3: High-level block diagram

good sensitivity and low price compared to the superheterodyne architecture.

Some standard RFICs were evaluated for the RF section, including the *CC1100* [63] and *RFM22* [64]. Although these ICs operate in the same frequency band, they do not support the modulations and encodings of EPC Gen 2. The following problems prevent the CC1100 IC from being used as a UHF RFID receiver (the same problems are attributed to the RFM22, but with different numbers):

Data rate

The CC1100 supports a maximum data rate of 500kBaud, while EPC Gen 2 can go upto 640kHz. Not all modes can be supported due to this limitation. For ASK modulation, which EPC Gen 2 uses, this number goes down to 250kBaud for the IC.

Selectivity

During a tag backscatter, two signals are present in the frequency spectrum: a large continuous wave (CW) from the reader which powers up the tag and the small tag backscatter signal. As described in Section 4.2.1, the reader signal power can be 0dBm and the tag backscattered signal power can be as low as -80dBm. The frequency component of the tag backscatter is at some distance from the large CW on the frequency spectrum; the distance is the baseband frequency, e.g. 256kHz. At 256kHz, the filters can manage an attenuation of approximately 20dB, so the reader signal will overwhelm the tag signal.

Saturation

At 250kBaud and 915MHz, the saturation limit is -15dBm for the CC1100. The reader signal will saturate the chip. To overcome this, attenuation can be set, but the attenuation will also bring down the sensitivity.

Frequency Hopping

Knowledge of the next frequency hop is needed beforehand to shift to it in time. More details on this topic will be presented in the next section.

Based on these requirements, a UHF RFID reader IC was selected. The use of a UHF RFID reader IC presents some problems of itself, which will be discussed further.

5.3.3 Synchronization

Frequency Hopping

UHF RFID operates in the ISM unlicensed band and shares the spectrum with other devices. To mitigate potential interference, FCC instructs to use frequency hopping. In the ISM band, 902-928MHz, a device can occupy a channel for at most 400ms [65]. The regulations also state that the next channel to be occupied must be selected pseudo-randomly.

The frequency hopping provision presents a problem for the receiver design. In a normal RFID system, the reader transmitter and receiver are combined in an embedded system, and the receiver knows the frequency at which the transmitter sent the signal. Since the receiver is decoupled from the transmitter, the receiver must have knowledge of the frequency channel of transmission.

In general, three methods can be identified to overcome the channel hopping issue. The first method is to listen to all the channels. Depending on the region of operation, this could be a simple task, like in Europe, where the number of channels is low. For North America, where there are 50 channels, in the frequency range from 902-928MHz, this is not such a simple task.

The second solution involves predicting the next channel hop, through a stepped serial search. A certain amount of time is required to acquire a lock on the channel, either by scanning the spectrum until finding the transmitting channel, or randomly hopping, and then predicting the next hop. This will work if there is knowledge of the algorithm used for determining the next channel hop. Based on the FCC specifications, the algorithm is to be pseudo-random, so it is up-to the manufacturer to implement the algorithm for channel hopping. In some cases, this can be determined by reverse engineering the algorithm with the help of a spectrum analyzer.

The third solution is for the receiver to somehow be directly notified the next frequency hop by the reader or host PC. The most widespread communication protocol between PCs and RFID readers, LLRP, specifies a function called *NextChannelHop()* which tells the channel of the next transmission. In this scenario, a PC calls this function through LLRP and reports it to the receiver device through Ethernet. With this approach, there are time delay issues and not all UHF RFID readers support LLRP.

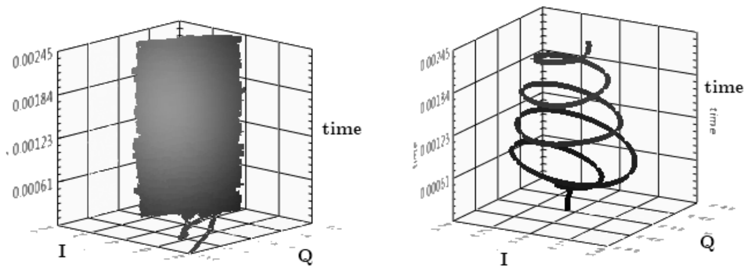
Frequency offset

Oscillators have a rating of their stability, i.e. offset from a desired frequency, expressed as parts per million (ppm). The EPC Gen 2 standard defines the minimum stability rating for the oscillator to be 10 ppm in Dense Reader mode [27]. The RFID reader uses the same local oscillator for sending the signal and receiving the backscattered signal, so no frequency offset will be present in the reader (except from Doppler shifts due to moving tags, but they are negligible even on fast moving tags, e.g. tags on trains [66]). The frequency offset is a problem for the ARR, which is decoupled from the transmitter.

A frequency offset can be modeled as the multiplication of the signal by e^{jwt} where w is the frequency. This multiplication causes an instantaneous change in phase in the I/Q constellation, which causes a rotation. An experiment was setup to showcase the problem of frequency offset. A UHF frontend, consisting of an antenna, bandpass filter and mixer, and the analog output from the RFID reader were connected to an oscilloscope. The signal during a tag-reader exchange was captured. The I/Q constellation vs. time was then plotted in LabView. Fig. 5.4 shows the obtained results; the z-axis is time and the y and x axes are I and Q. Fig. 5.4(a) shows the I/Q constellation of receiving a PR-ASK signal successfully by the RFID reader. Fig. 5.4(b) shows the obtained signal on the UHF frontend. If two LOs are used without any provision to deal with frequency hopping, a rotation appears, as seen in Fig. 5.4(b), and the signal cannot be successfully demodulated.

If a radio was tuned to the same channel as the transmitter, e.g. 902.75MHz, then it would see a large signal adjacent to the tag channel in the $\leq$ 10 kHz range. Figure 5.5 shows how the frequency offset looks in the time domain. The top row is the clean reader and tag signal, as seen on the RFID reader. The tag signal is the high frequency square wave at the end. The bottom row is the received response with frequency offset. The strong signal from the reader is modified, but the high frequency weak tag signal cannot be seen, but rather the large blocker signal at around 8kHz is seen.

Figure 5.6 shows the frequency spectrum during the exchange of messages between



(a) Without frequency offset (b) With frequency offset

Figure 5.4: Frequency offset in I/Q constellations

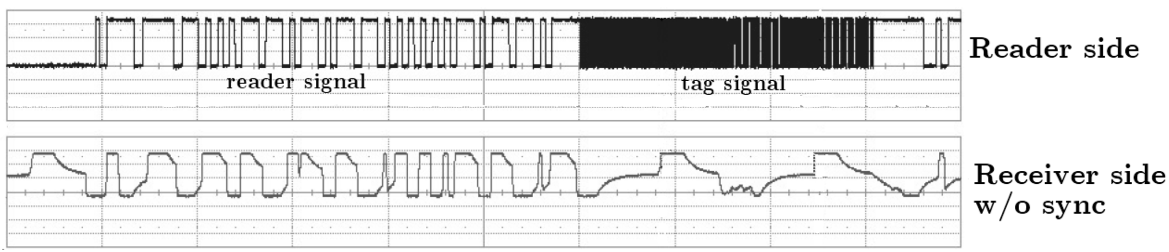


Figure 5.5: Frequency offset in time domain

the reader and the tag, from the point of view of the receiver with no frequency offset compensation, tuned to the channel of communication. At point 1, the frequency offset at 8kHz can be seen. Point 2 is the reader PIE signal at 40 kHz and point 3 is the tag backscatter signal at 160kHz. The frequency offset is 20dB larger than the backscatter signal of the tag.

Synchronous detection

To mitigate the frequency offset and deal with frequency hopping, the receiver uses a method called *synchronous detection*. In this method, the clock is retrieved through the air, instead of using a local oscillator. Figure 5.7 shows conceptually the frequency domain during the tag transmission. The reader sends a large signal at a fixed frequency called the continuous wave (CW) and the tag responds with a weak backscatter signal. The CW signal is used as an input to the mixer instead of the LO.

The synchronous detection method is shown in Fig. 5.8. The dotted lines display the frequency components at the various stages of the design. The signal to the LO is taken from RF signal path and is amplified to remove any modulation, i.e. the backscatter

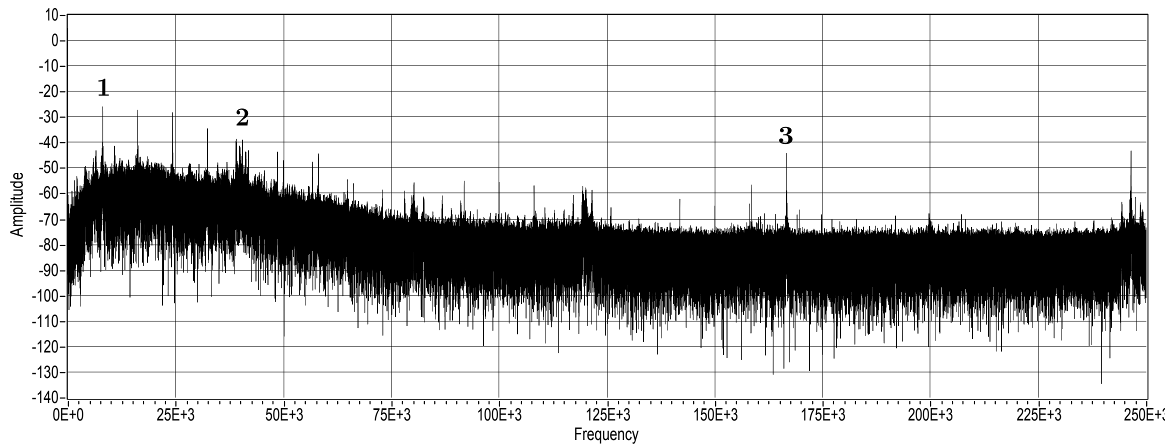


Figure 5.6: Frequency spectrum from receiver viewpoint

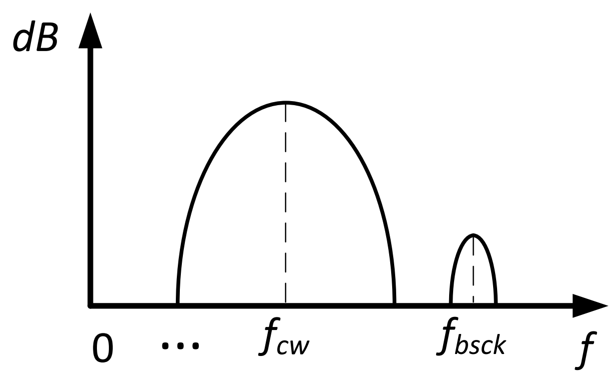


Figure 5.7: Spectrum during tag backscatter

signal. The mixer outputs the difference of the frequencies (the sum of the frequencies is filtered out). After a baseband filter, only the tag backscatter signal remains. Another way of implementing such a system would be to use antennas of different gains. The lower gain antenna would miss or have an attenuated modulation signal.

For the reader signal, there is no continuous wave present, but the same approach can be applied, Fig. 5.9. The reader is self-mixed with an attenuated or amplified version of itself. At the output of the mixer is the downconverted reader signal. This signal is then slightly attenuated, provided the same bandpass filter as in the tag case is used.

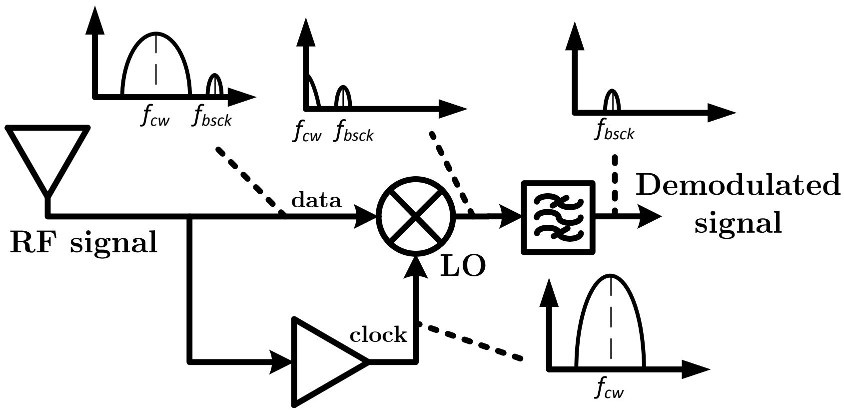


Figure 5.8: Synchronous detection during tag backscatter

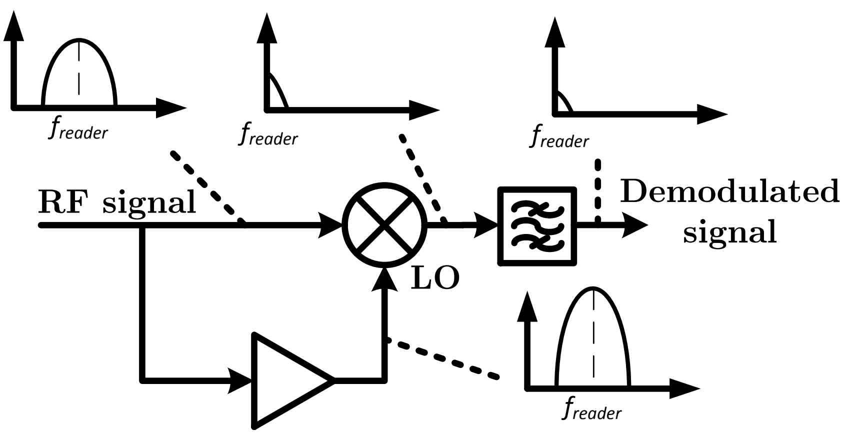


Figure 5.9: Synchronous detection during reader transmission

5.4 Digital section

The RF section provides a digital signal which still has to be decoded and reported to the host PC. The decoding and communication was implemented on an FPGA. FPGAs provide excellent performance characteristics and lots of flexibility to accommodate changing standards. They also allow the capability of putting a soft-core CPU inside, allowing the benefits of both FPGAs and CPUs. The soft-core CPU was implemented inside the FPGA to deal with the communication with the host. The CPU implemented a TCP/IP stack so that communication was relatively easy.

5.4.1 Communication

Another question to be addressed in the ARR is how it will communicate the data it has received. This can be achieved through the following ways:

- Air-communication
  - UHF RFID
  - Other wireless standard
- Wire communication
  - Ethernet

Communicating through the air-interface introduces the following problems: potential interference, more complicated RF section, and using the bandwidth that could be used for reading tags. For the ARR, Ethernet communication was selected.

The host PC has to have a custom application running in order to process the packets from the ARR. The custom application is based on LLRP, so the device can be integrated with existing systems, where the communication protocol between the reader and the host PC is based on LLRP.

Chapter 6

Receiver Implementation

6.1 Overview

This chapter goes into the implementation details of the ARR. It builds on the previous chapter and gives more concrete details of how the various sections of the receiver were built. Starting with the hardware section, progressing to the digital section, and finally the PC host section.

6.2 Hardware

6.2.1 RFIC

The Austria Microsystems AS3992 was selected as the RFIC. The RFIC is an EPC Gen 2 compatible front-end, which has a direct conversion RF section and EPC Gen 2 protocol handling capability. Fig. 6.1 shows the architecture of the RFIC.

Through register settings, the IC can support different modes and settings such as the gain of the receiver chain and filter selection. The reader IC also has provisions to decode tag signals by decoding the Miller and FM0 encoding. By itself, the reader IC does not support receiving and decoding the PIE signal, so the decoding part was outsourced to another digital section.

Another issue for the IC is the maximum input power. The reader signal can be upto 36 dBm (after the antenna) and the $1dB_{cp}$ for the IC is 10dBm. Assuming the reader antenna is 6dBi and the receiver antenna is 3dBi, the closest a reader antenna can be to the receiver antenna is 0.7 meters, based on the Friis equation:

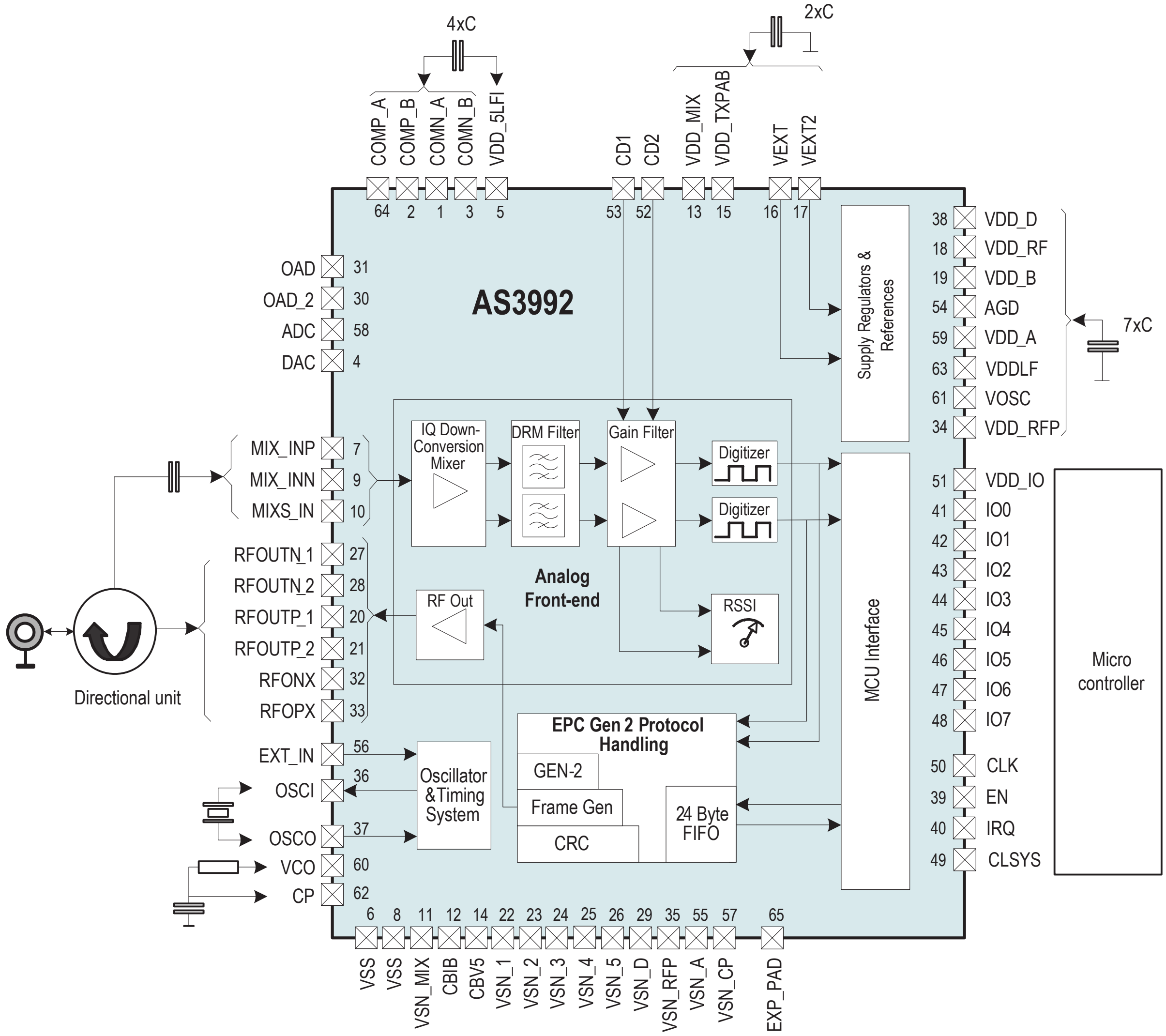


Figure 6.1: AS3992 architecture [67]

$$P_R = \frac{P_T G_T G_R \lambda^2}{(4\pi d)^2} \tag{6.1}$$

where P_R is the received power, P_T transmitted power, G_T and G_R the transmitted and received power respectively, d distance between receiver and transmitter, λ wavelength of the signal.

Most reader ICs regularly operate solely, i.e. performing the demodulation, decoding, and protocol processing. They send the data to an FPGA or microcontroller through some communication interface. The AS3992 is capable of this with the EPC Gen 2 protocol. Since the IC does not act as a reader in the application, the protocol processing abilities of the chip cannot be used. Fortunately, most chips include a *direct mode*, where the protocol processing is bypassed and a demodulated analog or digital signal is output. In this mode, the chip acts only as an RF front-end.

The IC also has an oscillator and timing system. Unfortunately, it cannot be used as discussed in the previous chapter due to the frequency offset problem. To mitigate the issue, synchronous detection was used. To achieve synchronous detection outlined in the previous chapter, the external VCO port, EXT_IN, was used of the AS3992. An external low gain loop antenna was used to provide an attenuated version of the signal for synchronous detection. Another solution would be to use an amplifier on the RF signal path, but the power consumption and cost would rise.

The sensitivity of the receiver is configurable through register settings, which allows increasing or decreasing the read range of the receiver. The step size of the read range was experimentally determined to be around 50 cm. The output from the RF section is the I and Q datapaths. Fig. 6.2 shows the reader-tag exchange as seen by the AS3992 chip using synchronous detection. The Q-channel can be seen to have a higher amplitude than the I-channel. Fig. 6.3 shows the spectrum of the signal. Compared to the large blocker introduced in the previous chapter, Fig. 5.6, the output is much cleaner, and the reader and tag signal are much more visible.

Fig. 6.4 shows the block diagram of the parts used from the IC. The output from the AS3992 to the digital section is the signal after passing through the comparator. Fig. 6.5 shows the reader ACK command and the tag EPC response digital signals.

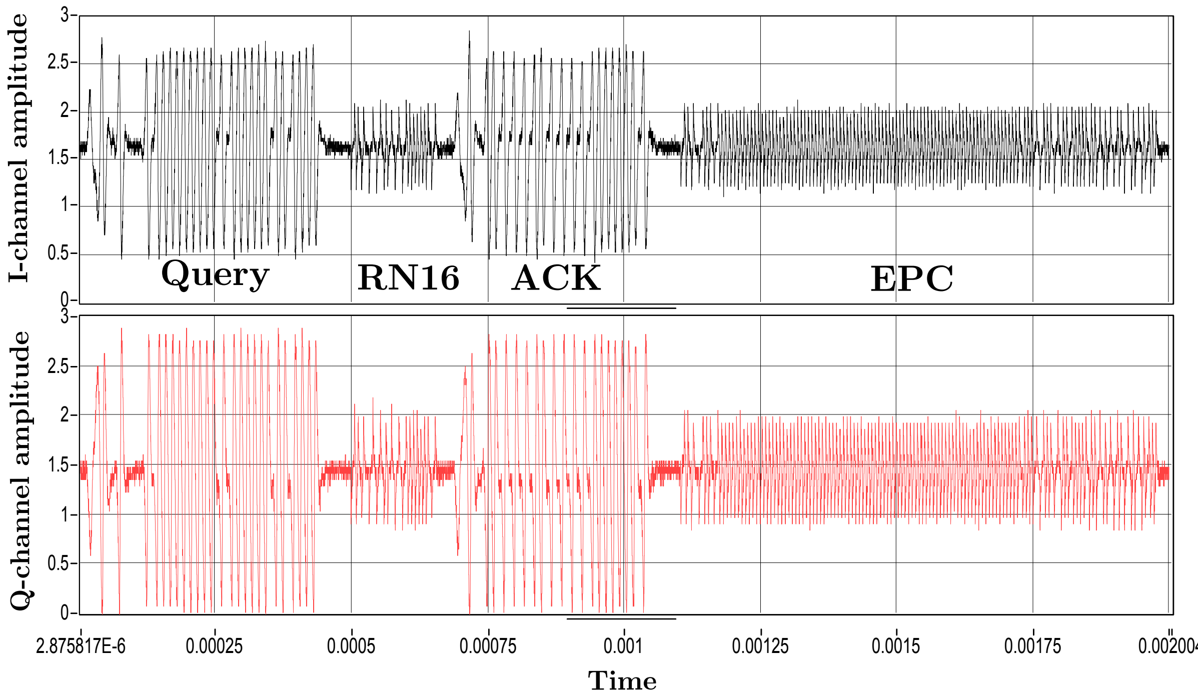


Figure 6.2: AS3992 analog output

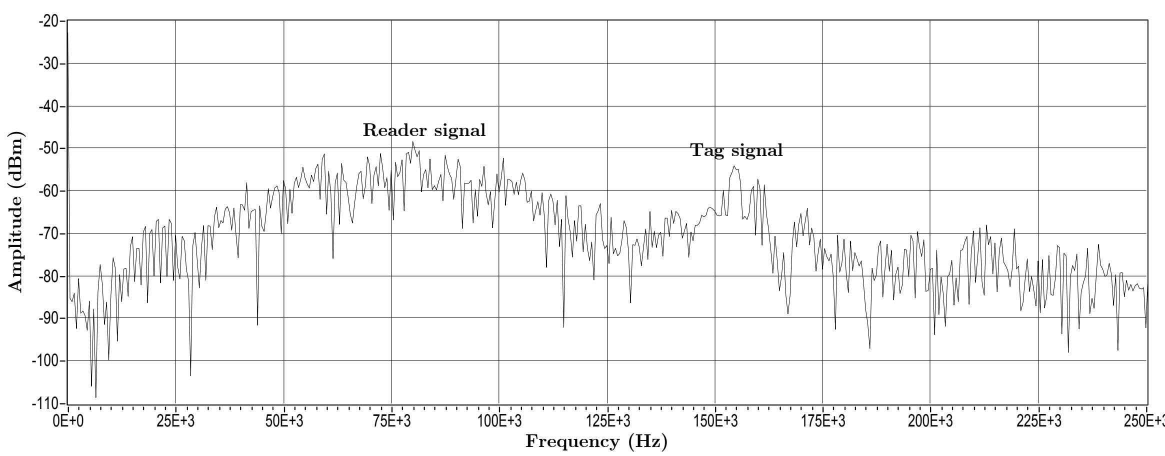


Figure 6.3: AS3992 output spectrum

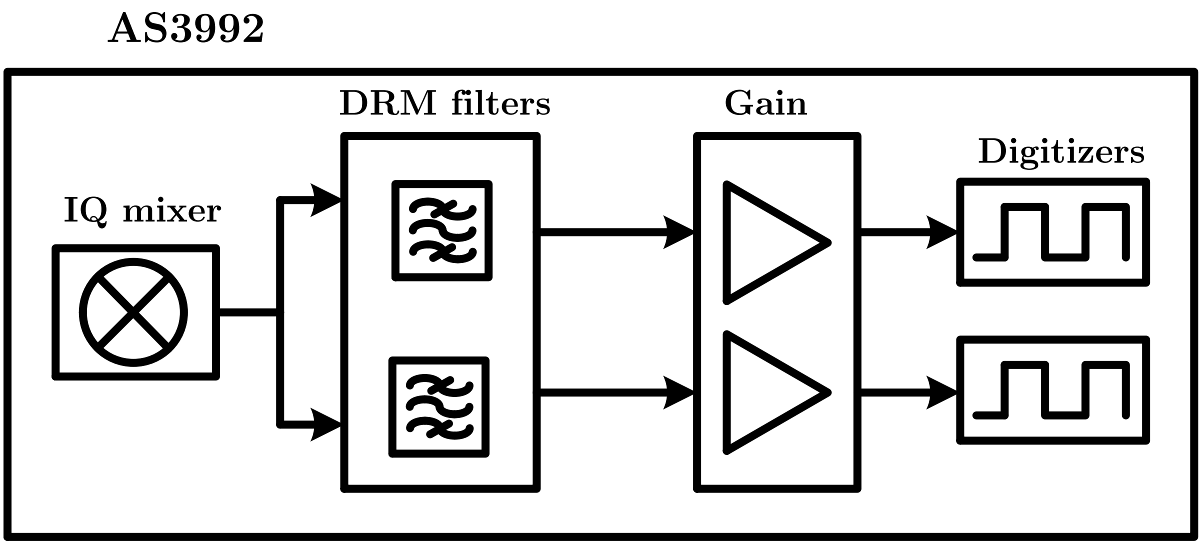


Figure 6.4: AS3992 subsystem

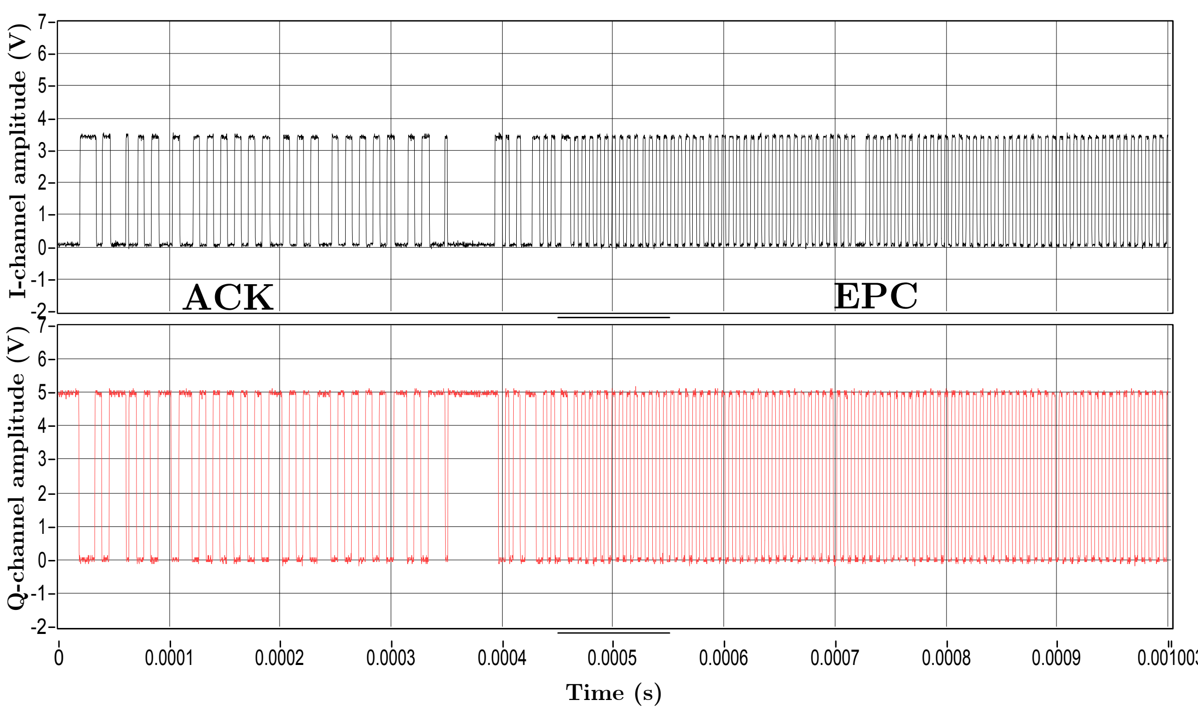


Figure 6.5: AS3992 digital output

6.3 FPGA subsystem

6.3.1 Overview

Fig. 6.6 shows the overview of the program running on the FPGA. This section will go over the details of each block in the system. The main blocks of the figure are the reader PIE decoder, FM0 decoder for the tag signal, reader command decoder, and tag command decoder. Gates are used for the tag signal. Once the reader receives an *ACK* from the reader, the gates are opened for decoding the tag signal. This is done to have the tag state machine correctly operate. The system was implemented in Verilog and running on a Xilinx Spartan 3E starter kit.

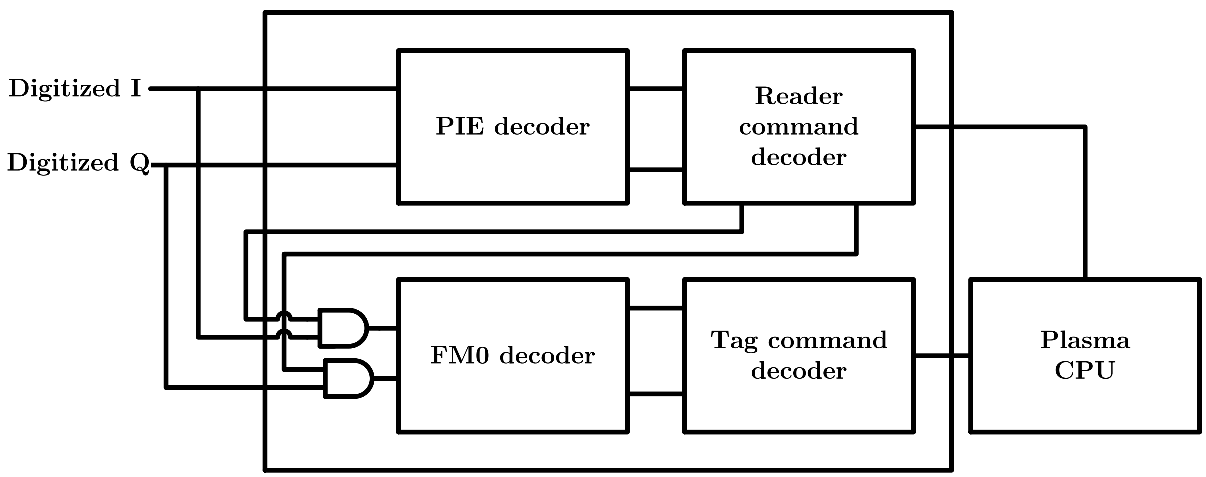


Figure 6.6: FPGA system

6.3.2 Reader decoder

The PIE decoder module samples the input waveform and outputs the data symbols; it also provides a symbol clock, which rises whenever a symbol has been decoded. The symbols come in six varieties: *data-0*, *data-1*, *TRcal*, *RTcal*, *invalid* and *delim*. The symbols can also have different parameters depending on the *TARI* (length of data-0) value set by the reader.

The signal is oversampled by 625 samples due to the default clock of 50MHz on the FPGA, which can be lowered if power consumption is a concern. A lookup table is used to determine the symbol. A counter *hi_cnt* is started on a high signal. Whenever a falling edge is detected, a counter *lo_cnt* is started and the *hi_cnt* is stopped, Fig. 6.7. A rising edge indicates the end of a symbol. Furthermore, the type of symbol: *TRcal*, *RTcal*, *data-0*, *data-1*, *invalid*, and *delim* is determined from the length of the symbol, *cnt_sum_reg*, and the high count, *hi_cnt*, through a lookup table. The low count, *lo_cnt*, is only needed to determine the mode of operation.

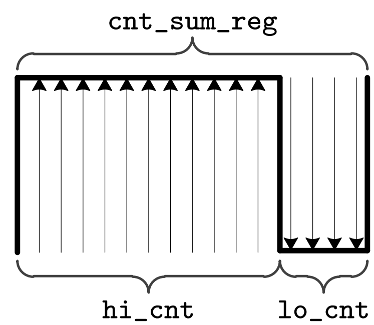


Figure 6.7: Oversampling of the reader signal

The command decoder is a state machine that is sensitive to symbols from the PIE decoder, shown in Fig. 6.8. On each symbol clock from the PIE decoder, the machine changes state. The state machine begins by receiving the frame-sync, Fig. 2.13, character-by-character. A *delim* brings the state machine into the *DELIMITER* state, a *data-0* afterwards brings it to the *DATASYN* state, finally a *RTcal* denotes the *FRSYN* state. From the *FRSYN* state, the state machine branches into one of three directions depending the next received symbol. A *TRcal* marks a *Query* command and goes into the *PREAMBLE* state, from there to the final state *QUERY*. A *data-1* denotes either a *Select* or *QueryAdjust* command, going through intermediary *SELQADJ* and *SELQADJ1* states. A *data-0* from *FRSYN* denotes either a *QueryRep* or *ACK*, going through the intermediary *QREPACK* state. The command decoder stores the reader command and parameters received after reaching a final state into a register accessible by the soft-core CPU. It also checks the CRC of the received packets to see if the packet is not erroneous. When entering the *DATASYN* state, the CRC16 and CRC5 decoders are enabled. Each subsequent received bit is also transferred to the CRC calculators. On finishing receiving most commands, the calculated CRC is compared to the received CRC. If they are equal, then the command was received correctly.

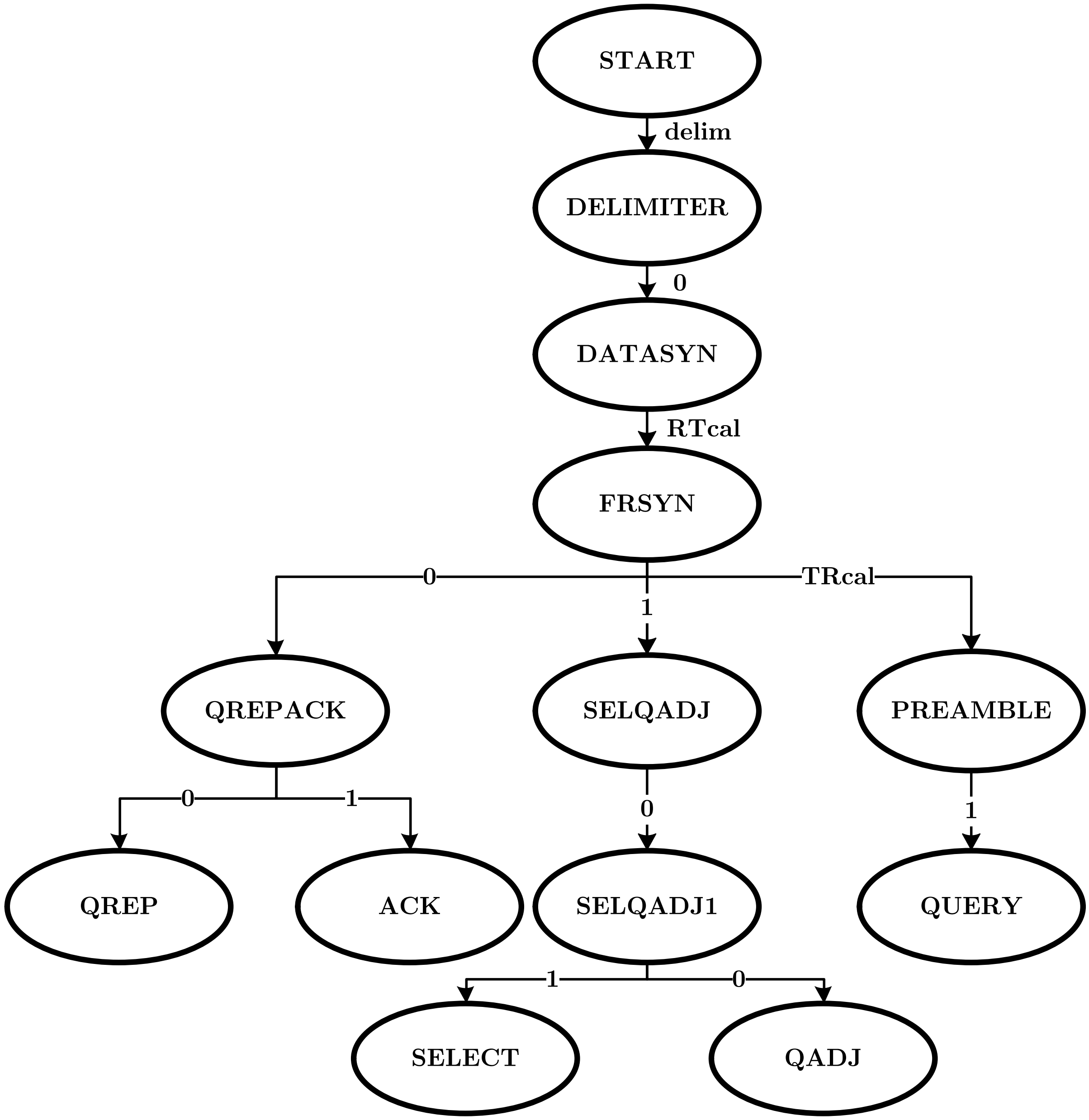


Figure 6.8: Reader command decoder

6.3.3 Tag decoder

The tag decoder decodes the FM0 signal. The method used for decoding this signal is a modified version of the method presented in [68]. The method is similar to the PIE decoder method. A close look at the FM0 waveforms in Fig. 2.11, the following rectangular waves in the waveform can be identified, shown in Table 6.1. The method based in the paper [68] proposed looking at the duty cycles of the rectangular waves to decode them. Duty cycle requires a division operation which is not efficient in FPGAs. The method used in this implementation is a modified version, where a lookup table is used to compare the high and low counters to symbol values that are obtained experimentally.

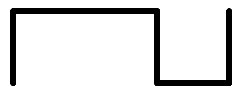
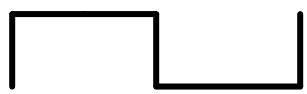
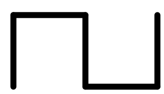
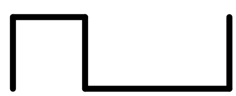
Symbol	**Waveform**	**Bit(s)**
RW0		10
RW1		11
RW2		0
RW3		1

Table 6.1: Rectangular wave decoding

After receiving the decoded bits, they are passed through the tag command decoder to retrieve the EPC of the tag. Figure 6.9 shows the command decoder used for this. First, the FM0 preamble is received, after which the EPC bits. After receiving the final EPC bit, the state machine verifies the CRC of the received EPC

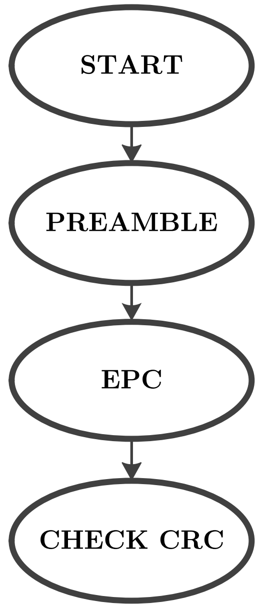


Figure 6.9: Tag command decoder

6.4 Firmware

The Plasma soft-core CPU [69] was selected to run on the FPGA to send the Ethernet packages. It is a 32-bit open source CPU with MIPS compatible instructions. The Plasma CPU runs the Plasma RTOS, which deals with the TCP/IP layers.

The VHDL code of the soft-core CPU was modified to add connections to the registers from the decoded bitstreams. Fig. 6.10 shows these connections. Two registers containing the tag decoded signal and the reader decoded signal were added to the memory map of the CPU at addresses *0x40000000* and *0x40000001*. This way, the registers can be accessed from the RTOS level. To indicate that a reader or tag signal has been successfully decoded, two interrupts were introduced, $INT1$ and $INT2$, which would be asserted on successfully decoding either signal from the associated state machine.

A program was written on top of the Plasma RTOS in C to send packets through the Ethernet to a designated server once an EPC has been decoded through UDP. The program sleeps until an interrupt has been received. It then prepares and sends a packet through Ethernet using the UDP protocol. The packet structure is presented in Fig. 6.11. RSSi (Received Signal Strength indicator) is a placeholder for future work.

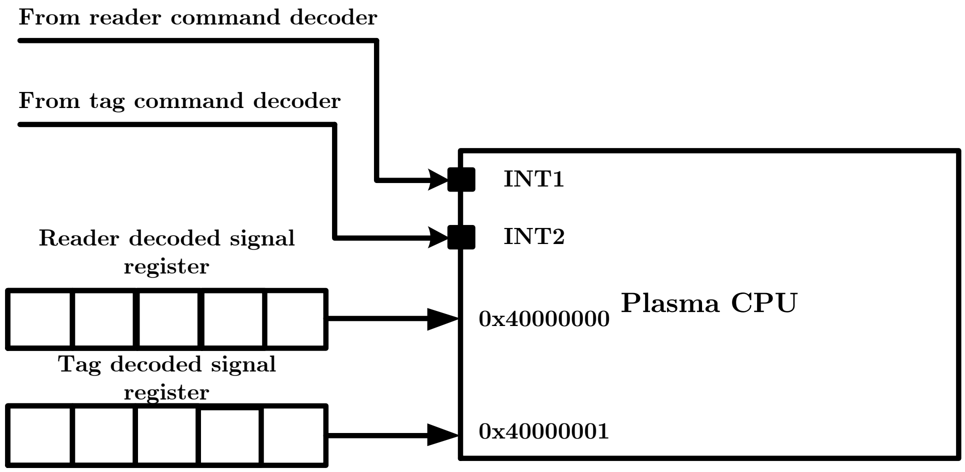


Figure 6.10: Plasma connections

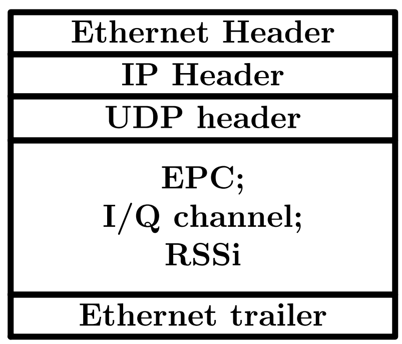


Figure 6.11: Ethernet packet structure

6.5 Software

A command-line program was coded in C# in Microsoft Visual Studio to control the RFID reader. The program established an Ethernet connection to the reader at a set IP address and configured it to the mode selected. Next, it commanded the reader to continuously send *Query* commands to the tag. The response from the tags was displayed on screen.

Wireshark was used to receive the packets from the receiver. The program was selected due to its powerful filtering features and ability to look at the Ethernet packet contents in detail. The display was selected to filter out all packets except coming from a certain IP address, then the data was verified by looking at the fields of the IP packet.

Chapter 7

Performance and testing

7.1 Overview

This chapter presents the tests that were conducted on the receiver to characterize its performance. The receiver was tested for range, read rate, and performance with the tag under different orientations. At the end of the chapter, a comparison is made between the ARR to the other approaches, outlined in Chapter 3. Each of the tests starts with a short description of the goal and setup of the experiment, then the results and finally discussion.

7.2 Experiments

7.2.1 Range

The first set of experiments on the receiver was performed to characterize its performance based on the distance from the reader. The design of the ARR relies both on the reader and tag signals to successfully decode EPCs. A tag is considered successfully read if an Ethernet packet is received containing the tag's EPC. Wireshark was used to count the number of packets, which was an indicator for performance. The reader was set to Hybrid mode, 160kHz FM0, 30dBm output power for 60 seconds. A Higgs3 [70] passive dipole and PowerP [71] semi-passive tag were used for the tests.

Reader range

First a passive dipole, then a semi-passive tag were placed at a distance of one meter away from the receiver. Fig. 7.1 shows the setup. The reader antenna was set to output at full power. The distance between the ARR and the reader antenna, d, was increased from one to eight meters, with an interval of one meter. Fig. 7.2 shows the read rate results for both semi-passive and passive tags. At some distances d, the effects of multipath and fading made the tag unreadable. In such cases, the reader antenna was slightly moved to the side to mitigate this effect. More discussion on this is presented in the next section.

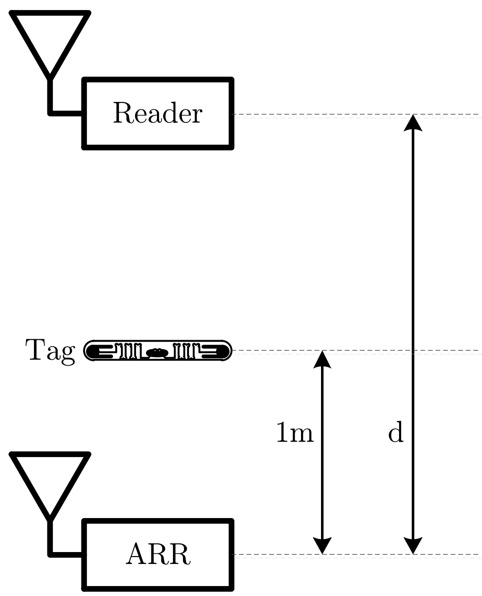


Figure 7.1: Range experiment setup

The results show that the distance from the reader to the receiver does not affect the performance when the distance is within 8 meters, which is the room length. Semi-passive tags have a read rate of about 140-160, while passive under 100 packets per minute. Since semi-passive tags have batteries, they respond with a much better signal leading to less EPCs received in errors.

Maximum range

The goal of this experiment was to determine the maximum distance that the receiver can sniff the tag response. A similar setup was made to the previous experiment, but the distance d was fixed at 8 meters, while the distance from tag to receiver was varied.

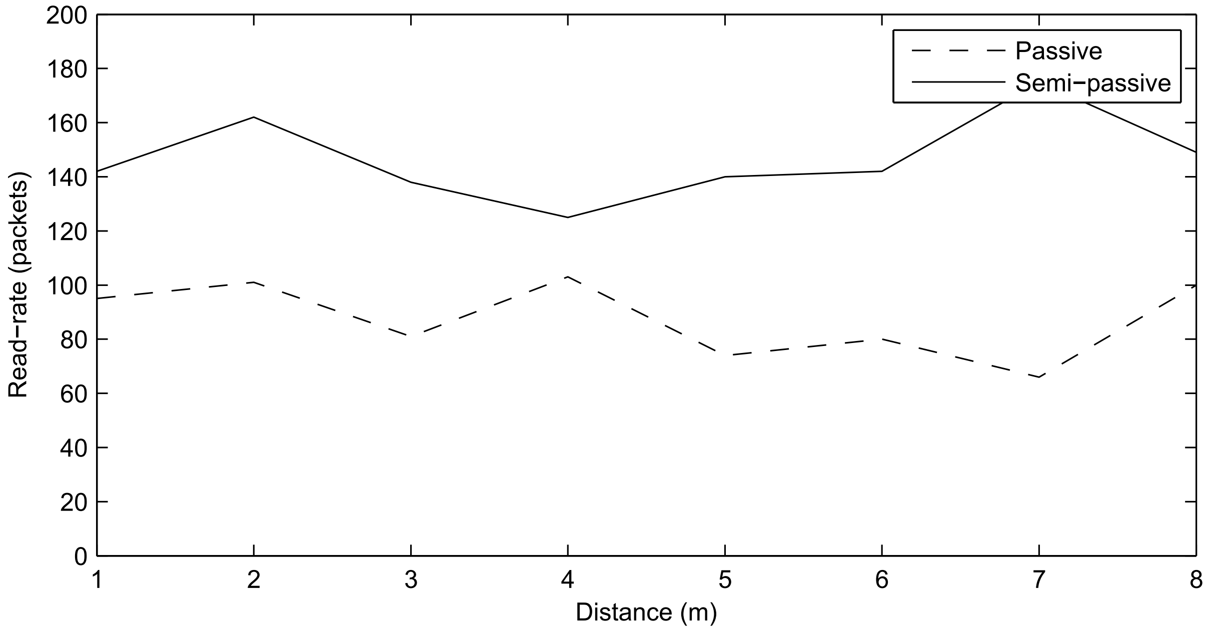


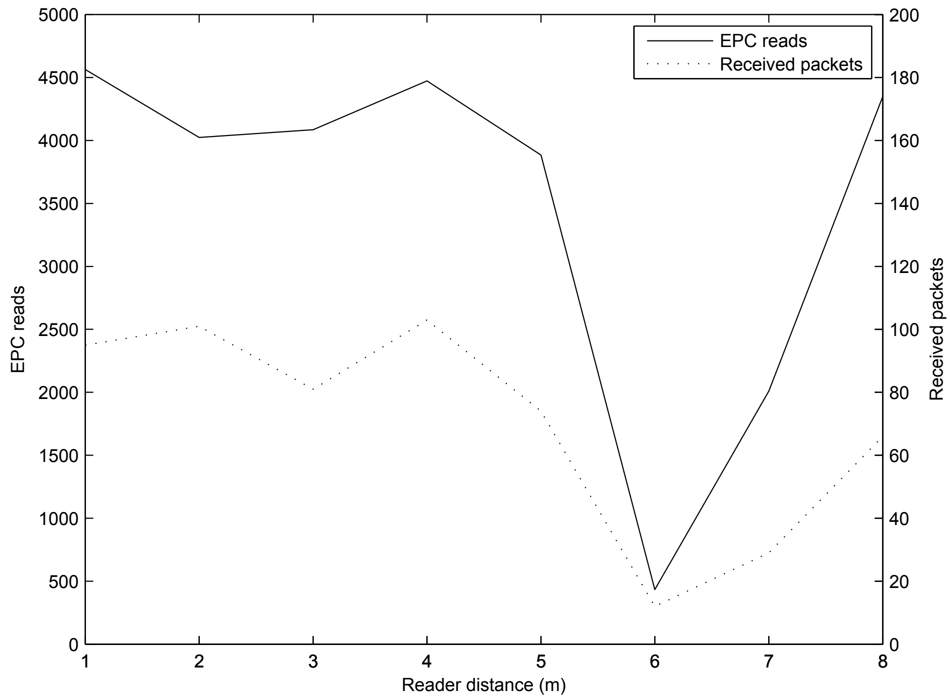
Figure 7.2: Reader range vs read rate

The reader was set to transmit for 60 seconds and the tag was moved away from the receiver until the receiver could not sniff the EPC anymore. A test was made without Ethernet sending: a counter was implemented on the FPGA and Ethernet was disabled. The reader was set to transmit a *Query* every second for 60 seconds. A logic analyzer was then used to get the counter value. A tag was considered sniffed if the receiver could read more than 5% of the EPC commands. For passive tags, this distance was determined to be 3.25 meters and for semi-passive it was determined to be 5.5 meters. Depending on the application, the range can be reduced by adjusting the attenuation registers of the AS3992 chip.

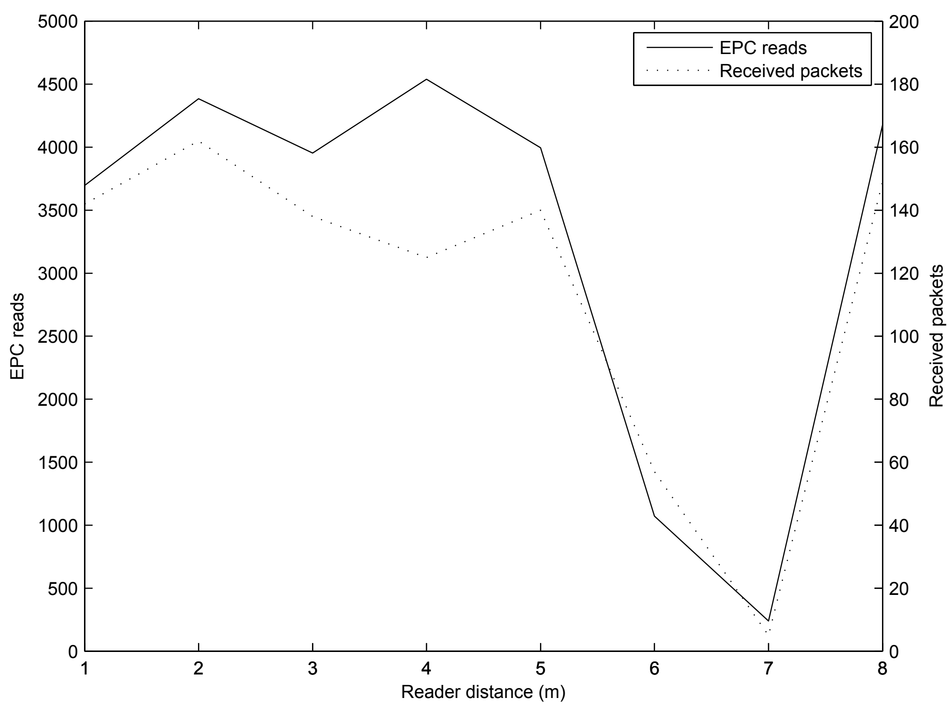
7.2.2 Read rate

In this experiment, the read rate of the ARR is compared to the read rate of the reader. The setup was the same as in the first experiment. The distance from the reader to receiver was varied. Fig. 7.3 shows the results. The right y-axis shows the number of reads by the reader, the left y-axis the number of packets received from the ARR, and the x-axis is the distance of the tag from the reader.

At 6 and 7 meters a dip can be seen in the graphs. This is due to the multipath effect,



(a) Passive



(b) Semi-passive

Figure 7.3: Reader range vs read rate

which renders the the tag almost unreadable, and only a few EPCs are received. At 8 meters, the tag is no more in a fading zone and the read rate returns to normal. The read rate of the ARR, here considered to be the amount the Ethernet packets received, is approximately 4% of the read rate the reader. This is attributed to the latency of Ethernet packet preparation and sending. Once an EPC has been successfully decoded, the receiver spends time preparing the Ethernet packet discarding the EPCs in this time.

With the Ethernet disabled and the counting done internally as in the "Maximum range" test, after the reader sent 60 *Query* commands and the tag responded with 60 EPCs, the ARR can sniff 38-42 EPCs for semi-passive and 27-31 EPC for passive tags at a one meter distance. Thus, read rates of 66% for semi-passive and 50% for passive tags were achieved.

The ARR also highly depends on the read rate of the reader. If the reader is in a fading area, as seen at distances 6 and 7 meters, and constantly sending out Queries to the tag, the tag will respond with RN16. Since the reader does not receive these RN16 due to fading, it is unable to complete the Query round and get the EPC even though the ARR might still successfully receive the packets. Thus, to make the ARR solution more practical, changes must be made to the EPC Gen 2 protocol to mitigate this behavior. Modifications to the protocol are not unheard of, and some companies do so to better adapt to some applications [72].

7.2.3 Orientation

In these sets of experiments, the orientation of the tag was varied with respect to the ARR. The previous experiments had the reader, receiver, and tag antennas set in the best orientation.

Tag Orientation

The tag was fixed at 0.3, 0.6, and 1 meters from the ARR. The orientation of the tag, α, was changed with respect to the ARR. Fig. 7.4 shows the setup. Fig. 7.5 shows the results. The results show that the read rate is consistent for all orientations, except for 90° where it drops to zero, which is to be expected.

Orientation to ARR

In this experiment, the tag was oriented straight, but placed at an angle to the ARR, α, Fig. 7.6. The distance was also changed to 0.3, 0.6, and 1 meters. The results are shown

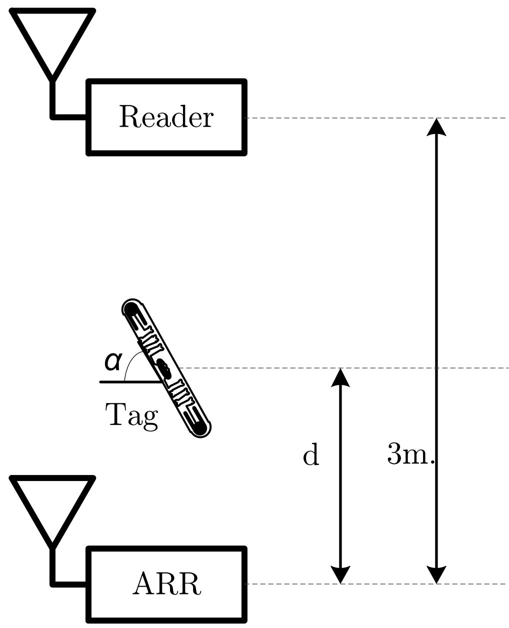


Figure 7.4: Orientation experiment setup

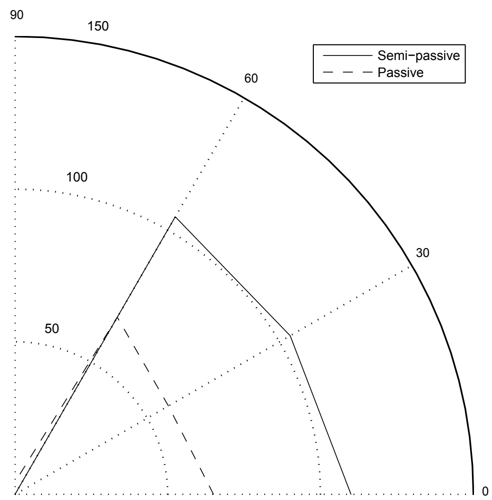
in Fig. 7.7.

Results show that the read rate scales down quickly when the tag is not perpendicular to the receiver. This is attributed to the patch antenna used for the receiver. The read rate results show a similar pattern to the radiation pattern of the antenna. An isotropic antenna could be used instead, but the gain offered by such antenna is in the order of 1.5dBi, and will decrease the maximum range of the receiver significantly.

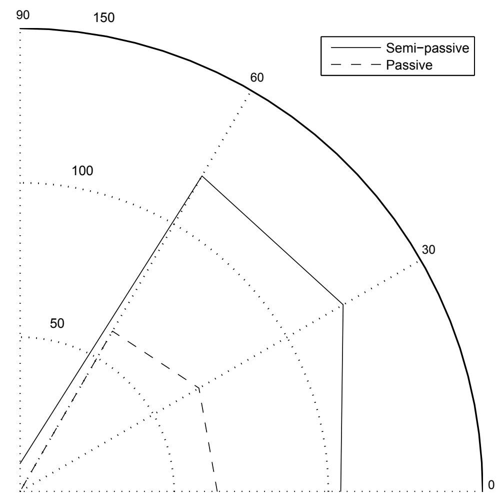
Using an isotropic antenna, the results for all the orientations were around 20 packets per minute for semi-passive tags. The maximum distance of reading was one meter. With a passive tag, the maximum distance the tag can be seen was approximately 40 cm and the read rate was poor with 2-3 packets. Since an isotropic antenna has a radiation pattern which closely resembles a circle, this is to be expected. The small gain of the antenna, which is in the order of 1.5dBi, makes for a poor read rate and most EPCs are not decoded correctly.

7.2.4 Reader power

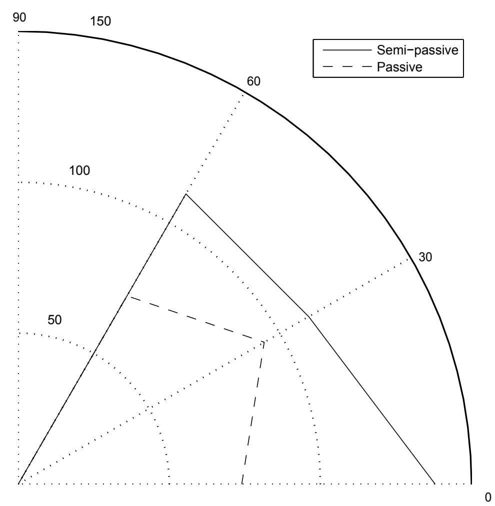
This experiment tests the relationship between the reader power and the receiver performance. The reader antenna was placed at a fixed distance of 5 meters and the reader output power was varied from 15dBm to 30dBm. A passive tag was placed in-between



(a) 0.3 meters



(b) 0.6 meters



(c) 1 meters

Figure 7.5: Read rate vs orientation

the reader and the receiver, which is one meter away from the receiver. The read rate of the receiver was recorded. Fig. 7.8 shows the results.

At the 22dBm mark, the performance decreases significantly. This is the threshold where the receiver does not receive enough power to its local oscillator to correctly decode the tag. Based on the Friis equation, the power at the LO port can be estimated to be -12dBm at this power and distance. Thus, theoretically, if the reader is located at a distance of 12.5 meters and is transmitting at full strength, the receiver will have enough power for its LO port.

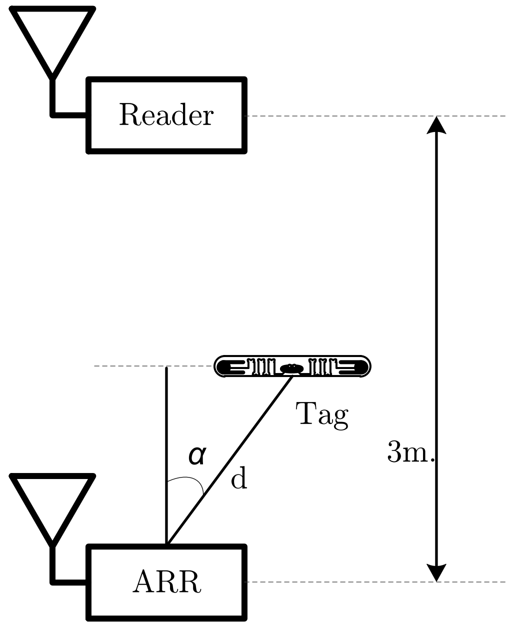


Figure 7.6: Orientation of tag to ARR experiment setup

7.3 Comparison to other receivers

This section compares the receivers outlined in Chapter 3. The comparisons are made based on values determined experimentally and obtained from literature. Comparisons are made between maximum distance and percentage of successful EPC decodes.

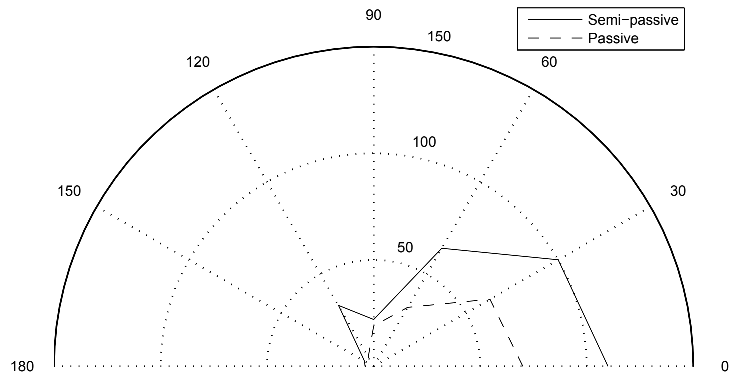
7.3.1 Tests

Table 7.1 presents a comparison of the maximum read ranges of the different receivers. The Sensatag and current thesis implementation were determined experimentally, while the Gen2 Listener value is based on [4].

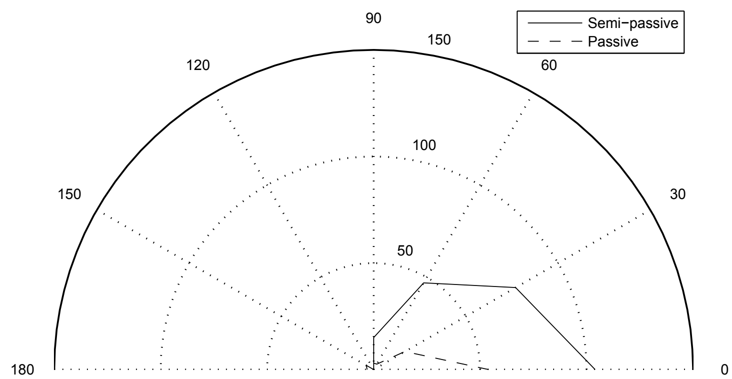
Tag type	Sensatag	Receiver	Gen2 Listener
Passive	0.6m	3.25m	*>12m*
Semi-passive	1.45m	5.5m	N/A

Table 7.1: Maximum read ranges

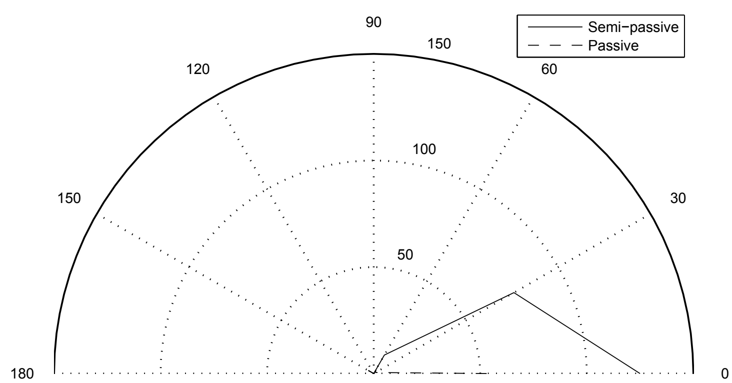
The values of the table are to be expected. The Sensatag, based on an envelope



(a) 0.3 meters



(b) 0.6 meters



(c) 1 meters

Figure 7.7: Read rate vs orientation to receiver

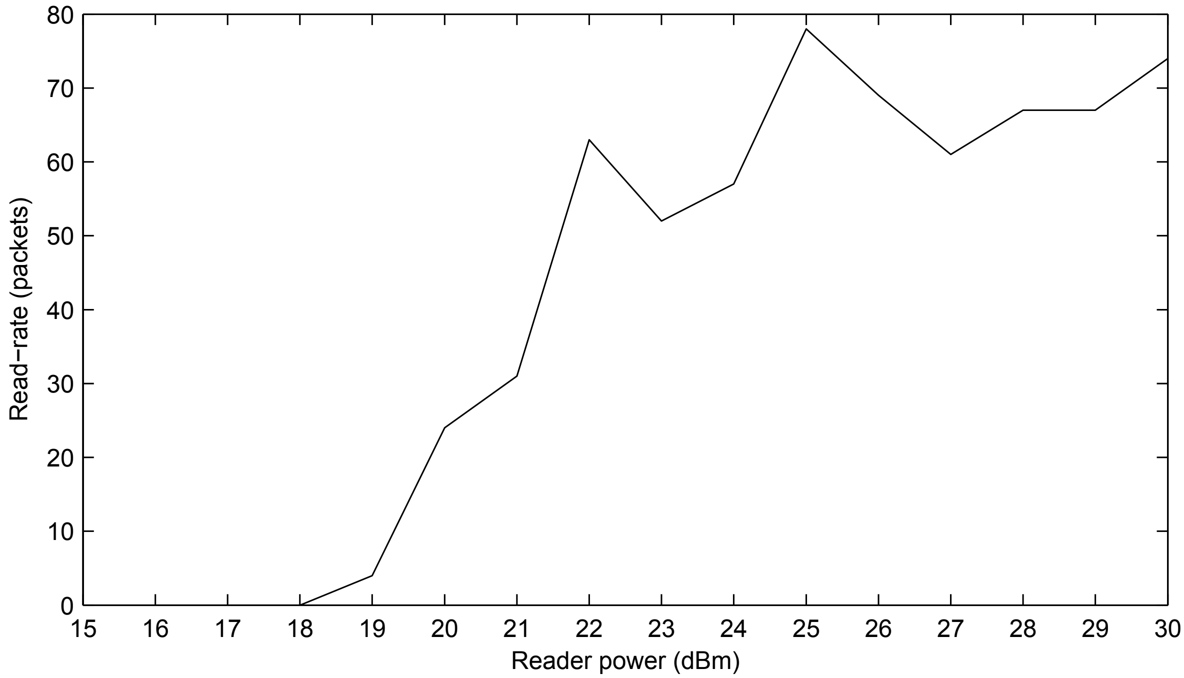


Figure 7.8: Reader power vs read rate

detector, provides the worst performance of the three. The Gen2 Listener, based on a SDR, provides the best performance. The thesis implementation shows results that fall in-between the Sensatag and Gen2 Listener. Table 7.2 compares the success rate at which the EPC packets were successfully decoded at a one meter distance. The results for the Gen2 Listener were taken from [17], while the receiver and Sensatag results were obtained experimentally. For the experimentally obtained results, a passive tag was placed one meter away from the receiver, and the tag antenna was placed five meters away from the receiver. The reader was programmed to send a *Query* every second for 60 seconds.

Tag type	Sensatag	Receiver	Gen2 Listener
Passive	17%	50%	70% [17]

Table 7.2: Percentage of successful decodes

7.3.2 Discussion

In general, the three implementations have the same advantages and issues as their respective architectures presented in Table 2.2. The Gen2 Listener offers the best performance in read range and read rate, but it has a limitation due to frequency hopping. The results presented were obtained with a reader transmitting at a fixed channel. The device was originally designed to operate in Europe, where UHF RFID has 2MHz allocated to it. In North America, the device is able to listen to only four channels at a time due to this limitation. EPC responses being sent from the other 46 channels will not be captured. Another limitation is the cost of the hardware. The USRP, on which the SDR is running on, costs around $1000, limiting wide scale deployment needed in cases such as for proximity localization.

The Sensatag is a low cost solution compared to the Gen2 Listener and the ARR. The device consists of mostly passive components, making it have low power consumption and can be run from batteries. The use of an envelope detection scheme limits its performance as can be seen from the tests. Another issue is the variable selectivity due to the architecture in use: in some channels the device will be able to decode EPCs, while in others it may not. The ARR offers better performance than the Sensatag, but worse than the Gen2 Listener. The advantage of it is that it overcomes the limitations of both approaches. The use of an industry UHF RFID reader IC as the RF section cuts down costs compared to the USRP, allowing it to be widely deployed for use in localization methods. Using synchronous detection deals with the frequency hopping issue and the limitation of the Gen2 Listener. An issue for the ARR is the Ethernet preparation time: EPCs could be discarded if the reader is sending Queries continuously. This problem can be corrected by implementing a counter for the EPCs and sending Ethernet packets at fixed intervals with the counter value, not in real-time, as soon as an EPC has been received, as it is done now.

Table 7.3 shows a comparison of the approaches. The criteria selected for the advantages and issues is based on specific applications in mind. For example, for localization approaches cost-effective receivers are preffered, since the techniques would require multiple of them to implement proximity or multilateration localization. For proximity localization, range performance is an important criteria. The ability to work in all frequency channels and bands is an important criteria as well.

Implementation	Advantages	Issues
Gen2 Listener	+Great performance	-2MHz bandwidth -High cost
Sensatag	+Low cost +Low power consumption	-Limited performance
ARR	+Good performance +Deals with Frequency hopping +Uses industry IC	-Discarded EPCs during Ethernet packet preparation

Table 7.3: Comparison of implementations

Chapter 8

Applications

8.1 Overview

This chapter presents applications where the augmented system can be used. First, implemented applications are described, then potential applications. The implemented applications include a portal and protocol analyzer. Potential applications include a EPC Gen2 sniffer, localization system, and Internet of Things sensor.

8.2 Portal

An RFID portal can be used to track people or packages passing through some area. For the ideal RFID portal system, the reader should achieve 100% read accuracy when tags pass through the confined area. The reader should not read them when they are not present in the confined area. The read accuracy performance is the most important factor for RFID portal systems.

Portals exhibit the problem of *cross-reads* — a tag that is outside of the confined area is read. Fig. 8.1 shows the cross-reading problem. *Tag 1* is passing through the portal, while *Tag 2* is outside the portal, but within the read range of the reader and is read by the portal.

To mitigate this issue, the reader transmit power could be lowered to shrink the effective read range. This presents a problem if a tag is placed inside a box or on a human body while passing through a portal. The tag might not receive enough power to energize itself in this case. Another potential solution would be to reduce the sensitivity of the reader. However, the same problem may occur where the reader might not be

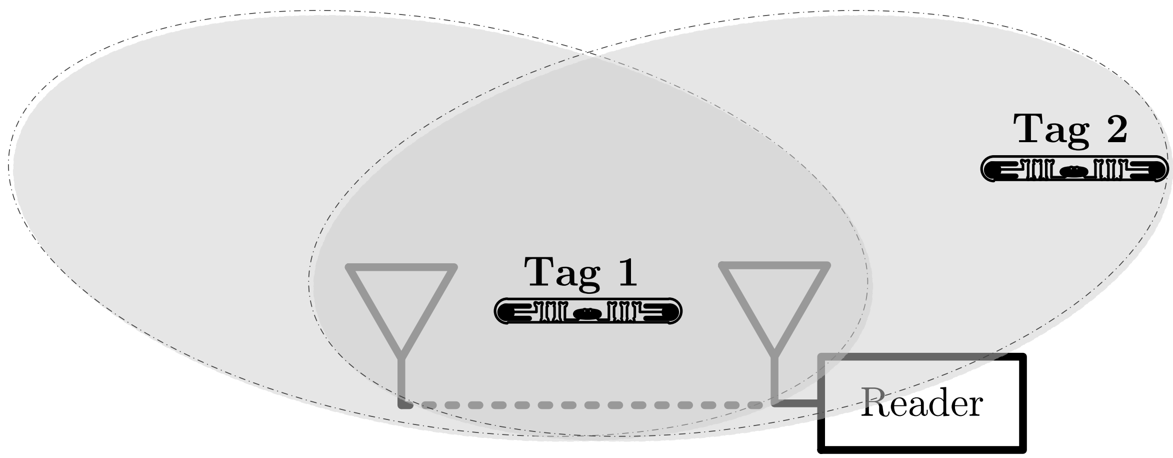


Figure 8.1: RFID portal cross-read problem

sensitive enough to pickup the tag signal. A third solution would be to use directed antennas. In such a case, the tag may be missed, since it spends little time inside the read range of such antenna. Filtering out tags which appear on both antennas also does not solve the problem, since the intersection of the radiation patterns of the two antennas is beyond the portal. The solution proposed in this thesis is to use the augmented RFID system to create a confined area, as illustrated in Fig. 8.2. By configuring the read range of the ARR through the registers, a confined zone can be created that is fully within the portal. As illustrated in the figure, the ARR would only see tags passing through the portal, in this case *Tag 1*, but not see *Tag 2*, which is seen by the reader antennas.

This application was implemented and tested. The receiver was configured for the maximum attenuation and used a 3dBi patch antenna. Passive and semi-passive tags were placed outside the portal, but within the read range of the antennas. A semi-passive tag was placed into the pocket of a person which went through the portal. The reader would see all three tags, but the receiver would see only the one in the pocket. Next, the tags outside the portal range were brought closer to the receiver until the receiver detected them. It was determined that the receiver would see the tags outside the confined portal area when they were within 30cm of the receiver. This is due to the antenna radiation pattern that has sidelobes on the sides and behind it. Using more directed antennas could solve this problem.

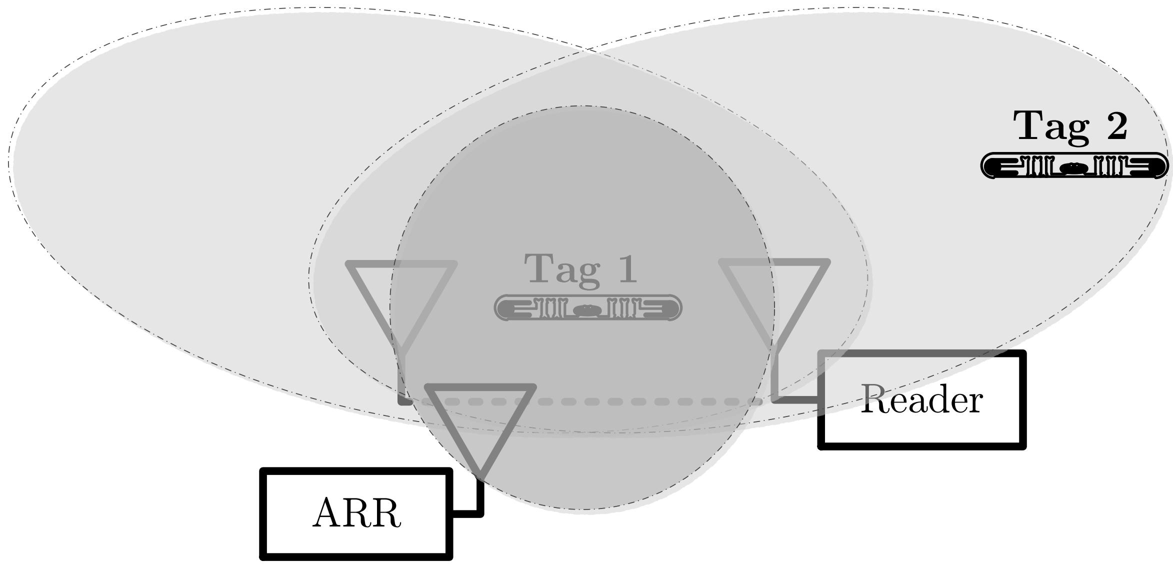


Figure 8.2: RFID portal with ARR

8.3 Protocol analyzer

EPC Gen 2 provides very basic security features for accessing tags' memory. The reader can send cover-coded data to the tag. In this case, the cover code is the RN16 response from the tag. The RN16 is then XORed with the reader-supplied password and sent out. Using the augmented RFID system, the weakness of such approach and how it can be circumvented is described below.

Fig. 8.3 shows the packet exchange when accessing restricted tag memory. The security revolves around the RN16 responded from the tag. The first *Req_RN* requests the tag for a handle, which is later attached to every command sent by the reader henceforth. Next, the reader requests another RN16 from the tag, the format is

$$\{RN16|CRC16\}.$$

This RN16 is then used to cypher the Access password within the *Access* command, the format of the command is

$$\{OPcode|Password \oplus RN16|handle|CRC16\}.$$

The *Access* command brings the tag into a secured state, from which *Read*/*Write* commands can be issued.

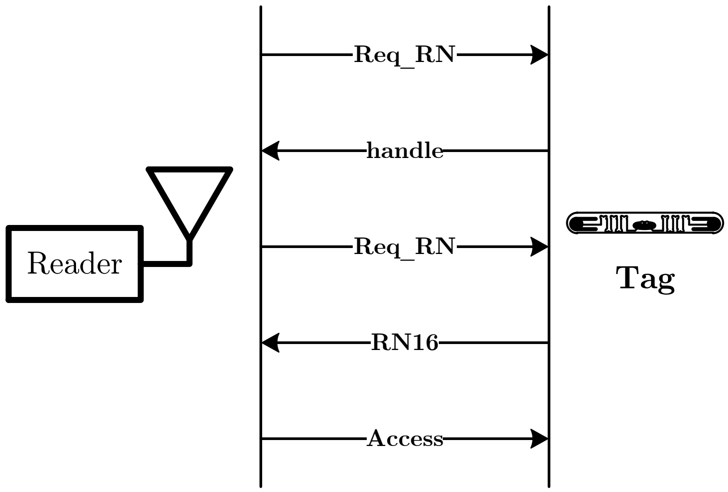


Figure 8.3: Security exchange in the EPC Gen 2 protocol

Using the ARR, this exchange can be intercepted which would compromise the security of the system. The cypher for the Access password is created by XORing the RN16 with the access password. This operation is reversible if the RN16 is captured, thus making the Access password visible and allowing unrestricted access to the tag memory.

The firmware on the FPGA was slightly modified to be able to capture the RN16. Referring to Fig. 6.9, the state EPC was changed to RN16. The response to the *Req_RN* command is RN16 and CRC16. The validity of the captured tag packet is checked by calculating the CRC16 of the RN16 and comparing it to the captured CRC16. The tag command decoder would be opened after receiving the reader *Req_RN* command.

Fig. 8.4 shows the analog signal of the captured reader *Req_RN* command. It includes the opcode for the command, the handle, and the CRC16. Fig. 8.5 shows the tag response to the command: beginning with the FM0 preamble, the RN16, 0x1ce8, is next, and finally the CRC16, 0xd8c8. The RN16 in this command is used for the cypher. Fig. 8.6 shows the correctly decoded RN16 and CRC16 packet underlined in Wireshark.

8.4 Potential applications

8.4.1 Localization system

A localization system can be implemented with the augmented RFID system using multiple ARRs, through proximity localization. The ARRs would have a fixed location and report tags that are in their proximity. Fig. 5.2 shows the approach. The ARRs, denoted

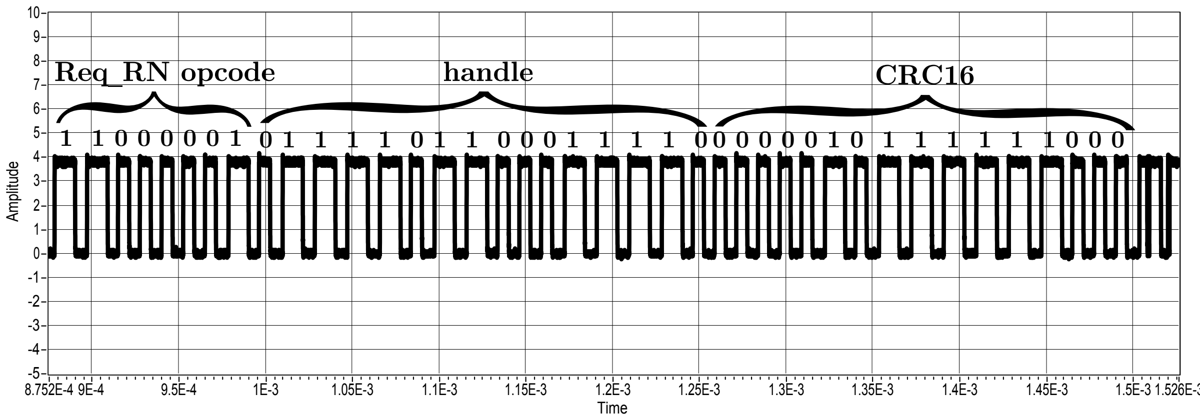


Figure 8.4: Captured Req_RN command

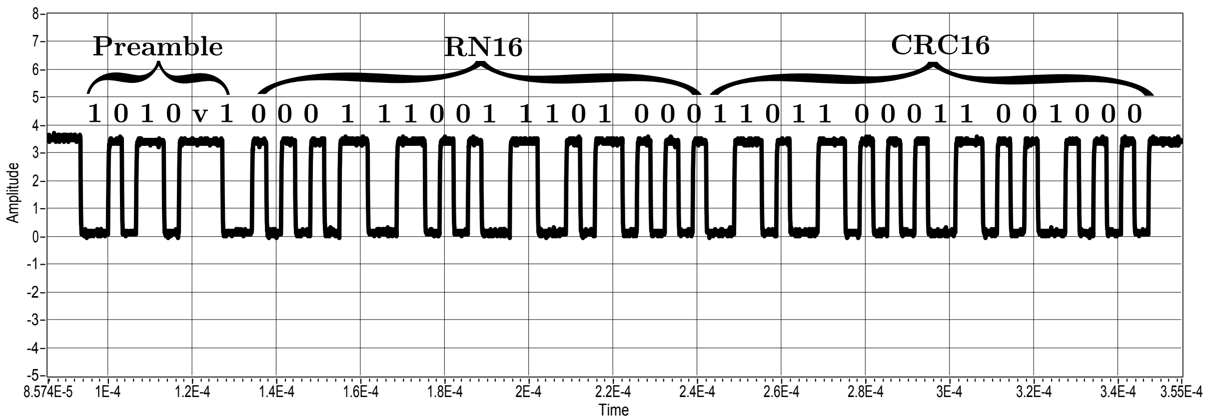


Figure 8.5: Captured RN16 command

```
0000  ff ff ff ff ff ff 00 10  dd ce 15 d4 08 00 45 00   ........ ......E.
0010  00 53 00 00 00 00 80 11  b8 6e c0 a8 00 75 c0 a8   .S...... .n...u..
0020  00 66 10 07 c3 50 00 3f  22 bd 52 4e 31 36 31 63   .f...P.? ".RN161c
0030  65 38 64 38 63 38 31 30  30 30 38 63 30 34 00 00   e8d8c810 008c04..
0040  d4 f0 10 01 04 6c 10 01  04 7c 00 00 00 00 00 00   .....l.. .|......
0050  00 7c 00 00 00 00 10 01  04 6c 00 01 b8 e1 10 00   .|...... .l......
0060  00 00 00 00                                        ....
```

Figure 8.6: RN16 Ethernet packet

R_n, have fixed and known locations. The circles around them denote their read ranges. Once a tag responds to a reader query, the ARR closest to the tag will pick up the signal. The ARR will then report to the host PC, with the tag EPC and its location data appended.

Other localization methods outlined in Chapter 2, besides proximity, can be improved using the augmented system. A radio map, based on the signal strengths seen by the multiple receivers would give a more precise set of measurement values. Triangulation from using multiple point of reference can also be improved. The improvements are based on the fact that multiple anchor points are created through the use of multiple receivers.

8.4.2 Internet of Things sensor

The Internet of Things refers to a concept of devices connected in an Internet-like structure and having unique identifiers [73]. The idea is at a conceptual stage, but there are implementations using various technologies. RFID is considered to be one of the potential technologies in the IoT. Services such as Cosm [74] have been created to facilitate the creation and adoption of IoT. Cosm is a hub for real-time sensor data. Devices send data to the hub, from which other devices can query the data or the data can be visualized.

RFID in the context of IoT has been used in creating an RFID ecosystem at a college campus [75]. Fixed readers provided location information for read tags. Using RFID readers alone provides a coarse-grained localization to the tags, i.e. localize to a building or room. With an augmented RFID system, fine-grained localization can be achieved.

A potential application is an IoT sensor. A localization system can be built with the techniques outlined in the previous section, with the added functionality that the ARRs report their data to a central hub, Cosm. Each ARR would have its own datastream, i.e. unique identifier in the Cosm service, with its exact coordinates. A stream of EPCs that pass through the given receiver can be shown in this datastream. Users can query this data from anywhere, visualize on it map environments, or process it.

Chapter 9

Conclusion

9.1 Concluding remarks

Conventional UHF RFID systems suffer from issues that limit the applications where RFID can be used. The issues are the lack of a well defined read zone, interference, and environment sensitivity. The thesis proposes an augmented system which can mitigate these problems through a new receiver device, called the Augmented RFID Receiver. The augmented RFID system is a system which is an improvement over the ubiquitous reader-tag system currently seen in UHF RFID systems. In this work, a conventional UHF RFID IC, in combination with an FPGA was used to create the receiver, which augmented the RFID system. The use of a conventional IC allows for a cost-effective way of implementing the system. The conventional IC is modified to use synchronous detection to overcome synchronization issues — frequency hopping and frequency offset.

The thesis compared this approach to two other similar implementations, the Sensatag and Gen2 Listener. The Augmented RFID Receiver offers good performance and low-cost due to the use of an industry UHF RFID reader IC and novel way of synchronizing with the reader. The ARR suffers from latency in Ethernet packet creation though, which causes some EPCs to be discarded. However, the receiver does overcome the limitations of the similar implementations, namely it deals with frequency hopping, allowing the receiver to capture EPCs in all channels. Quantitatively, the receiver achieved a read rate of 50% for a passive tag and 66% for a semi-passive tag that are placed one meter away. The maximum range, between the ARR and the tag with the reader located within 8 meters of the ARR, the receiver can decode EPCs properly is 3.25 meters for passive and 5.5 meters for semi-passive tags. Two applications were implemented to showcase the receiver: a protocol analyzer and an augmented portal.

9.2 Contributions

The thesis contributed the following:

- A survey of augmented approaches for UHF RFID systems.
- The design and implementation of a receiver for UHF RFID signals.
- A novel way to synchronize with UHF RFID readers through synchronous detection.
- An investigation of the performance of the system under various conditions.
- A demonstration of the augmented system as a protocol analyzer and a portal receiver.

9.3 Future Work

This work implements one mode of operation for UHF RFID systems, namely Hybrid mode. Various modes are used for different environments. Some modes have good noise immunity but slow speed, while others are the direct opposite. One possible extension is to implement all these modes supported by the EPC Gen 2 standard.

Another extension would be to improve the read rate of the receiver. This could be done by improving the DSP algorithms used, which currently uses oversampling in decoding the reader and tag encodings.

This work described the implementation of the platform of an augmented RFID system using only one receiver. To fully use the receiver-based localization approach, multiple receivers must be implemented. Algorithms must then be used for accurate localization of the tags.

The proximity approach presented in the thesis can be significantly improved by introducing RSS for the received EPCs. The hardware, the AS3992 chip, has the provisions for sensing the received signal strength of both the reader and the tag signal.

As seen in Chapter 7, the receiver relies on the reader's *Query* and *ACK* commands to receive the EPCs. If the reader is in a fading zone, then no EPCs can be captured, even though the receiver might not be in a fading zone itself. The EPC Gen 2 standard can be modified to be better suited for a receiver-based approach.

Chapter 4 introduced the problem of forward link limited tags. An extension of the ARR could be to add a transmitter front-end, which would boost the reader signal and thereby power up the tags. This would extend the range of passive tags.

References

[1] M. Bolić, D. Simplot-Ryl, and I. Stoymenović, *RFID Systems: Research Trends and Challenges*, Wiley, 2010.

[2] K. Finkenzeller, *RFID handbook*, Wiley, 2010.

[3] A. Athalye, V. Savić, M. Bolić, and P.M. Djurić, "A Radio Frequency Identification System for accurate indoor localization," *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1777–1780, May 2011.

[4] D. De Donno, F. Ricciato, L. Catarinucci, and L. Tarricone, "Design and applications of a Software-Defined listener for UHF RFID systems," in *2011 IEEE MTT-S International Microwave Symposium Digest (MTT)*, June 2011, pp. 1–4.

[5] A. Bensky, *Short-range wireless communication: fundamentals of RF system design and application*, vol. 1, Newnes, 2004.

[6] P. Vizmuller, *RF design guide: systems, circuits, and equations*, vol. 1, Artech House, 1995.

[7] Q. Gu, *RF System Design of Transceivers for Wireless Communications*, Springer-Verlag, 2005.

[8] P. Cruz, H. Gomes, and N. Carvalho, "Receiver Front-End Architectures Analysis and Evaluation," Available: `http://cdn.intechopen.com/pdfs/9961/InTech-Receiver_front_end_architectures_analysis_and_evaluation.pdf` [Mar. 30, 2012].

[9] J. Carr, *RF Components and Circuits*, Newnes, 2002.

[10] G. Kalivas, *Digital radio system design*, Wiley, 2009.

[11] M. Zou, V. Dvorkin, and J. Wong, "Quad Demodulators Arm Direct-Conversion Receivers," *Microwaves & RF*, vol. 43, no. 2, pp. 86–88, 2004.

[12] R. Svitek, "DC Offsets in Direct-Conversion Receivers: Characterization and Implications," *IEEE Microwave Magazine*, vol. 6, no. 3, pp. 76–86, 2005.

[13] B. Razavi, "Design considerations for direct-conversion receivers," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal*, vol. 44, no. 6, pp. 428–435, 1997.

[14] L. Besser and R. Gilmore, *Practical RF circuit design for modern wireless systems: Passive circuits and systems*, vol. 2, Artech House, 2003.

[15] J. Love, *RF front-end: world class designs*, Newnes, 2009.

[16] T. Hentschel and G. Fettweis, "Software radio receivers," *CDMA techniques for third generation mobile systems*, vol. 487, pp. 257–283, 1999.

[17] D. De Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: towards distributed RFID sensing with software-defined radio," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, 2010, pp. 97–104.

[18] S. Miles, *RFID technology and applications*, Cambridge University Press, 2006.

[19] Motorolla, "Baggage Tracking RFID Solutions," Available: `http://www.novacommunications.com/images/productpdfs/Baggage_Tracking_RFID_Solutions.pdf` [Mar. 12, 2012], 2006.

[20] M. Bolic, A. Borisenko, and P. Seguin, "Automating Evidence Collection at the Crime Scene using RFID Technology for CBRNE Events," to be published in Forensic Science Policy & Management: An International Journal.

[21] AVID, "American Veterinary Identification Devices," Internet: `http://www.avidid.com/` [Mar. 20, 2012].

[22] OpenBeacon, "OpenBeacon Active RFID Project," Internet: `http://www.openbeacon.org/` [April 1, 2012], 2012.

[23] Alien Technology, "RFID vehicle tracking," Available: `http://www.alientechnology.com/docs/CS_STS.pdf` [Mar. 5, 2012].

[24] T. Blecker and G. Huang, *RFID in Operations and Supply Chain Management*, Erich Schmidt Verlag, 2008.

[25] PowerID, "PowerP RFID Tags for People Tracking PowerP Specifications," Available: http://www.power-id.com/Data/pdf/PowerP_0311.pdf [May 1, 2012].

[26] R. Want and D. Russell, "Ubiquitous Electronic Tagging," *IEEE Concurrency*, pp. 1–6, July 2000.

[27] EPCGlobal, "Specification for RFID Air Interface EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz," Available: http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf [Mar. 1, 2012].

[28] EPCGlobal, "EPCglobal Standards Overview," Available: http://www.gs1.org/gsmp/kc/epcglobal [Mar. 1, 2012].

[29] G. Benthien, "Digital Encoding And Decoding," Available: http://gbenthien.net/encoding.pdf [Mar. 5, 2012].

[30] D. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, Newnes, 2007.

[31] D. Mccarthy, "Understand RFID , Part 1 : Technology," Available: http://www.eetindia.co.in/STATIC/PDF/200905/EEIOL_2009MAY04_RFD_TA_01.pdf?SOURCES=DOWNLOAD [Mar. 10, 2012].

[32] Y. Chen and F. Zhang, "Study on Anti-collision Q Algorithm for UHF RFID," in *Proceedings of the 2010 International Conference on Communications and Mobile Computing*, 2010, vol. 3, pp. 168–170.

[33] EPCGlobal, "Low Level Reader Protocol," Available: http://www.gs1.org/gsmp/kc/epcglobal/llrp/llrp_1_1-standard-20101013.pdf [Mar. 8, 2010].

[34] A. Vries and P. Dietrich, "Standards facilitate RFID adoption," Available: http://rfdesign.com/mag/709RFDEf1.pdf [April 4, 2012].

[35] M. Zhu, *Positioning Algorithms for RFID-Based Multi-Sensor Indoor / Outdoor Positioning Techniques*, Ph.D. thesis, RMIT University, 2011.

[36] C. Angerer, M. Holzer, B. Knerr, and M. Rupp, "A flexible dual frequency testbed for RFID," in *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*, 2008.

[37] N. Roy, A. Trivedi, and J. Wong, "Designing an FPGA-based RFID reader," *XCell Journal*, vol. 2, 2006.

[38] M. Buettner, "A flexible software radio transceiver for UHF RFID experimentation," Available: `ftp://ftp.cs.washington.edu/tr/2009/10/UW-CSE-09-10-02.PDF` [Mar. 15, 2012].

[39] A.P. Sample, D.J. Yeager, P.S. Powledge, A.V. Mamishev, and J.R. Smith, "Design of an RFID-based battery-free programmable sensing platform," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 11, pp. 2608–2615, 2008.

[40] M. Buettner, R. Prasad, A. Sample, D. Yeager, B. Greenstein, J.R. Smith, and D. Wetherall, "RFID Sensor Networks with the Intel WISP," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, 2008, pp. 393–394.

[41] T. Li, A. Borisenko, and M. Bolic, "Open Platform Semi-passive RFID tag," to be published in Ad Hoc Now 2012, 2012.

[42] L. Chen, S. Zhang, Z. Wang, and L. Li, "A New Simulation Platform for UHF RFID Tag Development," in *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*. Sept. 2011, pp. 1–3, Ieee.

[43] M. Feldhofer, M. Aigner, T. Baier, M. Hutter, T. Plos, and E. Wenger, "Semi-passive RFID development platform for implementing and attacking security tags," in *2010 International Conference for Internet Technology and Secured Transactions (ICITST)*, 2010, pp. 1–6.

[44] Wireshark Foundation, "WireShark," Internet: `http://www.wireshark.org/` [May 2, 2012].

[45] Frontline Test Equipment, "FTS4BT Bluetooth Protocol Analyzer & Packet Sniffer," Internet: `http://www.fte.com/products/fts4bt.aspx` [May 2, 2012].

[46] Fluke Corporation, "AirMagnet," Internet: `http://www.flukenetworks.com/enterprise-network/wlan-security-and-analysis` [May 2, 2012].

[47] CISC, "RFID MeETS," Internet: https://www.cisc.at/?id=23 [May 1, 2012].

[48] RFID Journal, "CISC Launches RFID Tag Evaluation System," Available: http://www.rfidjournal.com/article/view/6792 [May 3, 2012].

[49] L. Catarinucci, D. De Donno, M. Guadalupi, F. Ricciato, and L. Tarricone, "Performance analysis of passive UHF RFID tags with GNU-radio," in *2011 IEEE International Symposium on Antennas and Propagation (APSURSI)*, 2011, pp. 541–544.

[50] J.S. Park, J.W. Jung, S.Y. Ahn, H.H. Roh, H.R. Oh, Y.R. Seong, Y.D. Lee, and K. Choi, "Extending the Interrogation Range of a Passive UHF RFID System With an External Continuous Wave Transmitter," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 8, pp. 2191–2197, 2010.

[51] N. Kenarangui, *Real Time Location Tool for Precision Tracking of Passive UHF RFID Tags in Two Dimensions*, Ph.D. thesis, University of Texas, 2010.

[52] G. Narayanaswamy, *Blocking Reader: Design and implementation of a low-cost passive UHF RFID Blocking Reader*, Ph.D. thesis, University of Texas, 2010.

[53] H.Y. Chen, A. Bhadkamkar, and D.W. van der Weide, "Piggyback modulation for UHF RFID sensors," in *2010 IEEE MTT-S International Microwave Symposium Digest (MTT)*, 2010, pp. 1776–1779.

[54] M. Bolić, A. Athalye, and T.H. Li, "Performance of passive UHF RFID systems in practice," *RFID Systems: Research Trends and Challenges*, 2010.

[55] FCC, "CFR Title 47 Part 18," Available: http://www.gpo.gov/fdsys/pkg/CFR-2003-title47-vol1/pdf/CFR-2003-title47-vol1.pdf [Mar. 3, 2012].

[56] Impinj, "Monza 5 Tag Chip Datasheet," Available: www.impinj.com/Documents/Tag_Chips/Monza_5_Datasheet/ [Mar 30, 2012], 2012.

[57] Alien Technology, "Higgs 4 EPC Class 1 Gen 2 RFID Tag IC," Available: http://www.alientechnology.com/docs/products/Alien-Technology-Higgs-4-EPC-Class-1-Gen-2-RFID-Tag-IC.pdf [Mar 15, 2012].

[58] Impinj, "Indy R2000 Reader Chip (IPJ-P200) Electrical , Mechanical , & Thermal Specification," Available: http://www.impinj.com/Documents/Reader_Chips/Indy_R2000_Datasheet/ [Mar. 30, 2012].

[59] Intelleflex, "The Intelleflex XC3 Technology Platform," Available: http://www.intelleflex.com/downloads/white-papers/Intelleflex-XC3-ISO-C3-White-Paper.pdf [May 2, 2012].

[60] T. Li and M. Bolić, "Performance of passive and semi-passive UHF RFID systems," in *CCECE 2010*, 2010.

[61] D.R. Novotny, J.R. Guerrieri, and D.G. Kuester, "Potential interference issues between FCC part 15 compliant UHF ISM emitters and equipment passing standard immunity testing requirements," *IEEE International Symposium on Electromagnetic Compatibility*, pp. 161–165, 2009.

[62] T. Sanpechuda and L. Kovavisaruch, "A review of RFID localization: Applications and techniques," *ECTI-CON 2008, 5th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, vol. 2, pp. 769–772, 2008.

[63] Texas Instruments, "CC1100: Low-Cost Low-Power Sub-1GHz RF Transceiver," Available: http://www.ti.com/lit/ds/symlink/cc1100.pdf [Apr. 10, 2012].

[64] HopeRF, "RFM22 ISM Transceiver module," Available: http://www.sparkfun.com/datasheets/Wireless/General/RFM22.PDF [May 2, 2012].

[65] GS1, "Regulatory status for using RFID in the UHF spectrum," Available: http://www.gs1.org/docs/epcglobal/UHF_Regulations.pdf [May 3, 2012].

[66] X. Zhang and M. Tentzeris, "Applications of Fast-Moving RFID Tags in High-speed Railway Systems," *International Journal of Engineering Business Management*, vol. 3, 2011.

[67] Austria Microsystems, "AS3992 Datasheet," Available: http://www.es.co.th/schemetic/pdf/AS3992.pdf [May 1, 2012].

[68] N. Bautista, "Enhanced FM0 decoder for UHF passive RFID readers using duty cycle estimations," in *2011 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, 2011, pp. 306–312.

[69] S. Rhoads, "Plasma - most MIPS I(TM) opcodes :: Overview," Internet: http://opencores.org/project,plasma [May 2, 2012].

[70] Alien Technology, "Higgs-3," Available: http://www.alientechnology.com/docs/products/Alien-Technology-Higgs-3-ALC-360.pdf [May 2, 2012].

[71] PowerID, "PowerP RFID Labels for People," Internet: http://www.power-id.com/Products/PowerP.aspx [May 2, 2012].

[72] Intelleflex, "Comparison of Intelleflex Semi-passive BAP, Active, and Passive RFID," Available: http://www.intelleflex.com/Products.Semi-Passive-vs-Active-RFID.asp [May 1, 2012].

[73] IoT-A, "Internet of Things Architecture," Internet: http://www.iot-a.eu/public/front-page[May 1, 2012].

[74] Cosm, "cosm - Connect to your world," Internet: http://cosm.com [May 1, 2012].

[75] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using RFID: the RFID ecosystem experience," *IEEE Internet Computing*, vol. 13, no. 3, pp. 48–55, 2009.