Deanship of Graduate Studies

Al-Quds University

Development of A Software-Defined Radio Testbed for RFID Generation-2 Reader

Mohran Nidal Fuad Jazi

M.Sc Thesis

Jerusalem-Palestine

1436-2015

Development of A Software-Defined Radio Testbed for RFID Generation-2 Reader

Prepared By:

Mohran Nidal Fuad Jazi

B.Sc.: Electronic Engineering, 2011, Palestine

AL-Quds University, Palestine

Supervisor: Dr. Samer Bali

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Electronic and Computer Engineering/ Faculty of Engineering/ Graduate Studies

Jerusalem-Palestine

1436-2015

Al-Quds University

Deanship of Graduate Studies

Master of Electronics and Computer Engineering

Thesis Approval

Development of A Software-Defined Radio Testbed for RFID Generation-2 Reader

Prepared By: Mohran Nidal Fuad Jazi

Registration No: 21120131

Supervisor: Dr. Samer Bali

Master thesis submitted and accepted, Date: .....

The name and signatures of examining committee members are as follows:

1- Head of committee	Dr.Samer Bali	Signature: .....
2- Internal Examiner	Dr. Ali Jamoos	Signature: .....
3- External Examiner	Dr. FYHD TUMHR	Signature: .....

Jerusalem-Palestine

1436-2015

Declaration:

I certify that this thesis submitted for the degree of Master, is the result of my own research, except where otherwise acknowledged, and that this study (or any part of the same) has not been submitted for a higher degree to any other university or institution.

Signed: ……

Mohran Nidal Fuad Jazi

Date: …….

Dedication

To my loving parents, brother, sister for the sacrifices they had to make in life for me; and all my admirable doctors for their priceless knowledge, grateful support and patience.

Acknowledgments

Above all, Praise and thanks are due to Allah for his mercy, blessing and taking care of us every step of the way towards success. I would like to express my sincere gratitude and heartfelt thanks to my supervisor, Dr. Samer Bali. I'm greatly indebted to his assistance, guidance support, and his logical way of thinking have been of great value to me. Their valuable advice and constructive comments have been of great value throughout the development of this research.

I would like to extend my gratitude to professor Thomas Kaiser for his dedicated support, encouragement, supervision, and suggestions through my research at Duisburg-Essen University. I extend my thanks to Eng. Marc Hoffmann for his support. Also, I extend my gratitude to DAAD for their financial support through PalestineCD project.

I gratefully acknowledge the support and generosity of the Duisburg-Essen University, without which the present study could not have been completed. Really, this chance was invaluable.

Special thanks to Dr. Hanna Abdel Nour, Dr. Ali Jamoos and Dr. Labib Arafeh for their moral support, comments and encouragement.

I am very grateful to my dear parents and my friends whom I consider as my brothers. Thank you all for being always there when I needed you most. Thank you for believing in me and supporting me. I believe that without your support and your prayers, none of this work would be accomplished.

I sincerely feel that only Allah can reward all the good people mentioned above.

Finally, I hope this thesis be a useful addition to the research work.

Abstract

Radio-Frequency Identification (RFID) wireless technology is becoming the most popular and important instrument that is used in many applications such as logistic chains, tracking and localization items. RFID has the capability to read the items without need line of sight. In addition, RFID is used for applications that require relatively long distance compared to the traditional barcode system. As well as, RFID tags can be reprogrammable and their cost is very low.

As RFID technology continues to grow rapidly, different issues and challenges are arisen. One important challenge is that the researchers in this field find that the existing commercial RFID readers look like a black box that suffer from limited configuration, and thus, modifications to MAC or PHY layer parameters are not possible.

In this thesis, a new implementation of an RFID reader Testbed based on EPC Generation-2 standard is presented. This implementation is done on the new generation of Universal Software Radio Peripheral (USRP N210) platform which is programmed using Software Defined Radio (SDR) built on GNU Radio framework. In addition, the performance credibility of the implemented reader working in Ultra-High Frequency (UHF) is tested for reading commercial tags. It is found that the performance of the implemented reader is as good as the performance of commercial UHF RFID readers in the reading range coverage. Therefore, our reader can be used in the research community for research work. We perform two research experiments to show the configuration flexibility of our reader Testbed. In the first experiment, we use our reader and commercial tags to study the impact of capture effect which

increases the performance of our reader in the collision case works with high percentage up to the reading range of our reader which is 6 m. In the second experiment, the performance of Dynamic Framed Slotted ALOHA (DFSA) algorithm is investigated. DFSA is used to solve the collision issue when many tags respond simultaneously to the reader. In addition, we determined the best value of the parameter C for our system which is equal 0.3 based on DFSA algorithm.

Keywords: EPC Gen2 Protocol, Radio-Frequency Identification (RFID), Software Define Radio (SDR), Reader, tag, USRP, GNU-Radio, Dynamic Frame Slotted ALOHA, Testbed.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

Radio Frequency Identification (RFID) is a wireless technology that allows small, cheap chips, remote sensing interrogation and other identifying information. In addition, RFID is used to manage, and track the tagged objects. RFID is similar to barcode identification, but it has more additional features, such as non-line of sight, greater coverage range, reprogrammable, and the capability of scanning multiple objects at the same time. The main components of a traditional RFID system are reader and tag [1]. The reader has two antennas one for transmitter and one for receiver, whereas the tag contains of integrated circuit(IC), memory, and antenna. Each tag has a unique identification number, moreover, the reader and tags communicate with each other through the electromagnetic waves.

Although there are many types of RFID systems, the latest developments in RFID technology have focused on passive Ultra High Frequency (UHF) RFID and it is standardized by EPC class-1 Gen-2 protocol [2]. This protocol defines the communication between the reader and passive tags with a carrier wave in the band 860-960 MHz. These passive tags do not have any energy source, which makes them reusable and inexpensive to produce. The reader sends the carrier wave, which is modulated by the tag and backscattered again to the reader [3, 4].

Nowadays, the application for UHF RFID is growing rapidly, and the need to do research based on real-time experiment is becoming more and more important. For example, there is a growing interest in the reliability and performance of RFID readers in the supply chain for detection, localization and tracking. However, there is a little published work on RFID performance in these definitions [4, 5]. Therefore, a real time testbed is needed.

1.2 Problem Statement

The lack of experimental low-level RFID systems is the result of the current lack of tools available to researchers. On one hand, conventional RFID readers are considered as black box systems that provide limited software configuration. As a result, they do not provide the flexibility to apply modifications to the MAC or PHY layer behaviour. This makes the study or the enhancement of the existing protocols very difficult. On the other hand, there are several test-beds and measurement equipment's that are commercially available and dedicated for RFID. However, their cost is high and also most of these equipment's are closed source. Therefore, the researchers in RFID field need a powerful research testbed for a reader in order to perform their research experiments.

1.3 Contribution

In this thesis we present a platform for UHF RFID testbed to read the commercial tags and give users a complete control of the MAC and the PHY layers based on the new generation of USRP N210 and the EPCglobal Class-1 Generation-2. An experimental study was performed to measure our RFID reader testbed performance using the EPCglobal Class-1 Generation-2, and it is found that its performance is as good as the performance of commercial UHF RFID readers. We use our reader to study the impact of capture effect.

Also, we use this testbed to introduce a comprehensive study and implementation for Dynamic Framed Slotted Aloha (DFSA) anti-collision algorithm.

1.4 Related Work

In this section we review the state of the art on RFID Gen2 reader and some related issues based on EPCglobal Class-1 Generation-2 protocol such as Dynamic Framed Slotted Aloha (DFSA) implementation. The literature on this topic is fairly restricted. The first implementation for Ultra High Frequency (UHF) Gen2 reader that enables PHY/MAC designs to be prototyped and evaluated was proposed by Buettner and Wetherall in [5, 10]. However, this implementation is based on the old generation of USRP (called USRP1) and was dedicated to GNU Radio (V3.3.0). A Gen2 RFID monitor based on USRP2 which is capturing the commercial reader transmissions in real time was introduced in [11]. Figure1.1 shows the monitor system, the USRP2 captures the reader transmissions. Furthermore, the digitized signal streamed over the PC through the GigE cable to be decoded.

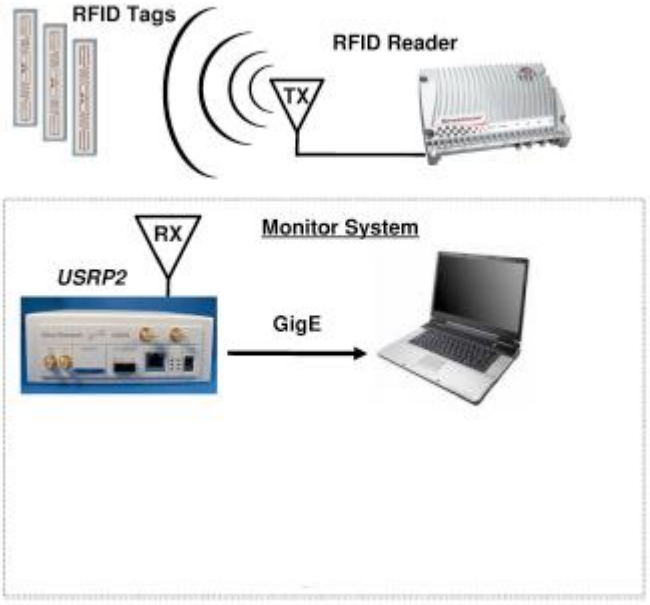

Figure 1.1: Monitor System Diagram [11].

In [12] an RFID distributed system was used to listen to the commercial reader transmissions (called RFID listener) based on USRP1. In addition, the author was investigated the cooperative reception techniques like combining and interference cancellation. A High frequency (HF) multiplexer for multiple antennas based on USRP1 was investigated in [3] to enhance the reading range. The multiplexer can be used on the transmitter and the receiver side. It can include four antennas or less. Also the reading range for multiplexer significantly decreased by the noise and interference after two meters. The reading range without multiplexer reached about six meters. The basic principle of the reader was used with some modifications in [13] to analyze the performance of the passive UHF RFID tags based on Software Defined Radio (SDR) that allows flexibility to check the tag performance for any operating frequency. Moreover, they presented methodology to measure tag sensitivity, Signal to Noise Ratio (SNR), and numerical results for five different tags. RFID listener was proposed in [14] based on a Software-Defined Radio (SDR), which receives only the decoded signal between RFID reader and the interrogated tag and tests different timing clock recovery schemes for the tag signal reception. All implementations are based on older GNU Radio versions and the USRP1 except the RFID monitor.

An implementation for Gen2 RFID reader and a newly design software define radio for a tag was presented in [15]. The authors used two USRP1 devices: one for a reader and for a tag. However, the code was not available online for reference. In [16] Zheng et al. modified the source code presented in [10] to be compatible with USRP N210, but this implementation worked only with the non-commercial wireless sensing platform (WISP) tags, i.e., it is not compatible with commercial Gen2 UHF RFID tags. As well as, the author named it Open RFID Lab (ORL) [17]. The effect of different clock recovery

strategies introduced in [18] based on USRP N210. However, reading performance was not investigated in this study and the source code is not available as an open source for reference. For the lake of literature review, only selected publications are included. To the best of our knowledge, there is no complete implementation for an RFID reader based on the current generation of USRP N210 and EPC gen2 UHF standard to read the commercial tags.

Nevertheless, RFID also presents technical issues, one of which is a multiple collision tags. Also, when the number of RFID tags in the work range of the reader increase, tag collision problem becomes more considerable. Because of the collision signals between multiple tags, some tags would not be recognized if no anti-collision algorithm presented.

In this thesis we studied the anti-collision problems for EPCglobal Class-1 Generation-2, specified for passive UHF RFID system. In this case, we only take Aloha-based schemes into consideration that are chosen by the EPCglobal Class-1 Generation-2 protocol.

ALOHA protocol is used in the data-link layer for local area networks with broadcasting topology. Additionally, ALOHA networks were developed at the University of Hawaii to create a wireless communication network in 1970s by Norm Abramson, but due to its simpleness, and with some modifications ALOHA are used for passive RFID system MAC Mechanisms. The RFID systems use Dynamic Framed Slotted Aloha (DFSA) anti-collision protocol, as upgraded version of pure ALOHA. Whereas, the Mechanism of Pure ALOHA was simple for station to send the data, as soon as request is received, but it reduces the throughput if more than one stations transmit at the same time, while medium is occupied [19, 20]. To enhance the throughput Slotted ALOHA protocol [21] was developed, where the time is divided into equal size intervals known as slots and the transmission time of the data is equal to the slot size. Each station can transmit its data at

the beginning of the next available time. While, the throughput was still not good enough as it is not possible to predict the number of slots that needed to all stations to transmit their data. In addition, there are no mechanisms to control the collision, which mean the numbers of collision cases increased. In [22] Framed Slotted ALOHA was developed to increase the throughput and solve the collision problems. In this mechanism, we sent through each transmission a frame that included a number of time slots. Furthermore, to make it more efficient, frame length should be adaptive (DFSA) as introduced in [23]. In DFSA the reader sends a parameter Q that includes the number of time slots through the Query command, which tags receive and set up their counters as a random value from 0 to $(2^{Q} - 1)$, the tag that chooses the slot number zero sends its information back to the reader. As slot number of each tag is independently chosen, the collision happens inevitability. As well as, the problem with anti-collision is to estimate the number of the tags in the population and increase the throughput of RFID system.

Estimation of tags, which needs retransmission was introduced in [24]. Vogt's was investigated An estimation procedure that estimates the number of tags as a minimum error between the observed value, including number of empty slots, collided slots, successful slots, and their expected value pairs. To decrease system complexity, available frame length were limited to powers of two, which according to [25, 26] lowers the system throughput to 35%. Furthermore, the maximum throughput can obtain when the frame size equal to the number of the tags. A threshold 1.15 is defined in [27, 28], so retransmission is necessary if estimated number of tags greater than 1.15 times that the number of tags in the previous frame. The distribution of tags in the frame based on multinomial distribution, where the probability of slot occupancy is calculated from binomial distribution was described in [29]. Author in [25, 30] was recognized the last z frames. In addition, the probability distribution was updated, so distribution of tags is estimated accordingly. Liu et

al. in [31], used a different slot time duration, which increased the system efficiency, but the system was lacked from any tag estimation technique. All introduced algorithms entering into probability distribution, and tags estimation techniques.

EPCglobal Class-1 Generation-2 presented DFSA based on Q-algorithm to solve the collision problem [2]. We noticed that, none of the presented works evaluate the performance and enhancement of DFSA based on Gen2 RFID reader and the new generation of USRP N210.

1.5 Methodology

In the research community Software-Defined Radio (SDR) has recently become realized in many RF applications. Furthermore, it is chosen to implement and evaluate improvements on the reader side. The SDR allows the computer to handle many of the signals processing within the software, whereas this was handled by hardware components. This transition leads to several benefits, for instance the SDR is able to be more reconfigurable, flexible, and upgradable and more cost efficient when compared to hardware based radio.

In this thesis, we achieve our goal as following:

1. A Universal Software Radio Peripheral (USRP N210) made by Ettus Research [7] and host computer are used to build the hardware part of our SDR system.
2. The host computer can manage the USRP N210 through the use a compatible software package called GNU Radio [6] which is provided all the signal processing runtime to implement software radios under Linux operating system.
3. GNU Radio is interfaced with the USRP N210 to create our Software Defined Radio (SDR) system.

1.6 Organization of Thesis

The rest of the thesis is organized as follows. In chapter two, we present an RFID overview and discriminates the different types. In addition, the EPC Class-1 Generation-2 is described as well as clarifying RFID communication concepts. In chapter three, we explain the platform considerations, for choosing the used hardware. Furthermore, we introduce the USRP hardware, the GNU Radio software and capabilities. In chapter four, the experiment results of the implemented reader, is presented in terms of a discussion. Finally, conclusions and future work are drawn in chapter 5.

Chapter 2

Radio Frequency Identification System

2.1 Overview

Several decades ago, Radio Frequency Identification (RFID) came to existence. Furthermore, it replaces the traditional barcode system gradually. RFID is used in many different applications, such as secure entry cards, animal identification, supply chain to manage the flow items [32] and automatic identification systems.

The main components of an RFID system are RFID readers, RFID tags, and middleware. RFID tags and readers exchange data through radio waves. The data that is stored in the tag has an identification number to recognize the items. The reader starts to send the carrier wave to RFID tags and when the tags receive this carrier wave begin to broadcast their data to the reader. Additionally, the reader gathers the tag data details and sends it to a host computer, which stores to be processing and uses it in an application programs, such as programs contain an inventory system, repository management system, or a database. There are three different types of RFID technologies which are: active, passive, and semi-passive. Nonetheless, Passive RFID technology is most often used compared to active RFID technology due to certain problems, such as cost, size, longevity, etc.

In section 2.2, we introduce the frequencies and wavelength for RFID systems. In addition, four types of RFID frequency bands are introduced. The RFID system components and

applications are presented in sections 2.3 and 2.4, respectively. In section 2.5, different RFID standards are investigated. The EPC Class-1 Generation-2 protocol specifications are described in section 2.6. Finally, the RFID anti-Collision protocols are discussed in section 2.7.

2.2 Frequency Bands

RFID systems work on different frequencies depending on the type of the application. Moreover, the frequency and wavelength are the major factor of radio wave. A higher frequency corresponds to a shooter wavelength, and a lower frequency corresponds to a longer wavelength. There are four classes of frequencies used in RFID system: Low Frequency (LF), High Frequency (HF), Ultra High Frequency (UHF), and Microwave Frequency. The frequency bands used by RFID systems and their wavelengths are outlined in Table 2.1.

Table 2.1: Frequency bands and their wavelengths used by RFID systems [32].

Frequency Band	Frequency Range	Wavelength
Low Frequency	9-135 kHz	2300m
High Frequency	13.553-15.567 MHz	22m
Ultra High Frequency	860-960 MHz	33cm
Microwave Frequency	2.4-2.4358 and 5.8 GHz	12cm

2.2.1 Low Frequency RFID System

As indicated in Table 2.1, the low frequency range is 9-135 kHz. Low frequency RFID systems use a frequency range of 125–134 kHz. In addition, low frequency communications are managed by the International Organization for Standardization (ISO) specification 18000-2. Moreover, the oldest RFID systems are the low frequency systems. Radio waves in these systems are able to passing through the opaque materials. The tags that operate in the low frequency have a read range approximately 0.5 meter and they are mainly used for animal tagging, and access control [32].

2.2.2 High Frequency RFID System

As mentioned in Table 2.1, the range for the high frequency is 13.553–15.567 MHz. As well as, high frequency communications are managed by ISO/IEC (International Electrotechnical Commission) specification 18000-3. The Tags that used by the high frequency are less expensive than the low frequency tags. The High Frequency FRID systems are used in many applications such as smart cards, luggage control and libraries. Nowadays, DHL shipping company was implemented an item-level tagging using 13.56MHz tags and they shipped more than one billion packages each year [32].

2.2.3 Ultra High Frequency RFID System

The range for ultra-high frequency is 860–960 MHz. Additionally, Ultra high frequency communications are managed by EPCglobal Class-1 Genre ation-2 and ISO specification. UHF RFID tags used in different applications, for instance, management applications and supply chain applications for pallet since they are very inexpensive to implement. The reading range for UHF tags about five to six meters and are available as both active and

passive tags. Nevertheless, the main issue with UHF tags is the contradictory frequency applications around the world [32]. Table 2.2 shows the ultra-high frequency regulations for RFID system in some countries.

Table 2.2: RFID Frequency Regulations [33].

Country	Frequency
Germany	865.6–867.6 MHz
India	865–867 MHz
New Zealand	864–868 MHz
Russian Federation	865.6–867.6 MHz
United Kingdom	865.6–867.6 MHz
United States	902–928 MHz
France	865.6–867.6 MHz
China	840.5–844.5 MHz
Canada	902–928 MHz
Australia	920–926 MHz
Japan	952–954MHz

2.2.4 Microwave Frequency RFID System

As presented in Table 2.1, the frequency of a microwave is 2.45 GHz. Furthermore, Microwave frequency communications administered by ISO/IEC specification 18000-4. This frequency used for cordless phones, microwave ovens, and medical equipment, consequently the possibility for interference between these devices and RFID systems increase. In general, Microwave tags faster than UHF tags in the reading rate, but more

vulnerable to degradation from solid substances. Microwave active tags have a read range of 100 meters, whereas passive tags have a read range of 10 meters [32].

2.3 RFID System Components

A typical RFID system is shown in Figure 2.1. The major components of an RFID system are RFID readers or interrogator, RFID tags or transponder, and middleware. The reader sends electromagnetic signals and the tag receives these signals through antenna to be identified. Also, RFID tags broadcast their data (includes the identification number to recognize the objects) they are in the surrounding area of a reader. The reader gathers the tag data details and sends it to a host computer to be processed. In addition, the host computer can be connected via internet for global networking.

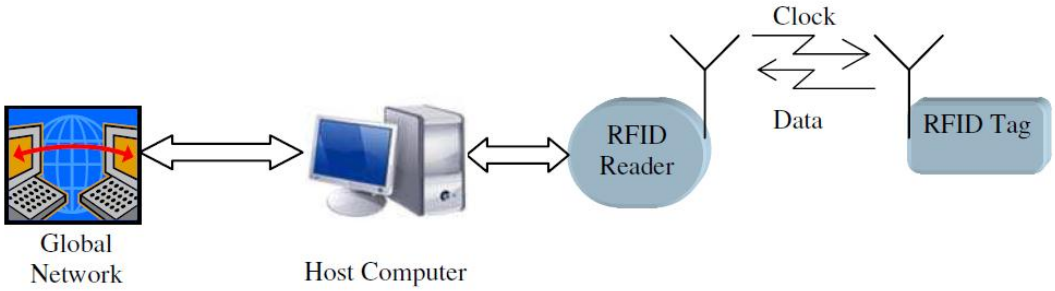

Figure 2.1: A block diagram of RFID system [34].

2.3.1 Tags

RFID tags are precise items that can be attached to goods, animals, or people to identify and monitor using radio waves. Tags are made up of an integrated circuit (IC) and an antenna. An integrated circuit consists of three major components: a microprocessor that used to process the signals received from the reader, a memory to supply a unique identification number for the tag, and antenna which needed to communicate with the reader and to expand the reading range. But, different antenna types are designed to suit

various environments and different tag applications. In general, RFID tags are primarily categorized into active tags, passive tags, and semi-passive tags [35].

Active tags have an equipped battery to provide the required power to power up the integrated circuit and send the signal to the reader. As well as, Active tags can be read from a longer distance (20 meters to 100 meters) [36] over the passive tags due to the equipped battery. The disadvantages of active tags are the cost and size because the internal battery [35].

Passive RFID tags are not equipped with any power source and activated by the reader through the radio wave. When the passive tags located in the range of the radio frequency wave field of the reader, it uses that energy to power itself up and communicate with the reader. The advantages for passive tag that inexpensive, small size, and no need for an internal power source. Nonetheless, the disadvantages that they have limited read rang and required a higher powered reader [35].

Semi-passive tags have a built-in battery but are not used for RFID communication with a reader. But this power source is used to power up the integrated circuit. Therefore, the tag utilizes all the energy gathered from the radio wave of the reader to broadcast its information. Therefore, semi-passive tags have a longer read range than passive tags [35].

2.3.2 Readers

RFID reader is the connector between the RFID tag and middleware. There are three main components of RFID reader: the antenna and radio frequency electronic module is used for communication with RFID tag, and the controller electronic module is used for communication the middleware. In addition, the reader communicates with the RFID tag to read the data, pass on data to and from the middleware, use the anti-collision algorithms to

separate many tags. The RFID readers are classified according to their communication interface as serial readers, network readers, and stationary readers [35, 37].

Serial readers utilize a serial port to transmit commands performed by the user or the application of the host system. The main benefit of serial readers is that the serial port connections are very reliable. Nevertheless, two disadvantages are a lower information transfer speed and limited cable length [35].

Network readers have the capability of connecting to wired or wireless host systems. In addition, network readers have no cable-length limitations. However, the connection is not very reliable, as in serial readers [35].

Stationary readers are typically mounted on walls, gateways, or any appropriate structure in the read area. Sometimes, these readers are mounted on moving objects like forklifts and trucks. Stationary readers contain external antennas. An example of a stationary reader type is the RFID printer, which is capable of printing bar codes and writing on its RFID tag [35].

2.3.3 RFID middleware

RFID middleware is used to manage the flow of data between RFID readers and enterprise applications. Furthermore, RFID middleware moves the information stored in a tag from the RFID reader to the appropriate enterprise system in a tag-read process, and moves the information from the enterprise system to the appropriate RFID reader and eventually to the correct tag in a tag- write process [37].

2.4 Applications of RFID

RFID has the ability to identify, locate, track, and monitor objects. As a result, RFID technology has numerous applications in our daily life. A few of those applications are briefly reviewed in this section.

2.4.1 New born Infant Tracking

A major problem that many hospitals face is the possibility of inadvertently mismatching newborns with their parents. Furthermore, this problem has raised major legal liabilities and generated enormous emotional pain for parents. Hospitals offer a better method to guarantee that the right newborn baby is given to the right parent by using RFID technology. Protected wristbands with RFID tags are affixed to the baby and the mother. Then, unique identifiers of the baby's and mother's RFID tags are linked together in the database. This process ensures that each baby is placed with the correct mother by matching the unique identifiers of the RFID tags [35].

2.4.2 Attraction Park children positioning

Parents face the possibility of losing their children in public places. A number of attraction parks have set up a child tracking system using RFID to overcome this issue. A bracelet with an RFID tag is affixed to the child's wrist, and RFID readers are placed tactically around the park grounds in order to provide full coverage so that the child can be tracked easily. These details are well protected by the information system and are only given to the person in charge of the child [35].

2.4.3 Ticketing

RFID systems are commonly used for airline ticketing purposes. The Lufthansa "ticketless flying" project replaced the conventional paper ticket and boarding pass with new contactless smart cards. Passengers book their flights using an RFID-enabled unique card number. Then an electronic ticket, associated with the customer's personal data along with the flight details, is generated and saved in the system. At the terminal, the customer only needs to have the smart card on his/her person, even without removing it from a wallet or briefcase, in order to obtain a printed, detailed receipt. Even at the boarding gate, the customer only needs to present the smart card [22].

2.4.4 Public Transportation

Public transportation by bus is one of the major applications of RFID. Conventional paper tickets are now replaced by contactless smart cards. Passengers are no longer required to have the exact change or money since smart cards have the ability to be loaded with a large amount of money. The customer no longer needs to know the exact price of the fare, as the system automatically debits the correct price from the card. Also, customers can use the same card for all transportation routes [22].

2.4.5 Animal Identification

RFID has allowed the rancher to obtain the exact number of his/her cows automatically at a distance by using a mobile phone instead of counting each cow on the ranch. An RFID tag, affixed to the animal's ear, stores details about the animal—breed, pedigree, birth date, vaccination details, and temperature profile. RFID readers placed on the farm read data from these tags and transfer it to a mobile phone, and laptop. Today, many animals are

tagged, including cats and dogs. Tags can store not only a pet's identification number but also its unique identifier, name, address, and vaccination records [35].

2.4.6 Vehicle Immobilization

All new manufactured vehicles are now equipped with RFID-based anti-theft systems. A vehicle immobilizer is a security gadget installed in a vehicle to make it difficult for unauthorized users to have access to the vehicle. Typical anti-theft systems sound the horn and flash the headlights when the vehicle has been illegally accessed. However, the RFID anti-theft system immobilizes the engine, prohibits the flow of fuel, impedes the electrical supply, and stops all other moving parts, when it detects an unauthorized access. RFID readers that are installed in vehicle door locks and the ignition read the RFID tagged keys and ensure that the valid key is used to open the door and start the engine. Otherwise, readers will prevent mobilization of the vehicle and send an alert to the owner of the vehicle regarding unauthorized access [35].

2.5 RFID Standards

Standards guarantee that products have at least certain features, such as quality, interoperability, reliability, and safety. At present, there are numerous groups working towards standardization of RFID. The main organizations creating standards in the RFID field are the International Organization for Standardization and EPCglobal Inc.

2.5.1 International Standard Organization

International Standard Organization (ISO) develops and publishes international standards. In addition, it is located in Geneva, and Switzerland. ISO is a combination of the national

standards organizations of 163 countries [38]. Furthermore, the ISO primarily works in the development of RFID technological standards [39].

2.5.2 EPCglobal

The most powerful organization in RFID is the EPCglobal, a group of vendors and manufacturers decided to create a worldwide, industry-driven standard for RFID, known as the Electronic Product Code (EPC). EPC is the unique identification number for each RFID tags. Figure 2.2 shows an EPC example. Moreover, the EPC manager field is used to identify the manufacturer. The object class field identifies the type of product. The serial number field uniquely identifies a particular product [2].

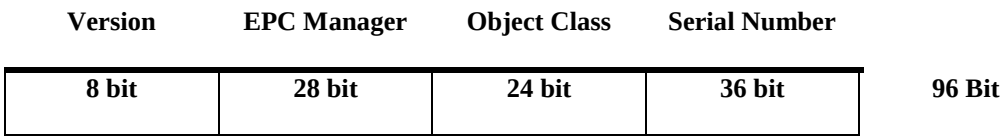

Figure 2.2: Electronic Product Code

The group financed the research of Auto-ID Labs at the Massachusetts Institute of Technology (USA), University of Cambridge (United Kingdom), University of St. Gallen & ETH Zurich (Switzerland), Fudan University (China), Information and Communications University (South Korea), University of Adelaide (Australia), and Keio University (Japan). The Auto-ID Centre produced the original ideas for implementing the “Internet of Things”. They realized that research work needed to be standardized to make it successful. As a result, EPCglobal was formed to develop standards for the EPC to uphold the use of RFID [32, 40]. EPCglobal has defined a class structure for RFID tags, which consists of five classes, as shown in Table 2.3.

Table 2.3: Classes of Tags [32, 35].

Class	Range	Description
0	$< 3m$	Read-only UHF passive tags. In addition, number programmed into tag during production.
1	$< 3m$	UHF or HF passive tags and Write-Once-Read-Many.
2	$< 3m$	Passive read-write tags. Also, data can be added to the tag by a qualified reader at any point in the supply chain.
3	$< 100m$	Semi-passive tags read-write with built-in battery and can record parameters like temperature, and pressure.
4	$< 300m$	Read-write active tags with integrated transmitters and on-board batteries.
5	Unlimited	Fundamentally readers with on-board batteries. Additionally, can provide power to other tags and communicate with devices other than readers.

Since there are no agreements regarding RFID standards between ISO and EPCglobal, EPCglobal presented its UHF Class-1 Generation-2 standard to be included as an ISO standard, and the ISO integrated this standard as ISO 18000. Consequently, the EPCglobal Class-1 Gen-2 standard became equivalent to ISO 18000 6C standard [39].

2.6 EPC Class-1 Generation-2 Protocol

The EPC Gen2 standard controls the communication between the reader and the passive UHF tags. The reader sends a modulating RF signal that contains all the communication parameters to the tags in the population. In addition, the reader transmits a continuous wave (CW) in the full communication session to ensure that the tags remain energized since that we used fully passive tags that haven't any energy source. The tag received the

(CW) and then modulated by the antenna reflection coefficient of the tag antenna as backscattering modulation. The reader communicates the tag within the frequency range from (860-960) MHz, 868 MHz is for Europe (ETSI) and 915 MHz is for US (FCC).Additionally, the operational frequency is chosen by local radio regulations[2]. The communication parameters are described in the following.

2.6.1 Reader (Interrogator) to Tag Communications

The reader transmits information to the tags by modulating an RF signal using a variety of Amplitude Shift Keying (ASK), in terms of Double-Side-Band ASK (DSB-ASK), or Single-Side-Band ASK (SSB-ASK) with Pulse-Interval Encoding (PIE) format. In addition, the reader uses a fixed modulation format in each inventory round [2].

Reader to tag communication link use PIE of the binary data stream at the reader. By this scheme, the information is carried by the duration of the encoded symbols. Each bit is mapped as shown in figure 2.3, where Tari indicates a data-0 and data-1 varies from 1.5 to 2 Tari. Moreover, Tari is the time unit reference chosen by the reader and goes from 6.25 μs to 25μs [2].

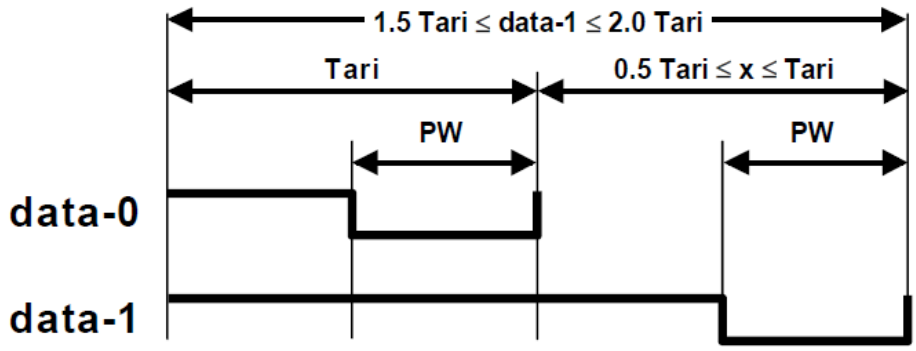

Figure 2.3: Illustration of PIE Symbols [2]**.**

The RF envelope of the reader to tag link is illustrated by Figure 2.4 and Table 2.4, where A is the maximum amplitude of the RF envelope, measured in units of V/m or A/m respectively. As well as, the pulse width (PW) is measured between 0.265Tari and 0.525Tari in unit of µs. The modulation depth is defined as $\frac{A-B}{A}$, where A and B are the highest and lowest amplitude level of a symbol [2].

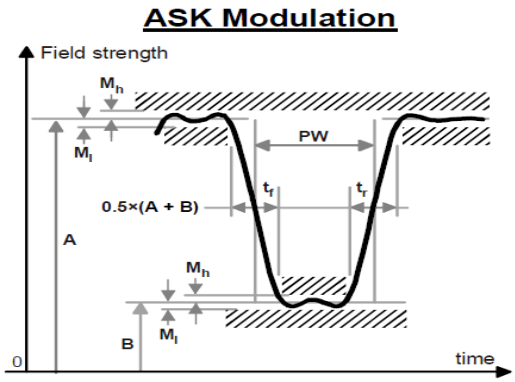

Figure 2.4: Reader to Tag RF Envelop [2].

Table 2.4: RF Envelop Parameters [2].

Tari	Parameter	Symbol	Minimum	Maximum	Units
6.25 µs to 25 µs	Modulation Depth	(A– B)/A	80	100	%
	RF Envelope Ripple	$M_h = M_l$	0	0.05(A– B)	V/m or A/m
	RF Envelope Rise Time	$tr_{,10-90\%}$	0	0.33Tari	µs
	RF Envelope Fall Time	$tf_{,10-90\%}$	0	0.33Tari	µs
	RF Pulse width	PW	MAX(0.265Tari)	0.525Tari	µs

The reader power-up RF envelop parameters are shown in Figure 2.5 and Table 2.5. Thus, as obvious when the carrier level increasing above the 10% level, the power-up envelope increments until the ripple limit M_l. Nonetheless, the RF envelop shall not breakdown under 90% through the interval T_s, after that when the carrier wave starts decreasing below the 90%, the envelop fall until the limit M_s and the power is off. In addition the reader shall stay powered off for 1 ms before the powering up start a new cycle [2].

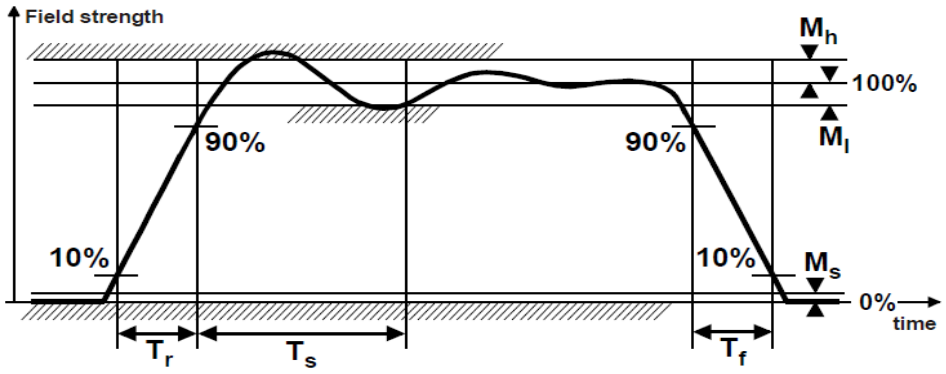

Figure 2.5: Reader Power-Up and Power-Down RF Envelop [2].

Table 2.5: Reader Power-Up and Power-Down Waveforms Parameters [2].

Parameter	Definition	Minimum	Maximum	Units
T_r	Rise time	1	500	µs
T_s	Settling time		1500	µs
T_f	Fall time	1	500	µs
M_s	Signal level when OFF	-	1	% full scale
M_l	Undershoot	-	5	% full scale
M_h	Overshoot	-	5	% full scale

The initiate packet from reader to the tag shall start with a preamble or a frame-sync. A preamble is sent before each Query command. Furthermore, it includes several critical time period which define link timing between the reader and the tag and all the other signalling start with a frame-sync. Figure 2.6 shown both a preamble and frame-sync, where a preamble includes a fixed-length start delimiter, a data-0 symbol, an Reader to Tag calibration (RTcal) symbol, and a Tag to Rader calibration (TRcal) symbol. The reader specifies tags Backscattering Link Frequency (BLF) using TRcal and Divided Ratio (DR). Equation 2.1 shows the relationship between BLF, TRcal and DR.

$$BLF = \frac{DR}{TRcal} \tag{2.1}$$

Where DR is the Divided Ratio (either 8 or 64/3), the value of RTcal and TRcal that the reader used in each inventory round shall agree with the constraints in Equation 2.2

$$1.1 \times \text{RTcal} \leq \text{TRcal} \leq 3 \times \text{RTcal} \tag{2.2}$$

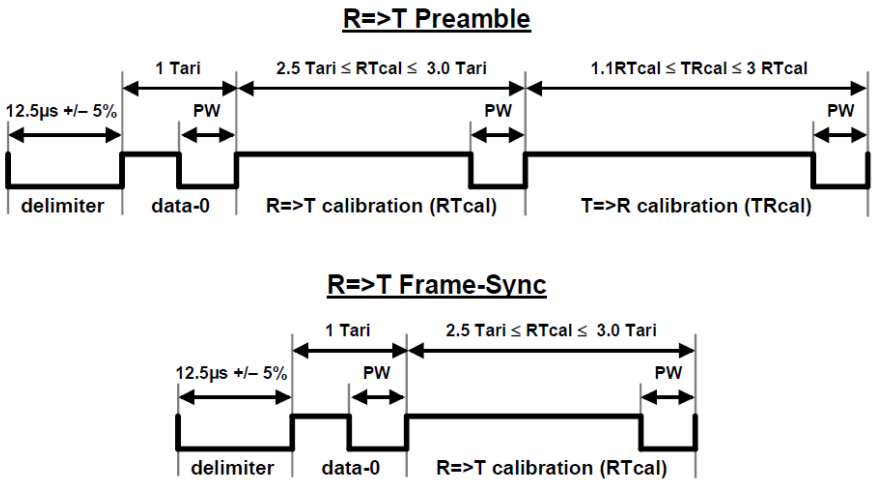

Figure 2.6: Reader to tag Preamble and Frame-Sync [2].

2.6.2 Tag to Reader (Interrogator) Communications

The passive tag utilizes a backscattering modulation. The tag modulates the incoming signal from the reader by switches the reflection coefficient of its antenna between two states in accordance with the data being sent. The reader specify the data encoding and the modulation format in the Query command that initiate the round, thus the modulation form is ASK. Also, Phase Shift Keying (PSK) can also be used by the tag and the reader can demodulate the two types [2].

The passive tag utilizes in the uplink communication FM_0 or Miller encoding. Figure 2.7 Shows the FM_0 encoding, where introduces phase inversion at the end of every symbol, and a phase transition in the middle of a data-0 symbol, whereas, data-1 has no transition [2].

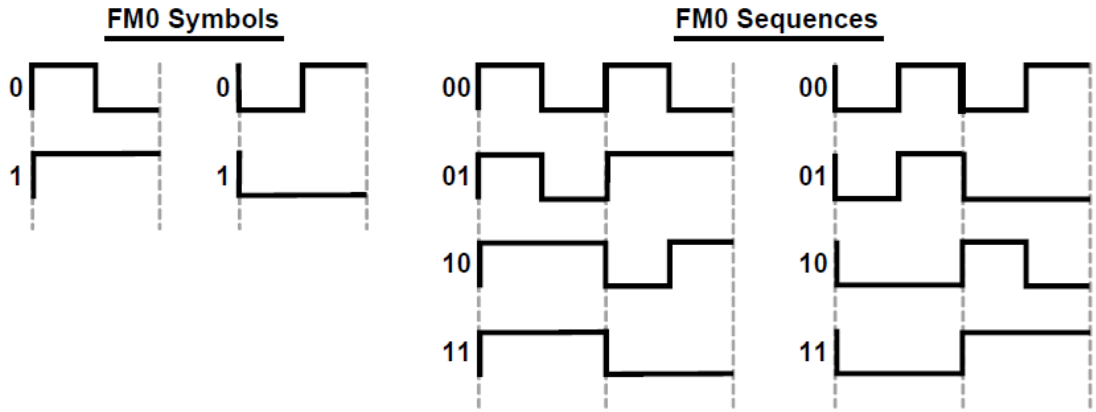

Figure 2.7: FM_0 Symbols and Sequences [2].

Miller coding introduces a sub carrier sequences, thus each bit can be encoded to include of (2, 4, 8) cycles. This encoding technique introduces more resiliency as there are more subcarrier cycles per bit. Figure 2.8 presents a different miller encoding [2].

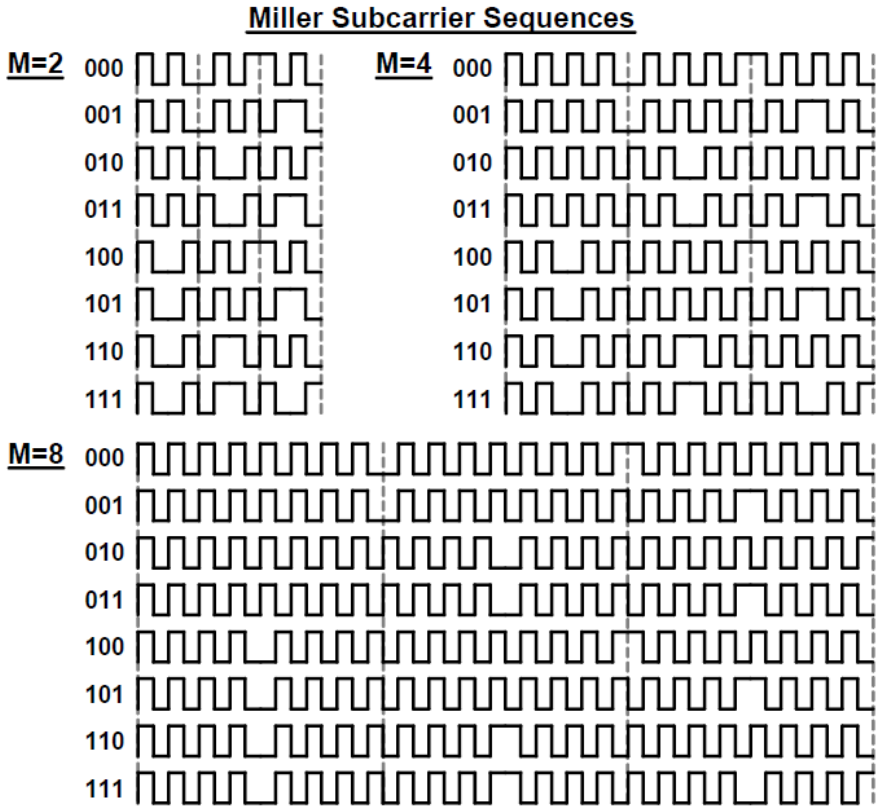

Figure 2.8: Illustration of the different miller type data encoding [2].

2.6.3 Cyclic-Redundancy Check (CRC)

The reader uses a Cyclic-Redundancy check (CRC) to ensure that the information backscattered from tag to reader is correct and a tag uses A CRC to ensure that the commands from the reader to tag are valid. There are two types of CRC: 16- bit and 5-bit CRC. At power-up, a Tag calculates and saves into memory a 16-bit Stored CRC. During inventory, a Tag may backscatter either this Stored CRC, or a 16-bit Packet CRC that the Tag calculates dynamically [2].

2.6.4 Link Timing

The reader used a fixed reader to tag link rate for each inventory round. Thus, if there is a prior changing in the link rate then the reader transmits a CW of 8 RTcal. Figure 2.9 shows

a single tag reply to the reader and the timing requirements, where the reader transmits a select command allows the reader to select a particular Tag population prior to inventorying, the reader sends a Query command to the tags that includes all the communication parameters. As a result, the tag reply a random 16 bit number (RN16), that is then decoded and echoed from the reader in terms of an acknowledge (ACK) command. When the tag receives the ACK, and verifies the transmitted RN16, it backscatters its EPC and the reader transmits a Query Repeat (QueryRep) to ensure there is no tag stayed in the population. Nevertheless, if the reader decodes an invalid EPC from the tag it sends Negative Acknowledgment (NAK) command to the tag. The standard specifies T_1 and T_2 as part of the timing requirements for the tag and reader response respectively. Hence these parameters are the timing between dependent transmissions, such as the ACK reply to a RN16 tag response. T1 Specified as The time from the last rising edge of the last bit of the reader transmission to the first rising edge of the Tag reply. Where T_2 Specified as the end of the last bit of the Tag reply to the first falls edge of the reader transmission, and the time between the commands specified by T_4 [2].

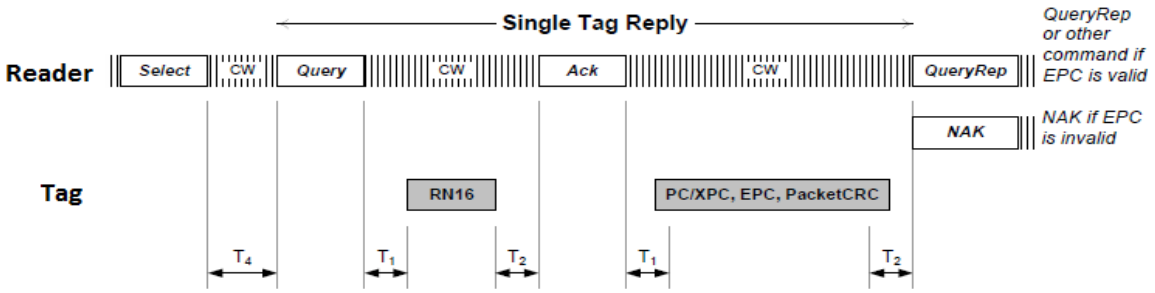

Figure 2.9: Link Timing [2].

Table 2.6 describes all the parameters that shall send through the Query command to the tags in the population. Also, Figure 2.10 shows a Query Command that contains the communication parameters. For instance, the number of bits for command equal four (1000), and Divided Ratio (DR) contains one bit (zero or one) etc.

Table 2.6: Query Command Parameters

	Command	DR	M	TRext	Selection	Session	Target	Q	CRC
# of Bits	4	1	2	1	2	2	1	4	5
Description	1000	0: 8 1: 64/3	00: M=1 01: M=2 10: M=4 11: M=8	0: No pilot tone 1: Use pilot tone	00: All 01: All 10: ~SL 11:SL	00: S0 01: S1 10: S2 11: S3	0: A 1: B	0-15	CRC-5

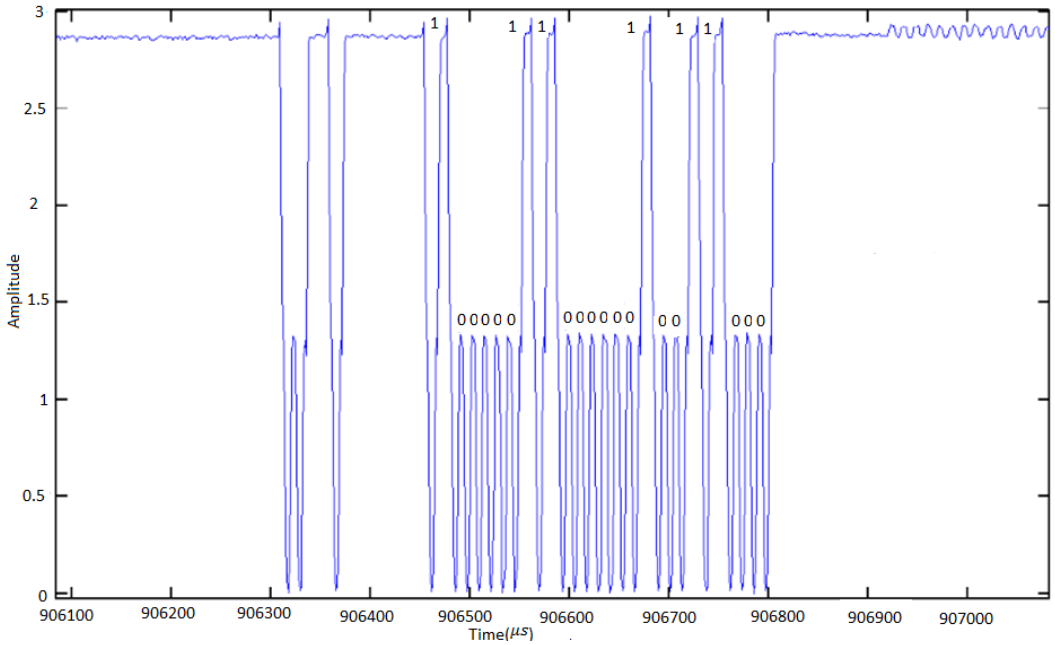

Figure 2.10: Query Command.

2.7 RFID Anti-Collision Protocol

An RFID system consists of many RFID tags and readers. RFID has the capability of scanning multiple objects simultaneously. Nonetheless, readers should be able to identify each individual tag separately from the hundreds of tag responses in order to read the data stored in them. When several tags reply to a reader query at the same time, contradictory communication signals might cause interference, or collision. Collisions happen when

readers and tags functioning on the same channel transmit simultaneously. If there is only one reader and only one tag in the RFID system, then they are able to communicate without any collisions [41].

The algorithms that are used by the readers and the tags to solve the collision problem are known as anti-collision protocols. Additionally, anti-collision protocols allow multiple tags to be identified simultaneously. These protocols should detect and separate all the tags quickly before the tag leaves the reading zone. The main anti-collision protocols used in EPCglobal Class-1 Generation-2 are Aloha Anti-Collision Protocol and Dynamic Framed Slotted Aloha [39].

2.7.1 Slotted ALOHA Protocol

The aim of the RFID reader is to recognize the RFID tags in the population. However, when several tags response at the same time, the collision happens. Aloha protocols are the main algorithm to solve this issue.

The time in Slotted ALOHA protocol divided into equal intervals known as time slots and the transmission time of the data is equal to the slot size. Each tag can resend its EPC at the beginning of the next available time slot. When slotted ALOHA protocol is used in RFID system as shown in Figure 2.11. For example, the reader transmits a REQUEST command that contains three time slots to the tags in the reading zone, each tag choose a random time slot to resend its EPC. Nevertheless, the reader send three time slots and we have four tags in the population, definitely two or more tags will select the same time slot. When two or more tags reply to the reader simultaneously in the same time slot, collisions occur at the reader. As a result, the reader will not be able to identify the serial number of any tags, and these tags must be read again [22].

Reader to Tag	Time Slot 1	Time Slot 2	Time Slot 3
Tag1		1000011	
Tag2	10111010		
Tag3	11011001		
Tag4			01001001
	Collision	Success	Success

Figure 2.11: Slotted ALOHA Anti-Collision Protocol.

The throughput (S) of the Slotted Aloha anti-collision protocol with the offered load (G) is [22]:

$$S = G\, e^{-G} \tag{2.3}$$

The maximum throughput for Slotted ALOHA when $G = 1$, substituting this value in Equation 2.3:

$$S = 1\, e^{(-1)}$$

$$S = \frac{1}{e}$$

$$S = 36.8\%$$

When the number of the tags increase in the reading zone of the reader, more collision will happen, thus throughput for the system will decrease. If we increase the time slots will solve this problem. But this manage decreases the performance of the anti-collision algorithm since it must listen for all feasible tags for the period of all the time slots, even though there is only one tag in the reader zone. Dynamic Slotted ALOHA was presented to solve this problem [22] as an improvement to Slotted ALOHA.

2.7.2 Dynamic Framed Slotted ALOHA (DFSA) Protocol

The Dynamic Framed Slotted ALOHA (DFSA) has been developed which become more reliable than Slotted ALOHA. In DFSA, the frame size changes after each round which is dependent on the number of the tags in the reading zone. Additionally, it is very important to choose an appropriate frame size that contains the number of time slots. Whereas, if the initial frame size is small and the number of the tags in the population is large, then the number of collide slots increase. If the initial frame size is large and the number of tags small, then empty slots increase. As result, the performance of the system degrades [42].

EPC Class-1 Generation-2 protocol utilizes the Dynamic Framed Slotted Aloha (DFSA) technique to identify all the tags in the population, and takes the benefit of Q-algorithm to specify the number of time slots required in each frame to send through the Query command. The reader begins an inventory round by sending a Query command and the Q parameter; those tags receive this Query command select randomly a Slot Number (SN) between $0\ to\ 2^Q - 1$ and store this value in the slot counter. Tags that choose randomly the slot number 0 generates a random 16-bit number called (RN16) and back it to the reader. Three scenarios may happen when each tag in the population chooses randomly the slot number [2, 39, 43]:

- Idle transmission: In this case no one of the tags select the SN zero, thus the reader receives empty slot.
- Single transmission: Only one tag select the time slot zero and generate a random 16-bit (RN16) and resend it to the reader. In addition, the reader inform all the tags in the population that only this tag can use the wireless channel to send its EPC to the reader. As a result, this tag can successfully send its EPC while the other tags are silent.

- Collided transmission: In this scenario, more than one tag selects the SN zero, thus many tags send RN16 to the reader and collision happens.

In the EPC Class-1 Generation-2(Gen-2) the Q parameter plays an important role. If the value of the Q parameter large and the number of the tags in the reading zone small, then the chance for empty slot increases. On the other hand, when the value of Q parameter is small and the number of the tags is large, the probability of collided slots increases in the system and the efficiency become worse. Due to, the value of Q parameter should be selected carefully through the system. The EPC Gen-2 utilizes the Q-algorithms to change the value of Q (the number of time slots). Figure 2.12 shows the Q-algorithm used by EPC Gen-2, where Q a parameter is specify the number of time slots that available for the tags in the population and Q_{fp} indicates the floating-point depiction of Q. The reader rounds the Q_{fp} value to the nearest integer and assigns this value for Q in the Query command.

$$Q = round(Q_{fp}) \tag{2.4}$$

There is another parameter c is used to adjust the rate of changing Q, the values for c between 0.1 and 0.5, this value selected by us based on experimental result for our system because this value Constitute an important point for system designer. The value for Q_{fp} initialized to 4 and rounded to the nearest integer, then send through the Query to the tags in the population. Each tags select a random Slot Number (SN) and replies to the reader. If only one tag has selected the value 0 for the slot counter, then the reader will receive a successful reply and the current value of Q and Q_{fp} will remain unchanged. If an idle transmission happens, the Q-algorithm decreases the value of Q_{fp} by c and sends the new value through the Query to the tags in the reading zone. In addition, if more than one tag choses the SN zero the collision happens, then the Q-algorithm increase the value of Q_{fp}

by c to sends this new value in the next Query. This process continuous until all the tags in the population identified successfully.

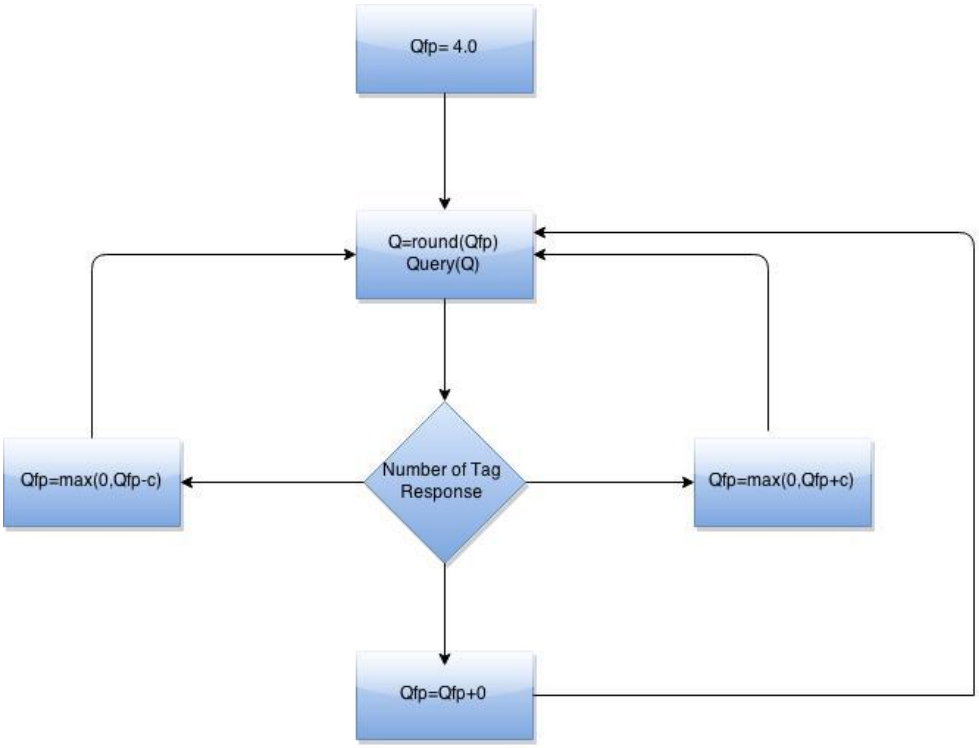

Figure 2.12: Q-algorithm used by EPC Gen-2.

In the DFSA it is important to increase the throughput by reducing the number of Collision slots(C), Empty Slot (E) and increase the number of success slots through our system. Only thing that we can adapt is the frame size, when the frame size is large and the number of tags small, then the probability of empty slots increases, thus we should select the frame size carefully. Consequently, the throughput function dependents on two variables: the frame size (L), and the number of tags in the population (n) and defined as [44]:

$$U(n,p) = np(1-p)^{(n-1)} \qquad (2.5)$$

Where $p = \frac{1}{L}$ the probability of finding the tag within the slot of the frame L. In addition, to find the maximum throughput we should find the first derivative of Equation (2.5):

$$\frac{dU(n,p)}{dp} = n(1-p)^{(n-2)}\big((1-p) - p(n-1)\big) = 0 \qquad (2.6)$$

We can obtain the maximum throughput when $p = \frac{1}{n}$, the number of tags equals the frame size($n = L$), given the maximum throughput $= \frac{1}{e} = 36.8\%$. As a result, we evaluate and implement DFSA based on RFID Gen-2 reader as an example on the MAC layer behaviour.

2.8 Summary

In this chapter, a comprehensive coverage of an RFID interrogation and components of the RFID system are presented and described. Furthermore, the main parameters are covered based on the EPC Gen-2 standard such as modulation types, coding techniques and timing requirements. Finally, the DFSA anti-collision protocol is described. The next chapter introduces the Software Defined Radio (SDR) platform.

Chapter 3

Software Defined Radio Platform

3.1 Introduction

A Software Defined Radio (SDR) is a Radio system where the components that implemented in hardware (amplifiers, filters, etc.) can be designed by means of software based on computer. The implementation of the radio functions in software rather than in hardware is much easier than redesign the hardware to support new functionality. In addition, different input signals can be processed without the need of changing the hardware. The flexibility of software-based applications makes SDR an excellent choice to avoid issues with compatibility and hardware reusability. The transmitted signal is generated by the software. Furthermore, the received signal is proceed and demodulated within software algorithm [45].

In Figure 3.1, the SDR is divided into three blocks. The first block on the left indicates the RF frontend of the hardware which serves as interface to the analog RF domain. In addition, an analog RF signal can be received or transmitted over antennas that are connected to the RF frontend called daughterboard. The upper path presents the receive path (Rx) and the lower path is the transmit path (Tx). In the second block in the middle, the daughterboard connected to the USRP (SDR platform developed by the Ettus Research [7]) motherboard , which the analog signal converted to digital samples, then transferred

to the Field-Programmable Gate Array (FPGA) to meet the requested frequency and sampling rate. The data sampled sent by the USB or Gigabit Ethernet connection to the host PC as described in the third block on the right. Finally, the GNU Radio controls the signal processing capabilities (fully designed in software). More explanation for what we have mentioned will be fully described in the next sections.

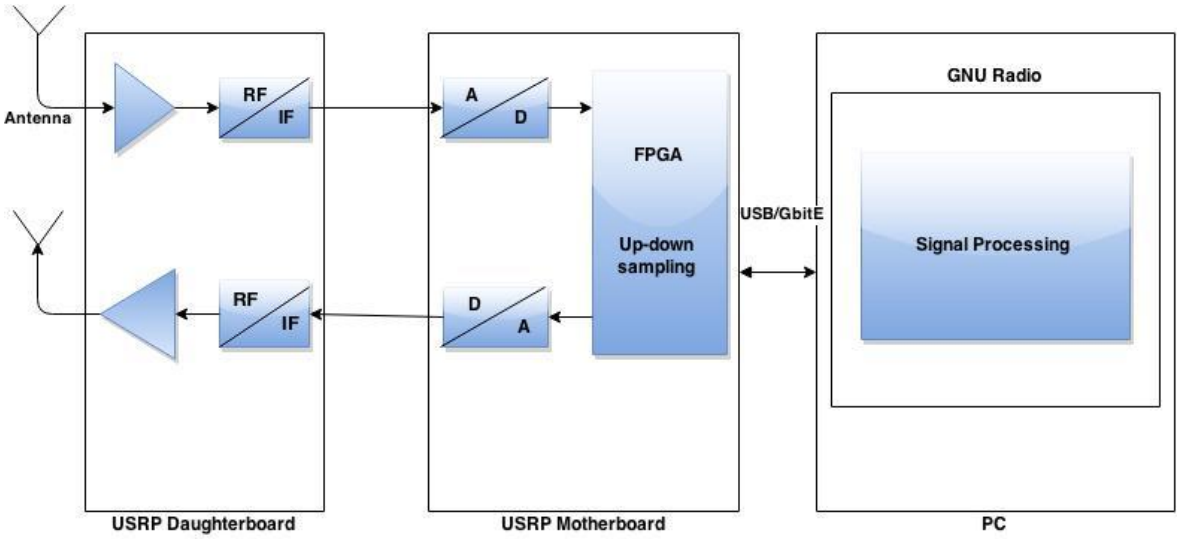

Figure 3.1: Software-Defined Radio Block Diagram.

3.2 Universal Software Radio Peripheral

The Universal Software Radio Peripheral (USRP) is used as an interface between the host PC and the frontend daughterboard. In addition, USRP is a reconfigurable hardware peripheral that allows general purpose computers to function as high bandwidth software defined radios. The USRP connected to PC via USB2.0 or Gigabit Ethernet connection. In a USRP-based SDR, the role of the host computer is to do all the signal processing such as modulation and demodulation [46]. Figure 3.2 shows two versions of USRPs called USRP1 and USRP N210 respectively.

Figure 3.2: USRP1 and USRP N210 [7].

3.2.1 Universal Software Radio Peripheral (USRP1)

The first SDR developed by the Etuss Research is USRP1 [3, 7]. It communicates with the host computer through the USB2.0 connection, capable of transfer speeds of up to 32 MB/s. In addition, USRP1 contains four 12-bit, 64MSamples/sec analog to digital converters (ADCs) and four 14-bit, 128MSamples/sec digital to analog converters (DACs) connected to an Altera Cyclone EP1C12Q240C8 FPGA. The FPGA is used to connect between USRP and the host PC. The motherboard had four sockets (2 Tx, 2 Rx) in order to connect 2-4 RF frontend daughterboard. There are different daughter-boards, each designed for a specific frequency. The maximum bandwidth is 8 MHz due to the data rate of the USB interface and the bandwidth limitations of a bus connected USRP are dictated by the maximum data rate of the connection technology used and the processing power of the host PC [46]. The USB connection is a limiting factor regarding to the data rate, thus it produces a high latency for the whole transmission. A complete architecture of the USRP1 is illustrated by Figure 3.3.

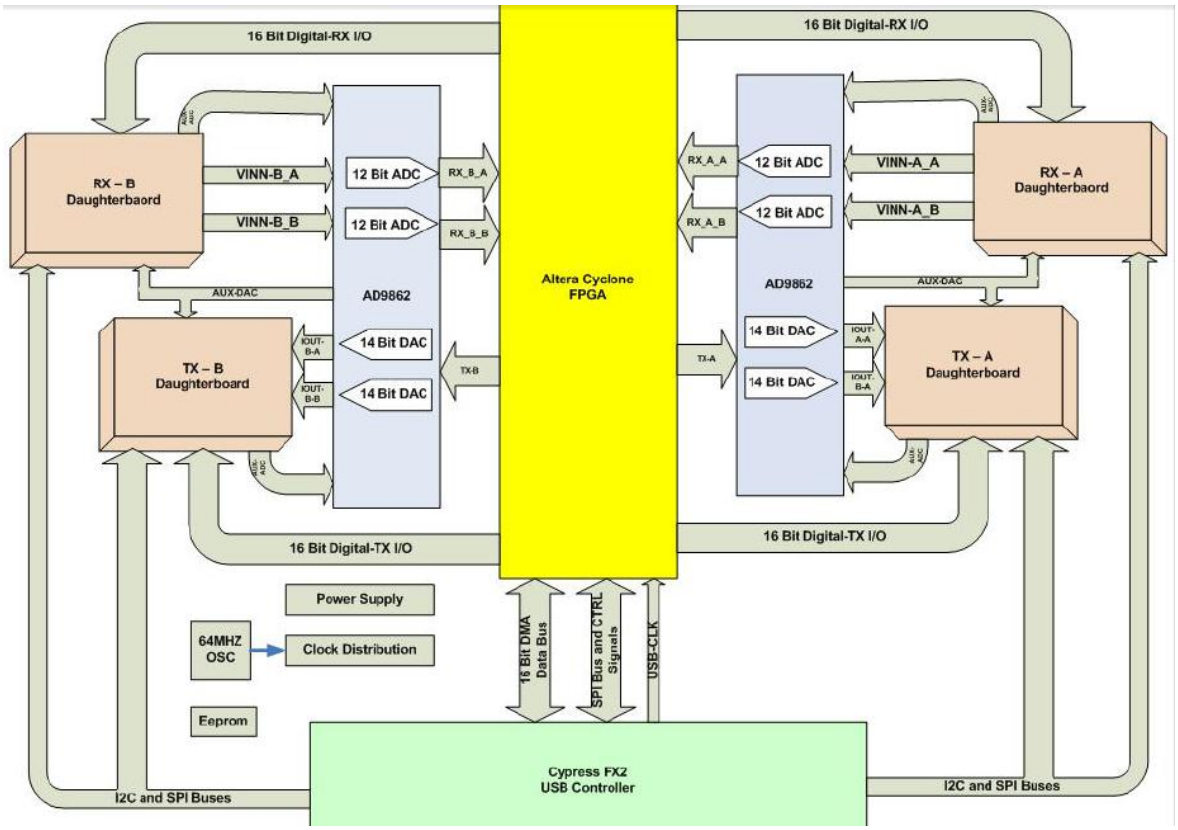

Figure 3.3: USRP1 Hardware Architecture [46].

3.2.2 Universal Software Radio Peripheral (USRP N210)

The USRP N210 is the latest model of the networked series developed by Etuss Research [3, 18]. It communicates with the host computer with Gigabit Ethernet connection. Two 14-bit, 100MSamples/sec analog to digital converters (ADCs) and Two 16-bit, 400MSamples/sec digital to analog converters (DACs) connected to Xilinx Spartan 3A-DSP3400 FPGA. The motherboard contains 1 Tx and 1 Rx ports. Furthermore, the effective bandwidth is 25 MHz due to the fast Gigabit Ethernet interface which is desirable. A modular design allows the USRP N210 to operate from DC to 6 GHz, while an expansion port allows multiple USRP N210 series devices to be synchronized and used in a MIMO configuration. In addition, an optional GPDSO module can also be used to discipline the USRP N210 reference clock to within 0.01 ppm to synchronize many USRP

up to 8 USRPs [7]. Figure 3.4 shows a complete USRP N210 hardware, and Table 3.1 summarizes the differences between USRP1 and USRP N210.

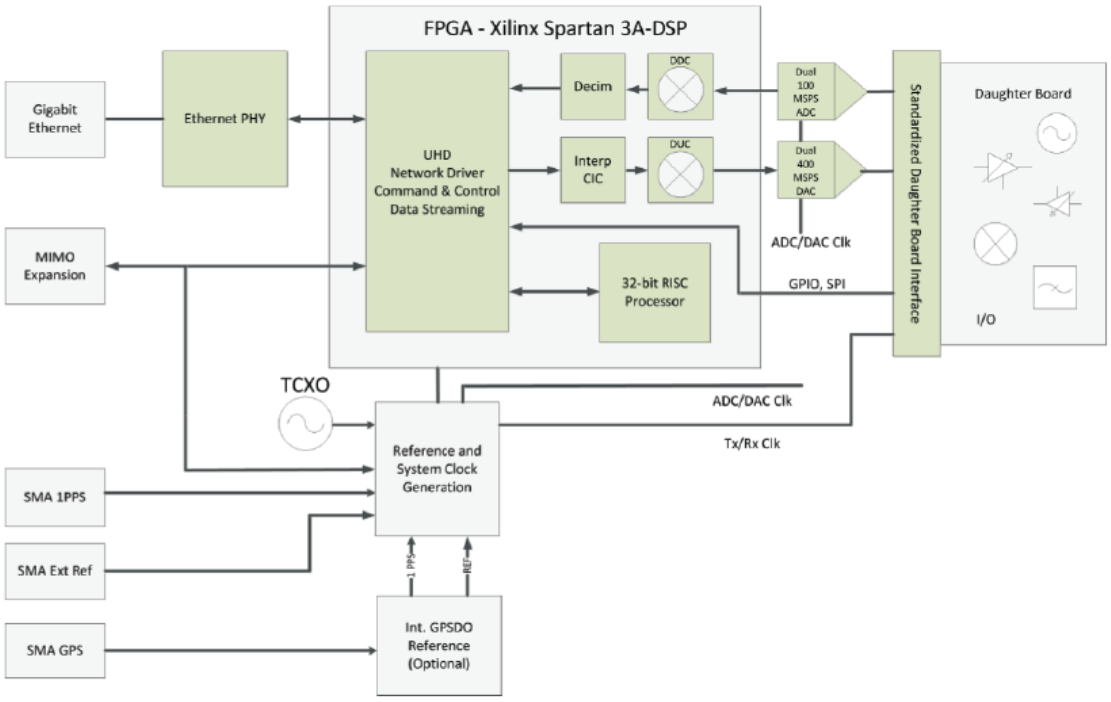

Figure 3.4: USRP N210 Hardware Architecture [7].

Table 3.1: USRP1 versus USRP N2010

Interface	USRP1	USRP N2010
ADCs	64 MS/s 12-bit	100 MS/s 14-bit
DACs	128 MS/s 14-bit	400 MS/s 16-bit
RF Bandwidth	8 MHz at 16 bits	25 MHz at 16 bits
FPGA	Altera EP1C12Q240C8	Xilinx Spartan 3A-DSP3400
PC connection	USB 2.0	Gigabit Ethernet
Daughterboard Capacity	2 TX and 2 RX	1TX and 1 RX
Power	6V,3A	6V,3A

3.3 Daughterboards

Ettus Research provides an RF frontends called daughter-boards to be interfaced with the USRP's motherboard. Each daughterboard has different specifications like frequency range and power. The signal on the daughterboard is already filtered, amplified and tuned to a baseband frequency. Also, there are a Basic Rx/Tx boards with no frequency conversion or filtering. They only provide a direct RF connection to the motherboard. Table 3.2 shows different types of daughterboards.

Table 3.2: Frequency Range and Application of several USRP Daughter-boards [7]

Identifier	Frequency Range	Area of Application
RFX900	750 to 1050 MHz	GSM
RFX1200	1150 to 1450 MHz	GPS
RFX1800	1.5 to 2.1 GHz	GSM
RFX2400	2.3 to 2.9 GHz	WLAN, Bluetooth
XCVR 2450	2.4 – 2.5 and 4.9 – 5.9 GHz	WLAN
SBX	400 MHz - 4.4 GHz	Radar Research, WiMAX

3.4 GNU Radio

GNU Radio is an open source development tool kit that supplies signal processing through software defined radio [6]. They are different types of block that used by GNU Radio. For instance, signal generator, filters, modulator/demodulator etc. As well as, each block has a number of input/output interfaces, thus we can write any application to transmit and receive the data through the hardware and each block can be edited, upgraded or you can

create a block independently and use it for your application. Moreover, this makes the GNU Radio user friendly and supports the real world radio system mainly in academic and research environment [47].

GNU Radio's applications are primarily written in the Python programming language while the signal processing path is written in C++ language, where each block programmed in C++ and Python is used to setup all input arguments and variables, connect the flow graph blocks which makes GNU Radio a rapid application development environment [47]. The software structure is illustrated in Figure 3.5, where the Simplified Wrapper and Interface Generator (SWIG) block enabling the implemented block in C++ to be compatible and interfaced with the main Python program.

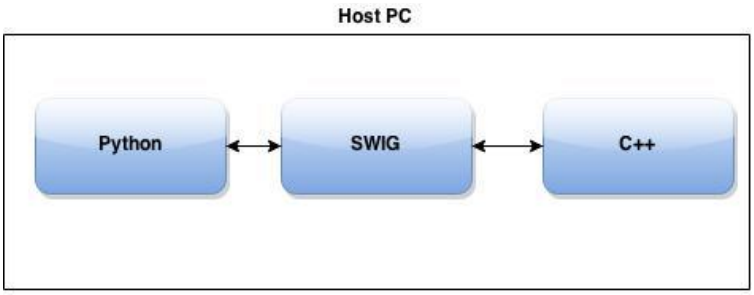

Figure 3.5: Software Architecture in GNU Radio.

GNU Radio runs under several operating systems like Linux, Mac OSX, and windows. But, it works natively under Linux. Additionally, the new version of GNU Radio requires Universal Hardware Driver (UHD), making it more platforms versatile which can support of interface applications like Matlab.

3.5 RFID Reader Implementation

In this section, we describe the software implementation which is based on GNU Radio (V3.6.2). In [5], the authors proposed an SDR system implementation for the EPC Gen2 reader. However, this implementation was dedicated to GNU Radio (V3.3.0) and compatible with the old generation of USRP called USRP1. We developed an implementation that is compatible with the latest generation of Ettus research USRP N210 and RFX900 daughterboard [7]. The original implementation proposed in [5] was published as open source code and our own implementation is based on it. We modified the libraries definition and all the files headers in order to be compatible with GNU Radio (V3.6.2). Figure 3.6 describes the system software implementation as a software blocks. Each block is responsible for a certain task. The Gen2 logic Block generates the commands (based on the Gen2 specifications that mentioned in chapter 2) for transmission. In addition, these commands are then sent to an amplifier and sent it through the USRP hardware to the tags in the population. In the receive chain there is an Rx block which receive the backscattered signal from the tags and passed to the match filter to maximize the Signal-to-Noise-Ratio (SNR) of the tags transmissions from the reading zone. The command gate acts as signal gate and responsible for gating the received information and separating the tag response from the carrier wave signal. If the received signal ungating by the command gate, then a clock recovery resamples the tag response thus the tag decoder block is responsible for determining the tag response (i.e., RN16, EPC). According to the tag response, a certain command is generated at the Gen2 logic block and transmitted through the USRP block where the modulation takes a place. By this implementation based on the new generation of the USRP we can read only a single tag in each inventory round, so we implemented the Dynamic Framed Slotted ALOHA (DFSA) protocol that discussed

in chapter 2 inside the Gen2 Logic block based on Q-algorithm to solve the collision problem.

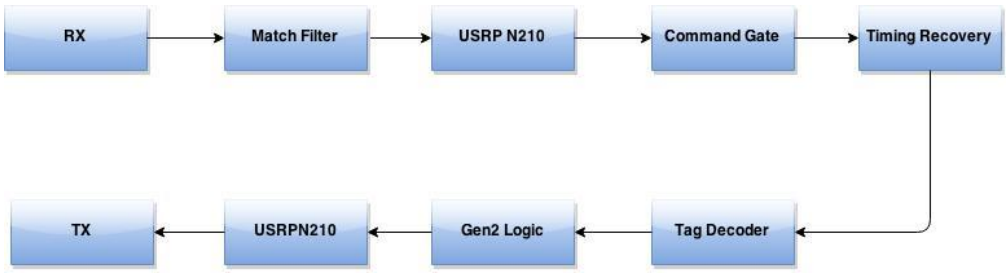

Figure 3.6: Gen2 RFID Reader System Architecture.

3.5.1 Gen2 Timing Constraints

The Gen2 protocol [2] set up strict timing requirements for the reader and tags communication as mentioned in chapter 2. If the reader commands are sent too late or too soon, then the tag will ignore these commands from the reader and the reader can not decode the tag transmissions. Through our implementation we set the communication parameters between the reader and tag based on the Gen2 specifications to solve the timing problem.

We set the preamble parameters that contain: Delimiter width, Tari, Pulse Width (PW), RTcal and TRcal as follows:

- Delimiter width= 12.5 μs
- Tari= 24 μs
- PW= 12 μs

The value for RTcal as Gen2 protocol specification is shown in Equation 3.1.

$$2.5 \times \text{Tari} \leq \text{RTcal} \leq 3\,\text{Tari} \quad (3.1)$$

Thus we choose for our implementation $\text{RTcal} = 3\text{Tari} = 3 \times 24 = 72\mu s$. The value for the tag Backscatter Link Frequency (PLF) varies from $40\,KHz\ to\ 640\,KHz$ as specification, we select the value for PLF equals $40\,KHz$. Finally we calculate the value for TRcal from the equation 3.2

$$PLF = \frac{DR}{TRcal} \quad (3.2)$$

Where the value for DR=8 and PLF =$40KHz$, by substituting this value in Equation 3.2:

$$TRcal = \frac{8}{40KHz} = 200\ \mu s \quad (3.3)$$

These parameters are very important for our implementation in order to overcome the timing issue between the reader and tags.

3.5.2 System Implementation challenges

Through our implementation for Gen2 RFID reader we faced a lot of challenges and issues that need to be resolved which can be summarized as follows:

- The implementation for Buttner code based on the old generation of the USRP and the old GNU Radio (V 3.3.3), which means this version cannot support the new generation of the USRP, and does not support the UHD, that is used in newer versions of GNU Radio (3.6.2). This is noted to be a general problem with the GNU Radio/USRP development reuse, as many blocks are developed for certain versions of GNU Radio. We changed all the header files and paths to be compatible with new version of GNU Radio and USRP.

- The main issue in our implementation is to reach the commercial reader power which is equal 1W to energize the tags in the reading zone. To solve this problem we used SBX daughterboard but this daughterboard did not achieve the desired power. As a result, this daughterboard not good for this job because Tx power 20 dBm (We could see that the reader send a Query command, but there is no tag response). Nevertheless, we used RFX900 daughterboard and we got Tx output power 30dBm (1W). Figure 3.7 shows SBX and RFX900 daughterboards respectively.

Figure 3.7: SBX and RFX900 daughter-boards.

- Latency Problem: As mentioned before the Gen2 protocol dedicates strict timing requirements for reader and tag transmissions, thus the reader should response quickly to the tag responses, for instance when the reader send a Query command to the tag and the tag response with RN16, the reader send ACK to the tag, if the reader late to send the ACK, the tag ignores this command and cannot reply its EPC. The old generation of USRP faced this problem because the USB2.0 connection is a limiting factor regarding to the data rate between the USRP and the host PC. Nonetheless, this issue is solved in our implementation based on the new generation of USRP by using the Gigbit Ethernet connection, which is faster than USB2.0 connection.

- The sample rates that used by USRP1 Differs from that used by USRP N210, thus we changed the sampling rates to be compatible with our implementation. The USRPN210 hardware samples at$100MS/s$, but we cannot send that many samples over the Ethernet. So, we should down sample to get 1MHz (1 sample perμs). As a result, we changed the sample rate for Rx/Tx from/to USRP to be 1MHz.

3.6 Summary

In this chapter, the main concept of SDR platform based on USRP and GNU Radio is introduced and illustrated. Furthermore, The SDR architecture and components are highlighted such as USRP types and USRP daughterboards. Then, the implementation for our reader is described and finally the system challenges are presented. The following chapter presents new open source RFID reader.

Chapter 4

New Open Source RFID Reader

4.1 Introduction

The shortage of low experiments on RFID systems is the result of the current lack of research tools available to researchers. As mentioned before, the commercial RFID readers are closed boxes that give the final reading of the commercial tags. Therefore, the commercial readers have many tuning parameters and configuration that cannot be changed, and the commands between the reader and tags cannot be revealed. In addition, the commercial reader does not provide any indication about what is happening at the MAC and the PHY layers of the system. This makes the study improvement of EPC Gen2 protocol very difficult .There are some testbeds and measurement equipment's that are commercially available and dedicated for RFID. However, their cost is high and also most of these equipment's are closed source, and thus, there is no ability to modify or to enhance the protocols [5].

Our new open source Gen2 reader platform provides a basis for researchers to conduct the RFID research field. In this thesis, we have implemented the UHF RFID Gen2 reader, and it can be used to read the commercial tags. Furthermore, the modifications to the MAC and the PHY layers are simple and flexible, and can be achieved by rewrite the software program, which is not possible in the commercial reader system.

4.2 RFID Reader Setup

In this section, the Gen2 reader is described and evaluated based on a real time testbed, with focus on the degree to which the platform can be used for further research.

As mentioned before, our testbed is based on the new generation of USRP which is called USRP N2010 and the daughterboard RFX900. Without any modifications this daughterboard provides a limited frequency range (900-920MHz) and this frequency doesn't cover the European frequency band of (868MHz) for UHF RFID transmission. As well as, a transmission power of the RFX900 is 200 mW only and this is not enough to interrogate commercial tags. To reach the power for the commercial reader (1W), the ISM band-pass filter is removed and replaced by a 100 PF capacitor to increase the transmission power to 500 mW and cover the European RFID frequencies (i.e., 860 – 960 MHz) as mentioned in [3]. Figure 4.1 shows the USRP N210 with the RFX900 daughterboard.

Figure 4.1: USRP N210 with RFX900 Daughterboard.

Furthermore, the RFX900 daughterboard is connected to Alien ALR-696-C circular antenna with gain of 8.5 dBi [48], one for the transmitter and the other for the receiver. In this setup, a transmission power of 1W is achieved. Finally, the USRP N210 is connected

to a Desktop core i7 with 3.2-GHz processor running under Ubuntu 12.4. A testbed of the measurement setup that was used for our architecture is presented in Figure 4.2. Additionally, an overview over the parameters used during measurement is summarized in Table 4.1.

Figure 4.2: Two circular antennas are connected to USRP N210 which works as a reader.

Table 4.1: Measurement Parameters

Parameter	Setting
Reader Frequency	868 MHz
Sample Rate	1 MHz
Decimation Factor (USRP)	100
Software Decimation	2
Tx Gain	25
PLF	40 KHz
Encoding	Miller 2

4.3 RFID Reader Performance Evaluation

For our reader to be useful, it should be able to read the commercial tags at a range of at least few meters. The full communication cycle between the reader and the tag is shown in Figure 4.3, where the reader sends a Query command to the tag, the tag responds by transmitting random pseudo 16 bits termed as (RN16), the reader sends back an acknowledgment (ACK) to the tag in term of the same received RN16 value. Upon receiving a correct ACK, the tag responds back to the reader by transmitting its EPC values, which consists of 96 bits of data, finally the reader sends a QREP, which indicates the beginning of a new slot.

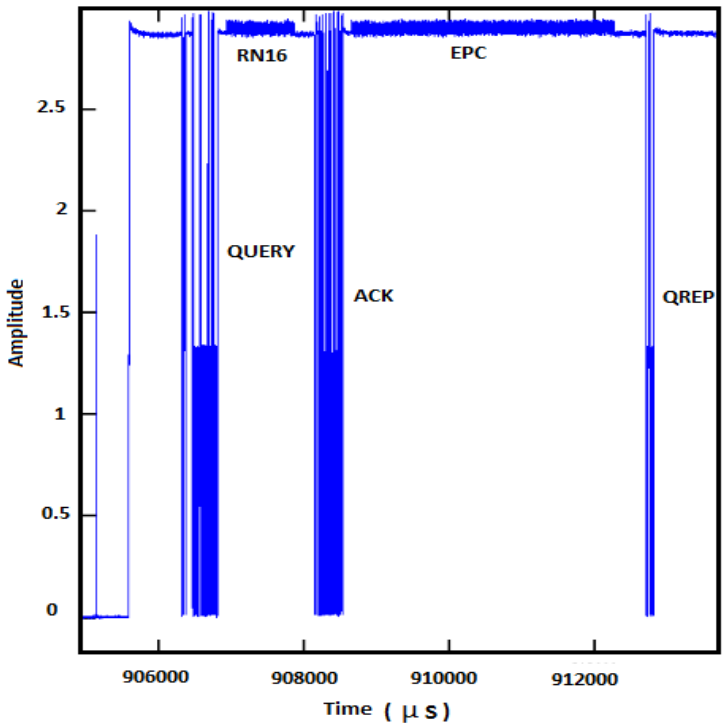

Figure 4.3: Gen2 RFID Reader Full Communication Cycle.

The reading performance of our reader is investigated. In our setup, the reader sends a Query command that contains one slot in each cycle to read a single tag. As well as, in

every test the tag is placed at different distance to check the performance of the reader. For each experiment we let the reader active for five minutes and the following counters are taken from the log file:

- N_Q = The number of queries that sent from the reader.
- $N_{(EPC\_correct)}$ = The number of EPC that analyzed successfully by the reader.
- $N_{(EPC\_error\_v-ACK)}$ = The number of wrong EPC that analyzed by the reader with valid ACK.
- $N_{(EPC\_error\_i-ACK)}$ = The number of wrong EPC that analyzed by the reader with invalid ACK.

The aim of this experiment is to find the Reader Success Ratio (R-SR) versus the reading distance. R-SR is defined by $\frac{N\_((EPC,correct))}{N_Q}$. The results are plotted in Figure 4.4. It is found that the reader has a success ratio more than 94% until 4.25 m. However, after about 4.5 m the reader degrades steadily and has 65% success rate at 6 meters.

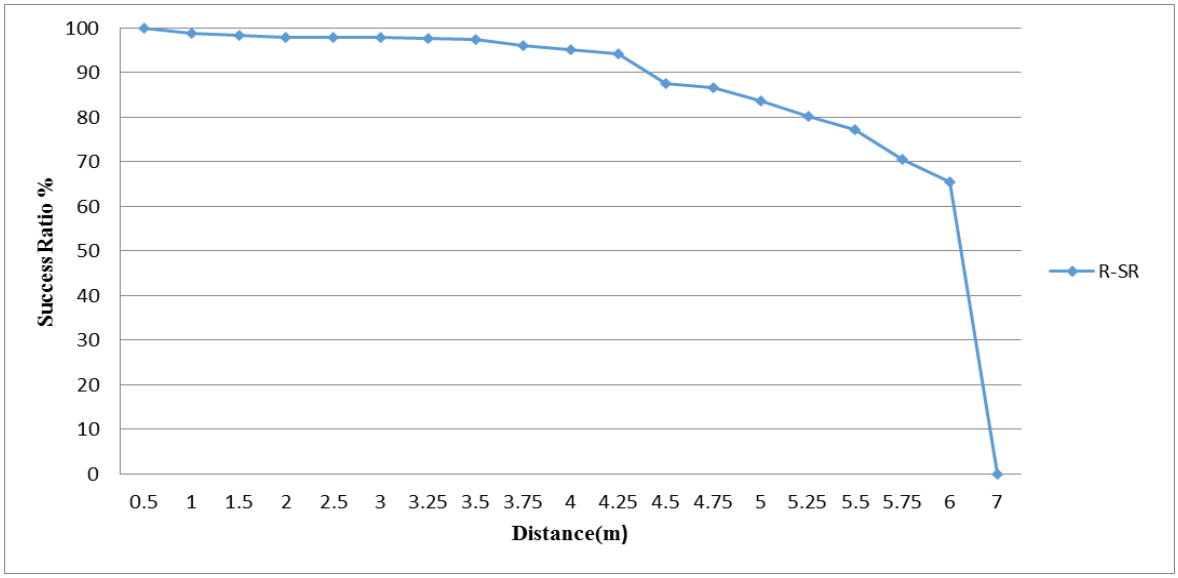

Figure 4.4: Success Reading Ratio versus Reading Distance.

Also, EPC error ratio versus reading distance is calculated and the results are shown in Figure 4.5. There are two types of error ratios. The first type of error is called the EPC error with valid ACK. This error occurs when the reader sends a query command and the tag replies with its own RN16, then the reader sends back a correct ACK command to the tag, and finally the tag sends its own EPC. However, the reader decodes the EPC incorrectly. The EPC error ratio with valid ACK is defined by $\frac{N_{(EPC\_error\_v-ACK)}}{N_Q}$ .The second type of error is called EPC error with invalid ACK and it refers to the error occurred when the reader decodes the RN16 command incorrectly. This error ratio is defined by $\frac{N_{(EPC\_error\_i-ACK)}}{N_Q}$. Finally, the EPC error ratio is the sum of the EPC error ratio with valid ACK and the EPC error ratio with invalid ACK.

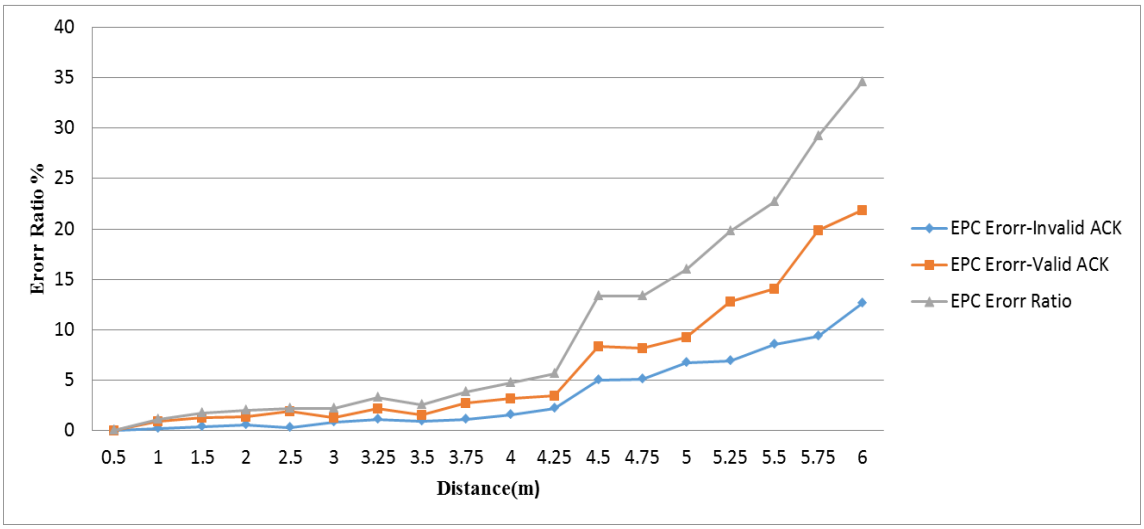

Figure 4.5: Error Ratio versus Reading Distance.

4.4 Using Our Reader in Research Studies

We implement our reader as a user-level software that is able to read the commercial tags. Our platform can be used in the research community for research work .In addition, modifications on MAC or PHY layers are simple and flexible.

In the following subsections, we present examples on two research studies that explain how our reader can be used. First, we use our reader and commercial tags to study the impact of what is called capture effect. Second, the performance of Dynamic Framed Slotted ALOHA (DFSA) described in chapter 2 based on EPC Gen2 standard is investigated as an example on the MAC layer behaviour.

4.4.1 Capture Effect

When one tag signal is greater than other one and reader can successfully resolve the stronger one, this is called capture effect. In our experiment, the reader informs the two tags that is only one time slot is available for them in each QUERY per round. Since the two tags are located at the same distance in the reading zone, collision (most likely) will occur. To check the impact of capture effect through our system, we put the two tags at different distances and observe when the reader will be able to completely resolve one of them. Even though the two tags transmit their signals to a reader simultaneously, one of the tags will be successfully identified due to capture effect. Figure 4.6 shows our experiment setup. The tags are placed at a variable distance from the reader antennas, and the probability of capturing is measured as distance is varied. The parameters that are used in our experiment are presented in Table 4.2.

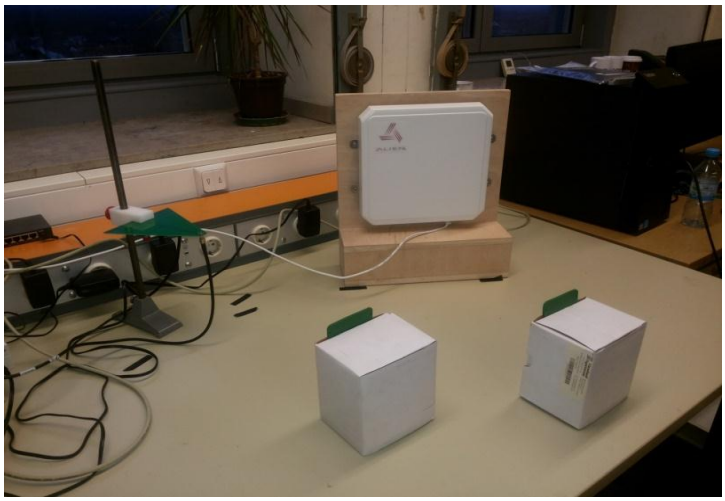

Figure 4.6: Experiment Setup.

Table 4.2: Measurement Parameters**.**

Parameter	Setting
Reader Frequency	868 MHz
Sample Rate	1 MHz
Decimation Factor (USRP)	100
Software Decimation	2
Tx Gain	25
PLF	40 KHz
Encoding	Miller 2
NUM_CYCLES	1000

We made a several experiments and each experiment is performed at a specific distance and it has duration of five minutes (this mean that our reader sends about 3000 Query command). From the log file we calculate the following:

- The number of all queries issued by the reader.

- The number of EPC decoded correctly.
- Probability of capturing= $\frac{number\ of\ EPC\ decoded\ correctly}{number\ of\ all\ queries}$.

The probability of capturing as a function of distance is shown in Figure 4.7. We notice that our reader has a probability of capturing of approximately 79% until 4 m and then decrease gradually to reach 20% at 6 m. As we see from the plot in Figure 4.7, capture effect which increases the performance of our reader in the collision case works with high percentage up to the reading range of our reader which is 6 m.

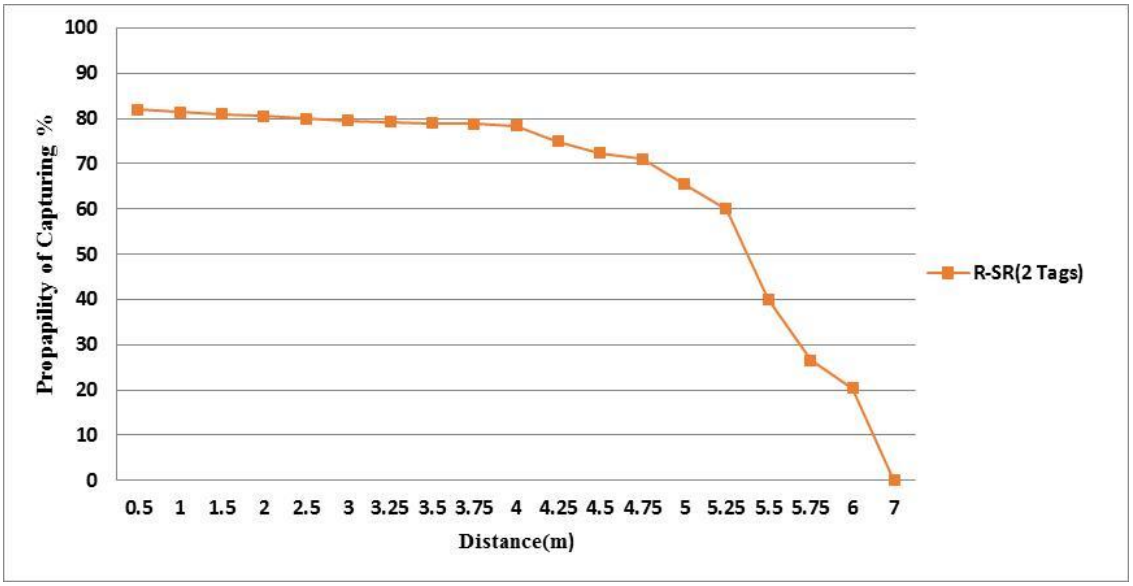

Figure 4.7: Probability of Capturing Versus Reading Distance.

4.4.2 Performance of Dynamic Framed Slotted ALOHA (DFSA)

The EPC Gen2 protocol describes Q-algorithm for adaptively changing the frame size to match the population size as mentioned in chapter 2. In other word the EPC Gen2 standard based on Dynamic Framed Slotted ALOHA (DFSA) is used to solve the collision issue when many tags respond simultaneously to the reader. To see how the EPC Q-algorithm

works in practice after implementation, we place multiple commercial tags away from our reader and evaluate its performance.

Figure 4.8 shows an example of a message exchange between our reader and three tags in the population. Our reader transmits a Query command with parameter Q that indicates four time slots in the frame. The first slot immediately follows the Query command, the tag had chosen this slot and transmits its RN16, then the reader acknowledged the RN16 and the tag transmits its EPC. Since we specified four time slots through the Query command, the reader sends three additional Query Repeats for looking to any remaining tag in the reading zone. In this case, there are two remaining tags in the population transmit its EPC to the reader. This procedure continuous until all the tags identified.

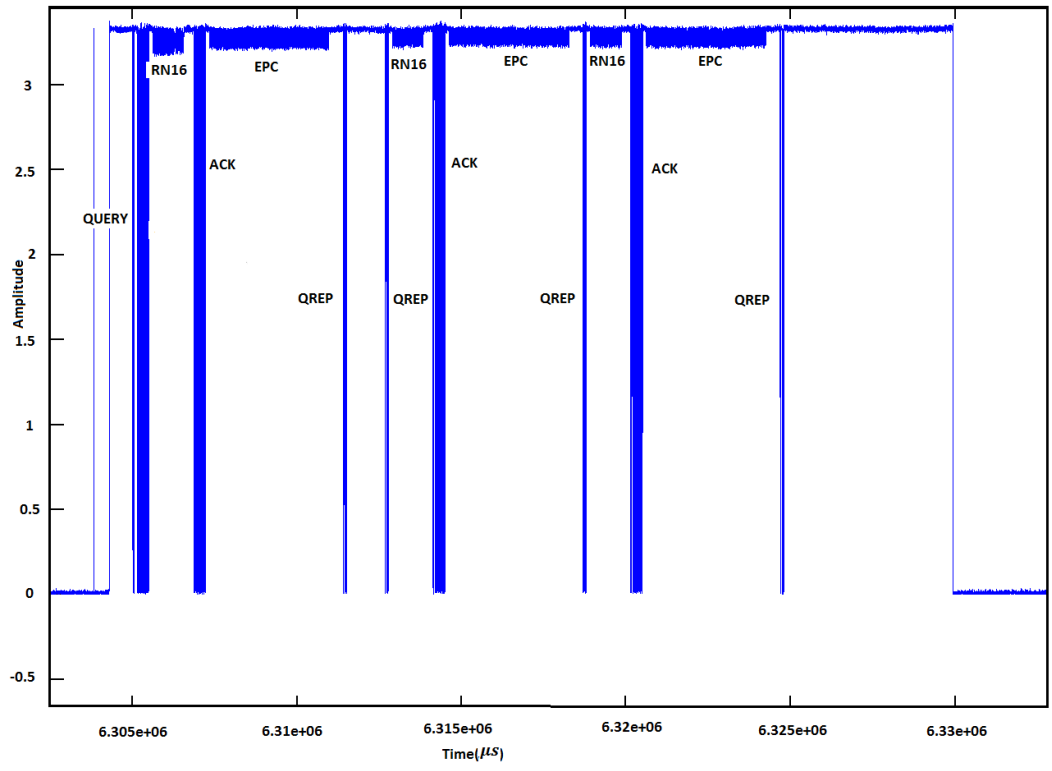

Figure 4.8: Communication Cycle between Our Reader and Tags Based on DFSA.

To test the Q-algorithm, the same setup that mentioned in section 4.2 is used. Nonetheless, the tags were put together on board one meter away from our reader, and they were

separated 20 centimeters from each other, in order to decrease tag-tag interference [49]. During our measurement, the tags board placed in a fixed position.

In our measurements, we use two cases: normal Q-algorithm case, which mainly depends on the parameter C, and optimal algorithm case in which we set the Q parameter (number of time slots) to be equal the number of tags in the interrogation area to reach the maximum throughput for DFSA, which is approximately 37%. In the optimal case, Q -algorithm does not depend on the value of parameter C.

In the Q-algorithm case and the optimal Q algorithm case, the number of tags is changed to take the values 2, 4 and 9 tags. Figure 4.9 shows an example for our system setup based on 9 tags (ALN-9640) in white color.

Figure 4.9: System Setup with commercial RFID Tags.

The additional parameters that are changed through our setup are listed in Table 4.3, where we set the reading cycle to 1000 for the reader power up command. In addition, we set

initial Q (INIT_QFP) to 3, which mean that the Query command will include 8 time slots. C value is varied from 0.1-0.5 in order to choose the optimal value for our reader.

Table 4.3: USRP N210 Run Parameters for Q-algorithm.

Variables	Value
NUM_CYCLES	1000
CHANGE_Q	true
INIT_QFP	3
Rx_gain	24
C	0.1-0.5

We made the experiment at fixed distance as we mentioned before and it has duration of five minutes (this mean that our reader sends about 3000 Query command). As well as, from the log file we calculate the following:

- The number of all Queries issued by the reader.
- The number of all Qrep issued by the reader.
- The number of RN16's decoded correctly.

➢ Efficiency = $\frac{S}{(E+c+S)}$.

Where:

S: the number of successful slots.

E: the number of empty slots.

c: the number of collided slots.

The summation of Query and Qrep commands equals total number of slots (E + S + C), and the number of RN16 decoded correctly indicates for the number of successful slots.

Figure 4.10 shows the efficiency for the EPC Q-algorithm and optimal Q versus the number of tags when we use two commercial tags. As well as, the efficiency for Q-algorithm dependent on the value of the parameter C which can be selected by the system designer [2], So when we change the parameter C from 0.1 to 0.5 the efficiency for Q-algorithm changes. For instance, when we set the parameter C to 0.2, the efficiency equals 21% .This result is due to the initial value of Q is relatively large and the number of tags is small, thus the chance of the empty slots increase and the efficiency decreases. Whereas, when the number of time slots equals the number of tags (optimal case of Q-algorithm) the efficiency increased to reach 33% which is very close to the theoretical value of 36.8%. Comparing results of normal case with the result of optimal case, we can notice from figure 4.10 that the best value of parameter C is equal to 0.3 where the maximum efficiency is about 27%.

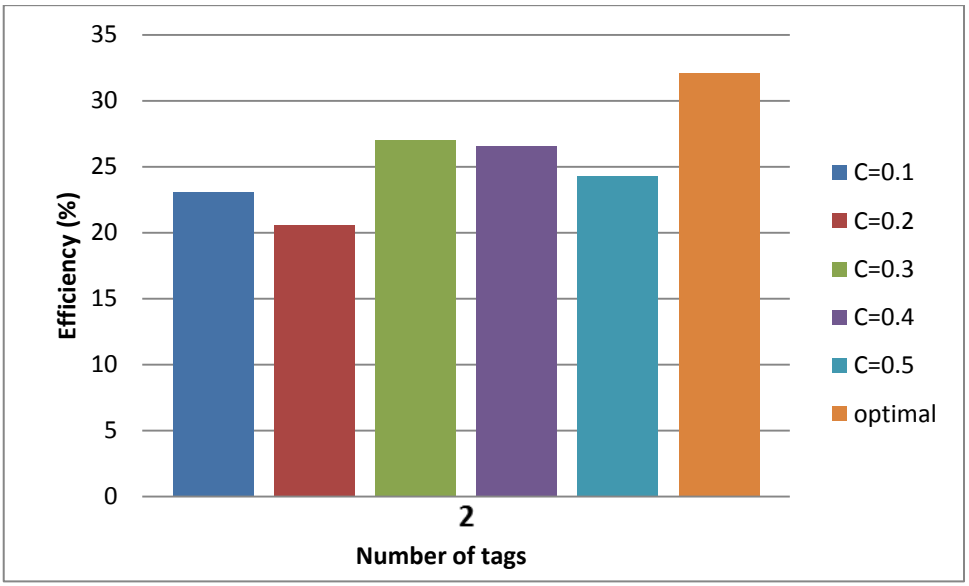

Figure 4.10: Efficiency versus Number of Tags**.**

We repeated the same experiment but we change the number of tags to 4 commercial tags. Figure 4.11 displays the efficiency for Q-algorithm and Q optimal versus the number of tags when we use 4 commercial tags. As well as, the value for the parameter C is changed through each experiment and the efficiency is calculated. For example, when the value of parameter C is set to 0.2 the efficiency about 23%. However, when the number of time slots equals the number of tags (optimal case of Q-algorithm) the efficiency increased to reach 30%. The best value of parameter C is equal to 0.3 where the maximum efficiency is about 25%.

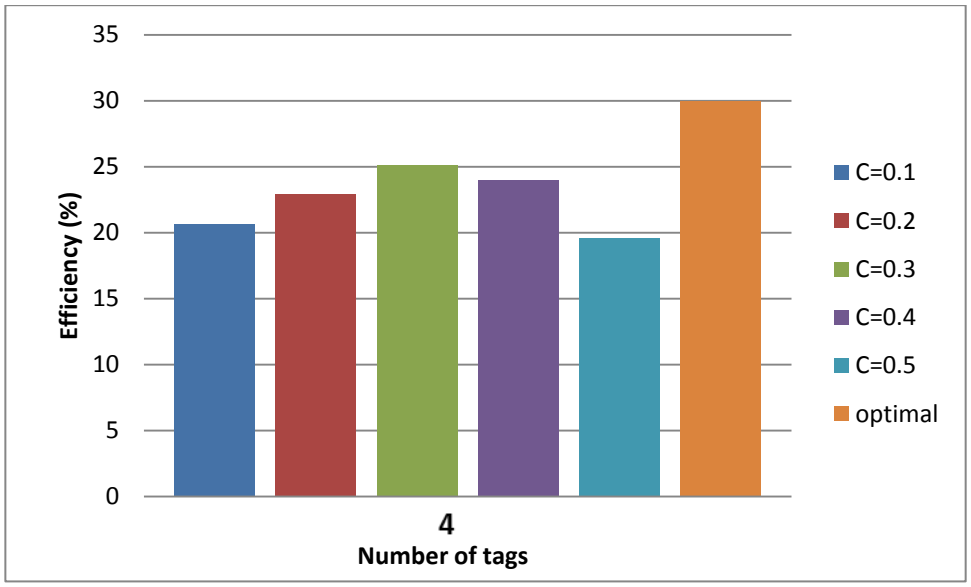

Figure 4.11: Efficiency versus Number of Tags.

The latest experiment we made based on 9 commercial tags .Figure 4.12 describes the efficiency for Q-algorithm and optimal Q versus the number of tags. We let our reader to send in each QUERY command 8 time slots .Indeed, the number of tags in the reading zone is greater than the number of time slots .As a result, the collision slots increase and the system efficiency decreases. For instance, when the value of the parameter C is set to 0.2 the efficiency reach 19%. Nevertheless, when the number of time slots equals the

number of tags (optimal case of Q-algorithm) the efficiency increased to reach 29%. The best value of parameter C is equal to 0.3 where the maximum efficiency is about 23%.

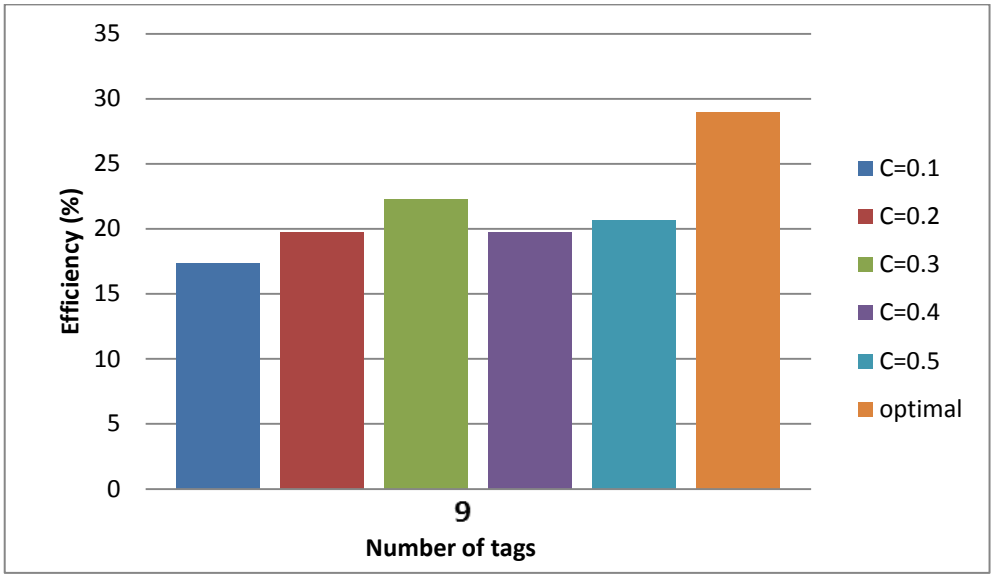

Figure 4.12: Efficiency versus Number of Tags.

Through our experiments to check the efficiency for our system with changing the number of commercial tags, we saw that the parameter C play an important role in determining the efficiency. As a result, we have succeeded in determining the value of optimal C for our reader to be equal 0.3 as seen in Figures 4.10, 4.11 and 4.12, respectively.

4.5 Summary

In this chapter, we presented a novel Gen2 UHF RFID Reader platform that provided deep vision into the operation of RFID system. In addition, our reader is developed using the new generation of USRP N210 and GNU Radio which can communicate with the commercial tags up to 6 meters. We perform two research studies based on our reader to show the flexibility of our reader testbed. The impact of the capture effect is investigated and we found that the capture effect works with high efficiency for our reader. Furthermore, the implementation for DFSA algorithm is illustrated and we determined the best value of the parameter C for our system which is equal 0.3.

Chapter 5

Conclusion and Future Work

5.1 Conclusion

In this thesis, we have shed light on RFID wireless technology, which has been adopted in many applications and it is supposed to replace the traditional barcode technology in the near future. Since, the RFID-tagged objects do not require being in line-of-sight with the reader for their identification, multiple tags can be read simultaneously. Moreover, the tags are reprogrammable and very cheap. In addition, this field attracted many researchers in recent years.

The implementation of a novel UHF Gen2 RFID reader based on the EPC protocol is presented and its performance is investigated. The system is basically based on the new generation of USRP which called USRP N210 and GNU-Radio Toolkit, thus this platform introduces more capabilities such as the high speed Giga Ethernet connection and the high speed analog to digital and digital to analog converters. As a result, we solved by this platform the problems that the old generation of USRP faced such as the latency issue and timing requirement for the EPC Class-1 Generation-2 protocol. Furthermore, our implementation provided the flexibility to apply modifications to the MAC or the PHY layer behavior, thus helps a lot of researchers for their research work as a real world testbed without the requirement of changes to the existing hardware. We then moved to discuss the implementation of DFSA as an example on the MAC layer to solve the

collision problems which occurred when many tags respond to the reader simultaneously. we have also seen the measurement setup and results for our reader. Performance results show that our implemented reader provides a reading range up to six meters while other implementations based on the same USRP has a reading range no more than 20 cm. Also, we reached the commercial reader reading rang.

We have also seen two research studies based on our reader. The impact of capture effect is checked and illustrated .We notice that our reader can decode one of two tags successfully with high efficiency within the reader range which is 6 m. As well as, the implementation of DFSA algorithm was achieved and the system efficiency is introduced. Indeed, the parameter C is very important in our system and we succeeded to find the best value of parameter C value which is equal 0.3 to get the best efficiency for the Q-algorithm.

.

5.2 Future Work

At the end of this thesis, several topics are still needed to be addressed in the future work. They can be summarized as follows:

- We have used the DFSA to solve the collision problem and we have seen the impact of the parameter C on throughput, thus we can investigate how we can enhance the performance for this algorithm to read the tags as fast as possible. Furthermore, we can investigate the implementation of Code Division Multiple Access (CDMA) based on our reader, including complete analysis on Gen2 system real performance and a comparison between the two implementations [43, 44].
- Recently, there is a new programmable Intel Wireless Identification and Sensing Platform (WISP) tag and it is a family of sensors that are powered and read by UHF RFID readers. Furthermore, WISP tag contains a fully programmable 16 bit microcontroller unlike the commercial tags that look like black boxes. Thus if we implement the operation of commercial tags using WISP tags, then it would be compatible with our reader. As a result, we have a programmable reader and a programmable tag, and this will open the way for a lot of researcher work [16].
- The reading range for our reader is approximately up to 6 meters, as future works we will work to increase the reading range by make a power amplifier on the transmitter side in order to get higher transmission power .In addition, we will make a low noise amplifier on the receiver side to reduce losses [3].

Acronyms and Abbreviation

ACK: Acknowledgment.

ADC: Analog to Digital Converter

ASK: Amplitude-Shift Keying.

CRC: Cyclic Redundancy Check.

CW: Continuous Wave.

DAC: Digital to Analog Converter.

DFSA: Dynamic Frame Slotted ALOHA.

DR: Divided Ratio.

DSB-ASK: Double-Sideband Amplitude-Shift Keying.

EPC Gen2: Electronic product code Generation 2.

EPC: Electronic product code .

ETSI: European Telecommunications Standards Institute.

FCC: Federal Communications Commission.

FPGA: Field-Programmable Gate Array.

GPS: Global Positioning System.

GSM: Global System Mobile.

HF: High Frequency.

IC: Integrated Circle.

IEC: International Electrotechnical Commission.

ISO: International Organization for Standardization.

LF: Low Frequency.

MAC: Media Access Control.

PHY: Physical.

PIE: Pulse-Interval Encoding.

PLF: Backscatter Link Frequency.

PR-ASK: Phase-Reversal Amplitude Shift Keying .

PSK: Phase Shift Keying or Phase Shift Keyed.

PW: Pulse Width.

QREP: Query Repeat.

RF: Radio Frequency .

RFID: Radio-Frequency Identification.

RN16 : 16-bit Random or pseudo-random number.

R-SR: Reader Success Ratio.

RTcal: Reader -to -Tag calibration.

Rx: Receive Path.

SDR: Software Defined Radio.

SN: Slot Number.

SNR: Signal to Noise Ratio.

SSB: Single Sideband .

SSB-ASK: Single-Sideband Amplitude-Shift Keying.

TRcal: Tag -to -Reader calibration.

Tx: Transmit path.

UHF: Ultra High Frequency.

UHD: Universal Hardware Driver.

USRP: Universal Software Radio Peripheral.

WiMAX: Worldwide Interoperability for Microwave Access.

WISP: Wireless Identification and Sensing Platform.

WLAN: Wirless Local Area Network.

Notations

C: The number of collided slots.

E: The number of empty slots.

G: Offer load.

L: Frame Size.

M_h: RF signal envelope ripple (overshoot).

M_l: RF signal envelope ripple (undershoot).

M_s: RF signal level when OFF.

$N_{(EPC\_correct)}$ = The number of EPC that analyzed successfully by the reader.

$N_{(EPC\_error\_v-ACK)}$ = The number of wrong EPC that analyzed by the reader with valid ACK.

$N_{(EPC\_error\_v-ACK)}$ = The number of wrong EPC that analyzed by the reader with invalid ACK.

N_Q = The number of queries that sent from the reader.

n: Number of tags in the population .

P: Probability of finding the tag within the slot of frame L.

Q: Slot-count parameter.

Q_{fp}: Floating point.

s: The number of successful slots.

T_1: Time from Interrogator transmission to Tag response.

T_2: Time from Tag response to Interrogator transmission.

T_3: Time an Interrogator waits, after T1, before it issues another command.

T_4: Minimum time between Interrogator commands.

T_f: RF signal envelope fall time

T_r: RF signal envelope rise time

T_s: Time for an RF signal to settle to within a specified percentage of its final value.

$U\ (n, p)$: Throughput function.

Bibliography

[1] K. Finkenzeller, *RFID Handbook: Radio-Frequency Identification Fundamentals and Applications*, 2nd ed. New York: John Wiley & Sons, 2000.

[2] EPCglobal Inc., EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz-960 MHz, 2013, version 2.0.0 ratified.

[3] G.Smietanka, S.Brato, M. Freudenberg, and J. Götze, "Implementation and extension of a GNU-Radio RFID reader," *Advances in radio science*, vol.11, pp. 107-111, 2013.

[4] Buettner, M. and Wetherall, D.: An Empirical Study of UHF RFID Performance, in: 14th ACM international conference on Mobile computing and networking (MobiCom 08), pp. 223-234, 2008.

[5] Buettner, M.; Wetherall, D., "A software radio-based UHF RFID reader for PHY/MAC experimentation," *RFID (RFID), 2011 IEEE International Conference on*, vol., no., pp.134, 141, 12-14 April 2011.

[6] GNU Radio, "The free and open software radio ecosystem," 2014. [Online]. Available at: http://www.gnuradio.org.[Accessed Saturday November 2014]

[7] Ettus Research, 2014. [Online]. Available at: http://www.ettus.com. [Accessed Saturday November 2014]

[8] C. Law, K. Lee, and Y. K. Sin, "Efficient memoryless protocol for tag identification," in *Proc. DIALM*, 2000, pp. 75-84.

[9] K. H. Rahman, F. Ahmed, S. A. Sagor,and M. G. Mostafa, "An efficient anti-collision technique for radio frequency identification systems," in *Int. Conf. Comp. Sci. Convergence Inform. Technology*, 2007, pp. 1–6.

[10] M. Buettner and D. Wetherall, "A Flexible Software Radio Transceiver for UHF RFID Experimentation," *UW TR: UW-CSE-09-10-02*, 2009.

[11] M. Buettner and D. Wetherall,, "A Gen 2 RFID Monitor Based on the USRP," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 3, pp. 41–47, 2010.

[12] D. De Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, “Challenge: Towards Distributed RFID Sensing with Software-Defined Radio,” *in Proc. of the 16th annual International Conference on Mobile Computing and Networking*, 2010, pp. 97–104.

[13] L. Catarinucci, D. De Donno, M. Guadalupi, F. Ricciato, and L. Tarri-cone, “Performance Analysis of Passive UHF RFID Tags with GNU- radio,” *in Proc. of the IEEE International Symposium on Antennas and Propagation (APSURSI)*, 2011, pp. 541–544

[14] D. De Donno, F. Ricciato, and L. Tarricone, “Listening to Tags: Uplink RFID Measurements with an Open-Source Software-Defined Radio Tool,” *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 1, pp. 109–118, 2013.

[15] A. Briand, B. B. Albert, and E. C. Gurjao, “Complete Software Defined RFID System Using GNU Radio,” *in Proc. of the IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, 2012, pp. 287–291.

[16] Y. Zheng and M. Li, “ZOE: Fast cardinality estimation for large-scale RFID systems.” *in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, 2013, pp. 908–916.

[17] Wireless And Networked Distributed Sensing (WANDS) group, “Open RFID Lab (ORL),” 2014, available at: http://pdcc.ntu.edu.sg/wands/ORL/ .

[18] Bothe, A.; Schraeder, C.; Aschenbruck, N., "An UHF RFID performance evaluation architecture based on traces from a software defined transceiver," *RFID Technology and Applications Conference (RFID-TA), 2014 IEEE* , vol., no., pp.72,77, 8-9 Sept. 2014

[19] N. Abramson, “The Aloha system-another alternative for computer communications,” in *Amer. Federation Inf. Process. Societies*, 1970, vol. 37, pp. 281-285.

[20] N. Abramson, “Development of the AlohaNet,” in *IEEE Trans. Inform. Theory*, 1985, vol. IT-31, pp. 119-23.

[21] S. S. L. L. Kleinrock, “Packet switching in a multi-access broadcast channel: Performance evaluation,” *IEEE Transactions on Communications*, vol. 23, no. 4. pp. 410–423, 1975.

[22] K. Finkenzeller, *RFID HANDBOOK* (*3rd ED), Fundamentals and Applications in Contactless Smart Cards and Identification*. West Sussex PO19 8SQ, England: John Wiley and Sons Ltd., 2003.

[23] F. C. Schoute, "Dynamic frame length aloha," *IEEE Transactions On Communications*, vol. COM-31, no. 4., pp. 565–569, 1983.

[24] H. Vogt, "Efficient object identification with passive rfid tags," in *Proc. Int. Conf. Pervasive Computing*, (Zurich, Switzerland), pp. 98—-113, August 2002.

[25] C. Floerkemeier, "Bayesian transmission strategy for framed aloha based rfid protocols*," in Proceedings of 2007 IEEE International Conference on RFID,* (Gaylord Texan Resort, Grapevine, TX, USA), pp. 228—-235, March 2007.

[26] C. Floerkemeier, *Infrastructure Support for RFID Systems*. PhD thesis, ETH University, 2006.

[27] M. K. B. Zhen and M. Shimizu, "Framed aloha for multiple rfid objects identification*," IEICE Transactions on Communications*, vol. E80-B, no. 3., pp. 991—-999, 2005.

[28] K. C.-D.-B. S. H.-S. L. C.-S. P. J.-S. C. X. Fan, I. Song, "Gen2-based tag anti-collision algorithms using chebyshev's inequality and adjustable frame size," *ETRI Journal*, vol. 30, no. 5., pp. 653—-662, 2008.

[29] W.-T. Chen, "An accurate tag estimate method for improving the performance of an rfid anticollision algorithm based on dynamic frame length aloha," *IEEE Transactions on Automation Science AND Engineering*, vol. 6, no. 1., pp. 9–15,2009.

[30] C. Floerkemeier, "Transmission control scheme for fast rfid object identification*," in Proceedings of the Fourth Annual International Conference on Pervasive Computing and Communications Workshops* (PERCOMW'06), (Pisa, Italy), March 2006.

[31] J. T.-H. M. J. W. D. Liu, Z. Wang, "Aloha algorithm considering the slot duration difference in rfid system," *in Proceedings of the 2009 IEEE International Conference on RFID,* (Orlando, USA), pp. 56–63, April 2009.

[32] Brown, D.E.RFID Implementation.NY:McGraw-Hill,2007.

[33] "Regulatory status for using RFID in the UHF spectrum." *Frequency Regulations UHF*.14 October 2014.EPCglobal, Web. 20 Jan 2015.Available at:

<http://www.gs1.org/docs/epcglobal/UHF_Regulations.pdf>

[34] Stevan Preradovic and Nemai Karmakar (2011). Fully Printable Chipless RFID Tag, Advanced Radio Frequency Identification Design and Applications.

Available from: http://cdn.intechweb.org/pdfs/14423.pdf

[35] Banks, J., D. Hanny, M. A. Pachano, and L. G. Thompson. *RFID Applied*. Hoboken, NJ: John Wiley & Sons, 2007.

[36] RFID Journal home page, "The basics of RFID technology". Available at: http://www.rfidjournal.com/article/articleview/1337/1/129/

[37] Hunt, V. D., A. Puglia, and M. Puglia. *RFID: A Guide to Radio Frequency Identification*.Hoboken, NJ: Wiley-Interscience, 2007.

[38] "About ISO." *ISO*. 2015. International Organization for Standardization, Web. 2 Feb 2015.Available at: http://www.iso.org/iso/about.htm

[39] Azambuja, M.; Marcon, C.A.M.; Hessel, F.P., "Survey of Standardized ISO 18000-6 RFID Anti-collision Protocols," *Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference on* , vol., no., pp.468,473, 25-31 Aug. 2008.

[40] "The Labs." AUTO-ID LABS. Auto-ID Labs, Web. 6 Feb 2015.Available at:

http://www.autoidlabs.org/the-labs/page.html.

[41] Rahman, K.H.; Ahmed, F.; Sagor, S.A.; Mostafa, M.G., "An efficient anti-collision technique for Radio Frequency Identification Systems," *Computer and information technology, 2007. iccit 2007. 10th international conference on* , vol., no., pp.1,6, 27-29 Dec. 2007.

[42] S. Kaewsirisin, P. Supanakoon, S. Promwong, N. Sukutamtanti, U. Ketprom, "Performance study of dynamic framed slotted Aloha for RFID systems," in *Elect. Eng. Electron. Comput. Telecommun. Inform. Technology*, 2008, vol. 1, pp. 413-416.

[43] Vahedi, E.; Ward, R.K.; Blake, I.F., "Performance Analysis of RFID Protocols: CDMA Versus the Standard EPC Gen-2," *Automation Science and Engineering, IEEE Transactions on*, vol.11, no.4, pp.1250,1261, Oct. 2014

[44] S□olić, P.; Radić, J.; Roz□ić, N., "Energy Efficient Tag Estimation Method for ALOHA-Based RFID Systems," *Sensors Journal, IEEE* , vol.14, no.10, pp.3637,3647, Oct. 2014.

[45] M. Dillinger, K. Madani and N. Alonistioti, *Software Defined Radio: Architectures,*

Systems and Functions. Wiley & Sons, 2003.

[46] F. Hamza, (2008). *The USRP Under 1.5X Magnifying Lens*

http://gnuradio.org/redmine/attachments/129/USRP_Documentation.pdf.

[47] Eric Blossom et al. *Welcome to GNU Radio*. 2014. URL: http://gnuradio.org/redmine/projects/gnuradio/wiki (visited on 17/2/2015).

[48] Alien Technology, Morgan Hill, CA, USA, “Alien Technology”, [Online]. Available http://www.alientechnology.com(visited on 17/2/2015).

[49] Jae Sung Choi; Mingon Kang; Elmasri, R.; Engels, D.W., "Investigation of impact factors for various performances of passive UHF RFID system," *RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference on* , vol., no., pp.152,159, 15-16 Sept. 2011

الموضوع: تطوير قارئ تجريبي باستخدام برنامج تعريف الراديو للجيل الثاني من تقنية تحديد الهوية باستخدام الامواج الكهرومغناطيسية (RFID)

إعداد: مهران نضال فؤاد جازي

إشراف: د. سامر بالي

الملخص

تكنولوجيا تحديد الهوية بالامواج الكهرومغناطيسية (RFID) اللاسلكيه اصبحت الاداه الاكثر شيوعا واهميه، والتي يتم استخدامها في العديد من التطبيقات على سبيل المثال في السلاسل اللوجستيه،التتبع ،وتحديد مواقع الوحدات. (RFID) لديها القدره على قراءه الوحدات من دون الحاجه الى خط الافق.بالاضافه الى ذلك، يتم استخدام (RFID) للتطبيقات التي تتطلب مسافات طويله مقارنه بنظام (Barcode). وكذلك يمكن ان يتم اعاده برمجه البطاقه ,والسعر يكون اقل ما يمكن.

كما لا تزال تكنوجيا (RFID) تنمو بسرعه يبقى هناك العديد من القضايا والتحديات المختلفه . يواجه الباحثون في هذا الحقل ان القاريء التجاري يشبه الصندوق الاسود والذي يعاني من التكوين المحدود ،وبالتالي التعديلات على طبقه (MAC او PHY) ليست ممكنه.

في هذه الاطروحه، تم تقديم تنفيذ جديد لتحديد الهويه بترددات الراديو للقارىء على اساس معيار الجيل الثاني ل EPC. ويتم هذا التنفيذ بناءا على الجيل الجديد من (USRP N210) والتي تم برمجتها باستخدام برنامج تعريف الراديو (SDR) المبني على اطار (GNU Radio). بالاضافه الى ذلك ، تم التحقق من مصداقيه اداء القارىء المقترح الذي يعمل تحت الترا الترددات العاليه (UHF) من خلال قراءه البطاقات التجاريه .ووجد ان اداء القاري هو جيد مثل اداء القارىء (UHF RFID) التجاريه .القاريء يمكن استخدامه في الاوساط البحثيه للعمل البحثي. .تم استخدام القاريء والبطاقات التجاريه لدراسه تاثير ما يسمى تاثير الالتقاط . بالاضافه الى ذلك ، تم التحقيق في اداء خوارزميه الاطار الديناميكي المقسم (DFSA) .