Open Platform Semi-Passive Ultra High Frenquency Radio Frequency Identification Tag

by

Tzu Hao Li

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

School of Information Technology and Engineering
Faculty of Engineering
University of Ottawa

© Tzu Hao Li, Ottawa, Canada, 2011

Abstract

Radio frequency identification (RFID) is a rapidly emerging technology that enables automatic remote identification of objects. Passive and semi-passive RFID systems can be distinguished from other forms of wireless systems, because the RFID tags (transponders) communicate by way of backscatter. In addition, passive tags derive their energy from the RF energy emitted by the reader. RFID technology can provide a fully automated data capture and analysis system.

Compared to a passive RFID system, an open platform semi-passive UHF RFID tag can provide identification, security, low-power (compared to a wireless sensor network(WSN)), medium range and medium processing speed. However, the field of semi-passive RFID is still under development, and has yet there are no open development platforms available.

This thesis develops a prototype of a semi-passive UHF RFID tag that is compatible with the leading UHF RFID standard EPCglobal Gen 2 Class 1. I alsot has the flexible I^2C and analog digital converter(ADC) interface, which allows the additional of external analog and digital sensors. The sensor data can be read by microcontroller and stored at memory. Standard reader can get sensor data by sending QUERY and READ command to tag.

Test results of our open platform semi-passive UHF RFID tag demonstrated that it can achieve a read rate above 50% when an open platform semi-passive UHF RFID tag is placed four meters from the reader antenna and the reader output power is set to 21 dBm. In addition, the proposed semi-passive open platform RFID tag consumes very little power (4.9 mA in 2V with system frequency set to 8MHz).

Acknowledgements

I would like to thank to my supervisor: Dr. Miodrag Bolić. He gived me the opportunity to join of the RFID research group. With his encouragement, guidance and suport from the initial to the final level enabled me to develop and understanding of the subject. It is my great honour to work with Dr. Miodrag Bolić. Special thanks to my thesis committee: Dr. Chung-Horng Lung and Dr. Mustapha Yagoub for their time and comments. Also, thanks to Alexey Borisenko for helping me to run the exeriment and comment out my thesis.

Lastly, I offer my thanks and appreciations to my parents and colleagues who willingly helped me out with their abilities and supported me in any respect during the completion of the thesis.

Tzu Hao Li

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Radio frequency identification (RFID) technology is automatic, wireless data capturing functionality that uses radio frequency waves to transfer data between a reader (interrogator) and a tag (transponder). The tag is normally attached to an item in order to identify, categorize and track it. RFID systems have attracted a lot of attention due to their potential ability to identify an object without contact or line of sight. RFID systems operate at several frequency bands from 125 KHz to 5.6 GHz. The RFID systems that operate at 125/134 KHz are classified as low frequency (LF), 13.56MHz as high frequency (HF), 303 MHz to 2.4GHz as ultra high frequency (UHF), and 2.4GHz and above as super high frequency (SHF)[1]. The reason for several frequency bands for the RFID system is that one band cannot provide everthing required in terms of read range, environmental factors, data rate, etc. Each frequency provides unique performance characteristics for various usage scenarios. Table 1.1 summarizes the frequency bands and corresponding applications.

Table 1.1: RFID frequency and applications[1]

Classification	**Frequency Band**	**Applications**
LF	125/134 KHz	Access Control, Animal-ID
HF	13.56 MHz	Access Control
UHF	303/433MHz	Transport
	866∼928 MHz	Transport, Inventory, Supply chain management
SHF	2.45 GHz	Transport
	5.6GHz	Under development

Typically, RFID systems consist of a reader, tags and antennas, which together allow information and commands to be exchanged using wireless transmission. Figure 1.1 shows a typical RFID system. All tags contain a unique ID that is read by the reader. In general, engineers describe the communication channel from reader to tag as the forward link and the communication channel from tag to reader as the reverse link [5]. RFID systems can be described as special types of sensors that can detect an item's name. The tag can be classified as one of three types: passive, semi-passive, or active. The passive tag is battery-less and extracts power from the RF signal transmitted by the reader. The semi-passive tag incorporates a battery-assisted-circuit (BAC) to power the tag IC, however, the battery is not used to broadcast or amplify a signal to the reader[6]. Communication from passive or semi-passive UHF tags to the readers is performed using backscatter modulation [7]. Active tags are full-fledged radios, integrating an RF transmitter, battery, receiver and control circuitry [5]. They do not use backscatter modulation, but generate their own signal and transmit it to the reader autonomously.

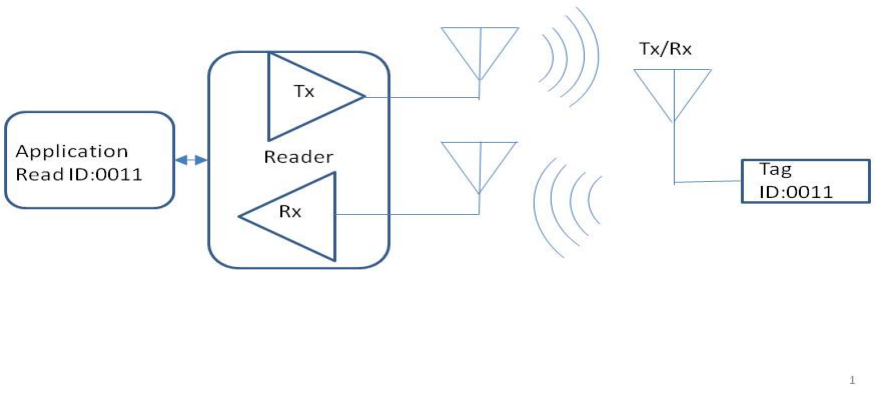

Figure 1.1: A typical RFID system

Continuous wireless sensor systems are of important for safety in many fields and wireless sensors technologies have been widely adapted for use in numerous practical applications. The current capabilities of continuous sensing, detecting, identification, localization and ease of deployment are a considerable improvement over traditional wired sensor technology. UHF semi-passive RFID is one of these wireless sensor technologies. A semi-passive UHF RFID sensor platform can provide middle operating range compared to

a passive RFID system, and low-power compared to a wireless sensor network. Today's RFID passive systems have relatively low reading accuracy, due to a combination of factors including low power of operation, distance between reader and tags, number of tags, distance between tags, and material [8]. This presents a major obstacle for a wider adoption of RFID systems. If we also consider that RFID technology is frequently employed in security and privacy-sensitive areas, with important problems still awaiting resolution [9], it is not surprising that RFID has not achieved the success that many experts have expected.

The semi-passive RFID field is still under development, and there are no open development testing platforms available. It makes it difficult for researchers to develop and evaluate their ideas in practical scenarios. Thus, they either use commercially available UHF RFID tags and readers, or resort to simulation studies. However, simulation results are often different than actual results due to variations in deployment environments. Commercially available UHF RFID tags and readers are closed devices. They do not allow modification of the link layer protocol or customization of the interface for external devices. The tags have application-specific integrated circuits application-specific integrated circuits (ASIC), and are not programmable.

There has been a significant research and development effort, much of it still ongoing, aimed at overcoming the above mentioned challenges. Other research fronts have emerged as well. Wireless sensor network (WSN) is an example of a wireless sensor technology that has been applied to many practical wireless sensing applications. These devices have an onboard RF transmitter to generate carrier frequency, enabling them to transmit data to the base station. WSN devices should have minimal transmit time in order to limit energy consumption and achieve an acceptable device operating life time [10]. As WSN uses a multi-hop algorithm, for reliable communication it must either transmit more information or add extra devices; both these methods increase system and network complexity. Network interference is another issue for this solution, since WSN tries to provide optimal service to increase devices' operating life time, and does not explicitly consider deploying many devices in a small area. The issues of power consumption, no unique naming and no standard routing protocol make them unsuitable for certain applications.

RFID technology is another short range method for wireless sensor applications. One of these applications is called wireless sensor identification platform (WISP). WISP device are battery-less, and work with the EPCglobal Gen 2 Class 1 standard protocol [11]. Passive RFID sensor platforms solved the issues of WSN but their short range and low

processing power limit extensibility and usability. There are several existing semi-passive development platforms, including TU Graz tags [12], CAEN tags [13], and Condex tags [14]. These also comply with the EPCglobal Gen 2 Class 1 protocol. TU Graz tag is an FPGA-based development platform. FPGA was chosen to create the development platform to allow for easy integration of additional devices and support extensions. However, because of this, it also consumed a lot of power. CAEN and Condex were designed for low cost, low power platforms, and they were implemented based on a microcontroller platform. Only CANE had an integrated temperature sensor. The development tags developed by CAEN and Condex were proving concepts for research projects, and are not available for purchase. These three semi-passive development platforms are not open source platforms, and researchers cannot get detailed hardware and software information. Software is limited to purchasers and can not be published without the company's permission.

1.1 Thesis statement

Automated data collection with a well accepted standard is one of the advantages that RFID systems have over many other competing technologies [15]. An infrastructure with open platform semi-passive RFID sensor tags will enable many important activities including (1) development and construction of RFID sensor networks, (2) analysis and evaluation of various RFID protocols in terms of tag performance and power consumption, (3) development, implementation and testing of new RFID protocols and security and privacy schemes, (4) development of advanced techniques for RFID signal processing, and (5) antenna design for tags.

The objective of this thesis is to create a new open hardware and open source platform for semi-passive RFID tags, and thereby advance RFID technology. This research also addresses the limitations of existing testing platforms. The objectives are (i) to develop an extensible hardware architecture for semi-passive RFID tags and (ii) to create an environment for easy programming and testing. The hardware will be extensible in that any sensor could be attached to the tag via a standard interface. We implement an open platform semi-passive UHF RFID tag, and the result of the analysis demonstrate the viability and application of this testing platform. A semi-passive UHF RFID sensor tag can track temperature and identify objects, and the wireless nature of the network increases the flexibility and mobility of the subject wearing them. A semi-passive UHF RFID system uses the backscattering method, so the device does not need an RF trans-

mitter to transmit data and it does not waste energy when wirelessly transmitting data to a base station. A well defined UHF RFID standard could seamlessly integrate large numbers of proposed devices into an existing UHF RFID network, and easily integrate sensors to increase its functionality.

In summary, members of today's large RFID research community do not have a readily available and easily managed hardware platform on which to evaluate their work. The closed nature of commercial RFID systems is also an obstacle from an educational viewpoint; students and aspiring researchers would benefit from a platform that allowed them to study various RFID problems with greater flexibility. We propose to address this through the research described herein.

As this platform is the first prototype board, and budget and time are limited, we required to reduce some of the functionality and supporting modes of the platform. Thus the open platform UHF semi-passive RFID sensor tag is only tested in North American frequency bands. Another limitation of the device is that the reader transmitted signal and backscattering signals rate are fixed to 40 KHz and 256KHz/Miller 4, respectively. We intend to expand the functionality and supporting modes in future work.

To prove our open platform semi-passive UHF RFID tag can operate as a commercially available standard semi-passive tag, we are conducting several experiments to test the overall performance of tag with a commercially available EPCglobal Gen 2 Class 1 RFID reader. The results allow us to evaluate our open platform semi-passive RFID tag. The details of the experiments are presented in chapter 7.

1.2 Contribution

In this thesis, we designed new semi-passive UHF RFID tag. The work involved creating a printed circuit board (PCB),

firmware, and application software to meet the following objectives: the tag must be compatible with EPC Class 1 Generation 2 standard, must be low power, and must be expendable (to allow the addition of compatible sensors). Two papers were published based on this work, [16] and [17].

The open platform semi-passive UHF RFID tag has been designed to provide a friendly development environment for researchers. According to the experimental results, our tag is capable of operating as a commercially available semi-passive UHF RFID tag. We also demonstrated the RFID sensor network to prove the expandability of the open platform semi-passive UHF RFID tag.

1.3 Thesis organization

This section provides a brief outline of the content of the subsequent chapters. The thesis is organized as follows.

Chapter 2 provides background information on the issues and concepts addressed with in the thesis. This includes an introduction to wireless systems, such as RFID, and WSN, and a review of existing applications.

Chapter 3 describes the performance of passive and semi-passive RFID systems. It demonstrates the performance of non-ideal UHF RFID systems.

Chapter 4 presents the hardware design of the semi-passive UHF RFID sensor tag. An explanation of the hardware architecture is followed by section introducing each component of the device.

Chapter 5 demonstrates the software architecture for this open platform project. The firmware design for the microcontroller is presented first, followed by the graphic user interface that allows user to control and access tag data.

Chapter 6 presents several applications for this open platform RFID tag.

Chapter 7 shows the outcomes of the testing and the analysis of the results to obtain a representative set of performance measures. A comparison is made with a commercially available semi-passive RFID tag.

The conclusion of the thesis is presented in Chapter 8. It includes an outline the contribution of the thesis and suggests possible future work.

Chapter 2

Background

2.1 Short range wireless system

The definition of short range wireless system [18] is classified and based on the wireless communication range of two devices. Typically, short range wireless system communication range is from a few centimeters up to several hundred meters. In general, short range wireless systems are low power, low cost and small, and they are focused on indoor application. As well, most short range wireless systems are operating in unlicensed bands, such as the industrial, scientific and medical (ISM) bandwidth. Short range wireless system are ubiquitous in modern society nowadays. The RFID system is one of these short range wireless systems.

2.2 RFID

RFID is a rapidly emerging technology for the automatic remote identification of objects [5] The basic principles of communication by means of reflected power have been known for more than 60 years [19], but since the cost of ASICs has decreased during the past two decades, the cost-performance ratio has become mature enough for RFID to be widely accepted. The clear advantages of this technology over traditional identification methods, (e.g. bar code), resulted in numerous research and commercialization efforts in the early 2000s. RFID tags are distinguishable from other short range wireless systems because they communicate by way of tags backscatter reader signals and the tags derive some or all of their energy from the RF energy emitted by the reader [20]. Most RFID applications involve a large number of densely co-located tags that are in the field of

view of the reader simultaneously.

2.2.1 Ideal passive/semi-passive RFID System

An ideal RFID system can be characterized and summarized as follows [16]:

1. The reader read zone is well defined. It should be able to read all tags inside the read zone when it sends out a query command. And the reader should not read any tags outside the read zone.
2. Reader and tags communication should not be affected by physical orientation.
3. Reader and tags communication should not be affected by close objects.
4. Reader and tags communication should not be affected by the environment.
5. Reader and tags communication should be collision free and the reader should be able to read all tags at once.

In the ideal RFID system, the reader would be able to read tags as long as tags are inside the read zone, and it would not read stray tags. Even though this ideal RFID system is unrealistic in practice. It can help us evaluate current RFID systems and focus on their weaknesses.

2.2.2 EPCglobal Class 1 Gen 2 protocol

Due to the different frequency bands and tag types of RFID systems, several organizations including EPCglobal and ISO have been working on standardization. The electronic product code (EPC) Gen 2 Class 1 RFID system was adopted as an international standard by ISO/IEC, as ISO 18000-6 [21]. EPCglobal Gen 2 Class 1 RFID systems operate in the UHF range of 860 to 960 MHz. The EPCglobal Gen 2 Class 1 specification describes the communication between an RFID tag and the RFID reader, and specifies the air interface. It adapted "Reader Talk First" principles whereby readers always issue commands and tags always listen and respond to these commands. The objective of this protocol is to singulate a tag in a multiple tag environment, in order to read its identity or other information stored in its memory [22]. Table 2.1 summarizes the features of UHF EPCglobal Gen 2 Class 1. It is becoming the most accepted protocol in UHF passive and semi-passive RFID systems. The EPC code is intended to be the next generation

of the barcode (or universal product code (UPC)) which is found on virtually on every consumer item today [3]. Figure 2.1 illustrates the 96 bit EPC layout. The purpose of EPC is to provide an unique ID to any item. EPC is comprised of four parts: the header, the EPC manager field, the object class field and the serial number field. EPC length is flexible, and it can vary from 64 bits to 496 bits or more. This capability allows EPC to uniquely identify all items.

- Header: EPC's version number.
- EPC manager field: Manufacture number.
- Object class field: Class of product.
- Serial number field: Unique ID of this item, separate item belongs to same class of product.

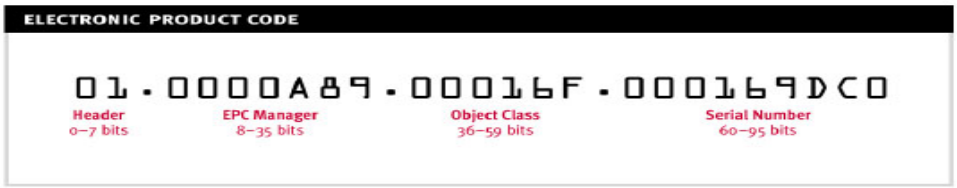

Figure 2.1: 96 bit EPC layout [3]

Table 2.1: UHF EPCglobal Class 1 Gen 2 Features [2]

Requirement	**Gen 2 Capability**
Global regulatory compliance	Europe, North America, Japan, etc
Operation in noisy environments	Multiple sessions, dense reader modes
Fast operation	$>$ 1600 tags/sec USA, 600 tags/sec Europe
Privacy protection	EPC code not broadcasted, 32-bit kill password
Memory write capability	$>$ 7 tag/second write rate, optional user memory
Group searches & filter	Flexible select command

2.3 Related work

Wireless sensor systems are rapidly emerging systems for automatic remote monitoring. Table 2.2 illustrates some of the short range wireless technologies and their corresponding products. Every technology has its advantages and weak points. For example, WISP has an unlimited device life time, but it can only operate less than three meters, while WSN, active and semi-passive RFID systems device life is limited by battery.

2.3.1 RFID system

Several research efforts have focused on the hardware development of programmable RFID readers and tags. Angerer et. al. [23] presented a dual frequency RFID reader test bed that allows some modification of reader functionality. Ying [24] developed a verification platform for a Gen 2 RFID reader based on a soft-core processor residing within an FPGA. Buettner et. al. [25] developed a GNU radio based monitor for protocol and communication analysis of Gen 2 RFID systems. Modifiable RFID tag hardware platforms with potential for incorporation of sensors are presented in [26], [27].

Passive RFID system

One of the existing passive RFID systems is WISP designed by the Intel Research group. It is an open platform RFID programmable passive sensor tag [27], and WISP contains an onboard microcontroller and digital sensors. WISP was designed as an EPCglobal Gen 2 Class 1 passive RFID tag. As it is a battery-less, WISP can provide a maintenance-free wireless identify and sensor network; users do not need to replace the battery. However, the trade-off of battery-less design is less operating range; WISP's is about ten feet (three meters). In most wireless sensor networks, this operating range is not acceptable as it could only send the sensor data 1 bit per query command, since it needs to collect enough power to power up the sensor. This low processing ability limits its widespread use. As well, due to very low processing power, the WISP firmware can not handle complicated signal processing or complex algorithm. WISP does not support READ, WRITE commands.

Semi-passive RFID system

The semi-passive sensor tag is another approach using RFID technologies in wireless systems. TU Graz UHF Demotag designed by IAIK is a semi-passive re-programmable

Table 2.2: Wireless sensor system devices

	WISP	TelosB	Identec I-Q310	TU Graz
Wireless technology	Passive UHF RFID	ZigBee	active RFID	Semi-passive UHF RFID
Protocol	EPCglobal C1 G2	ZigBee	ISO18000-7	EPCglobal C1 G2
Power consumption	less than 1 mA	25 mA	17 - 20 mA	38 mA
Range up to (m)	3	50	100	15
Network topology	Star	Star and Mesh	Star and broadcast	Star
Anti-collision algorithm	Slotted Aloha	Contention based CSMA/CA contention free GTS	ISO18000-7	Slotted Aloha
Unique naming	Object naming service and assign unique address when manufacture	none	Object naming service and assign unique address when manufacture	Object naming service and assign unique address when manufacture
Frequency	902-928MHz	2.4GHz	433MHz	860-928MHz
Lifetime	Unlimited	Battery life cycle	Battery life cycle	Battery life cycle
Max Symbol Rate	64Kbps	62.5Kbps	27.7Kbps	100Kbps (FM0)
Extensibility	Open Platform	Open Platform	No	Limited

RFID tag. It contains an onboard microcontroller and supports the EPCglobal Gen 2 Class 1 protocol. As it is semi-passive, TU Graz has an onboard power source to power the microcontroller. This provides longer operating range, greater processing ability, and extension support, (e.g. security or additional peripherals) compared to passive UHF RFID systems. The TU Graz tag is mainly designed for security functionality as it requires high speed processing and consumes 38 mA. This tag does not include design detail; schematic or layout are not provided. As they did not reveal their analog front-end or digital sections, we can not evaluate or modify their design to meet research project requirements. The price of TU Graz UHF Demo tags is approximately $ 650 to $750 per tag.

The EM Microelectronic company has many specialized RFID components for different RFID applications. One of their products is a battery-assisted passive contactless integrated circuit (IC) which help users design semi-passive RFID applications. The EM battery-assisted passive contactless integrated circuit is available in ASIC architecture. This chip is fully EPCglobal Gen 2 Class 1 compliant and supports all forward and return link data rates [28]. It can operate in both passive and semi-passive modes. All logic circuits are built inside the chipset and are non changeable; thus this chipset has no hardware or software flexibility. It has a serial bus interface to allow for an antenna. Researchers can not use this chipset to understand UHF RFID architecture nor alter the hardware and software design.

Active RFID system

Active RFID system is another RFID technology that can be applied in wireless sensor network. It has a battery and, an RF transmitter, and provides the longest transmission range compared to passive and semi-passive RFID tags. IdentecI-Q310 is one of the existing products adapted active RFID technology. It is ISO 18000-7 standard compliant. As it contains an RF transmitter, IdentecI-Q310 consumes more power than semi-passive tag (approximately 17 to 20 mA in working mode), and requires extra 0 dBm power for transmitting purposes. It is not a totally open platform, so the user does not have full access to the source code. The ISO 18000-7 standard [29] proposes framed slotted ALOHA as an anti-collision protocol. Even though the ISO 18000-7 standard provide an anti-collision algorithm based on a frame length adaption mechanism, a particular one is not specified, leaving it up to the vendor [30].

2.3.2 ZigBee

ZigBee is another short range wireless technology. It defines a set of communication protocols for low data rate short range wireless networking. ZigBee based wireless devices operate in the 868 to 870 MHz, 902 to 928 MHz, and 2.4 to 2.5GHz frequency bands. The maximum symbol rate is 62.5 K bits per second. ZigBee is mainly intended for low data rate, low cost, and low power application. Its technology is a wireless mesh networking standard. According to this standard, Zigbee devices have three roles: router, coordinator, and end device. A Zigbee router is capable of relaying messages, and a Zigbee coordinator is the principal controller of a personal area network and router functionality. A ZigBee end device has the smallest memory size and fewest processing capabilities and features; it does not act as a coordinator or router. An end device is normally the least expensive device in the network [31].

An existing development platform adapting Zigbee technology is the Code Blue wireless sensor network developed by Harvard university [10]. It is a vital signs wireless sensor device that can measure a patient's heart beat rate, and is wirelessly transmitted the data to a local server. The Code Blue devices have an integrated RF transmitter, which requires power to transmit data to a base station. The devices typically consume approximately 23 mA in receive mode [32]. The issues of power consumption, and lack of unique naming capability make these devices unsuitable for certain applications. Another drawback for WSN technology is that it is designed for middle and long range transmission. If many WSN devices are placed in a small area, (e.g. several sensor devices on a human body), the air traffic collision will reduce system data throughput and efficiency.

2.4 Open source platform

An open platform in software architecture is a system based on an open standard interface that allow users to study, modify, integrate, distribute, make, and use the design or hardware based on that design [33]. Ideally, open source platforms adapt commercially available components and highly standardized protocols to allow user to easily reproduce the open source hardware. Open source platforms gives total freedom to use the platform, and allow them to share their knowledge through the open source society. Using an open source platform, researchers can build prototype systems, and since open platform use open standard interfaces, the open platform is flexible enough to integrate with other

systems.

Adapting and developing open platform and open source can benefit both the authors and the community. An open source platform design has no black box inside the design. By releasing the design and source code available, everyone can perform a code review and verify the correctness of the algorithm. Open source platform provide the potential for unlimited evolution and improvement, as application life is not dependent on authors or the original developing team. An open source platform grants the right to redistribute modifications and improvements, which allows modified software to be shared by communities. Researchers can re-use the open source platform without worrying violating patents, and this is significant motivation for people to use them.

One of the most successful open source platforms is Linux, which is part of the Unix-like family using the Linux kernel [34]. Linux is an open platform that can be installed on a wide range of hardware, including smart phones, embedded systems, video game consoles, personal computers and work station servers. Linux is one of the greatest open source platform software functionalities license by GNU General Public License.

TelosB wireless mote, developed by the University of California at Berkely is another successful open source platform. It is used in wireless sensor network application. TelosB mote has an IEEE 802.15 radio with an integrated antenna. Its block diagram, schematics, and source code were published for the research community. TelosB mote is provided as an open platform for wireless sensor networks, and researcher can study and modify both the software and hardware design to meet their requirements. Researchers can also freely publish their work based on TelosB mote. This open source platform helps to develop and evaluate wireless sensor network technology.

Chapter 3

Performance of passive and semi-passive RFID system

This chapter explains the performance of passive and semi-passive RFID systems. To do this, it is important to understand the performance of non-ideal RFID systems. There is a limited amount of experiments performed, the analysis and comparisons of the read ranges and rates of passive and semi-passive RFID systems together. A large body of research work has produced several research papers dealing with performance of RFID systems. However, they focus on the tag reflection coefficient of the nearby material [5], tag impedance matching [35], reflected environment [36][37][38], and tag chip sensitivity threshold [39]. In addition, only maximum read range is considered in these papers. Furthermore, not much has been published on analyzing the performance of passive and semi-passive RFID systems with bi-static or mono-static reader antenna. The analysis of non-ideal RFID systems can help us explain the weak points of RFID passive and semi-passive systems.

The simplest practical RFID system from an analysis viewpoint consists of a single stationary reader and a single stationary tag. Our setup for examining the performance of such a system consists of an EPCglobal Gen 2 Class 1 compliant tag and a reader. The EPCglobal Gen 2 Class 1 standard uses a dynamic frame slotted Aloha based anti-collision protocol, which enables multiple tags to communicate with a single reader. In this protocol, the reader requests tags to reply to its commands in defined time slots. The reader specifies a fixed number of *slots* in an 'Inventory Round' or a 'Query Round'. An inventory round is defined as a single cycle of an algorithm by which a reader attempts to singulate the tags within its environment. Singulation is defined as the process of

identifying a single tag and reading its ID number. A Query Round begins with a *Query command* which specifies a so-called Q parameter where the number of slots is equal to 2^Q. Each tag in a population then selects a random slot from these slots to communicate with the reader. The reader then sends out successive *Query Rep* commands which designate the start of each slot. A reader could also send *Query Adjust* commands that dynamically increase or decrease the number of slots in the round. In its chosen slot, the tag replies with a 16-bit random number (RN16) using backscatter modulation. Upon successful reception of RN16, the reader sends an *Acknowledge* command with the same RN16 back to the tag. If this number matches the number that the tag originally sent out, the tag backscatters a protocol control (PC) header, followed by its EPC ID and a 16 bit CRC.

In our experimental setup, the EPCglobal Gen 2 Class 1 reader is attached to a host computer that is capable of monitoring the read rate of a detected tag i.e. the ratio of the number of times a tag responded successfully to the number of Query Rounds sent out by the reader. We use a commercial UHF EPCglobal Gen 2 Class 1 passive dipole tag. The reader transmits at a power of 30 dBm over a 6 dBi gain circularly polarized antenna. In addition we deploy a sniffer device in the proximity of the tag, to examine the actual communication taking place over the wireless channel. This sniffer device is connected to an oscilloscope that stores snapshots of the baseband signals going between the tag and the reader. Figure 3.1 shows the captured waveform for single reader, single tag scenario, where "QueryRep" commands indicate a reader-tag communication slots are present. In its selected slot, the tag backscatters an RN16 as seen in Figure 3.1. This is then followed by transmission of the Acknowledge command by the reader and the subsequent backscattering of the EPC ID by the tag.

3.1 Background studies

There are several papers in which the performance of passive RFID systems is based on read range or power efficiency. The following background provides a brief introduction to passive RFID system performance for those unfamiliar with antenna theory. Here, we illustrate the transmission power between the reader and the tag in detail.

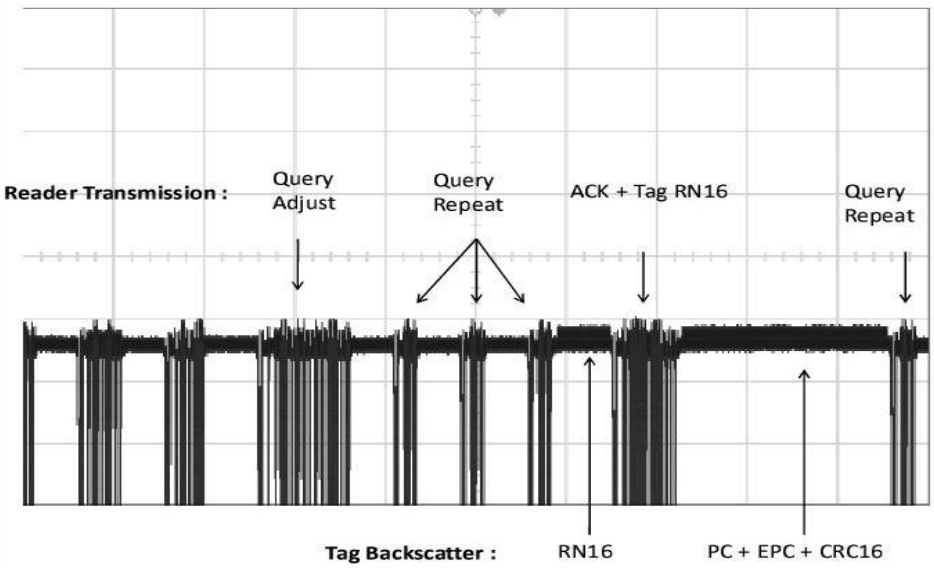

Figure 3.1: Communication between a single Gen 2 reader and single Gen 2 tag

3.1.1 Path Loss

Link budget refers to the amount of power needed to successfully deliver transmitted data to a receiver across a wireless link. The power received by receiver can be calculated from Friis Equation 3.1:

$$P_r = (1 - |\Gamma_t|^2) P_t G_t G_r (\frac{\lambda}{4\pi r})^2 \tag{3.1}$$

where P_r is power at the receiver, P_t is transmitted power, G_t is the gain of the transmitter antenna, G_r is the gain of the receiver antenna, λ is the wavelength, $|\Gamma_t|$ is the transmitter reflection coefficient and r is the distance between the transmitter and the receiver. It shows that received power is inversely proportional to squared distance.

The RFID reader transmit power is set by a combination of practicality and regulation, In North America, the maximum power allowed for operation in the frequency band 902-928 MHz without license is 36 dBm including antenna gain. Passive tag is simple as it extracts the energy from the RF signal transmitted by the reader. The forward link limited range depends on the turn-on threshold of tag IC.

Since a passive tag does not have an onboard battery, the transmitted power associated with the tag is only part of the energy the tag receives from the forward link. If T_b is the backscatter transmission loss (power loss in IC and impedance mismatch), then

the reverse link budget is given by:

$$P_{r,reader} = (1 - |\Gamma_t|^2)(1 - |\Gamma_r|^2)T_b P_{t,reader} G_t^2 G_r^2 (\frac{\lambda}{4\pi r})^4$$

where $|\Gamma_t|$ is the receiver reflection coefficient. Here, the reader antenna sensitivity plays an important role in the reverse link limited range. In most passive RFID systems, the read range is limited by the forward link limiting the range of the signal so that the tag would not be able to extract enough energy to turn-on the IC [40].

3.1.2 Backscatter Transmission loss

The maximum power of the transmitter/receiver is achieved when the antenna and IC have the same impedance[40]. This can be described by the maximum power transfer theorem:

$$\tau = \frac{4R_{load}R_{rad}}{|Z_{ant} + Z_{load}|^2} \tag{3.2}$$

where R_{load} is the resistant of the load, R_{rad} is the resistant of the antenna radiant, Z_{ant} is the impedance of the antenna, and Z_{load} is the impedance of the load.

The power transferred to the tag IC is maximum when $\tau = 1$ and power transferred efficiency = 50%. If $\tau < 1$, the read range is proportional to the square root of τ. In most cases, the power transferred efficiency is approximately 30%. Modern tag ICs consume 20 to 150 μW when being read. As a result, tags require about 60-450 μW of power to be delivered from the antenna. If the worst case is 450 μW, the read range is approximately 1.25 m; if the best case is 60 μW, the read range is about 3.42 m (with transmit 1W EIRP).

3.2 RFID system description

3.2.1 Hardware

In this experimental setup, the EPCglobal Gen 2 Class 1 reader is monitoring the readability of a detected tag (i.e. the percentage of tags that responded successfully at a specific range regardless of tag orientation to the Query Rounds sent out by the reader). We use two different types of commercial UHF EPCglobal Gen 2 Class 1 passive tags and one semi-passive tag. Table 3.1 summarizes the specifications of the two UHF RFID readers used in this experiment. A mono-static RFID reader uses a single antenna and supports bidirectional, full-duplex Tx/Rx port. In contrast, bi-static reader uses one

Table 3.1: RFID Readers for this experiment

Reader	Mono-Static Reader	Bi-Static Reader
Antenna Gain	7.5dBi	6 dBi
$\|\Gamma\|^2$	0.09	0.11
Output Power	1W	1W
Sensitivity	$\approx$ -77 dBm	$\approx$ -70 dBm
Polarization	Circular	Circular

antenna for transmitting and another for receiving. Both readers operate in frequency hopping mode in the range of 902-928 MHz. The experiments are conducted in a normal indoor computer lab environment and in an anechoic chamber.

3.2.2 System Setup

Our experimental setup is shown in Figure 3.2. The RFID reader antenna and RFID tags were placed in a highly reflected environment (normal computer lab room) and in an anechoic chamber. The reader antenna and tag were placed approximately 60cm above the ground in the reflected environment and 20 cm above the ground in the anechoic chamber. Tags were initially placed 0.91 cm away from the reader antenna and moved away in 10 cm increments. An appropriate tag read operation was attempted repeatedly for eight tag orientations at each position.

In order to examine the effects of tag proximity, we used an experimental setup consisting of two EPCglobal Gen 2 Class 1 reader with a 6 dBi gain antenna and three different types of EPCglobal Gen 2 Class 1 tags. The tags were placed one meter away from the reader antenna and the reader output power was set to 30 dBm (1 Watt) as this is the maximum allowable transmitting power according to the regulation [41]. All tags are placed in the same plane on a single cardboard platform with the best possible orientation angle to the reader antenna. The steps were repeated while increasing the distance between the tag and the reader antenna in 0.1 meter increments. This was done to eliminate the influence of orientation sensitivity on the measurements. The experimental setup is shown in Figure 3.2.

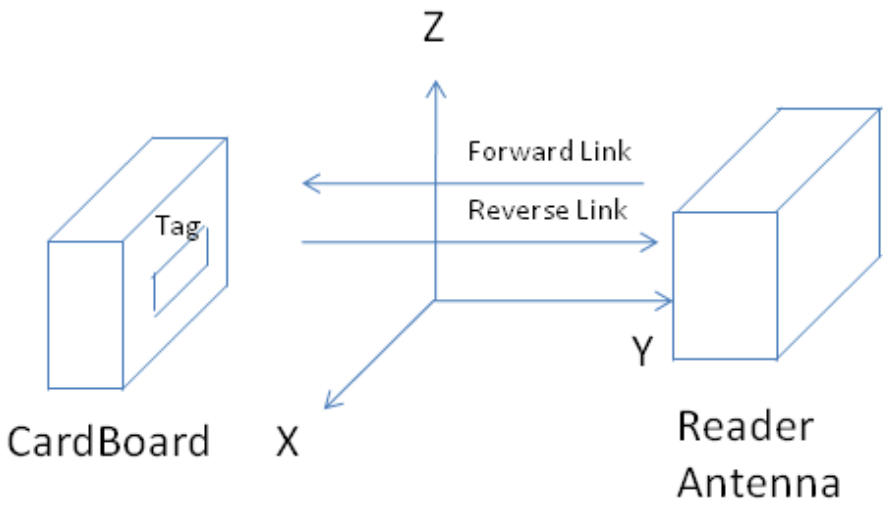

Figure 3.2: Experimental setup top view

3.3 Results

The received signal strength indicator (RSSi) showed the average power level of the reader received packet in the reverse link. Figures 3.3 and 3.4 show RSSi in dBm versus distance (in meter) of dipole passive tag with orientation $\theta = 0°$, $\phi = 0°$ and $\theta = 60°$, $\phi = 0°$, respectively. θ is moving from the X axis to the Y axis in the XY plane, and ϕ is moving from the Z axis to the Y axis in the ZY plane. The combination of these two angles represents tag orientation in a three dimensional axis. Figures 3.5 and 3.6 show RSSi in dBm versus distance (in meter) of a dual-dipole passive tag, and Figures 3.7 and 3.8 illustrate RSSi in dBm versus distance (in meter) of semi-passive (dipole) tag with the same orientation as the dipole passive tag. Note that an RSSi value of less than -90 dBm indicates that the reader was not able to detect the tag at the current position.

Each figure contains four sets of data lines that track RSSi measurements performed by the reader with the mono-static antenna and the bi-static antennas in the anechoic chamber and the computer lab, respectively. Given that each measurement is one reading attempt, if the reader cannot detect a tag, the tag is not readable at that position and orientation. Table 3.2 shows the readability results for the dipole passive tag, the dual-dipole passive tag, and the semi-passive tag. Results are aquired in the anechoic chamber and the computer room while changing the distance between the reader and the tag from 0.91m to 4 m. Table 3.3 shows the maximum read range of all tags regardless of tag

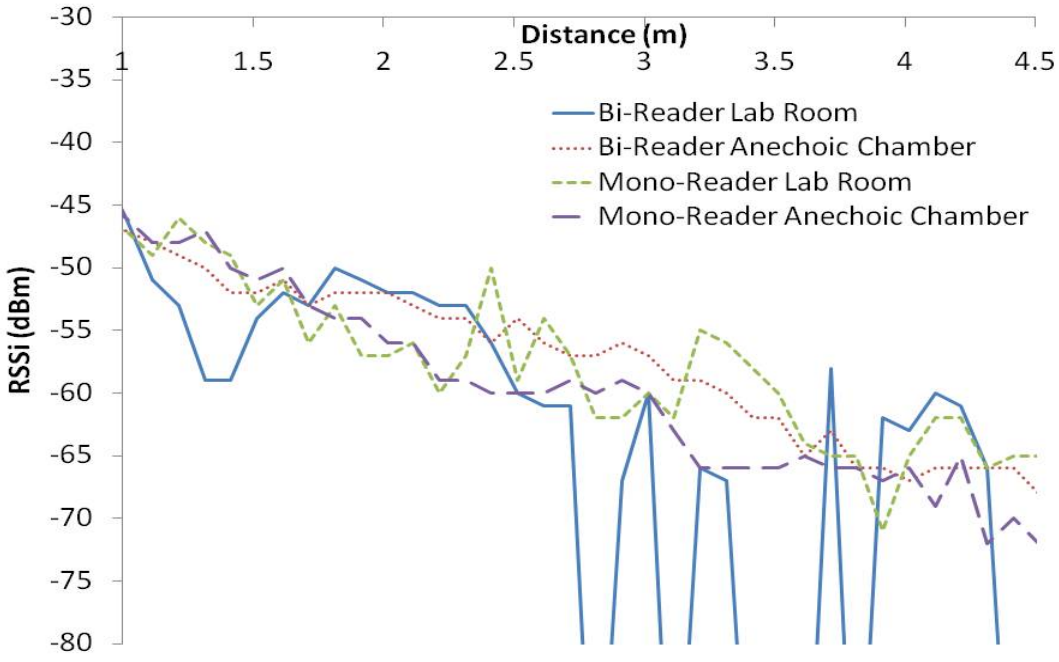

Figure 3.3: RSSi of dipole passive tag at tag orientation θ=0, ϕ=0

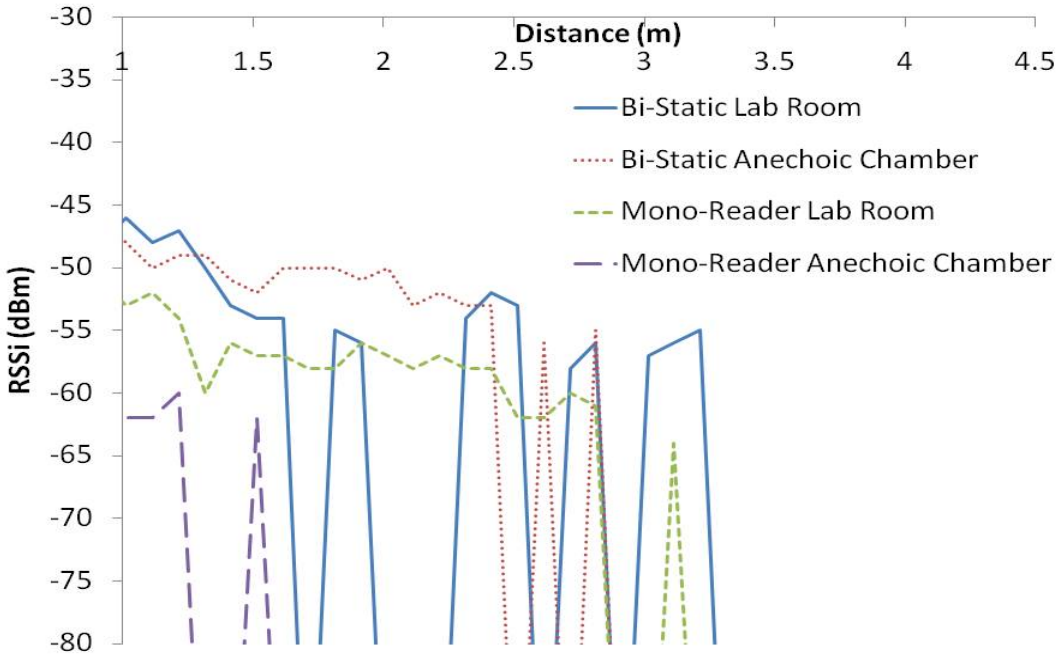

Figure 3.4: RSSi of dipole passive tag at tag orientation θ=60, ϕ=0

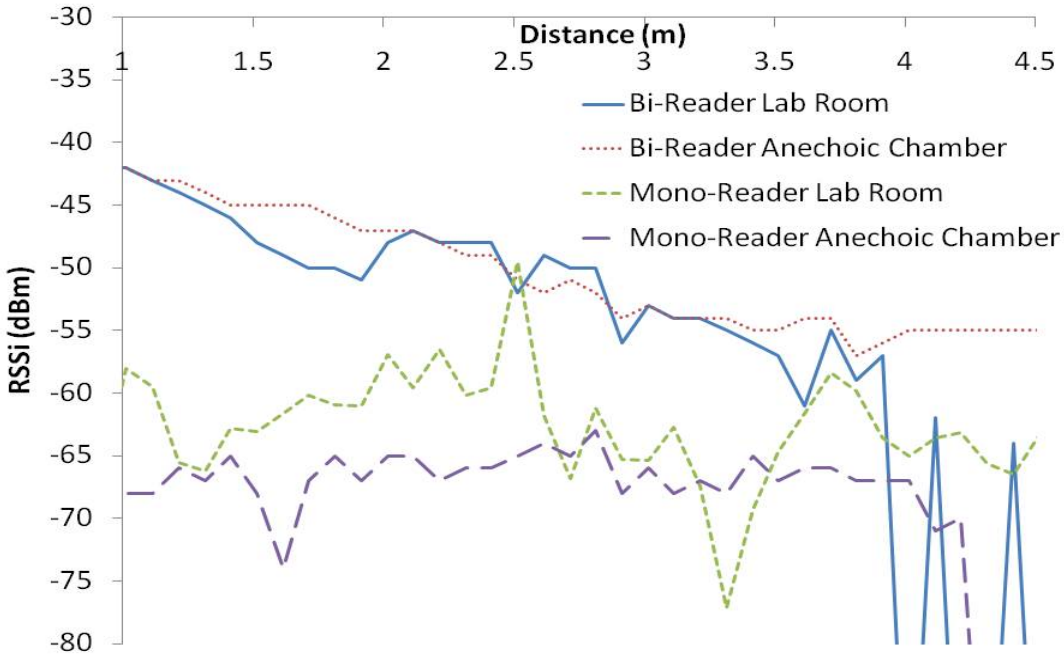

Figure 3.5: RSSi of dual-dipole passive tag at tag orientation θ=0, ϕ=0

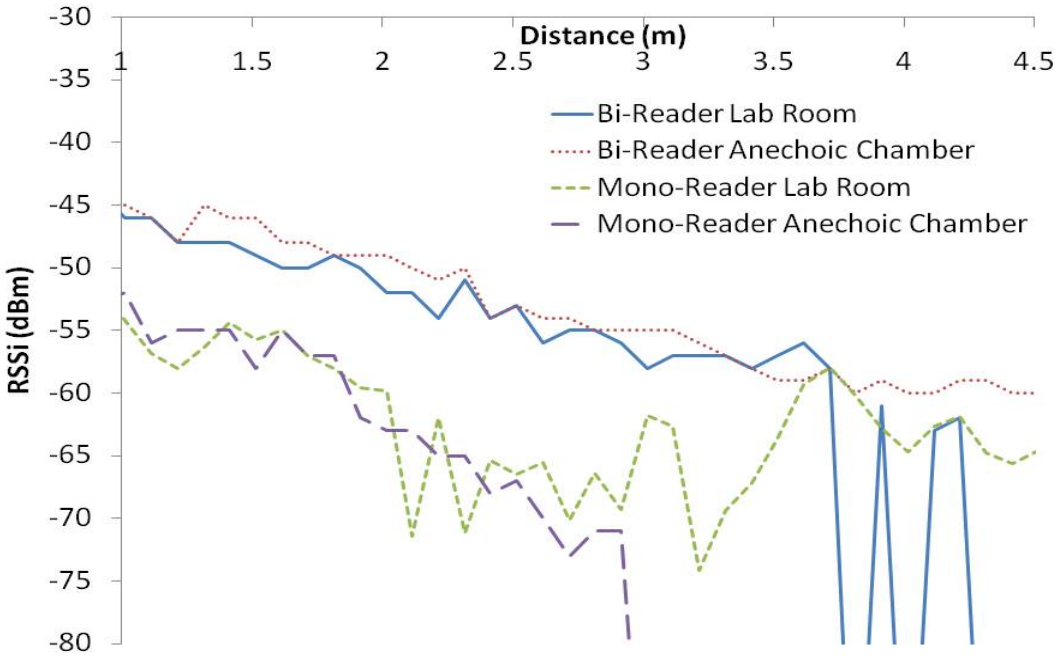

Figure 3.6: RSSi of dual-dipole passive tag at tag orientation θ=60, ϕ=0

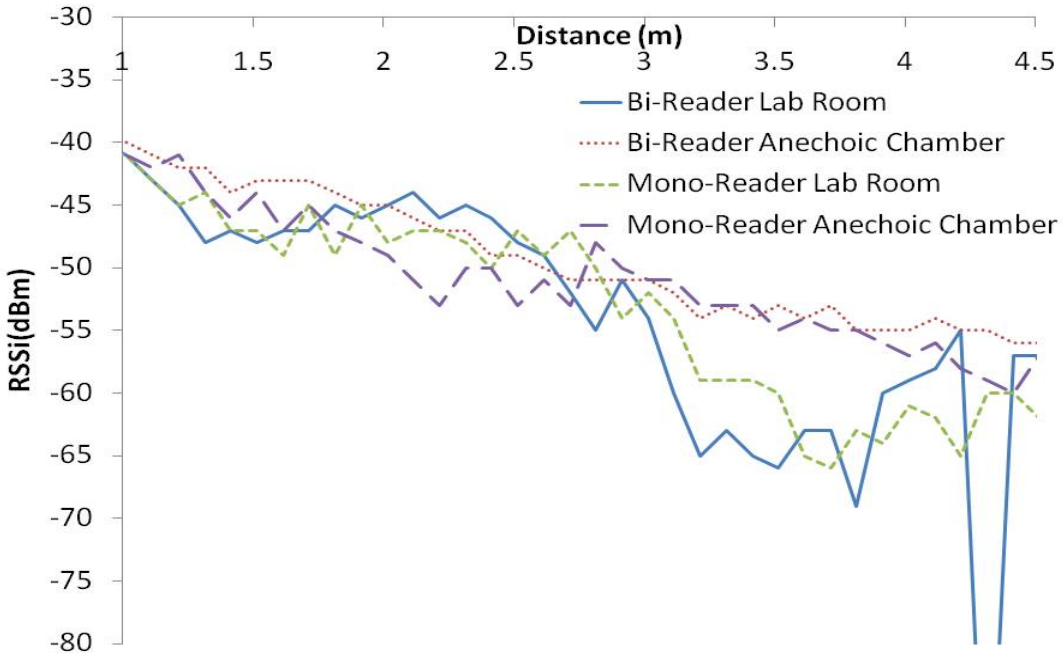

Figure 3.7: RSSi of semi-passive tag at tag orientation θ=0, ϕ=0

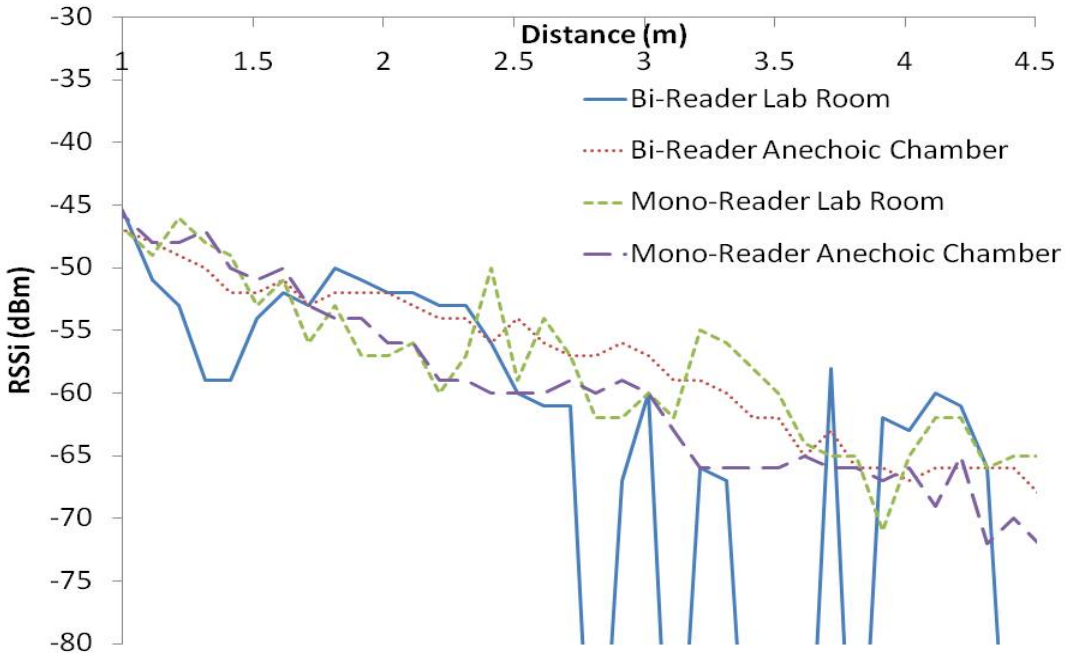

Figure 3.8: RSSi of semi-passive tag at tag orientation θ=60, ϕ=0

Table 3.2: Readability of tags from 0.91m to 4 m

Tag Type	Readability at Computer Lab		Readability at Anechoic Chamber	
	Mono Static Reader	Bi Static Reader	Mono Static Reader	Bi Static Reader
Dipole Passive Tag	80.6%	73.0%	78.2%	82.7%
Dual-Dipole Passive Tag	100%	87.9%	97.6%	100%
Dipole Semi-Passive Tag	100%	100%	91.9%	95.2%

Table 3.3: Maximum Read Range of tags

Tag Type	Maximum Read Range(m)	
	Mono Reader	Bi Reader
Dipole Passive Tag	10	10
Dual-Dipole Passive Tag	9	9
Dipole Semi-Passive Tag	43	12

orientation.

3.4 Analysis

Lack of Well defined Read Zone

With respect to the reader antenna, a practical single reader-single tag system does not have a specific read zone in which the tag exhibits a 100% read rate and outside which it exhibits a 0% read rate. It has been shown in several independent studies that, in the case of passive RFID systems, such as the one currently under consideration, the read range depends mostly on the power in the forward link needed to power tags IC [40], [42], [43], [44]. In free space, as a tag moves away from a reader, the mean value of the power it receives drops off as per the Friis Equation 3.1. As the power drops, so does the tag's read rate until the tag reaches position where it is unable to receive sufficient power and the read rate drops to zero. As seen in Figures 3.3 to 3.7, even in an anechoic chamber, there is a gray area around the reader antenna where the tag may or may not

be read in a very close area. Thus, in a practical system it is not possible to define a clear read zone as described for the ideal system. This is due to the inherent properties of electromagnetic radiation which is the basis of communication between the reader and the tag.

Sensitivity to Reader configuration

Reader antenna configuration and sensitivity affect system performance. As the received power can be calculated from Friis Equation 3.1, theoretically the power should decay exponentially at the rate of $(\frac{1}{r})^2$.

From Figures 3.5, the RSSi (in dBm) of a mono-static reader did not decay at the rate of $\frac{1}{r}^2$ in the anechoic chamber. A dual-dipole passive tag is symmetrically-illuminated. The return signal from such a tag will have a reverse polarization sense, and will be ineffectively received by the mono-static antenna[40]. As shown in Figures 3.5 and 3.6, the reader with the mono-static antenna received smaller RSSi than the reader with the bi-static antenna, when both had the same tag at the same position and orientation. Although the EIRP of the mono-static reader exceeds the EIRP of bi-static reader by 1.5 dB, it has significant interfering signal leakage into the receiver, from the antenna reflections or the leakage [40].

Sensitivity to tag orientation

From the Friis Equation 3.1, the radiation pattern affects both the transmitted and received power. The orientation of the tag should be considered when evaluating tag performance. Comparing Figures 3.3 to 3.8, shows that the orientation affects both the read range and the RSSi value, particularly for the dipole tag. When orientation of the tag with the dipole antenna is $\theta = 60°$ and $\phi = 0°$, it is approximately 5 to 7 dB less than the RSSi of the dipole tag oriented at $\theta = 0°$, and $\phi = 0°$ at same position in the anechoic chamber. On the other hand, a dual-dipole passive tag is not very sensitive to tag orientation, and only drops about 1 to 2 dB at $\theta = 60°$, and $\phi = 0°$ compared to $\theta = 0°$, and $\phi = 0°$ at the same tag position in the anechoic chamber. Sensitivity to tags‘ orientation should be considered for determining tag performance.

As in Figures 3.3 to 3.8, all tag’ read ranges drop significantly when the orientation becomes less favourable for the tag. Semi-passive tags with integrated batteries are less sensitive than passive tags because passive tags are required to collect more power to turn on the IC. In addition, the results demonstrate that the read rates depend on the relative orientation of the tag and the reader antennae and on the distance between tag and reader.

The problem of orientation sensitivity can be handled by innovative tag antenna designs incorporating multiple dipoles or monopoles. In fact, ensuring orientation insensitivity is one of the most important goals when designing tag antennae. Experimentation with different tag orientations is published in several studies including [45]. Note that experimentation on the dependency of orientation to read rate in [45] is performed with EPCglobal Class 1 tags (a generation before Gen 2).

Sensitivity to deployment environment

The performance of an RFID system is mainly dependent on the operating environment. Examining the RSSi value of the lab room in Figures 3.3 to 3.8 revealed blind spots where tags cannot be detected. However, they can be detected at more distance positions. These phenomena are caused by cancellation of the reflected signals and the direct signal. When the reflected signals and direct signal have the same amplitude but are out of phase, they cancel each other out. RFID systems do not have this type of problem in the anechoic chamber.

The performance of a practical system is highly dependent on the environment in which is deployed. Like any other wireless system, the nature of the environment affects the multipath and fading properties of the channel. This effect is more pronounced in RFID systems due to the passive nature of tag operation and the inherently low signal to noise ratio (SNR) of the weak backscatter signal. Figures 3.3 to 3.8 shows the readability performance in the cluttered environment of a computer lab and in the anechoic chamber. As seen, the deployed environment hampers the readability performance of the system and also introduces some blind/null spots due to multipath interference and channel fading. Compared to the readability in the anechoic chamber, it is obvious that it is difficult ti specify the range, even for a fixed relative orientation of the reader and tags antenna.

From the experiments above, the readability and read range of a tag are not solely dependent on the distance between the reader and the tag; they are also affected by factors such as orientation and environment. A similar inference has been drawn in [44] and [46] where the authors suggest defining read range as the range in which a predefined read rate or accuracy of tag reading can be achieved.

Tables 3.2 and 3.3 show the performance of passive and semi-passive tags. Semi-passive tags are superior to passive tags. However, when the readability metric is considered when the read range is less than four meters, semi-passive tags did not have an advantage compared to dual-dipole tags, as shown in Table 3.2. In addition, the per-

formance of semi-passive tags is highly dependent on the sensitivity of the receiver, the output power, and the antenna gain of the RFID reader. The transmission power of a mono-static reader exceeds that of a bi-static reader by 3 dB, resulting in no benefit to the semi-passive tag in the bi-static case.

The performance measurement of RFID system offers promising results in terms of a reader's operating range. The performance depends on many factors, including reader antenna configuration, tag sensitivity on orientation, reader-tag readability and maximum read range. The results show that dipole antenna type tag (dipole passive tags and semi-passive tags) are orientation sensitive, and the reading range differs when the orientation changes. On the other hand, the performance of dual-dipole passive tags is not affected by tag orientation, but by reader antenna configuration. Interestingly, a semi-passive tag that has a very long maximum read range does not provide maximum reliability. For example, a semi-passive tag did not achieve 100% readability for a mono-static reader at a range of less than four meters, even though its maximum read range is up to 43 m in a mono-static configuration. Environment also impacts the reliability of an RFID system, as the reader cannot communicate with a tag if the tag is in a blind spot in a reflected environment.

Reliability is one of the major problems of RFID systems. Lack of well defined read ranges mean an RFID system can be unreliable because it may not be read at a particular read range. We determined the performance of an RFID system by analysing a set of experimental results based on the reader's readability and the RSSi measurements. The performance metrics are evaluated based on the tag's position and orientation, the tag model, and different configurations of the reader's antenna.

Chapter 4

Hardware

This chapter discusses the architecture of the hardware design of the open platform semi-passive UHF RFID tag. The hardware structure consists of two components: analog and digital. The salient features of open platform semi-passive UHF RFID tag are as follows:

- The tag is built on a custom designed printed circuit board (PCB) using discrete components.
- Digital and analog sensor interface are implemented, and are easily integrated by the user, thereby allowing sensors or peripherals to simply be added to the tag.
- The digital section contains a general purpose microcontroller providing the user freedom to extend EPCglobal Gen 2 Class 1 protocol by adding new commands and/or functionalities.
- The tag has a JTAG interface for programming and debugging, which help developer reduce developing debugging time.
- Open source code.

4.1 Architecture

Figure 4.1 shows the high level overall architecture of the open platform semi-passive UHF RFID tag. The RF signal received by the antenna is fed through a bandpass filter circuit to an envelope detector, which removes the carrier signals and extracts the baseband signals. The baseband analog signal is fed to a hysteresis comparator that compares the signal with its low pass version, then generates a digital output that

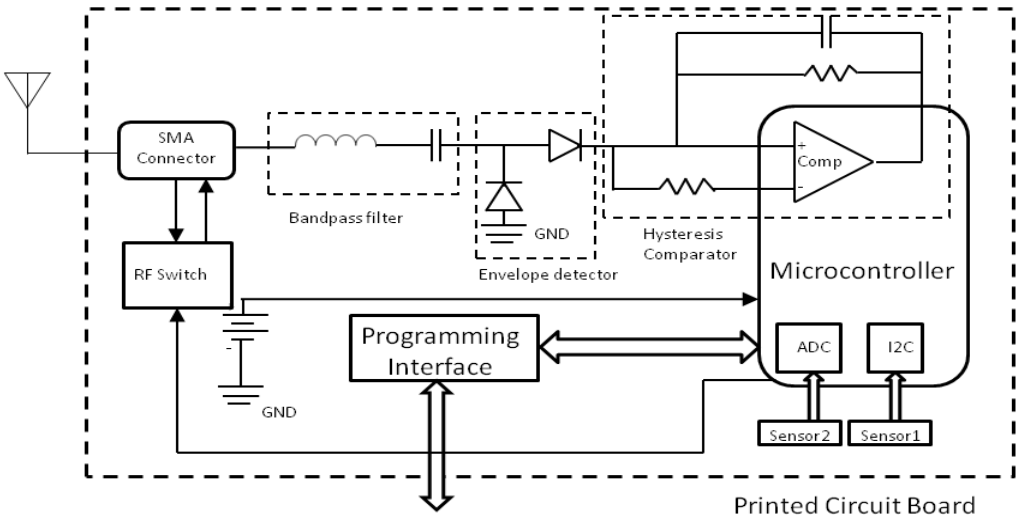

Figure 4.1: Overall architecture of proposed tag platform.

contains the encoded information received by the tag. This signal is processed by the digital section that performs much of the MAC layer protocol activity and higher layer functionality as needed. On the transmit side, the information to be conveyed from the tag is appropriately encoded in the digital section and used to control the backscatter modulator that encode the information to the signal reflected from the tag antenna.

The tag's programmability, and the fact that it will be built using discrete components rather than an ASIC means it will require more power than conventional passive and semi-passive tags. Hence, open platform UHF RFID sensor tags are powered by an on-board battery. However, they do not have an onboard radio, and will communicate using backscatter modulation as described previously. By providing an external power source, the microcontroller will be able to process complex algorithms, including project requirements such as security and/or digital signal processing. Even with a battery on board, a passive tag protocol can still be evaluated with and later implemented on ASIC where it will not need a battery.

4.1.1 Analog front-end

RFID tag analog design involves many challenges and tradeoffs to ensure that the RF front-end has sufficient signal strength and bandwidth while keeping the cost, size and power consumption as low as possible. Since an RFID tag is a mobile device, the power should be the minimum required to provide maximum device life time. In our design, we use only passive components on the analog front-end except for the comparator which is part of the microcontroller. Doing this reduces the power required for our RFID tag.

According to [4], in North America UHF RFID systems communicate using a 902MHz to 928MHz frequency spectrum. This ultra high frequency signal carries baseband information. When an RFID tag receives an RF signal, the first step is to remove the carrier, so the tag can demodulate the baseband signal into digital zero and digital one. We use simple and passive carrier removers and, envelope detectors, to remove the carrier and extract baseband information from RF signals. The carrier remover takes out all ultra high frequency signals and passes only low frequency signals. It may also allow unwanted low frequency signals from outside the UHF RFID frequency spectrum to pass into the comparator, and these unwanted baseband signals may interfere with the RFID baseband signals. To avoid this, we used a series inductor (L) and capacitor (C) to form a band pass filter. When L and C are connected in series to an AC signal input, inductive reactance magnitude (X_L) increases as frequency increases while capacitive reactance magnitude (X_C) decreases with an increase in frequency. At resonant frequency these two reactances have equal magnitude but opposite signs, therefore, they cancel each other out which creates a short circuit. Another reason to use a band pass filter is that it makes it easier to tune the inductor and capacitor values to match the network impedance. A perfectly matched network impedance will allow maximum RF signal power pass through this network.

As UHF RFID tag should be low cost and low power, we use the simplest bandpass filter, LC series circuit. Inductive reactant magnitude X_L increases as frequency increase while capacitive reactant magnitude X_C decreases as frequency increase [47]. Therefore, this simple LC series circuit can be used as bandpass filter. At a particular frequency, the two reactants are equal in magnitude but opposite in sign where $X_L = -X_C$. In other words, there is no impedance resistance. In such a case, LC series circuits can considered as short circuits. The frequency at which this happens is called resonant frequency (f_r) for this particular circuit design. When the frequency is moving away from f_r, the reactant is increased which caused the impedance mismatch and the signal

gets reflected back.

The impedance of the LC series circuits is given by the sum of the inductive and capacitive impedances. Equation 4.1 to 4.9 show the impedance calculation for LC series filter $Z = Z_L + Z_C$. By substituting equation 4.5 and equation 4.6, we can use equation 4.8 to get the total impedance for LC series circuits. Equation 4.8 can be re-written as equation 4.9, which shows that when $\omega^2 LC = 1$, the impedance will be zero which will be short circuit. If $\omega^2 LC \neq 1$, the impedance will not be zero.

By applying 915MHz as the central frequency, L = 11 nH and C = 3pF, we can get Z = 5.26jΩ. This theoretical impedance value will be used to design the bandpass filter. However, as the PCB trace factor shows, inductance and capacitance deviation, it may require further tuning on these values to match impedance.

$$Z = Z_L + Z_C \tag{4.1}$$

$$Z_T = \sqrt{R_T^2 + X_T^2} \angle \theta \tag{4.2}$$

$$R_T = R_L + R_C \tag{4.3}$$

$$X_T = X_L + X_C \tag{4.4}$$

$$Z_L = j\omega L \tag{4.5}$$

$$Z_C = \frac{1}{j\omega L} \tag{4.6}$$

$$\theta = tan^{-1} \frac{X_T}{R_T} \tag{4.7}$$

$$Z = j\omega L + \frac{1}{j\omega L} \tag{4.8}$$

$$Z = \frac{(\omega^2 LC - 1)j}{\omega C} \tag{4.9}$$

One very common passive carrier signal remover is called an envelope detector. It is simple and no external power is required as it uses only pairs of diodes and capacitors. As RFID tag range is dependent on the received signal strength, we use another common approach to obtain higher voltage levels; it is known as the Dickson charge pump, and comprises: multiple stages of pairs of diodes connected in series so the output voltage level of the signals is increased [5]. The power efficiency improves by adding up to five stages to Dickson charge pump. Five stages is the limit, however, because [5] shows the efficiency does not increase. So we use a five stage Dickson charge pump for our tag platform.

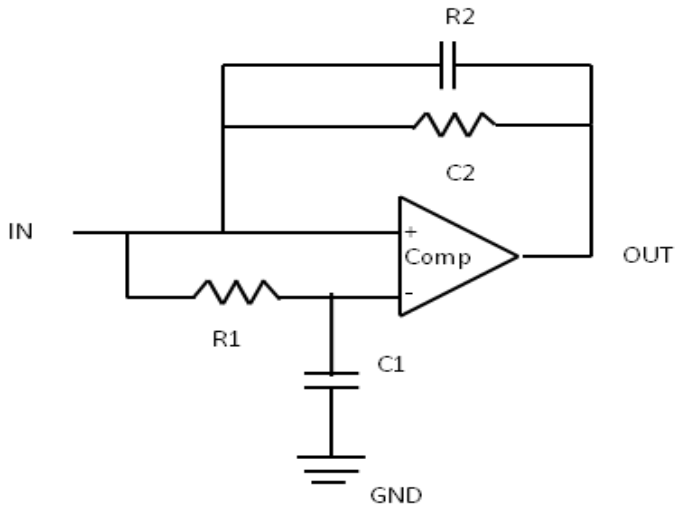

Figure 4.2: Schematic diagram of data slicer.

There are two methods to demodulate baseband signals: use analog digital converter (ADC) to digitize the baseband signal then perform complex digital signal processing (DSP) to demodulate it, or use a comparator to digitize the baseband signal then perform simple DSP to demodulate. In the case of tag, the tag processing power and battery power are limited, and the first solution requires high speed ADC and DSP to demodulate the baseband signals. As the RFID reader baseband signals can be in range of 40 KHz to 135 KHz [4], the ADC and microcontroller must operate at a high frequency to process and demodulate the baseband signal, which will reduce battery life and increase tag cost as high frequency ADC is expensive. We chose the second method to digitize and demodulate the baseband signal. The comparator will digitize the signal, then pass it to a microcontroller which will demodulate it. Another reason for using this method is that the microcontroller comes with the comparator, and this also reduces costs. As the digitized signals are only 1 bit, the microcontroller can demodulate the reader baseband signals in low frequency mode; in our case, an 8MHz system clock cycle will be sufficient.

The data slicer, shown in Figure 4.2, generates one bit digital output by comparing the input signal to its RC low pass (R1 and C1) output threshold. R2 is used to add extra hysteresis while C2 together with R2 is used to form a rapid threshold. Refer to [48] for more detailed information.

The value of these four components can be calculated using the following steps:

1. We limited the UHF RFID reader data rate to 40 KHz as we set the ASK data rate of reader signals to 40 Kbps, i.e. the time interval is about $T_0 = 25\mu s$

2. We are using R_1 and C_1 to create delay. As R_1 and C_1 will be part of the analog network and will affect network impedance, we have to select the appropriate R_1 and C_1 value. We chose $C_1 = 3$ pF to minimize the capacitance introduced into the network where $R_1 = 1\text{M}\Omega$

3. We are adding extra hysteresis which can reduce the sensitivity when the analog signal is compares with its own low pass version. When the analog signals is greater than its low pass version, the hysteresis adds extra offset to it, so the output does not trigger on and off when analog signal has very close amplitude as its low pass version. Also we adding a decay time constant to reduce the sensitivity that comes from a squelch or resistive hysteresis.

4. In order to provide fast offset into an analog signal, C_2 should be equal to C_1, and R_2 should be greater than R_1. We use $C_2 = C_1 = 3\text{pF}$. $R_2 = 10 * R1 = 10\text{M}\Omega$

5. The offset can be calculated as $V_{offset} = \frac{R_1}{R_2} * digital_high_voltage = 0.1 * digital_high_voltage$.

After performing these steps, we use $R_1 = 1M\Omega$, $R_2 = 10M\Omega$. $C_1 = 3\text{pF}$ and $C_2 = 3\text{pF}$. Figure 4.3 shows the baseband analog signals and digitized signals.

The RF switch is another key component if our open platform UHF RFID tag. It should work well in the frequency band of 902 to 928 MHz, and the insert loss should be as low as possible while working in receiving mode (switch ON). At the same time the RF switch should backscatter the input RF power as much as possible when the switch is OFF.

4.1.2 Digital section

Power consumption is an important criterion for the RFID tag digital section. The tag must be in full operation while the power consumption is as low as possible. The main component of the digital section is the microcontroller.

Microcontroller

We use Microchip PIC24FJ64GA004 as our microcontroller for this RFID tag due to its low cost, extension support for different applications and fields, the availability of

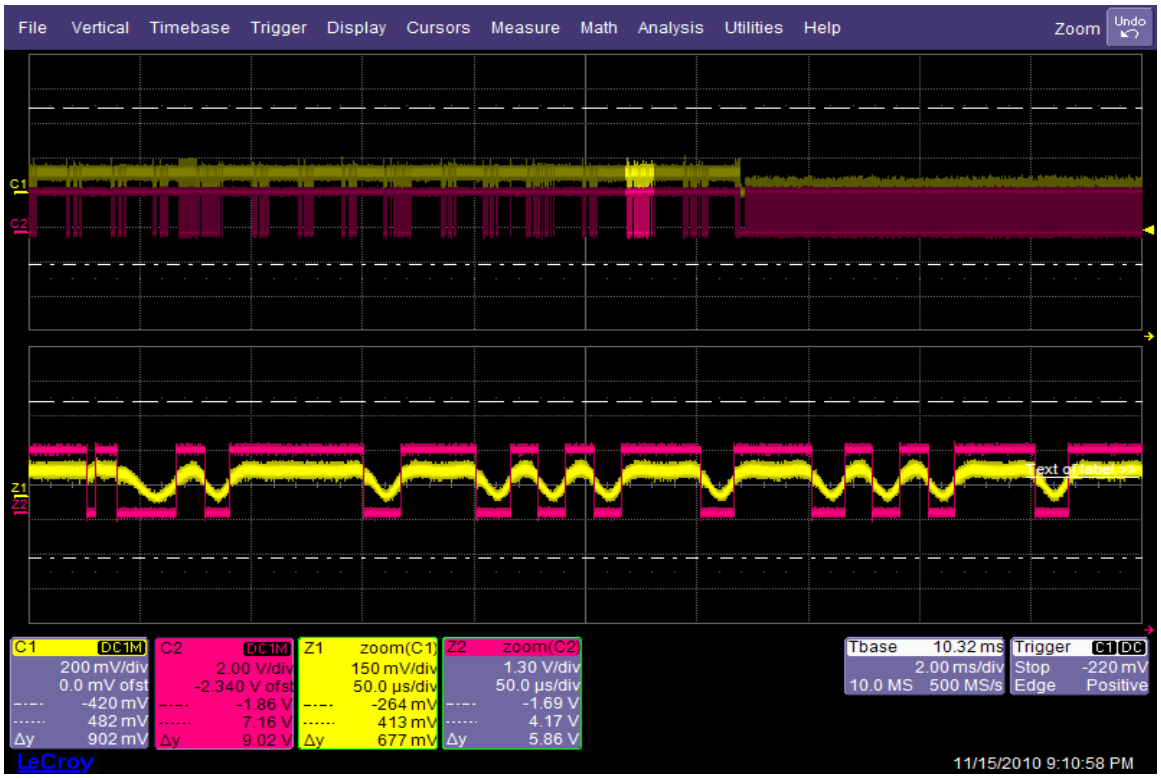

Figure 4.3: Received and digitized baseband signal

low cost or no cost or development tools, and its serial programming capability (and re-programming with flash memory). The PIC24FJ64GA004 microcontroller is in the family of Harvard architecture RISC 16 bits microcontrollers made by Microchip Technology.

PIC microcontrollers are popular with both industrial developers and hobbyists, due to their low cost, wide availability, large user base, extensive collection of application notes, availability of free development tools and samples for academic, and re-programming capability.

The most notable features of this microcontroller family are [49]:

1. Data stored in program memory can be accessed directly by using a feature called Program Space Visibility.

2. Interrupt sources can be assigned to distinct handlers using an interrupt vector table.

3. A 17 x 17 bit single-cycle hardware multiplier and other DSP operations.

4. Hardware support for 32 x 16-bit division.

5. Hardware support for loop indexing.

6. Direct memory access.

7. A software control system clock.

The microcontroller will manage the EPCglobal Class 1 Gen 2 protocol, decoding the reader signal and encoding the tag backscatter signal. As mentioned in Chapter 1 this RFID tag only supports a backscattering signal rate of 256KHz/Miller 4 due to the microcontroller working frequency. As the working frequency is proportional to the power consumption [49], we must decrease the frequency as much as possible to reduce the overall power consumption. Our experiment found, the minimum frequency we can achieve that supports this backscattering rate is 4 million instructions per second which is 8 MHz system clock. Even though we target this frequency, researchers can adjust the system clock to meet their project requirement.

The PIC24FJ64 family has two ADC and I^2C interface modules. Analog and digital sensors can be attached to the RFID tag. This functionality is not limited to sensors; it can be used in many other applications. RFID tag can use I^2C to communicate with other digital components, including memory or custom digital devices. ADC can be used to communicate with low frequency analog devices as well.

Chapter 5

Software

This chapter discusses the architecture of the software design of open platform semi-passive UHF RFID sensor tags. The software can be classified in two sections: micro-controller firmware, and RFID reader software.

5.1 Firmware architecture

Figure 5.1 shows a high level overview of the tag firmware. The firmware is developed in C and Assembly languages using the MPLAB Integrated Development Environment (IDE) [50], which is a free, integrated gcc-based toolset for the development of embedded applications employing Microchip's PIC and dsPIC microcontrollers[51]. It provides user friendly, flexible techniques to develop applications for embedded systems without compromising performance. MPLAB supports both Assembly and C programming

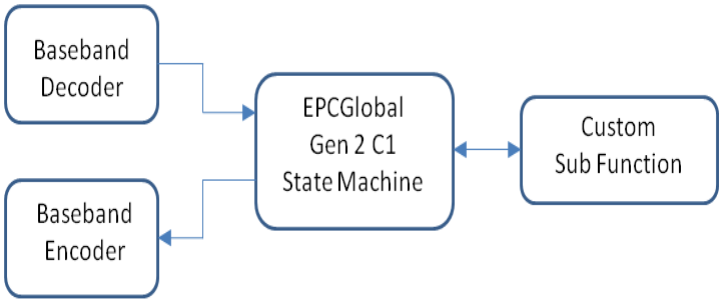

Figure 5.1: Tag module diagram

language.

The modules can be classified as:

1. Baseband Decoder – pulse interval encoding (PIE) decoder.
2. Baseband Encoder – Miller 4 (M4) encoder.
3. EPCglobal Gen 2 Class 1 state machine – main state machine incorporate EPCglobal Gen 2 Class 1 state.
4. Custom Sub Function – Custom sub-function defined by user.

Baseband Decoder/Encoder handle physical layer protocol. The EPCglobal Gen 2 Class 1 state machine handle EPCglobal Gen 2 Class 1 protocol, and Custom Sub Function handles user defined sub-fuctions. If users are developing a physical layer, they should only need to modify the Baseband Decoder/Encoder modules. The security algorithm and external device access should be implemented in the Custom Sub Function module. The user may have to do minimal modifications of the EPCglobal Gen 2 Class 1 state machine to call the Custom Sub Function. Modification of the EPCglobal Gen 2 Class 1 state machine should be as small as possible to avoid violating EPCglobal Gen 2 Class 1 protocol.

5.1.1 Baseband decoder

The PIE (pulse interval encoding) decoder module samples the input waveform and outputs the data symbols. The symbols are of six types: data-zero, data-one, TRcal, RTcal, invalid [4]. Figure 5.2 shows the PIE data-zero and data-one. The symbols can also have different parameters, depending on the TARI (length of data-zero) value set by the reader. Currently only one TARI value of 25 us is supported. The TARI value used by the reader is determined from the pulse width (PW) which is constant for all symbols in the same TARI. As the microcontroller working frequency gets higher, the power consumption also increase. It is necessary to limit the supported TARI value to provide an acceptable device life time. In order to achieve lowest possible working frequency, this block is implemented in Assembly language, which may increase the difficulty of maintenance and extensibility.

When the baseband signal rises, the internal timer will start to count clock cycles. When the baseband signal falls, the microcontroller will generate an interrupt to calculate how many clock cycles were present during the high pulse to determine the coming

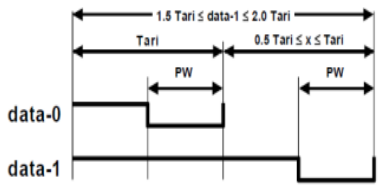

Figure 5.2: PIE symbol[4]

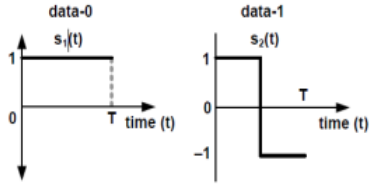

Figure 5.3: Miller symbol[4]

symbol. This data symbol is stored in memory and passed to the EPCglobal Gen2 Class 1 state machine block to decode the command.

5.1.2 Baseband encoder

The Miller encoder encodes the incoming carrier wave signal into a Miller waveform. There are three types of Miller waveforms: M=2, M=4, and M=8. They are characterized by the number of clock cycles in one symbol (i.e. M=2 has 2 cycles, M=4 has 4 cycles and so on). Figure 5.3 shows the encoding schemes. This tag only supports M=4 mode, as M=4 has better performance than FM0 [52] and M=2, also it has a higher data rate than M=8. Figure 5.4 shows the state diagram for Miller encoder. After the Miller state machine outputs the symbols, they are XORed with the Miller clock cycle, then output to produce the correct waveform.

5.1.3 EPCglobal Gen 2 Class 1 state machine

This is the main state machine of the tag. All the EPCglobal Gen 2 Class 1 commands are addressed here and all operations are performed here. It also prepares response packets to be sent back to the reader. There are four states within the state machine: START→ ARBITRARY→SECURE→CUSTOM . The REPLY and ACKN states are omitted to reduce system processing time. When a tag receives an RN16 or READ command, the state machine will call the REPLY function to backscatter the corresponding message

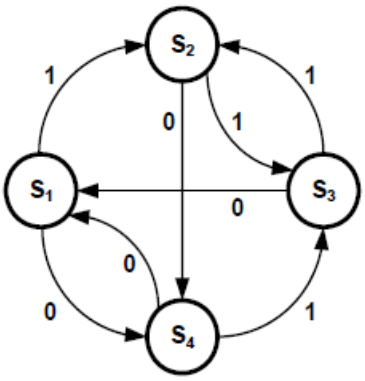

Figure 5.4: Miller Finite State Machine[4]

and return back to the original state. Access commands are only in the SECURE state. The state machine is sensitive to command opcodes it receives. A transition occurs when the received command match to command mask and length. The CUSTOM state provides the freedom for users to call their custom sub-function, and they can define their condition to enter and exit this state.

5.1.4 Custom sub-function

This is the block for implementing custom function. This sub function block designs support add-on components. Interface protocol to external peripherals can also be implemented at this block. For demonstration purposes, we have implemented the I^2C master protocol function. At this sub-function, the tag will read digital sensor data via the I^2C interface. Another example is that we are able to control the ADC hardware and read its buffer.

5.2 RFID reader software

We provide simple RFID reader software, so users can control the standard RFID reader. This software has two parts: low level reader protocol and a graphic user interface.

5.2.1 Low level reader protocol

Low level reader protocol (LLRP) is a low-level interface protocol used to control RFID air protocol operation timing and access to air protocol command parameters [53]. LLRP

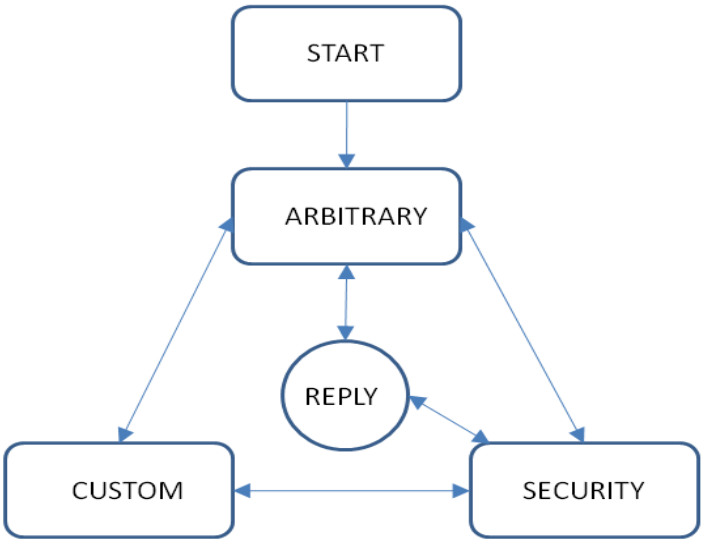

Figure 5.5: EPCglobal Gen 2 Class 1 state

is a specification for the network interface between the reader and its controlling software or hardware. Having already standardized the tag and reader radio frequency (RF) air interface protocol with the UHF EPCglobal Gen 2 Class 1 standard, this specification was the practical, and logical next step to facilitate the adoption of EPC and RFID technology.

5.2.2 Graphic user interface

Graphic user interfaces (GUI) simplify the use of application by presenting information in a manner that encourages a rapid learning curve and intuitive manipulation[54]. The visual object represents a physical object and abstract data, and it provides the user with an intuitive method to provide input and observe results. Figure 5.6 shows the RFID reader GUI we developed for this project. It allows the user to connect to a standard reader that supports the LLRP. This GUI was developed in C# language using Microsoft Visual Studio IDE. It provides built-in tools to create form designs for building GUI applications, and it accepts many plug-ins and libraries that enhance its functionality and, extensibility, and reduce the time required to totally redesign some functions. Microsoft provides "Express" editions of Visual Studio 2010 components at no cost.

This GUI supports most of the EPCglobal Gen 2 Class 1 commands, including Query,

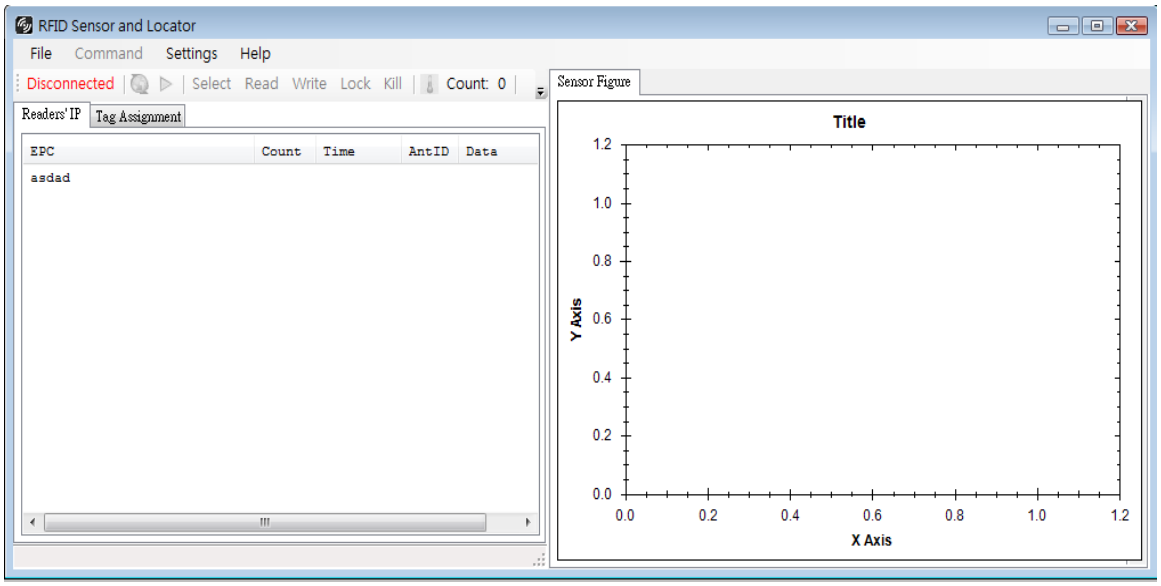

Figure 5.6: A screen shot of RFID Reader GUI

Read, and Write. We can use the Read and Write commands to execute user defined sub-functions. The GUI can present the read data in graphical format. We use open source library ZedGraph[55] to present the graphic format.

5.3 Open platform license and website

Our open platform semi-passive RFID tag has a GNU General Public License. The GNU General Public License is a free, copy-left license for software. It allows both both author and users to freely distribute copies of the open source software. We are publishing the content of our open platform semi-passive RFID tag on Wiki page [56], and people can access the source code and schematics there for their reference.

Chapter 6

Application

The RFID open platform tag will create new experimentation opportunities, and enable research advances in the areas described in this chapter.

6.1 Physical and Link Layer Protocols

The protocol used for communication between the reader and the tag has a direct impact on the performance, cost, and applicability of a RFID system. A protocol must specify physical (PHY) layer parameters such as symbol timing, encoding and modulation schemes, and data rates. For UHF RFID systems, goverment regulates the parameters permitted, and they are also limited due to passive tags' requirement to absorb power from the reader transmission signal. Thus, the choice of symbol timing parameters is an important process involving various tradeoffs. Most RFID applications involve large populations of tags in close proximity to one another. In these situations, the anti-collision and medium access control schemes play an important role in terms of performance and reliability. When there are multiple readers involved, the system will become more complicated. Readers-tags and readers-readers collisions [57] [58] require more advanced anti-collision algorithm. Most RFID standards use a variant of tree-based protocols [59] or ALOHA-based protocols [4] [60] for collision resolution. Beyond standards, development of new RFID protocols is a very interesting area of research [61] [62] [63] [64]. Much of this work is focused on improving the anti-collision schemes applied in today's standards, in order to improve the scalability and performance of high volume RFID systems [65] [66] [67] [68]. These protocols are based on a reader talks first (RTF) approach. There are also research efforts and commercial products that explore the use of a tag

talks first (TTF) approach to protocol development [69]. Some of the earlier work in this area focused on collision resolution in multi-reader scenarios using carrier-sensing at the readers [70] or designing a TDMA-like access protocol [71]. Most of these studies use simulations to evaluate performance, or they have very limited scope when they perform experiment. The RFID open platform tag will provide a semi-passive RFID platform for studying the performance on the tag side. Researchers can modify the encoder/decoder block for the physical layer parameters to improve the system performance. They can also easily modify the blocks and re-program new firmware into the open platform semi-passive UHF RFID tag to compare system performance.

6.2 RFID Sensor Networks

Traditional wireless sensor networks use hardware that is much more capable than a semi-passive RFID tag. Specifically, these are a programmable microcontroller with extensible capability and low energy consumption that can run small operating systems on board [72] [73], and a network protocol stack (often resembling that of the internet) [74], and an RF transceiver (e.g., IEEE 802.15.4). All these obviously increase cost, size, and power consumption. For example, a sensor TelosB mote [75] [76] can cost more than a semi-passive RFID tag, but a TelosB mote device battery lasts for months or years since the device is inactive 99% of the time. Since sensors do consume energy, sensor-equipped tags are typically semi-passive or active. Several vendors also manufacture semi-passive tags that can have a range of sensors attached. Open platform semi-passive UHF RFID tags bring programmability directly to the sensor-equipped tags creating the possibility of point-to-point RFID sensor networks [77]. Sensor values can be read by a reader as tag stored data using the tag memory for intermediate storage, and a semi-passive tag processor can perform preliminary computation on such data. Tag anti-collision performance can be improved in crowded tag environments by eliminating unnecessary tag responses (e.g. using tags that only respond if a pre-programmed condition applies) [77]. Support for multi hop routing opens up the possibility of building a real sensor network with this technology. Open platform semi-passive UHF RFID tags provide the expandability to add digital/analog sensors on board, to create an RFID Sensor Network.

6.3 Security and Privacy

Since RFID tags typically contain sensitive information and they can be read wirelessly, security and privacy are critical concerns. Although, these issues could be addressed using traditional security and cryptographic techniques (e.g. WiFi or cellular network systems), UHF RFID systems could not easily adopt these techniques due to their low processing power, little or no on-board power, limited storage, susceptibility to physical attacks, and protocol PHY time constraint requirements [78]. Security and privacy has become one of the biggest challenges to UHF RFID technology. Given that many forms of attack are possible, researchers have even described various taxonomies of RFID security threats. (see, e.g., Garfinkel, Juels and Pappu [79], or Karygiannis, Phillips and Tsibertzopoulos [80]. Though tag data is encrypted, many attacks use cryptanalysis or eavesdrop on tag data to uncover useful information in the application domain. Even when cryptanalysis is not successful, unique identifiers returned by the tag can be used to track or clone individuals and objects. And using similar methods, information on writable tags can be overwritten, even with off-the-shelf readers. Such spoofing attacks can be used to fool access control systems, contact-less payment systems, and others. This also creates a host of side issues including the launching of RFID viruses [81]. Simpler attacks are also possible at lower layers, such as jamming, or cloning (transmitting the same RF signal as the tag without trying to demodulate and decrypt the data), and replay or relay attacks. Current research only addresses some of these issues. Many attacks can be thwarted by using cryptographic protocols that provide different combinations of support for authentication and privacy [82]. Computation, communication and storage requirements are important design issues here, as the ultimately impact the energy budget of a tag. Open platform semi-passive UHF RFID tags offer a platform for studying security vs. energy tradeoffs, and the potential to implement such protocols in a working system. To study these aspects, the cryptographic primitives can be implemented directly on the microcontroller. Researchers can modify the tag firmware of the EPCglobal Gen 2 Class 1 state machine to provide and enhance security. For example, they can encrypt the EPC so that an intruder can not eavesdrop on a tag's EPC.

6.4 Antenna Design for Tags

The antennae used on the reader and tag side have a significant impact on overall performance. The type of tag antenna determines the orientation sensitivity of the tag

with respect to the reader antenna. Tag antenna design for passive and semi-passive tags is an important research area [83], [84], and [5]. Today's antenna designers test the performance of their designs by simulating and measuring antenna parameters such as reflection coefficient, radiation pattern, polarization and gain [85], [86]. However, the actual performance of an antenna in a system cannot be measured until the antenna is actually built and attached to an RFID tag. Some research has been done on verification platforms for tag antennae [87]. An open platform semi-passive UHF RFID tags, and standard SMA connector, provide a real platform for antenna designers to test performance by directly connecting their antenna. Higher level researchers can evaluate their protocols, security schemes, ad-hoc networks and signal processing techniques using a variety of antennae. Since antennae have such a direct impact on performance, this analytical capabilities of the open platform semi-passive UHF RFID tag can be of tremendous value in evaluating research in the above mentioned areas. As the tag provides standard interfaces to commercial antennae, researchers can use it to compare the antenna performance by using the same testing platform.

Chapter 7

Results and discussion

This chapter discusses the prototype of an open platform semi-passive UHF RFID tag. Several experiments were performed in this thesis, including computation of read rate and range, measure of power consumption in different scenarios , and attaching a sensor to an open platform semi-passive UHF RFID tag. Figure 7.1 shows the first prototype of an open platform semi-passive UHF RFID tag. The experiments were performed in a computer lab with dimensions of ten meters long , ten meters wide and three meters high.

7.1 Read rate and read range

We first performed several experiments related to read rate and RSSi. Read rate is defined as the number of responses from the tag divided by the number of queries sent. RSSi illustrates the tag sensitivity and read range. If RSSi is too low, the tag will not be able to process the signal properly for forward link, and the reader cannot decode tag backscattering signals for backward link. Both parameters can help evaluate the performance of an open platform semi-passive UHF RFID tag in a computer lab.

7.1.1 Fixed reader and tag distance

In order to examine the performance of our open platform semi-passive RFID tag, we used an experimental setup consisting of an EPCglobal Gen 2 Class 1 reader with a 6dBi gain of circularly polarized patch antenna, a commercial semi-passive tag, and an open platform semi-passive RFID tag with a 3dBi linearly polarized patch antenna. The tags were placed four meters from reader antenna, and the reader output power was changed

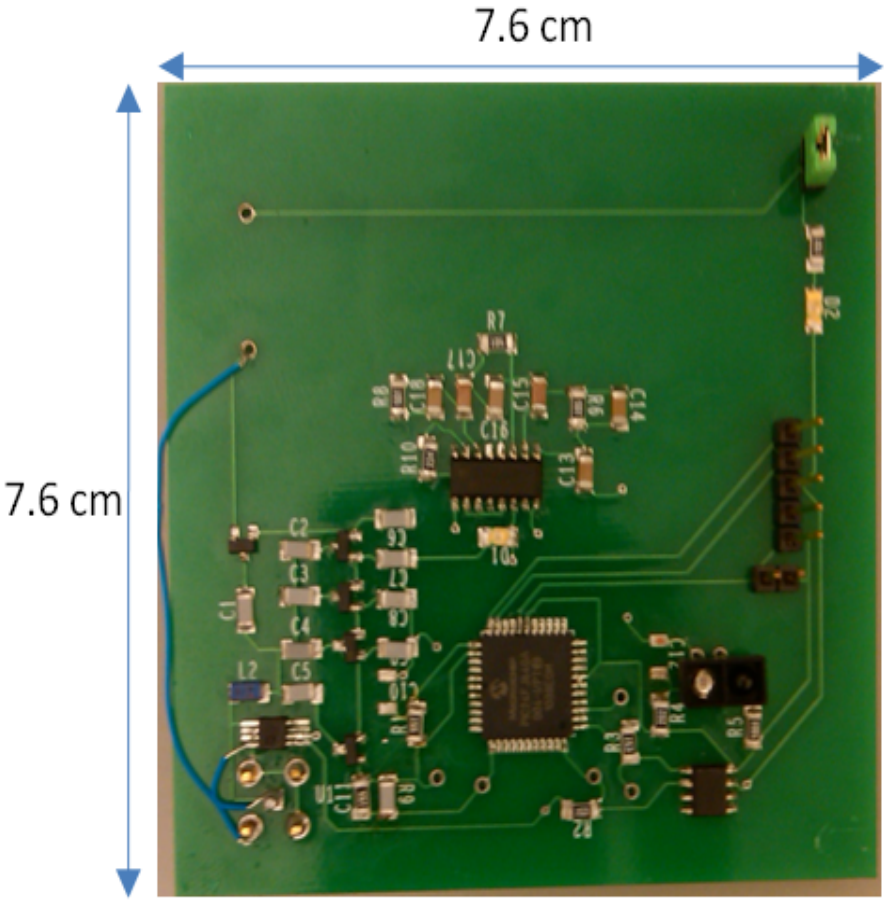

Figure 7.1: First prototype of an open platform semi-passive RFID tag

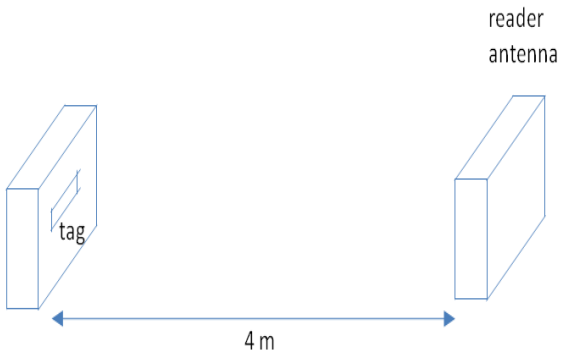

Figure 7.2: Experimental setup for examining tag read rate.

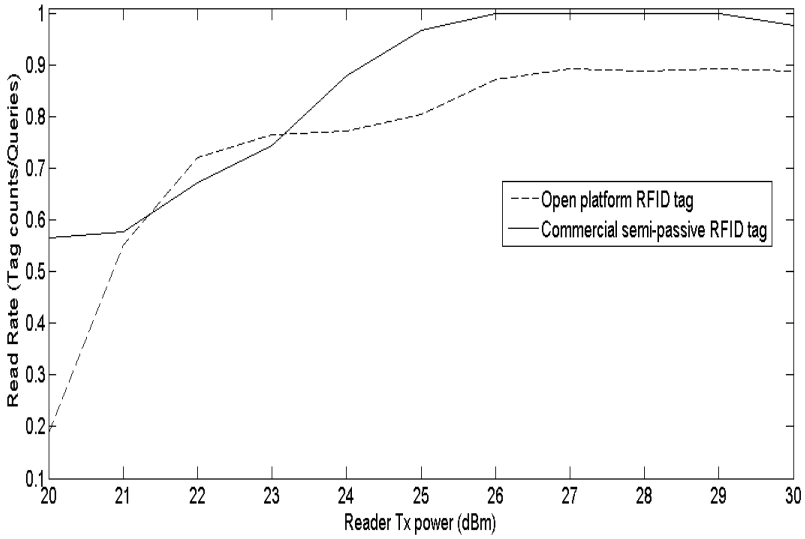

Figure 7.3: Read rate of open platform semi-passive tag and commercial semi-passive RFID tag in a Computer lab

in fixed steps in the range from 20 to 30 dBm, so that when reader transmitting power is less than 20 dBm, the open platform semi-passive UHF RFID tag read rate drops to zero, and 30 dBm is the maximum allowable reader transmitting power. We placed the tag four meters away from the reader antenna, as this distance provides the best read rate for both tags in the computer lab. The open platform semi-passive RFID tag and commercial semi-passive tag are placed in a plane on a single cardboard platform with the best possible orientation angle relative to the reader antenna. This is done to eliminate the influence of orientation sensitivity on the measurements. The experimental setup is shown in Figure 7.2. Initially, reader output power at 20 dBm. A total of 1000 query rounds were sent by the reader, and the number of responses from the tag and average of RSSi value from all query rounds were noted. RSSi values were collected only when the reader was able to process the tag responding signal. We only test one tag at time, to eliminate the influence of shadowing effects [40]. The read rate results are shown in Figure 7.3, and the RSSi results in Figure 7.4. To further analyze the performance, we repeat the same experiment setup with addition of a cardboard box in between the reader and the tag. This can help us observe the read rate and RSSi value in non line of sight situation. The results are shown in Figure 7.5 and Figure 7.6.

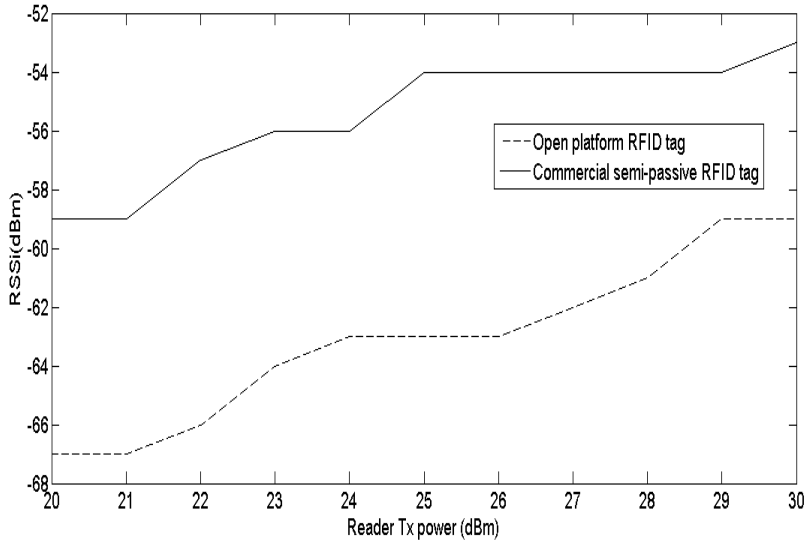

Figure 7.4: RSSi of open platform semi-passive tag and commercial semi-passive RFID tag in a Computer lab

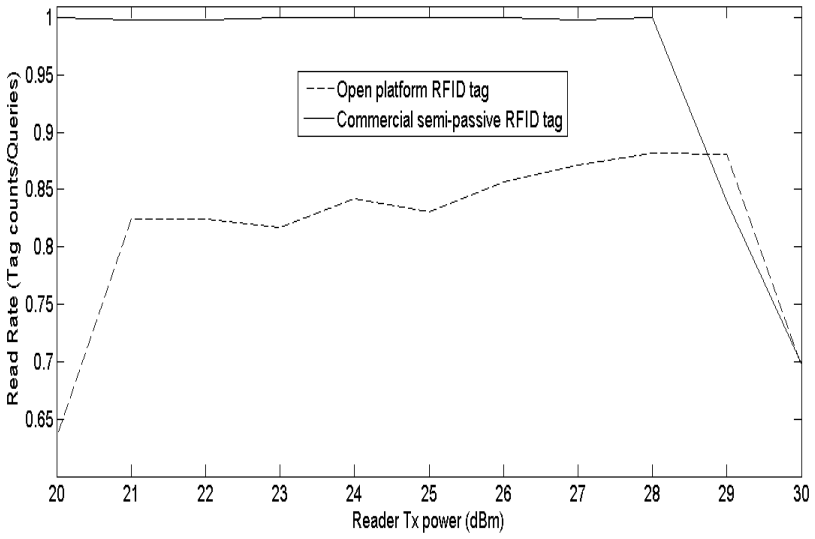

Figure 7.5: Read rate of open platform semi-passive tag and commercial semi-passive RFID tag with non-line of sight in a Computer lab

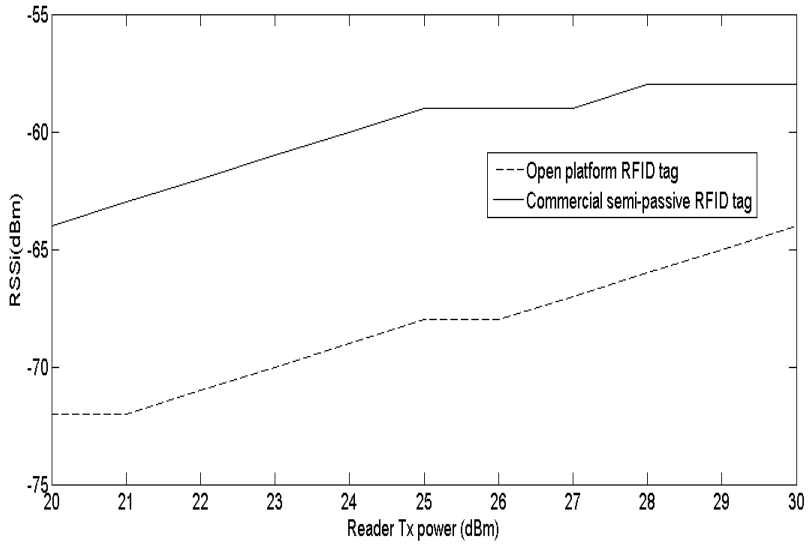

Figure 7.6: RSSi of open platform semi-passive tag and commercial semi-passive RFID tag with non-line of sight in a Computer lab

7.1.2 Fixed reader output power

In this set of experiments, we used a similar setup in 7.1.1. The difference was that we fixed reader output power at 30 dBm, due to maximum allowable reader transmitting power and varying reader-tag distance. The orientation of the tag and reader antennas were fixed to avoid influence of other parameters to read rate besides distance. The experiment started by placing the tag at a distance of two meters from the reader antenna. The measurements were repeated while increasing the distance between the tag and the reader antenna in 0.2 metersteps. Due to the room length, maximum distance we performed measurements at was nine meters. Our open platform semi-passive RFID tag and commercially semi-passive tag were placed in the plane on a single cardboard platform, with the best possible orientation angle to the reader antenna. A total of 1000 query rounds were sent by the reader, and the number of responses from the tag and average of RSSi value from all query rounds were noted. The results show in Figure 7.7 and Figure 7.8.

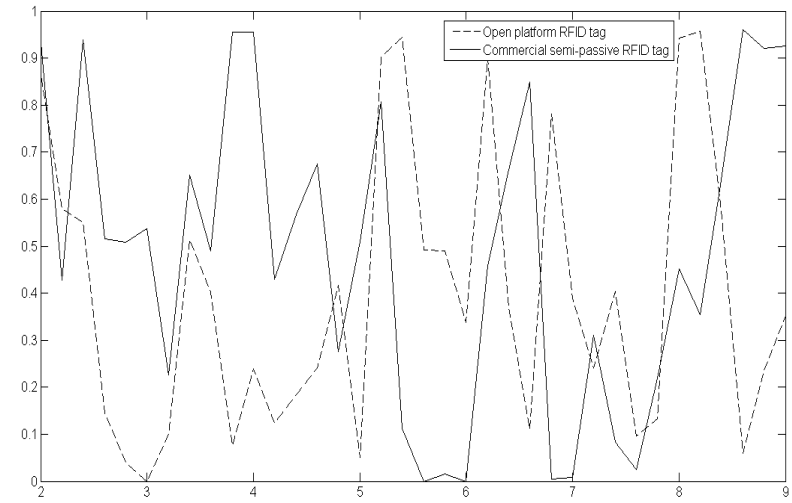

Figure 7.7: Read rate vs Distance of open platform semi-passive tag and commercial semi-passive RFID tag in a Computer lab

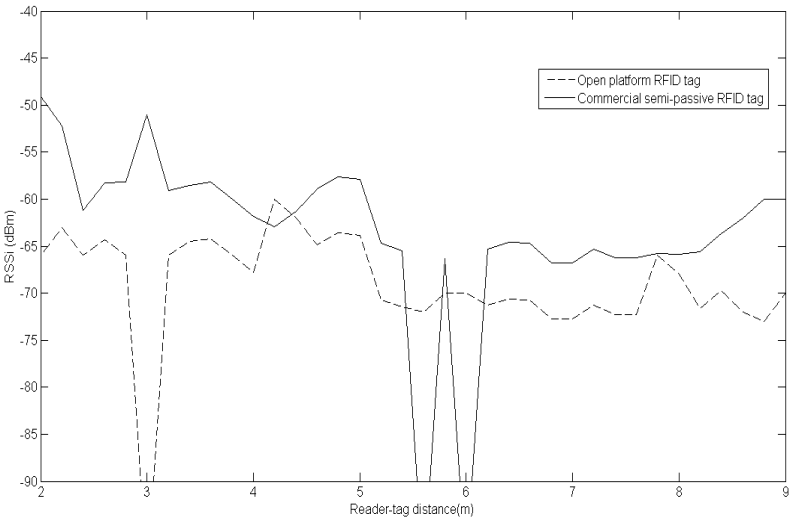

Figure 7.8: RSSi vs Distance of open platform semi-passive tag and commercial semi-passive RFID tag in a Computer lab

Table 7.1: Commercially available antennas

Antenna	Loop antenna	Dipole antenna	Patch antenna
Antenna Gain	1.5 dBi	1.8 dBi	3 dBi
Polarization	Linear	Linear	Linear
Pattern	Omni-directional	Omni-directional	Omni-directional
Connector	SMA	SMA	SMA

7.1.3 Evaluate effects of different commercially available antennas

In this experiment, We tested the performance of the open platform semi-passive UHF RFID tag with different commercially available antennae. We chose a monopole antenna (Figure 7.9), a loop antenna (Figure 7.10), and a patch antenna (Figure 7.11). All three antennae had a standard SMA connector directly connected to the open platform semi-passive RFID tag. Table 7.1 presents some important characteristics of the three antennas. We used an EPCglobal Gen 2 Class 1 reader with a 6dBi gain circularly polarized patch antenna to transmit the wireless signal, and we used the same experiment setup as Subsection 7.1.2. In order to avoid the null reading point, we repeat the experiment. The read rate results are shown in Figure 7.12 and Figure 7.14. The RSSi results are shown in Figure 7.13 and Figure 7.15.

7.1.4 Impedance measurement

The following experiments show the network the impedance of an analog network of open platform semi-passive RFID tag. In the first set of this experiments, we used a voltage controller oscillator (VCO) as a signal generator to feed UHF signal to the analog network. A VCO is an electronic oscillator designed to generate continuous wave. The frequency is varied by input voltage level. The signal generated by VCO will be input of analog network. We observed the output voltage signal at the end of the analog network to determine the return loss of this network. Figure 7.16 shows the block diagram of this experiment. The result of frequency versus output voltage of analog network is illustrated in Figure 7.17. The second part of this experiment was to use a vector network analyzer to observe the impedance of this analog network. We set the starting frequency at 800

Figure 7.9: Commercially available 915MHz monopole antenna

Figure 7.10: Commercially available 915MHz loop antenna

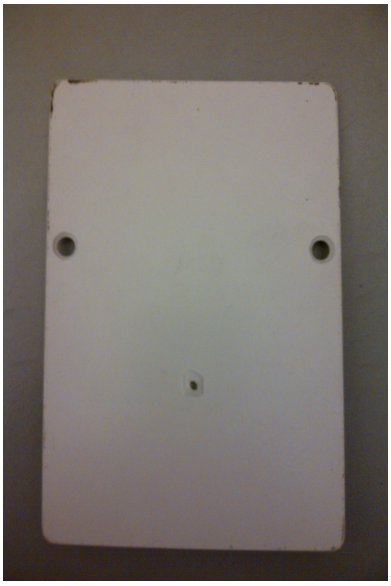

Figure 7.11: Commercially available 915 MHz patch antenna

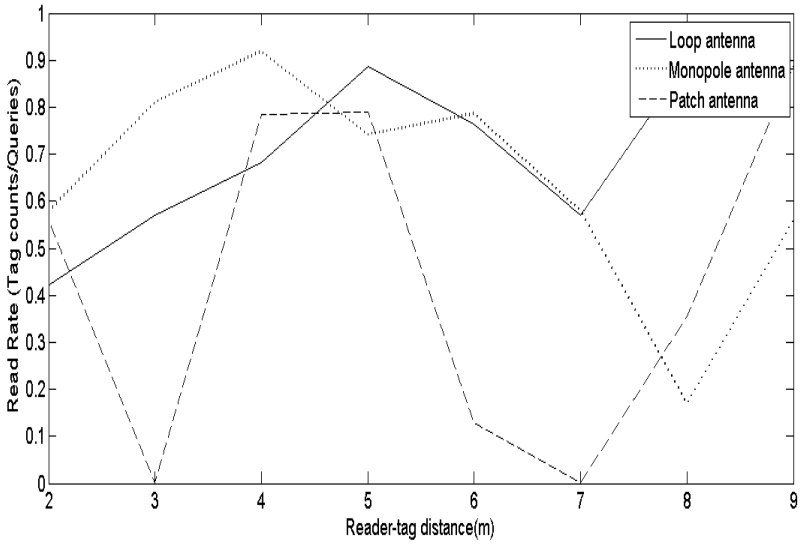

Figure 7.12: Read rate of open platform semi-passive tag in a Computer lab

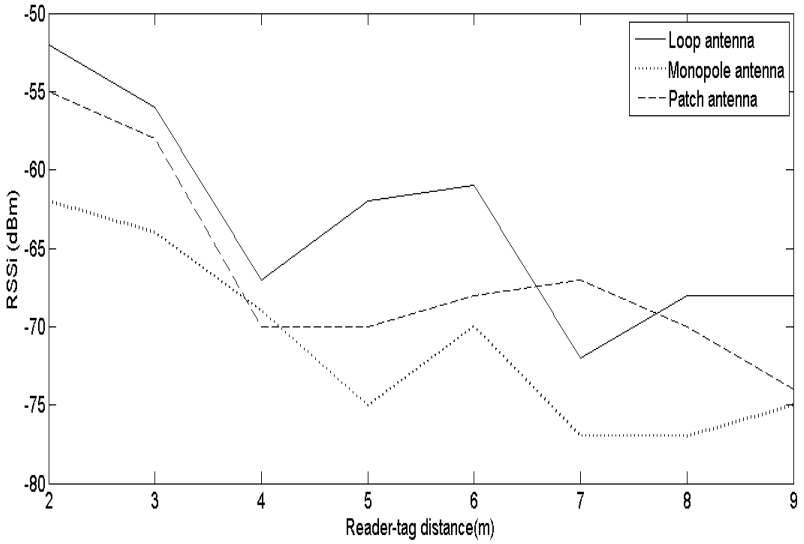

Figure 7.13: RSSi of open platform semi-passive tag in a Computer lab

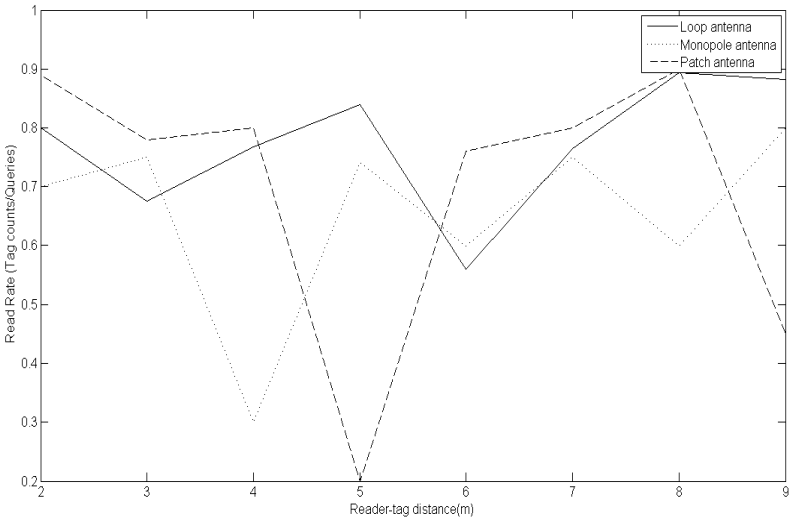

Figure 7.14: Read rate of open platform semi-passive tag in a Computer lab

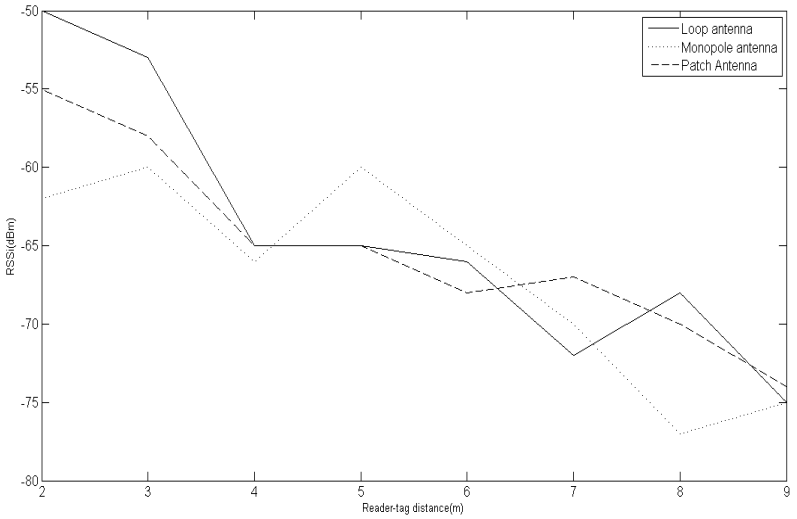

Figure 7.15: RSSi of open platform semi-passive tag in a Computer lab

MHz and stop frequency at 1 GHz. Figure 7.18 shows the Smith chart of impedance of open platform semi-passive RFID tag.

7.1.5 Analysis

The measurement results showed our open platform semi-passive RFID tag can operate as regular semi-passive tag, and that it is compatibility with commercially available antennas with standard SMA connector. It can provide a read rate above 80% when reader output is greater than 24 dBm and reader-tag distance is less than four meters.

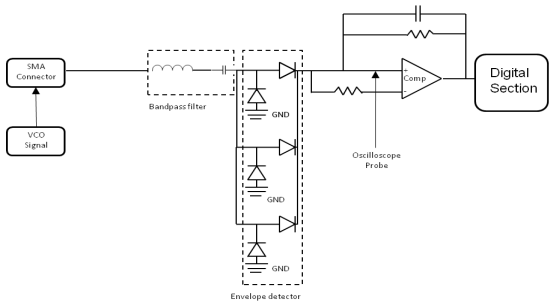

Figure 7.16: Block diagram of a circuit used to measure impedance experiment

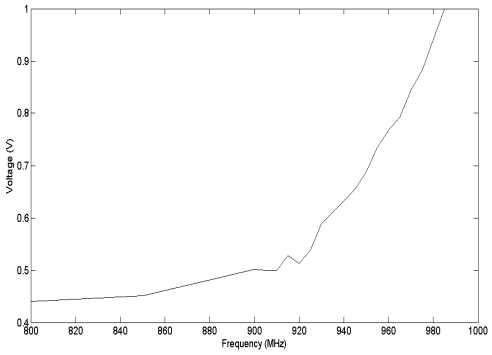

Figure 7.17: Frequency (MHz) vs Output voltage of analog network (V) of the open platform semi-passive RFID tag

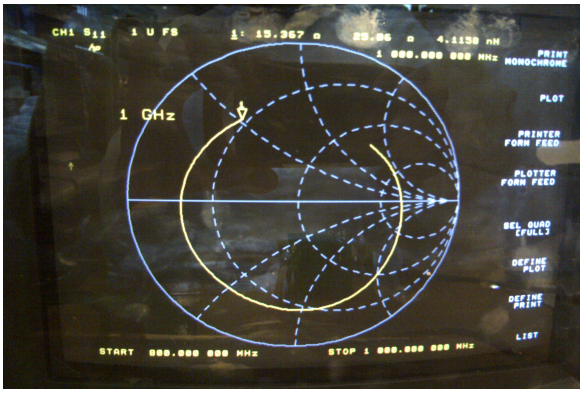

Figure 7.18: Smith chart of network impedance of open platform semi-passive tag

From the results, we also observed several issues for this prototype of an open platform semi-passive UHF RFID tag. Figure 7.3 shows the best read rate of the tag is approximately 90%. There are two reasons for this: the comparator did not digitize the signal properly due to analog baseband signals that were still too sensitive to its low pass version, and the tag input impedance was mismatched so the the analog baseband signals was very weak at certain frequencies. These issues reduced the performance of the open platform semi-passive RFID tag. Another observation shown in Figure 7.3 illustrates the sensitivity of the open platform semi-passive RFID tag. When the reader transmit signal power is less than 21 dBm, and reader-tag distance is around four meters, the read rate of the tag drops exponentially. Figure 7.4 shows that when the RSSi falls below -87 dBm, the reader can no longer detect the tag. Figure 7.3 and Figure 7.4 provide very interesting observations. In this Figure 7.3, the read rate of the open platform semi-passive UHF RFID tag and a commercially available semi-passive tag drop around zero at certrain points, and the read rate varies, regardless of reader-tag separation. This is due to null reading points we mention in Chapter 3. At null reading point, the reader signal and reflected signal cancel each other out. When we increase the reader-tag separation, the tag is no longer in null reading points, so the read rate increase back to normal. Another observation, from Figure 7.7 shows much variation in the read rate of the open platform RFID tag and the commercial semi-passive tag, which demonstrates how the environment can seriously impact the performance of an RFID system. Figure 7.4 shows the RSSi value drop as reader-tag distance increases, except at null reading points. Comparing Figure 7.12, 7.14, 7.13 and 7.15 shows by repeating the experiments that the performance of read rate varies due to null reading point. This concludes when reader can receive the tag signals, the signal streangth is following Friis Equation 3.1, the reader-tag distance increases, and the power drops. Figure 7.17 and Figure 7.18 points out that this open platform semi-passive RFID tag is not well tuned to the desired frequency, and it required addition tuning to achieve good performance. This is one of the root causes that impact the performance of the tag, and all these factors bring down the performance. The hysteresis comparator also reduces the tag performance, as the calculated value can not be used directly in practice. The environment has a big impact on UHF RFID tag performance, as shown from Figure 7.3 to 7.13. The reflect reader signal may bring down the read rate, but it also helps reader-tag communication when tag-reader is in non-line of sight situations.

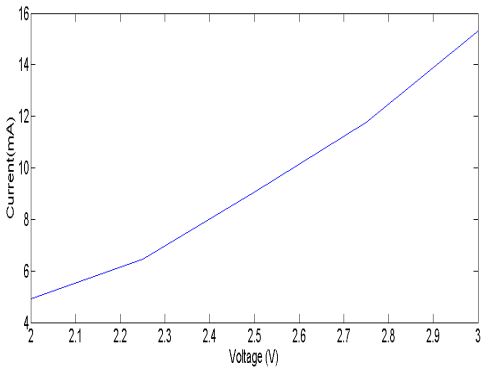

Figure 7.19: Voltage (V) VS Current (mA) of open platform semi-passive RFID tag

7.2 Power consumption

Another important parameter to use to evaluate the semi-passive RFID tag is the power performance. As a semi-passive tag requires battery assistance, the device life relies on battery life. We are measuring the voltage and current at different scenarios to determine overall power performance.

7.2.1 Voltage versus current

First experiment was to measure the voltage versus current. We begin at 3V that the regular 2 x AAA fully charged batteries will supply. Then we reduced the input voltage from 3V to 2V in 0.25 V steps. According to PIC microcontroller manual, the minimum supply voltage in 8MHz is 2V. We used multimeter to measure the current; the outcomes were shown in Figure 7.19. The results were gathered while the open platform semi-passive RFID tag was backscattering to the RFID reader.

7.2.2 Backscattering power consumption

In this experiment, we measured the current vs input voltage when the open platform semi-passive UHF RFID tag is communicating with the reader, and when it is outside of the reading zone of the reader. Table 7.2 shows the current measurement results for various input voltage source.

Table 7.2: Power consumption in executing mode and idle mode

Voltage (V)	Backscattering Mode (mA)	No backscattering mode (mA)
3	15.32	15.32
2.75	11.76	11.76
2.5	9.06	9.06
2.25	6.46	6.45
2	5.0	4.9

7.2.3 Analysis

Figure 7.19 shows that the open platform semi-passive RFID tag consumes much more power at a higher input voltage than at lower voltage: 45mW vs. 8.9 mW respectively. Limiting the input voltage to 2V does not affect read rate and RSSi of the open platform semi-passive RFID tag and also saves considerable power which increases device life cycle. Table 7.2 shows us that the backscattering mode does not drain more current than non backscattering mode. Thus, the semi-passive open platform RFID tag does not waste energy when transmitting data.

7.3 Application of the open platform semi-passive RFID sensor network

In this section, we integrated a digital temperature sensor into the open platform semi-passive RFID tag. The tag uses I^2C protocol to communicate with the sensor. The access temperature data function block implements inside custom sub-function blocks. Figure 7.20 shows the state diagram of open platform semi-passive RFID sensor tag. We modified the original state diagram of EPCglobal Gen 2 Class 1 to fit sensor network requirement. The state of ARBITRARY, READ, REPLY are defined in EPCglobal Gen 2 Class 1. We added new state ReadSensor to read sensor data. When tag first boots up, it acceses to temperature sensor to gather temperature data, then save the date and generate corresponding CRC value based on temperature data. The reason to do this is that CRC calculation requires 225 ns when tag system frequency is set to 8MHz. According to EPGglobal Gen 2 Class 1 [4], the tag needs to response in approximately 40 ns when backscattering signals rate is set to 256KHz/Miller 4 mode. The tag can not generate CRC value in real time when tag system frequency is running in 8MHz. Figure

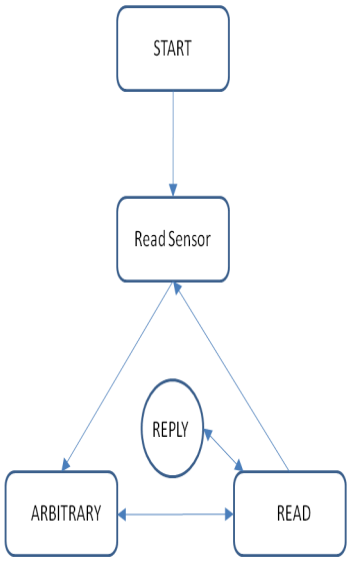

Figure 7.20: Open platform semi-passive RFID sensor tag block diagram

7.21 shows the flow chart of this process.

In the firmware code for the PIC microcontroller, we needed to add new function ReadSensor Data. This function has access to the temperature sensor via I_2C bus. The function is implemented in custom subfuction block. As mentioned above, the tag calls this function at initial stage to get sensor data and generate CRC value. Then the tag state moves to READY state and waits for a reader command. After tag responses READ command to reader, the tag will call this function to access new temperature data, then go to ARBITRARY state. We only needed to do small modification to original tag firmware code.

On the GUI side, we added the target tag's EPC into sensor tag list, shown in Figure 7.22. By doing this, the GUI will automatically request data from this tag. This is specific functionality we implemented for this application. We set the interval of each query round to one second. At the beginning of experiment, we place the tag in the computer lab. During the experiment, we placed a finger on the digital sensor for several minutes, then remove it. The results, in Figure 7.23, show that the temperature increase in middle of the experiment, and then drop back to room temperature.

We repeated the experiment described in 7.2.1 to measure the voltage and current, to determine the power consumption for open platform semi-passive RFID sensor tag. During the experiment, we access the temperature sensor once per second. Figure 7.24 shows the measurement result. The overall power consumption of the tag is almost the

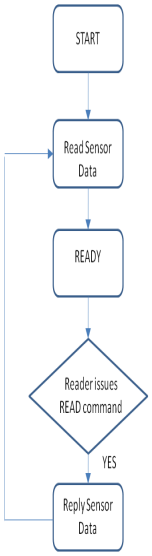

Figure 7.21: Open platform semi-passive RFID sensor tag flow chart

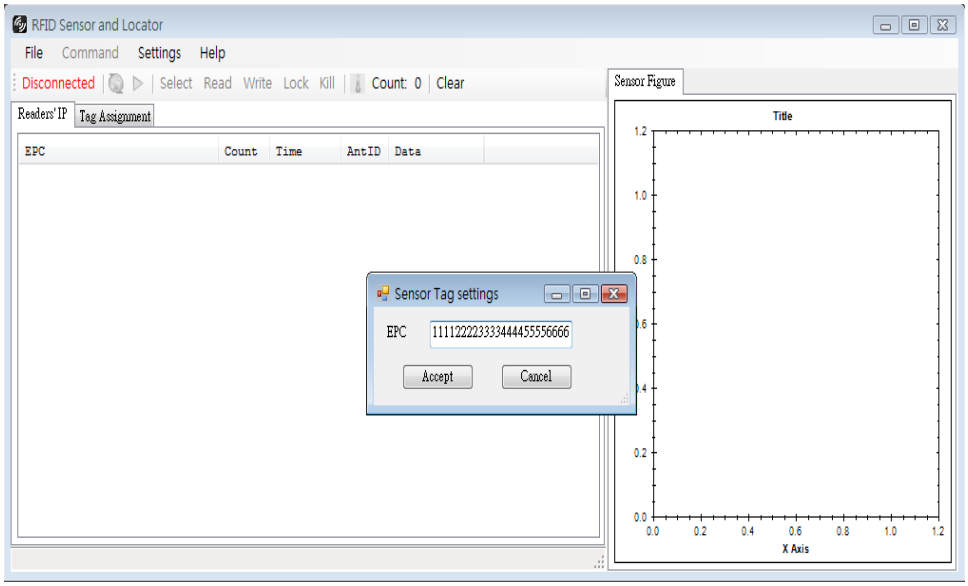

Figure 7.22: Add EPC into sensor tag list

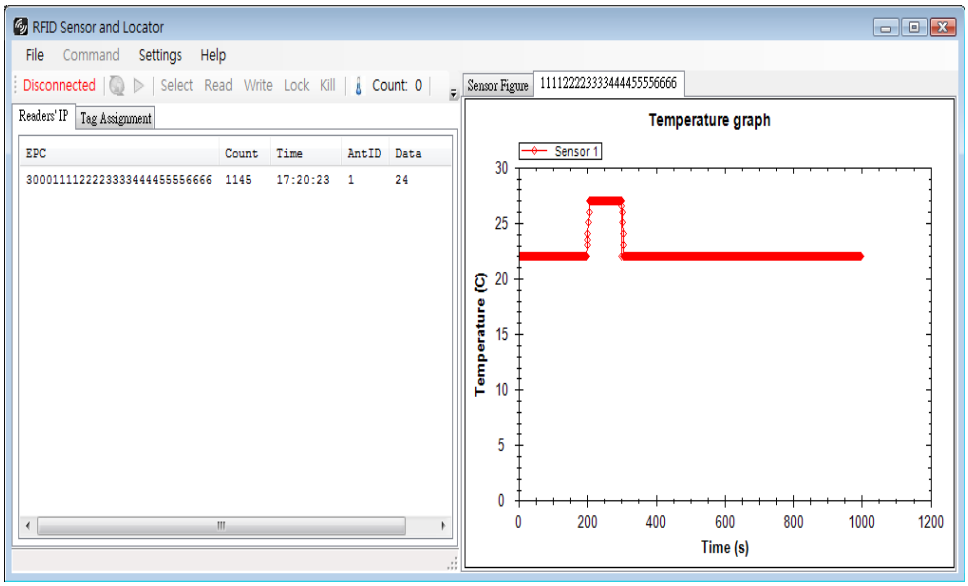

Figure 7.23: Open platform semi-passive RFID sensor tag result

same as open platform semi-passive RFID sensor tag. According to sensor data sheet, the digital sensor requires 100 nA in executing mode[88]. The results shows the open platform semi-passive RFID sensor tag can be used as low power wireless sensor.

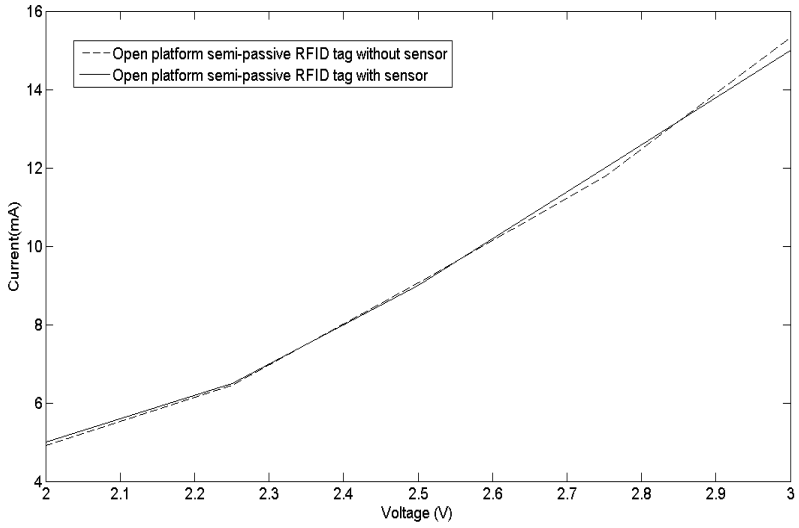

Figure 7.24: Voltage versus current of Open platform semi-passive RFID tag and Open platform semi-passive RFID sensor tag

Chapter 8

Conclusion

This thesis demonstrates an open platform semi-passive RFID sensor tag with an RFID reader GUI system. We experimented with the performance characteristics of commercially available passive and semi-passive tags, and found the passive tags were highly affected by range, environment and the antenna type. The performance of an open development platform for semi-passive UHF RFID sensor tags was eavluated according to range, reliability and power consumption. Range and reliability were compared to commercially available semi-passive tags, and device lifetime to other short range wireless sensor devices. We also integrated a temperature sensor, which allowed us to demonstrate the extensibility of this tag in both hardware and software.

8.1 Contribution

The main contribution of this thesis is the development of an open platform semi-passive UHF RFID sensor tag. Compared with commercially available semi-passive tags, it was found that the open platform tag could operate as a standard semi-passive tag, and could also support the addition of external sensors. The tag can be integrated into many other applications involving short range communication, and it supports the basic EPCglobal Gen 2 Class 1 [4] commands required to operate as a standard semi-passive UHF RFID tag. We expanded the tag into an RFID sensor network, and succssfully demonstrated how it can be integrated with a digital sensor. Standard RFID reader can get the sensor data from the open platform semi-passvie UHF RFID tag.

8.2 Future work

After analyzing the results from chapter 7 and considering the suggestions of others, we have determined there are four main extensions to this work. One extension is to enable full support of transmitted reader signals and backscattering signals data rates without increasing the working frequency of the microcontroller (our study limited the transmitted reader and backscattering signals data rates). A full support data rate RFID tag would give user more freedom. A possible solution is to integrate a complex programmable logic device (CPLD) into open platform RFID tags, as the microcontroller could offload the encoder/decoder functionality to the CPLD.

The second extension is to improve the read rate. We need to tune the input impedance to the desired frequency. Comparator hysteresis is another component requiring further investigation to provide maximum performance.

Another extension to this work is to improve power management. First, we could add 2V voltage regulator to limit the supply voltage to 2V. From the testing result, the tag only consumes 8.9 mW, and this could extend tag device lifetime. Another approach would be to replace the general purpose PIC microcontroller with an extreme low power PIC microcontroller. According to PIC website, the active mode current is only 50 uA/MHz [89].

Further research could be done on integrating different sensors and hardware. This thesis explored basic functionality of a semi-passive RFID sensor tag with an integrated temperature sensor, and explored the creation of a short range sensor network. However, there is still much room for investigation.

Appendix A

Acronym

ADC	analog digital converter
ASIC	application-specific integrated circuits
BAC	battery-assisted-circuit
CPLD	complex programmable logic device
DSP	digital signal processing
EPC	electronic product code
HF	high frequency
GUI	graphic user interfaces
IC	integrate circuit
IDE	integrated development environment
ISM	industrial, scientific and medical
LF	low frequency
LLRP	low level reader protocol
M4	miller 4
PC	protocol control

PCB	printed circuit board
PHY	physical
PIE	pulse interval encoding
PW	pulse width
RF	radio frequency
RFID	radio frequency identification
RN16	16-bit random number
RSSi	received signal strength indicator
RTF	reader talks first
SHF	super high frequency
SNR	signal to noise ratio
TTF	tag talks first
UHF	ultra high frequency
UPC	universal product code
VCO	voltage controller oscillator
WISP	wireless sensor identification platform
WSN	wireless sensor network

Bibliography

[1] K. Finkenzeller, *RFID Handbook*, Wiley, second edition edition, 2003.

[2] M. Bolić, *ELG 6158: Radio Frequency Identification (RFID) Technology*, University of Ottawa, 2009.

[3] S. Meloan, "Toward a Global Internet of Things," http://java.sun.com/developer/technicalArticles/Ecommerce/rfid/, 2003.

[4] EPCglobal Inc., "EPC radio frequency identification protocols class 1 generation 2 UHF RFID protocol for communications at 860 MHz 960 MHz)," Standard Specification version 1.2.0, October 2008.

[5] D.M. Dobkin and S.M. Weigand, "Environmental effects on rfid tag antennas," in *Microwave Symposium Digest*, June 2005.

[6] H.C. Liu, M.C. Hua, C.G. Peng, and J.P. Ciou, "A novel battery-assisted Class-1 Generation-2 RF identification tag design," in *IEEE Trans. on Microwave Theory and Techniques*, 2009, vol. 57, pp. 1388–1397.

[7] K.V.S. Rao, "An overview of backscattered radio frequency identification system (RFID)," in *Microwave Conference*, 1999, vol. 3, pp. 746–749 vol.3.

[8] A. Rahmati, L. Zhong, M. Hiltunen, and R. Jana, "Reliability techniques for rfid-based object tracking applications," in *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2007, pp. 113–118.

[9] K. Koscher, A. Juels, T. Kohno, and V. Brajkovic, "EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond," in *ACM Conference on Computer and Communications Security*, 2009, pp. 33–42.

[10] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," in *International Workshop on Wearable and Implantable Body Sensor Networks*. Citeseer, 2004, vol. 5.

[11] "Wisp wiki," http://wisp.wikispaces.com/, Last access date: 2011/04/01.

[12] IAIK TU Graz, "RFID tag emulators for HF and UHF frequency range," http://www.iaik.tugraz.at/, Last access date: 2011/04/01.

[13] CAEN RFID, "CAEN RFID," http://www.caenrfid.it/rfid/, Last access date: 2011/04/01.

[14] Confidex, "Confidex RFID C1G2 UHF tag solutions," http://www.confidex.fi/, Last access date: 2011/04/01.

[15] M. Aigner, T. Plos, A. Ruhanen, and S. Coluccini, *Secure Semi-Passive RFID Tags Prototype and Analysis*, BRIDGE project, 2009.

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

[17] T. H. Li and M. Bolić, "Performance of passive and semi-passive UHF RFID systems," in *23rd Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2010.

[18] A. Bensky, *Short-range Wireless Communication: Fundamentals of RF System Design and Application*, Newnes, 2004.

[19] A.P. Subramanian, P. Deshpande, J. Gaojgao, and S.R. Das, "Drive-by localization of roadside WiFi networks," in *The 27th Conference on Computer Communications*, pp. 718–725.

[20] C. Floerkemeier and M. Lampe, "RFID middleware design: addressing application requirements and RFID constraints," in *Proceedings of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies*, p. 224.

[21] RFID Journal, "ISO18000-6," http://www.rfidjournal.com/article/view/2481/1/1, Last access date: 2011/04/01.

[22] S. Ahson and M. Ilyas, *RFID handbook: applications, technology, security, and privacy*, CRC, 2008.

[23] C. Angerer, M. Holzer, B. Knerr, and M. Rupp, "A flexible dual frequency testbed for RFID," in *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, p. 3.

[24] C. Ying, "A Verification Development Platform for UHF RFID Reader," in *WRI International Conference on Communications and Mobile Computing*, 2009.

[25] 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.

[26] A.K. Jones, R.R. Hoare, S.R. Dontharaju, S. Tung, R. Sprang, J. Fazekas, J.T. Cain, and M.H. Mickle, "A field programmable RFID tag and associated design flow," in *14th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, 2006, pp. 165–174.

[27] AAP Sample, DDJ Yeager, PPS Powledge, AAV Mamishev, and JJR Smith, "Design of an rfid-based battery-free programmable sensing platform," .

[28] EM Microelectronic, "1 kbit read/write, ISO 18000-6c epc c-1 g-2 passive / battery-assisted passive contactless ic," http://www.emmicroelectronic.com, Last access date: 2011/04/01.

[29] International Organization for Standardization, "ISO/IEC 18000-7: Information technology radio frequency identification for item management - part 7," 2009.

[30] E. Egea-López, J. Vales-Alonso, A. Martínez-Sala, M. Bueno-Delgado, and J. Garcia-Haro, "Performance evaluation of non-persistent CSMA as anti-collision protocol for active RFID tags," *Wired/Wireless Internet Communications*, pp. 279–289, 2007.

[31] S. Farahani, *ZigBee wireless networks and transceivers*, Newnes, 2008.

[32] MEMSIC, "TELOSB MOTE PLATFORM," http://memsic.com/, Last access date: 2011/04/01.

[33] OSHW, "OSHW definition," http://www.openhardwaresummit.org/oshw-definition-v1-0/, Last access date: 2011/04/01.

[34] D. Bovet, M. Cesati, and A. Oram, *Understanding the Linux kernel*, O'Reilly & Associates, Inc., 2002.

[35] C.H. Loo, K. Elmahgoub, F. Yang, D. Elsherbeni, A.and Kajfez, A. Kishk, and T. Elsherbeni, "Chip impedance matching for UHF RFID tag antenna design," in *Progress In Electromagnerics Research*, 2008, pp. 359–370.

[36] M. Nikkari, T. Bjorninen, L. Sydanheimo, L. Ukkonen, A. Elsherbeni, Fan Yang, and M. Kivikoski, "Performance of a passive UHF RFID tag in reflective environment," in *Antennas and Propagation Society International Symposium*, July 2008.

[37] A. Lazaro, D. Gribau, and D. Salinasu, "Radio link budgets for UHF RFID on multipath environments," in *IEEE Transactions on Antennas and Propagation*, 2009, vol. 57, pp. 1241–1251.

[38] M. Polivka, M. Svanda, P. Hudec, and S. Zvanovec, "UHF RF identification of people in indoor and open areas," in *IEEE Transactions on Microwave Theory and Techniques*, 2009, vol. 57, pp. 1341–1347.

[39] Jong-Wook Lee, Hongil Kwon, and B. Lee, "Design consideration of uhf rfid tag for increased reading range," in *Microwave Symposium Digest*, June 2006, pp. 1588–1591.

[40] D. M. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*, Elsevier - Newnes, 2007.

[41] Federal Communications Commission, "PART 15–RADIO FREQUENCY DEVICES," http://ecfr.gpoaccess.gov/, Last access date: 2011/04/01.

[42] V. Derbek, C. Steger, R. Weiss, J. Preishuber-Pflugl, and M. Pistauer, "A UHF RFID measurement and evaluation test system," *Electrotechnic and Informationstechnick*, vol. 124, no. 11, pp. 384–390, 2007.

[43] K. N. Ramakrishnan, "Performance benchmarks for passive UHF RFID tags," M.S. thesis, University of Kansas, 2005.

[44] P. Nikitin and V. Rao, "Performance limitations of UHF RFID systems," in *IEEE Antennas and Propagation Symposium*, 2006, pp. 1011–1014.

[45] S. D'Mello, E. Mathews, L. McCauley, and J. Markham, "Impact of position and orientation of RFID tags on real time asset tracking in a supply chain," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 3, no. 1, pp. 1–12, 2008.

[46] I. A. Currie and M. K. Marina, "Experimental evaluation of read performance for RFID-based mobile sensor data gathering applications," in *Proceedings of the 7th International Conference on Mobile and Ubiquitous Multimedia*, Umea, Sweden, 2008, pp. 92–95.

[47] R.C. Dorf and J.A. Svoboda, *Introduction to electric circuits*, Wiley, 2007.

[48] MAXIM, "Data slicing techniques for uhf ask receiver, application note 3671," http://www.maxim-ic.com/app-notes/index.mvp/id/3671, Last access date: 2011/04/01.

[49] Microchip Technology, "Pic24fj64ga004 family," http://ww1.microchip.com/downloads/en/DeviceDoc/39881D.pdf, Last access date: 2011/04/01.

[50] Microchip, "Mplab ide," http://www.microchip.com/, Last access date: 2011/04/01.

[51] Microchip Technology, "Mplab integrated development environment," .

[52] M. Buettner and D. Wetherall, "An empirical study of UHF RFID performance," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 223–234.

[53] EPCglobal Inc., "Low Level Reader Protocol (LLRP)," Standard Specification version 1.1, October 2010.

[54] B.H. Toby, "EXPGUI, a graphical user interface for GSAS," *Journal of Applied Crystallography*, vol. 34, no. 2, pp. 210–213, 2001.

[55] ZedGraph Wiki, "Zedgraph," http://zedgraph.org, Last access date:2011/04/01.

[56] T. H. Li and A. Borisenko, "Open platform semi-passive RFID tag," http://rfid.site.uottawa.ca/wiki/, Last access date: 2011/04/01.

[57] D.W. Engels and S.E. Sarma, "The reader collision problem," in *IEEE International Conference on Systems, Man and Cybernetics*, 2002, vol. 3, p. 6.

[58] J. Waldrop, D.W. Engels, and S.E. Sarma, "Colorwave: an anticollision algorithm for the reader collision problem," in *IEEE International Conference on Communications*, 2003, vol. 2, pp. 1206–1210.

[59] Auto ID Center, "Draft protocol specification for a 900 MHz class 0 RFID tag," http://www.gs1.org/docs/epcglobal/standards/specs/, February Last access date: 2011/04/01.

[60] Auto ID Center, "860mhz - 930mhz RFID tag RF and logical communication interface specification," November 2002.

[61] D.H. Shih, P.L. Sun, D.C. Yen, and S.M. Huang, "Taxonomy and survey of RFID anti-collision protocols," *Computer communications*, vol. 29, no. 11, pp. 2150–2166, 2006.

[62] Z.J. Guo and T.L. Hung, "Study on anti-collision algorithms in UHF RFID systems," *In Third International Conference on Genetic and Evolutionary Computing*, pp. 458–461, October 2009.

[63] K.W. Chin and D. Klair, "Aloha-Based Protocols," *RFID Systems: Research Trends and Challenges*, 2010.

[64] P. Popovski, "Tree-Based Anti-Collision Protocols for RFID Tags," *RFID Systems: Research Trends and Challenges*, 2010.

[65] J. Myung and W. Lee, "Adaptive binary splitting: a RFID tag collision arbitration protocol for tag identification," *Mobile networks and applications*, vol. 11, no. 5, pp. 711–722, 2006.

[66] J.R. Cha and J.H. Kim, "Novel anti-collision algorithms for fast object identification in rfid system," in *11th International Conference on Parallel and Distributed Systems*, 2005, vol. 2, pp. 63–67.

[67] X. Shi, X.W. Shi, Q. Huang, and F. Wei, "An enhanced binary anti-collision algorithm of backtracking in RFID system," *Progress In Electromagnetics Research*, vol. 4, pp. 263–271, 2008.

[68] W. Su, N. Alchazidis, and T.T. Ha, "Multiple rfid tags access algorithm," *IEEE Transactions on Mobile Computing*, 2009.

[69] A. Hoffman, J. Holm, and H.J. Marais, "A comparison of TTF and RTF UHF RFID Protocols," *RFID Systems: Research Trends and Challenges*, 2010.

[70] S. Jain and S.R. Das, "Collision avoidance in a dense RFID network," in *Proceedings of the 1st international workshop on Wireless network testbeds*. ACM, 2006, pp. 49–56.

[71] Z. Zhou, H. Gupta, S.R. Das, and X. Zhu, "Slotted scheduled tag access in multi-reader RFID systems," in *IEEE International Conference on Network Protocols*. IEEE, 2007, pp. 61–70.

[72] TinyOS community forum, ," http://www.tinyos.net, Last access date: 2011/04/01.

[73] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," *ACM Sigplan Notices*, vol. 35, no. 11, pp. 93–104, 2000.

[74] J.W. Hui and D.E. Culler, "IP is dead, long live IP for wireless sensor networks," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, 2008, pp. 15–28.

[75] MEMSIC: wireless modules, ," http://www.memsic.com/products/wireless-sensor-networks/wireless-modules.html, Last access date: 2011/04/01.

[76] J. Polastre, R. Szewczyk, and D. Culler, "Telos: enabling ultra-low power wireless research," in *Fourth International Symposium on Information Processing in Sensor Networks*, 2005, pp. 364–369.

[77] M. Buettner, B. Greenstein, A. Sample, J.R. Smith, and D. Wetherall, "Revisiting smart dust with RFID sensor networks," in *Proceedings of the 7th ACM Workshop on Hot Topics in Networks (HotNets-VII)*, 2008.

[78] S.A. Weis, "RFID Security and Privacy," *Book of Extended Abstracts*, vol. 11, 2005.

[79] S.L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 34–43, 2005.

[80] A. Karygiannis, T. Phillips, and A. Tsibertzopoulos, "RFID security: A taxonomy of risk," *Com Proc. of China*, vol. 6, pp. 1–8, 2006.

[81] M.R. Rieback, P.N.D. Simpson, B. Crispo, and A.S. Tanenbaum, "RFID malware: Design principles and examples," *Pervasive and mobile computing*, vol. 2, no. 4, pp. 405–426, 2006.

[82] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approaches for Improving Security and Privacy Issues of RFID Systems," *RFID Systems: Research Trends and Challenges*, p. 447, 2010.

[83] K.V.S. Rao, P.V. Nikitin, and S.F. Lam, "Antenna design for UHF RFID tags: A review and a practical application," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 12, pp. 3870–3876, 2005.

[84] D. Deavours, "UHF RFID Antennas," *RFID Systems: Research Trends and Challenges*, 2010.

[85] A. Ibrahiem, T.P. Vuong, A. Ghiotto, and S. Tedjini, "New design antenna for RFID UHF tags," in *IEEE Antennas and Propagation Society International Symposium*, 2006, pp. 1355–1358.

[86] Y. Choi, U. Kim, J. Kim, and J. Choi, "Design of modified folded dipole antenna for UHF RFID tag," *Electronics letters*, vol. 45, no. 8, pp. 387–389, 2009.

[87] L. Mao, R. Song, Y. Li, and L. Chen, "UHF RFID Tag Antenna Design and a Novel Antenna Verification Development Platform," in *Fourth International Conference on Wireless Communications, Networking and Mobile Computing,*, 2008, pp. 1–3.

[88] ST, "Digital temperature sensor and thermal watchdog," http://www.st.com/, Last access date: 2011/04/01.

[89] Microchip Technology, "Extreme low power micrcontroller," http://www.microchip.com, Last access date: 2011/04/01.