Implementation and Applications of an Anti-Collision Differential-Offset Spread Spectrum RFID System

Document ID: PG-TR-060823-AR
Date: 23 August 2006

Anil Rohatgi
777 Atlantic Ave. Atlanta GA 30332-0250
Voice: (404)894-2951 Fax: (404)894-5935
http://www.propagation.gatech.edu

Implementation and Applications of an Anti-Collision Differential-Offset Spread Spectrum RFID System

A Thesis
Presented to
The Academic Faculty

by

Anil Rohatgi

In Partial Fulfillment
of the Requirements for the Degree
Master of Science in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
December 2006

Implementation and Applications of an Anti-Collision Differential-Offset Spread Spectrum RFID System

Approved by:

Dr. Gregory Durgin, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Andrew F. Peterson
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Gisele Bennett
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: August 2006

ACKNOWLEDGEMENTS

Without the support and guidance from family, friends and colleagues, the production of this document would not have been possible. First, I would like to thank my parents Ajeet and Rosine Rohatgi for supporting me in all aspects of my life regardless of what path I choose. I would like to thank my advisor Gregory Durgin, for taking me in and allowing me to develop my own research and ideas while offering his opinion, knowledge, and advice when needed. A special thank you to the rest of the Georgia Tech Propagation Group, who over the years have become like a family to me and have helped me brainstorm and problem-solve my way through this thesis. Lastly, I would like to thank the Georgia Institute of Technology for giving me the knowledge and resources to make this project possible.

TABLE OF CONTENTS:

LIST OF TABLES:

LIST OF FIGURES:

SUMMARY

Radio Frequency Identification (RFID) is quickly emerging as a technology with numerous applications with the potential to drastically change the world. RFID describes a system by which any product can be labeled with essentially any information that the owner can access at any time without having direct contact with the item. Essentially, any pertinent information about an item can be stored on the tag itself, making automation and control incredibly simple, fast, and noninvasive. However, before this technology can become widespread, certain problems and standards for solutions must be implemented.

This report documents the design, construction, and implementation of a differential-offset spread spectrum RFID system, to avoid the problem of anti-collision interference from multiple RFID tags. Anti-collision is the problem of separating the desired data of a single tag from the sea of backscatter produced by other tags when the interrogator sends a query signal into the sensing environment. Currently in industry, this problem is handled by establishing a two way communication link between the tags and the interrogator. However, the procedure to locate a desired tag is slow, and requires complex hardware on each tag in order to facilitate the communication. This additional complexity increases cost and power consumption. The proposed system eliminates the need for this excessive

hardware, and therefore drastically reduces the cost of each tag. Not only is this system cheaper to implement than the current two-way communication link standard with today's industry, but it is faster, requires less power, and by the nature of the design contains an inherent encryption scheme for the data being transmitted.

The basic principles of how this system is constructed are as follow. Specialized RFID tags were designed and fabricated in order to produce a pseudo random code unique to each tag. The design presented in this document allowed simultaneous interrogation of up to 255 tags within one sensing environment. Once queried, the tags then modulate the incoming signal from the interrogator with their own sequence, and reflect the signal back to the interrogator. What the interrogator then receives is a combination of backscatter from all of the tags within the sensing environment. From this point onward, specialized software written in Matlab and LabView uses these unique sequences to isolate the data from a desired tag away from the sea of information being transmitted from every tag. Using this system, numerous applications for experiments and measurements can be devised.

One such application this thesis focuses on is the use of this system to simultaneously measure signal strengths from multiple diversity antennas in order to optimize their position and orientation. Currently, the majority of antenna diversity measurements are taken by measuring the signal strength of

a given configuration one antenna at a time. Because only one antenna is functioning at a time, this measurement falls victim to the various effects produced when both antennas are operational and is not a true measurement of their combined overall performance. However, using the anti-collision RFID system proposed above, the signal strength produced by both antennas can be measured and recorded simultaneously to provide a true representation of their combined performance. This measurement can be used to find the optimal configuration for multiple antennas.

This thesis will fully explore the theories and procedures behind creating this system, and will provide the results and analysis of its performance.

CHAPTER 1:

RFID OVERVIEW

1.1 BRIEF HISTORY

Although the emergence of RFID technology is a recent development, the ideas behind it have been building for decades. Throughout the last century, scientists and researchers have been studying the effects of reflected backscatter in order to harness this potential technique for revolutionizing applications [14,15].

Interest in this field began not for commercial uses, but rather for military purposes. During the Second World War, the need for passive and covert means of transmitting and receiving information became an area of particular interest for countries with strong military agendas. In 1945 a soviet scientist named Leon Theremin invented a covert listening device that retransmitted incident radio waves with audio information modulation. Similarly in 1939, the British government saw the potential in this technology, and applied it to aid them in aerial combat. Their technology named the "Identify Friend or Foe System" or IFF used an early predecessor for RFID and used to label their aircrafts as a means to determine if an incoming plane belonged to them [1][2]. A transponder was placed on each of the British aircrafts, and upon being interrogated by an incoming electromagnetic wave, would transmit an

appropriate signal to identify itself as friendly. This system is often attributed to being the first obvious use of RFID technology [1,2].

In 1948, a ground breaking publication written by a research scientist named Harry Stockman called "*Communication by Means of Reflected Power,*" was the first article that explored the use of backscatter as a means for information transmission. This article investigated the possibilities presented by this technology and the problems associated with it. Unfortunately at the time it was written, science had not evolved to a point where the deployment of this technique was feasible. In fact Stockman himself states in his conclusions that, "considerable research and development work has to be done before the remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored"[3]. Regardless, for the next thirty years researches used this paper as a crucial reference to develop solutions for these problems and make RFID a practical technology [1,2].

1.2 RFID SYSTEM OVERVIEW

To understand the ideas and results presented in this thesis one must first have a basic understanding behind the theories and components that comprise a typical RFID system. A typical RFID system includes two parts: the interrogator and the tags. The interrogator consists of the transmitting and receiving antennas used to query an item for its information. The tags are the components physically placed upon each item where the information is stored.

A communication link is established between the interrogator and the RFID tags through propagation and modulation of radio frequency electromagnetic waves. Figure 1 shows a high level representation of an RFID system.

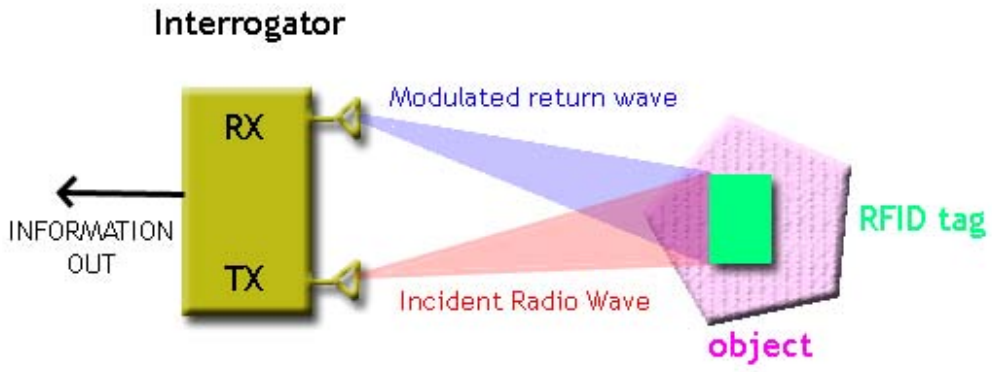


Figure 1. A high-level RFID system diagram. An interrogator illuminates a tagged object with its transmitter (TX) antenna; the tagged object then re-radiates power back towards the interrogator's receiver (RX) antenna.

All of these components will be discussed and explored in more detail in the following sections.

1.2.1 INTERROGATOR

The RFID interrogator is the component of the system that facilitates and initiates communication with the tags. This module consists of both the transmission antenna as well as the receiving antenna. Through the transmission antenna a continuous wave RF signal is broadcast into the sensing environment. The tags then modulate this signal and reflect it back towards the interrogator where it is captured by the receiving antenna. Inside the interrogator, special hardware and software decode the received signal and extract the desired information.

Currently there are eight different bands of frequencies used in RFID applications [2]. Globally each country has its own frequency band for RFID as well [14]. Listed below is a table outlining the benefits and typical applications for some commonly used RF frequency bands.

Table 1.Typical frequency bands used for RFID along with their corresponding advantages and applications [2]

Frequency Band	Characteristics	Typical Applications
Low 100-500 kHz	• Short to medium read range • Inexpensive • Low reading speed	• Access Control • Animal ID • Inventory Control
Intermediate 10-15 MHz	• Short to medium read range • Potentially expensive • Medium reading speed	• Access control • Smart Cards
High 850-950 MHz Ultra High 2.4-5.8 GHz	• Long read range • High reading speed • Line of sight required • Expensive	• Railroad car monitoring • Toll collection systems

1.2.2 RFID TAGS

An RFID tag works by modulating the incoming waveform transmitted from the interrogator, and reflecting this new signal back to the interrogator. The modulation stage is where the data from the tag is encoded into the waveform and propagated back to the system for recovery. To perform this modulation, an RFID tag exploits the impedance matching characteristics of transmission lines.

1.2.2.1 BRIEF TRANSMISSION LINE THEORY

The simplest way to model a wired connection in a conventional circuit is with a pure short-circuit. However, using a short-circuit makes the fundamental

assumption that the electrical signals propagate across the junction instantaneously. This is a valid assumption using DC or low frequency voltages over short distances. However, as the frequency of the voltage source and the distance of transmission increases, this assumption is no longer valid (approximately when the length of the line is 1/100 of the wavelength). In these cases, the effects of the travel velocity, propagation time, and loss mechanisms in the line must all be accounted for. These factors are all taken into account using a model of electrical transmission known as a transmission line. A typical transmission line setup is shown in figure 2 .

- Z_{source} = *impedance of the generator*
- Z_l = *impedance of the destination*
- Z_o= *intrinsic impedance of the transmission line*

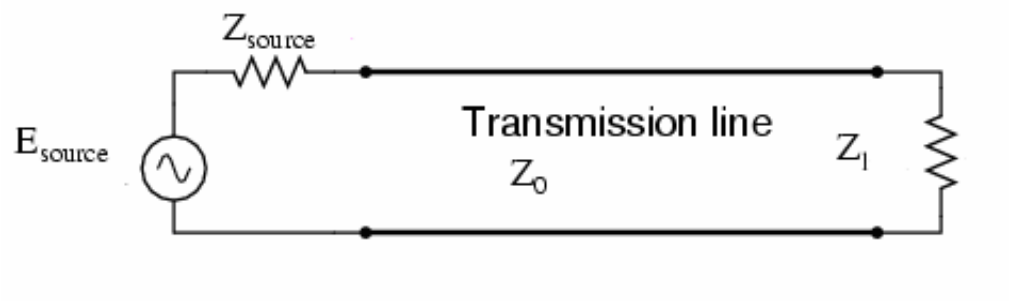


Figure 2. Typical transmission line representation with labeled representative resistances corresponding to physical loss mechanisms. Zsource represents the loss mechanism associated with the source, Zload is the mechanism associated with the load, and Zo is the mechanism associated with the material properties of the transmission line.

The impedances represented above account for all the mechanisms that change the property of an electrical signal as it propagates down the line. The source impedance and load impedance are controlled by the system design. The intrinsic impedance of the line is determined by the material properties of the transmission line and related by the equation 1.

- *w=frequency (Hz/m)*
- *L=inductance (H/m)*
- *R=resistance (OHMS/m)*
- *G=admittance (S/m)*
- *C= capacitance (F/m)*

$$z_o = \sqrt{\frac{jwL + R}{jwC + G}} \qquad (1)$$

Using the impedances above and the equation below, an effective impedance as seen by the source looking down the transmission line can be calculated

- $\beta = \frac{2\pi}{\lambda}$
- *l=length of T-line*

$$Z_{in}(l) = Z_o \times \frac{Z_l \cos(\beta l) + Z_o j \sin(\beta l)}{Z_o \cos(\beta l) + Z_l j \sin(\beta l)} \qquad (2)$$

This effective impedance takes into account the frequency and line length effects caused by the transmission line.

Another result of these factors manifests itself in the spawning of a reflected wave from the load of the system back to the source. The reflected wave is caused by the physical constraints imposed upon the system by the various impedances. In order to maintain the correct boundary conditions at the source and the load resistors, only part of the incident electrical power is absorbed and the rest is reflected back down the line. The equation that governs the amount of power that is reflected at each junction is a function of the intrinsic impedance of the line and the junction impedance given by:

$$\Gamma = \frac{Z_{junction} - Z_o}{Z_{junction} + Z_o}, \quad (3)$$

Where value Γ represents the reflection coefficient for a particular junction between line termination and the equivalent terminating impedance. The fraction of the power that gets absorbed by the load is described by:

$$P_{trans} = P_{inc}(\Gamma + 1) \quad (4)$$

Using the equations 3-4, there are several special case scenarios that can be derived and are included in the table below.

Special Case	**Γ value**	**Physical Interpretation**
Matched load $Z_l=Z_o$	0	No reflection
Open Load $Z_l=\infty$	1	Full reflection, in-phase
Shorted Load $Z_l=0$	-1	Full reflection, out-of-phase

1.2.2.2 RFID TAG ARCHITECTURE

Where typically in electronic devices the spawning of a reflected wave down a transmission line is viewed as a problem and an energy loss mechanism, RFID tags use this phenomenon to their advantage. A high level schematic for a typical RFID tag is shown in figure 3.

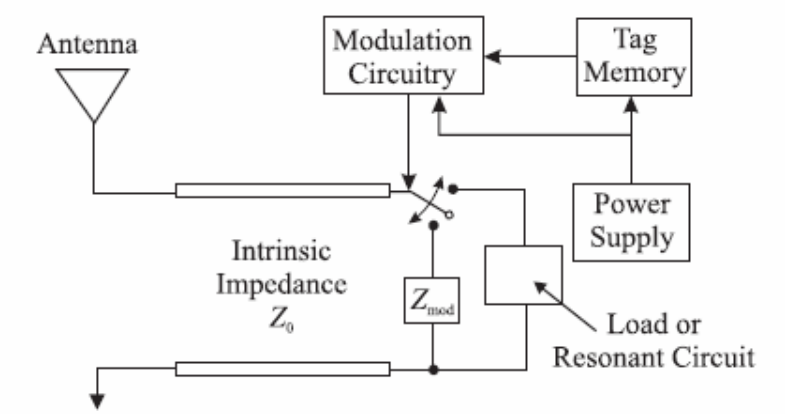


Figure 3. Typical RFID hardware diagram. The RF carrier wave is received through the antenna, and modulated by toggling the diode switch between a matched load and an open circuit. [4]

The tag essentially works as follows: first, the incident radio EM wave is received by the tag through the antenna. The radiated energy is then converted to electrical current and travels down a transmission line configuration with intrinsic impedance Z_0. At the end of the transmission line the electric waveform is met with a diode, represented as a switch in figure 3 and used to toggle between two types of load impedances. When the diode is forward biased, the current is allowed to flow through the matched load making $Z_l = Z_o$, and thus causes the reflection coefficient Γ to equal zero. When the diode is reverse biased, the load impedance essentially become infinite and makes the reflection coefficient Γ equal to one. In the first case, all of the forward traveling current is absorbed by the load and no power is sent backwards through the transmission line. In the latter, no power is absorbed, and all of it is reflected back down the line. In either case, the reflected power is propagated down the transmission line, and radiated out through the antenna. Both scenarios are represented in figures 4 and 5 presented below.

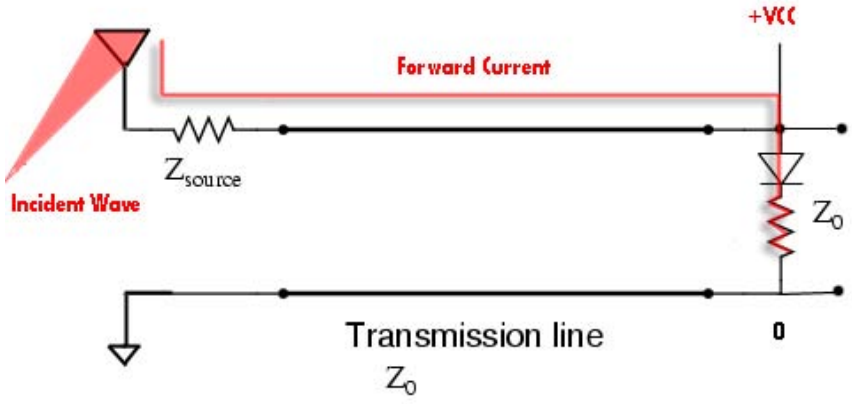


Figure 4. Forward biased RFID tag. All of the incident power is absorbed through the matched load. This configuration transmits a logical 0.

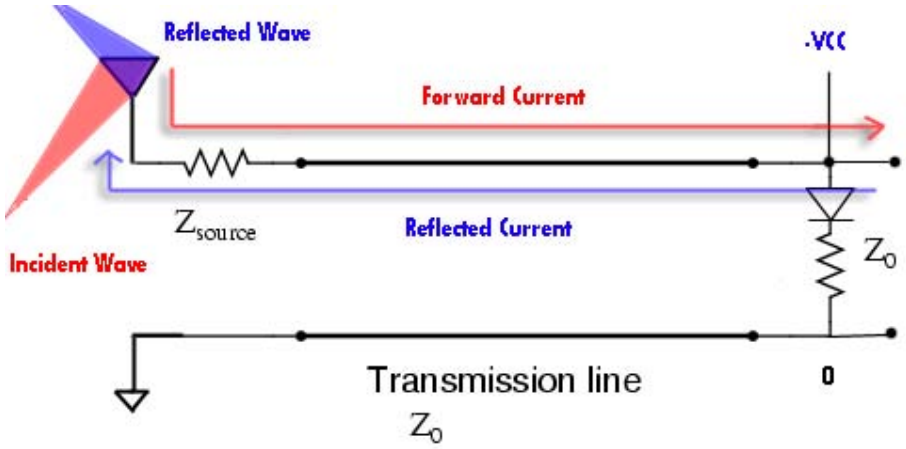


Figure 5. Reverse biased RFID tag. All of the incident power is reflected by the open circuit. This configuration transmits a logical 1

By toggling the bias voltage across the diode, the RFID tag can change between the two states shown in figures 4-5. When all the incident power is reflected the tag transmits a logical bit one. When no power is transmitted the tag transmits a logical bit zero. These bits are propagated through the modulated backscatter, and ride on top of the reflected wave to the receiver. There are several methods to encode the data onto the carrier wave [2,8].

- **Direct Modulation** – The amplitude of the carrier wave varies as a function of the bit pattern. A logical bit one will transmit higher amplitude than a logical bit zero. [2]
- **Frequency Shift Keying (FSK)**- Encodes the bit data by transmitting each bit type with a different frequency. Typically, a logical bit zero is transmitted as an amplitude-modulated clock cycle with a period equivalent to the one eight the tag's clock frequency. A logical bit one is transmitted with a period equal to one tenth the tag's clock frequency. By using the amplitude modulation to separate each bit transition, one simply needs to count the cycles between the peak detected clock edges to recover the data. [2]
- **Phase Shift Keying (PSK)**- Very similar to the FSK method, but instead of modulating the frequency of the waveform this method changes the phase of the carrier wave 180 degrees with each bit change. Two common methods used for PSK is to change the phase for logical bit zero transmitted, or to change the phase with every logic transition, i.e. zero to one or one to zero transition. [2]

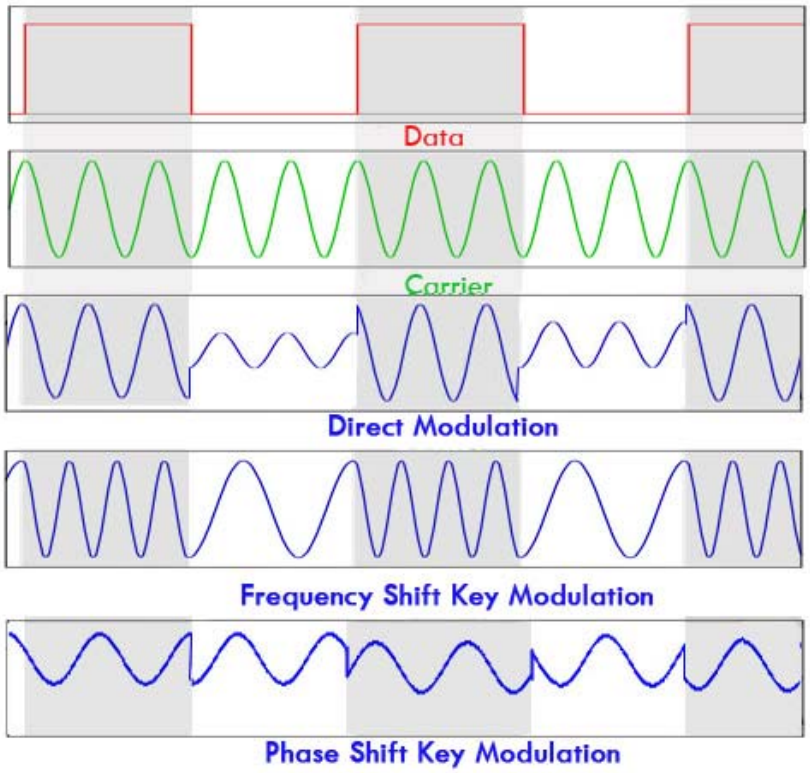


Figure 6. Various forms of carrier wave modulation. The top graphs is the original data needing to be encoded on the carrier wave in the second graph. The following graphs show the resulting waveform using various types of signal modulation.

Regardless of what method of carrier modulation is implemented, any voltage modulation sequence controlled through the tag's memory or circuitry will result in the transmission of a bit pattern that mimics the modulation sequence. Therefore, essentially any binary information stored on the tag can be wirelessly transmitted back to the receiver. This wireless information exchange is the basis for RFID.

1.2.2.2.1 RFID POWER

Another key element of an RFID system is the technology used to power the tags. Currently, there are two types of systems defined by their powering scheme [2, 4]. An active RFID tag uses an on board power source such as a

battery or a solar panel to power the chips necessary to run the RFID tag [2, 4]. Having a constant and reliable source of power allows an active RFID system to have a high read range; however, it also severely limits the shelf life of the tag which is dependant upon the lifetime of the power supply. A passive RFID tag uses a percentage of the power from the incoming RF signal to run the tag [2, 4]. Although this technique removes the RFID tag's dependence on the lifetime of an on board power supply, the amount of power that can be received and used by the RFID tag is often very small and fluctuates rapidly within the sensing environment. For these reasons the read range of a passive RFID system is much lower in comparison to an active system [4].

Both of these techniques are used in commercial applications. The active RFID tag is commonly found in toll booth passes where a single tag is in sensing environment and can be easily accessed and replaced when the power supply dies. In applications where there are a large number of RFID tags that are difficult to access, a passive RFID system would be more desirable. With each approach come advantages and disadvantages inherent to their design. Deciding on which system to use is a matter of weighing these factors to make the optimal choice for a given application.

CHAPTER 2:

ANTI-COLLISION PROBLEM

2.1 DEFINING THE PROBLEM

Although the implementation and design of an RFID system may seem rather straightforward from the sections presented above, there are numerous problems that must be addressed and solved before the system becomes practical. Conventionally, in many existing RFID applications a single-read RFID tag is sufficient [2]. An example of such a system is the automated toll booths that use RFID to identify when a pre-paid vehicle passes through a toll plaza. Since there is only one vehicle at a time passing through the toll booth, at each reading interval there is only one tag inside the sensing environment. However, with the extension of RFID for use in mass deployment for inventory management pioneered by large companies such as Wal-Mart, and the Department of Defense, these systems face numerous and more complex problems [7,14,16].

Since these large RFID systems use only one interrogator and multiple tags, the problem of signal collision arises. When the interrogator transmits a wave to query an item, what it receives is backscatter from every tag within its read range. The overall received signal is the superposition of the backscatter generated from every tag transmitting simultaneously represented by the

equation below and the figure 7. A single tag's information is buried within interference from every other tag transmitting simultaneously [5, 6].

- S_{rec}=*Received Signal*
- *N= number of tags*
- *t=tag number*
- S_t = *backscatter from tag t*

$$S_{rec} = \Sigma_t^N \; S_t \qquad (5)$$

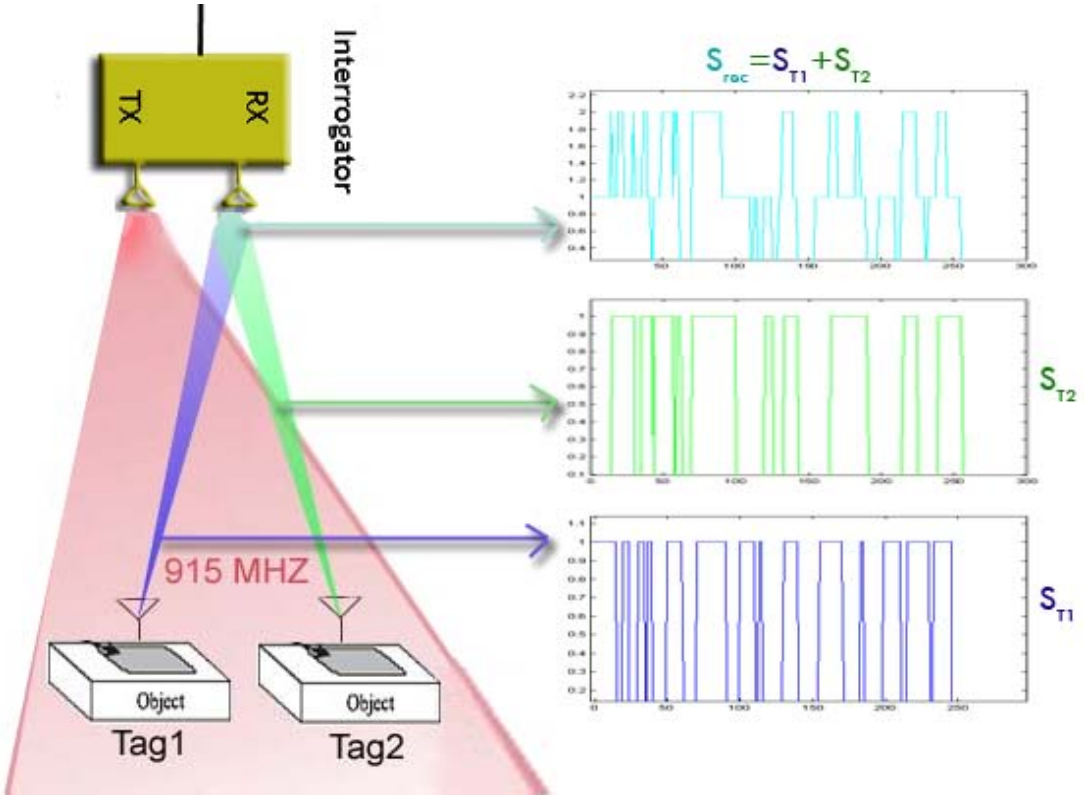


Figure 7. Graphical representation of the problem of signal collision. The interrogator illuminates the sensing environment with a carrier wave of 915MHz, and multiple tags are reflecting their backscattered waveform. S_{t1} is the signal from tag 1, and S_{t2} is the signal from tag 2. S_{rec} is summation of these two tag signals, and is effectively what is received by the interrogator through backscatter.

A simple way to visualize this phenomenon is to use the following analogy. Imagine a crowded room full of people representing the multiple tags, and a single interviewer representing the interrogator. The interviewer shouts a

question into the crowded room, and everyone begins to answer at one time. How does the interviewer select and distinguish a single individual's answer from the combined noise of everyone's response? This is in essence the problem of signal collision.

2.2 CURRENT SOLUTIONS

Currently in industry, a typical solution to multi-tag interference is found by establishing a two-way communication link between the tag and the interrogator. This standard of operation is known as Interrogator-Talks First (ITF) protocol, and is currently the Electronic Product Code (EPC) standard for handling anti-collision for RFID systems operating in the 860MHz-960MHz range [8,18]. Using this configuration, the interrogator must query each tag individually to discover if the tag has the correct ID. If it does not, the tag is commanded to shut down. Through sequential power up and shut down commands, the RFID system searches through all the tags within the environment until all audible tags are identified [5,18]. This method ensures that only a single tag is communicating with the interrogator at one time [2].

Although this solution works, there are many disadvantages to its implementation. First and foremost is cost. To create a two way communication link between the interrogator and tags, complex and specialized hardware must be on board each tag to demodulate and interpret signal commands and transmit responses to these queries. Not only is this hardware expensive and power-hungry, but given a large number of tags within

a sensing environment the anti-collision algorithm can be slow for the interrogator [18]. Furthermore, since there is no encryption or interference once a data link has been established, the typical RFID system is prone to privacy loss.

CHAPTER 3:

SPREAD SPECTRUM

3.1 INTRODUCTION

As discussed in chapter 2, the problem of multi-tag data interference is one that plagues the use of complex RFID systems. Current solutions to this problem are expensive, slow, and completely susceptible to privacy infringement. With the mass deployment of large scale RFID systems mandated and implemented by large companies, the latter concern is quickly becoming a controversial issue of personal privacy [9]. If RFID systems are to be used in applications ranging everywhere from grocery stores checkouts, medical history tracking, and even banking transactions, the amount of important and secure information being wirelessly transmitted becomes staggeringly evident. With this in mind, large corporations such as Microsoft are conducting research in how to secure these wireless links to make them nearly impossible to eavesdrop [9].

One solution to this problem is to use a technology known a spread spectrum signal modulation. This technology was developed for the German military in WWII as a means to wirelessly communicate between base stations without any information leaks. Since then, the technology has been modified and adapted for commercial applications ranging anywhere from wireless LAN protocols to cellular telephone communications. In an article entitled "Spread Spectrum

Goes Commercial,"author Donald L. Schilling explains why this modulation scheme has such a vast potential in revolutionizing wireless communications:

> "Spread-spectrum radio communications, long a favorite technology of the military because it resists jamming and is hard for an enemy to intercept, is now on the verge of potentially explosive commercial development. The reason: spread-spectrum signals, which are distributed over a wide range of frequencies and then collected onto their original frequency at the receiver, are so inconspicuous as to be 'transparent.' Just as they are unlikely to be intercepted by a military opponent, so are they unlikely to interfere with other signals intended for business and consumer users -- even ones transmitted on the same frequencies. Such an advantage opens up crowded frequency spectra to vastly expanded use." [6, 10]

This report presents the novel application of spread spectrum signal modulation for use in RFID system communications. As will be demonstrated and described below, applying this modulation scheme to RFID not only eliminates the susceptibility of a multi-tag system from privacy infringement, but concurrently solves the problem of anti-collision as well.

3.2 HOW SPREAD SPECTRUM WORKS

3.2.1 ENCODING

Spread spectrum takes an outgoing data signal and encrypts it using a high frequency pseudo-random noise sequence also called a chipping sequence. The unique sequence is referred to as "pseudo random" because although it appears to be random noise, the generated bit pattern is predictable and repetitive. By combining this pseudo random noise sequence with a lower frequency data signal, the overall spectrum of the combined signal is spread across a large frequency range. Thus, the resulting signal appears to be nothing more than Gaussian white noise and is very difficult to detect, demodulate, and jam. The encoding procedure is described using equation six, and graphically represented in figure 8.

- *PN(n) = pseudo random noise sequence (high frequency)*
- *D(n) = low frequency data*
- *S(n) = output sequence*

$$S(n) = D(n) \times PN(n) \qquad (6)$$

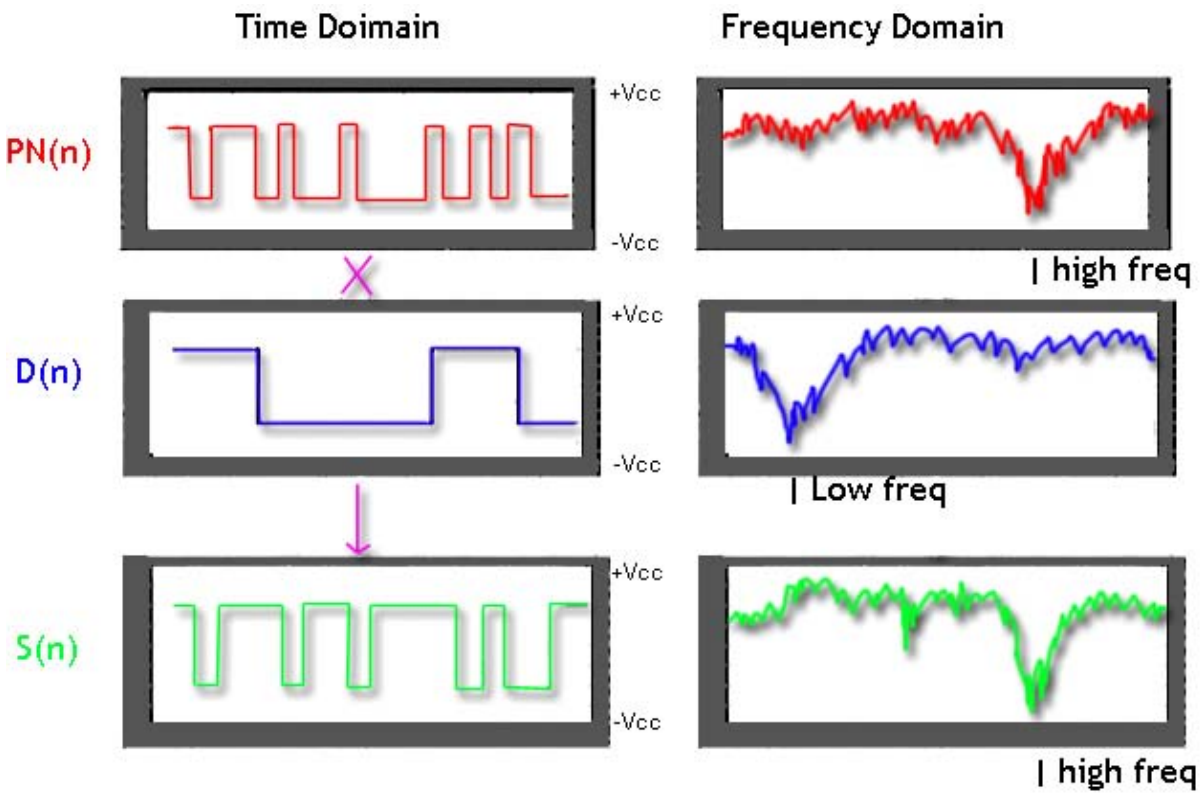


Figure 8. Graphical representation of the spread spectrum encoding algorithm. D(n) is the data desired to be transmitted. PN(n) is the high frequency pseudo random sequence unique to the tag which contains this data. S(n) is the result of the multiplication which is the overall signal that is transmitted. On the left column is the time domain signals and on the right is the frequency content of the corresponding signal.

3.2.2 DECODING

Using the encryption scheme described in the previous section, each tag responds to a query signal sent by the interrogator with a high frequency modulated data signal. Therefore, the overall received signal as seen from the interrogator is the linear superposition of multiple high frequency signals. The key to recovering a desired tag's data from this sea of high frequency backscatter is the predictability of the pseudo-random noise sequence unique to each tag. By knowing how to simulate these sequences in software, the data from each tag can be recovered using the following steps.

Using equation (5) assume that the signal S_{rec} represents the overall received signal of the interrogator. This signal is comprised of the linear superposition of each tag's output sequence S_t , where the subscript t represents the number of the tag. Also referring to equation (6), each of the tag's output sequences is represented by the product of its low frequency data D(n) with its unique high frequency modulation sequence PN(n). Combining and expanding equations (5) and (6) yields a complete expression representing the components of the received signal.

$$S_{rec} = \Sigma_t^N \left(PN_t(n) \times D_t(n) \right) \qquad (7)$$

At this point it is also important to notice the range of voltages that the received signal spans. Referring to the figure above, each tag's output ranges from a –Vcc value to +Vcc. Ensuring that the received signal contains a DC component equal to zero is essential for data recovery. Knowing this fact, in order to recover the data D(n) for a desired tag labeled td, one must first multiply S_{rec} by the simulated PN(n) unique to tag td. Assuming that the phase of PN(n) and the simulated PN (n) are aligned, this multiplication will cause the PN(n) term to converge to a constant DC offset value of +Vcc, and thus leaving behind only the D(n) term in the output expression for tag td. This operation is summarized in the following equations.

$$S_{temp}(n) = PN_{td}(n) \times S_{rec}(n) \tag{8}$$

$$S_{temp}(n) = PN_{td}(n) \times \Sigma_t^N \left(PN_t(n) \times D_t(n) \right) \tag{9}$$

$$S_{temp}(n) = \Sigma_t^N \left(PN_t(n) \times D_t(n) \right) + vcc + D_{td}(n) \tag{10}$$

Looking at equation (10), all of the summation factors that comprise $S_{temp}(n)$ are high frequency except for the DC offset +Vcc, and the desired tag's data $D_{td}(n)$. Applying a low pass filter to the resultant signal will remove all of the high frequency components, and therefore all of the other tag's modulated data signals. This operation only leaves behind the desired tag's data sequence $D_{td}(n)$ with a DC offset of +Vcc. Re-centering the data to have a DC mean of zero will remove the offset, and completely recover the desired data for a single tag. Figure 9 graphically represents the steps outline above for data recovery.

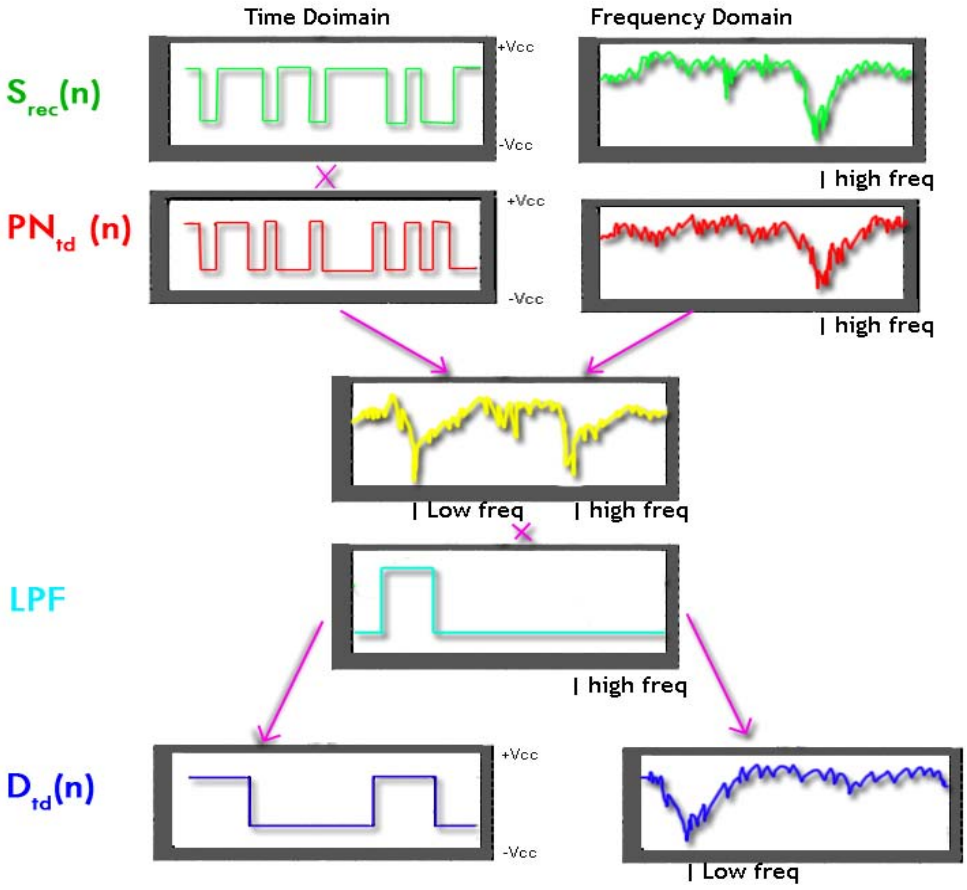


Figure 9. Graphical representation of the spread spectrum decoding algorithm. S_{rec} is the received backscatter seen from the interrogator, and the linear superposition of multiple tags' high frequency signals. PN_{td} is the pseudo random sequence unique to the desired tag. The product of these two results in a waveform who has both high and low frequency components. The high frequency components are removed through a low pass filtering operation, and only the desired tags data remains D_{td}.

3.3 SPREAD SPECTRUM WITH RFID

As demonstrated above, using spread spectrum signal modulation allows for a single tag's data to be recovered from a sea of backscatter. Not only does this method provide a solution for anti-collision, but without prior knowledge of how to generate the PN sequences in software no data can be recovered from the transfer [17]. Thus, the ability to decrypt a spread spectrum RFID tag is difficult. Using this method also eliminates the need for excessive hardware to

facilitate a two-way communication link between the RFID tags and the interrogator. Furthermore, receiving information from a single tag is fast because all of the tags are allowed to transmit at one time and there is no need to exhaustively search the environment for the correct tag. The ability to read from multiple tags simultaneously is another huge benefit to this system and can lend itself to a myriad of possible applications. If implemented correctly, an RFID system can be cheaper, faster, and more secure than the current ITF standard used in industry today.

CHAPTER 4:

SYSTEM DESIGN

4.1 HIGH LEVEL SYSTEM DESCRIPTION

A system designed to accommodate the spread spectrum anti-collision technique was constructed for use in experiments, measurements, and application testing. Specialized RFID tags were designed and fabricated with hardware capable of generating unique PN sequences to combine with their data. To query the tags, a carrier wave of frequency 915 MHz was sent from an RF signal generator and transmitted into the sensing environment. The illuminated tags then modulate the carrier wave with data, and reflect it back to the reader using the direct modulation scheme. The receiving antenna is attached to a custom IQ-demodulator and a baseband data acquisition board that performs analog-to-digital conversion of both in-phase and quadrature channels. The input waveform is then captured and processed using a combination of algorithms written in both Matlab and Labview software. Each component in this system will be discussed in detail in the following sections. Figure 10 shows the layout of the components described above.

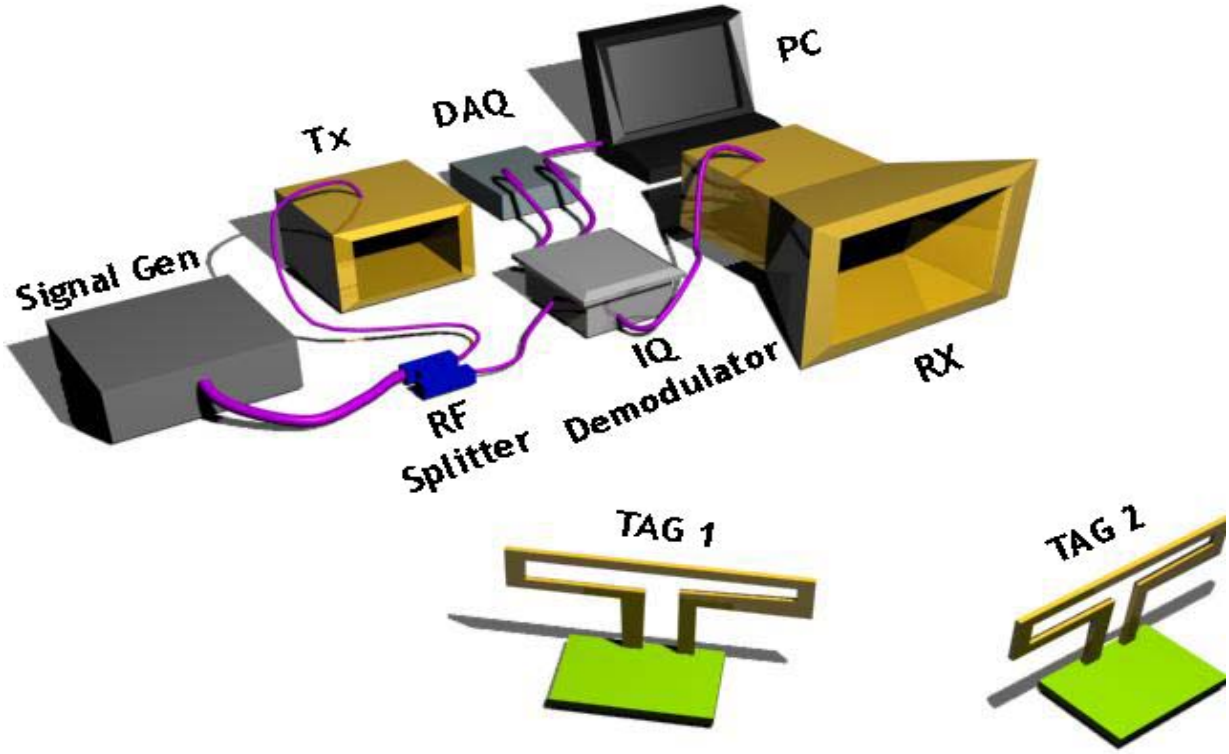


Figure 10. Diagram of the interrogator hardware layout. The signal generator is used to produce the pure RF frequency carrier wave which is propagated through the sensing environment using a rectangular waveguide (TX). The wave is modulated by the RFID tags and the backscatter is received through a directional horn antenna (RX). The backscatter is fed into an IQ demodulation circuit to remove the carrier wave modulation, and the recovered base band version of the bit stream is sampled with a data acquisition board. The final captured signal is piped into a PC for further processing.

4.2 SYSTEM HARDWARE

4.2.1 TAG LAYOUT

For the proposed system to function, each tag was designed and equipped with specialized hardware necessary to generate up to 255 unique PN sequences. The ID of each tag is reset-able on the fly and therefore can be changed without any connection to a computer or use of software. These PN sequences are combined with the tag's data, and the resulting bit pattern is used to bias a

PIN diode network attached to a transmission line. At the end of the transmission line is a folded dipole antenna whose dimensions are designed to accommodate reception and transmission at 915 MHz. Figure 11 shows a high level block diagram of the tag layout. Figure 12 is a photograph of the constructed tags.

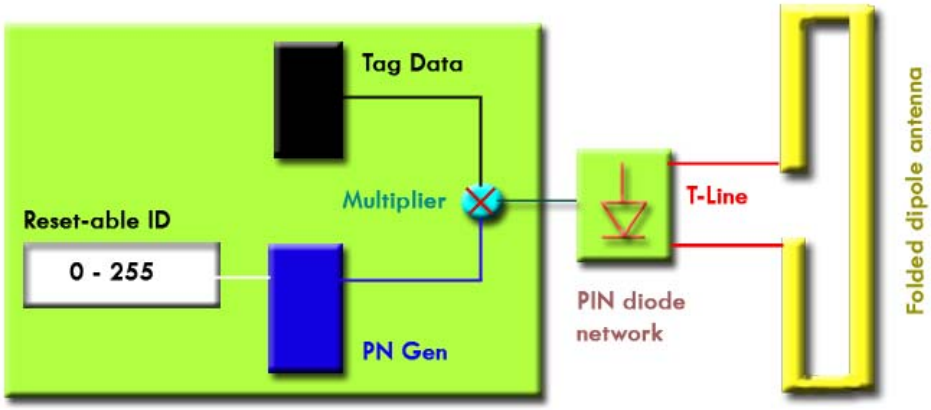


Figure 11. High level tag block diagram of the custom designed RFID tags. The ID of the tag is set and used to generate a unique pseudo random sequence that is then multiplied together with the data. The resulting waveform is then used to bias a pin diode network that terminates a transmission line and folded dipole antenna.

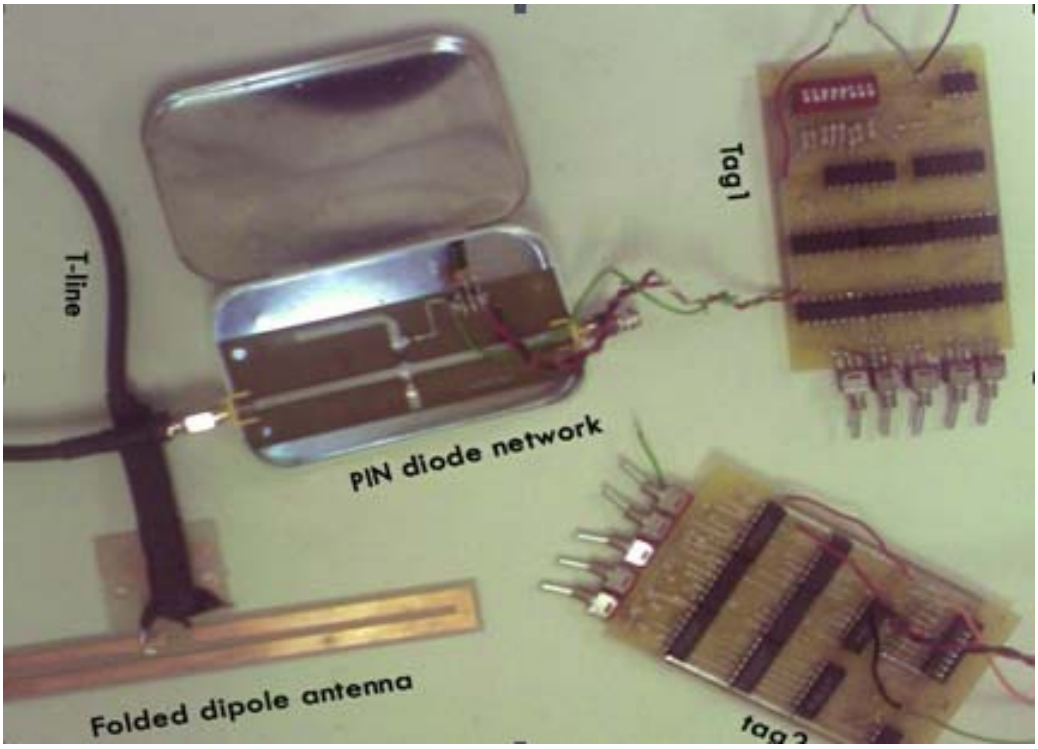


Figure 12. Physical Tag layout picture with every labeled component.

Using the principles of transmission lines discussed in section 1.2.2.1, the tag modulates the incoming waveform and reflects it back to the reader. By setting each tag to a separate ID number, the system can handle up to 255 different tags within the sensing environment. The key to this design is the ability to generate 255 unique PN sequences using minimal hardware on each tag. The following section will describe the theory and hardware behind the generation of these unique sequences.

4.2.2 PN GENERATORS

A PN generator is a system designed to create a bit sequence that appears to be random, but given prior information is completely predictable. These sequences are typically periodic as well. The most common way to generate a

pseudo random sequence in hardware is to use a shift register feedback network that is tuned to provide a random sequence with a desired period. A typical PN generator system is shown in figure 13.

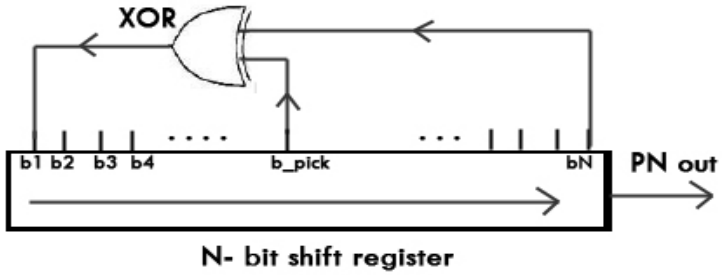


Figure 13. Typical PN sequence generator

The system in Figure 13 outputs a type of pseudo-noise called an m-sequence [13]. The shift register is typically initialized so that all the registers contain a value of one. Then, with each consecutive clock pulse the value from the previous register moves to the next register, i.e. b1-> b2->b3…bN. The value bN is the output bit for that clock cycle. The first bit b1 is fed a new value produced by the feedback network. This value is generated by taking the output bit bN, and XORing it with another register value in the sequence represented by b_pick. By varying the location of b_pick, completely different sequences can be generated. However, not every sequence has the same period. Only certain pick registers will generate a sequence of maximal length for a given shift register. The equation to determine the maximum possible period of a sequence for a given shift register is:

$$Max\ Length = 2^N - 1 \qquad (11)$$

Since our system was designed to accommodate 255 different tags, we needed a maximal length sequence of 255, the reason for which will be explained later. Therefore by using eight bit shift registers we were able to generate these sequences. Referring to figure 13, the pickoff points that generated maximal length sequences are b3 and b5. Figure 14 shows the pseudo-random noise sequence produced using pickoff point b3. Figure 15 shows the pseudo-random noise sequence produced using pickoff point b5.

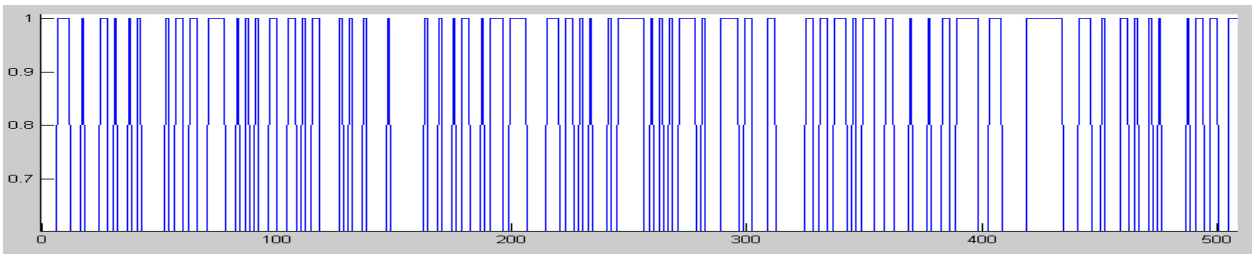


Figure 14. Maximal length sequence generated with an eight bit shift register feedback network with pickoff b3

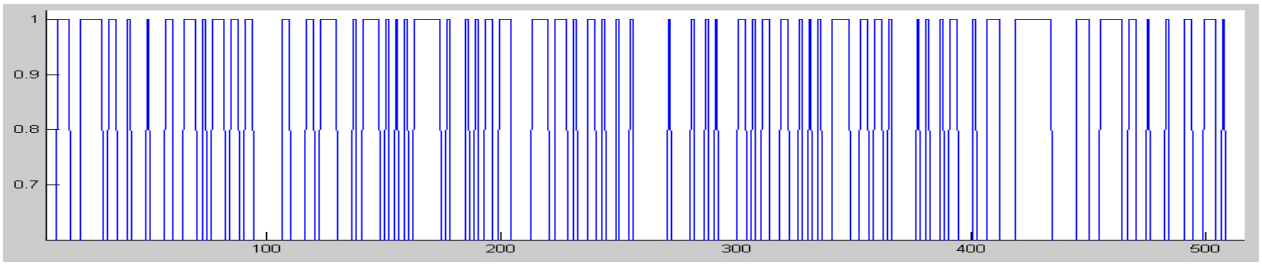


Figure 15. Maximal length sequence generated with an eight bit shift register feedback network with with pickoff b5

However, simply having a single PN sequence of code length of 255 bits is not enough to create a set of uniquely despreadable codes because all of the tags are designed and fabricated exactly the same. In order to accommodate 255 separate tags, each tag must be able to generate 255 unique and equal length

sequences. To accomplish this task, another method of sequence modulation was devised that uses a combination of two PN generators on each tag.

4.2.3 DIFFERENTIAL OFFSET MODULATION

In order for each tag to create 255 unique and equal length sequences without changing the hardware design for each tag, a scheme known as differential offset modulation was devised. Each tag is equipped with two PN generators designed to output a pseudo random sequence of length 255. The output of both generators is then combined together to produce a new PN sequence also of length 255. The output of two PN sequences XORed together is commonly referred to as a gold code [17]. The ID of the tag is encoded within the phase shift between the two sequences before they are combined. Thus, with a code length of 255 bits there are 255 possible phase shifts, and therefore 255 possible output sequences. A high level block diagram for this system is included as figure 16, as well as a schematic for this overall circuit.

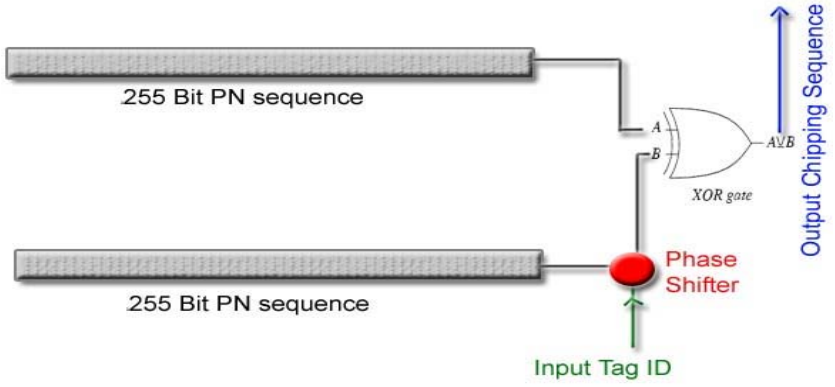


Figure 16. Differential offset modulation block diagram. Two PN sequences of length 255 are XORed together to create the output chipping sequence. The ID of the tag is encoded through control of the relative phase shift between these sequences before they are combined.

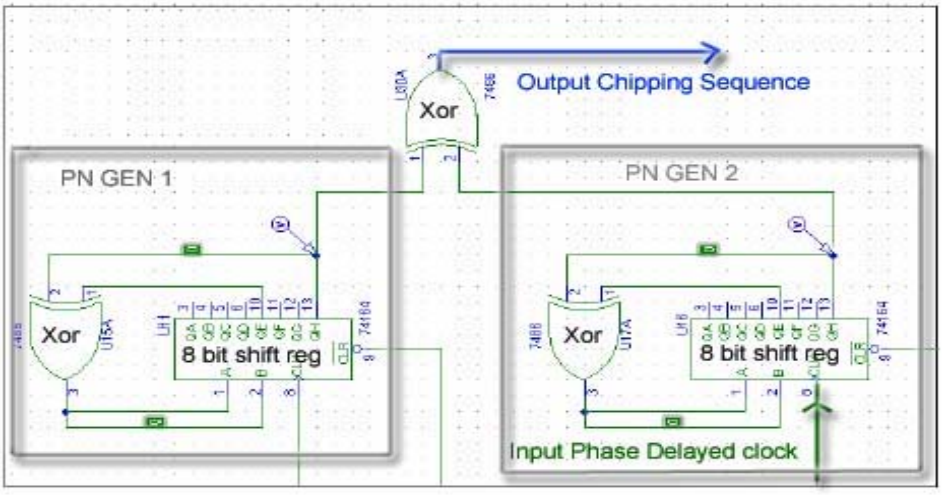


Figure 17. Preliminary differential offset circuit diagram showing the hardware configuration for the two PN sequence generators. These sequences are XORed together to create a tag's chipping sequence. The phase shift is induced by delaying the second PN generator's clock input.

4.2.3.1 PHASE SHIFT CIRCUIT

In order to create a user controlled phase shift on the tag, a special circuit was designed to control the shift registers for both PN generators. What this control circuit essentially does is delay the clock line input to the second PN generator by a set amount, and therefore causes the sequence to start at a different point in respect to the first PN generator. Dual four bit-binary counters were employed as a mechanism for timing the amount of bits needed to delay the second PN generator. An initial value was loaded into these counters using a set of dip switches, and can be changed on the fly to represent any number ranging from 0-255. When the tag is activated, the counters increment their value with every clock pulse until they reach the value 255. At this point, the clock line that feeds the second PN generator is allowed to begin pulsing, and thereby allowing the second PN generator to output its sequence. Figure 18 demonstrates the relative delay in clock signal

when the input tag ID is set to a large number. Figure 19 shows the corresponding delay in PN sequence generation when the input tag ID is set to a large number. Similarly, figures 20 and 21 show the same results when the tag ID is set to a small number.

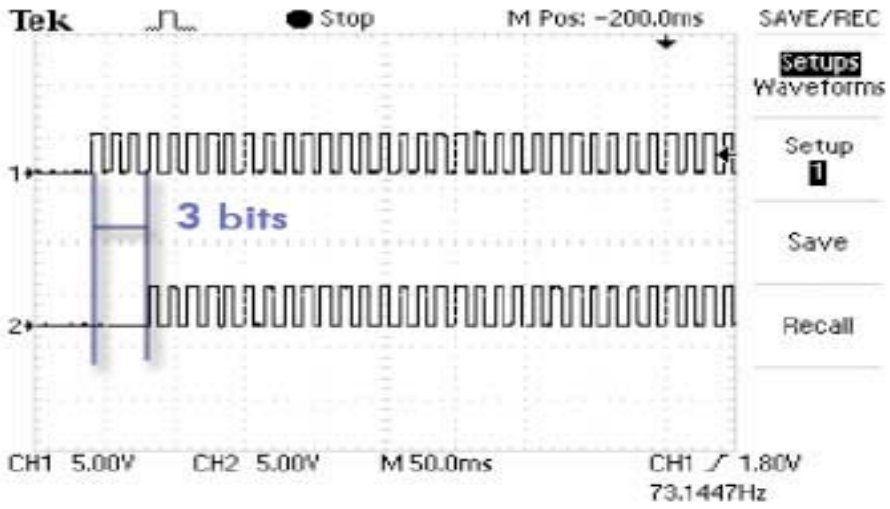


Figure 18. Clock signal delay when input tag ID is set to a large number.

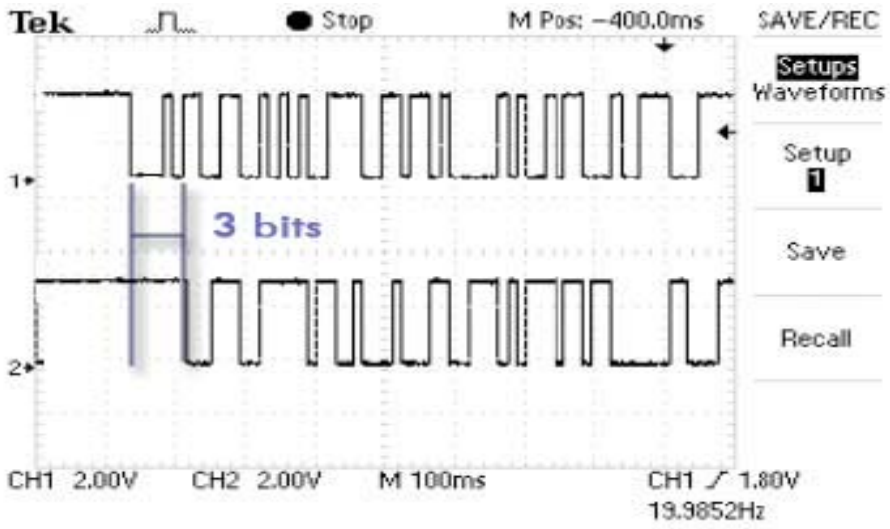


Figure 19. PN sequence offset when input clock signal is delayed by three bits

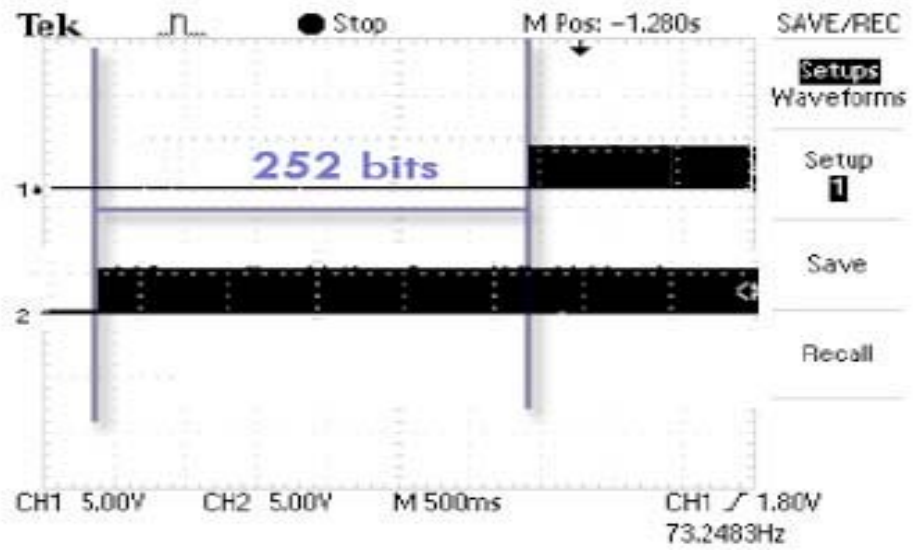


Figure 20.Clock signal delay when input tag ID is set to a small number.

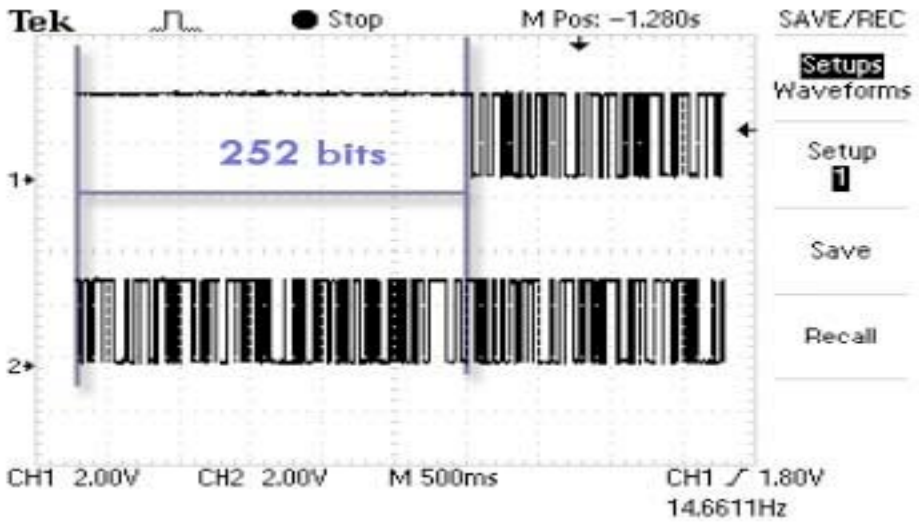


Figure 21. PN sequence offset when input clock signal is delayed by 252 bits.

Using the above method, the numeric identity of the tag is thus encoded through the initial value loaded into the counters and is related by the following equation:

$$TagID = 255 - Initial\ counter\ value \quad (12)$$

Because we used the counter as a timing device on the RFID tag, it was necessary to select chips that were synchronous to the on-board clock. However, this became a problem because synchronous binary counters roll over after they reach their final value. These chips have both an output that indicates when this condition is met and an input to tell the counter to hold, however, because these ports only refresh on a clock edge there is a one bit delay between the output of the condition flag and the input hold trigger. Without any extra circuitry the counters would continue to count indefinitely, and therefore could not trigger the phase delay circuit correctly.

In order to keep the counter from resetting itself every time it rolled over and consequently restarting the delay sequence, the outputs of the counter were fed through a series of AND gates set to trigger once the number 254 had been reached. On the following clock tick the output of the AND gates will be high. This value was inverted and fed directly into the count enable input of the counter forcing it to hold at value 255, and thus eliminating the one bit delay. To trigger the clock for the second PN generator, the output of the AND gates was then ANDed together with the original clock signal being fed into the first PN generator. This ensured that the clock signal would remain zero until the counter had reached its end value of 255. Once this number has been attained, output of the AND gates is one, and the original clock signal is allowed to pass

into the second shift register. A schematic of the complete phase delay circuit is included in figure 22.

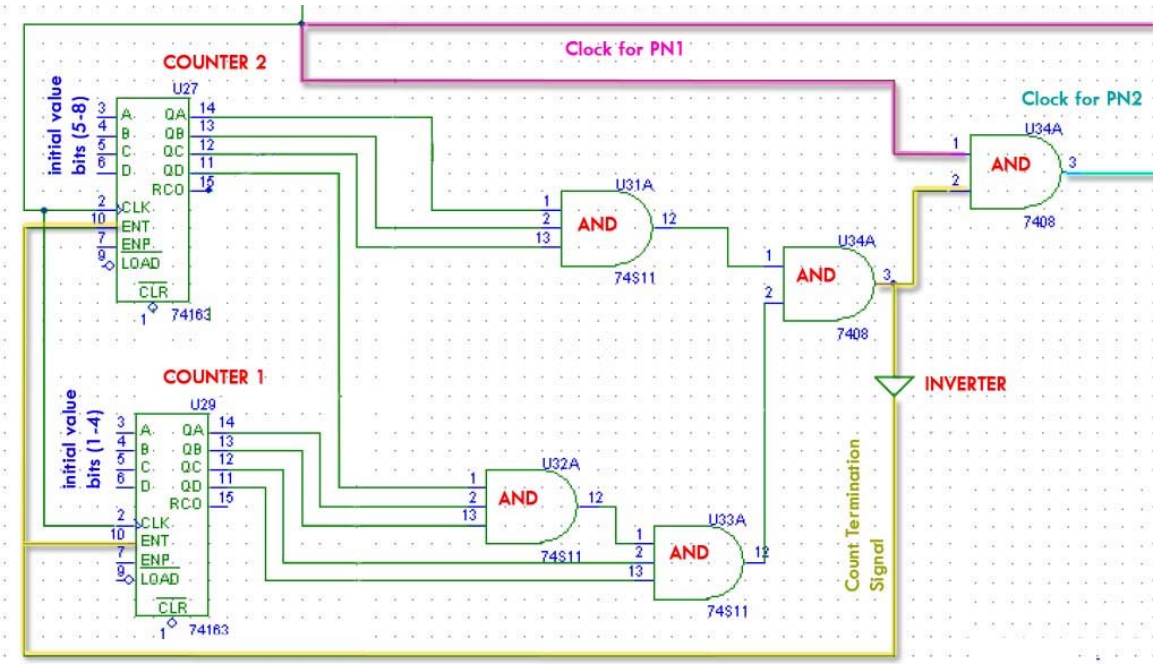


Figure 22. Complete phase delay circuit. Using the initial value loaded into the duel four bit binary counters, the circuit effectively counts the number of bits to delay the clock line input to the second PN generator.

4.2.3.2 SEQUENCE EXCLUSION

As stated above there are two pick-off points in an eight bit shift register that generate maximum length PN sequences. During the design process, a decision needed to be made to choose which of these pick off points to use for modeling and fabrication of the two on board PN generators. Since ultimately the goal is to use these sequences to help with anti-collision, the combination of generators that produces sequences with the lowest cross correlation would be the ideal choice. Cross correlation is the measure of how similar two sequences are in relation to each other and is defined by the equations below. [11]

- x_n, y_n= *jointly stationary random processes*

- *E(*)= expected value function*

$$R_{xy}(m) = E\left(x_{n+m} \times y_n^*\right) \qquad (13)$$

To calculate an approximation of this value for a set of finite sequences, the following equation was used. [11]

$$R_{xy}(m) = \begin{cases} \sum_{n=o}^{N-m-1} x_{n+m} \times y_n^* & m \geq 0 \\ R_{xy}^*(-m) & m<0 \end{cases} \qquad (14)$$

The lower the cross correlation between two RFID tag sequences, the easier it is to separate one from another.

To find the combination of PN generators that produced sequences with the lowest cross correlation, a function was written in MatLab to simulate all 255 possible output sequences for a given combination of generators. Each sequence was then cross correlated with every other sequence, and the maximum value of R_{xy} was stored in a two dimensional array. The results of this operation are shown in Figure 23 for each combination of generators, where 1.0 denotes maximum correlation (identical signals) and 0.0 denotes complete decorrelation between two signals.

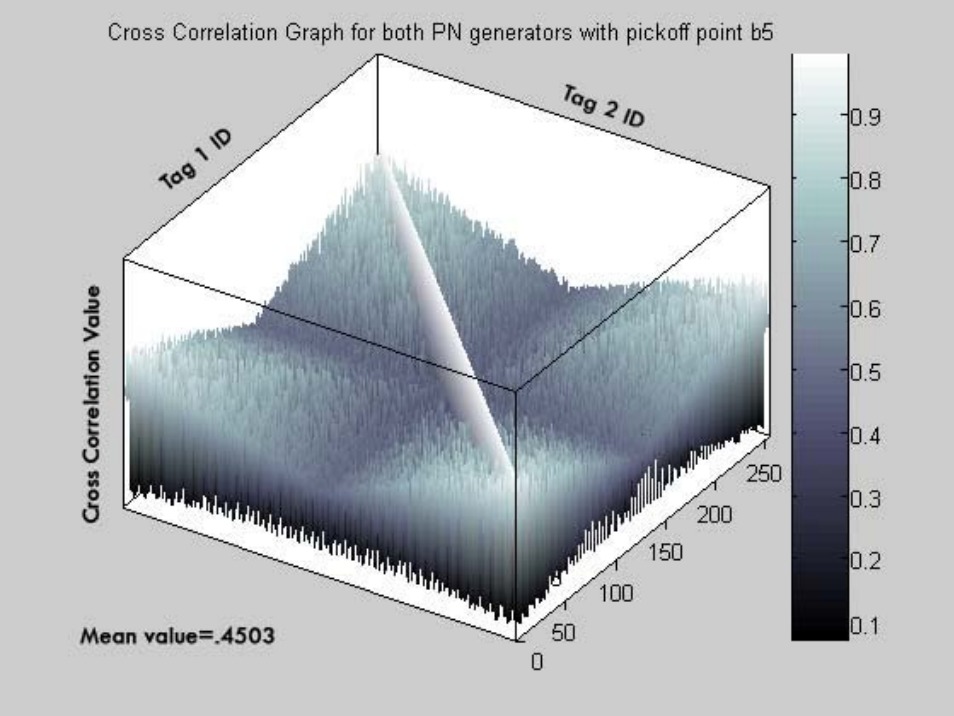


Figure 23. Graph showing the maximum cross correlation value between sequences of varying tag IDs created from two PN generators with pickoffs b5.

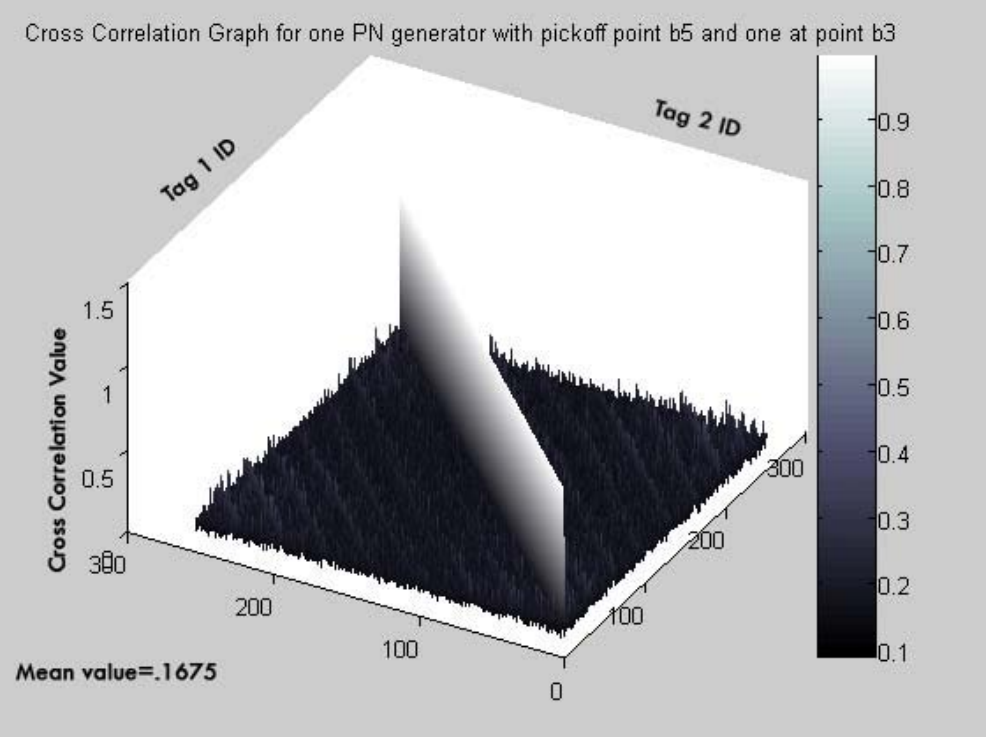


Figure 24. Graph showing the maximum cross correlation value between sequences of varying tag IDs created from one PN generator with pickoff b5 and the other with pickoff b3

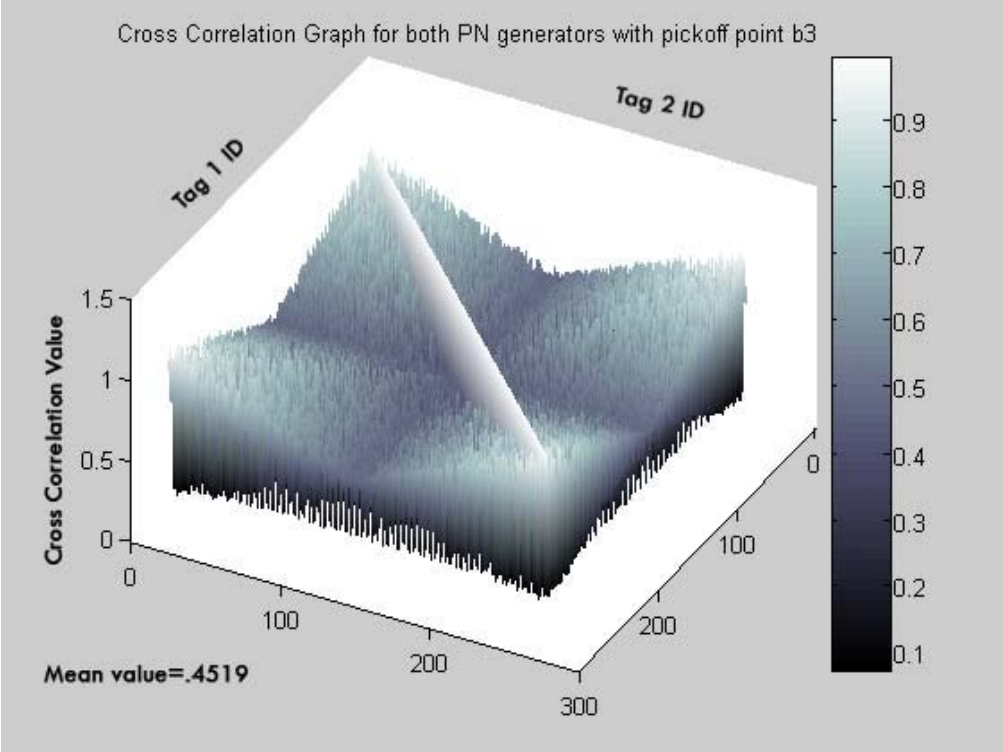


Figure 25. Graph showing the maximum cross correlation value between sequences of varying tag IDs created from two PN generators with pickoffs b3.

It is intuitive to determine from the previous figures that the arrangement that produces the lowest mean cross correlation sequences is the combination of both types of PN generators. Therefore on each tag there are both types of PN generators used for the differential offset spread spectrum RFID scheme.

4.2.4 COMPLETE TAG DESIGN

Figure 26 is a complete and labeled photo of the final RFID tag design .

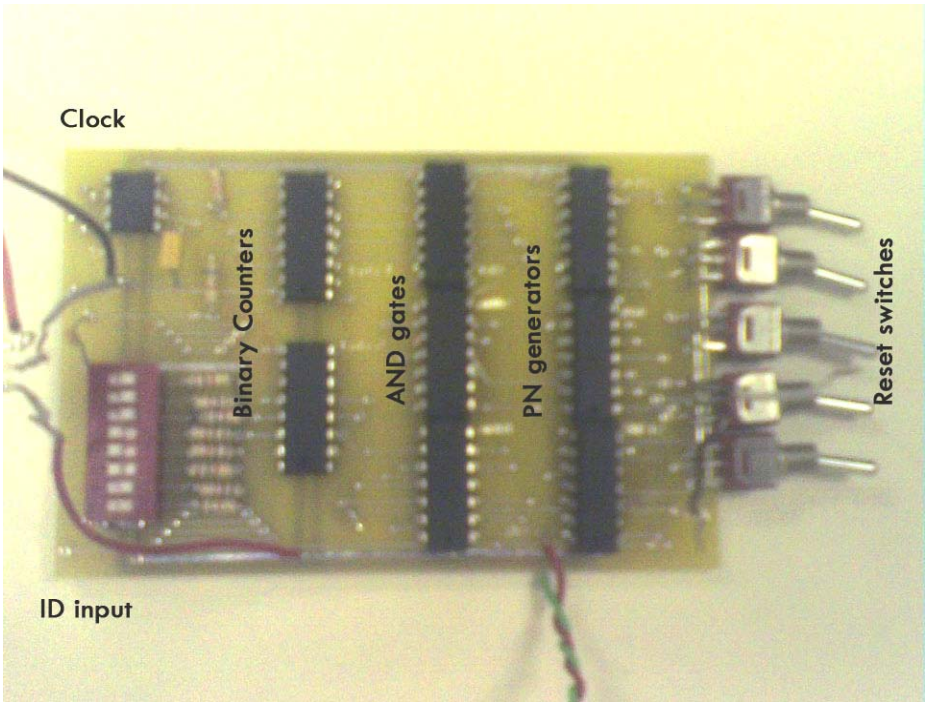


Figure 26. Complete RFID tag photo with labeled components. The ID is set using the dip switches on the left. To reset the tag with a new ID, the set of switches on the right must be flipped sequentially from top to bottom and then back.

The set of dip switches on the left hand side of the board are used to load a new value into the counters and effectively change the ID of the tag. The counters themselves are four bit binary counters with part number 74163. For the onboard synchronization of the chips, a standard TTL 555D timer was biased to produce a clock signal at 1 KHz. The shift registers are eight bit synchronous parallel load chips with part number 74164. Aside from these components, the board also contains two quad AND gate chips, one inverter chip, and one XOR gate chip. On the right hand side of the board are a set of five toggle switches used to systematically change the inputs of the chips to allow them to be reset with a new tag ID. To change the ID of the tag, these switches must be flipped upward sequentially starting from the bottom switch

to the top. Next, the value in the dip switches can be changed to any desired ID from 0-255. Finally, all of the switches must be flipped downward sequentially from top to bottom to allow the tag to start generating its new chipping sequence.

The RFID tag board was powered using an external 9 volt battery source. This battery is connected to a voltage regulator used to step its voltage down to the standard TTL operating voltage 5 volts. The entire tag draws a current of 0.02 amps, making its total power consumption 0.1 Watts.

4.2.5 INTEROGATOR HARDWARE

Aside from the tags, to complete the spread spectrum RFID system specialized hardware needed to be designed, fabricated and assembled to create the interrogator. In the following sections we will briefly explore these hardware components.

4.2.5.1 TRANSMISSION HARDWARE

To generate the pure RF wave used to query the sensing environment, a Rhode & Schwarz SM1.0 continuous wave signal generator set to output an RF signal at frequency 915 MHz with amplitude of 10 dBm was used. The generated signal is split using an RF signal splitter with a frequency range from 1-2GHz, and fed into a custom fabricated rectangular waveguide used for wave transmission. The signal is also fed into a custom designed and created IQ demodulator that

will be described in the next section. The transmission hardware setup is pictured below in figure 27.

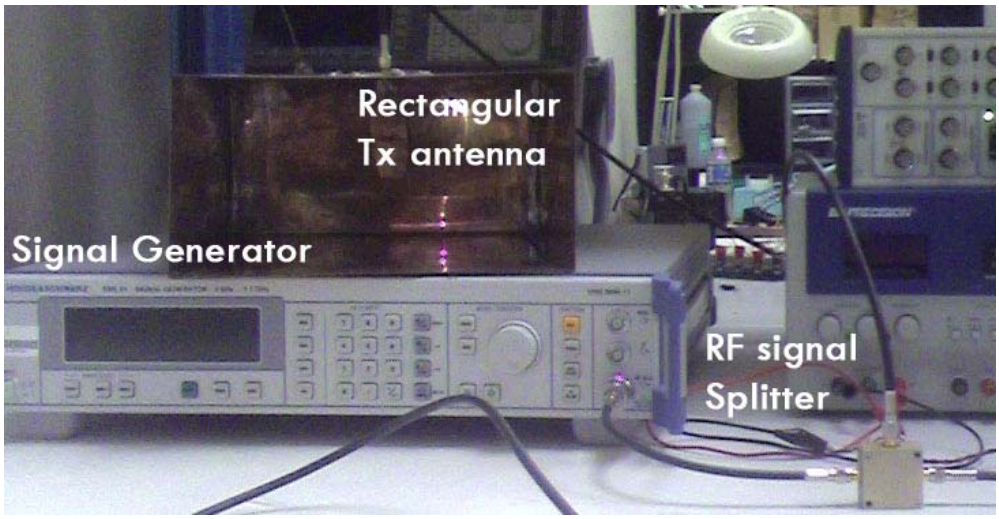


Figure 27. Transmission hardware photograph. The signal generator is used to generate the pure RF carrier wave that is transmitted through the TX antenna.

4.2.5.1 RECEIVING HARDWARE

The pure RF wave is then propagated into the environment and modulated by the tags' hardware. The backscatter is received by the interrogator using a directional horn antenna that was designed and built by Yenpao "Albert" Lu. When fed with a standard 50 Ω coaxial line, the antenna has a peak gain of 10.1 dBi, and a beam width of 40^{o} [4]. A photograph of this horn antenna is shown in Figure 28.

Figure 28. Directional horn antenna photograph.

The output of the receiving antenna is connected to the input of the custom IQ-demodulator also designed by Yenpao Lu. As mentioned above, this component receives input from the signal generator as well. What the IQ demodulation circuit essentially does is remove the carrier wave modulation from the received backscattered waveform. What remains is a baseband representation of the bit pattern received through the backscatter. The IQ demodulator also removes the DC component of the backscattered waveform to center the signal on zero volts. As mentioned earlier, this is essential for the spread spectrum algorithm to work. A photograph of the IQ- demodulator is included in figure 29.

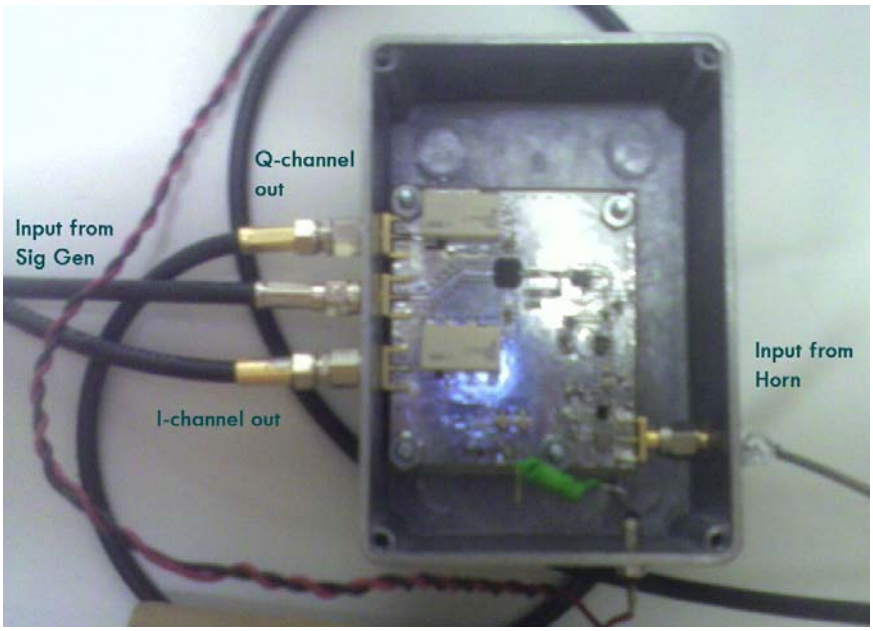


Figure 29. IQ demodulation circuit. This circuit recieves input from the signal generator as well as the recieveing (RX) antenna of the interrogator. The output of this circuit is the baseband representation of the received bit pattern split into its in-phase and quadrature componants.

The output from the IQ demodulator is split into its in-phase and quadrature channels, and is fed directly into a baseband data acquisition board. A National Instruments data acquisition board is used to sample the data and transfer it into the computer for software processing. Figure 30 shows the receiving hardware setup.

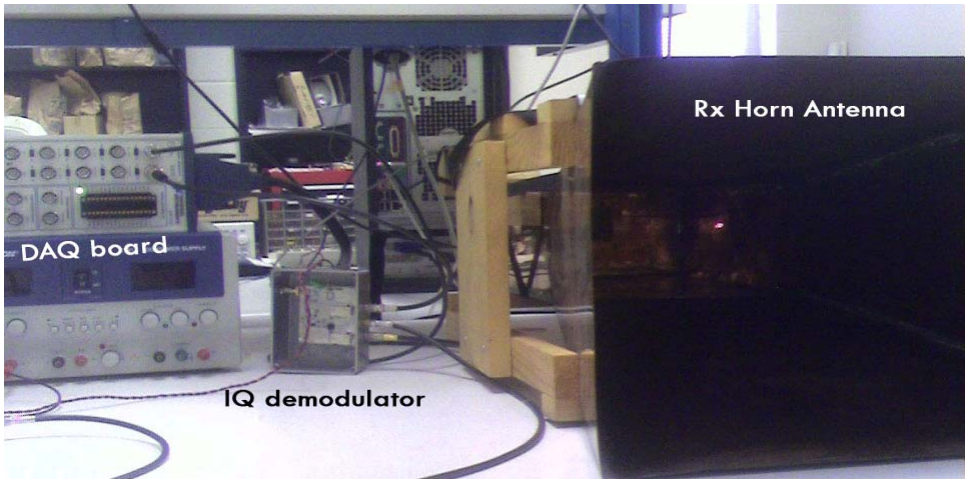


Figure 30. Receiving hardware photograph. The backscattered waveform is received through the (RX) horn antenna and sent into the IQ demodulation circuit where the carrier wave modulation is removed. The output of the demodulation circuit is the base band representation of the in-phase and quadrature channels of the bit pattern received through the backscatter. These outputs are fed into the DAQ board and sampled by the computer.

4.3 SYSTEM SOFTWARE

Once the signal has been received and sampled by the hardware, the majority of the signal isolation algorithm is carried out in software. To do so, several programs and functions were written using a combination of MatLab and LabView software packages. In the following section, the theories, functionality, and interfaces for these programs will be described.

4.3.1 WAVEFORM CAPTURE

The first stage in software processing begins with the waveform capture. The in phase and quaderature channels of the waveform are fed into two separate inputs to the data acquisition board. From this point, each channel is processed separately using the same Labview program. For the majority of the experiments, a sampling rate was chosen to be twice the Nyquist rate. Since

the tags' internal clock outputs bits at a frequency of 1 kHz, the data acquisition board was programmed to sample the input at a rate of 4 kHz. Trials of running the program with a higher sampling rate were performed, but ultimately increasing the sampling rate did not affect the quality of the program's performance. A sampling rate of 4 kHz proved to be an optimal balance between speed, storage, and quality.

After the waveform is captured and sampled, it is then cropped into a section that contains one period or 255 bits of the backscattered sequence. The equation that relates the number of samples required for capturing a desired number of bits at a given sampling rate and bit frequency is included below.

$$Sample\ number = Desired\ bit\ number \times \frac{Sample\ frequency}{Bit\ Frequency} \tag{15}$$

Concurrently as the above cropping operation is performed, the driver program also loads into memory the computer simulated sequence for the desired tag. This sequence is generated using a program written in Matlab that will be discussed at a later section. After the cropping operation is performed, the simulated sequence and captured sequence are the same length and each contains 255 bits of data. Using this fact, each sample in the simulated sequence is assigned the same time step as the corresponding sample in the

captured sequence. Doing this ensures the correct preservation of the time domain during the data processing stage.

4.3.2 WAVEFORM PROCESSING

Now that the captured sequence and the simulated sequence are synchronized in time, both sequences are passed into the data processing stage where the spread-spectrum demodulation is performed. Following this algorithm, both sequences are multiplied together and the result is sent through a 6^{th} order Butterworth low pass filter with a cutoff at 60 Hz (the low frequency data rate). The magnitude response for this filter is shown in figure 31.

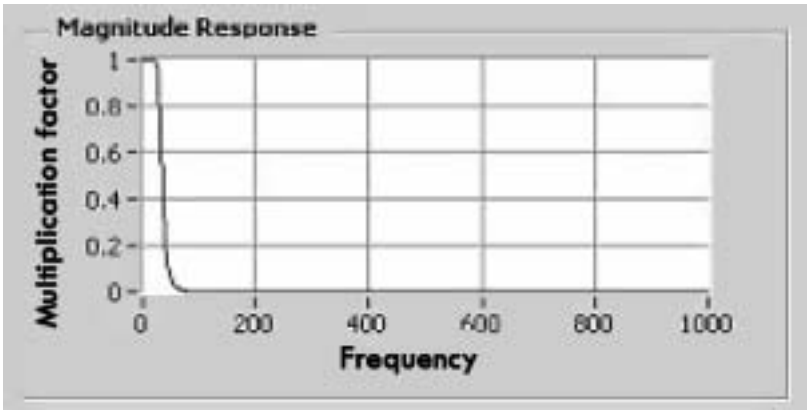


Figure 31. Low pass filter magnitude response. 6^{th} order butterworth filter with cutoff frequency of 60Hz

As stated above, if the simulated sequence is aligned with the transmitted PN sequence of the desired tag, the multiplication will result in the production of a low frequency component as well as a DC offset. This condition will be referred to as convergence. However, using the program described above there is no assurance that the simulated sequence and the transmitted sequence are

aligned. It is for this reason that the data processing stage is nested inside a loop whose iteration count ranges from zero to the sample number calculated using equation 15. With each successive iteration, the simulated sequence is circularly rotated one sample to the right before the multiplication is performed. Rotating the input sequence with each iteration ensures that at some point in the loop, the PN sequences will be aligned. At this point, the resulting product of the multiplication will produce a DC component whose magnitude is greater than zero. The iteration that produces a DC component with the largest value is the iteration where the two PN sequences are in phase, and therefore the low passed data recovered during this iteration is stored as the correct data received from the desired tag.

4.3.3 DRIVER PROGRAM OVERVIEW

Included in Figure 32 is a high-level block-diagram showing the overall flow of the software algorithm described in the previous section. In actuality, the driver function created in LabView contains many more components that are not represented in figure 32, but are not essential to understand how it works. For a complete overview including every software component in the main driver program refer to the appendix. Several variations of this program were written to perform different tasks and take different measurements. These programs are also included in the appendix.

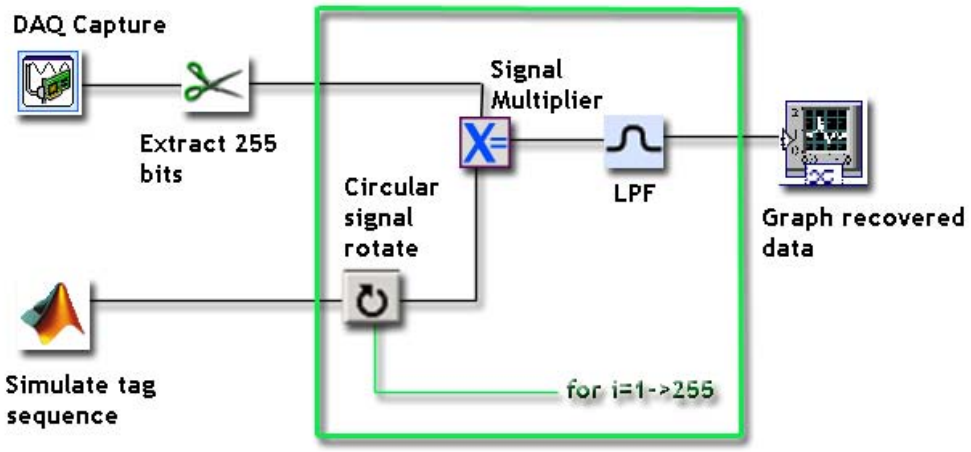


Figure 32. LabView software flow diagram. The data is first captured, sampled, and then cropped to include one period of 255 bits. Concurrently Matlab is used to simulate the desired tags chipping sequence. These outputs are fed into an iterative loop, where they are multiplied together. With each iteration, the simulated sequence is circularly rotates one bit to the right to ensure that at some point the sequence will converge. At this point, the product is low pass filtered and the data is recovered.

4.3.4 MATLAB FUNCTIONS

As mentioned above, the driver function created in LabView receives input generated by programs written in Matlab. Overall, nearly 10 different programs were written in Matlab to facilitate this algorithm and help with debugging. However, only the functions directly involved with the algorithm will be described in the following sections. For a complete list and source code for the remaining functions, refer to the appendix of this document.

4.3.4.1 SEQUENCE SIMULATION

In order to predict the output PN sequence for a desired tag, programs in Matlab were developed to simulate the hardware onboard each tag. The function PNgen accepts an initial condition array and an array index. The initial condition array contains the values present in each register of a given shift register before the sequence generation begins. Typically for our purposes all

of the registers are initialized to hold a value of one. The array index corresponds to the pick register number used for the hardware PN generator. For the PN generators designed for this system, this value is typically either a three or a five. The function iterates through the number of steps equivalent to the sequence period length, and produces an output array unique to the hardware PN generator configuration.

The function SimSeq is used to simulate the differential offset hardware for a given tag ID. The function is passed two PN sequences unique to the onboard PN generators that are simulated using the PNgen function. The third input corresponds to the ID of the desired tag. To produce the final output PN sequence unique to a given tag, the Simseq algorithm circularly rotates the second input PN sequence by the initial counter value. This value is calculated using the following equation that is a derivation of the hardware equation provided above.

$$Shift\ Amount = 255 - Tag\ ID \qquad (16)$$

Once the second PN sequence is rotated by the appropriate number of bits, it is then XORed with the first PN sequence to produce the final output sequence for a given tag ID. Figure 33 shows a flow diagram for the software sequence generation.

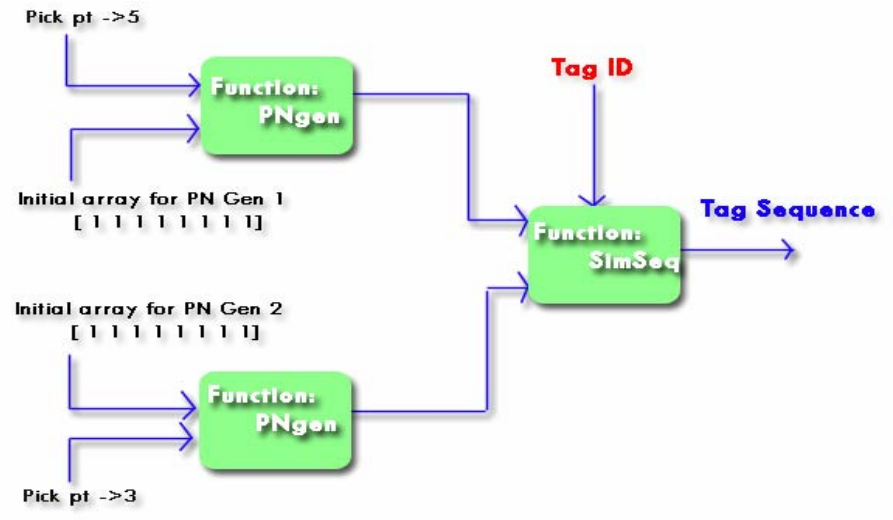


Figure 33. Software sequence generation flow diagram. The function PNgen is used to generate the two PN sequences on board each tag. These sequences are fed into the function SimSeq to simulate the chipping sequence on the desired tag.

4.3.4.2 ID DECODE

An important functionality of the anti-collision RFID system is for the computer to be able to recognize what tag it is communicating with. Given a single tag within the sensing environment the computer should be able to capture the backscatter and immediately identify the ID of the tag based upon its simulated PN sequence. This functionality is a good way to calibrate the software to simulate the correct output sequence per tag, and also check if the software simulation corresponds correctly to the tag hardware.

A function named IDdecode was written in Matlab to perform this operation. A single tag is placed in the sensing environment and the data multiplication stage is bypassed. This bypass causes the backscatter created by the tag to only represent the unique PN sequence generated onboard. This waveform is sampled, captured, and cropped through the LabView driver program, and

exported to Matlab. The IDdecode function imports this data and processes it to recover the ID of the tag. The function iterates a loop from zero to 255, and uses the sequence simulation functions described above to generate the PN sequence for a tag whose ID is equal to the iteration number. The simulated sequence is then cross correlated with the backscatter data, and the maximum cross correlation value is stored along with its sample index location. The iteration number that produces the greatest cross correlation value is the tag's ID. To provide a visual comparison between the backscatter and the simulated sequence, the maximum cross correlation sample index is used to shift the simulated sequence in phase with the backscatter. These two sequences are then plotted next to each other. Presented below in figure 34 is successful tag identification. Although there exist some bit errors evident through visual inspection of these two plots, because the tag hardware produces PN sequences with a low mean cross correlation value, the program is still able to select the correct tag ID.

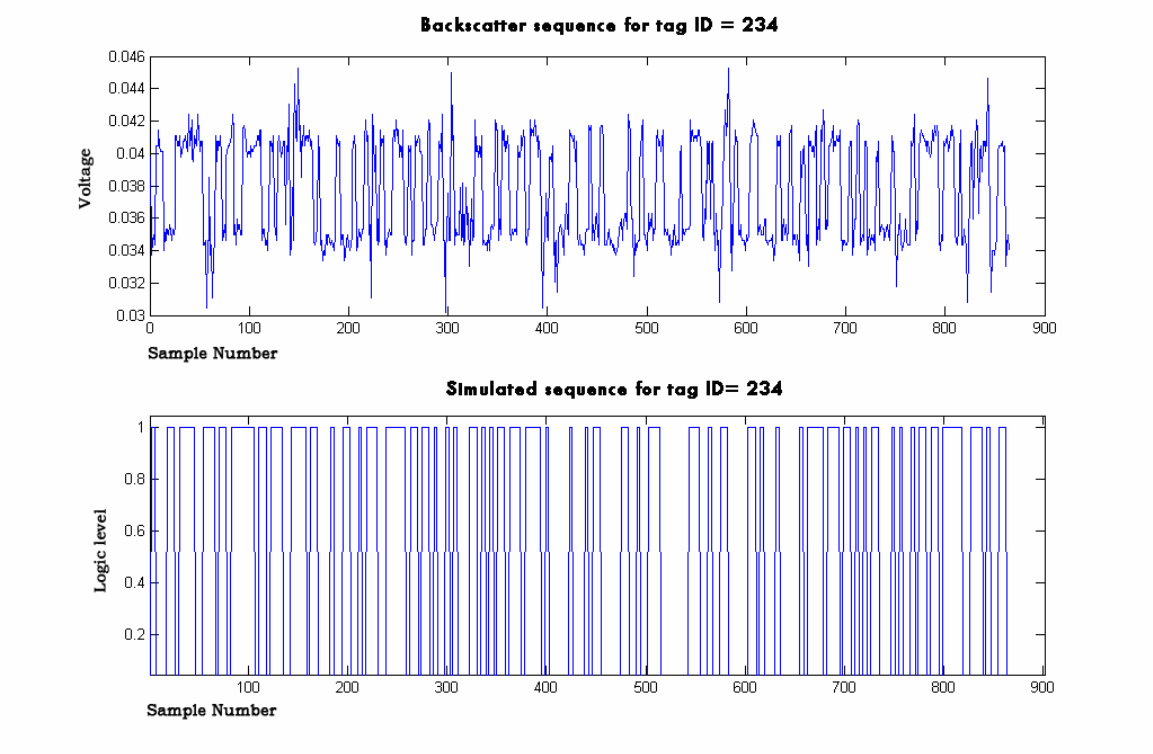


Figure 34. Successful tag identification. The top graph is the received backscattered waveform from a single tag. The second graph is the simulated chipping sequence of the same ID.

4.3.5 DATA DEMODULATION RESULTS

By combining all of these software elements between LabView and Matlab, the following results were obtained that demonstrate a successful data demodulation. For this experiment, two tags were placed inside the sensing environment with one tag set to transmit data in the form of a low frequency square wave (approx. 10 Hz). Using the Labview driver function, the backscatter was captured and processed. Matlab was used to pre-simulate the unique PN sequence for this tag. The input data and results of this experiment are shown in Figures 35 and 36.

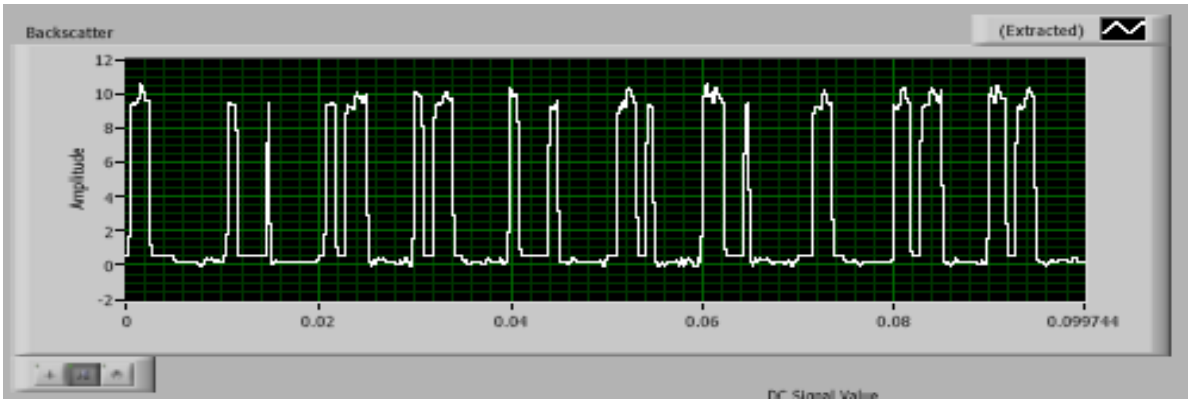


Figure 35. Input received backscattered waveform .

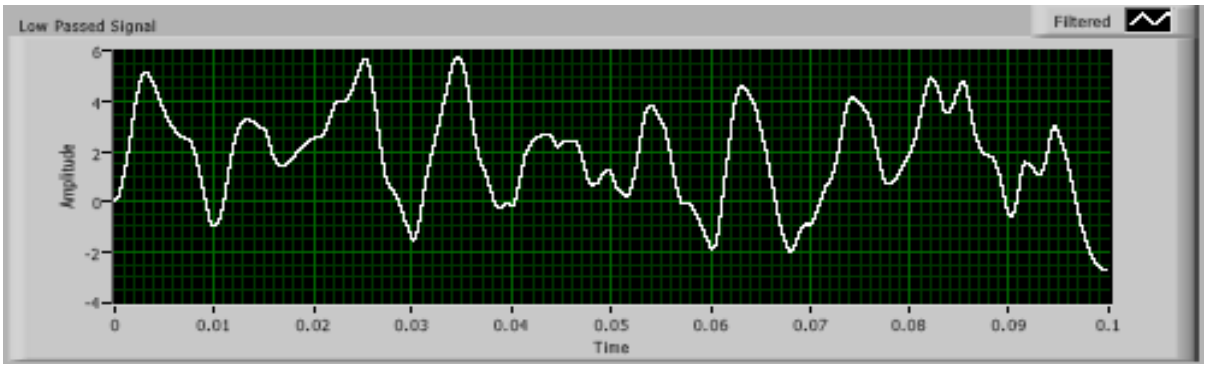


Figure 36. Results of the multiplication and low pass filtering operation.

After the low-pass stage, a new step was added in order to recover the sharp boundaries of the bits in the data stream. These sharp edges are lost due to the low pass filtering operation. To recover these edges, a threshold operation was run using a threshold equal to the RMS value of the low passed data. Any sample value less than this threshold was set to represent a logical zero and any sample value greater than the threshold was set to represent a logical bit one. The result of running the threshold operation on the LPF data is shown in figure 37. An oscilloscope capture of the data from the tag is also included as figure 38 to show how close the recovered data is to the original tag data.

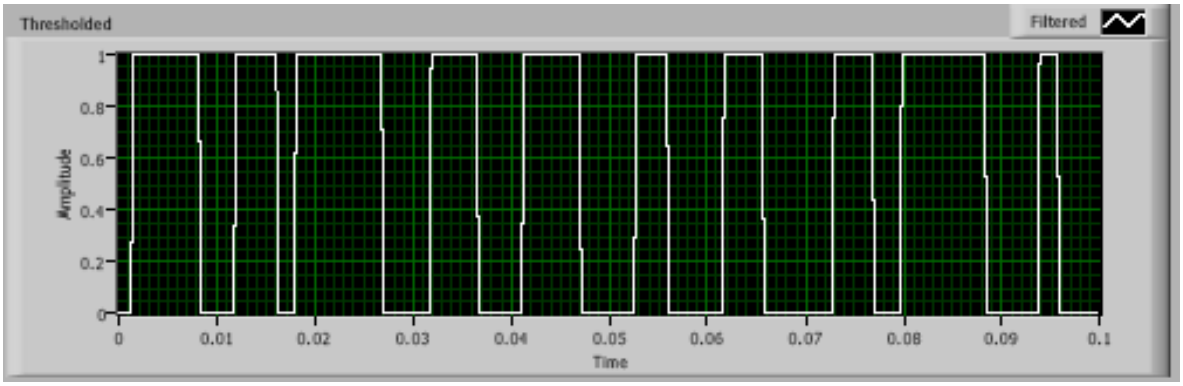


Figure 37. Results of a threshold operation performed on the LPF output waveform. The threshold used is the RMS value of the LPF waveform.

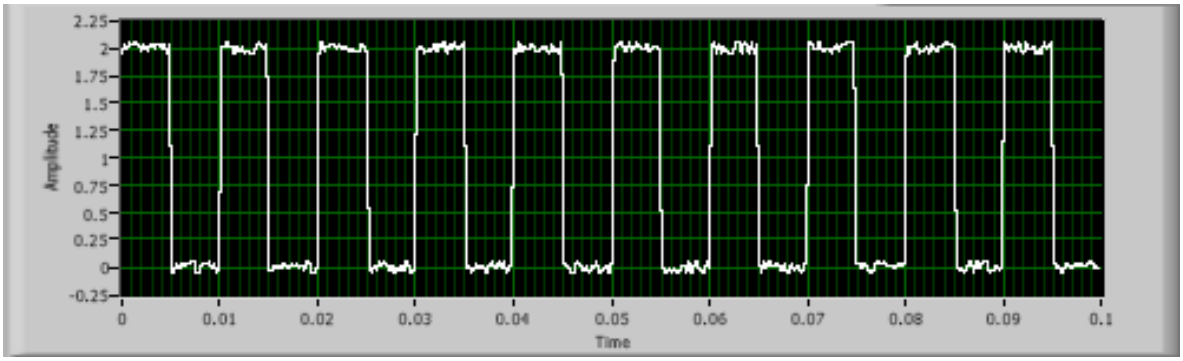


Figure 38. Desired tag's data sequence.

As you can see from the preceding figures, using differential offset spread spectrum to encode, transmit, and demodulate tag data proved to be very effective. Aside from being able to encode and demodulate a tag's data successfully, several tests were run to try and demodulate a desired tag's data using another tag's PN sequence. As predicted, these tests produced results that did not resemble the original data at all, meaning that data transmission is securely encrypted and cannot be recovered without prior knowledge of the system hardware. This technique could be incredibly useful applications that require a high level of privacy protection.

CHAPTER 5:

APPLICATION: OPTIMAL ANTENNA DIVERSITY AND ORIENTATION

5.1 DEFINING THE PROBLEM

In the world of wireless communications, the establishment of a pure line of sight link is nearly impossible for practical applications. In cluttered indoor environments, backscattered signals are especially susceptible to interference phenomenon because all of the communication power is provided from a single source. Common causes of interference such as polarization mismatch and small scale fading can drastically undermine the integrity of a backscatter link [19, 20]. Signal strengths for these backscatter links are therefore generally very weak, so any small amount of noise or interference will increase the bit error rate. It is for this reason that many companies and research groups are looking into multiple antenna arrangements for wireless components in an attempt to minimize situations where the link establishment is weak [19, 20].

Deciding on the position and orientation to place these antennas in respect to each other and the source to achieve maximum signal strength is not a simple task. The electromagnetic theories and equations that govern propagation in multiple antenna situations are complicated to calculate, but their effects on the link are profound. In this chapter we will propose a method that uses the anti-collision algorithm outlined above to concurrently measure the signal strength contribution from multiple antennas in a backscatter environment.

The ability to do so will offer the user a complete and comprehensive analysis of an antenna configuration and make it easier to identify the optimal antenna positions and orientations for a desired wireless link.

5.2 CAUSES OF INTERFERENCE

In any wireless link there are numerous factors that can affect signal strength. In this section we will explore two major causes for signal interference in backscatter links, and provide solutions to help eliminate their effects.

5.2.1 MULTI PATH INTERFERENCE

One common problem that occurs when propagating information in a cluttered environment is multi-path interference. Multi-path interference occurs in situations where the surroundings in an environment prevent the establishment of a line of sight link. The information is transmitted by bouncing the backscattered wave off of the environment to reach the receiver. However, if multiple waves are scattered in complicated environments, their path is unpredictable. When the paths of two waves cross in space, the signal at that point is the linear superposition of those waves. If these waves are in phase they will constructively add to produce higher signal strength, however, if the waves are out of phase they will destructively sum to produce lower signal strength. A typical multi-path scenario is shown in figure 39.

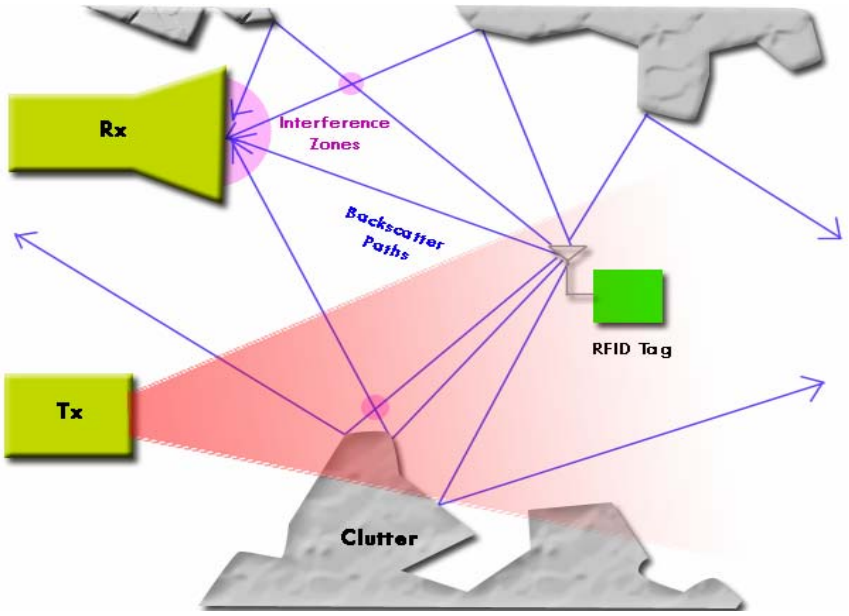


Figure 39. Multi-path interference scenario. The backscattered signal is bounced off the clutter in the surrounding environment, and reflected toward the receiving antenna (RX) where it interferes with itself.

The interference zones create pockets of high and low signal strength distributed throughout the environment where the signal strength is drastically different than the average signal strength in the environment. Therefore as the receiver or tag is moved through the environment, the received signal strength fluctuates rapidly as a function of space [20].

One solution to these rapid drops in signal strength is a concept known as space diversity [12,13]. Space diversity describes a method that uses multiple antennas placed at difference locations in space in order to minimize the probability that the tag or receiver is located in a null [20]. Because these peaks and nulls fluctuate very rapidly in space, if one antenna is in a null region there is a good chance the other antenna may have a signal. Although the concept seems simple, as stated earlier the location of these peaks and

nulls is very difficult to predict. Therefore, deciding upon the optimal distance and orientation to place the antennas in respect to each other is not a simple choice. It requires measurement.

5.2.2 ANTENNA POLARIZATION

Other than interference caused by a backscattered signal interacting with itself, an RFID wireless link can also fall victim to the interrogator's signal interfering with the tag's backscatter. In this case, the pure waveform sent out by the interrogator to query the tags is scattered by the environment and reflected back to the receiver before it is modulated [19]. Figure 40 demonstrates this scenario.

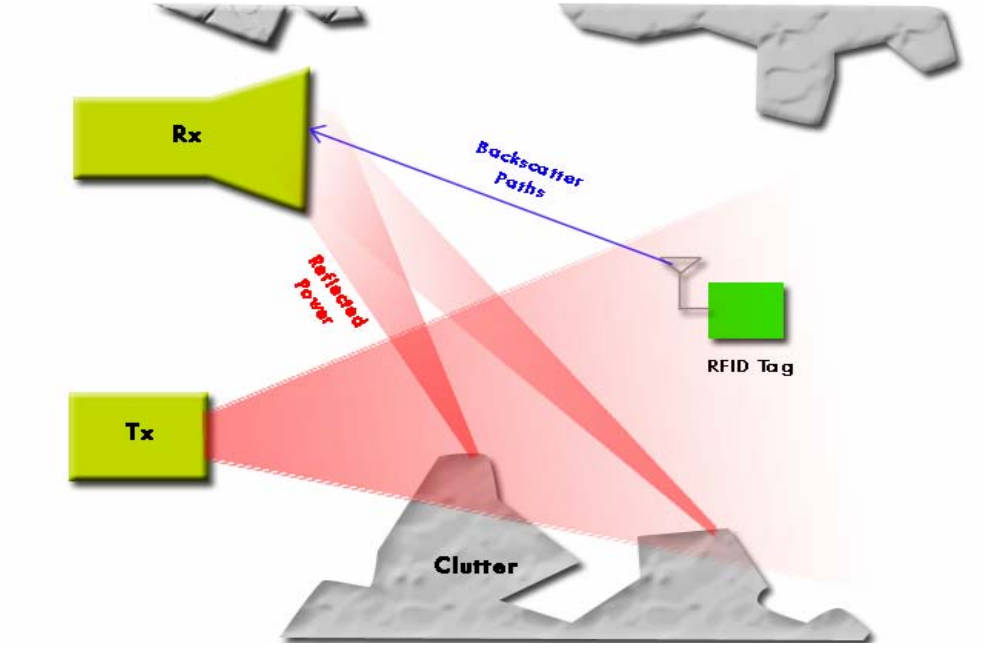


Figure 40. Interrogator backscatter interference scenario. The carrier wave is reflected off the surrounding clutter in the environment, and interferes with the backscatter from the RFID tags.

This type of interference is especially bad because the un-modulated power transmitted from the interrogator is a lot stronger than the backscattered

waveform. If care is not taken, the backscattered waveform may get buried underneath the pure interrogator signal. This signal can not be filtered out because it is caused by the carrier wave and is in the same band as the backscatter.

One solution to this problem exploits a property of electromagnetic propagation known as polarization [20]. Polarization describes the overall orientation of the electric field in respect to the propagation direction. An important property of this value is that antennas can be oriented to maximize or minimize absorption of a wave based on it. If an antenna is oriented in the same direction as a wave's polarization, it will be fully absorbed. Conversely, orienting an antenna orthogonal to a wave's polarization direction will minimize its absorption [19, 20].

Using this knowledge, rotating one of the antennas in the interrogator orthogonal to the other prevents the waveform produced by the transmitter from being absorbed by the receiver. This eliminates the reflected power interference. However, the tag antenna needs to interact with both antennas of the interrogator, so it is typically oriented at an angle between the two [20]. Doing so limits the amount of power absorbed and reflected by the tag, but eliminates the potential for interference as well. This method of interference prevention is known as cross polarization [19,20].

5.3 SYSTEM DESIGN

In order to minimize the effects of wave interference in a wireless link, multiple antenna arrays can be designed to exploit the solutions to interference presented above. However, finding the optimal orientation and diversity for a given application is difficult. In the following section we will explore a system designed and created for this project that will allow the users to fully analyze the performance of a multi-antenna array.

5.3.1 THEORY

The same system described above used to solve the problem of RFID signal collision can be extended for use in concurrent multiple antenna signal strength measurements. If the data multiplier stage is bypassed in the RFID tag hardware, then only the PN sequences unique to each tag are transmitted. The result of the demodulation stage thus leaves behind only a constant DC value after the low pass filter. The magnitude of this DC offset corresponds to the signal strength contribution of a single tag in a multi-tag environment. The following figures demonstrate the theory behind the signal strength recovery using a single tag's backscatter.

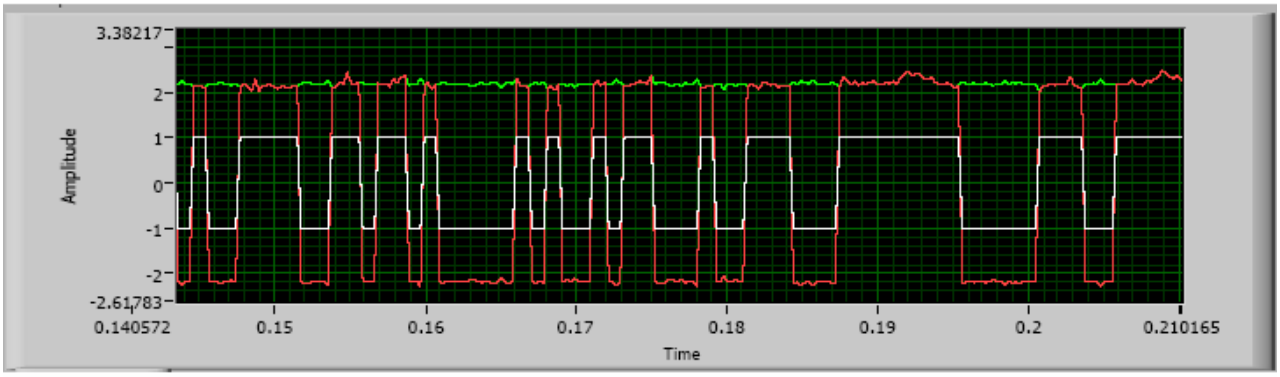


Figure 41. Single tag backscatter multiplication results where the simulated chipping sequence and the backscattered chipping sequence are in phase. The red waveform is the backscatter, the white is the simulated sequence, and the green is the product.

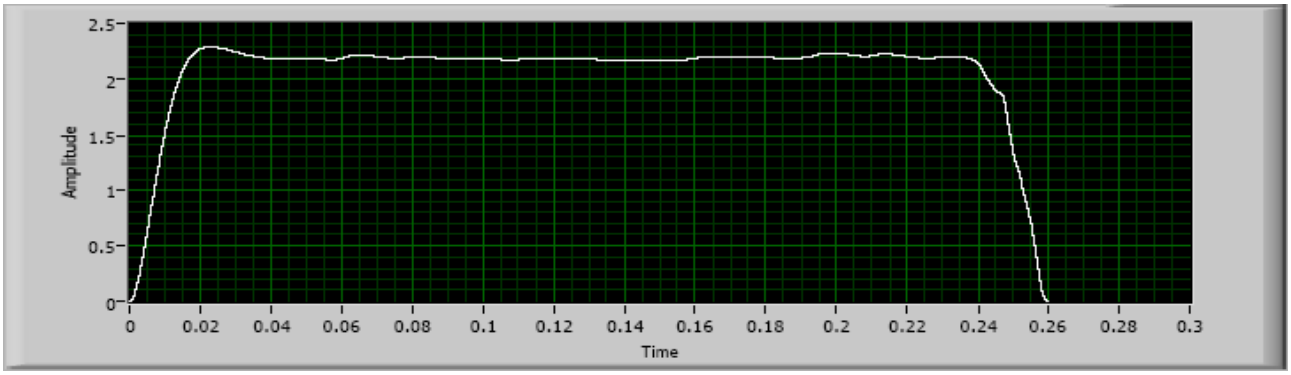


Figure 42. Result of the data demodulation stage. The RMS value of this graph corresponds to the signal strength contribution of a single RFID as seen by the interrogator

By varying the orientation and position of each RFID tag's antenna, the signal strength contribution from that antenna in a multi-antenna environment can be measured. These measurements can be taken for multiple tags concurrently, and thus the performance of an antenna configuration at a given instant can be effectively recorded.

5.3.2. SYSTEM SETUP

Using the solutions for interference prevention discussed above, a test rig was constructed to accommodate a dual antenna signal strength performance experiment. To construct this rig, two angularly marked surfaces were created

with indications at every 10 degrees. A pivot was placed in-between these surfaces to allow them to rotate in respect to one another. The back surface was placed in a fixed orientation with the interrogator. The front surface is allowed to pivot freely. Also on the front surface are two armatures that can pivot to vary their angle in respect to each other. The antennas are fastened to these angular guides and rotated to determine their angular diversity. The antennas can also slide up and down the armatures to vary their separation distance. A picture of this setup is shown in figure 42 below.

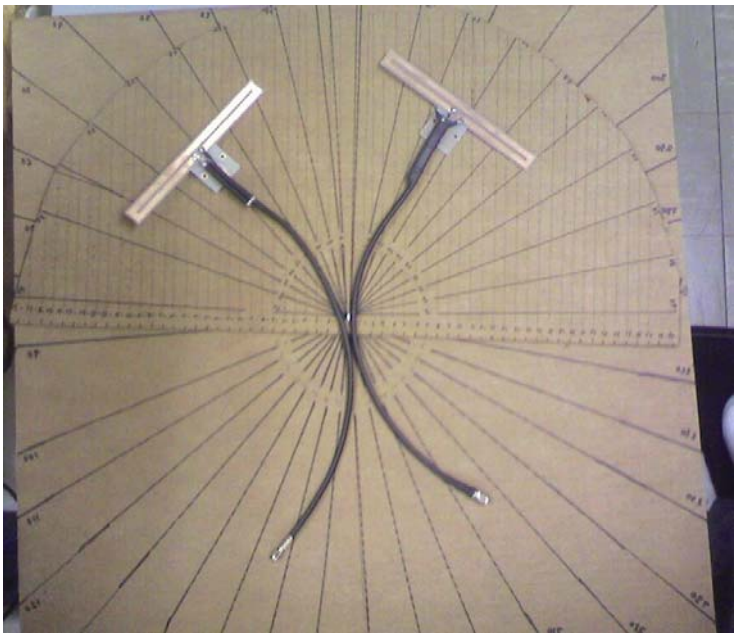


Figure 43. Photograph of the dual antenna orientation rig. The antenna armatures can rotate to determine angular diversity. The antennas themselves can slide up and down the arms to vary their separation distance.

Using this setup, polarization and spatial diversity could be varied for both antennas, and the effect of their change on the signal strength of the link

could be monitored. Figure 44 shows the basic layout of the duel tag measurement setup.

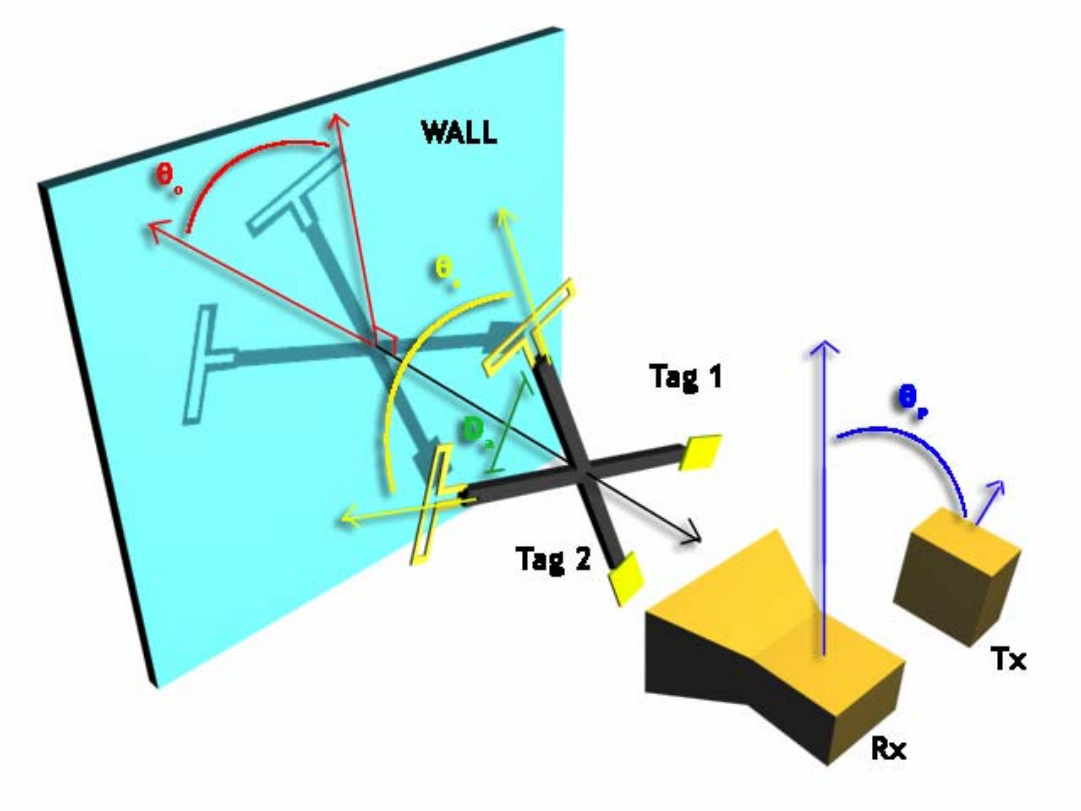


Figure 44. Antenna diversity and polarization measurements setup. Θ_a is the polarization angular diversity between the two antennas, D_a is the spatial distance between the two antennas, θ_p is the polarization angle between the interrogator antennas, and θ_o is the orientation angle between the antennas and the interrogator.

.

By varying the angles and distances in figure 44, many test cases for antenna diversity and polarization could be created and explored. Θ_a is the polarization angular diversity between the two antennas, D_a is the spatial distance between the two antennas, θ_p is the polarization angle between the interrogator antennas, and θ_o is the orientation angle between the antennas and the interrogator.

5.3.3. TEST CASES

For each test case, Θ_a, D_a, and θ_p were set to specify the current antenna arrangement. Next, a measurement of the signal strength for each tag was taken at every 10 degree increment of θ_o. Using these parameters and exploiting the potential solutions to interference, six test cases were devised and their results are provided in this document. The six cases are shown in the following figures.

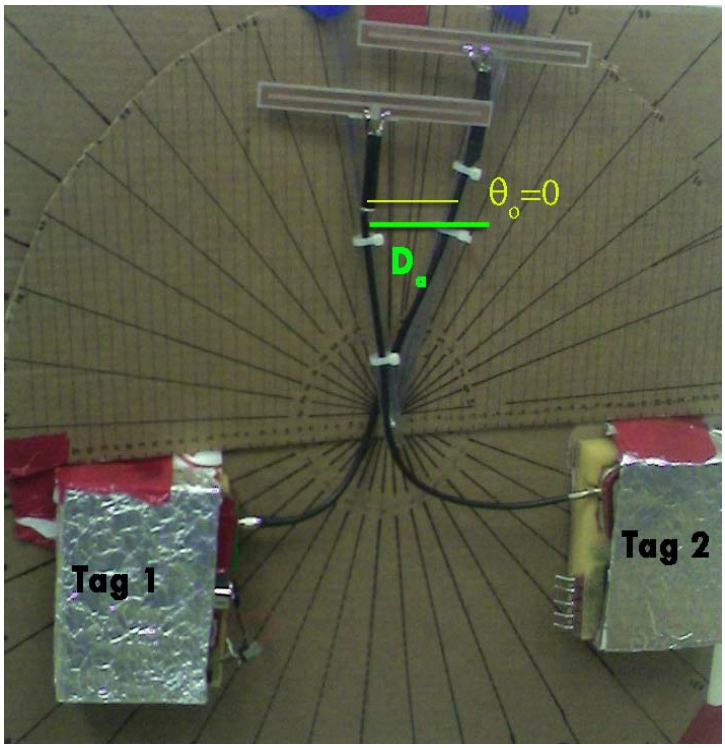


Figure 45. Antenna diversity case one. Angular diversity is 0 degrees.

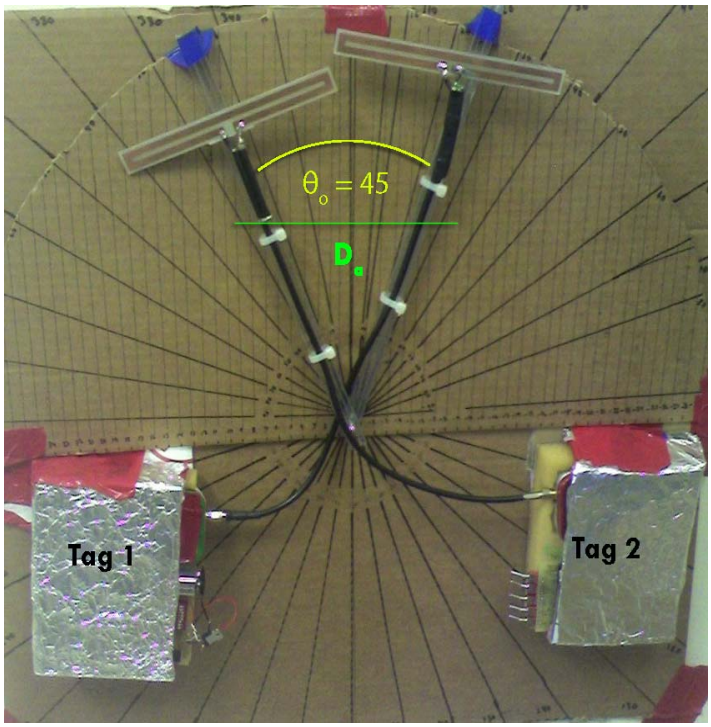


Figure 46. Antenna diversity case 2. Angular diversity is 45 degrees.

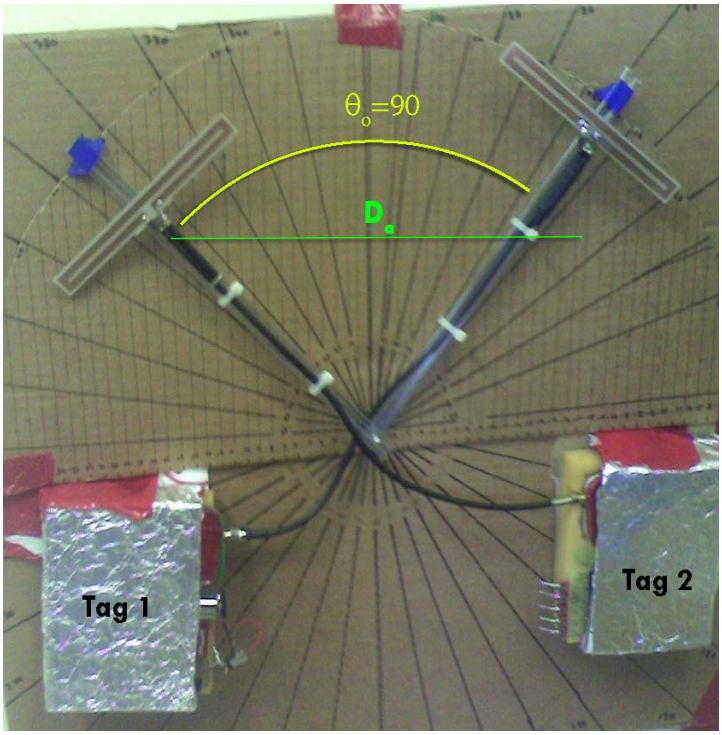


Figure 47. Antenna diversity case 3. Angular diversity is 90 degrees.

The three arrangements shown above were tested with the interrogator both linearly polarized, $\theta_p = 0$, and cross polarized, $\theta_p = 90$. Figures 48 and 49 showcase these orientations respectively. The value of D_a was varied for each test and will be labeled in the final graphs.

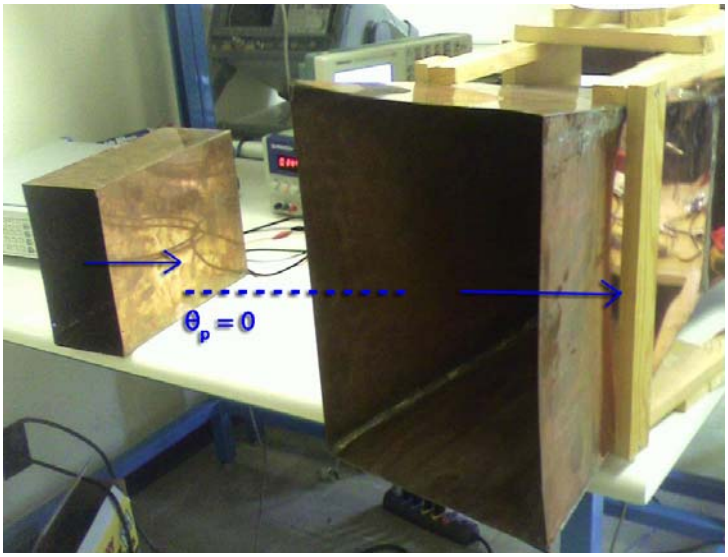


Figure 48. Linearly polarized interrogator, meaning the antenna feeds for both interrogator antennas are facing the same direction.

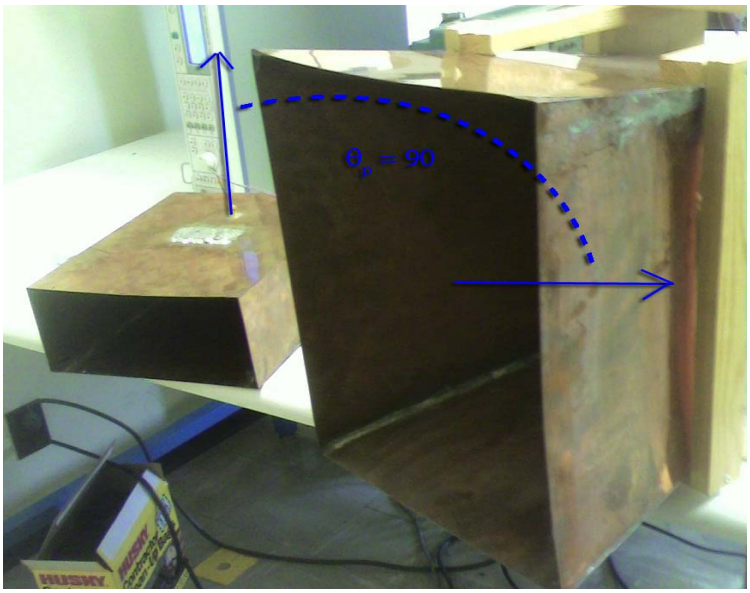


Figure 49. Cross polarized interrogator, meaning the antenna feeds for both interrogator antennas are orthogonal to each other.

5.3.4. MEASUREMENTS

To take the measurements, a modified version of the main driver program was created. The main alteration to the original driver is that the input signal is split and multiplied separately by both tags' simulated PN sequences in order recover the signal strength from each tag at one instant. This program was run for every reading on both the in-phase and quadrature outputs produced by the IQ demodulation circuit. The output of each measurement is the I-channel received signal strength and Q-channel received signal strength for each tag. These readings were taken at every ten degree increment of θ_o. The total power reflected from each tag at each reading is calculated using the following equation.

$$P_{rec} = \sqrt{\left(RSS_{Ichannel}\right)^2 + \left(RSS_{qchannel}\right)^2} \qquad (17)$$

Figure 50 shows the GUI that was built to observe each measurement for both channels. It is important to notice the relative flatness of the low passed signals from each tag. The RMS value of these curves was used as a measure of the received signal strength for each antenna.

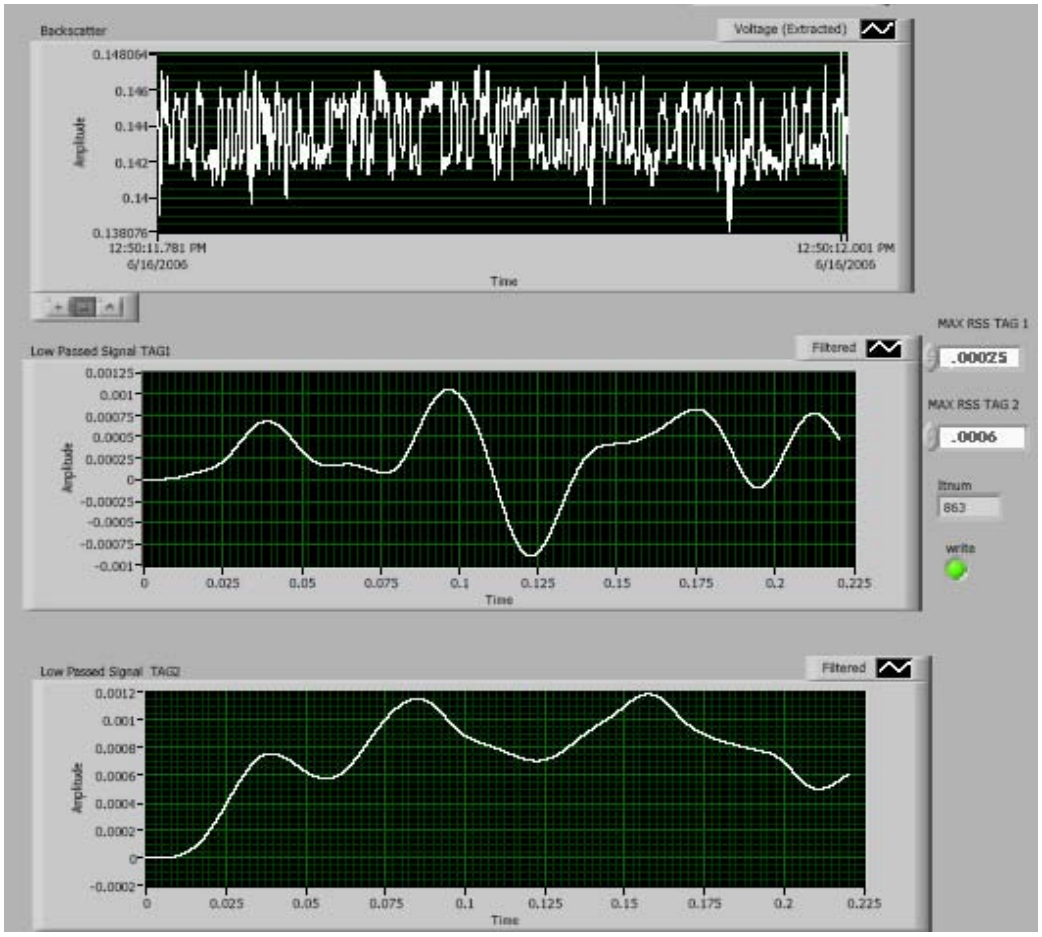


Figure 50. I channel multi-tag antenna signal strength measurements. The top waveform is the backscattered signal received by the interrogator. The second graph is the convergence result of the data demodulation stage for tag 1. Similarly the following plot is for tag 2. The RMS value of these plots corresponds to the signal strength contribution to the wireless link from these tags.

5.4 RESULTS

Provided in the figures 51-56 are the results of the multi-antenna configuration experiment. A separate graph is provided for each of the cases to show the power contribution of each antenna as a function of the orientation angle θ_o.

5.4.1 LINEARLY POLARIZED INTERROGATOR

The following figures were produced using a linearly polarized interrogator. This means that the feeds from both the reception and transmission antenna are pointing in the same direction.

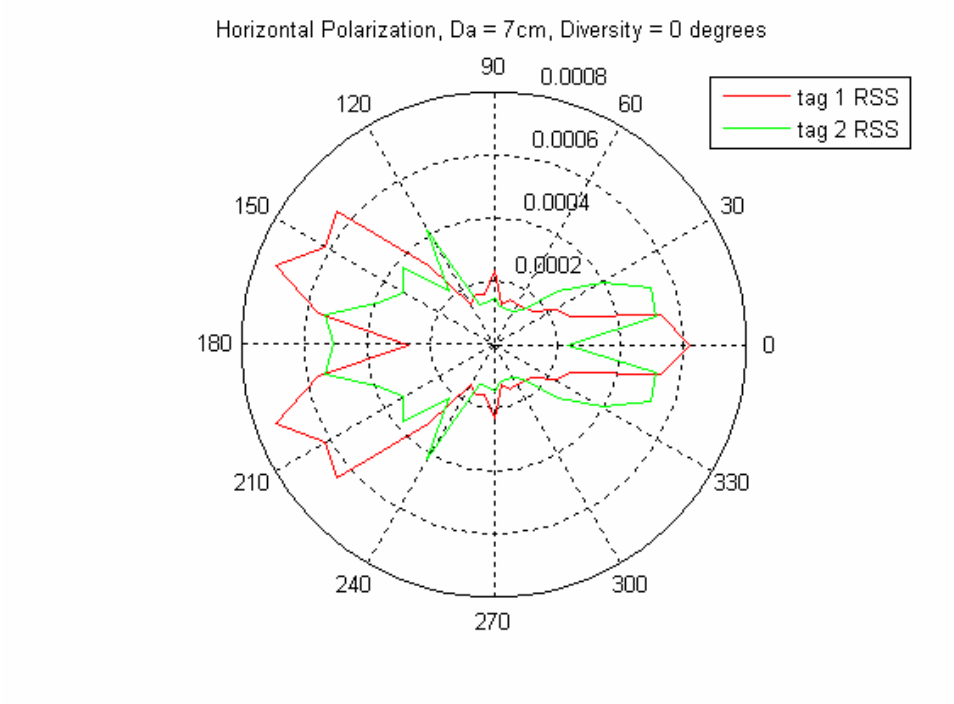


Figure 51. Antenna signal strength plot as a function of angular orientation with respect to the interrogator. Da= 7cm and angurlar diversity =0. Linearly polarized antenna.

Figure 51 shows the power received by the interrogator from each RFID tag as a function of orientation to the interrogator. Through visual inspection the overall envelope trend of the configuration appears correct. When the antennas are oriented in line with the polarization angle of the interrogator, the measurements from both RFID tags are at a peak. This occurs at zero degrees. When they are oriented orthogonal to the interrogator's polarization

angle the signal strength from both antennas is a lot weaker. This occurs at 90 degrees. Since there is no angular diversity between the antennas, you would expect the trends in the graph for both tags to mimic each other as demonstrated in the preceding figure.

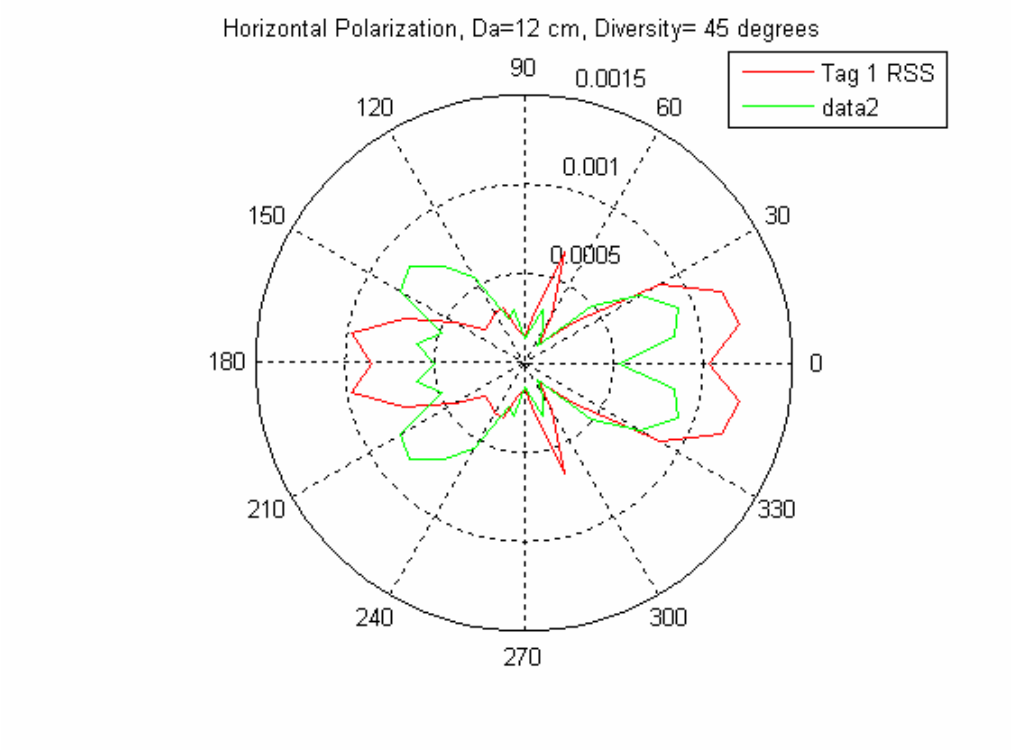


Figure 52. Antenna signal strength plot as a function of angular orientation with respect to the interrogator. Da= 12cm and angular diversity =45 degrees. Linearly polarized antenna.

Similar to the previous case, the overall envelope of the antennas signal strength measurements occur as expected. However, since the two antennas have an angular separation of 45 degrees centered on the zero degree mark, each antenna has an angular orientation of 22.5 degrees with the rotation axis. Thus, the angular orientations that bring the antennas into complete polarization match with the interrogator are positive and negative 22.5

degrees. If you observe the graph, you can see that the maximum peak angles occur at these predicted locations. However, also due to the angular diversity between the two antennas you would expect the plot of one antenna to lag the other one with an angular difference of 45 degrees. The reasons preventing this trend from occurring are presented in the following section of the paper.

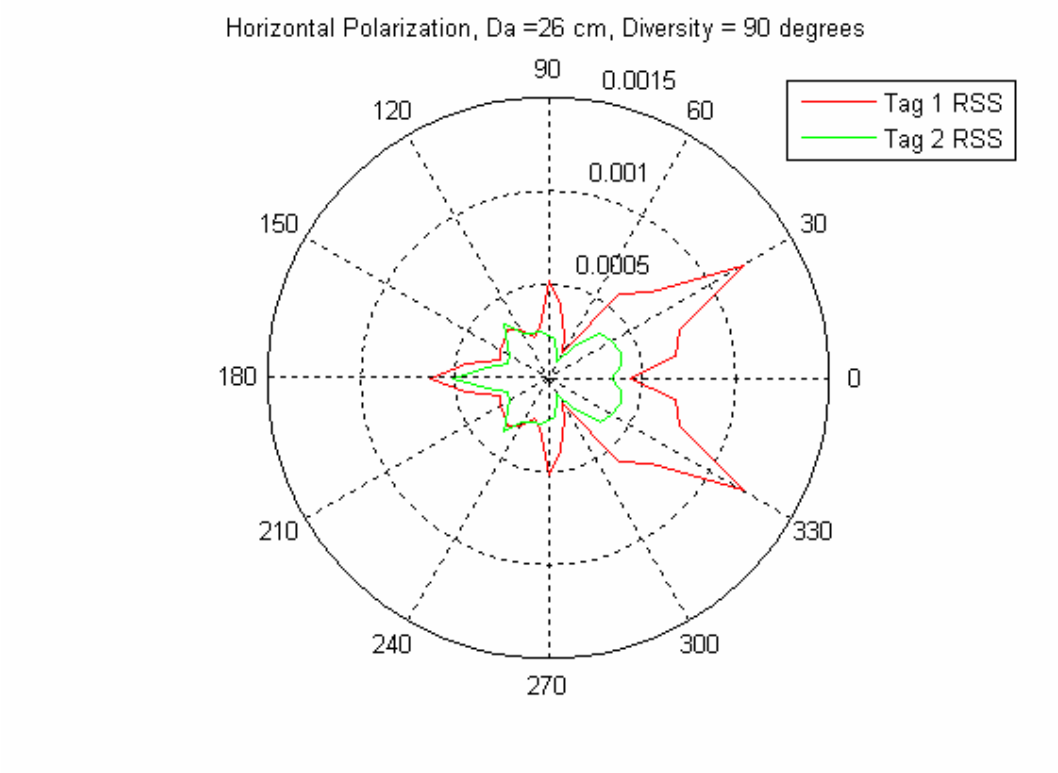


Figure 53. Antenna signal strength plot as a function of angular orientation with respect to the interrogator. Da= 26cm and angular diversity =90 degrees. Linearly polarized antenna.

The analysis of figure 53 is nearly identical to that of figure 52. The only difference is the angular diversity between the two the antennas is 90 degrees. This should cause the maxima of the orientation plot to occur at approximately positive and negative 45 degrees. Through visual inspection, it can be seen that the maxima of both plots occurs at nearly positive and negative 30 degrees.

This error could be caused by inaccuracies in measuring the angular orientation of the antenna configuration. The discrepancy could also have come through the interpolation of data points. Since the readings are only taken at 10 degree increments, the angle 45 degrees is never measured directly. Therefore, the computer linearly interpolates the data between 40 degrees and 50 degrees to generate the plot. Although the general angular location of the maximums is off by a few degrees, their angular separation is greater than in the previous cases as would be expected.

5.4.2 CROSS POLARIZED INTERROGATOR

The following figures were made using a cross polarized interrogator. This means that the feeds from the reception and transmission antenna are pointing in orthogonal directions.

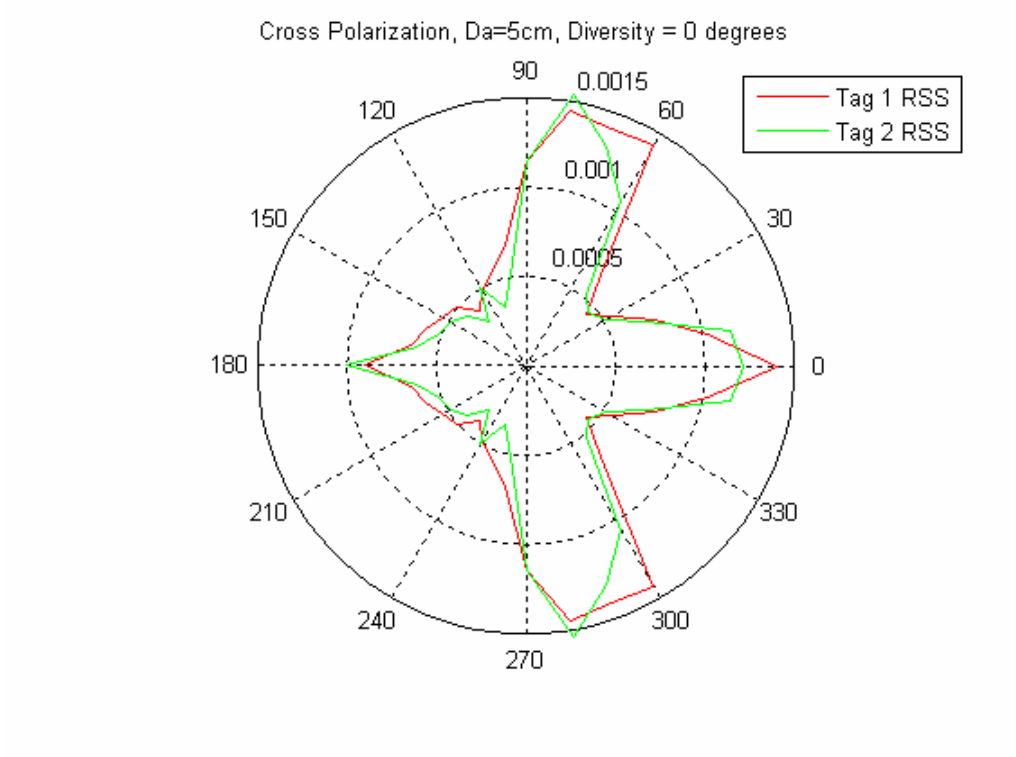


Figure 54. Antenna signal strength plot as a function of angular orientation with respect to the interrogator. Da= 5cm and angular diversity =0 degrees. Cross polarized antenna

.

The analysis for antenna configurations using a cross polarized interrogator is not as straightforward as in the linear polarization cases. This is because there is no optimal polarization angle where the tags will be aligned with the interrogator. In these cases, the signal strength of an antenna is both a function of respective orientation to the interrogator as well as a function of the carrier wave to signal interference. However, similarly to the linear

polarization configurations, it is expected that at some angle there is an optimal balance of these two factors. Through visual inspection of figure 54, this angle occurs at positive and negative 60 degrees. Electromagnetic propagation theory would predict this angle to occur at positive and negative 45 degrees. This 15 degree discrepancy may be caused by the same errors that produced the 15 degree discrepancy in figure 53. The peak at zero and 180 degrees are caused by the polarization match between both tag antennas and the receiving antenna.

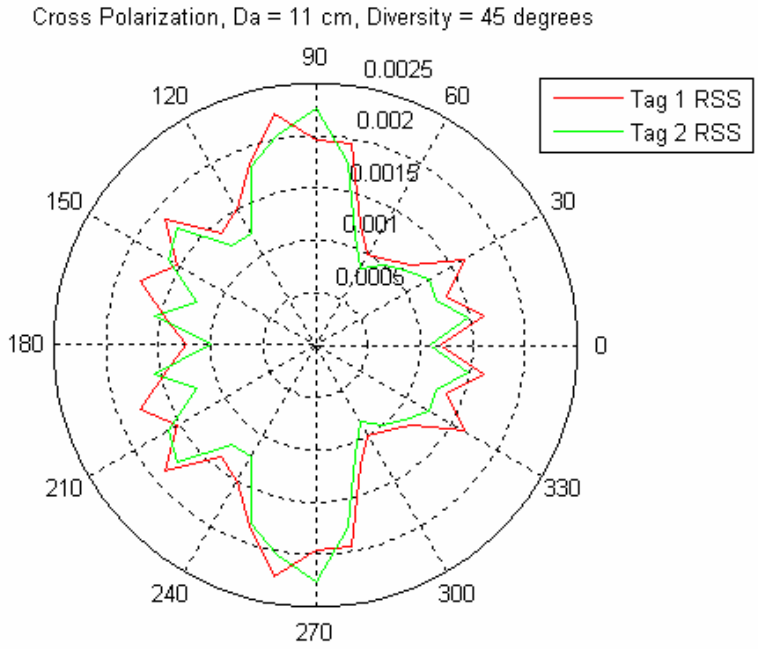


Figure 55.Antenna signal strength plot as a function of angular orientation with respect to the interrogator. Da= 11 cm and angular diversity =45 degrees. Cross polarized antenna

The case presented in figure 55 is a particularly interesting one. As mentioned earlier, using a cross polarized antenna one would expect the optimal balance of angular orientation and carrier wave to signal interference to occur at 45 degrees. Therefore, placing the antennas at 45 degrees with respect to each

other ensures that at nearly every orientation one of the antennas will be closely aligned with this angle. Therefore, you would expect the signal to stay relatively stable as its orientation angle changes. Comparing figure 55 to the other the plots shows this configuration to be the most stable, and therefore the most desirable antenna configuration for the duel antenna experiment.

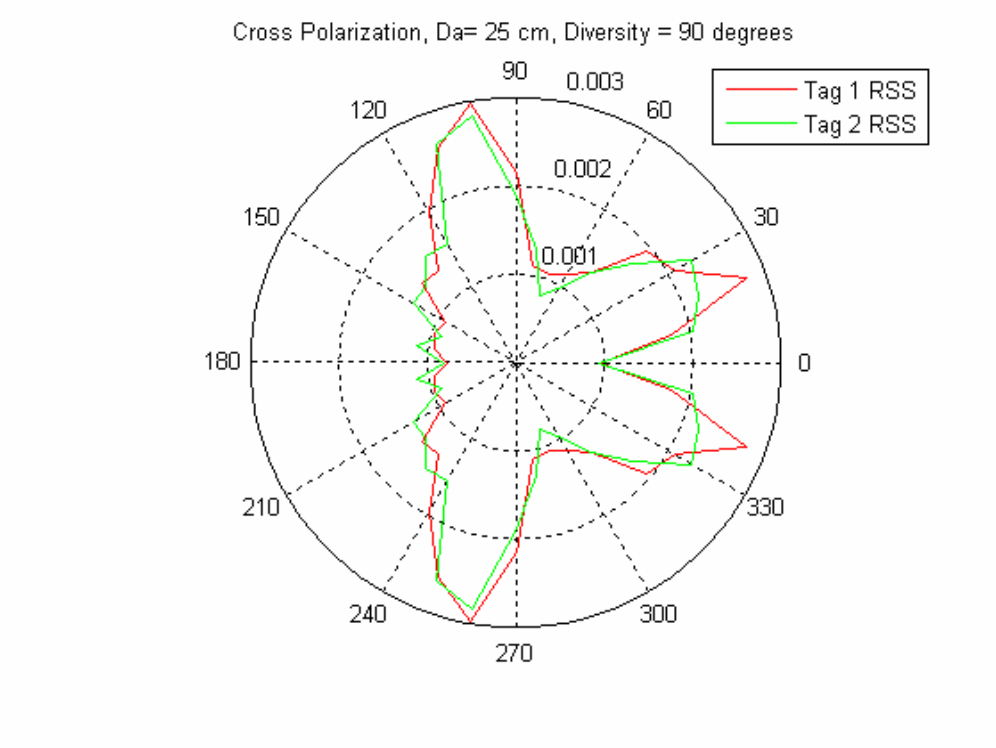


Figure 56. Antenna signal strength plot as a function of angular orientation with respect to the interrogator. Da= 25 cm and angular diversity =90 degrees. Cross polarized antenna

In figure 56, the angular diversity between the RFID tag antennas is 90 degrees. As the antenna configuration is rotated, it is expected that there would be extreme peaks and nulls caused by the drastic angular diversity. Since the antennas are orthogonal to each other, when one is situated at the maximum orientation angle of positive or negative 45 degrees, the other antenna is

positioned at the other maximum orientation angle. This causes the strong peaks. Also as would be expected, these peaks resemble those in figure 54 but with a greater angular separation resulting from the greater angular diversity.

5.5 DISCUSSION

Through inspection of the preceding results, some general trends about antenna diversity and polarization can be deduced. The overall shapes of the plots follow basic electromagnetic theory in predicting the signal strength for an antenna arrangement at varying orientation in respect to the interrogator [20]. Also as expected, the test case that provides the least fluctuation in signal strength and the best stability is the cross polarized configuration with the antennas oriented 45 degrees from each other. However, there are some consistent and unexpected trends that may challenge the feasibility of this approach.

If you observe the graphs above, it is easy to see through visual inspection that trends for both antennas' received signal strength plots are nearly identical in each graph. This should be the case where the angular diversity is equal to zero; however, as the angle between the antennas is increased the plots should rotate with respect to each other. In a point where one antenna experiences a null in respect to the interrogator, the second antenna should experience the same null as it rotates into the same position. But, it appears that the overall signal strength of the system varies identically for each antenna as function of angle. I believe the reason for this error is caused because the anti-collision

algorithm presented in this paper is extremely dependant on the bit pattern received by the computer. However, as the signal strength decreases, so does the ability to resolve the bit stream. Also, the magnitude of the received signal strength for both antennas decreases. When the ability to resolve the bits diminishes, then the convergence condition that provides the exclusion properties of the algorithm fails. This can be seen by fluctuation of the convergence curves shown above for a single measurement. At this point, the convergence of each tag simply returns a signal strength value as a function of the magnitude of the overall link.

Other causes for errors in the backscatter could result the following electromagnetic phenomenon as well.

- Shielding – Although the RFID tags were encased in an aluminum foil enclosure, some of its components may still have interfered with the backscatter. Without ideal shielding, the modulation circuitry, balun, and DC feed wires may all have been backscattering more modulation than the tag antennas.
- Coupling – When dealing with a carrier frequency of 915 MHz, antennas with a separation distance less than 15 cm will begin to couple with each other, meaning their pattern will change in polarization and directivity. Power leaking from one antenna to the other can change the transmitted bit pattern for the RFID tags.

- Near Field Material Effects- Since the antenna measurements were taken with the rig placed directly against the wall, the material properties of the drywall and irregular metal studs may have affected the antenna patterns. These materials can cause coupling and distort the antenna patterns to yield unpredictable results.
- Multi-path – Since the illumination may not be a pure plane wave, there will be choppy irregular results superimposed atop the expected trends.

In conclusion, the anti-collision RFID method of multiple-antenna signal strength measurements has many pros and cons. As it stands now, the system is useful for observing the overall trends in performance for a given multi-antenna configuration, but falls short in the ability to show the independent contribution of each antenna.

CHAPTER 6:

CONCLUSIONS AND FUTURE WORK

The preceding document provided a brief history and discussion about the theories behind RFID. The paper further presented a new approach to anti-collision RFID using a differential offset version of the spread spectrum technique. It then explored the design and implementation stages behind creating a fully function RFID system to accommodate this new approach. Furthermore, it continued to present experiments and results for applying this system to a new application for monitoring multi-antenna configurations.

6.1 ACCOMPLISHMENTS

Below is a list of the accomplishments resulting from this project.

- A new system for anti-collision RFID was devised which has many advantages to current industry standards.
- Specialized hardware was fabricated and assembled to create a custom interrogator used to query the RFID system and receive the tag backscatter.
- RFID tags were designed and fabricated to accommodate the spread spectrum algorithm with minimal hardware by using a new sequence generation scheme known as differential offset.
- Software was written in Labview and Matlab to interpret the backscattered waveform to recover data for a desired tag.

- A novel application for this system was developed for use in antenna diversity and polarization experiments.
- The software and hardware designed for the anti-collision RFID system was adapted to accommodate this new application.
- A special test rig was designed and constructed to generate multiple antenna test cases for individual signal strength measurements.
- Measurements were taken and analyzed using the modified system and newly designed test rig.

Throughout this project there have been various successes for proof of concept. Use of the system to encode, encrypt, transmit, and demodulate data from multiple tags was a success. Using the system for multiple antenna signal strength resolution worked well as an overall measure for antenna configuration performance, but fell short in the ability to resolve individual antenna contributions. However, given some future work, this system can be improved and expanded.

6.2 FUTURE WORK

Although the system performed the basic functionality outlined by the project proposal, there are modifications that can be made to improve its performance.

- **Sampling:** One of the main problems with the program is sampling the incoming signal. It was stated earlier that the sampling rate for the data

acquisition board was programmed to be 4 kHz. This number was calculated under the assumption that the internal clock on the RFID tags is 1 kHz. However, through investigation it was found that the on board clock for each tag ranged anywhere from 970 Hz to 1.2 kHz. This mismatch causes a successive drift in the bits when synchronized with the simulated sequence. This drift results in increasing periodic errors in the demodulation operation, and can drastically affect the results of the algorithm. Future work on this system could include finding better hardware for the onboard timing, or creating an adaptive sampling rate to mimic the imperfections in the hardware.

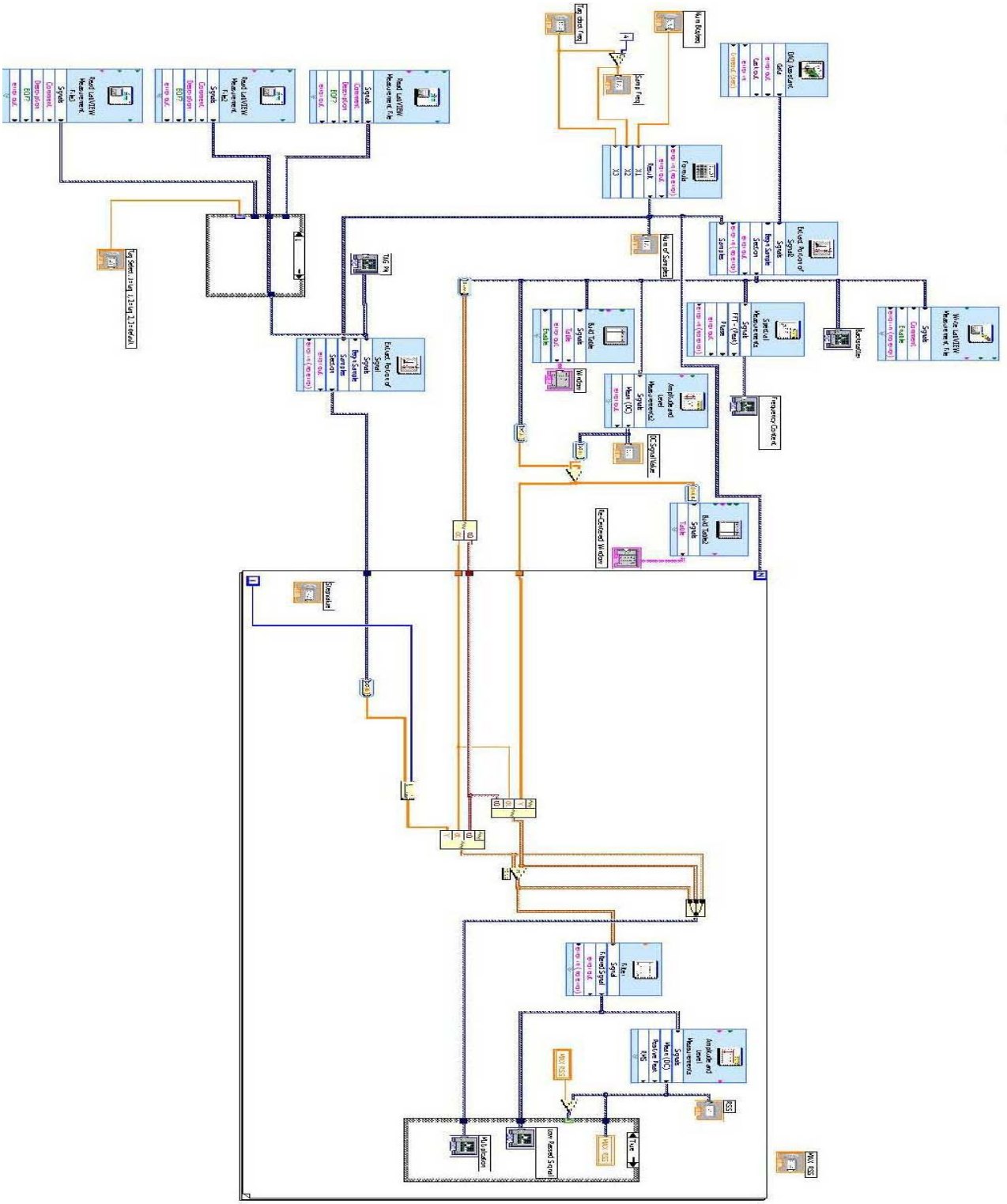
- **Backscatter Resolution:** As stated above, one of the main reasons that the multi-antenna signal strength exclusion experiment did not meet all of its goals was the inability to resolve the transmitted bit pattern at a low power orientation. Finding the optimal placement for the receiver antenna to maximize the bit resolution was tedious and difficult task. Future work could be done to fine tune the receiver hardware to increase the backscatter resolution in low power configurations.
- **Power Consumption:** Currently the RFID tags that were designed and built for this project are independently powered using a nine volt battery. Since the tags were built using standard TTL chips and hardware, their power consumption is rather high. The power supply on the tags only lasted about 10 hours before dying. Future work could be

made to replace the TTL components with low power surface mount chips, and devise a more renewable or longer lasting power source.

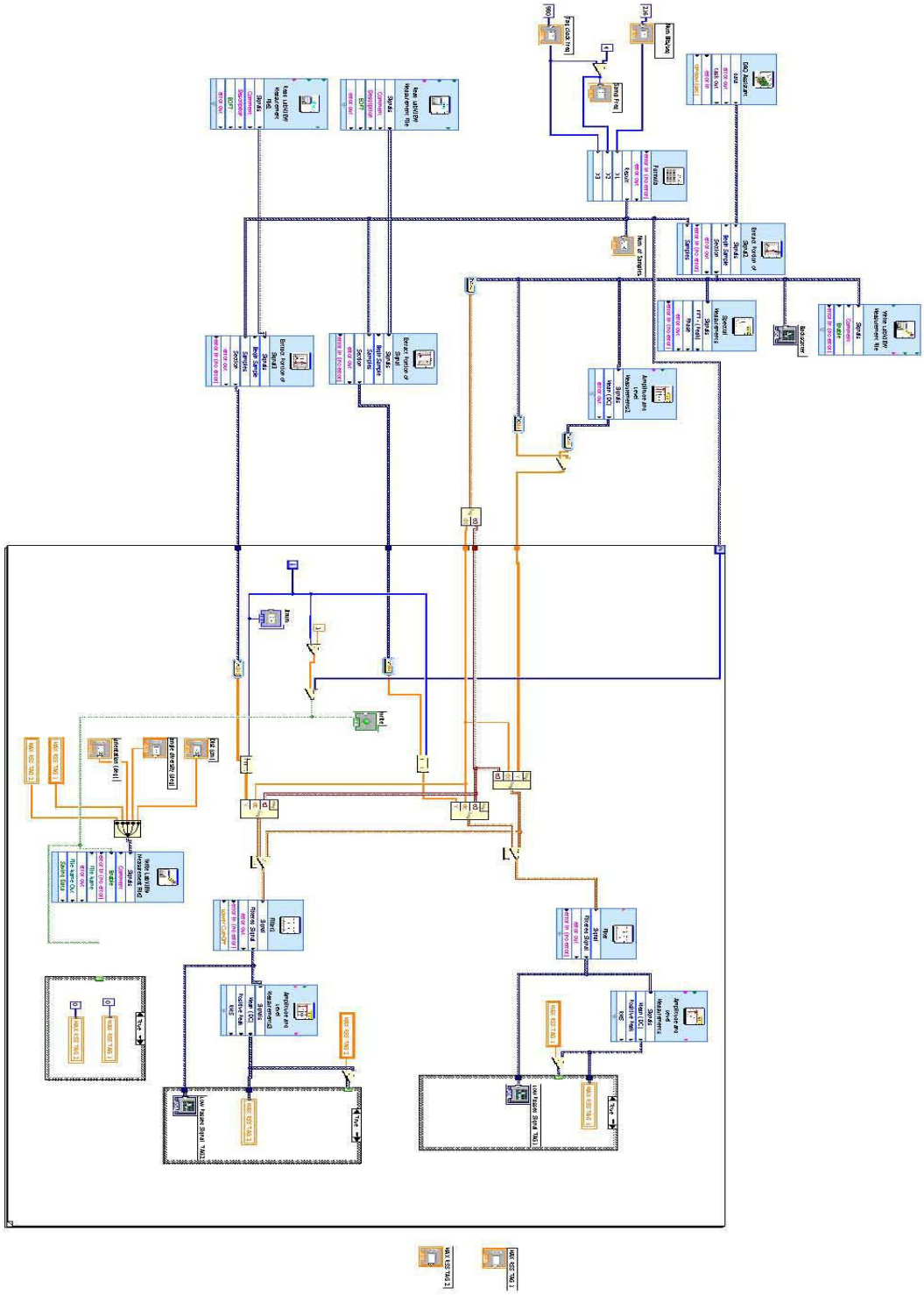
- **Miniaturization:** Similar to the last recommendation for future work, shielding the next step for this project includes miniaturization of the RFID tags. If this system is to be deployed for mass use, the tags will need to be smaller and less obstructive. This can easily be done by replacing the TTL components and fabricating the hardware with surface mount chips. The diode network and transmission line can also be printed on the same board as the tag circuitry to make them small and compact.
- **Applications:** Although this project proved this system can be successfully built, future work could be done to apply it to other uses. Because it is so versatile and adaptable, many possible applications can be devised for use of this system including but not limited to, antenna diversity experiments, antenna design optimization, Inter-tag coupling analysis, and anti-collision development and commercialization.

Although there were many successes in this project, there is still much work that can be done to improve the system. Using the guidelines for future work outline above, this system can be made smaller and more efficient to the point where mass implementation for commercial use is completely feasible. The possibilities are vast and endless.

APPENDIX A: MAIN DRIVER PROGRAM

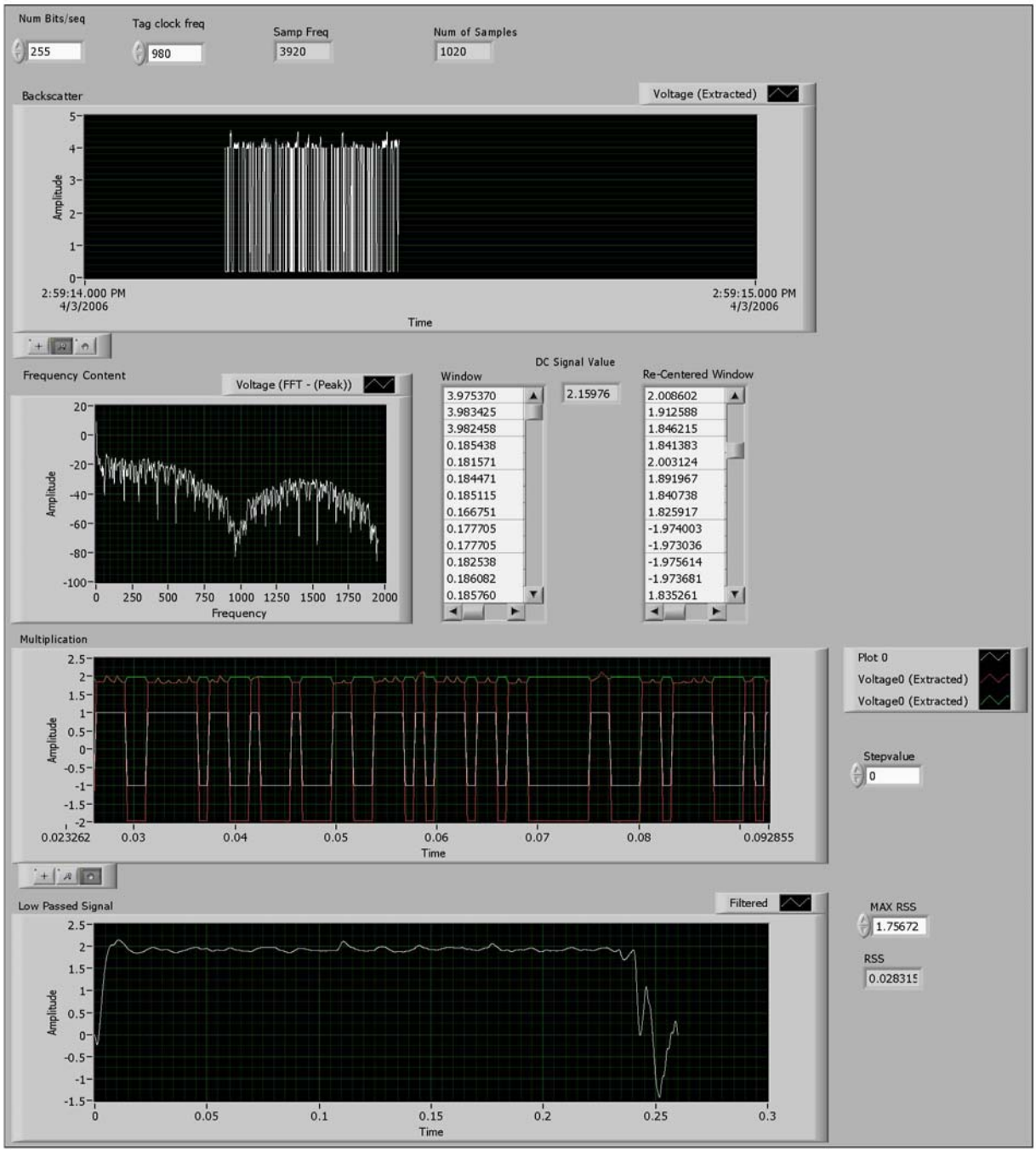


APPENDIX B: MULTIPLE ANTENNA MEASURMENT DRIVER



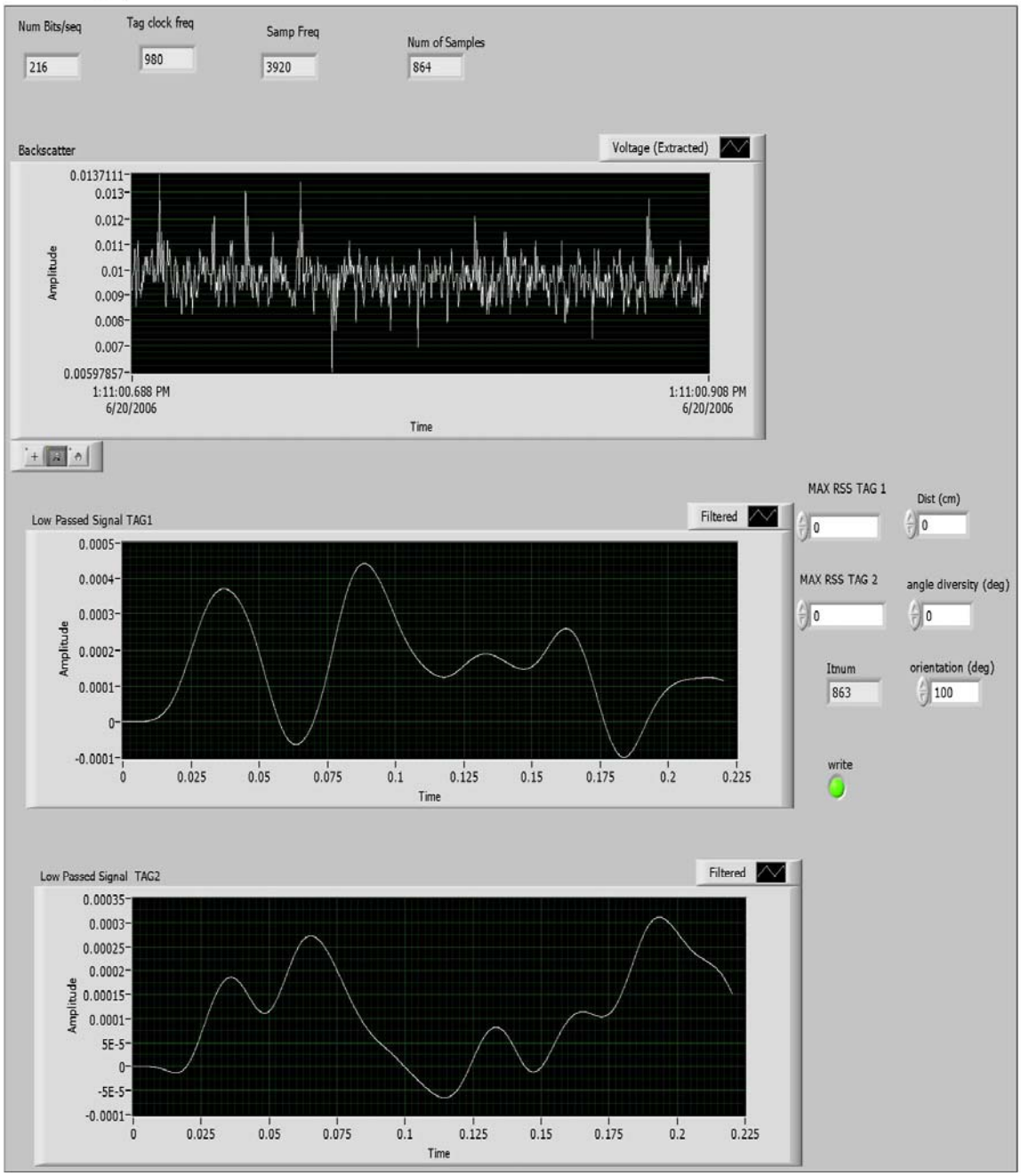
APPENDIX C: MAIN DRIVER GUI - CONVERGING TAG

driver1tag.vi
C:\Documents and Settings\admin\Desktop\Anils app\Polarization\working\driver1tag.vi
Last modified on 4/3/2006 at 2:13 PM
Printed on 4/3/2006 at 3:19 PM

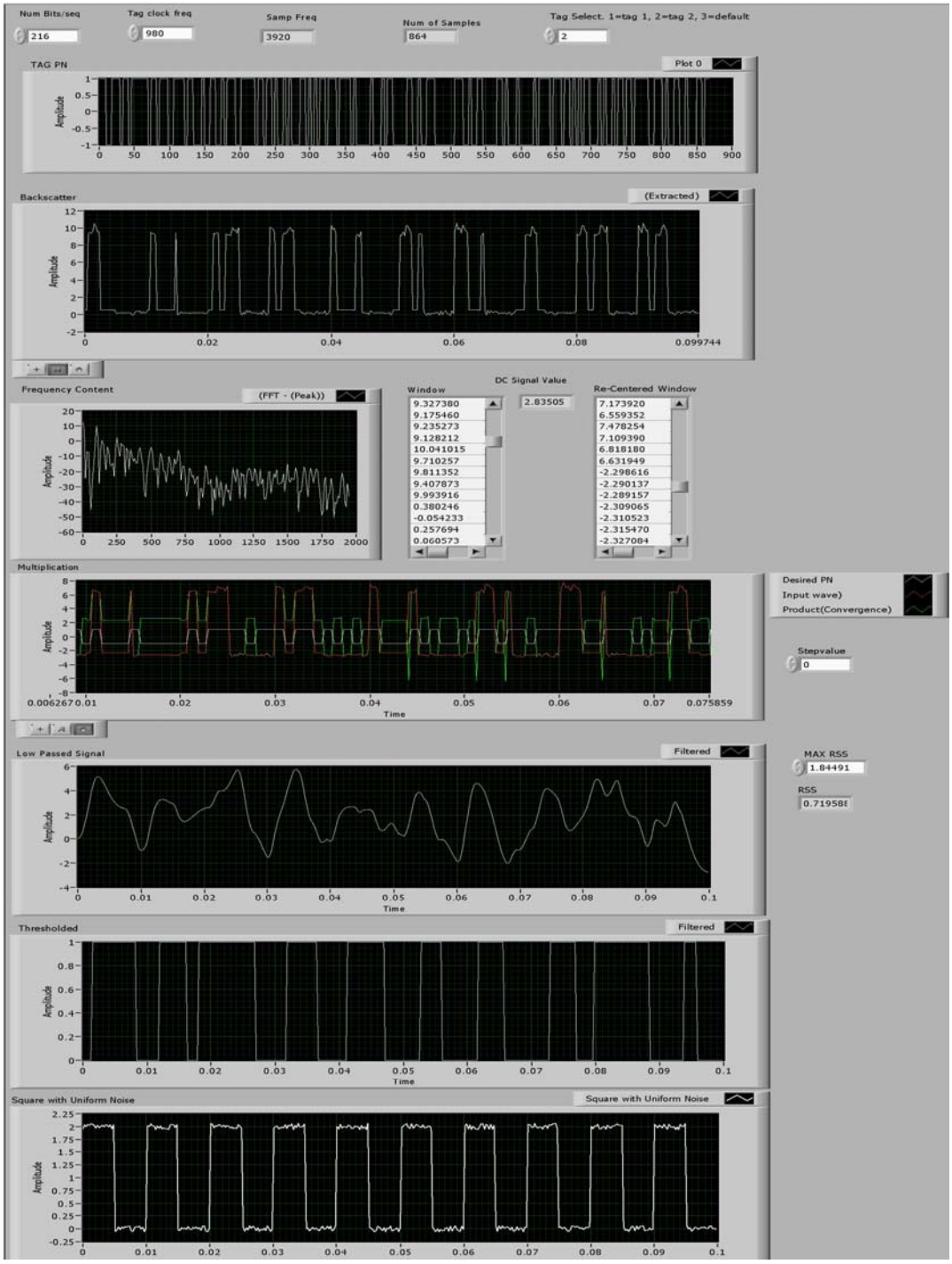


APPENDIX D: MULTI TAG SIGNAL STRENGTH CONVERGENCE GUI

-I CHANNEL CONVERGE



APPENDIX E: DATA RECOVERY GUI - SUCCESS



APPENDIX F: SEQUENCE SIMULATION FUNCTIONS

```
%Anil Rohatgi
%PN generator
%Given initial conditions and a pickoff point
%Function generates a PN sequence of 256 bits

function PNout=PNgen(init, pick)
reg=init;
offset=16;

for i=1:2:255*2+offset
    xor1=reg(8);    %take output
    xor2=reg(pick); %take pickoff bit
    PN(i)=xor1;     %set output to PN bit
    PN(i+1)=xor1;
    reg=circshift(reg,[0,1]);   %rotate shift register
    reg(1)=xor(xor1,xor2);      %Xor the two bits and set
the first bit
end
PNout=PN(offset+1:255*2+offset);

end
```

```
%Generates a simulated signal given two PNs
%Function takes in two PNs of 256 bits
%Returns the result of these xored together with a given
shift

function sim= simseq(PN1, PN2, shiftamt)
    PN2=circshift(PN2,[0,shiftamt]);
    sim=xor(PN1,PN2);
end
```

APPENDIX G: IDdecode program

```
%Driver function for ID decode
%given an input data stream
%Decode what RFID tag is transmitting

PNin=csvread('C:\Documents and Settings\admin\Desktop\Anils
app\Polarization\PNout\outputseq.txt');
                    %read captured waveform
input=zeros(1,length(PNin));
nodat=76;

avg=(max(PNin)-min(PNin))/2;

for i=1:length(PNin) %used to redo the input to match the
simseq from range -1 to 1
    if(PNin(i)>=0.0192144)
        input(i)=1;
    else
        input(i)=0;
    end
end

init=[1,1,1,1,1,1,1,1]; % initial condition for the
registers
pickoff1=5;     %pickoffpoint for PN1
pickoff2=3;     %pickoffpoint for PN2
PN1=PNgen(init,pickoff1);   %generate first PN sequence
PN2=PNgen(init,pickoff2);   %generate second PN sequence

error=10000;      %initialize the bit error to large
maxcorr=0;
ID=0;           %initialize tag ID

for i=1:length(PN1)     %test all possible shift amounts
  PNtemp=simseq(PN1,PN2,i);
  PNtemp=PNtemp(nodat+1:length(PNtemp));
  PNtemp=Upsamp(PNtemp,length(input));
  Xcr=crosscorr(PNtemp,input,length(input)-1);  %computer
cross correlation
  corcoeff=max(Xcr);        %find the maximum correlation
coefficient
    if(corcoeff>maxcorr)    %If it is a better match than
the previous codes
        maxcorr=corcoeff;   %set the new max to this value
```

```
        index=find(Xcr==corcoeff);  %Find the shift amnt
that created this value
        PNused=circshift(PNtemp,[0,index]); %change the
output to match this
        ID=i;   %The shift with highest correlation is the
ID
        error=sum(abs(PNused-PNtemp));
        Xcrout=Xcr;
        PNnoshift=PNtemp;
    end
end

ID/4
subplot(2,1,1); plot(input);
subplot(2,1,2); plot(PNused);
PNout=zeros(1,length(PNused))-1;        %recentering around
0
PNout=PNout+PNused*2;
csvwrite('C:\Documents and Settings\admin\Desktop\Anils
app\Polarization\tag1PN.txt',transpose(PNout));
```

APPENDIX H: PROGRAM USED TO TEST THE CORRECTNESS OF A PN GENERATOR SEQUENCE VS SIMULATION

```
%ouput tests_
%takes two consecutive tests of a given PN gen
%compares it to the theoretical
%mesures their correlation

init=[1,1,1,1,1,1,1,1];
nodat=78;

PN3_r1_in=transpose(csvread('outputseq.txt'));
PN3_r2_in=transpose(csvread('outputseq.txt'));

% PN3_sim=PNCode(8,[8,5],1);
PN3_sim=PNgen(init,5);
PN3_sim=PN3_sim(nodat+1:length(PN3_sim));
PN3_sim_up=upsamp(PN3_sim,length(PN3_r2_in));

PN3_r1_in=PN3_sim_up;


Xcr=crosscorr(PN3_r1_in,PN3_r2_in,length(PN3_r2_in)-1);
corcoeff=max(Xcr);
index=find(Xcr==corcoeff);  %Find the shift amnt that created
this value



PNused=circshift(PN3_r2_in,[0,-index]); %change the output to
match this

subplot(2,1,1); plot(PN3_r1_in);
subplot(2,1,2); plot(PNused);

figure(2); plot(Xcr);
```

APPENDIX H: PROGRAM USED TO TEST THE CLOCK DELAY CIRCUIT

```
%this function reads in a duel clock signal
%and calculates the phase difference between
%the two signals

p=dlmread('C:\Documentsand Settings\admin\Desktop\Anils
app\clockout.txt',',');

clock1in=p(:,2);
clock2in=p(:,3);
%plot some figures of both clock signals
figure(1)
subplot(2,1,1)
plot(clock1in,'r');
subplot(2,1,2)
plot(clock2in,'g');

%plot some figures of both clock signals

% locate the starting trigger of both signals
c1start=min(find(clock1in==1));
c2start=min(find(clock2in==1));

c1temp=find(clock1in==1);
% c1start=c1temp(10);

diff=abs(c1start-c2start);
ID=diff/(10);
ID=round(ID)
bin=dec2bin(ID)
setbin=dec2bin(256-ID-1)
```

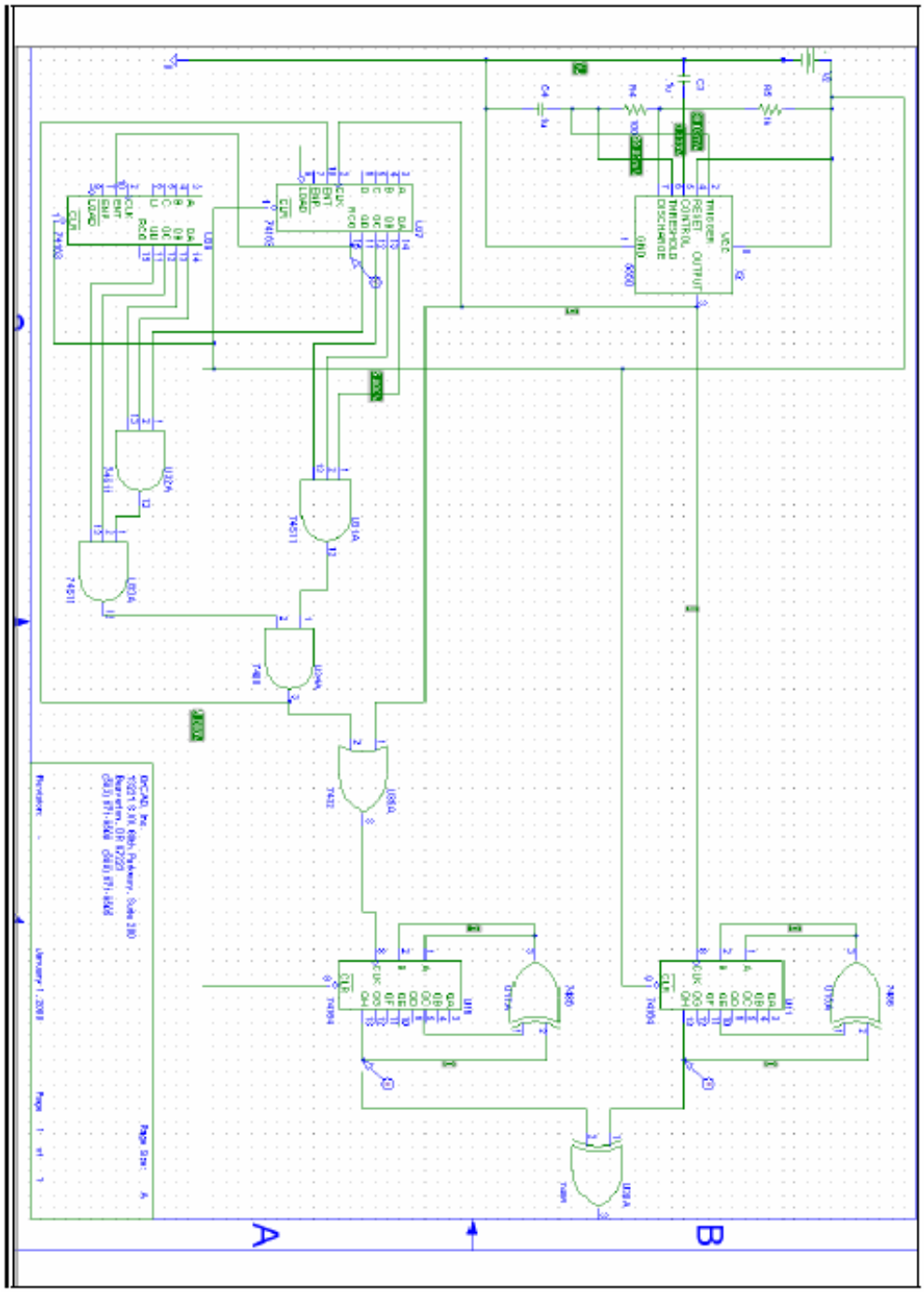
APPENDIX I: PROGRAM USED TO PLOT THE POLAR RSS GRAPHS

```
%Load and plot the data for the 6 cases
%Creates a polar plot of each antennas power as a
function
%of orientation

It1 = csvread ('Ic6t1.txt');
Qt1 = csvread ('Qc6t1.txt');
It2 = csvread ('Ic6t2.txt');
Qt2 = csvread ('Qc6t2.txt');


Pt1 = sqrt(It1.^2 + Qt1.^2);
Pt1flip= [transpose(Pt1),transpose(Pt1(length(Pt1):-
1:1))];

Pt2 = sqrt(It2.^2 + Qt2.^2);
Pt2flip= [transpose(Pt2),transpose(Pt2(length(Pt2):-
1:1))];

theta = 0:10:180;
thetaflip = [theta, theta+180];
thetarad= thetaflip*pi/180;

polar(thetarad,Pt2flip,'r');
hold on
polar(thetarad,Pt1flip,'g');
```

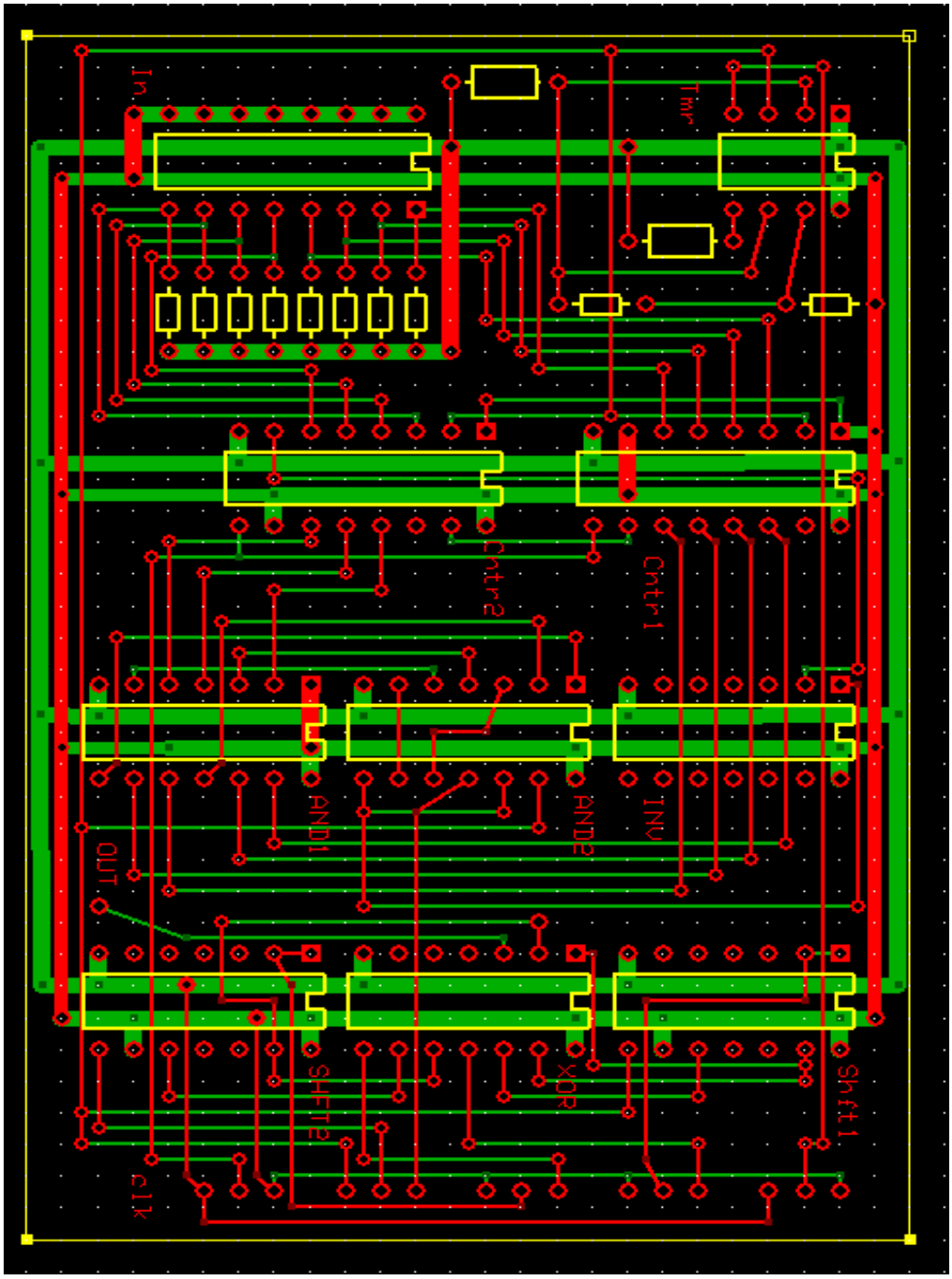
APPENDIX J: PROGRAM USED TO PLOT THE 3D CROSS CORRELATION GRAPHS

```
% Cross correlation generator given different
% Hardware configurations
% Used to find sequences with the least correlation with
% eachother in order to get the most effective anti-
collision.

xvec=[1:254];       %initialize the xvector
yvec=[1:254];       %initialize the yvector
init=[1,1,1,1,1,1,1,1]; %initialize the registers
PN1=PNgen255(init,5);      %generate PN sequences for
this hardware
PN2=PNgen255(init,3);      %generate PN sequences for
this hardware

for i=1:length(xvec)    %toggle shift amount.. (ID1)
    for j=1:length(yvec) %toggle shift amount..(ID2)
        Seq1=simseq(PN1,PN2,i); %Generate the sequence of
ID1
        Seq2=simseq(PN1,PN2,j); %Generate the sequence of
ID2
        xcvec=crosscorr(Seq1,Seq2,length(xvec)-1); %cross
corrilation of
                                                   % each
set of IDs
        maxval=max(xcvec);   % maximum value of the
correlation
        Graph(i,j)=maxval;
    end
end
```

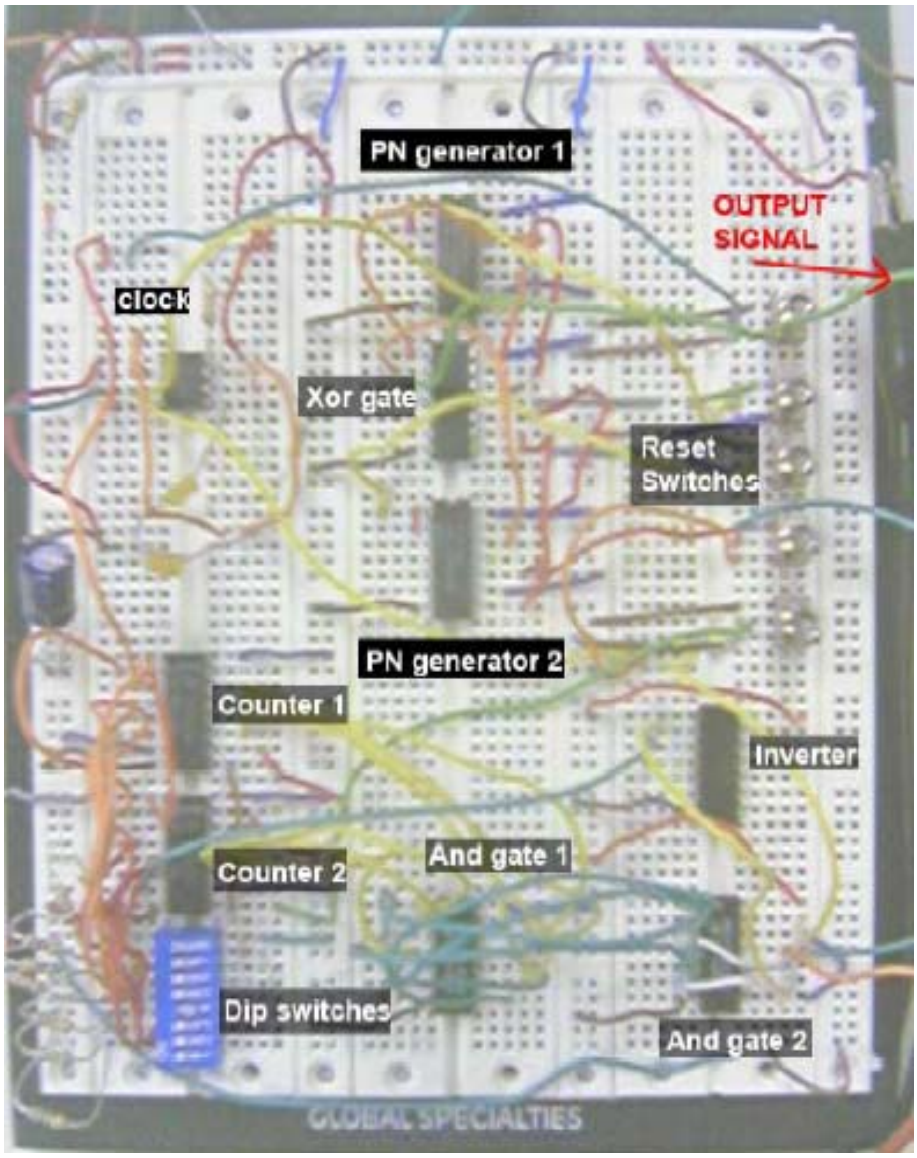
APPENDIX K: TAG SCHEMATIC



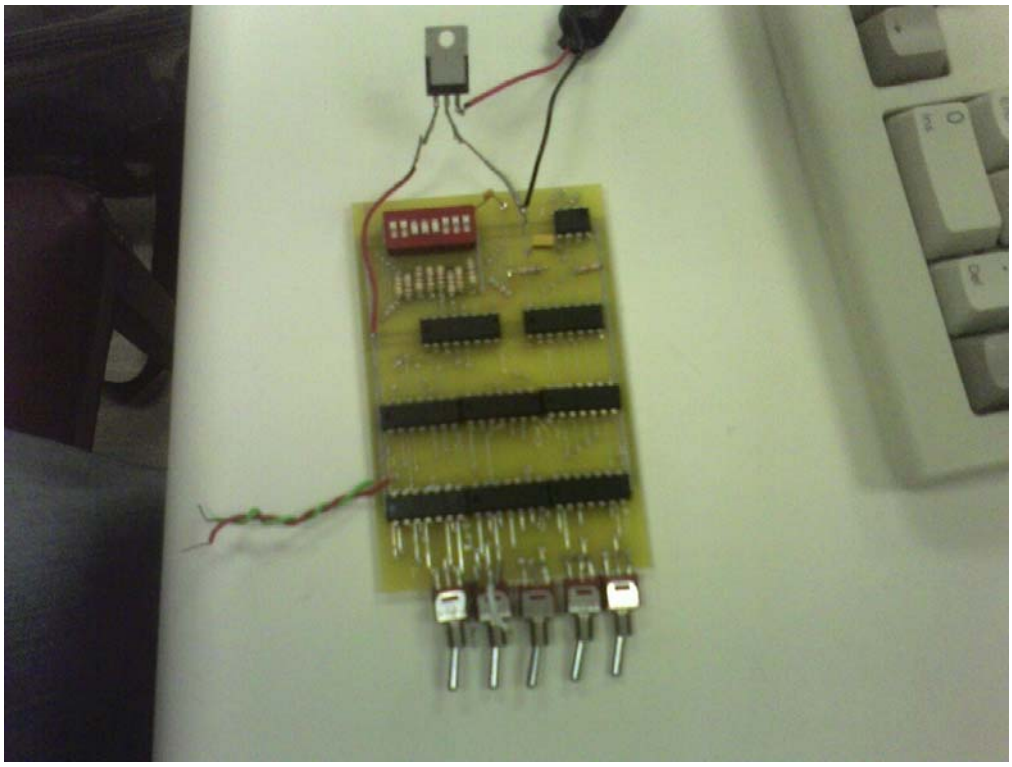
APPENDIX L: TAG LAYOUT

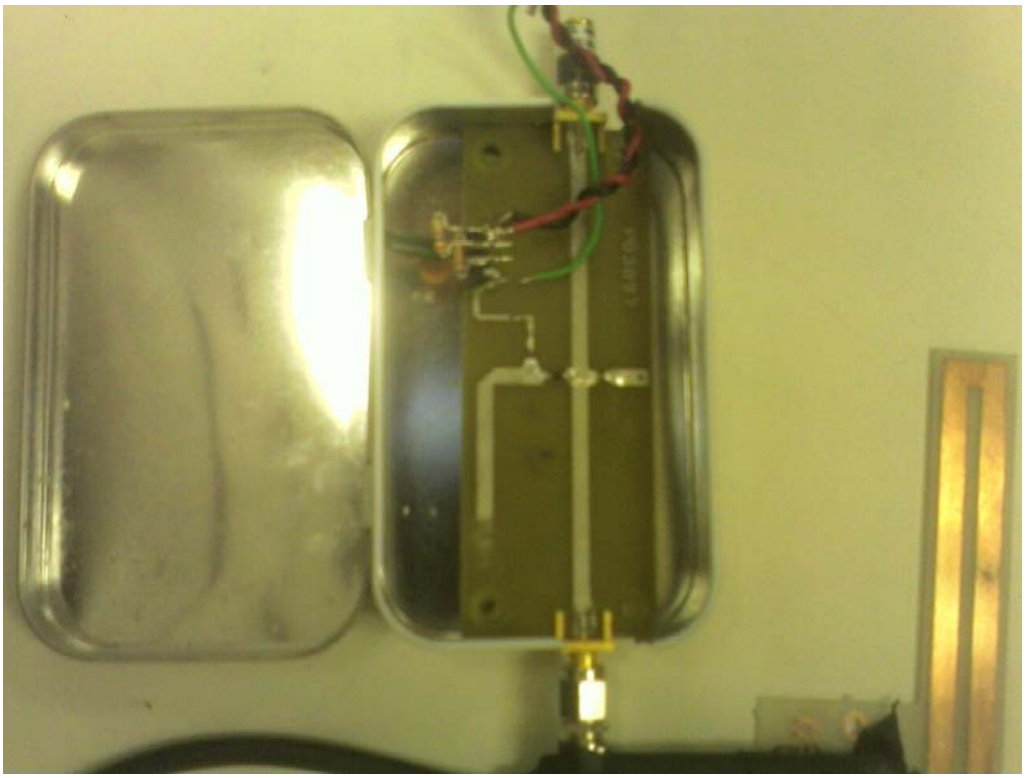


APPENDIX L: FIRST GENERATION TAG

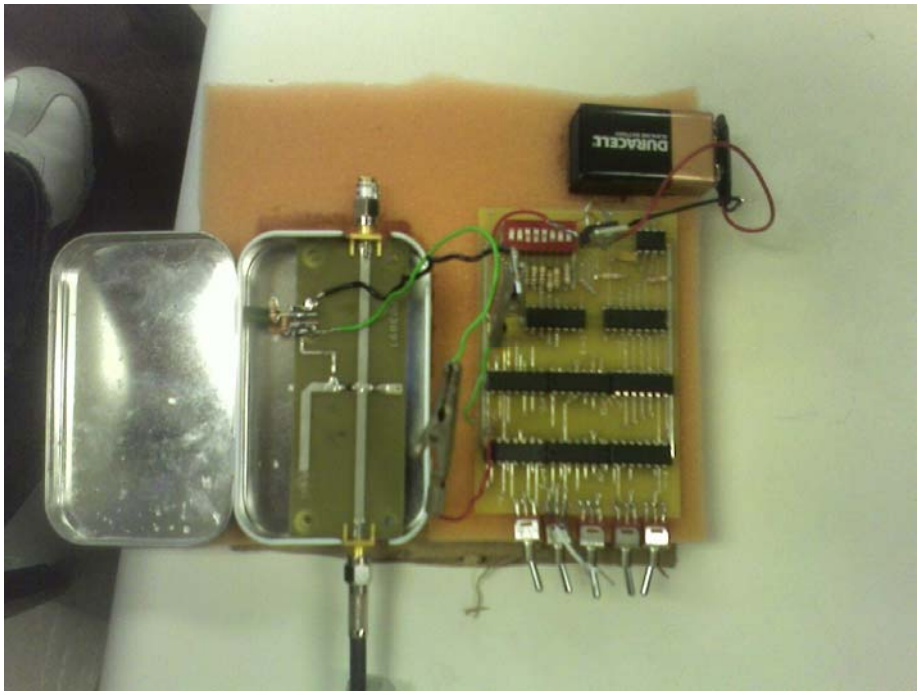


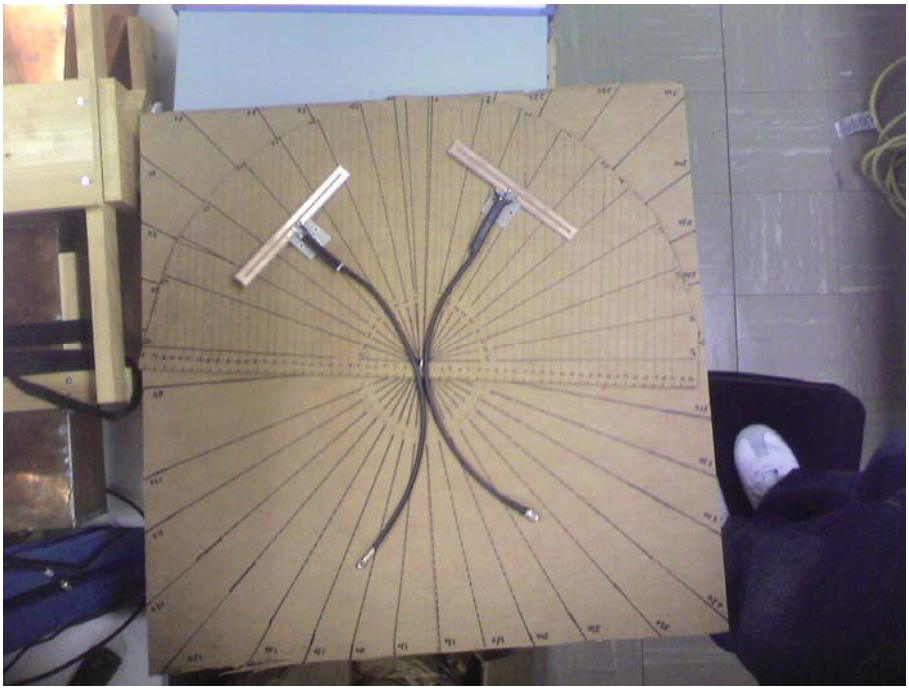
APPENDIX M: SECOND GENERATION TAG





APPENDIX M: ANTENNA MEASUREMENT SETUP





References:

[1] Jerry Landt, *"Shrouds of Time, The History of RFID",* The Association for Automatic Identification and Data Capture Technologies.

[2] Mario Chiesa, Ryan Genz, Franziska Heubler, Kim Mingo, Chris Noessel, Natasha Sopieva, Dave Slocombe, Jason Tester, *"RFID: A Week-Long Survey on the Technology and Its Potential",* Harnessing Technology Project, March 2002

[3] Harry Stockman, "*Communication by Means of Reflected Power*", *Proceedings of the IRE*, pp1196-1204, October 1948.

[4] Griffin, Joshua, "A Radio Assay for the Study of Radio Frequency Tag Antenna Performance", Georgia Institute of Technology. Fall 2005.Technical Report PG-TR-050504-JDG, hjttp://www.propagation.gatech.edu/Archive/PG_TR_050504_JDG/PG_TR_050504_JDG.pdf , June 2006.

[5] Mike Beigel, "Dynamic Performance of Inductive RFID Systems", European Conference on Circuit Theory and Design, Aug. 1999, Stresa, Italy, http://www.beitec.com/articles/dynamic/dynamic1.htm, June 2006

[6] Randy Roberts, "Introduction to Spread Spectrum." *The ABCs of Spread Spectrum -- A Tutorial*. Sept. 2004. SSS online, Inc. http://www.sssmag.com/ss.html, June 2006.

[7] Anonymous, "Wal-Mart RFID Deadline Won't Be Met," Official Board Markets, vol. 81, no. 1, p. 4, 2005.

[8] "Specification for RFID Air Interface", EPCglobal Inc., 31 January 2005, Version 1.0.9, 94 pgs.

[9] Kim Hargraves, Steven Shafer, *"Radio Frequency Identification (RFID) Privacy: The Microsoft Perspective" ,* Workshop on RFID: Applications and Implications for Consumers, June 21, 2004

[10] Donald L. Schilling, Raymond L. Pickholtz , Laurence B. Milstein, *Spread Spectrum Goes Commercial,* IEEE Spectrum, August, 1990

[11] Orfanidis, S.J., Optimum Signal Processing. An Introduction. 2nd Edition, Prentice-Hall, Englewood Cliffs, NJ, 1996.

[12] W. C. Jakes, " A comparison of Specific Space Diversity Techniques for Reduction of Fast Fading in UHF Mobile Radio System," IEEEE Transaction on Vehicular Technology, vol. VT-20, no. 4, pp. 81-91, Nov. 1971

[13] Gregory D. Durgin, "Space-Time Wireless Channels", Prentice Hall, NJ, 2003.

[14] K.V. Seshargiri, Pavel V. Nikitin, Sander F. Lam, "Antenna Design for UHF RFID Tags: A Review and a Practical Application", IEEE Transactions on Antennas and Propagation, Vol 53. NO 12, Dec 2005.

[15] K. Finkenzeller, RFID *Handbook: Radio Frequency Idnetification Fundamentals and Applications,* 2nd ed. Wiley, 2004

[16] R. Bansal, "Coming soon to a Wal-Mart near you," *IEEE Antennas and Propag. Mag.,* vol 45, pp 105-106. Dec 2003

[17] Jibrail W, Ali Wm, "Performance Comparison of PN-CODES For The Acquisition Of DS Spread-Spectrum Signals", *International journal of electronics [0020-7217],* vol 75. 1993, pp 607-625.

[18] Wang TP, "Enhanced binary search with cut-through operation for anti-collision in RFID systems", *IEEE communications letters [1089-7798*], vol. 10, issue 4, 2006, pp 236-238

[19] Narayanan RM, Atanassov K, Stoiljkovic V, Kadambi GR, "Polarization diversity measurements and analysis for antenna configurations at 1800 MHz", *IEEE transactions on antennas and propagation [0018-926X*], 2004, vol.52, issue 7, pp 1795 -1810

[20] Dietrich CB, Dietze K, Nealy JR, Stutzman WL, "Spatial, polarization, and pattern diversity for wireless handheld terminals", *IEEE transactions on antennas and propagation [0018-926X],* 2001, vol.49, issue 9 pp 1271 -1281