



**PERFORMANCE ANALYSIS OF EFFECTIVE RANGE
AND ORIENTATION FOR UHF PASSIVE RFID**

THESIS

Paul N. Roque, First Lieutenant, USAF

AFIT/GCO/ENG/08-06

**DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY**

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GCO/ENG/08-06

**PERFORMANCE ANALYSIS OF EFFECTIVE RANGE
AND ORIENTATION OF PASSIVE UHF RFID**

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Paul N. Roque, BS

First Lieutenant, USAF

March 2008

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Abstract

The purpose of this research is to characterize the performance of UHF passive RFID tags. Factors of importance are the impact of tag orientation and distance from the RFID reader. Within this study, a comprehensive literature review of RFID technology is presented as well as the methodology used for the research. Furthermore, an analysis of RFID tag experiments is discussed and the results reviewed. To accomplish this task, two main objectives have been established as goals for the study. The first objective is to determine an optimum tag orientation within the RFID reader's normal read range. Once the optimum tag orientation is determined, the orientation is used to perform range variation tests. The end goal of these tests is to find the maximum range at which the tags are readable under normal conditions using standard equipment.

Grasping an idea of RFID tag boundaries contributes to the security and privacy of the technology. This is extremely important as RFID tags are becoming the logistical tool of choice for Department of Defense (DoD) supply chains. This fundamental study creates a foundation that may support both offensive and defensive oriented research. By understanding tag weaknesses and strengths, users of the technology can make sound decisions that lead to the protection of valuable information and assets.

Acknowledgments

I would like to express a tremendous appreciation to my faculty advisor, Dr Richard Raines, for his patience and guidance throughout the course of my academics and research. His positive outlook and insight kept me on track. I would, also, like to thank faculty member, Dr Michael Temple for his support and pro insight on the graduate experience. Gratitude is also given to Capt Ryan Thomas for his flexibility and understanding in this effort. I would like to share many thanks to my family, for their love and support to help me get where I am today. Most importantly, I want to thank my wife. She has been the most understanding and supportive force to help me get through my AFIT career. She's been wonderful and has helped me overcome many obstacles. She will always have my love and thanks.

Paul N. Roque

Table of Contents

	Page
Abstract.....	iv
Acknowledgements.....	vi
Table of Contents.....	viii
List of Figures.....	viii
List of Tables.....	ivx
List of Equations.....	x
I. Introduction.....	1
1.1 Background.....	1
1.2 Research Goals.....	2
1.2.1 Optimum Orientation.....	2
1.2.2 Readability at Range.....	2
1.2.3 Future Enhancements.....	3
1.3 Preview.....	3
II. Literature Review.....	4
2.1 Chapter Overview.....	4
2.2 RFID System.....	4
2.3 RFID Tags.....	5
2.3.1 Form Factor.....	6
2.3.2 Power Source.....	8
2.3.3 Air Interface.....	9
2.3.3.1 Operating Frequencies.....	9
2.3.3.2 Encoding.....	11
2.3.3.3 Coupling.....	11
2.3.4 RFID Memory.....	13
2.3.5 RFID Standards.....	14
2.3.6 Tag Protocol.....	17
2.4 Readers.....	20
2.5 Middleware.....	22
2.6 RFID Security.....	23
2.7 Chapter Summary.....	24

III. Methodology	26
3.1 Introduction	26
3.2 Problem Definition	26
3.3 Research Objectives	267
3.3.1 System Boundaries	268
3.3.2 System Services	268
3.3.3 Performance Metrics	29
3.3.4 Parameters	29
3.3.5 Factors	30
3.4 Evaluation Technique	31
3.5 Experimental Design	32
3.6 Result Analysis and Interpretation	34
3.7 Summary	35
IV. Analysis and Results	36
4.1 Introduction	36
4.2 Tag Readability	36
4.2.1 Tag Orientation	37
4.2.2 Computation of Effects	38
4.2.3 Analysis of Variance	40
4.3 Signal Interference	41
4.4 Summary	48
V. Conclusions and Recommendations	50
5.1 Introduction	50
5.2 Research Objectives	50
5.2.1 Orientation	52
5.2.2 Range	51
5.3 Future Research	51
5.4 Summary	52
Bibliography	52

List of Figures

Figure	Page
1. RFID Disc Tag [13]	6
2. Glass RFID Transponder [14].....	7
3. RFID Key Fob [15].....	7
4. Near-Field Communication Using Inductive Coupling [4].....	12
5. Far-Field Communication via Backscattering [4].....	13
6. Reader State Diagram Using Slotted Aloha [1].....	19
7. Tag State Diagram in Slotted Aloha [1].....	20
8. Gen2 Protocol State Diagram [1].....	21
9. Tag Orientations.....	38
10. Readability at Distance.....	42
11. Second Ranged Experiment.....	43
12. Geometry of Signal Reflection.....	44

List of Tables

Table	Page
1. RFID Frequencies and Associated Read Ranges [10].....	10
2. EPCglobal Standards [1].....	15
3. ISO Standards [1].....	16
4. Frame for UHF Class1 Gen 2 Tag Response [11].....	18
5. Readability Values (Reads/Sec) for Experiment 1.....	37
6. Computation of Effects for Orientation Experiment.....	39
7. 90% Confidence Intervals for Orientation Experiment.....	40
8. ANOVA for Experiment 1.....	40
9. ANOVA for Experiment 1 Including the 5 m Range.....	41
10. Average Readability of Tags at Distance.....	42
11. Theoretical Destructive Interference Points.....	48

List of Equations

Equation	Page
1. Friis Equation.....	32
2. Confidence Interval Equation.....	33
3. Confidence Interval Equation.....	33
4. Path Loss Equation.....	41
5. Destructive Interference Equation.....	44
6. Geometrical Proof of Angle of Incidence and Reflection.....	45
7 – 10. Solving Ground Length from Reader to Point of Reflection.....	45
11 – 14. Solving Ground Length from Point of Reflection to Tag.....	46
15. Distance from Reader to Point of Reflection.....	46
16. Distance from Point of Reflection to Tag.....	46
17. Distance from Reader to Tag.....	46
18-19. Incorporating Equations 4 and 5.....	47
20. Distance of Destructive Interference.....	47

PERFORMANCE ANALYSIS OF EFFECTIVE RANGE AND ORIENTATION OF UHF PASSIVE RFID

I. Introduction

1.1 Background

Radio Frequency Identification (RFID) systems are communication devices used for tracking and, as the name implies, identification of various objects. More commonly found in the logistics world, these devices are making their way into the commercial world and are even finding applications in medicine and retail. When new technology is introduced into mainstream operations, some of the highest concerns are the security and privacy of the product. Unfortunately, many times these new products are driven by cost and pure functionality with little to no security aspects taken into consideration. However, as the technology becomes more popular, functional gaps and holes are discovered and many times exploited. Even though it is too late to build the system on a more secure platform, understanding the unadvertised characteristics and capabilities of a system can go a long way to increasing its reliability as a secure system.

RFID belongs in the category of systems that were developed and initially designed with little to no security aspects taken into consideration. That being said, efforts are being made to create RFID tags and readers with encryption and other modules to make the product more secure. To aid in this effort, a better understanding of these devices is required.

1.2 Research Goals

The overall research goal is to characterize RFID readability in relation to two operational factors, orientation and range. Having a firm grasp of the effects of these factors on the technology allows one to know the boundaries and capabilities of RFID. With this knowledge, one can build attacks and defenses that take advantage of these characteristics. This research examines both factors independently and attempts to complete the following objectives

1.2.1 Optimum Orientation

RFID relies on radio signals for communication. As such, there is no need for a direct line-of-sight within the system. This does not mean that performance is equal among all tag orientations within the reader field. The first objective of this research is to determine an optimum orientation for tags in the RFID system and to gain an understanding of how much of a factor it plays into tag readability.

1.2.2 Readability at Range

The second objective takes the optimum orientation into account and attempts to characterize how RFID performs outside of normal operating boundaries. A determination of tag readability is documented and factors contributing to or detracting from performance are discussed. Max read range is of great interest for this part of the study. If RFID systems under normal configurations and settings can be read at ranges far beyond advertised specification, this creates potential security gaps that need to be addressed and resolved.

1.2.3 Future Enhancements

As mentioned above, once the unadvertised characteristics of RFID systems are determined, this leaves the possibility of future research into this subject open to explore a multitude of defenses and exploits. The baseline created by this research will hopefully build upon RFID capabilities and contribute to future enhancements.

1.3 Preview

Chapter 2 provides an overview of RFID systems, to include a discussion on tags, readers and their various uses. Background into how the tags communicate is provided, as well as case studies that highlight how RFID has been exploited. Chapter 3 details the methodology used to address the objectives of this research. Some theoretical analysis is provided as well as a discussion into the tools used for analysis. Chapter 4 provides experiments results and analysis, showing the effectiveness to which the objectives were completed. Finally, Chapter 5 summarizes the research findings and discusses possible research that could stem from this study.

II. Literature Review

2.1 Chapter Overview

This chapter covers the passive RFID Tag system, to include its hardware and software components. Additionally, the chapter describes the protocols involved to prevent collision among multiple tags. The final portion of the chapter describes RFID vulnerabilities that have been explored and scenarios where those vulnerabilities could possibly be implemented.

2.2 RFID System

The RFID system is composed of three main components, the RFID tag, the tag reader and the middleware. The RFID tag, or transponder, is the component that is tracked and contains data of value to the user. The reader, or interrogator, transmits the RF waves that initialize communication with RFID tags and extract data from the waves emitted back from the tags. The final component to the system is the middleware. Middleware includes all the software that connects the RFID system to the intended application.

The purpose of an RFID system is to identify an object and retrieve data from the object that is later used for a particular application. The objects have an RFID tag attached or implanted in them. These tags come in various shapes and sizes, but a typical tag is comparable to a credit card. RFID tags can be passive, semi-active, or active. In the RFID world, passive devices rely on the RF energy emitted by the reader to power an on-board antenna and circuitry. Semi-active devices have an on-board power source that is used for communications purposes. Active devices use an on-board power source for

antenna and circuitry operations. After receiving a signal from an RFID reader, the tags respond to the reader with data. Readers can take the form of a handheld gun-type device or take the form of a portal that can be setup around the conveyor of a packing and shipping company. When the reader receives the data from the tag it sends it to the middleware. The middleware keeps track and processes the collected data and presents the data in a form that is usable.

RFID tag applications are typically found in logistics, however, they are slowly finding their way into commercial applications and have also shown practical use where it is necessary to track or identify an object. RFID tags are being used as bar code replacements due to its flexibility in not having to be in direct line of sight of the RFID reader. This quality has influenced major companies and even the DoD to further develop and investigate this technology for logistical operations. The relatively small and unobtrusive shapes of tags have found usefulness in tracking species of interest such as whales or birds. RFID technology is also being used in security applications in the form of proximity cards for building entry or identification. Retail is finding use in RFID tags as a convenient way to process customer purchases and even collect data on consumer tastes, however, this has raised privacy issues. Malicious entities can also track RFID tags and use their information to select targets for nefarious deeds. More on this topic will be covered later in this chapter.

2.3 RFID Tags

The RFID tags, or transponders, are small electronic devices that relay data to readers via an on-board antenna. The two most fundamental capabilities of a tag are its ability to

share information over RF and the ability to tether it to an item. In addition, tags may have the capability to be permanently disabled, written to, or have the processing power to follow anti-collision protocols and implement basic encryption [1].

2.3.2 Form Factor

RFID tags take on various shapes and sizes dependent on their use and operational environment. The passive tag is generally smaller in shape and is made of materials that are easy to mass produce at a low cost. One of the more common transponders takes the form of a disc about the size of a coin. These are generally made out of durable plastic and usually have a hole in the center for fasteners.

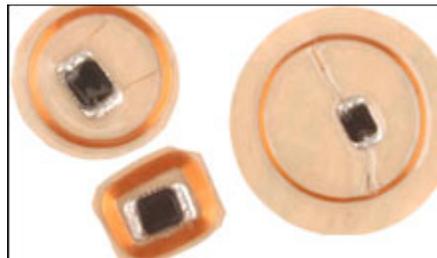


Figure 1. RFID Disc Tag [13]

Glass transponders have also been developed. These types of transponders are usually injected under the skin of an animal for tracking purposes and are 12-32 mm in length. The glass tube transponders usually contain a coil wrapped around a ferrite rod that is connected to a capacitor leading to a microchip [2].



Figure 2. Glass RFID Transponder [14]

Another popular type of housing for RFIDs is plastic packages similar to those found on car keys for electronic immobilization systems. This type of housing is very rugged and is meant to withstand heavy mechanical vibrations.

RFID tags have also taken the shape of keys and key fobs. The Exxon Mobil Speedpass is a popular version of the key fob. These keys are typically implemented for use in applications where security is required.



Figure 3. RFID Key Fob [15]

RFID systems also take advantage of the contactless smart card form factor. Similar in size to credit cards, these RFID systems may have a relatively longer read

range due to a potentially larger coil area. These have been used increasingly in building access or for use in commerce.

In the logistics world, the smart label has been the form factor of choice. Usually paper thin, these transponders are etched onto plastic foil, then laminated and back coated with adhesive [2]. These labels are the easiest to apply to pallets and crates for shipping. They are now finding use in applications such as luggage tracking, or wherever bar codes were used to track items.

With the push to adopt RFID technology, it has found itself in a variety shapes dependent on its intended application. Tags have even been created as small as 0.4mm by 0.4mm with a 0.06mm thickness [3].

2.3.2 Power Source

Tags can be classified by how they generate power for operation. The three different classifications include passive, semi-passive and active. The method by which tags are powered depends on factors such as ideal shelf-life, operational environment and desired read ranges.

Passive tags do not have an on-board power supply, but rely on the electromagnetic field generated by the interrogator. The energy from the field is rectified and properly amplified to provide power for the internal circuits. The methods by which this energy is harnessed is explained later in a discussion of near-field and far-field coupling. Research in the remaining chapters focus on passive tags due to their increasing popularity in DoD logistical applications [4].

Semi-passive tags have an on-board power supply. However, these transponders still rely on the interrogator RF fields to supply power for communication. The on-board battery is reserved for embedded circuit functions. This presents both an advantage and disadvantage for semi-passive tags. Since the on-board circuitry relies solely on the battery, power from the RF field can be concentrated on communications, thus boosting read ranges. However, the drawback is added cost and they may not be practical for mass distribution to match the scale of passive RFID technology. Also, longevity of the semi-passive tag is limited to the life-span of the battery, typically five to ten years [1,9].

Active tags rely solely on an on-board battery for communications, processing, and all other tag functions. This type of tag may have the longest possible read range depending on how much power it dedicates to communication. A drawback for the active tag is its short life-span of one to five years due to a limited power supply. Applications that require an RFID tag to perform measurements or calculations without the presence of an interrogator look to this type of tag given its flexibility [1,9].

2.3.3 Air Interface

RFID tags can be classified by communication methods used between the RFID tag and reader. RFID operating frequencies are first described, and various communications modes discussed. Finally, tag coupling methods for extracting energy from the RF field are presented.

2.3.3.1 Operating Frequencies

RFID tags can operate, communicate and interact at various frequency ranges across the spectrum. However, as with any device that utilizes radio waves, the

frequencies, operating power and spectrum are regulated by a governing body. For example, in the US the 902 MHz to 928 MHz frequency band is used for tags operating at the ultra-high frequency (UHF) spectrum. This particular range is within the Industrial Scientific Medical (ISM) range, so interference with other technologies is a concern. Furthermore, to prevent spectrum monopoly, the Federal Communications Commission instituted that frequency-hopping be used for RFID technology operating in this range to compensate for the limited bandwidth [1,4].

Regulations aside, RFID tags are capable of operating across the spectrum to include low frequency (LF), high frequency (HF), the previously mentioned UHF, and microwave frequencies. Depending on the desired read range, certain frequencies are more appropriate. With the exception of the microwave frequencies, the greater the desired read range, the higher the frequency required as shown in Table 1.

Table 1. RFID Frequencies and Associated Read Ranges [10]

Frequency	Typical read range
Low-Frequency (LF) 124 kHz – 135 kHz	Up to half a meter
High-Frequency (HF) 13.56 Mhz	Up to 1 meter
Ultra High-Frequency (UHF) 860 MHz – 960 MHz	4 to 5 meters
Microwave 2.45 GHz	Up to 1 meter

The environment also plays a role in determining a suitable operating range. Certain frequencies propagate better through different mediums, such as the case with LF being more suited for aquatic applications [1]. Tags for whale tracking take advantage of the fact that waves travel further along aquatic rather than atmospheric paths.

2.3.3.2 Encoding

RFID transponders can be classified by the way they transfer data to and from interrogators. This data transfer can be classified into two methods, half/full duplex and sequential. These methods describe when and who talks in the communication process. For the half/full duplex schemes, data transfer is constant, regardless of whether or not communication occurs simultaneously (as in full duplex) or alternates (as in half duplex). Sequential systems communicate using with pulses data transfer occurring between power transmissions to the tag [2].

RFID tags can also be broken classified according to how they represent analog signals. Several encoding methods have been adopted for the tags, including schemes from previous technology such as the Universal Asynchronous Receiver/Transmitter (UART) chip. Some of the more popular schemes include Biphase Manchester encoding, EPC Miller encoding and FSK subcarrier encoding [1].

2.3.3.3 Coupling

Passive RFID tags do not have an on-board power supply and rely coupling to convert the RF waves from an interrogator into useable energy. There are different coupling techniques used in passive RFID technology, indicating near-field and far-field.

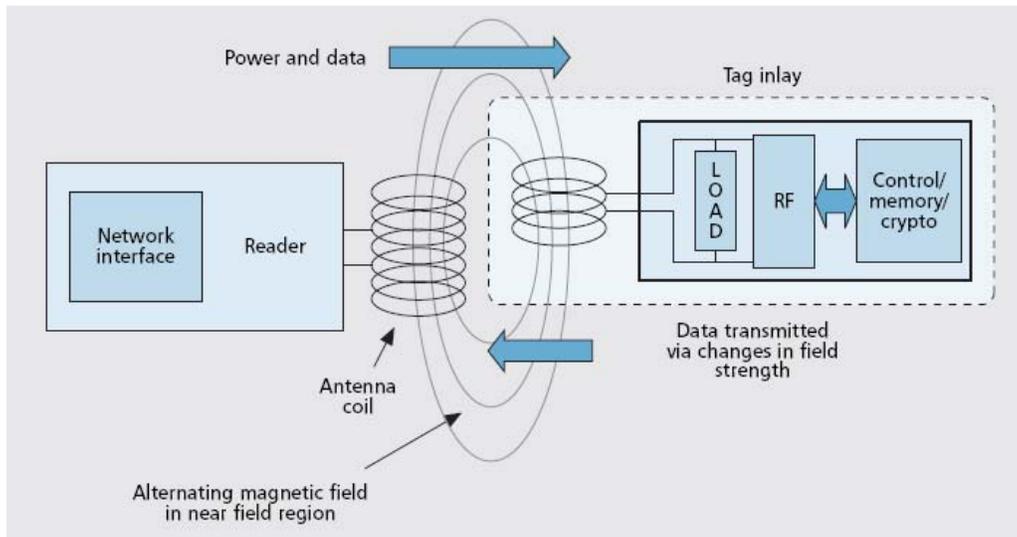


Figure 4. Near-Field Communication Using Inductive Coupling [4]

Near-field coupling, shown in Figure 4, relies on induction to generate energy for the circuit. Depending on the antenna, near-field systems use a field (electric for a dipole or magnetic for a coil) to produce a current strong enough to power the tag [4]. Distinguishable signals are produced from the tag to the reader by varying the load on the antenna. Tags using this coupling typically operate at the lower frequencies of 128 kHz and 13.56 MHz due to the boundary between near-field and far-field being inversely proportional to frequency [4,5].

Far-field coupling, as shown in Figure 5, relies on an impedance mismatch between the tag's antennas to create energy. This "backscattering" uses the reflected energy to transfer data back to the reader. To vary the reflected signal, load modulation is used in the form of a resistor placed between the tags' antennas. These tags usually operate in the UHF or microwave band. Such high frequency operation is attributed to

EM field's inverse proportionality to the distance between the tag and reader [4]. With this higher frequency, longer read ranges into the tens of meters are possible [10].

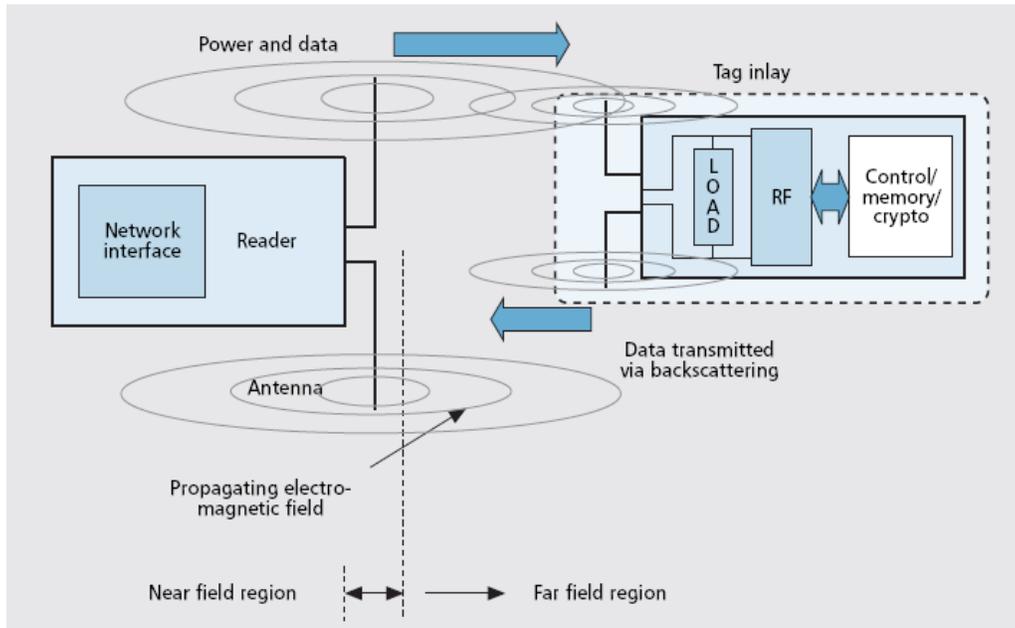


Figure 5. Far-Field Communication via-Backscattering [4]

2.3.4 *RFID Memory*

RFID tags can also be defined by the capability required for a specific application. For example, tags can be designed to fulfill a simple on/off task using a single bit memory. Tags are also capable of performing more complicated tasks such as encryption or authentication.

The most basic tag is the 1-bit tag. This type of tag responds to an interrogator with a simple yes or no. These tags dominated the market early on given their simplicity

and lower cost. Also known as Electronic Article Surveillance (EAS) tags, they can be found in the retail world as anti-theft devices.

On the opposite end of the capacity realm, tags can include microprocessors and integrated circuits. These tags are limited by physical size and cost. The present cost is five cents for a typical UHF passive tag. Current technology only gives practical tags the capability to contain kilobits worth of data. To produce tags with more memory or feature stronger encryption functions, there is a trade-off between cost and size [6].

2.3.5 RFID Standards

Like most communication technologies, RFID tag designs comply with industry standards. In the RFID world, the two major governing bodies are Electronic Production Code Global (EPCglobal) and the International Standards Organization (ISO). These two organizations have standards for tags based upon factors such as air interface, read/write capability and frequency range. Table 2 and Table 3 provide representative standards from each organization.

EPCglobal is one of the predominant developers of standards for RFID tags. EPC has created a class system that allows developers to create tags based on contents, encoding methods and air interfaces [1].

Table 2. EPCglobal Standards [1]

Class	Description
Class 0	Passive, read-only
Class 0+	Passive, write-once but using Class 0 protocols
Class I	Passive, write-once
Class II	Passive, write-once with extras such as encryption
Class III	Rewritable, semi-passive, integrated sensors
Class IV	Rewritable, active, “two-way” tags that can talk to other tags
Class V	Can power and read Class I, II, and III tags and read class IV and V tags, as well as acting as Class IV tags themselves

Along with the classes, EPCglobal has created standards for advances in tag technology in the form of generations. For example, Class II tags are passive tags that can be written to and have the capability for encryption. Class I Generation 2 (Gen 2) tags offer a longer password and cyclic redundancy check (CRC) among other things. A perk in having industry standards is the mandate of key features. EPC tags must be able to be killed in addition to support for CRC [1]

Table 3. ISO Standards [1]

Standard	Title	Description
18000-1	Generic Parameters for the Air Interface for Globally Accepted Frequencies	Principles and architecture for an RFID standard
18000-2	Parameters for Air interface Communications below 135 kHz	LF, two tag types, optional anti-collision, passive, inductive coupling
18000-3	Parameters for Air interface Communications at 13.56 MHz	HF, two modes: 1. 105.94 kbps from tag to reader 2. 423.75 kbps from tag to reader, passive, both use inductive coupling, FDX
18000-4	Parameters for Air interface Communications at 2.45 GHz	Microwave: passive and semi-passive, backscatter, HDX
18000-5	Withdrawn	Withdrawn (5.8 GHz)
18000-6	Parameters for Air Interface Communications at 860 to 930 MHz	UHF, three types: 1. pulse interval encoding, aloha anti-collision 2. Manchester encoding, Binary Tree anti-collision, 3. EPC Gen2 passive backscatter, HDX
18000-7	Parameters for Air Interface Communications at 433 MHz	UHF, long range Read/write, active, HDX

The other industry standard developer, ISO, has actually been around longer than EPC. As such, EPC does submit its standards to ISO for approval. These organizations do not conflict with each other. Rather, they cover different aspects of RFID. The ISO focuses on standards for data transfer and is more concerned with the air-interface and RFID applications. EPC has a broader approach and provides standards for how an entire RFID system should operate. The ISO 18000 series covers RFID tags [1].

2.3.6 Tag Protocol

The air interface of RFID tags pertains to the data-link layer of the open systems interconnection (OSI) model for these devices. Tags communicate through the air interface so it's important understand this level of protocol. Of note are how the tags store data and the more complex procedures that cannot function without the air interface, such as singulation and anti-collision. Singulation is the process that an RFID reader follows to uniquely identify a tag among many within its reading range. This process, along with anti-collision protocol, ensure tags do not communicate with the reader simultaneously, essentially jamming transmissions.

Using the EPCglobal standards, the most basic passive UHF tag divides its data into three different sections: CRC, EPC and Password. The CRC is used for data verification to ensure that data received at the reader matches data sent by the tag. The EPC portion of the tag contains unique identification information. As seen in Table 4, this identification portion itself is split into three different layers to address the various ways to identify an object. The first way is the tag's pure identity, defined by an abstract name/number. The second layer addresses how that pure identity is encoded into a

scheme that is known to others, such as the bar code scheme. The final identification layer is the physical representation of the encoded information that is written into the tag’s memory [1].

Table 4. Frame for UHF Class 1 Gen 2 Tag Response [11]

	Header	RN	CRC-16
# of bits	1	16	16
Description	0	Handle, EPC	

The password portion of the tag’s memory contains pertinent information that allows a tag to be accessed if password protected. This section also contains the “kill code” for tags. When a tag is killed, it is permanently disabled and can no longer transmit or receive data.

The air interface is primarily used for anti-collision when there are multiple tags within read range of an interrogator. The majority of these procedures for passive tags utilize protocols where the reader initializes the communication session. This makes sense because the tags rely on waves from the reader for power. For EPC gen2 tags and ISO18000-6 type tags, a variation of Slotted Aloha is used for communication between tag and reader [1].

Slotted Aloha is a Reader Talk First (RTF) protocol that begins with the reader energizing tags through RF fields and sending requests for identification as shown in Figure 6. An improvement over regular Aloha, the slotted version scales well with a high

amount of tags, adding singularity to a good anti-collision protocol. In this case, singularity is the process of organizing a group of tags into a serial entity for easy processing. Once energized, the tags broadcast their ID in intervals only at the beginning of particular time slots, rather than randomly. The process, shown in Figure 6, illustrates the tag waiting for its time slot before sending the requested information. This allows the reader a better chance to receive a clear signal from a tag as well as account for new tags in a more organized way. The slots for transmission are determined during the REQUEST phase of communication. The reader broadcasts available slots and the tag randomly chooses a slot and broadcasts during that time. If there are no collisions in that slot, the reader enters a SELECT phase and associates the ID of the tag with the particular time slot. The reader then enters the READ phase where data is exchanged with the tag [1].

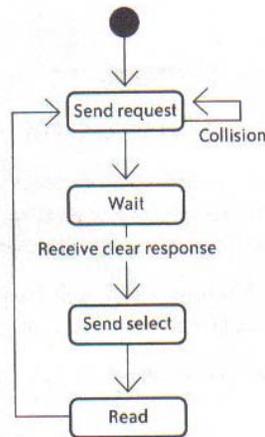


Figure 6. Reader state diagram using Slotted Aloha [1].

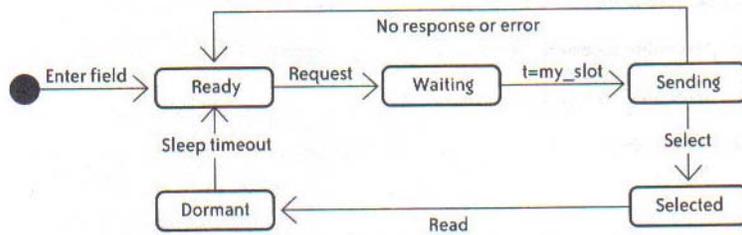


Figure 7. Tag state diagram in Slotted Aloha [1].

2.4 RFID Readers

RFID readers have several functions in the overall RFID system. One of the most important reader functions is to supply power to passive tags to enable a communication session between the two. Once a connection is setup there are key reader operations responsibilities.

To keep track of multiple tags, readers create an *inventory* of the tags within its read space. With the use of singulation protocols such as Slotted Aloha, the reader is able to identify each unique tag and gather its EPC memory contents. Inventory is done through a series of commands including *query*, *ack* and *nak*. These commands have the purpose of directing a tag through an identification and session creating/ending process [1,6].

The reader is also granted *access* to the tag's memory. This access pertains to read/write privileges to the tag's memory. Aside from basic read/write functions, the abilities to kill or lock a tag are included in access operations. With these commands, tags are brought through various stages of operation. Figure 8 outlines the states that a tag will

immediate contact with the tag. Some readers have two antennas for transmitting and receiving operations. In a conveyor situation, placement of the antennas does matter for better tracking of items. Typically, the desired position of the receiving antenna is further down the conveyor where it can take in the backscatter from tags that have been pinged with energy from the transmitting antenna [1].

The controller portion of the reader is responsible for processing the signals taken from the antenna. Responses to tags entering the reader space are also handled by this component. It also has the important job of determining whether an event of interest has occurred and should be sent to the network interface for later processing within the middleware [1].

The network interface is the link between the reader and the user interface. In the past, this was achieved through a serial connection. However, as technology improves and RFID becomes more common place, support for other interfaces such as Ethernet and Bluetooth can be expected [1].

2.5 Middleware

Middleware of the RFID infrastructure comes into play after events are generated via certain tag/reader events and that data is stored in tracking software. The main advantage of middleware is that it organizes thousands of into a user friendly format. Middleware typically follows a logical architecture such as EPCglobal's Application Level Events (ALE) specification. These architectures provide a structure for information flow to include how events originate, filtering data elements according to scenario, and data modeling [1].

2.6 RFID Security

The RFID system is a target rich environment. Potential targets for exploitation can be found in all steps of the system. Everything from the underlying database, to the business transactions at Point of Sale (POS) is vulnerable to manipulation. Identifying attack vectors has been a challenge for security analysts as RFID technology itself, has been used as a security measure such as smart cards. Several methods for attacking RFID systems include RF manipulation, spoofing, malicious insertion attacks, replay attacks, denial of service or tag data manipulation [8].

In 2003, a team from Johns Hopkins University was able to reverse engineer the Exxon Mobil SpeedPass. The SpeedPass is a key fob type RFID tag that uses an encrypted 40-bit key and a proprietary encryption algorithm developed at Texas Instruments. The fact that the algorithm is private is not a good practice. History often has shown that when systems are not subjected to honest peer review, they have fail when later exposed to the public. The team approached the SpeedPass by first using a “black box” technique to break the algorithm. They observed outputs to certain controlled algorithm inputs to the algorithm and began to uncover the encryption used by the tags. Once they discovered the algorithm, the team began to brute force keys for the tag with the use of Field Programmable Gate Arrays (FPGA). With the use of two captured challenge/response pairs, they were able to recover a SpeedPass key and have the process streamlined in under an hour. This attack was attributed to the weak encryption algorithm as well as the relatively small key size used in the SpeedPass [8].

Man in the Middle (MIM) and cloning attacks have been successful with RFID technology mostly because of the tags' small size and low cost. Proximity cards have been shown to possess these vulnerabilities as well. The majority of these cards, which are used for access control, respond to readers in their vicinity. If the card location is known on a person's body, high gain antennas can be used to solicit a response. In 2003, Jonathan Westhues was successful in reverse engineering and reproducing proximity cards. He did this by analyzing signals that were emitted from energized cards and developed a way to determine whether 1s or 0s were being transmitted to access controllers. From this information, he was able to develop a device that cloned access cards capable of successfully replicating the Motorola flexpass system [8].

RFID devices have also spawned alerts in the privacy world as this technology is being adapted into retail items and even government issued documents. If such devices are not secured, a potential thief could equip a portable RFID reader, walk into a high traffic area and have access to a wealth of information on potential targets. This could lead to all types of scenarios involving identity theft or explosive devices set to detonate when in the presence of an American passport. Along with privacy risks, unsecure RFID tags in retail business are an invitation for malicious entities to alter, or prematurely kill the EPC value on goods [8].

2.7 Chapter Summary

This chapter covered the passive RFID Tag system, to include its hardware and software components. Additionally, the chapter described the protocols involved to prevent collision among multiple tags. The final portion of the chapter described some

RFID vulnerabilities that have been explored and scenarios where those vulnerabilities have been implemented.

III. Methodology

3.1 Introduction

This chapter present the problem definition, objectives to be accomplished, and the evaluation technique to reach the objectives. First, the problem definition details the questions to be answered and takes into consideration the research applications. Second, the objectives are stated and the limiting factors and performance metrics involved are discussed. Finally, the evaluation technique and experimental design are explained.

3.2 Problem Definition

At some point, RFID devices may be heavily relied upon for tracking and logistics functions within the Armed Forces. RFID provides advantages over traditional barcode systems that make RFID an attractive alternative. As RFID technology finds increased use in military and defense applications, the need to understand its abilities and limitations is important. As with all communications devices, the security and privacy of transmissions is always a concern and should be taken into account.

To attain a measure of the security for communications devices, the likelihood of intercepting transmissions needs to be evaluated. At a more fundamental level, the RFID read ranges are of significant importance. The greater the read range, the easier it would be for an outside entity to intercept the signals. Security of RFID devices can be improved through an understanding of the reception boundaries. A false sense of security can lead to unauthorized access to sensitive information. Advertised capabilities should be evaluated to define the true operation space.

The limited power created by the tag's inductive antenna dictates the RFID read range. Passive UHF RFID read ranges are typically up to 10 m. This is the advertised (IEEE specification data) read range for ensured reliable communication. However, it cannot be assumed that RFID tag signals cannot exceed this specification under normal conditions using standard equipment. This is investigated in the context of this research.

3.3 Research Objectives

This research focuses on two main objectives:

1. Determining the optimum RFID tag orientation for open-air reception using a commonly used antenna configuration.
2. Determining the maximum range at which an RFID tag can be successfully identified using standard equipment and optimum tag orientation.

The first objective focuses on tag orientation and its readability. Tag orientation may significantly boost or diminish read rate. It is important to attain an accurate picture of the multi-dimensional operating space to determine potential limitations on tag placement around the antennas. This will improve efficiency for logistic operations utilizing RFID systems.

The second objective evaluates the actual read range of RFID tags using the standard configuration. The range of the tag backscatter beyond typical read ranges is evaluated. This contributes to the security of the RFID system by determining the actual boundary in which signal interception may occur.

3.3.1 System Boundaries

The system under test (SUT) contains an RFID system required for normal communication. The RFID system is composed widely used tag and reader with receive and transmit antennas. For the first objective, the SUT will be arranged similar to a logistical portal setup. Tag orientation will be adjusted to cover all faces of a box. Transmissions will occur in a large auditorium similar in dimensions to a logistics processing station. As regulated by the Federal Communication Commission (FCC), the transmitter is limited to $P_t = 1$ W of total power with $G_A = 6$ dB (4.0) of gain for the directional antennas. Under these conditions, the effective isotropic radiated power (EIRP) is given by $P_t \times G_A = 4$ W. Furthermore, the system uses frequency hopping spectrum sharing.

The second objective utilizes the RFID system within standard configurations. However, the reader and antennas are incrementally placed further away from the tag to determine a maximum read range. The read cycle will be set to one as there is only one tag that that is of concern during the experiments. The count, the number of times a read takes place during a current session, is set to 10 so that the max reads/sec will be 100. Again, the transmit power and antenna gain are fixed to maintain $EIRP = 4$ W.

3.3.2 System Services

The test system provides communication between the RFID tag and reader. For this research, successful communication is a positive identification of the RFID tag by the reader. If the reader does not successfully identify the tag, it is considered a failure.

Failures are most likely to occur via a lack of power needed for successful transmission or a transmission that experiences an uncorrectable error.

3.3.3 Performance Metrics

Since tag readability is the trait of an operational tag, the performance metric for both objectives is reads/sec. Reads/sec is the ratio of how many times a reader is able to successfully read a tag to how many seconds the reader has been given to read the tag. As tags move out of optimal read range, the read rates should diminish showing an inverse relationship between distance and reads/sec.

3.3.4 Parameters

Parameters for the experiment are as follows:

- RFID System
 - Reader – Alien ALR-9800 reader capable of reading EPC Class 1 Gen 2
 - Reader Antennas – Two Alien ALR-9611 circular polarized antennas designed for operation in the 902MHz to 928MHz UHF band.
 - Tag – Alien ALL-9540 squiggle tags are passive and operate in UHF
- Environmental
 - Temperature – Operational range for Alien Squiggle Gen 2 tags is -25° C to 65° C. The experiments will be conducted in a temperature controlled auditorium so extreme temperature effects can be negated.
 - Humidity – Operational range for Alien Squiggle Gen 2 tags is 5 to 85% relative humidity.

- Altitude – Dayton, OH is 750 feet above sea level. This is not at an extreme elevation where high or low pressure affects radio waves.
- Vibration – The components under test will remain in a stable environment and will not experience any vibration on any axis.
- Reader Orientation – Fixed orientation to provide a constant frame of reference
- Tag Orientation – Tag orientation affects the way signals from the reader are transmitted and received. Orientations, relative to the reader antennas, will be at 0° to 360° in 90° increments as well as top and bottom.
- Reader -Tag Distance – The distance for successful communication is reliant on sufficient power for the signal to propagate between the two. Path loss also comes into play.
- Electromagnetic Interference – Outside UHF signals may interfere with signals. However, frequency hopping minimizes these collisions.

3.3.5 Factors

There are two main factors that are varied to complete the research objectives. The first factor is the tag orientation. The tag is placed around a box to simulate possible tagging locations on package. The second factor is the distance between the tag and the reader antennas.

The tags employ a dipole antenna with a squiggle design. The squiggle design allows the antenna to cover more surface area and improve response ranges. The tags used are not as omni-directional as the dual dipole configuration, but they are more common because of their costs-per-performance. Finding an optimal orientation for these

dipole squiggle tags is important to improve efficiency in supply chains. It is of importance to note, that dual-polarized reader antennas operate better along the perpendicular plane of the antenna and the results should reflect this.

The second objective relies on the optimal tag orientation and the reader's ability to read the tag as separation distance increases. The ALR-9800 reader antennas are circularly-polarized. It is expected that the operating boundary will be mostly radially symmetrical regardless of antenna orientation. If an optimum orientation is found, this orientation will be used to determine the max read ranges and will be noted. Otherwise, the same antenna orientation used in objective one will be maintained for the second part of experimentation. During this part of the research, distance between the RFID reader and tag will be the distinguishing factor.

3.4 Evaluation Technique

The evaluation technique is a direct measurement experiment without use of simulations. It is necessary to take hard measurements to accurately characterize the behavior of the RFID system in relation to tag orientation and possible read ranges. Direct measurement for this type of system is not costly and does not require extreme environmental conditions.

Theoretical analysis does not accurately account for unexpected environmental conditions that are present in real-world RFID scenarios. However, theoretical analysis may be useful in providing estimates for read ranges. Given a certain amount of path loss, it is possible to find effective ranges. However, this requires a path loss estimate and assumes that the reader's antenna is relatively isotropic.

From a theoretical standpoint, it is possible to determine if an RFID tag can receive enough power to properly function using the Friis equation.

$$r = \frac{\lambda}{4\pi} \sqrt{\frac{P_t G_t G_R}{P_{th}}} \quad (1)$$

Where r is the distance between reader and tag, λ is the wavelength of the signal, P_t is the power of the reader, G_t is the gain of the reader antenna, G_R is the gain of the tag antenna, and P_{th} is the operating power threshold of the tag. Again, this would require a known path loss and dividing it into the product of the reader transmitting power and the reader and tag antenna gains. However, in a real environment, there are dramatic losses as the distance between transmitting and receiving antennas increase. Furthermore, the backscattered energy from a passive UHF RFID tag is emitted from a linear polarized antenna, while the reader antennas are both circular polarized. This circular-to-linear polarization mismatch affects the read range by a factor of $1/\sqrt{2}$ [16].

3.5 Experimental Design

The experimental design for the first objective is a two factor full factorial design with replications. This type of design tells us about two main effects and prevents interaction between the two factors from creating experimental error. In this experiment, the two factors are tag orientation and distance. To satisfy large population requirements, 30 replications were performed for each of the 6 possible antenna orientations and 5

ranges that show a decreasing trend in readability. A two-way ANOVA test creates a model for subsequent analysis.

The two factor design model provides statistics for each experimental configuration of interest. We will be able to observe the effects brought about by the factors. Also, given an expected measure of error, we can determine a confidence interval from the data provided by this type of experiment.

Communication between the tag and reader is expected to fail at various ranges for a given tag orientation. This does not allow for a direct comparison of maximum range performance between tag orientations. Thus, the largest value of reads/sec is be collected as a sample. This allows for a best-case measurement throughout all replications.

Although the best-case measurement is to be sampled, knowing how much it varies from the best-case mean is also of interest. Assuming that errors follow a normal bell-curve distribution, the best case mean can tell if enough replications have been completed via the confidence interval equation.

$$z = \frac{\bar{x} - \mu}{\frac{s}{\sqrt{n}}} = z \left(1 - \frac{\alpha}{100} \right) \quad (2)$$

$$r = \left(\frac{100 z s}{\alpha \bar{x}} \right)^2 \quad (3)$$

Where \bar{x} is the mean of samples taken from a baseline experiment, s is the sample standard deviation, and z being the standard normal for a chosen confidence level, α .

A baseline is taken from samples while the tag is at an optimal operating range from the RFID reader. The measurements taken at a 1m distance showed that best case samples had little variation. At the optimal reading range, performance was consistent and averaged 96.43 reads/sec with a standard deviation of $\sigma = 1.04$. Assuming a 90% confidence level to account for the high amount of path loss expected for range experiments, the confidence interval equation shows that no more than 3.89, or approximately 4 replications are needed to capture an accurate picture of RFID performance. However, since the boundary at which tag failure occurs is being tested, 30 replications per measurement are performed to ensure anomalies are accounted for in a normal distribution.

The second objective uses the optimal orientation to test the greatest possible read range using standard equipment and settings. While in optimal orientation, coarse measurements of 2 meter increments are taken until obvious failures in readability occur. Once a range is found that characterizes the tag failure point, measurements are taken in one-half meter increments to attain an accurate picture of tag readability at non-optimal ranges.

3.6 Result Analysis and Interpretation

Since a two factor experiment is used, the interaction and effects from the factors can be used to test the differences among the trial means. This is done by completing an ANOVA. First, the Total Sum of Squares is divided into two components, including the

Sum of Squares for the factors (SS_x) and Sum of Squares for the Error (SSE). Then, create an F-ratio of the Mean Square (MS_x) for factors to the Mean Square for Error (MSE). This allows a test of the null hypothesis, that the factors are equal. In this case, the null hypothesis is that there is no interaction between the factors.

Depending on the result of the F-ratio, more replications may be needed if the null hypothesis is not rejected. Furthermore, if the ratio is larger than the F-distribution table value, we can determine if any one of the factors is more significant than errors generated through experimentation. If this ratio comparison fails, more replications would be needed to satisfy conditions met by the selected confidence interval.

3.7 Summary

In summary, the experiment has two objectives. The first objective is to find the optimal orientation for the RFID tag. This objective will be met by completing a 2-factor ANOVA test to interpret the data and determine if the numbers of replications are valid and if the factors in question play a significant role in RFID tag readability. Readability is expected to be different for each orientation, especially for orientations where the backscatter of the tag does not transmit on a plane that falls on the reader's antenna field.

The second objective is to determine a maximum read range using the optimal orientation. It is expected that range will be more significant in tag readability. In a relatively open environment under normal operating conditions, the tag should not be as dependent on orientation. Also, as seen with most digital applications, functionality is either all or nothing and the RFID tags should reflect such in these ranged experiments.

The next chapter discusses how these objectives are completed and details an analysis of the data collected from experiments.

IV. Analysis and Results

4.1 Introduction

This chapter discusses RFID tag orientation and range experiments using standard configurations as well as an analysis into the tag performance during the experiments. The chapter begins with an analysis of the data collected. Next, any significant unexpected behavior is investigated. Finally, a model of tag performance is created that illustrates the maximum ranges at which RFID system performs given an optimum orientation and standard settings.

4.2 Tag Readability

To determine the effects on tag orientation, an Alien ALR-9800 reader in standard configuration was used to read an Alien Class 1 Gen 2 squiggle tag. The tag was positioned at a manufacturer recommended reading range of 1 m from the reader antenna pair. While at this distance, samples were taken to find the effects of tag orientation on readability. Tag orientation was accomplished by attaching a tag to a cardboard box and rotating it in 90° increments to cover a 360° flat axis as well as a top and bottom facing orientation. Then, ranging tests were completed by moving the box away from the antenna pair in 1 meter, then, one-half meter increments when readability gaps were discovered. Samples were taken by observing reads/sec via the reader Java GUI and

noting the best case measurement over a 30 second period, ample time for the reader to obtain a best case measurement.

The squiggle tags utilize a dipole antenna for backscatter communications to the reader. This means that the tags will most likely have less functionality when not perpendicular to the reader antennas (12). Tag orientation is indeed a factor of orientation. The extent to which it is a factor is reflected in ANOVA calculations.

For the first experiment, the average readability values can be seen in Table 5. Measurements were taken starting at optimal read ranges and continued in 1 meter increments until failure for most orientations were met. As expected, the stronger measurements were taken at tag orientations whose perpendicular plane matched the direction of the reader antennas. The strongest measurements were found consistently at the 360 degree and upward facing orientations.

Table 5. Readability Values (Reads/Sec) for Experiment 1

Orientation						
	0°	180°	90°	270°	up	down
1m	99.23	98.93	87.9	91.3	99.13	93.86
2m	93.33	91.93	90.73	91.16	92.66	99.33
3m	99.1	98.83	90.33	82.03	92.53	90.83
4m	99.06	94.36	88.67	45.33	99.1	90.26

4.2.1 Tag Orientation

As mentioned earlier, orientation plays a significant role in tag readability. Figure 9 shows various tag orientations in relation to the reader antennas. The reader antenna pair is two circular polarized antennas set next to each other.

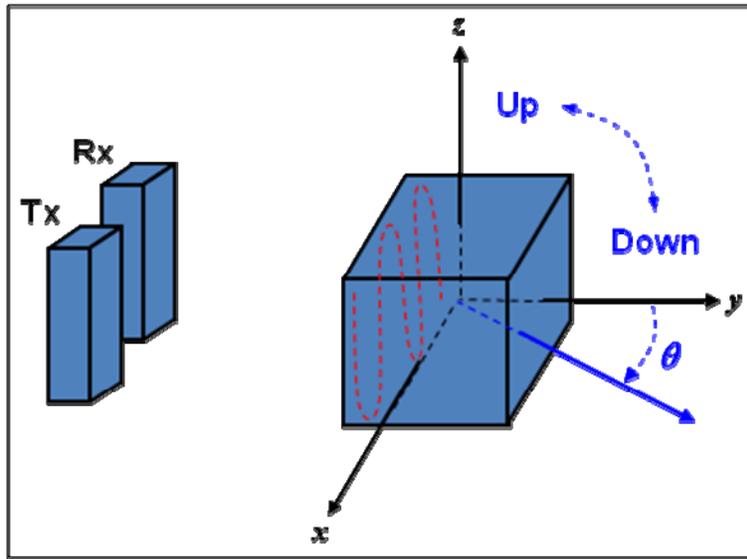


Figure 9. Tag Orientations

As shown in Table 5, readability was highest when in direct line-of-sight from the antennas. A drop in readability is noted at the 90° and 270° orientations. This is attributable to the tag's horizontal polarization. The circular polarization of the reader's antenna is able to energize the tag, however, because of the tag's linear nature, the backscatter does not radiate towards the reader's receiving antenna when placed at the 90° and 270° faces of the box.

4.2.2 *Computation of Effects*

For the first experiment, Table 6 shows that for the operating distances of 1 to 4 meters the mean distance (2.5 m) with mean orientation (tag placed dead center in the box with equal surface area facing all orientations) has a readability of 91.66 reads/sec. It is also shown that the 0° orientation outperforms the average by 6.02 which is significantly higher than second highest performing orientation, 180° (4.35). The 270°

orientation performed worst having 14.21 less reads/sec than the average. From this experiment, the 0° orientation is more suitable for subsequent ranged experiments. Although the 180° orientation performs well, the 0° orientation consistently yielded a higher readability.

Table 6. Computation of Effects for Orientation Experiment

	Orientation						Row Mean	Row Effect
	0°	180°	90°	270°	up	down		
1m	99.23	98.93	87.9	91.3	99.13	93.86	95.06	3.40
2m	93.33	91.93	90.73	91.16	92.66	99.33	93.19	1.53
3m	99.1	98.83	90.33	82.03	92.53	90.83	92.28	0.61
4m	99.06	94.36	88.67	45.33	99.1	90.26	86.13	-5.53
Column Mean	97.68	96.0125	89.4075	77.455	95.855	93.57	91.66	
Column Effect	6.02	4.35	-2.26	-14.21	4.19	1.91		

The confidence intervals shown in Table 7 confirm the reliability shown in the 360° and upward facing orientations. For the 90% confidence interval we can expect a nominal test failure rate when using the 360° or 180° orientations. Thus both are appropriate for the ranging tests for the second objective. However, with the 360° orientation being 90% sure that the measurements taken will have been within the 97.23 to 98.13 readability interval, it becomes the most reliable orientation for the ranging experiments.

Table 7. 90% Confidence Intervals for Orientation Experiment

Orientation	Mean	Std Dev	Confidence Interval (90%)	
360°	97.68	2.96	97.23	98.13
180°	96.02	3.46	95.50	96.54
90°	89.41	4.68	88.70	90.12
270°	77.46	48.66	70.10	84.82
up	95.86	3.75	95.29	96.44
down	93.58	3.84	93.00	94.16

4.2.3 Analysis of Variance

The results of the ANOVA test for experiment 1 can be found in Table 8. Orientation plays a larger factor for the first experiment (larger F-value). This is expected since measurements were only taken at optimal reading ranges. If the 5 meter range was included with the data, distance becomes the major factor as shown in Table 9. Since the P-values are extremely close to zero for effects between and within groups there are no significant effects when using an alpha of .01 (90% confidence level).

Table 8. ANOVA for Experiment 1

ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Distance	8072.57	3.00	2690.86	7.73	0.00	3.81
Orientation	33997.37	5.00	6799.47	19.52	0.00	3.04
Interaction	39722.13	15.00	2648.14	7.60	0.00	2.06
Error	242403.93	696.00	348.28			
Total	324196.00	719.00				

Table 9. ANOVA for Experiment 1 Including the 5 m Range

ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Distance	508487.33	4.00	127121.83	455.77	0.00	3.34
Orientation	152452.82	5.00	30490.56	109.32	0.00	3.04
Interaction	306657.73	20.00	15332.89	54.97	0.00	1.90
Error	242657.43	870.00	278.92			
Total	1210255.31	899.00				

4.3 Signal Interference

From the data collected, it is obvious that tag readability does decrease in a manner that would be expected from theoretical path loss. Rather, there are definite nulls that the tag experiences at various ranges depending on the orientation. An idea of the theoretical path loss experienced can be calculated using the following equation:

$$\text{Path Loss} = 20 \log_{10} \left(\frac{\lambda}{4\pi R} \right) \quad (4)$$

Where λ is the signal wavelength (902 MHz to 928MHz) and the propagation distance (meters) between tag and reader antennas is R . For the ranging experiment with the tag facing the antennas (0° orientation), definite nulls can be seen at 7 m and then the 8.5 m to the 9 m range. Table 10 highlights the average tag readability at these ranges.

Table 10. Average Readability of Tags at Distance

Distance (meters)	Readability (reads/sec)
6	39.16
6.5	89.96
7	5.33
7.5	48.16
8	10.86
8.5	0
9	0
9.5	53.8
10	67.76
10.5	0

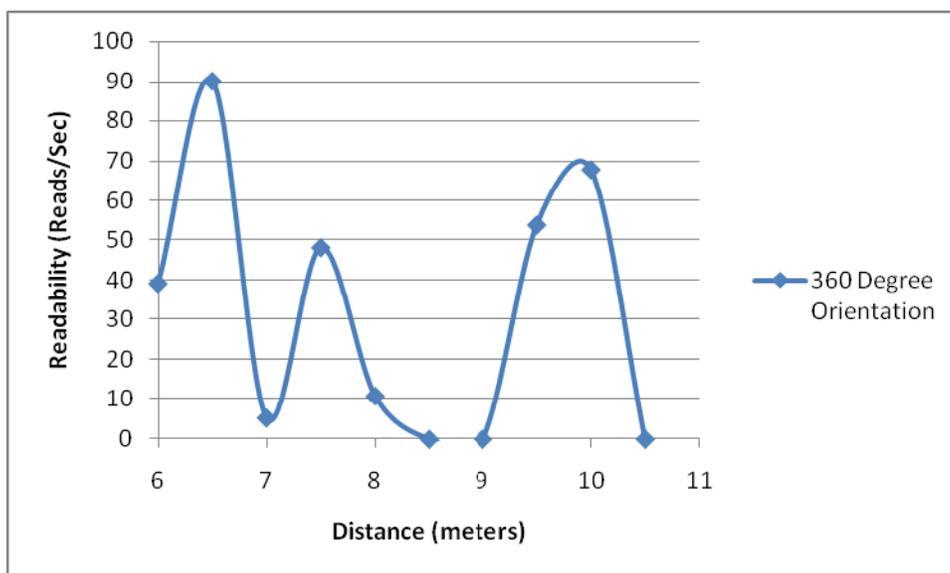


Figure 10. Readability at Distance

Figure 10 shows a graphical representation of readability data. From this view, there are obvious peaks and troughs that follow a systematic pattern. Before an analysis

of this pattern was performed, a second experiment was done to ensure that the nulls weren't attributable to unknown electromagnetic interference or an obstacle.

The verifying experiment was completed with the antenna pair facing a different direction while moving the tagged box along that plane. Again, as seen in Figure 11, the nulls once again occur at can be seen at the 7m, 8.5 and 9 m ranges.

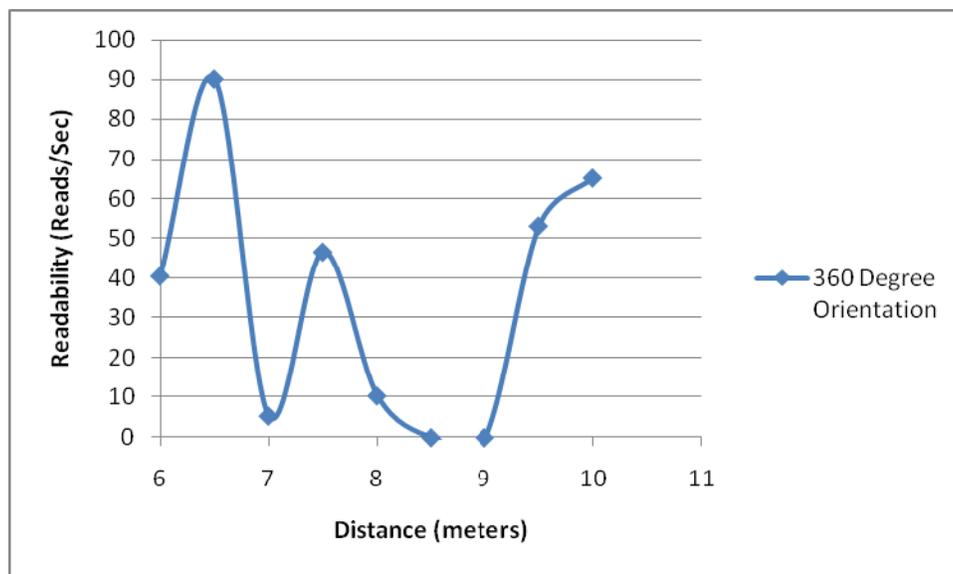


Figure 11. Second Ranged Experiment

To explain the reads/sec nulls, path loss due to destructive interference was investigated. Destructive interference can originate from a number of sources, but given that two separate experiments showed nulls at the same distances, interference from the reader antennas was considered for a theoretical explanation.

In a relatively open air environment, destructive interference is most likely to originate from signals being reflected from the ground. This reflected signal conflicts

with the original signal when they are 180° out-of-phase from each other. Being 180° out-of-phase, the peaks and valleys from two different signals cancel each other and create destructive interference at every odd numbered half wavelength. To validate this, the signal was modeled after Figure 12 and applied to the following equation:

$$R_1 + R_2 = R_D + m \left(\frac{\lambda}{2} \right) \quad (5)$$

Where R_1 represents the distance from the reader antenna to the reflection point. R_2 equals the distance from the reflection point to the tag, R_D is the direct path from the reader to the tag and m is a positive integer representing the order of the half wave.

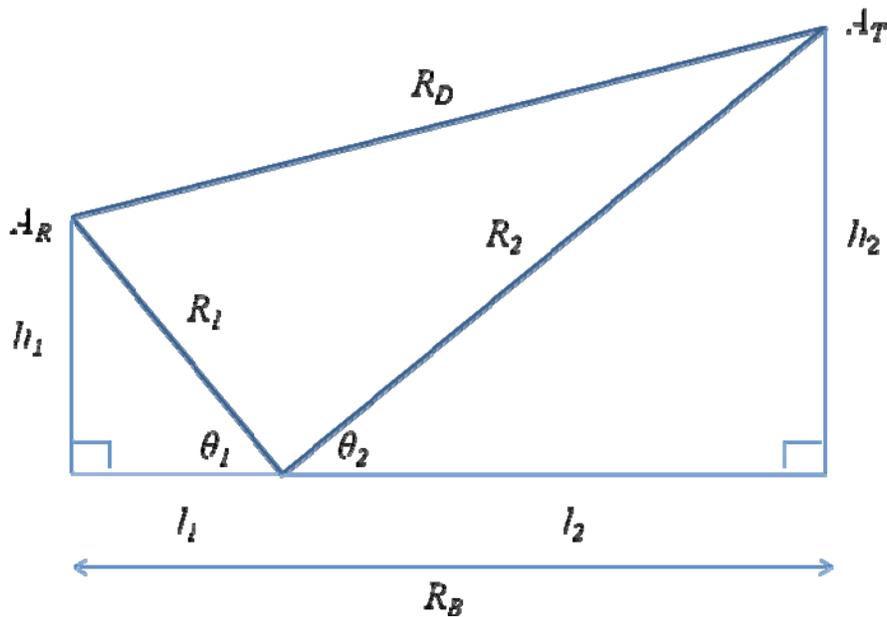


Figure 12. Geometry of Signal Reflection [17]

The height of the reader antenna, A_R , is represented by h_1 . The tag antenna, A_T , is at a height of h_2 . The angle of incidence is represented by θ_1 and the angle of reflection is θ_2 which are equal to each other due to planar reflection of an electromagnetic wave. The ground distances from the reader to the point of reflection and from that point to the tag, encompassed by R_B , are represented by l_1 and l_2 , respectively.

Since $\theta_1 = \theta_2$

$$\tan\theta_1 = \tan\theta_2 \Leftrightarrow \frac{h_1}{l_1} = \frac{h_2}{l_2} \rightarrow \frac{h_1}{h_2} = \frac{l_1}{l_2} \quad (6)$$

Solving for l_1 gives

$$l_2 = R_B - l_1 \quad (7)$$

$$\frac{l_2}{l_1} = \frac{R_B}{l_1} - 1 = \frac{h_2}{h_1} \quad (8)$$

$$\frac{R_B}{l_1} = \frac{h_2}{h_1} + 1 = \frac{h_2 + h_1}{h_1} \quad (9)$$

$$l_1 = \frac{h_1 R_B}{h_1 + h_2} \quad (10)$$

And solving for l_2

$$l_1 = R_E - l_2 \quad (11)$$

$$\frac{l_1}{l_2} = \frac{R_E}{l_2} - 1 = \frac{h_1}{h_2} \quad (12)$$

$$\frac{R_E}{l_2} = \frac{h_1}{h_2} + 1 = \frac{h_2 + h_1}{h_2} \quad (13)$$

$$l_2 = \frac{h_2 R_E}{h_1 + h_2} \quad (14)$$

Solving for R_1 , R_2 and R_D gives

$$R_1 = \sqrt{h_1^2 + l_1^2} = \sqrt{h_1^2 + \left(\frac{h_1 R_E}{h_1 + h_2}\right)^2} \quad (15)$$

$$R_2 = \sqrt{h_2^2 + l_2^2} = \sqrt{h_2^2 + \left(\frac{h_2 R_E}{h_1 + h_2}\right)^2} \quad (16)$$

and

$$R_D = \sqrt{R_E^2 + [(h_2) - h_1]^2} \quad (17)$$

Incorporating R_1 , R_2 and R_D into interference equation results in

$$\sqrt{h_1^2 + \left(\frac{h_1 R_D}{h_1 + h_2}\right)^2} + \sqrt{h_2^2 + \left(\frac{h_2 R_D}{h_1 + h_2}\right)^2} = \sqrt{R_D^2 + [(h_2 - h_1)^2] + m \left(\frac{\lambda}{2}\right)} \quad (18)$$

For the experiments, the tag and reader were placed such that $h_1=h_2$, $R_D =R_B$ and $R_D =R_B$ Equation 18 reduces to

$$2\sqrt{h_1^2 + \left(\frac{R_D}{2}\right)^2} = R_D + m \left(\frac{\lambda}{2}\right) \quad (19)$$

Solving for R_D gives

$$R_D = \frac{4h_1^2 - m^2\lambda^2}{m\lambda} \quad (20)$$

Using this equation, theoretical distances for destructive interference can be calculated as shown in Table 11 where $h = .77$ m and the frequencies 902 MHz (Low), 915 MHz (Mid) and 928 MHz (High) were used to cover the frequency hopping range of the transmissions. Paying close attention to the odd numbered half wavelengths in Table 11, we see that they are comparable to the measured null points of 7 m and 8.5 to 9 m. Although not exact, the model shows that destructive interference caused by transmission signal reflection is a potential contributor to the read/sec nulls observed in Figure 10 and Figure 11.

4.4 Summary

This chapter discussed the experiments performed for the orientation and ranging objectives. Furthermore, nulls in RFID tag readability were discovered and verified through analysis. It was determined that orientation does matter for the RFID tags even at optimal reading ranges. Although tags were still readable, the dual polarized tags showed a significant drop in readability at the 90° and 270° orientations.

Table 11. Theoretical Destructive Interference Points

		Frequency Range				
		Low	Mid	High		
Half Wavelength	1	9.15	9.29	9.42	Distance (meters)	
	2	8.83	8.97	9.11		
	3	8.29	8.44	8.58		
	4	7.53	7.69	7.85		
	5	6.56	6.73	6.90		
	6	5.37	5.56	5.75		
	7	3.97	4.18	4.38		
	8	2.35	2.58	2.81		
	9	0.51	0.77	1.03		
	10	-1.54	-1.25	-0.97		

The ranging experiments showed that maximum reading range for an RFID system with standard configurations and direct line-of-sight is about 10 m. It was also shown that the tag does experience null spots that are attributed to multipath reflections. Those nulls were also modeled using the destructive interference equation attributing the destructive signal as a reflection from the floor. The next chapter summarizes the research as a whole and discusses any issues that arise from this research.

V. Conclusions and Recommendations

5.1 Introduction

This chapter reviews the results of the research determined by accomplishing the objectives described in Chapter 1. The results of each objective is briefly summarized and conclusions discussed. Finally, recommendations for future research into this subject are detailed.

5.2 Research Objectives

The most fundamental goal of this research was to characterize passive UHF RFID tags in order to increase knowledge about a technology that is becoming “main stream” as a tracking and identification tool. The characterization of tag performance aids in making the technology more secure by understanding aspects of its limits and boundaries. This can have a significant impact on DoD logistics operations by knowing where this technology is vulnerable to communication interception.

5.2.1. Tag Orientation

The research shows that tag orientation plays a major role in the tag’s ability to communicate not only under optimal conditions, but also at various ranges. The first objective involved characterizing the effects of orientation on tag readability within optimal read ranges. Using a standard reader configuration and setup, it was found that the dipole design of the tags affect tag readability. If the perpendicular plane of the backscatter does not transmit towards a reader’s receiving antenna, the likelihood of the tag being read decreases. This drop in readability occurred in the 90° and 270° orientations. However, if the tag is placed on an object that has a 0° or 180° degree

orientation to the reader's receiving antenna, reads/sec becomes more reliable and increases the distance at which tags can be read.

5.2.2 Range Variation

The second objective involved a ranging study to determine how a tag performs as it moves beyond the optimal read range. This objective takes into account the information discovered in the first objective by using the optimal orientation found for readability and testing its limits. A typical UHF passive RFID tag claims a max read range of 20 feet (~6.6 m). This study found that the read range for a leading commercial tag to be 10 m. However, null points were also discovered at 7 m and in the 8.5 to 9 m range. These points of little to no readability were verified to be attributable to destructive interference. To model the path loss, the ground reflection of the original signal was used to calculate null points. This proved to be accurate and allowed for a better understanding of the tag behavior.

5.3 Future Research

As RFID system implementations make headway into more applications, the need to understand and secure the technology becomes more important. This research represents a first-step baseline into RFID tag characterization. Spanning from this study, more work can be done to test more of the tag functionality as range varies. The ability to write or disable tags at specific ranges would be of interest to the security and privacy of the tags. The power requirements to perform those operations differ from typical acquisition and read functions and may exhibit a different max operating range.

As mentioned in Chapter II, researchers have found ways to use tags to implement malicious code on earlier generation tags. At the time of this research, the class and generation of tag used in this study was believed to be “standard” and will likely be utilized in the coming years. The ability to perform tag operations at range, while possibly increasing functionality for legitimate operations, could open more doors for malicious users to exploit the tags.

5.4 Summary

This research provides a first-step baseline characterization of Class 1 Gen 2 RFID tag readability. The study completed this characterization by investigating two major factors in tag operations, orientation and range. It was determined that orientation plays a significant role in tag readability, even at normal operating ranges. From this information, a max reading range was also determined for a tag under normal configuration.

The research results show that tags in specific orientations can be read at ranges a little more than twice the advertised optimum read range. By having a better understanding of tag capabilities, it would prove of great benefit to securing these systems. Furthermore, understanding operating range variability brings into light what other operations can be done to tags at range. Taking steps to improve the security closes the gaps that malicious entities could take to exploit critical mission systems.

Bibliography

1. Bhatt, Himanshu and Glover, Bill. *RFID Essentials*. California: O'Reilly Media, Inc., 2006.
2. Finkenzeller, Klaus. *RFID Handbook*. Wiley Inc, 2003, 2nd edition.
3. K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra small Individual recognition security chip. *IEEE Micro*, 21(6):43–49, 2001.
4. Chawla, Vipul and Sam Ha, Dong. An overview of Passive RFID. *IEEE Applications and Practice*, 45(9):11-17, 2007.
5. R. Want, *RFID Explained: A Primer on Radio Frequency Identification Technologies Synthesis Lectures on Mobile and Pervasive Computing*, Morgan & Claypool Publishers, 15 Oct. 2006.
6. Krishna, Pattabhiraman and Husak, David. RFID Infrastructure. *IEEE Applications and Practice*, 45(9):4-10, 2007.
7. Oswald Elisabeth and Rechberger, Christian. *Practical Template Attacks*, WISA 2004, LNCS 3325,440-456.
8. Thornton, Frank. *RFID Security Protect the Supply Chain*. Canada: Syngress Publishing., 2006.
9. Chawathe, Sudarshan S. Krishnamurthy, Venkat. Ramachandran, Sridhar. Sarma, Sanjay. *Managing RFID Data*. 30th VLDB Conference, 2004.
10. Juels, Ari. *RFID Security and Privacy: A Research Study*. RSA Laboratories, 28 Sept. 2005.
11. EPCglobal Class 1 Gen 2 standard White Paper.
12. Chau, T. C., Welt B. A., Eisentadt W. R. Analysis and Characterization of Transponder Antennae for Radio Frequency Identification (RFID) Systems. *Packaging and Technology Science*, 19(1):33-44, 2005
13. Syrma Technology, Clear Disc. www.syrmatech.co.in/images/clear_disc.jpg, 2006.
14. HWV Technologies, Glass Transponder. http://www.hvwtech.com/products/605/-33235_T.jpg, 2007.

15. TheRFIDShop, RFID Key Fob. <http://www.therfidshop.com/images/Key-Fobs1-web.jpg>, 2007.
16. V. Seshagiri Rao, Pavel V. Nikitin and Sander F. Lam. Antenna Design for UHF RFID Tags: A Review and a Practical Application. *IEEE Transactions on Antennas and Propagation*, 53(12):3870-3876, 2005
17. Kneeland, Timothy. "Performance Evaluation and Analysis of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices," AFIT Thesis AFIT/GCS/ENG/03-08.

REPORT DOCUMENTATION PAGE				<i>Form Approved</i> <i>OMB No. 074-0188</i>	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 06-03-2008		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From – To) June 2007 – March 2008	
4. TITLE AND SUBTITLE PERFORMANCE ANALYSIS OF EFFECTIVE RANGE AND ORIENTATION OF UHF PASSIVE RFID				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Roque, Paul N., First Lieutenant, USAF				5d. PROJECT NUMBER If funded, enter ENR #	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/GCO/ENG/08-06	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFIT (Center for Cyberspace Research) Dr Richard A. Raines				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The purpose of this research is to characterize the performance of UHF passive RFID tags. Factors of importance are the impact of tag orientation and distance from the RFID reader. Within this study, a comprehensive literature review of RFID technology is presented as well as the methodology used for the research. Furthermore, an analysis of RFID tag experiments is discussed and the results reviewed. To accomplish this task, two main objectives have been established as goals for the study. The first objective is to determine an optimum tag orientation within the RFID reader's normal read range. Once the optimum tag orientation is determined, the orientation is used to perform range variation tests. The end goal of these tests is to find the maximum range at which the tags are readable under normal conditions using standard equipment. Grasping an idea of RFID tag boundaries contributes to the security and privacy of the technology. This is extremely important as RFID tags are becoming the logistical tool of choice for Department of Defense (DoD) supply chains. This fundamental study creates a foundation that may support both offensive and defensive oriented research. By understanding tag weaknesses and strengths, users of the technology can make sound decisions that lead to the protection of valuable information and assets.					
15. SUBJECT TERMS RFID, Passive UHF, Signal Analysis					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)
U	U	U	UU	xx	Dr Richard Raines (937) 255-6565, (Richard.Raines@afit.edu)

