

PHYSICS BEHIND RFID SMART CARD SECURITY IN CONTEXT OF
PRIVACY

by
KIRTI CHOPRA

Presented to the Faculty of the Graduate School of
The University of Texas at Arlington in Partial Fulfillment
of the Requirements
for the Degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

THE UNIVERSITY OF TEXAS AT ARLINGTON

May 2010

Copyright © by KIRTI CHOPRA 2010

All Rights Reserved

ACKNOWLEDGEMENTS

When I joined University of Arlington two years ago, I had no background in RFID. I wish to thank my advisor, mentor and friend Dr. Daniel Engels, for introducing me to RFID and helping me move into this domain. He has allowed me tremendous flexibility and freedom in defining a topic and preparing my thesis. Meetings with him have always been motivating and filled with learning. Even with his really busy schedules, he has always made himself available for discussions through meetings, emails, and phone calls, at home or on the road.

I would also like to thank Dr. Stephen Gibbs and Dr. William Dillon for their support and valuable suggestions. I appreciate their willingness to serve on my committee.

I must also thank team at Revere Security and its CEO Rick Stephenson for supporting me during the project. I thank them for graciously accepting my constant presence for the last few months. I am also grateful to Ken at Revere security for providing me help with some of the technicalities of the project.

I am grateful to Bob Combs at University of Texas at Arlington for teaching me soldering. I also learnt a lot about technology through the small discussions that I had with him. His guidance and support is unforgettable. I am also thankful to Stanley Howard at University of Texas at Arlington for letting me work in his lab.

Special thanks go out to my husband Vishal Chopra for spending sleepless nights with me in lab and helping me do my experiments. Without his encouragement this thesis was not possible.

I would also like to thank my uncle and his wife Dr. Anil and Marisol Chopra for encouraging me to pursue MS in Electrical Engineering. Also thanks to their children Sumesh, Sonali and Meghali for their support.

Finally, I would like to thank my friends Tanvi, Amit, Shesh, Dinesh, Naveen, Sai and Jason for supporting me in my experiments. I acknowledge my elder sisters Priya, Puja and their husbands Dheeraj and Sunil, my younger sister Tripti, my brother and sister in law Amol and Richa, parents Virendra and Purnima and parents-in-law Vijay and Anita and cousin Akhil for their belief in me and unflinching support throughout my thesis. Their motivation for higher education has always been my driving force. I wouldn't be where I am if not for them.

April 19, 2010

ABSTRACT

PHYSICS BEHIND RFID SMART CARD SECURITY IN CONTEXT OF PRIVACY

KIRTI CHOPRA, M.S.

The University of Texas at Arlington, 2010

Supervising Professor: Dr.Daniel Engels

In this thesis I prove that existing HF protocol is not secure. Lack of security in turn leads to violation of privacy. The unique ID on the HF RFID smart card can be sniffed by any eavesdropper. Not only eavesdropping, but cloning of the card is another significant problem that poses a privacy threat. An attacker can skim the information on a proximity card and clone it to use for his malicious purposes. RFID smart cards are now widely being used in credit cards, access system, transit system and many more such application. Tampering or malicious usage of data on aforementioned cards raises security and privacy concern. HF RFID system works wirelessly with no line of sight. Its advantage speaks for its weakness. This wireless communication happens on a protocol. Precisely, it's the communication protocol that is more vulnerable to security attacks. There are a lot of HF protocols in use today but, I have looked into ISO 14443. The attacks possible on the card could be a relay attack, eavesdropping, skimming to name a few. This thesis focuses on skimming and eavesdropping attack.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	iii
ABSTRACT	v
LIST OF FIGURES	x
LIST OF TABLES	xii
Chapter	Page
1. INTRODUCTION	1
1.1 Introduction	1
1.2 Smart Cards	2
1.3 Types of Smart Cards	3
1.4 HF RFID System	3
1.4.1 RFID Tags	3
1.4.2 Difference between types of Tags	4
1.4.3 Readers	4
1.4.4 Antenna	4
1.5 RFID Smart Card Technology	5
1.6 ISO 14443 Protocol Overview	5
1.7 Thesis Statement	6
1.8 Thesis Objective	6
1.9 Contributions	6
1.10 Thesis Overview	7
2. RELATED WORK	8
2.1 Introduction	8

2.2	RFID cloning and authentication	8
2.3	Read ranges	10
2.4	Summary	11
3.	HF PROTOCOL - ISO 14443	12
3.1	Introduction	12
3.2	Physical Layer Attacks	14
3.2.1	Relay Attack	14
3.2.2	Replay Attack	15
3.2.3	Skimming	15
3.2.4	Eavesdropping	15
3.3	Security features in the protocol	15
3.3.1	Power	16
3.4	Timing	16
3.4.1	Frame format and Timing	17
3.4.2	Measurement of FDT	19
3.4.3	Timing before the PICC SOF	21
3.5	Protocol Vulnerability	22
3.6	Anticollison Sequence	23
3.7	Privacy	24
3.7.1	Attacks affecting Privacy	24
3.8	Summary	25
4.	HF RFID SYSTEM -IN THEORY	26
4.1	Introduction	26
4.1.1	Frequency, range and Coupling	26
4.1.2	Inductively Coupled Systems	27
4.1.3	Powering up passive transponders	29

4.2	Load Modulation	30
4.2.1	Load modulation with subcarrier	31
4.3	Magnetic field strength $H(x)$ in conductor loops	32
4.3.1	Magnetic flux	34
4.3.2	Inductance L	34
4.4	Interrogation zone of readers	35
4.5	Total transponder-reader system	36
4.6	Summary	38
5.	ANTENNA THEORY	39
5.1	Introduction	39
5.1.1	Radiation Pattern and Sensitivity	39
5.1.2	Near-Field and Far-Field Patterns	40
5.2	Loop Antenna	40
5.3	Patch Antenna	41
5.4	Yagi Antenna	41
5.5	Summary	42
6.	EXPERIMENTS	43
6.1	Introduction	43
6.2	Orientation Evaluation	43
6.2.1	TI reader	44
6.2.2	Openpcd reader	44
6.3	Sensitivity of HF and UHF antenna to TRF7960	45
6.4	Jamming	47
6.4.1	TI reader signal	47
6.4.2	Openpcd reader signal	48
7.	EXPERIMENTS - SECURITY ATTACKS	51

7.1	Introduction	51
7.2	Skimming Attack	51
7.2.1	Effect of Antenna dimension	52
7.2.2	Magnetic field strength Comparison	52
7.2.3	Effect of number of turns on loop antenna	53
7.2.4	Amplified Output power	53
7.2.5	Sensitivity of tag and antenna	54
7.3	Radiation pattern of different Antenna	55
7.3.1	Effect on read range with Loop antenna	56
7.3.2	Effect on read range with Patch antenna	56
7.3.3	Effect on read range with Yagi antenna	57
7.4	Eavesdropping Attack	58
7.4.1	Screenshot of readings	58
7.5	Increasing Sniffing range	59
7.6	Summary	60
8.	CONCLUSIONS	61
	REFERENCES	62
	BIOGRAPHICAL STATEMENT	66

LIST OF FIGURES

Figure	Page
1.1 RFID smart card transaction [25]	2
3.1 Basic relay attack setup [21]	14
3.2 Frame delay time PCD to PICC [28]	17
3.3 PCD to PICC FDT [28]	18
3.4 Pause A for a bit rate of $f_c/128$ [28]	19
3.5 Type A modulation waveform timing parameters [28]	20
3.6 Type B modulation waveform timing parameters [28]	21
3.7 Timing before the PICC SOF [28]	22
4.1 Coupling between tag and reader coil [16]	30
4.2 Load Modulation [16]	31
4.3 Two sidebands created by load modulation	32
4.4 Magnetic field strength at x [16]	33
4.5 Relationship between magnetic flux and flux density [16]	34
4.6 Interrogation zone of reader [16]	36
4.7 Tag reader orientation [16]	37
4.8 Equivalent circuit of reader with antenna L1 [16]	37
6.1 Orientation Evaluation	44
6.2 Openpcd orientation evaluation	45
6.3 Sensitivity of UHF antenna to HF reader	46
6.4 Sensitivity of HF antenna to HF reader	47
6.5 Spectrum Analyser reading	48

6.6	Orientation Evaluation	49
6.7	Jamming TI reader signal	49
6.8	Jamming openpcd reader signal	50
7.1	Skimming Attack	51
7.2	Magnetic field strength comparison	52
7.3	Effect of increasing no. of turns	53
7.4	Power Comparison	54
7.5	Experimental setup for skimming attack	54
7.6	Near field pattern of loop antenna	56
7.7	Near field pattern of patch antenna	57
7.8	Near field pattern of yagi antenna	58
7.9	Openpcd reader reading tag	58
7.10	Sniffing encoded tag id	59
7.11	Decoded tag id	59

LIST OF TABLES

Table		Page
3.1	Bit rates [28]	16
3.2	PCD field strength [28]	16
3.3	Pause A timing parameter for $f_c/128$ [28]	19
7.1	Maximum read range with no. of turns	55

CHAPTER 1

INTRODUCTION

1.1 Introduction

Technology is a key component in managing the flow of products and services. Through the use of existing technology we have access to information from a wide variety of sources. Sometimes this information can exist only in digital form. However, the problem arises when the information describes about actual physical objects, states or events.

Transforming physically embodied information into digital form so that people or machines can easily access it, becomes a problem. Thus, in a simple warehouse setting if an object is moved, the database for the goods in the warehouse will no longer be accurate; someone will still need to physically verify the presence of the object. A void gets created between digital and physical worlds. Methods have been developed and are being continuously improved to cover the gap between the digital and physical worlds. Methods known as Automatic Identification and Data Capture (AIDC) are available for identifying objects automatically, collecting data about them, and entering that data directly into computer systems.

AIDC is the means of capturing external data in a digital format that can be stored for analysis to verify identity and provide authorization to enter a secured system. Depending upon the application, data can be captured in different ways such as Bar code, biometrics, magnetic stripes, Optical Character Recognition (OCR), voice recognition, Radio Frequency Identification (RFID). All of these technologies are typically considered a part of AIDC.

Radio Frequency Identification is one among the potential solutions that fills the gap between the digital and physical worlds. The complete RFID system combines the technology of the tags and readers with access to global standardized databases. This system ensures real time access to up-to-date information about relevant products at any point in the supply chain. It is also widely being used in smart card for making



Figure 1.1. RFID smart card transaction [25].

transactions as seen in figure 1.1. Within no time a user gets done paying off his bills just by waving the card in front of the reader.

1.2 Smart Cards

RFID smart card owe its intelligence to an embedded integrated circuit chip that could be a microcontroller or a memory chip alone. Smart chips on the card enables the card to store large amounts of data or carry out user programmed functions on it. It can be programmed for functions like encryption of data on card or mutual authentication to make the card more secure. One of the primary funtions comprise of its intelligent interaction with the reader [9]. The card talks to a reader either by making a physical contact with it or contactlessly through radio frequency interface. It

comes in a variety of form factors such as plastic cards, key fobs, subscriber identification modules (SIMs) used in GSM mobile phones, and USB-based tokens. These are commonly used in transactions that require to be processed quickly or hands-free, such as in mass transit systems, where a smart card can be used without even removing it from a wallet[9].

1.3 Types of Smart Cards

Interfacing between the card and the reader can be done in two ways : with contact or without contact(contactlessly)[40].

- Contact Smart card- For a contact smart card to work it needs to be inserted into the smart card reader. It requires physical contact with the reader. Unlike a magnetic stripe card that is swiped, contact smart card needs to be inserted in the reader and kept there during use. This contact between the card and reader enables the card to communicate the information stored on it to the reader [40].
- Contactless smart card - Antenna on the contactless smart card enables it to transfer data using radio frequency signals to the reader. Radio frequency identification implies that the reader picks the radio signals transmitted by the tag. Smart card is a passive RFID tag [40].

1.4 HF RFID System

1.4.1 RFID Tags

This is the basic building block of RFID. Each tag consists of an antenna and a small silicon chip that contains a radio receiver, a radio modulator, control logic, memory, and a power system.

1.4.2 Difference between types of Tags

The power source and the transmitter in the tag create the difference between the passive, semi-passive and active tags. When the tag is completely powered by the incoming RF signal, the tag is a passive tag. Alternatively when a tag has its own power system which is powered by a battery, the tag is an active tag. Semi-passive tag is in between the active and the passive tag where the tags have a battery, like an active tag, but they still use the reader's power to transmit a message back to the RFID reader using the technique known as backscatter.

1.4.3 Readers

The RFID reader or interrogator is a radio transceiver that sends signals and retrieves information stored on the tags. The reader activates and establishes communication with the tag by emitting energy using radio waves. FCC regulations in the United States and ETSI in Europe govern the amount of power that can be delivered by the reader. (Federal Communications Commission FCC, ETSI European Telecommunication Standard Institute). Modulated data carrying the signal is sent by the reader's antenna to query the tag. The reader transmits continuously while listening to tag's response. Since the RFID reader also acts as a receiver, data coming from the tag is received and decoded as well. The information received by the reader from the tag is decoded and sent to the information system via middleware for further processing.

1.4.4 Antenna

Tags and readers both being radio devices have antennas. These are used to couple the reader and the tag so that information can be transferred between the

two. Radio energy is measured by two fundamental characteristics: the frequencies at which it oscillates and the strength or power of those oscillations.

1.5 RFID Smart Card Technology

The RFID chip on the card communicates with the RFID card reader through magnetic induction. Typical data rate for information exchange varies from 106 to 848 kbit per s [41][18]. While interacting chip carries data and a large area coil on the card is used for magnetic coupling to reader's magnetic field. Magnetic flux generated by the reader's antenna coil induces voltage in the transponder's coil by inductance. This voltage is rectified to serve as a power supply for the microchip on the transponder. The capacitor in the integrated circuit chip forms a resonant circuit with its antenna coil at a frequency that corresponds to reader's transmission frequency[16]. The cards work in close proximity to the reader abiding with certain standards. The defined standards for the card limits the power that can be transmitted by the reader.

1.6 ISO 14443 Protocol Overview

Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443)[9]. Primarily, standard for smart card govern physical properties, communication characteristics, and application identifiers of the embedded chip and data [13]. ISO 7816-1,2 and 3 is held as base reference for almost all standards. Contactless credit cards operate on ISO 14443 standard at 13.56 Mhz. ISO/IEC 14443 is a four-part international standard for Contactless Smart Cards operating at 13.56 MHz [39]. It has got four parts:

- Part 1 relates to the physical characteristics and dimension of the contactless cards.

- Part 2 pertains to radio frequency power and signal interface.
- Part 3 refers to initialization and anticollision protocols for Type A and Type B.
- Part 4 defines the high-level data transmission protocols for Type A and Type B.

1.7 Thesis Statement

Security attacks imply existing HF protocols do not protect privacy. Having identified possible security attacks, there is a need to look at the physics of the interaction between the card and the reader from privacy perspective that can help mitigate further security breaches.

1.8 Thesis Objective

- Address the security concerns involved in ISO 14443 from privacy perspective.
- Identify the maximum distance from which eavesdropping and skimming can be performed. By increasing the transmitted power of the reader antenna identifying the maximum distance from which aforementioned attacks can be performed.

1.9 Contributions

My contribution - I proved that, when an adversary goes beyond FCC power regulations, six times increase in transmitted power results in read distance four times the legal read range using same antenna. Also, eavesdropping at low cost using credit card size antenna is not as much a concern as skimming.

1.10 Thesis Overview

Smart cards technology has been gaining ground since last decade. Growing usage the technology in data sensitive domains like financial sector and access system raises concern about security of data. Privacy is a right of an individual. Security breaches owing to the lack of security in existing HF protocol may violate privacy of card user. This thesis discusses security in context of privacy.

Chapter 2 deals with the concern about HF security among security researchers. This chapter discusses the related work already done in the field of HF RFID system security.

Chapter 3 discusses HF protocol standard in context of power and timing constraints. Also, effect of these constraints on the vulnerability of protocol to security attacks in terms of privacy.

Chapter 4 relates to the near field communication theory that forms the backbone of communication between the tag and the reader. It discusses the physics behind tag-reader communication.

Chapter 5 deals with the antenna theory. Specifically, radiation patterns and sensitivity of different types of antenna as it relates to read range of the reader.

Chapter 6 presents experimental observations. Specifically, experiments performed using two different RFID readers. Also, comparison of reader sensitivity and effect on read range with difference in parameters of the two readers.

Chapter 7 presents second set of experiments which relate to security attacks in context of privacy. Particularly, skimming and eavesdropping attacks are looked at and also the physics behind these attacks.

Chapter 8 is a summary and conclusion of drawn from experiments.

CHAPTER 2

RELATED WORK

2.1 Introduction

Security pertaining to RFID technology has always been a paramount concern to security experts. The unique ID on the RFID tag can be intercepted by any eavesdropper. Not only eavesdropping, but cloning of the card is another major issue that poses a privacy threat. An attacker can easily clone a proximity card. As the technology is gaining grounds in various real life domains so does the security concerns. Researchers in the field have been trying to fill the gap between technology and its security loopholes. Its presence in information sensitive applications like credit cards and Euro Banknotes, E-passports, driver license and door access are raising alarming threat to privacy of individuals. So far, a lot of work has already been done to evaluate the security and privacy of the RFID system in different domains.

2.2 RFID cloning and authentication

In [23] Heydt-Benjamin et al. discuss the vulnerability of RFID enabled credit card to security attacks. Experiments performed in [23], found out that communication protocol ISO 14443 begins with a layer three handshake, further communication takes place at layer 4. It is also mentioned in [23] that the protocol ISO 14443 at the discretion of application designer can carry arbitrary commands. In lieu of physical keys, proximity card such as an RFID enabled credit card are being used that emits a static identifier. Westhues has demonstrated [23], [45] skimming a proximity card at a distance and through walls with an inexpensive device. A concealed sniffer in

[45] can easily sniff transactions from a distance by furnishing power to the tag as, it does not need to follow the legal power constraints. RFID tags are deployed as new information carriers on E-passports. It has also been demonstrated in [24] [36], that basic e-passport is prone to a cloning attack. According to [36], it is relatively easy to clone the digital signature on the e-passport, but infeasible to modify the data contents on it. Modification of the data on the e-passport becomes difficult due to the presence of biometric information such as finger prints or facial images. Also, digital signatures on e-passports required to verify the correctness of data coming from passport issuing authority does not offer any defense against cloning[30]. As they do not bind the data to a particular passport or chip. An intermediate report including results on biometric failure rates from its biometric passport program was released by Germany[30],[11]. The report also insisted on using Diffie-Hellman based "Extended Access Control for passports[30][11]. An overview of the vulnerability of the Dutch passports to eavesdropping due to poorly formed cryptographic keys is presented in [24],[30]. For Euro-banknotes [31] has proposed to implement cryptographic techniques on high powered devices for handling banknote, rather than in banknotes themselves. Using homomorphic properties without knowledge of plain text to transform ciphertext is called re-encryption[31]. Assuming plain text is known [31] employed re-encryption to enforce privacy of banknotes even if they transmit information promiscuously. Texas Instruments's cryptographically enabled RFID device DST (Digital Signal Transponder) was present in one of the first, widely accepted payment system in US[23]. TI DST is present not only in ExxonMobil speedpass, but also operates as a theft deterrent[23], in automobiles worldwide. Researchers at Johns Hopkins University and RSA Laboratories were able to find out the cryptographic key present in DST in less than thirty minutes. Using small number of FPGAs and brute force search they were able to skim a pair of challenge-response reading from

a target tag [23],[30]. In response to US Food and drug administration's plans to use tag as anti counterfeiting devices, TI and Verisign[30] proposed chain of custody approach. Their model claims to provide integrity assurance by digital signing of tag data. However, digital signature scheme proposed does not confer cloning resistance to tags. Avoine and Oechslin [2] have suggested some cryptographic models[30]. They have emphasized on security issues at different layers of communication protocol [30]. JHU-RSA team demonstrated a cloning attack by simulating DST present in the ignition key of a car and used it to steal their own car [30]. They also cloned their own speedpass token to purchase gasoline at a service station[30].

2.3 Read ranges

Discussion of privacy is baseless without read ranges. They play an important role in securing the privacy of tags. If an adversary could somehow furnish sufficient power to the tag thereby increasing its read range, he can successfully achieve his nefarious purposes by conducting any attack like replay and relay, clandestine scanning and tracking, eavesdropping et.al. US Department of Homeland Security[6][46] claims successful eavesdropping on 13.56 Mhz tags at a distance of 10 feet. A rogue reader is one that can transmit power beyond legal limits. Kirschenbaum and Wool [35] suggest a device powered by a battery for ISO 14443 tags that can potentially scan tags from a distance of 50 cm. This range is five times the nominal read range of 10 cm for contactless proximity cards. One of the reasons why U.S. State Department has decided to go for encryption in passports is a possibility of their eavesdropping from a 30 feet distance [38]. Kfir and Wool[34] demonstrated a relay attack thus undermining the proximity assumptions in a contactless card [30]. Irrespective of the fact as to how far apart are the reader and the tag a leech- device near the tag and the ghost-device near the target reader are sufficient to create an appearance of proximity

between the tag and the reader [35]. Resistant to replay attack is a new improved randomized hash lock scheme suggested by [32] that they claim also satisfies cross reader privacy definition.

2.4 Summary

A lot of research has been conducted in HF RFID security system. This is evident from the discussion of the work done by the researchers in this field. This is also an indicator of growing concern for security and privacy of an individual's card data.

CHAPTER 3

HF PROTOCOL - ISO 14443

3.1 Introduction

ISO/IEC 14443 is a four-part international standard for Contactless Smart Cards operating at 13.56 MHz in close proximity with a reader antenna [39]. Proximity Integrated Circuit Cards (PICC) are intended to operate within approximately 10cm of the reader antenna. ISO 14443 standard has got four parts:

Part 1 relates to the physical characteristics and dimension of the contactless cards. Several environmental stresses that the card can withstand without its functionality getting damaged is also listed. It mentions operating ambient temperature range of 0°C to 50°C.

Part 2 pertains to radio frequency power and signal interface. Defined in it are two signaling schemes, Type A and Type B. Communication for both the schemes is half duplex with a data rate of 106 kbit per second in each direction. No battery is required for the card and it gets powered up by RF field. The data transmitted by the card is load modulated with 847.5 KHz subcarrier.

Part 3 refers to initialization and anticollision protocols for Type A and Type B. It has data frame, timing, anticollision command and response defined in it. and part 4 to transmission protocol. Multiprotocol readers can be constructed on the basis of initialization and anticollision scheme. These readers can be capable of communication with both Type A and Type B cards. Both type of cards wait for a polling command in the field. Reader starts polling and can complete transaction with the card responding. It can then start polling again to transact with another card in the field.

Part 4 defines the high-level data transmission protocols for Type A and Type B. Proximity cards may or may not support part 4 protocols. It is an optional part of the standard. Card or PICC reports back to the reader if it supports Part 4 commands when replying back to the polling command of the reader. Protocols which are defined in part 4 can also transfer applications.

ISO/IEC 14443 defines the technology-specific requirements for identification cards conforming to ISO-IEC 7810 and thin flexible cards conforming to ISO-IEC 15457-1 and the use of such cards to facilitate international interchange [28]. This chapter discusses security features described in the protocol. Different types of attacks and timing constraints that affect the system sensitivity to attacks.

An attack is an act or action that exploits vulnerability or the use of an exploit to compromise a system. Basic classes of threat [17] include

- Disclosure which involves snooping and skimming.
- Deception i.e repudiation of origin.
- Disruption-adding chaff or extraneous data put by the adversary to the genuine data.
- Usurpation i.e modification of data or denial of service.
- Destruction which involves killing the tag or corrupting it with a malicious code.
- There could also be threat to access if the password is cracked.

Threats could be classified at various levels as Physical, Logical and Signal. At physical level an adversary could have direct access to physical bits. At the logical level one can send and receive coherent messages. At signal level an attacker can also detect signal traffic and broadcast noise. This chapter focuses on logical and signal threat.

3.2 Physical Layer Attacks

RFID security attacks can be classified as:

- Active which include replay, relay and skimming attack
- Passive- Eavesdropping

3.2.1 Relay Attack

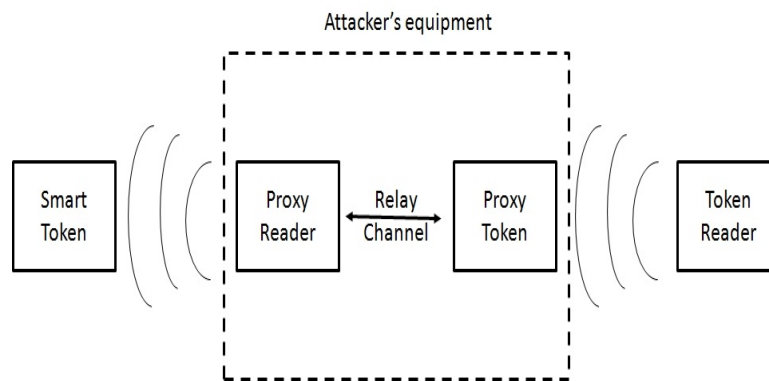


Figure 3.1. Basic relay attack setup [21].

A relay attack undermines the proximity assumptions in an RFID system [29]. In a relay attack, an attacker uses two devices, i.e. a reader and a tag respectively. To relay information at a distance, a suitable communication channel is chosen between the two devices. Using nomenclature of Kfir and Wool [35], the two devices referred to above can be termed as a ghost and leech. To place an attack, the attacker keeps the leech physically close to the target RFID device and the ghost close to the target reader [29] [35]. This setup appears to the target device and target reader as if they are in close proximity to each other. Figure 3.1 shows a basic relay attack setup [21].

3.2.2 Replay Attack

In replay attack the attacker uses a tags response to a rogue readers challenge to impersonate the tag [8].

3.2.3 Skimming

When a unauthorised reader surreptitiously reads tags from close proximity or from a distance that is termed as skimming attack [23].In this attack an adversary actively interrogates the tag [10].This attack can potentially hurt the privacy of a cardholder.

3.2.4 Eavesdropping

In eavesdropping attack an adversary passively listens to the conversation between the legal reader and the tag. This attack happens on live communication between the tag and the reader [23].

3.3 Security features in the protocol

This being a four layer protocol.Data sensitive transactions using this protocol need to be assured privacy of data at each layer. Therefore, layer 2,3 and 4 have set forth certain standards to ensure security of data transacted.These standards are set with regards to some of the parameters like power level,magnetic field strength,timing constraints etc.This section discusses various constraints imposed by the protocol in sync with FCC regulations. Communication between PICC and PCD can happen with four different bit rates as shown in table 3.1 .

Intial bit rate of $fc/128$ applies to initialization and anticollison sequence. Communication between PICC and PCD at other bits rates is optional.

Table 3.1. Bit rates [28]

Divisor D	etu	Bit rate
1	$128/f_c$ (9.4 μ s)	$f_c/128$ (106 kbit/s)
2	(optional) $128/(2 f_c)$ (4.7 s)	$f_c/64$ (212 kbit/s)
4	(optional) $128/(4 f_c)$ (2.4 s)	$f_c/32$ (424 kbit/s)
8	(optional) $128/(8 f_c)$ (1.2 s)	$f_c/16$ (848 kbit/s)

3.3.1 Power

Part 2 of the standard that is radio frequency power and signal interface specifies the characteristics of the fields to be provided for power and bidirectional communication between proximity coupling devices (PCDs) and proximity cards (PICCs) [28]. The PCD produces a high frequency alternating magnetic field. This field inductively couples to the PICC to transfer power and is modulated for communication [28]. As is stated in the standard PCD can generate field strength of atleast H_{min} and not exceeding H_{max} at manufacturer specified positions (operating volume) under unmodulated conditions. Values of H_{min} and H_{max} can be seen in table 3.2.

H_{min}	H_{max}
1.5 A/m (rms)	7.5 A/m (rms)

Table 3.2. PCD field strength [28]

3.4 Timing

Time in ISO 14443 protocol is based on elementary time unit or etu calculated by the following equation [28]:

$$1etu = 128/(Dx f_c) \quad [28] \quad (3.1)$$

where $D = 1, 2, 4, 8$ The initial value of the divisor D is 1, giving the initial etu as follows:
 $1 \text{ etu} = 128 / f_c$ where f_c is the carrier frequency as defined in ISO/IEC 14443-2.

3.4.1 Frame format and Timing

Frame comprises of frame delimiters at start and end with a string of data bits in between. It may or may not have error detection bits. Communication between a PICC and PCD occurs in frames. Pair of frames is exchanged to interact PCD to PICC followed by PICC to PCD. The sequence followed is:

PCD initiates communication. The information sent by the PCD could have optional error detection bits. The communication is then ended followed by a frame delay time PCD to PICC [28]. After PCD stops communicating, PICC starts communication from its end after a certain interval of time. Information sent by the PICC could be with optional error detection bits. After the PICC stops communicating this again is followed by a frame delay time PICC to PCD. [28]

where Frame delay time is the time between the two frames. It can be seen

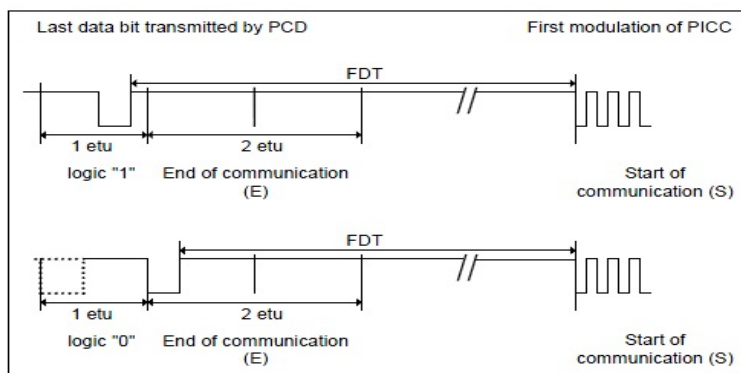


Figure 3.2. Frame delay time PCD to PICC [28].

from figure 3.2 that frame delay time from PCD to PICC overlaps with PCD end of communication.

FDT i.e after PCD transmitted its last pause and PICC begins transmitting its start bit within first modulation edge complies with the timing shown in figure 3.3 [28]. Value of n i.e an integer is defined in the following table: Values for n and FDT are defined based on the command type and the logic state of the last transmitted data bit in this command.

Command type		n (integer value)	FDT	
			last bit = (1)b	last bit = (0)b
REQA command WUPA command ANTICOLLISION command SELECT command		9	$(n \times 128 + 84) / f_c$ [= 1236 / f_c]	$(n \times 128 + 20) / f_c$ [= 1172 / f_c]
All other commands at bit rates				
PCD to PICC	PICC to PCD			
$f_c / 128$	$f_c / 128$	≥ 9	$(n \times 128 + 84) / f_c$	$(n \times 128 + 20) / f_c$
$f_c / 64$		≥ 8	$(n \times 128 + 148) / f_c$	$(n \times 128 + 116) / f_c$
$f_c / 32$		≥ 8	$(n \times 128 + 116) / f_c$	$(n \times 128 + 100) / f_c$
$f_c / 16$		≥ 8	$(n \times 128 + 100) / f_c$	$(n \times 128 + 92) / f_c$
$f_c / 128$ or $f_c / 64$ or $f_c / 32$ or $f_c / 16$	$f_c / 64$ or $f_c / 32$ or $f_c / 16$	Not applicable	$\geq 1116 / f_c$	$\geq 1116 / f_c$
All PICCs in the field shall respond in a synchronous way to the commands: REQA, WUPA, ANTICOLLISION and SELECT. This is needed for anticollision.				

Figure 3.3. PCD to PICC FDT [28].

3.4.2 Measurement of FDT

As specified in ISO 14443-2 FDT measurement starts at the beginning of the rising edge. It is illustrated in the figure below with small circles for a bit rate of $f_c/128$. The PauseA length t_1 is the time between 90 percent of the falling edge and 5 percent of the rising edge of the H-field signal envelope shown in figure 3.4 [28].

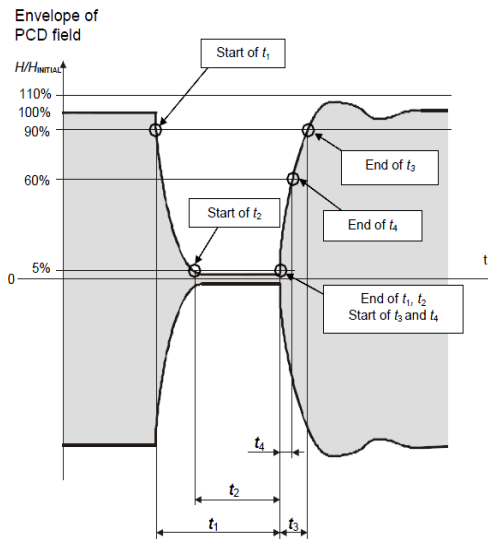


Figure 3.4. Pause A for a bit rate of $f_c/128$ [28].

The PCD shall generate a PauseA with timing parameters defined in table 3.3.

Parameter	Min	Max
t_1	$28/f_c$	$40.5/f_c$
t_2	$7/f_c$	t_1
t_3	$1.5 t_4$	$16/f_c$
t_4	0	$6/f_c$

Table 3.3. Pause A timing parameter for $f_c/128$ [28]

For ISO 14443A tags for a bit rate of $f_c/128$ the PICC can generate a PauseA with a rise time t_3 greater than both $0/f_c$ and $(t_1 - t_2) - 24.5/f_c$, and less than both $(t_1 - t_2) + 7/f_c$ and $16/f_c$ [28]. Figure 3.5 shows type A modulation waveform timing parameter for bit rate $f_c/128$.

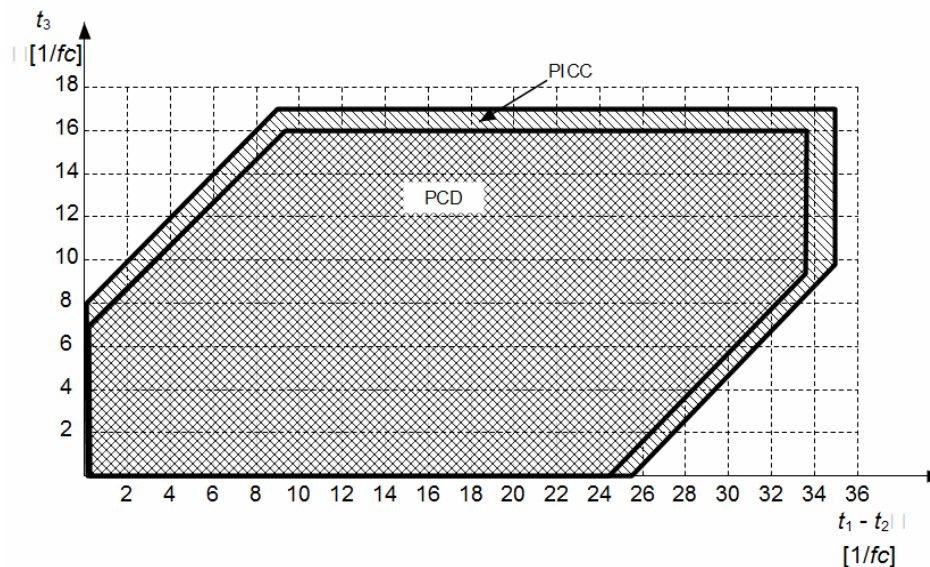


Figure 3.5. Type A modulation waveform timing parameters [28].

For a bit rate of $f_c/128$ the PICC shall be able to receive a modulation waveform with a rise time t_3 greater than both $0/f_c$ and $(t_1 - t_2) - 25.5/f_c$, and less than both $(t_1 - t_2) + 8/f_c$ and $17/f_c$ [28].

For ISO 14443 B tags for a bit rate of $f_c/128$ the PCD shall generate a modulation waveform with a fall time t_f between $0/f_c$ and $t_{f, \max, \text{PCD}} = 16/f_c$, and a rise time t_r greater than both $0/f_c$ and $t_f - 8/f_c$, and less than both $t_f + 8/f_c$ and $t_{r, \max, \text{PCD}} = 16/f_c$ [28]. Figure 3.6 shows type B modulation waveform timing parameter for a bit rate $f_c/128$.

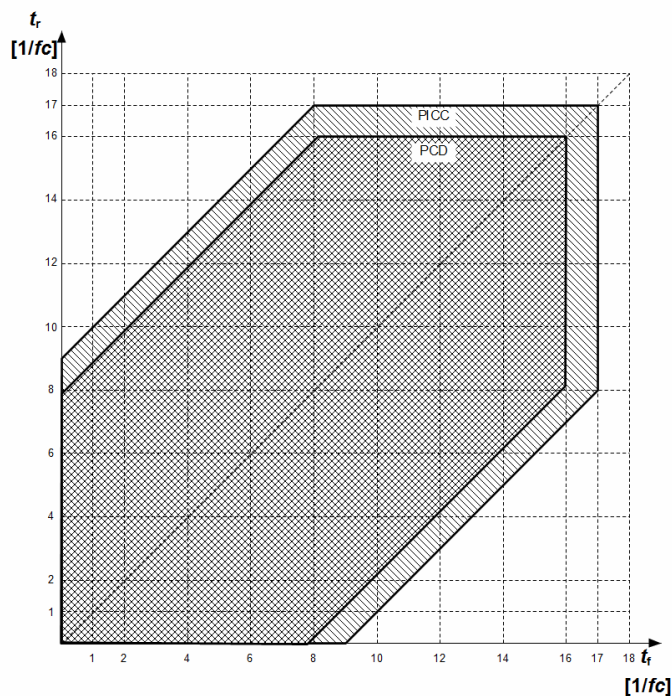


Figure 3.6. Type B modulation waveform timing parameters [28].

For a bit rate of $fc/128$ the PICC shall be able to receive a modulation waveform with a fall time t_f between $0/fc$ and t_{fmax} , $PICC = 17/fc$. With a rise time t_r greater than both $0/fc$ and $t_f + 9/fc$ and less than both $t_f + 9/fc$ and t_{rmax} , $PICC = 17/fc$ [28].

3.4.3 Timing before the PICC SOF

After PCD data transmission PICC shall respect the timing defined in figure 3.7. The default minimum values of TR0 and TR1 are defined in ISO/IEC 14443-2 and may be reduced by the PCD [28]. A guard time TR0 in which PICC shall not generate any subcarrier applies after any end of any command by PCD [28].

- TR0 shall be greater than $64/f_s$ (75.5 microsecond).

After the guard time PICC shall then generate a subcarrier with no phase transition for a synchronization time $TR1$ [28]. Initial subcarrier phase reference ϕ_0 is then established [28].

- $TR1$ shall be greater than $80/fs$ (94.4 microsecond).

The maximum value of $TR0$ is:

- $256/fs$ for ATQB
- $65536/fc$ for S(DESELECT)
- $(256/fs) * 2FWI - TR1$ for all other frames, where FWI codes an integer value used to define the FWT. $FWT = (256 * 16/fc) * 2^{FWI}$ where the value of FWI has the range from 0 to 14 and the value of 15 is RFU.

The maximum value of $TR1$ is $200/fs$. A PICC may turn on the subcarrier only

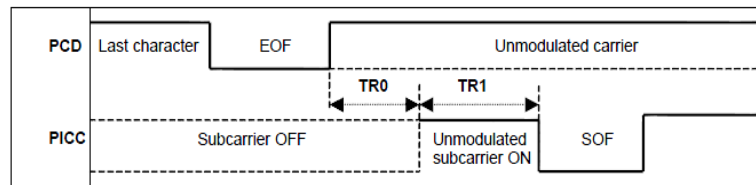


Figure 3.7. Timing before the PICC SOF [28].

if it intends to begin transmitting information[28]. The minimal and maximal values of $TR0$ and $TR1$ are applicable to PICCs. PCDs shall accept minimal and maximal values of $TR0$ and $TR1$ with a margin of $1/fs$ [28].

3.5 Protocol Vulnerability

The total time between the end of PCD transmission and the start of PICC transmission can be vulnerable to an attack. An adversary can potentially intercept or relay communication if his device operating time is less than the time between

PCD and PICC communication. Since, there is a flexibility in timing constraint this can happen to be an advantage to an attacker. Not only timing but, also field strength limitation and transmitted power level if increased beyond given limits can make the protocol vulnerable to an attack.

3.6 Anticollision Sequence

An anticollision sequence is managed by the PCD through a set of commands. The PCD is the master of the communication with one or more PICCs. It initiates communication with PICC by issuing a REQB/WUPB command and prompts PICCs for response. There is a possibility that two or more PICCs respond simultaneously during the anticollision sequence. This is called collision. PCD uses command set to handle sequences to separate PICC transmissions in time. The PCD may repeat its anticollision procedure until it finds all PICCs in the operating volume [28]. PICC communication will be under control of PCD having completed the anticollision sequence, allowing only one PICC to talk at a time. The anticollision scheme is based on definition of slots in which PICCs are invited to answer with minimum identification data [28]. The number of slots is parameterized in commands REQB/WUPB and it can vary from one to some integer number. PICCs are allowed to answer only once in the anticollision sequence. Consequently, even when multiple PICCs are present in the PCD field, there will probably be a slot in which only one PICC answers and where the PCD is able to capture the identification data. Based on the identification data the PCD is able to establish a communication channel with the identified PICC. An anticollision sequence allows selection of one or more PICCs for further communication at any time [28].

3.7 Privacy

Unauthorised dissemination of data is a privacy issue. While security depends on policy which says what system requirements are, how they are used and how to prevent security attacks. Privacy does not depend on any policy. There need to be mechanism in place that prevents security breaches and protects privacy.

3.7.1 Attacks affecting Privacy

There certain security attacks big for privacy. Due to lack of security these attacks are possible on the existing HF protocol. The two attacks are skimming and eavesdropping. In skimming an adversary could easily go beyond legal power limits and read the data on the card from a distance. He can also sniff live interaction between the reader and the tag from a distance using a sufficiently sensitive receiver. Once the privacy of an individual is hurt he becomes a victim to certain personal threats mentioned in [17].

- Action - Attacker can infer card usage behaviour of the card user.
- Association - can link or associate identity with an item.
- Constellation - mutiple tags form a constellation around the individual and the adversary can use this constellation to track people, without necessarily knowing their identities [17].
- Location - with association or constellation, location of know identifiers and constellation may be tracked.
- Preference - preference of the user may be discerned from tag data and identifier.
- Breadcrumb- associated tags form an identity link that may not be broken when the tag changes ownership. New owner may also be tracked.
- Sabotage - RFID tags could be killed.
- Eavesdropping - illicit listening.

- Traffic analysis - transactions between two individuals could be tracked by unauthorized agents by observing the movement of objects from one constellation to another [17].
- Skimming - illicit reading.

3.8 Summary

In this chapter we have covered power and timing constraints and how they relate to security and privacy. Tag id is a static identifier, thus can be easily tracked which happens to be a privacy violation. An adversary could also hack into a database or generate his own database associating individuals with their unique tag ids. Not only can an adversary play with transmitted power and timing constraint but he could also glean information like number of tags in the field. Thus, existing HF protocol is not secure enough to protect privacy.

CHAPTER 4

HF RFID SYSTEM -IN THEORY

4.1 Introduction

When the transponder is not in the interrogation range of the reader it remains passive. It gets activated on getting power from the reader. The power required to activate the transponder is supplied through the coupling unit(contactlessly). RFID systems could be half duplex,full duplex or sequential. In full and half duplex systems transponder's signal is broadcast only when the reader's RF field is on. Transponder sends data to the reader using load modulation. In sequential procedure the RF field of the reader switches on and off at periodic interval of time. One of the characteristics RFID systems depend on is operating frequency and the resulting range of the system[16]. Operating frequency is the transmission frequency of the reader. Different transmission frequencies can be classified into LF (low frequency 30-300 KHz), HF(high frequency, 3 Mhz-30 Mhz) and UHF (ultra high frequency, 300 Mhz - 3GHz) microwave more than 3Ghz. This chapter discusses the operating principle of the HF RFID systems. Also,Electromagnetic theory involved behind interaction of the transponder and the reader[16].

4.1.1 Frequency, range and Coupling

Depending upon the frequency and the range of the system they can be classified as following:- Close coupling system - In this type of system the transponder does not rely on the radiation of fields. System is coupled using both electric and magnetic field. It can operate within a frequency range of DC to 30 Mhz. Range of the system

is typically within a range of 1 cm. Such systems are primarily used in applications that require strict security requirements and not long range[16].

Long range systems- operate in the Ultra high frequency (UHF) band. They have a range above 1 m. These systems operate at a UHF frequency 868 Mhz (Europe)and 915 Mhz (USA) [16]. There operating principle is based on electromagnetic radiation and bacscatter. Typical range of 3 m can be achieved with a passive transponder while an active transponder may have a range of upto 15m. Though the battery power in an active transponder is just to power the microchip on the tag and not for data transmission.

Remote coupled system- are based on inductive coupling. Magnetic coupling between the transponder and reader can attain a read range of upto 1 m. This kind of systems work on frequency below 135 khz or 13.56 Mhz. This chapter focuses on the inductively coupled RFID systems

4.1.2 Inductively Coupled Systems

Inductively coupled transponders [4]draw energy from the reader based on electrical resonance effect. The tag's antenna element consists of an inductor coil and a capacitor so chosen that they resonate at 13.56 Mhz. The tags resonant frequency is determined by choosing the inductive and total capacitive values satisfying the following equation [4]:

$$f = 1/2\Pi\sqrt{LC} \quad (4.1)$$

Equation shown above implies that when the circuit is tuned the sum of capacitive and inductive reactances is zero. Consequently, the impedance in the tuned circuit is zero. Impedance minimized allows maximum Rf current to flow in the circuit in effect also maximising the sensitivity.

A resonating circuit's quality of absorbing power over its relatively narrow resonance band is given by its quality factor. It is generally defined for the coupling element in the circuit. RFID applications especially contactless smart cards require a high Q value. Antenna coil losses determines the effective circuit Q value. It can be calculated using the following equation [4]:

$$Q = \omega L / R_s \quad (4.2)$$

Where R_s is the coils total effective series loss resistance taking into account both the DC resistance and the ac resistance due to high frequency current flow. Practical Q values of coupling elements range between 30 and 80 for smart cards.

RF voltage induced across a tuned tag specifically to the microchip is Q times greater than the power delivered outside resonant bandwidth. Permeable materials such as metal and other dielectric mediums can detune and introduce damping resulting from dissipative energy losses in a resonant application like smart card. Vulnerability to detuning effects comes at cost of it being resonant. This vulnerability results in reduction of transponder's sensitivity and read range. Tag's parasitic capacitance and effective inductance gets undesirably altered with the presence of detuning elements. These elements can also weaken the energy coupling characteristic of the tag by distorting the magnetic flux lines[16].

A group of tags together may also result in detuning their respective antennas. This detuning is due to their mutual inductance. Whenever resonant circuits like near field tags come in close proximity to each other shift in tuning occurs and this is termed as resonance splitting. Amount of frequency shift is determined by the coupling coefficient k . Since, mutual coupling of the tags results in coupled tuned circuits [16]. Their degree of coupling also called coupling coefficient. This factor k is determined by the size, geometry and the spacing distance between the two

transponders. Tags with a bigger coil area are more susceptible to such undesirable mutual coupling effects [16].

Mutual inductance introduced between two transponders adds to the normal inductance of the antenna coil. Effective resonant frequency is reduced with this addition of this mutual inductance. Reduction in resonant frequency results in tag receiving less energy from the reader. Hence, the read range of the system is reduced significantly. A higher value of Q results in more pronounced effect. Cross coupling of tags may also result in tags being misinterpreted by the reader.

4.1.3 Powering up passive transponders

A transponder primarily consists of a microchip that carries data and a large area coil for coupling. Magnetic flux generated by the reader's antenna coil induces voltage in the transponder's coil by inductance. This voltage is rectified to serve as a power supply to the microchip on the transponder. The capacitor in the transponder's circuit is so chosen that it forms a resonant circuit with its antenna coil at a frequency that corresponds to reader's transmission frequency. Figure 4.1 shows the circuitry in both the transponder and the reader. It also shows the magnetic coupling between both the antenna coils. The two coils together can be interpreted as a transformer where in there is a very weak coupling between the two windings. Some of the factors that determine the efficiency of power transfer between the two coils are: operating frequency f , number of windings n , area A enclosed by the transponder coil, angle of the two coils relative to each other, distance between the two coils

As the frequency increases required coil inductance and hence the number of windings n decreases [16]. Since, the voltage induced in the transponder coil is still proportional to frequency so, reduced number of windings have no effect on efficiency

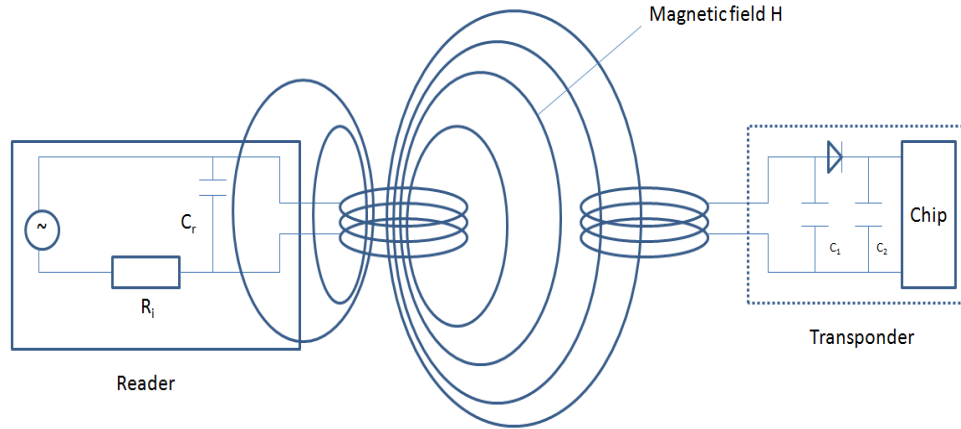


Figure 4.1. Coupling between tag and reader coil [16].

of power transfer. Therefore, at higher frequencies number of windings barely affects the efficiency of power transfer.

4.2 Load Modulation

Transformer type coupling of the primary coil at the reader end and the secondary coil at the transponder end occurs only in near field. The transponder draws energy from the alternating magnetic field of the reader. In response to readers command signal it replies using load modulation. Figure 4.2 shows load modulation. The feedback to reader antenna can be represented as a transformed impedance Z_t in the antenna coil of the reader [16]. Load resistor switching at the transponder's antenna brings about a change in Z_t at the reader end. This in turn changes the voltage at the reader's antenna. Change in voltage has an effect of an amplitude modulation [16] of the voltage U_1 at the reader antenna coil by the transponder. If the timing that takes control of switching resistors on and off at transponder's end is replaced by

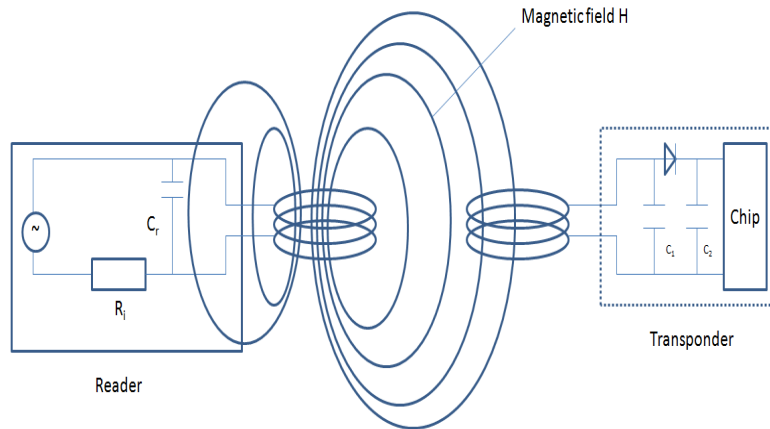


Figure 4.2. Load Modulation [16].

data. The result would be transmission of data from the transponder to the reader. Data transfer is thus, known as load modulation.

4.2.1 Load modulation with subcarrier

Voltage fluctuations in the reader antenna that represents useful signal is of a magnitude less than the output voltage of the reader. Since, a complicated circuitry would be required to detect a slight voltage change. Therefore, modulation sidebands resulting from amplitude modulation are used [16]. To get sidebands an additional load resistor is used in the transponder. Switching this resistor at a high frequency f_s creates two spectral lines around the operation frequency of the reader shown in figure [?]. This elementary high frequency is termed as subcarrier. Therefore, data transfer is by ASK, FSK or PSK modulation of subcarrier in time with data flow [16].

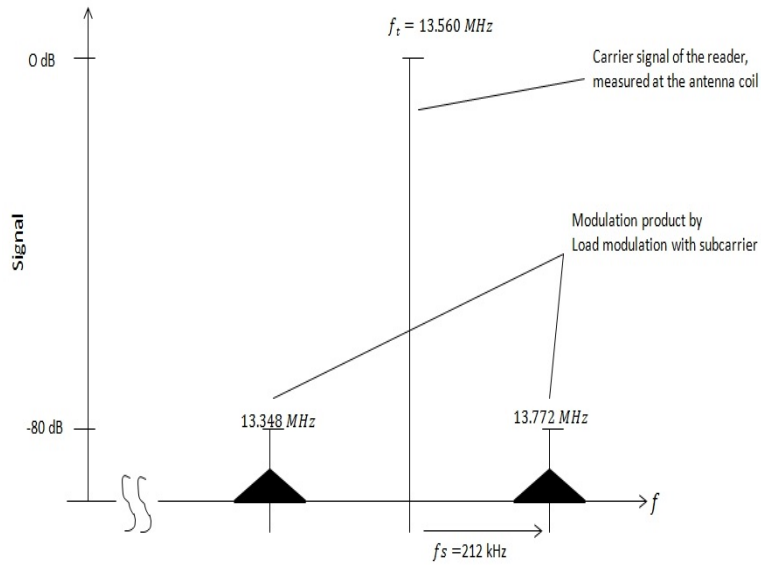


Figure 4.3. Two sidebands created by load modulation.

Two modulation sidebands formed on either side of the transmission frequency of the reader are separated from reader signal using band pass filter. Thereafter, it is amplified and can be demodulated.

4.3 Magnetic field strength $H(x)$ in conductor loops

When voltage is applied across two ends of an antenna coil. Current flowing through the coil produces alternating magnetic field. From figure 4.4 it can be seen that a point x in the center of the coil experiences maximum field strength.

As x is moved away from the center of the coil along its axis. It can be seen that on increasing x , magnetic field strength (H) decreases. Strength of the field and radius of the coil hold a constant relation upto a certain distance and then changes. Considering magnetic field in free space, it starts decaying at 60 dB per decade in near field of the coil [16] and flattens out to 20 dB per decade in the far field. To

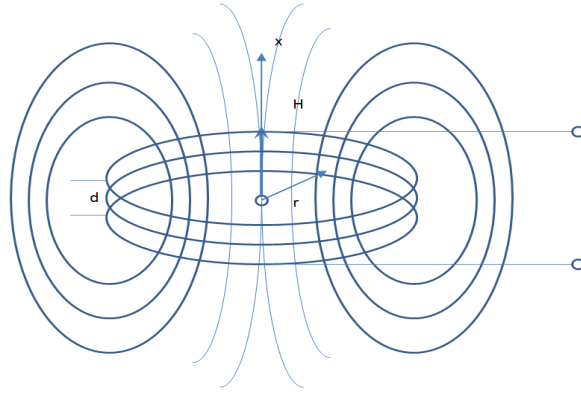


Figure 4.4. Magnetic field strength at x [16].

calculate path of field strength along the x axis of antenna coil following equation can be used [16].

$$H = I.N.R^2/2\sqrt{(R^2 + x^2)^3} \quad (4.3)$$

where N denotes number of windings R denotes circle radius r x is the distance from the center of the coil in x direction Boundary conditions for above equation is $d \ll R$ and $x < \lambda/2\pi$

Field strength path for a rectangular conductor loop is given by the following equation.

$$H = (N.I.ab/4\pi\sqrt{(a/2)^2 + (b/2)^2 + x^2}) \cdot ((1/(a/2)^2 + x^2) + (1/(b/2)^2 + x^2)) \quad (4.4)$$

Significantly higher field strength is experienced at the center of the coil for a small antenna. For distance ($x > R$) larger antennas generate a higher field strength.

4.3.1 Magnetic flux

Force exerted by the magnetic field is determined by the magnetic flux ϕ . More the magnetic flux through the coil more the force. Magnetic flux can be calculated using Magnetic flux density and area of the coil using following equation [16]:

$$\phi = B.A \quad (4.5)$$

Relationship between magnetic flux and flux density can be seen in figure 4.5

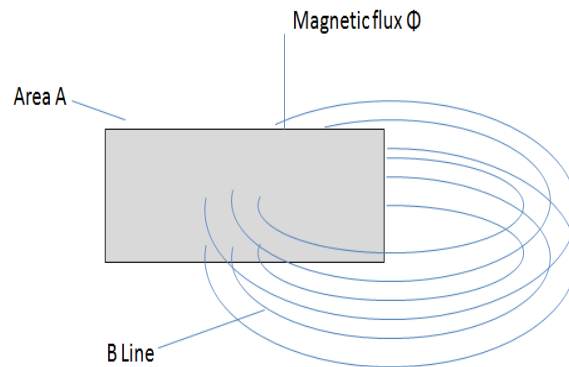


Figure 4.5. Relationship between magnetic flux and flux density [16].

Relation between magnetic field density and magnetic field strength is expressed as follows:

$$B = \mu_0 \mu_r H = \mu H \quad (4.6)$$

Constant μ_0 is the magnetic field constant ($\mu_0 = 4\pi * 10^{-6} Vs/Am$) and describes the permeability or magnetic conductivity of a vacuum. μ_r is called the relative permeability and indicates permeability of the material relative to μ_0 .

4.3.2 Inductance L

If the conductor is in the form of a loop magnetic field and flux generated around the conductor will be intense. Normally, in an antenna there are N conduction loops

of same area A through which same current I flows. Flux generated by each of the loops ϕ contributes equally to the total flux ψ [16] [7].

$$\psi = \sum \Phi = N.\Phi = N.\mu.H.A \quad (4.7)$$

Hence, inductance L is given by the ratio of interlinked flux ψ that arises in an area enclosed by current I , to the current in the conductor loop that encloses it.

$$L = \psi/I = N.\Phi/I = N.\mu.H.A/I \quad (4.8)$$

4.4 Interrogation zone of readers

If the transponder and the reader have a common central axis x as shown in the figure 4.7. magnetic field of the reader in this case is perpendicular to the transponder and maximum voltage induced into the transponder coil. A coil magnetized by a magnetic field H , if tilted at an angle v to the central axis of the coil then following equation applies:

$$u_0 v = u_0 \cos(v) \quad (4.9)$$

u_0 is the voltage induced when the coil is perpendicular to the magnetic field. No voltage is induced in the coil when $v=90^\circ$ that implies magnetic field is parallel to the transponder coil. Bending of magnetic field lines in the entire area around the reader coil forms interrogation zone of readers. Illustrated in the figure 4.6 it can be seen that since magnetic field lines emerge through the center of the coil and forms an oval shape on either side of the reader antenna coil. So, the tags antenna coil which cuts through the magnetic flux of reader coil gets an induced voltage. Different orientations of tag with respect to the reader coil can be seen in the figure 4.7.

We get an optimal read range when the transponder coil is parallel to the reader coil and when it lies in the same plane as the reader coil. If the transponder coil is

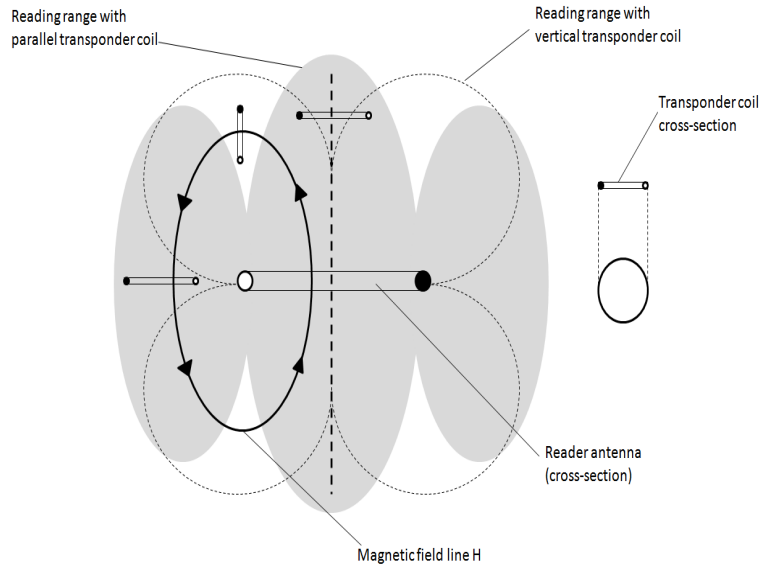


Figure 4.6. Interrogation zone of reader [16].

tilted at 90 degrees to the reader coil, no voltage is induced in the tag coil just above the reader coil as the magnetic flux now is parallel to the tag coil. Whereas moving the tag in the area where magnetic flux of the reader coil is parallel to the reader coil plane, the tag gets read.

4.5 Total transponder-reader system

Figure 4.8 shows an equivalent circuit for a reader. Coil L1 represents the conductor loop that generates magnetic alternating field. Resistance R1 corresponds to the ohmic losses of the wire resistance in the conductor loop L1. A capacitor is added in series to obtain maximum current in the conductor coil L1 at the reader operating frequency. Resonant frequency can be calculated using Thomson equation given below:

$$f = 1/2\pi * \sqrt{L1C1} \quad (4.10)$$

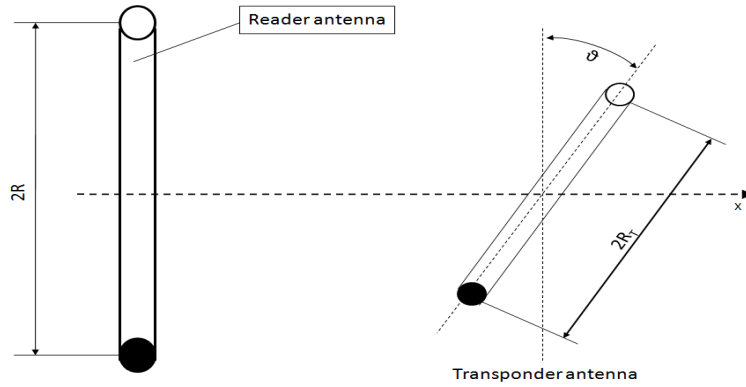


Figure 4.7. Tag reader orientation [16].

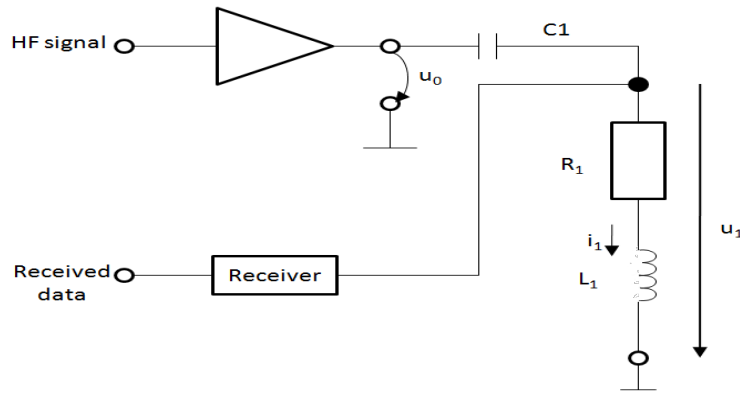


Figure 4.8. Equivalent circuit of reader with antenna L1 [16].

This being a series configuration total impedance is the sum of individual impedances i.e:

$$Z1 = R1 + j\omega L1 + 1/j\omega C1 \quad (4.11)$$

At resonant frequency L1 and C1 cancel each other. Consequently the total impedance of the system is determined by R1. It can be illustrated with the following equation.

$$j\omega L1 + 1/j\omega C1 = 0 \Rightarrow Z1 = R1 \quad (4.12)$$

At resonant frequency antenna current i_1 reaches a maximum and is calculated from source voltage u_0 of the transmitter high level stage and the ohmic coil resistance R_1 . It is calculated using the following equation:

$$i_1 = u_0/z_1 = u_0/R_1 \quad (4.13)$$

Voltage u_1 at the conductor loop L_1 and u_{c1} at the capacitor C_1 are in antiphase and cancel each other at the resonant frequency because current i_1 is same. Figures of a few hundred volts can be easily reached at L_1 and C_1 , despite a low source voltage u_0 . Theoretically, voltage at the conductor coil and the series capacitor can reach upto a maximum of 700V at resonant frequency. It can be seen in the graph below.

4.6 Summary

Near field is the region defined by the sphere of radius $\lambda/2\pi$. In this region magnetic field strength path follows a relation $1/d^3$ as can be seen in the graph below. This corresponds to a damping of 60 dB per decade. Substituting frequency 13.56 Mhz in $\lambda/2\pi$ yields a wavelength of 22 m. This implies that HF reader can emit upto 22m .But, the constraint is the loss of power with distance. Transition to far field happens after $\lambda/2\pi$. Upon transition to far field damping path flattens out. After separation of the field from antenna only free space attenuation of electromagnetic waves is relevant to field strength path. Field strength in far field decreases according to the relation $1/d$. This corresponds to a damping of 20dB per decade (of distance) [16].

CHAPTER 5

ANTENNA THEORY

5.1 Introduction

An antenna is a device that transmits and or receives electromagnetic waves which are often known as radio waves [5]. Antennas operate efficiently over a relatively narrow frequency band. These are typically resonant devices. To receive uninterrupted transmission they must be tuned to similar frequency as the radio system in which they operate [5].

5.1.1 Radiation Pattern and Sensitivity

Relative strength of the radiated field in various directions from antenna at a constant distance forms a radiation pattern. Radiation pattern also describes receiving properties of an antenna, therefore is a reception pattern as well. It is mapped either in a rectangular or a polar format [43].

For a given transmitted output power, the total amount of energy that is radiated remains constant. The energy radiated in one or more directions can be increased and decreased in other directions by focusing the energy. This is what gives an antenna "gain" [33]. The antenna size is referred relatively to the wavelength, which is the distance a radio wave will travel during one cycle. The wavelength is calculated as shown in the formula below [33]:

$$\lambda = c/f \tag{5.1}$$

Where, λ is the wavelength, and is expressed in units of length c is the speed of light, $3 \times 10^8 m/s$ f is the frequency For efficient transfer of energy, the impedance of the

radio, the antenna, and the transmission line connecting the radio to the antenna must be the same. Radios typically are designed for 50 ohms impedance and the coaxial cables (transmission lines) used with them also have a 50 ohm impedance. Efficient antenna configurations often have an impedance other than 50 ohms, some sort of impedance matching circuit is then required to transform the antenna impedance to 50 ohms.

5.1.2 Near-Field and Far-Field Patterns

Field pattern that exists close to the antenna is called near field pattern. Whereas, field pattern at large distances from the antenna is referred as far field pattern. Far field is also called radiation field. Near field is called induction field (although it also has a radiation component). Usually its the radiation pattern of an antenna that is of interest so antenna patterns are mostly measured in far field region [5].

5.2 Loop Antenna

A loop antennas typically sensitive to magnetic field than electric field (therefore it is also called a magnetic loop). The Faraday's law of induction (or the law of electromagnetic induction) states that the induced electromotive force $e(t)$ in a loop is directly proportional to the time rate of change of magnetic flux $\phi(t)$ through the loop according to the relation [44] [20]:

$$e = -d\phi/dt \quad (5.2)$$

where:

- e is the induced electromotive force, in V
- ϕ is the magnetic flux accross the circuit, in webers ($Wb \equiv Vs$)

Radiation pattern of loop antenna

5.3 Patch Antenna

A microstrip patch antenna has a upper and lower hemishpere microstrip patch radiator working against ground plane,which are oriented in close proximity and spaced apart from each other.It has a substantially omni-directional pattern.One of the radiators is excited in left hand circular polarization and the other one in right hand circular polarization.The field from the radiators is such that it adds constructively across their ground planes to achieve an omni-directional radiation pattern [19].

5.4 Yagi Antenna

The Yagi antenna is a commonly used antenna as it offers gain and directivity.It was developed by a Japanese engineer Yagi-Uda. Its designed using dipoles.A standard TV antenna has a series of dipoles in parallel to each other with fixed spacing between the elements. The determing factor for the number of elements used depends on the desired gain and the supporting structure limit. Taking an example of a three element Yagi.It consists of a director, a driven element, and a reflector. Reflector is to the right of the driven element.To allow for proper tuning the reflector is slightly longer than the driven element. The reflector is slightly longer than half wavelength and is simply a passive piece of metal.Director is at the front of the antenna. It is electrically and physically shorter than the driven element [5]. All of these elements work together to project a radiation pattern in the forward direction. This forward radiation pattern has gain [5]. This type of system is ideal for television broadcasts [5].

5.5 Summary

In this chapter antenna theory about Loop, Patch and Yagi antenna is presented, main focus being on the radiation pattern of the antennas. All the three antennas have got a different radiation pattern because of their differing structures. All of these antennas have been used in our experiments to see the effect on the read range of the reader.

CHAPTER 6

EXPERIMENTS

6.1 Introduction

In this chapter, various experiments for orientation evaluation, sensitivity and jamming HF signal for a reader - tag communication are discussed. One of the commonly used antennas in HF RFID system is a loop antenna. I have used Feig loop antenna (dimension 32.2 cm x 33.7 cm) and TI reader TRF7960 [27] for my experiments. Certain parameters play a significant role in affecting the read range of the reader antenna. Effect of following parameters is observed:

- Power
- Distance
- Protocol Timing Constraints
- Type of Antenna
- Number of turns in loop antenna
- Sensitivity of read range to tag and reader orientation
- Dimension of antenna
- Magnetic field strength

6.2 Orientation Evaluation

Transmitted power of an antenna is the amount of radio frequency energy that it produces as output. In spite, of the fact that the reader is transmitting at full output power, orientation of the tag to the reader plays a significant role in affecting the read range of the reader.

6.2.1 TI reader

Without amplifying the output power of the reader, distance at which tags are read is observed. With 200 mW power radiated by TI HF reader TRF 7960 EVM [27] antenna, orientation at which tags are read and also distance is noted.

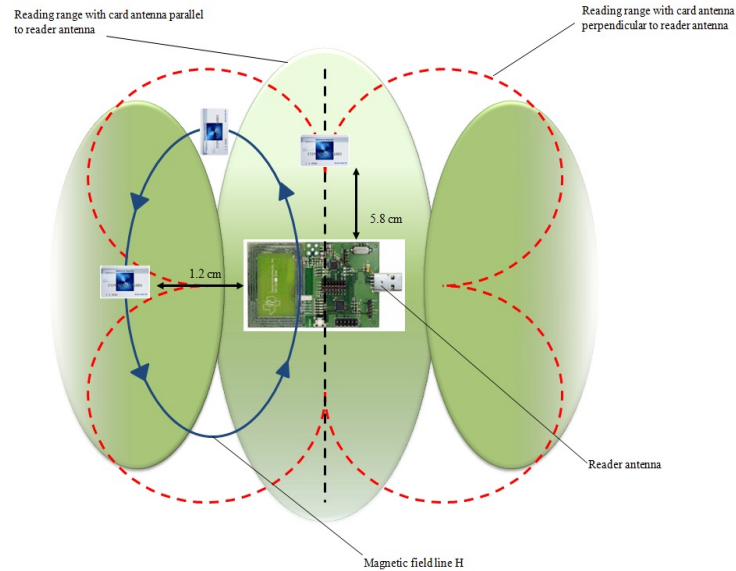


Figure 6.1. Orientation Evaluation.

As can be seen in 6.6 maximum read range is 5.8 cm when the tag is kept parallel to the reader. This is because maximum magnetic flux lines pass through the tag antenna coil when it is kept in center. This in turn induces voltage on the tag and enables it to respond to the reader's commands.

6.2.2 Openpcd reader

The orientation evaluation is done for a openpcd reader [22] as well. Angle and the distance at which the tag is read is noted and shown graphically in the polar plot 6.2. As can be seen in figure 6.2 maximum read range is more than 4 cm when the

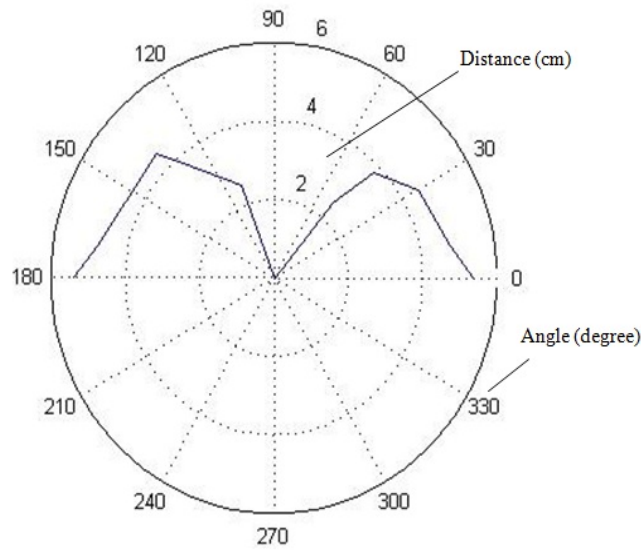


Figure 6.2. Openpcd orientation evaluation.

tag is at zero degree orientation to the reader. Range goes on decreasing as the tag orients from 0 to 90 degrees. At exactly 90 degree orientation the tag is not read. This is due to the fact no magnetic flux lines pass through the tag at all and there is no voltage induced in the tag antenna coil. Hence, the tag is not being read.

6.3 Sensitivity of HF and UHF antenna to TRF7960

Transmitted power of TI reader TRF 7960 [27] is observed at different orientations to a HF and a UHF receiving antenna. The receiving antenna's reading is seen on a spectrum analyzer. Figure 6.3 shows the experimental setup where a UHF Alien antenna is used to measure the transmitted power of TRF 7960 HF reader [27]. Reader is kept at different orientations to the antenna and maximum distance at which the reader signal is clearly heard is noted.

Similar experiment is repeated with a HF antenna and TI reader's transmitted power is observed at different orientations. Maximum distance at which the HF



Figure 6.3. Sensitivity of UHF antenna to HF reader.

reader's signal is heard clearly is noted. Figure 6.4 shows a setup wherein HF antenna is measuring the transmitted power of the HF reader on a spectrum analyzer.

The two receiving antennas were connected to a spectrum analyser to measure the transmitted power of the TI reader TRF 7960 EVM. Reading of the signal was as seen in the figure 6.5 On the spectrum analyzer -60 dBm is considered noise. Signal more than -60 dBm is considered as a clear signal from the reader. Graphs are plotted for different angular orientation and a comparison is made between HF and UHF antenna readings.

It is clearly seen from figure 6.6 sensitivity of the HF antenna to HF reader signal is more than a UHF antenna. This is due to the fact that HF antenna is tuned to the same frequency as the operating frequency of the HF reader.

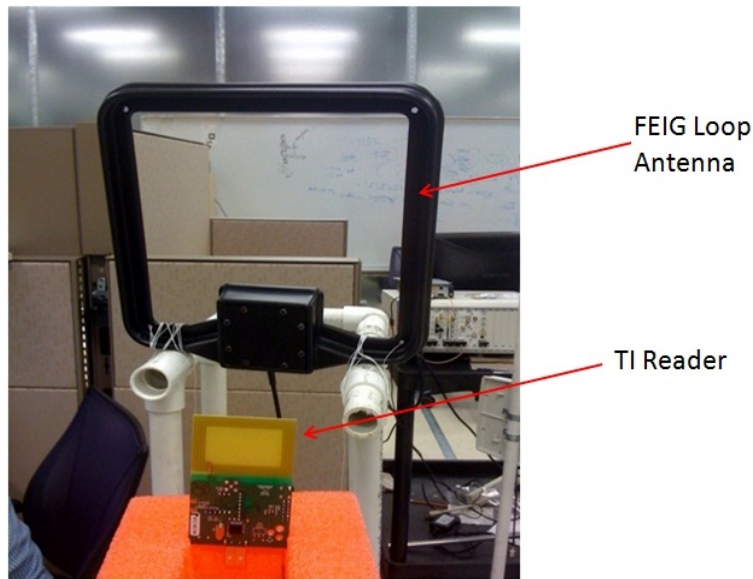


Figure 6.4. Sensitivity of HF antenna to HF reader.

6.4 Jamming

This experiment was performed to detect the presence of a adversarial sniffing device in the region where tag reader interaction is happening. Maximum distance at which the attacker could possibly be present is seen in case of both, TI reader and Openpcd reader interaction with the tag.

6.4.1 TI reader signal

In figure 6.7 the covered area in the polar plot is the area around the tag and reader where blocking happens. Reader used for blocking the TI reader signal was another TI reader with an amplified output power transmitted through feig antenna(dimension 32.2 cm x 33.7 cm). It is evident from the figure 6.7 that more blocking range is at zero degree orientation to the reader.It remains so till 60 degree orientation on either side and then goes on reducing till 90 degree orientation.

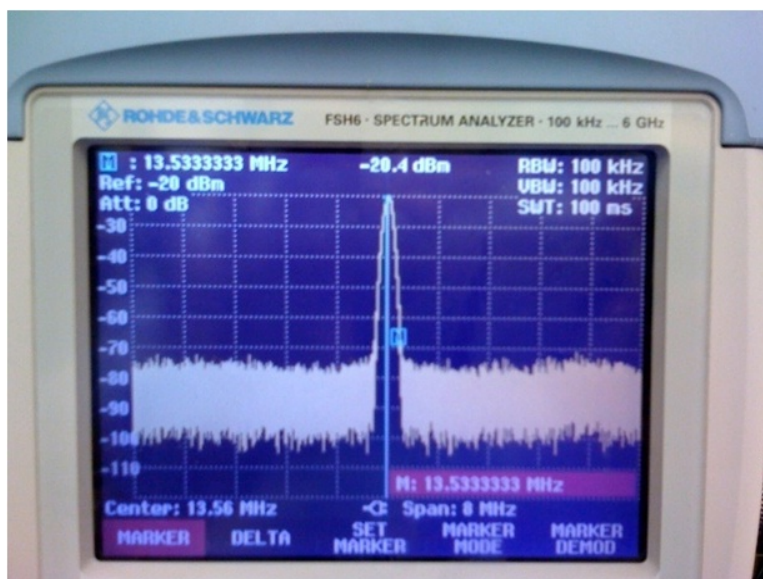


Figure 6.5. Spectrum Analyser reading.

6.4.2 Openpcd reader signal

Again, the same TI reader with amplified antenna output is used to block the signal of Openpcd reader. As can be seen from figure 6.8 the blocking range for an openpcd reader is almost half the blocking range of TI reader TRF 7960.

This owes to the number of turns on the loop antenna of each reader. Since, TI reader has got more number of turns on its antenna in comparison to openpcd reader. This results in better read range, thus more blocking range as well. Since the adversary can also hear the signal at a greater distance.

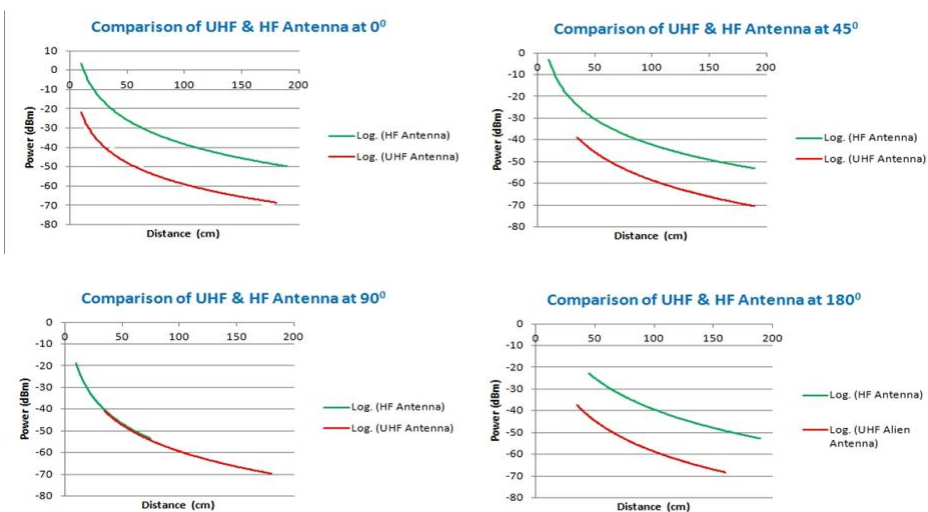


Figure 6.6. Orientation Evaluation.

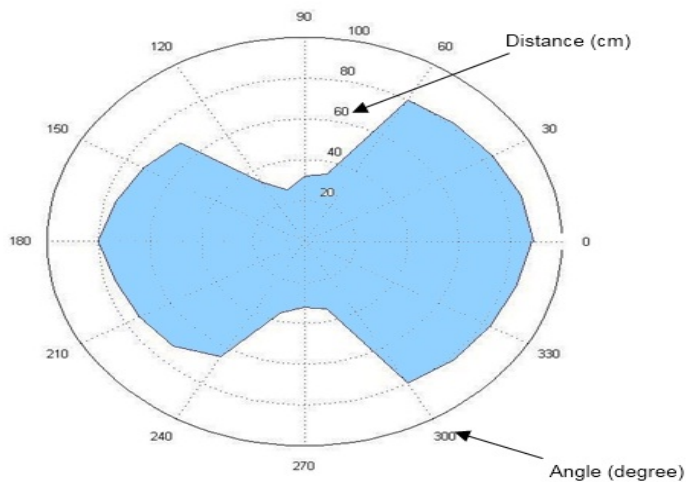


Figure 6.7. Jamming TI reader signal.

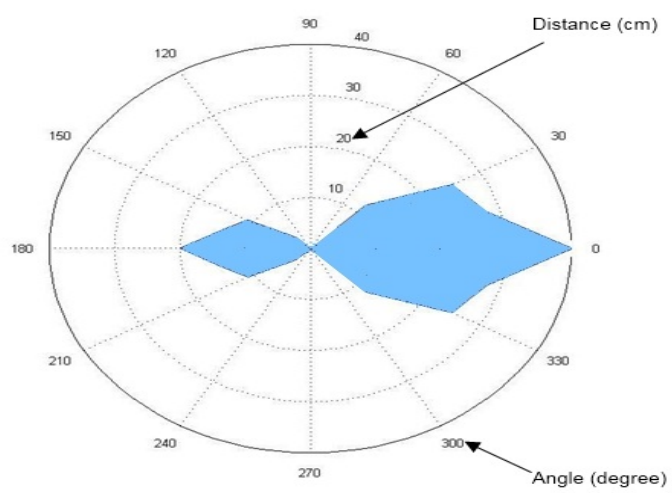


Figure 6.8. Jamming openpcd reader signal.

CHAPTER 7

EXPERIMENTS - SECURITY ATTACKS

7.1 Introduction

In this chapter skimming and eavesdropping attacks on a reader - tag communication are discussed. Skimming attack is performed using TI reader TRF 7960 [27], an amplifier and feig antenna (dimension 32.2 cm x 33.7 cm).Eavesdropping attack is performed using a proxmark sniffer [12] and TI reader TRF 7960 EVM [27].

7.2 Skimming Attack

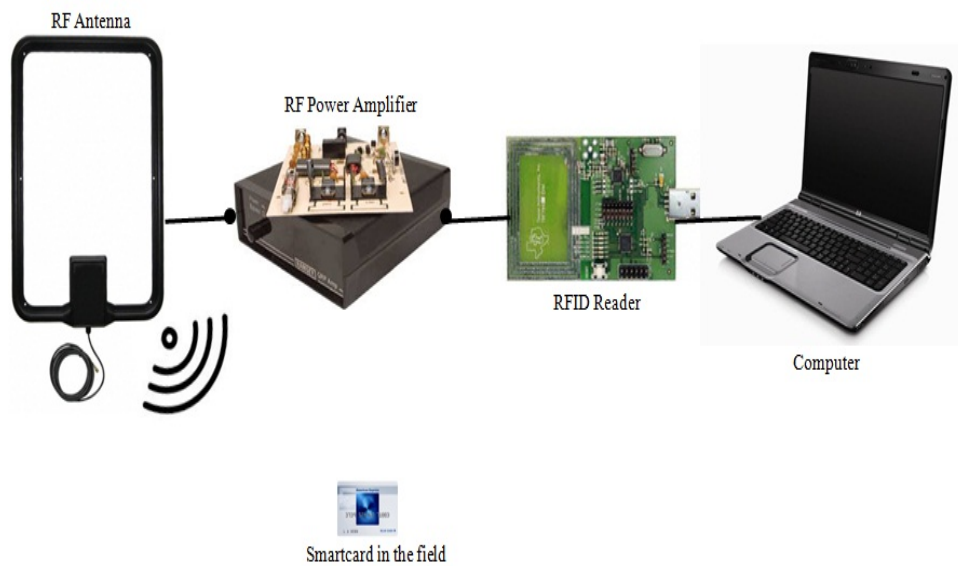


Figure 7.1. Skimming Attack.

7.2.1 Effect of Antenna dimension

As observed in the previous experiments with the standard reader and a smaller antenna, maximum read range of upto 5-6 cm could be seen. With the feig antenna (dimension 32.2 cm x 33.7 cm) read range increased to 10 cm. An increase in the read range owes to the larger dimension of the antenna in comparison to the smaller antenna. This proves that antenna dimension affects the read range of the reader.

7.2.2 Magnetic field strength Comparison

Having looked at the antenna dimension we compared magnetic field strength of the two antennas. Equation used to calculate the magnetic field strength of the two antennas is given below:

$$H = (N.I.ab/4\pi\sqrt{(a/2)^2 + (b/2)^2 + x^2}) \cdot ((1/(a/2)^2 + x^2) + (1/(b/2)^2 + x^2)) \quad (7.1)$$

In figure 7.2 it can be seen that bigger antenna i.e the feig antenna's magnetic field

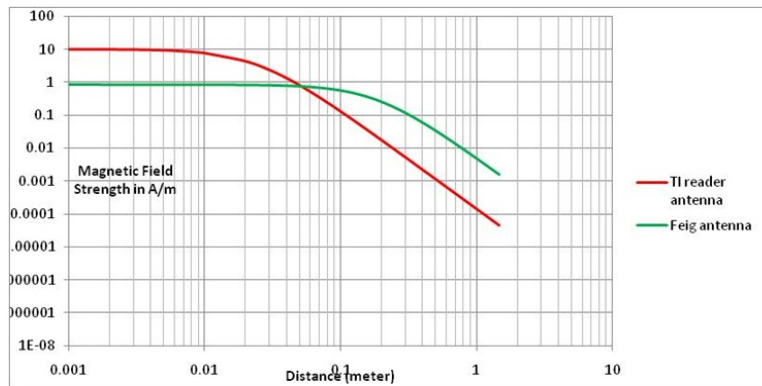


Figure 7.2. Magnetic field strength comparison.

strength is less than the smaller TI reader's magnetic field strength upto approximately 5 cm. Beyond 5 cm magnetic field strength of the feig antenna is more than the TI reader antenna. This goes in line with theory explained in [26] i.e small sized

antennas have higher field strengths closer to the antenna than larger sizes but this falls-off more quickly [26].

7.2.3 Effect of number of turns on loop antenna

As is evident from the equation of H in the previous section that magnetic field strength is directly proportional to the number of turns on the loop antenna. An effect of increasing the number of turns on the loop antenna shows the increase in the magnetic field strength of the antenna. This can be seen in figure 7.3 From fig

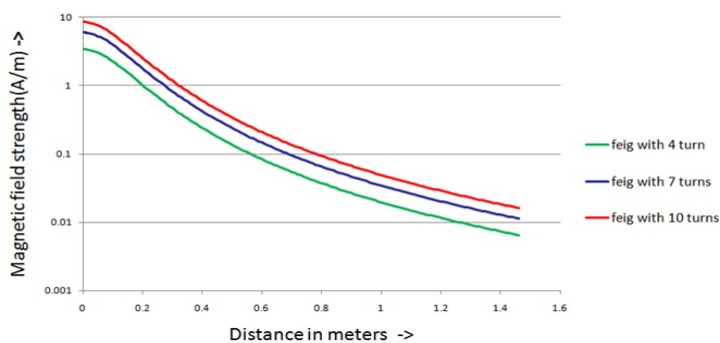


Figure 7.3. Effect of increasing no. of turns.

7.3 it can be seen that increasing the number of turns from 1 to 10 on a bigger feig antenna. At same distance more magnetic field strength can be experienced by the tag. This shows that not only the antenna dimension but also increasing the number of turns on the magnetic loop antenna upto a certain extent shows an increase in the magnetic field strength at same distance.

7.2.4 Amplified Output power

When the output power of the standard TI reader TRF7960 [27] is fed to an power amplifier, output of which in turn drives the feig antenna. There was a six times

increase in the output power of the feig antenna seen on the CRO. After amplification output power is seen to be 6W. This increase in power leads to better sensitivity of antenna at same distance. Also an increase in range. As can be seen from 7.4 that after

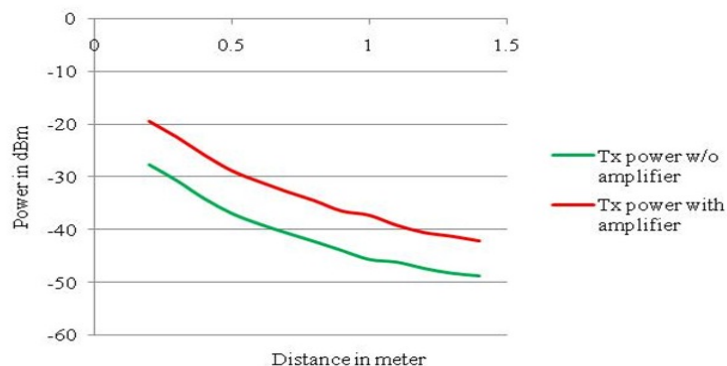


Figure 7.4. Power Comparison.

amplification power at same distance is more than power without amplification. Better power at greater distances implies better read range.

7.2.5 Sensitivity of tag and antenna

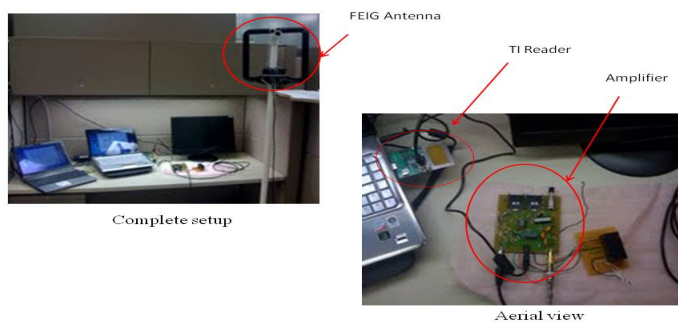


Figure 7.5. Experimental setup for skimming attack.

According to [14] for a tag dimension $46 \times 75 \text{ mm}^2$ over the center of antenna, minimum operating field of the tag is $H_{\text{min}} = 85 \text{ mA/m rms}$ when the tag is placed parallel to the antenna, at transmitting power 4 W . Knowing the read range of the standard TI reader for a tag antenna dimension $46 \times 76 \text{ mm}^2$, magnetic field strength that activates the tag can be calculated at that distance. This is calculated using following equation :

$$H = (N \cdot I \cdot ab / 4\pi \sqrt{(a/2)^2 + (b/2)^2 + x^2}) \cdot ((1/(a/2)^2 + x^2) + (1/(b/2)^2 + x^2)) \quad (7.2)$$

Value of minimum operating field for tag antenna dimension $46 \times 76 \text{ mm}^2$ is calculated to be 52.23 A/m . Distance at which a feig antenna (dimension $32.2 \text{ cm} \times 33.7 \text{ cm}$) can read a tag requiring minimum operating field 52.23 A/m is given by table 7.1

Feig antenna (no. of turns)	Read range (in cm)
1	11
4	28
7	36
10	42

Table 7.1. Maximum read range with no. of turns

From table 7.1 it can be seen that for 10 turns on the loop antenna (dimension $32.2 \text{ cm} \times 33.7 \text{ cm}$) read range is increases 4 times when the power of the antenna is increased 6 times the legal power limits for the same antenna.

7.3 Radiation pattern of different Antenna

This set of reading were taken to observe the near field pattern around three antennas. Also sensitivity of these antennas at different distances is seen. Purpose is to

analyze the effect of using a omnidirectional and a directional antenna either tuned or not tuned to operating frequency of the tag.

7.3.1 Effect on read range with Loop antenna

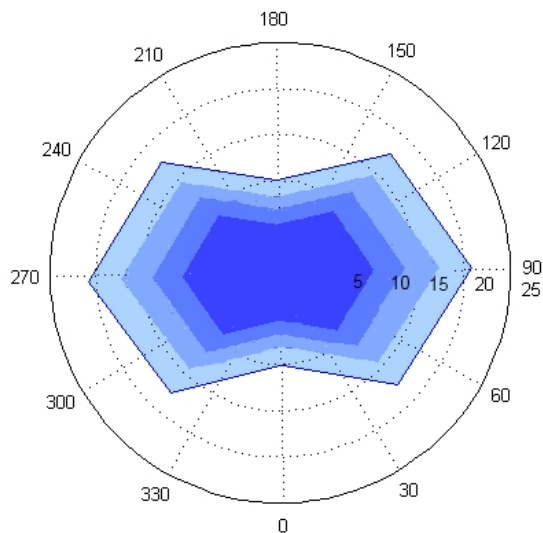


Figure 7.6. Near field pattern of loop antenna.

Figure 7.6 shows the field pattern around a loop antenna. Shaded region shows the field around the antenna where the tags can be read. It's not only the presence of tag in the field but orientation of the tag to the antenna is equally important for the tag to be read.

To compare loop antenna near field radiation pattern with another antennas. Radiation pattern of patch antenna is observed. It is as shown in figure 7.7

7.3.2 Effect on read range with Patch antenna

These readings were taken with a spectrum analyser when power is -59.5 dBm. Distance at which -59.5 dBm is seen on spectrum analyser is noted. It is observed

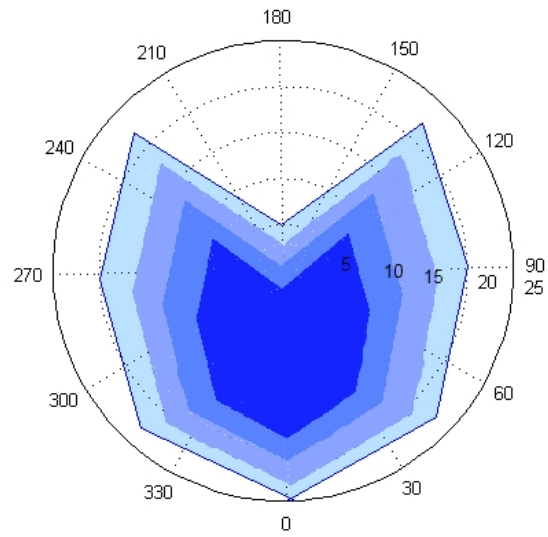


Figure 7.7. Near field pattern of patch antenna.

that field is in more in front of the antenna and at a larger distance in comparison to field behind the antenna. One possible reason for this is that patch antenna is a directional antenna. In comparison to loop antenna radiation which is almost uniform around the antenna, radiation pattern of patch antenna is non uniform.

7.3.3 Effect on read range with Yagi antenna

Another antenna used is a yagi antenna which is also a directional antenna. Field pattern seen around a yagi antenna is shown in figure 7.8. As seen in figure 7.8 probability of tag being read is more when it is at an orientation of 0 or 180°. Read distance at 90 and 270° is comparatively less than 0 degree orientation.

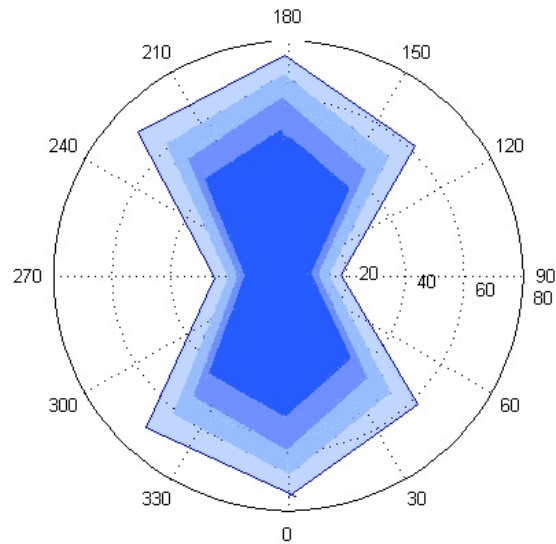


Figure 7.8. Near field pattern of yagi antenna.

7.4 Eavesdropping Attack

Eavesdropping attack is implemented using a proxmark sniffer [12]. With a credit card size antenna the sniffer was able to sniff upto 3 cm from the reader. Figure 7.9 shows a screen shot of openpcd reader [22] reading the tag id.

7.4.1 Screenshot of readings

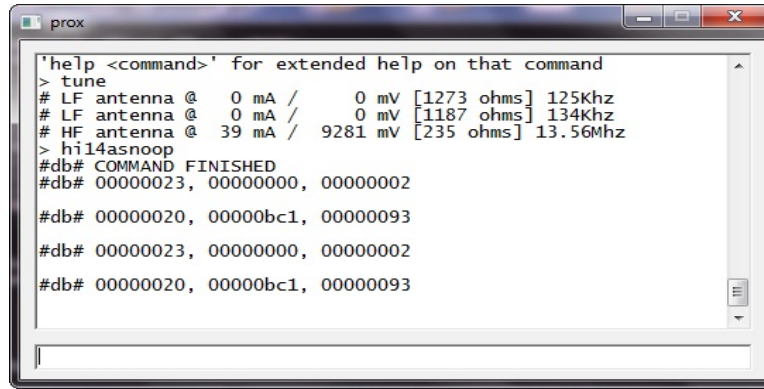
```

Command Prompt - librfid-tool.exe -S
Layer 2 success (ISO 14443-3 A): 04 16 b3 e9 17 02 81
Protocol success (Mifare Ultralight)
Size: 512 bytes
scanning for RFID token...
scanning for RFID token...
Layer 2 success (ISO 14443-3 A): 04 16 b3 e9 17 02 81
Protocol success (Mifare Ultralight)
Size: 512 bytes
scanning for RFID token...
scanning for RFID token...
Layer 2 success (ISO 14443-3 A): 04 16 b3 e9 17 02 81
Protocol success (Mifare Ultralight)
Size: 512 bytes
scanning for RFID token...
scanning for RFID token...
Layer 2 success (ISO 14443-3 A): 04 16 b3 e9 17 02 81
Protocol success (Mifare Ultralight)
Size: 512 bytes
scanning for RFID token...
scanning for RFID token...
Layer 2 success (ISO 14443-3 A): 04 16 b3 e9 17 02 81
Protocol success (Mifare Ultralight)
Size: 512 bytes
scanning for RFID token...
scanning for RFID token...

```

Figure 7.9. Openpcd reader reading tag.

Figure 7.10 shows the encoded tag is sniffed by the proxmark sniffer [12] from 3 cm when the sniffer is parallel to the tag and the reader. Figure 7.11 shows the



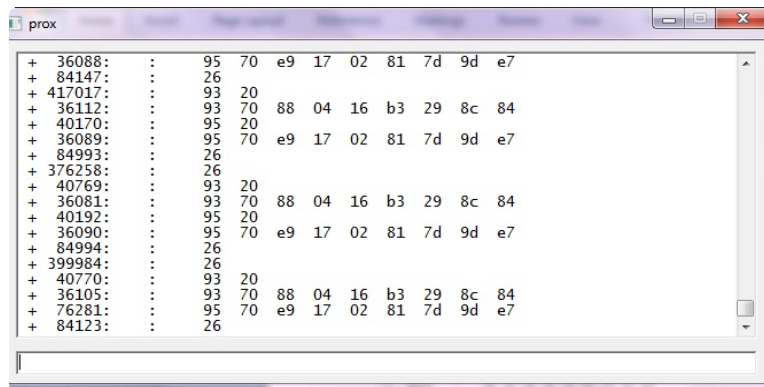
```

prox
'help <command>' for extended help on that command
> tune
# LF antenna @ 0 mA / 0 mV [1273 ohms] 125Khz
# LF antenna @ 0 mA / 0 mV [1187 ohms] 134Khz
# HF antenna @ 39 mA / 9281 mV [235 ohms] 13.56Mhz
> hi14asnoop
#db# COMMAND FINISHED
#db# 00000023, 00000000, 00000002
#db# 00000020, 0000bc1, 00000093
#db# 00000023, 00000000, 00000002
#db# 00000020, 0000bc1, 00000093

```

Figure 7.10. Sniffing encoded tag id.

decoded tag id.



```

prox
+ 36088: : 95 70 e9 17 02 81 7d 9d e7
+ 84147: : 26
+ 417017: : 93 20
+ 36112: : 93 70 88 04 16 b3 29 8c 84
+ 40170: : 95 20
+ 36089: : 95 70 e9 17 02 81 7d 9d e7
+ 84993: : 26
+ 376258: : 26
+ 40769: : 93 20
+ 36081: : 93 70 88 04 16 b3 29 8c 84
+ 40192: : 95 20
+ 36090: : 95 70 e9 17 02 81 7d 9d e7
+ 84994: : 26
+ 399984: : 26
+ 40770: : 93 20
+ 36105: : 93 70 88 04 16 b3 29 8c 84
+ 76281: : 95 70 e9 17 02 81 7d 9d e7
+ 84123: : 26

```

Figure 7.11. Decoded tag id.

7.5 Increasing Sniffing range

Sniffing range can be improved by using a bigger antenna. A more sensitive receiver could be used for eavesdropping which can improve the range of sniffing.

7.6 Summary

In this chapter skimming and eavesdropping attack is discussed and it can be said that skimming attack range is more than the eavesdropping range at low cost.

CHAPTER 8

CONCLUSIONS

This thesis proves that the existing HF protocol is not secure. It is possible to skim RFID smart card from a distance. An adversary can go upto the extent of using a bigger antenna to hack information from a distance. He can also go beyond legal power limits and amplify the transmitted power of the antenna to skim the tag data. Effect of using a bigger antenna and a power amplifier is observed on the skimming range in this thesis. It is seen that six times increase in transmitted power level leads to four times increase in the read range of the legal reader. If this setup is used by an adversary he can glean the information on the tag from a distance without card user's knowledge.

Eavesdropping is done using a proxmark [12] sniffer. It is seen that by using a credit card size antenna it is possible to sniff tag reader communication upto 3 cm from the reader. Sniffing range could be improved by using sensitive receive circuit and a bigger antenna.

Thus, it can be concluded that eavesdropping is less of a concern than illicit reading or skimming because eavesdropping range is smaller for low cost.

REFERENCES

- [1] Y. An and S. Oh. RFID System for User's Privacy Protection. In *Communications, 2005 Asia-Pacific Conference on*, pages 516–519, 2005.
- [2] G. Avoine and P. Oechslin. A scalable and provably secure hash-based RFID protocol. In *Third IEEE International Conference on Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops*, pages 110–114, 2005.
- [3] C.A. Balanis. *Antenna theory*. Wiley New York, 1997.
- [4] S.S. Basat, K. Lim, J. Laskar, and M.M. Tentzeris. Design and Modeling of Embedded 13.56 MHz RFID Antennas. 2008.
- [5] V. Bhavsar, N. Blas, and H. Nguyen. Measurement of Antenna Radiation Patterns Laboratory Manual, 2000.
- [6] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. In *14th USENIX Security Symposium*, volume 1, page 16. USENIX, 2005.
- [7] M.J. Brady, T. Cofino, H.K. Heinrich, G.W. Johnson, P.A. Moskowitz, and G.F. Walker. Radio frequency identification tag, oct28 1997. US Patent 5,682,143.
- [8] M. Burmester and B. De Medeiros. RFID Security: Attacks, Countermeasures and Challenges. *Computer Science Department, Florida State University Retrieved November, 21:2007*, 2007.
- [9] C. Cagliostro. Smart Cards Primer.
- [10] Eurecom R. Molva E. Blass INRIA M. Soos C. Castelluccia Orange Labs M.Robshaw Olivier Billet Jonathan Etrog Iwen Coisel CEA-LETI F. Vacherand,

- O. Savry. RFID-AP, WP1.2 State of the Art. In *RFID Security: State of the Art*, 2009.
- [11] Y.C. Chen, W. WANG, and M. Hwang. Low-Cost RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection. *Asian Journal of Health and Information Sciences*, 1(2):189–203, 2006.
- [12] G. de Koning Gans, J.H. Hoepman, and F. Garcia. A practical attack on the MIFARE Classic. *Smart Card Research and Advanced Applications*, pages 267–282.
- [13] C.A. Domains. Smartcards—An Analysis of History, Security Mechanisms, Implementation Issues, and Future Trends.
- [14] Feig Electronic. ID ISC.ANT300/300-A Manual, 2005.
- [15] em: talk. Microstrip Patch Antenna From Simulation to Realization.
- [16] K. Finkenzerler. *RFID handbook: fundamentals and applications in contactless smart cards and identification*. John Wiley and Sons Inc, 2003.
- [17] S. Garfinkel and B. Rosenberg. *RFID: Applications, security, and privacy*. Pearson Education India.
- [18] S.B. Guthery and T. Jurgensen. Smart Card Developer’s Kit. 1998.
- [19] E.A. Hall, T.H.B. Cranor, and G.J. Schmitt. Microstrip patch antenna with omni-directional radiation pattern, May 1990. US Patent 4,922,259.
- [20] G.L. Hall et al. *The ARRL antenna book*. American Radio Relay League, 1984.
- [21] GP Hancke, KE Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers and Security*, 2009.
- [22] Brita Meriac Kushal Das Harald Welte, Milosch Meriac. Openpcd reader.
- [23] T. Heydt-Benjamin, D. Bailey, K. Fu, A. Juels, and T. OHare. Vulnerabilities in first-generation RFID-enabled credit cards. *Financial Cryptography and Data Security*, pages 2–14, 2007.

- [24] TS Heydt-Benjamin, DV Bailey, K. Fu, A. Juels, and T. OHare. Vulnerabilities in first-generation RFID-enabled credit cards, 2006.
- [25] IPS Canada Inc. RFID 's Smart Card, 2008.
- [26] T. Instruments. HF Antenna Design Notes, Technical Application Report. *Texas Instruments Reports*, pages 11–08.
- [27] Texas Instruments. TRF7960 Evaluation Module.
- [28] ISO-IEC. ISO/IEC 14443. Identification cards - Contactless integrated circuit(s) cards - Proximity cards, 2008.
- [29] A. Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, 2006.
- [30] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pages 74–88, 2005.
- [31] A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In *Financial Cryptography*, pages 103–121. Springer, 2003.
- [32] A. Juels and S.A. Weis. Defining strong privacy for RFID. *ACM Transactions on Information and System Security (TISSEC)*, 13(1):1–23, 2009.
- [33] Paul Graham (K9ERG). A DISCUSSION OF ANTENNA THEORY.
- [34] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard. In *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pages 47–58, 2005.
- [35] I. Kirschenbaum and A. Wool. How to build a low-cost, extended-range RFID skimmer. In *Proc. 15th USENIX Security Symp*, pages 43–57.

- [36] E. Kosta, M. Meints, M. Hansen, and M. Gasson. An analysis of security and privacy issues relating to RFID enabled ePassports. *New Approaches for Security, Privacy and Trust in Complex Environments*, pages 467–472, 2007.
- [37] E. Longo and J. Stapleton. PKI Note: Smart Cards. In *PKI Note Series, PKI Forum*, 2002.
- [38] S. Muir. RFID security concerns. *Library hi tech*, 25(1):95–107, 2007.
- [39] A.A. Note. Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Card.
- [40] D. Paret. *RFID and contactless smart card applications*. John Wiley & Sons, 2005.
- [41] W. Rankl and W. Effing. *Smart card handbook*. John Wiley and Sons Inc, 2003.
- [42] T.A. Scharfeld. *An analysis of the fundamental constraints on low cost passive radio-frequency identification system design*. PhD thesis, Massachusetts Institute of Technology, 2001.
- [43] T.E. Scoughton. Antenna basics. *Microwave Journal*, 41(1):186, 1998.
- [44] R.D. Straw and R. Severns. *The ARRL antenna book*. ARRL, 1997.
- [45] J. Westhues. Hacking the prox card. *RFID: Applications, Security, and Privacy*, pages 291–300, 2005.
- [46] J. Yoshida. Tests reveal e-passport security flaw, August 2004. *EE Times*.

BIOGRAPHICAL STATEMENT

Kirti Chopra was born in Ghaziabad, India, in 1982. She received her B.Sc degree from Delhi University, Delhi, India in 2003, her M.Sc degree from Banasthali Vidyapith, Rajasthan India and MS degree from The University of Texas at Arlington in 2010 in Electrical Engineering. From May 2005 to June 2006 she worked in Centre for Development of Advanced Computing. From August 2006 to October 2007, she served Rockwell Automation India Ltd., Ghaziabad, India. She joined University of Texas at Arlington in August 2008 to pursue her research in RFID. Her current research interest is in the area of RFID security and wireless communications. She is a member of IEEE and honors society Eta Kappa Nu.