uOttawa

L'Université canadienne
Canada's university

t

**FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES**

uOttawa

L'Université canadienne
Canada's university

**FACULTY OF GRADUATE AND POSDOCTORAL STUDIES**

Jose Augusto Lima
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.A.Sc. (Electrical and Computer Engineering)
GRADE / DEGREE

School of Information Technology and Engineering
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Relay Attack in RFiD Systems Analysis and Modeling

TITRE DE LA THÈSE / TITLE OF THESIS

Ali Miri
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

Monica Nevins
CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

Amyia Nayak

Mohamed El-Tanany

Gary W. Slater
Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

# Relay Attack in RFiD Systems Analysis and Modeling

by

Jose Augusto Lima

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

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

*Your file Votre référence*
*ISBN:* 978-0-494-79708-2
*Our file Notre référence*
*ISBN:* 978-0-494-79708-2

# Abstract

A relay attack on an *RFiD* system is carried out by a team of two attackers: one stationed near the victim, and using a rogue Reader to activate the victim's TAG; and another stationed near the legitimate Reader, using a high-speed communication system to relay the communication between the victim's TAG to the legitimate Reader through the attackers in real time.

The relay attack is one of the most significant threats to the security of *RFiD* systems, because it is difficult to detect, is not thwarted by standard challenge-and-response security protocols and is independent of any cryptographic algorithms used to secure the *RFiD* communication.

In this thesis, we present an analysis of the relay attack in an *RFiD* communication system, including an analysis of the many factors which limit the distance at which the attack may be carried out.

A detailed *Simulink* model of an *RFiD* communication system was constructed in the IEEE14443 standard, and used to provide a simulation of the attack. The simulations show the feasibility of the relay attack.

Finally, three relay attack countermeasures are proposed, together with an estimation of the probability of success for each.

**Acknowledgements**

This thesis is the result of several years of research carried out during my time with the *CLICC* lab group. During this period I have had the pleasure of working with a great number of Professors and colleagues whose contributions to my research and the creation of the thesis deserved special mention. It is a pleasure to convey my gratitude to them all in this humble acknowledgment. Most of all, I would like to record my gratitude and thanks to Dr. Ali Miri and Dr. Monica Nevins for their outstanding supervision, advice and guidance from the very early stages of this research, through to its completion. Above all, they provided me with encouragement and support throughout this work. In particular, many thanks go to Raleigh Smith for his valuable scientific discussions, advice and his precious time. I would like to thank my wife Vera Lima and son Rafael Lima for their encouragement and the many hours they were without me.

## Glossary

**AM** Amplitude Modulation

**ADC** Analog to Digital Converters

**ASK Modulation** Amplitude Shift Keying Modulation

**API** Application Programming Interface

**ATQA** Channel Condition Message

**ATS** Answer to Select Message

**AWGN** Additive White Gaussian Noise

**B** Bandwidth

**BER** Bit Error Rate

**BPF** Band Pass Filter

**BPSK Modulation** Bipolar Phase Shit Keying Modulation

**BSC** Binary Symmetric Channel

**CRC** Cyclic Redundancy Check

**BB** Base Band

**DAC** Digital to Analog Conversion

**DSB ASK** Double Side Band Amplitude Shift Keying

**EVM** Error Vector Magnitude

**FF** Far Field

**FFC** Far Field Communications

**FFT** Fast Fourier Transform

**FER** Frame Error Rate

**FSL** Free Space Loss

**FWT** Frame Waiting Time

**FWI** Frame Waiting Interval

**I** In Phase signal

**IF** Intermediate Frequency

**IIP2** Second Order Input Intercept Point

**IIP3** Third Order Input Intercept Point

**IMD** Intermodulation Distortion

**IP** Intellectual Property

**ISO** International Standards Organization

**ISM band** Industrial, Scientific and Medical band

**IMR** Intermodulation Ratio

**LNA** Low Noise Amplifier

**LAN** Local area network

**LMS** Least Mean Squares

**LO** Local Oscillator

**MEMS** Microelectromechanical Systems

**MAC** Medium Access Controller

**MIL-STD462** Military Standard 462

**MTBF** Mean Time Before Failure

**NF** Near Field

**Nf** Noise Figure

**NFC** Near Field Communication

**NRZ** Non Return to Zero

**OIP2** Second Order Output Intercept Point

**OIP3** Third Order Output Intercept Point

**OOK Modulation** On Off Keying Modulation

**OTS** Off The Shelf

**OSR** Oversampling Rate

**PA** Power Amplifier

**PAM** Pulse Amplitude Modulation

**PCD** Proximity Coupling Device

**PICC** Proximity Cards

**PN** Phase Noise

**POS** Point of Sale

**PSK** Phase Shift keying

**QAM** Quadrature Amplitude Modulation

**QL** loaded Quality Factor

**QPSK** Quadrature Phase Shift Keying

**RATS** Request to Answer Selected

**RF** Radio Frequency

**RL** Return Loss

**RZ** Return to Zero

**RFiC** RF integrated circuit

**RFiD** Radio Frequency Identification

**REQA** Request for Acknowledgment

**RRC Filter** Root Raised Cosine Filter

**SEL** Select Message

**SAK** Select Acknowledge

**SINR** Signal to Interference plus noise ratio

**SISO** Single Input Single Output

**SNR** Signal to Noise Ratio

**TEM** Transverse Electric Magnetic

**UHF** Ultra High Frequency

**WiFi** Wireless Fidelity

**WiMAX** Worldwide Interpretability for Microwave Access

**Z** Impedance

**Z0** Characteristic Impedance

$\beta$ Electrical length per meter

$\lambda$ wavelength

$\epsilon_0$ Permittivity of free space

$\eta_0$ Free space impedance

$\eta$ AWGN

$\eta_t$ total noise

# Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

Radio-Frequency identification *(RFiD)* is fast becoming the lowest cost tool to provide secure and anonymous identification of individuals. Every day people use *RFiD* tags to gain access to restricted areas, to use restricted equipment as well as to make financial transactions at gas stations, cafeterias and the famous Canadian Tim Hortons. This technology is also used for highly sensitive authentication devices including passports. However, with the ever-increasing use of this technology comes the inevitable question of the security of the transaction and the authentication of the person that is trying to use the system.

During normal operation the system consists of a Reader and *TAGs* [15] . A *TAG* is used by someone to gain legitimate access to a restricted area. The *Reader* is located at the access point of the restricted area and continuously sends carrier to energize the *TAG* and poll for a response from the *TAG*. The *TAG* uses energy from the received carrier to respond to the *Reader* and handshaking between *Reader* and *TAG* is used to validate the *TAG*. If the *TAG* is valid the user gets access to the restricted area.

Relay attack [19] takes place in a following manner. Assume the victim *TAG* is far away from the point of access. There are two attackers: One with the rogue *TAG* near the reader at the point of entry; and one with the rogue *Reader* near the victim. The rogue *Reader* needs to be far enough away from the victim to evade detection, but close enough to successfully carry out the attack. The two attackers establish a communication system to relay in real time the handshaking messages without having to decrypt them; and thus, gain access to the restricted area.

*RFiD* systems have many potential vulnerabilities, including decryption of the authentication data, *TAG* theft and physical layer attacks [19], [43]. Decryption presents a challenging problem: the successful attacker requires a high level of sophistication, as well as complex equipment. Furthermore, the attacker, victim and rogue *Reader* all need to be in close proximity for the attack to succeed. The theft of a *TAG* is an immediate and obvious threat [42], but this attack succeeds only until the theft is detected. Physical layer attacks are intended to circumvent the cryptographic protection on the *RFiD* system while at the same time being undetectable by the victim.

The most insidious physical layer attack is the relay attack, which is described in detail in Chapter 2. A successful relay attack is dependent on Victim Distance and the delay added by the attacking system. This thesis focuses on the following:

- An estimation of the maximum distance the attacker can be positioned from the victim (Victim Distance)
- A simulation of the communication between attacker's rogue Reader and Victim's TAG
- An estimation of the maximum delay the attacker's system can introduce and carry out an attack successfully

In addition to its invisibility to the victim, and its orthogonality to the security algorithms of *RFiD* systems, the relay attack is superior to other known physical attacks, such as replay attack [43], because it cannot be overcome by standard countermeasures such as time-stamping, or challenge-and-response protocols[20]. That said, mounting a relay attack poses significant challenges [60], including overcoming signal loss and the interference between the transmit and receive antennas of the rogue Reader, as well as performing within the maximum system delay time defined by the ISO standard communication protocol[15]. These challenges are addressed in Chapters 3 through 5. If and when these challenges can be overcome by an attacker, the actual relay attack will be very hard to thwart. Therefore, gaining a better understanding of the challenges faced by a potential attacker, and constructing effective countermeasures, represent an important and active area of research.

In this thesis we present the most important impairments and device imperfections that affect practical *RFiD* relay attack systems. We provide a mathematical analysis of such attacks as well as a *RFiD* simulation tool, built using *Simulink*, that implements

*ISO14443* type A protocol. We use this to give simulation results of an attack and to demonstrate the effectiveness of novel countermeasures that minimize the success of this type of attack.

The scientific contribution of this thesis is a complete theoretical analysis that provides the groundwork for the *Simulink* model and simulation of the relay attack. We also show the extent of the vulnerability of the *RFiD* devices to relay attack. The novelty of this work is in presenting a detailed analysis of the *RFiD* systems when they are under relay attack; and the design of a model to simulate the communication between attacker and *Reader* during the attack.

**Organization of this Thesis**

Chapter 2, Background, presents the foundations of this technology including the discussion of several types of side attacks. We describe the modulation used by various standards and give an overview of the system used during a possible relay attack. This chapter provides a comprehensive overview of the characteristics of existing *RFiD* systems and their vulnerability to relay attack, and was published as a book chapter [60, Ch4].

In Chapter 3, Communication Channel, we study the communication channel for the *ISO14443* standard. The importance of this chapter is to provide the required information for the analysis of the relay attack. We determined the boundary between the Far and Near Field regions in the *Victim Distance* to ensure that Friis analysis can be applied to model the electronic system used during an attack.

In Chapter 4, End to End *RFiD* Systems Analysis, we provide relevant information about the result of the imperfections of electronic devices in the overall system performance. This includes *RF* imperfections as well as imperfections in baseband blocks such as *ADCs* and *DACs*. This chapter shows the independent contribution of each imperfection and the overall system performance degradation when all imperfections are considered. It is of fundamental importance in the analysis of the performance of the attack.

In Chapter 5, Relay Attack Model and Simulation Results, we present the details of the relay attack on *RFiD* devices. The effect of the attacker's relay system delay on the overall performance and success of the attack is shown. The maximum delay allowed for the attacking system to be successful is calculated. Furthermore, we present

analysis and simulation of the boundaries of the activation distance and reading range.

Chapter 6, Countermeasure Techniques for Relay Attack, presents three hardware counter-measurers for relay attack. One of the big advantages of these methods as compared with MAC based methods [20] and methods that use better cryptography, as suggested by Heydt-Benjamin *et al* in [23], is that they are backwards compatible with existing systems. Two of the methods presented in this chapter are novel. Comparison among these methods is also given.

Since *RFiD* technology is widely used, new devices and new requirements must evolve at a fast pace, so in Chapter 7 we present some directions in which the work of this thesis may be extended.

An overview of *ISO14443* standards and requirements is given in Appendix A in order to provide a basis for understanding the details behind the communication between *TAGs* (also know as PICC, or Proximity Cards) and *TAG* readers (also known as PCD, or Proximity Coupling Devices).

# Chapter 2

# Background

## 2.1 Introduction

*RFiDs* are widely used in devices such as access cards. An *RFiD* system is any Radio Frequency Identification system composed of one or more *TAGs* which are distributed within the population of users and one or more *Readers* that interact with and identify the *TAGs*. *RFiD* allow a user, who is in possession of a *TAG*, to validate himself to a (powered and usually immobile) *Reader*, with a minimum of interaction, a minimum of delay, and often no physical contact between the *TAG* and *Reader*. What is required is only that the *TAG* is placed close enough to the *Reader* to conduct the required electronic communication.

The growth in use of these devices worldwide has been exponential. Since in many cases, these systems are used for identification, their security is an extremely important consideration. We consider various kinds of attacks, including principally the relay attack, in Section 2.2, below.

Figure 2.1 depicts a typical *RFiD* communication system, which consists of a *TAG*, a *Reader*, and a server. Note that in an *RFiD* system, one needs to consider not only the communication system itself, but also the power needed by the *Reader* to be able to activate a passive *TAG*. This value is greater than the power required for the communication system to achieve a required *SNR* and operate properly. In particular, many of the commercial systems use passive *TAGs*, which do not have their own power source, and need to obtain their energy via the *Reader*'s carrier. As a result, during normal operation (not under relay attack) they can usually communicate with *Readers* no further than 1 meter away. This restricted passive *TAGs* range of operation

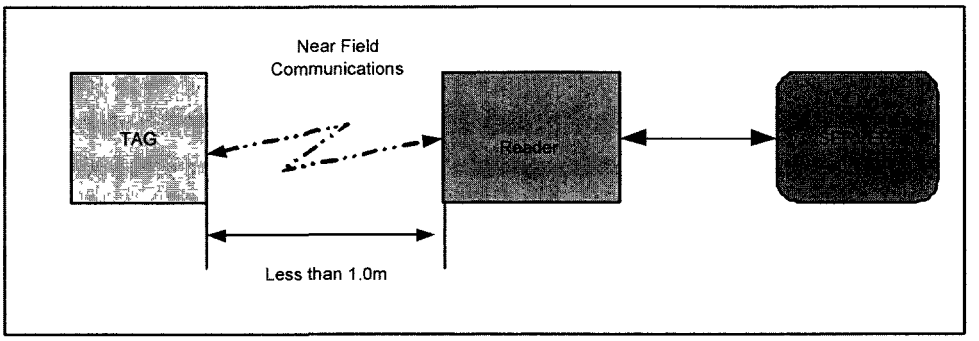


Figure 2.1: *RFiD* communication system

is often considered an addition to the security of the underlying *RFiD* system. Table 2.1 provides an overview of the frequency spectrum usage for typical *RFiD* applications. In this thesis, we focus on the *ISO14443* standard, which uses the 13.65MHz frequency band.

| Frequency band | Characteristics | Applications |
|---|---|---|
| 100 to 500 KHz | Short to medium range<br>Very low throughput | Access control, inventory<br>information, animal control |
| 12 to 13 MHz | Short range | Access control, smart cards |
| 900 MHz | Medium reading speed | Access control, smart cards |
| 2.45 and 5.8 GHz | Long range<br>Higher speeds | Vehicle identification,<br>toll collection |

Table 2.1: Frequency Spectrum Usage of *RFiD*

This chapter unfolds by introducing in Section 2.2 the *RFiD* vulnerabilities and the relay attack. We give a thorough description of an *RFiD* system in Section 2.3. Section 2.4 describes the main block constituents of the *Simulink* model of an *RFiD* system developed for this thesis.

## 2.2 *RFiD* Vulnerabilities and the *Relay Attack*

In this chapter, we introduce the principal concepts of several schemes used to attack the systems that use *RFiD* devices but we will focus primarily on so-called relay attacks. A theoretical relay attack analysis is provided together with details of its implementation. The purpose of this study is twofold: firstly, to provide a deeper understanding of *RFiD* vulnerabilities; and secondly, to serve as a background for the further analysis of security solutions needed to counter such attacks.

We consider only the scenarios in which the victim remains in possession of the *TAG* and he/she is not aware of the attack. These attacks belong to the class of physical layer attacks and they have the characteristic that they are carried out without the need of decoding any cryptographic key that may be used by the system.

The basic premise of a relay attack is similar to that of a man-in-the-middle attack. Given that a (passive) *TAG* is powered and responds to any *Reader*, an adversary can use a rogue *Reader* to initiate and establish the communication with a legitimate *TAG*. Information learned can then be relayed to a fake *TAG* (possibly at a great distance away) that can communicate with the legitimate *Reader* as a clone of the legitimate *TAG*. This type of attack can be performed without the legitimate *TAG* holder's knowledge. However, the attack needs to be done without introducing significant system delay, as this could foil the attack, see Section 5.2 for details.

In an example relay attack that involves a pair of colluding adversaries, adversary **A** and adversary **B** agreed to perform a purchase in the name of an innocent Speed Pass user herein called the victim. Adversary **A** (attacker) carries the rogue *Reader* and adversary **B** carries the rogue *RFiD TAG*. **A** gets within range of the victim and relays the information to adversary **B** who will buy goods using the real time relayed information collected from the victim by **A**.

As relay attacks are the focus of this thesis, let us now give a broad overview of various issues with regard to the modeling and implementation of this type of attack, as well as its implications to the users of *RFiD*-enabled devices.

### Relay Attack Characteristics

There are three major characteristics that make relay attack more difficult to circumvent over other types of *RFiD* attack systems. These are as follows:

- Contactless cards operate over a distance, which allows the attacker to position himself at some distance from the victim
- *TAG* activation is automated - there is no human intervention in the system
- The attacker does not need to decode the transmitted information, in other words, the secret key remains secret. This characteristic provides orthogonality for all the security cryptographic systems used in *RFiD*.

### Relay Attack System

Relay attack is an important area of research. Different work in the literature such as [19] and [23], have published information about the attack and its constraints. Many of these works have focused on the distance between the victim and Point of Sale *(POS)* herein *Relay Distance*. Reading range and activation range are two other distances that bound the maximum distance between *TAG* and rogue *Reader*, herein *Victim Distance*. Our work explores many factors which limit the victim distance at which the attack may be carried out. To perform the attack with success, the attacker has to overcome two main constraints. The first one is the inherent delay of the communication system responsible to relay the information. *ISO14443* establishes a maximum response time from the *TAG* when it is interrogated by the *Reader*. The second one is to assure proper data transfer during the communication between valid *TAG* and rogue *Reader* (Victim and attacker).

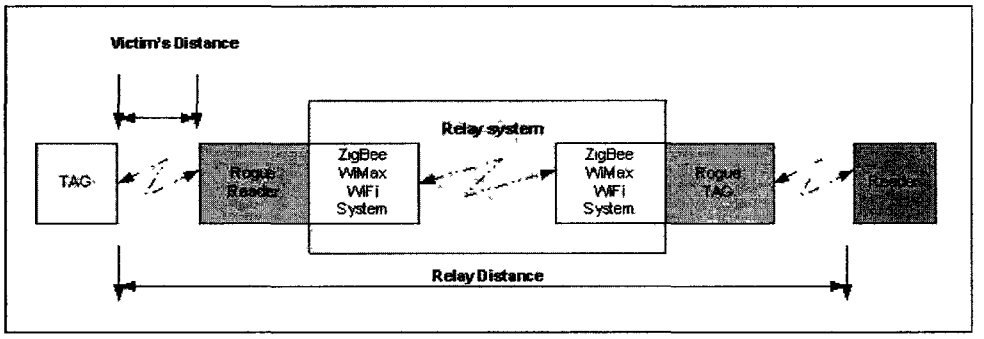


Figure 2.2: Relay attack system

The attacker's system in this case is depicted in Figure 2.2. Here, the system is composed of a rogue *Reader*, a " long distance" communication system, and a fake *TAG*. The choice of communication system depends on the distance over which the

relay needs to take place. In today's technologies, for short distances, the attacker could use *ZigBee* or *WiFi*, whereas for longer distances, *WiMax* or other cellular technologies would be more appropriate. That said, for longer distances delay issues may have to be addressed. It is worth noting that in practice the distance between rogue *TAG* and *Reader* is taken to be as small as necessary, given that the objective of the attack is to place adversary **B** close to the *Reader*, to gain illicit access.

## 2.3 *RFiD* System

In the first part of this section we describe the electrical characteristics of *TAGs* with respect to power consumption. In the second half we present the general hardware and firmware functionality of the *RFiD* system.

### 2.3.1 Characteristics of the Tags

Some *TAGs* have their own source of power but other ones need to receive a minimum amount of power to be energized and consequently be in operational state (*TAG* activation power). The information presented in this section is used in Chapter 5 during the analysis and model construction of the *RFiD* system.

#### Passive *TAGs*

Passive *TAGs* do not carry a battery. Therefore they need energy to be activated and part of the received energy (AC signal) is back-scattered to the *Reader*. Many of these *TAGs* use a robust type of modulation (see Section 2.3.2) and they operate in the near field of the antenna but others will operate in the far field.

#### Passive Illuminated systems

Passive *RFiD* systems generally suffer from poor communication reliability (high *BER*). This usually occurs due to the low signal level transmitted by the *TAG* to the *Reader* and the local interference resulting from the continued transmission of the carrier by the *Reader*. (Details about local interference, and a solution to the problem is proposed in Chapter 5.3.1). Passive Illuminated systems mitigate the carrier feedthrough interference generated by the *Reader* into the receiver in the presence of the *TAG*.

Passive illuminated systems use *TAGs* that do not carry batteries. Therefore to activate them, they must collect energy from an active device called the illuminator. This active device is usually located far from the *Reader* but it needs to be closer to the *TAG* for the *TAG* to be able to receive enough energy and be activated. The advantage of the system is to be able to operate at greater distances than the systems using passive *TAGs*. It also eliminates the need for the *TAG* to carry a battery, reducing its cost.

The advantage of using passive illuminated systems is that they are backwards compatible with existing systems. The system also offers an advantage when the *RFiD* frequency increases. If the frequency increases, the free space attenuation will also increase, which increases the energy required by the *Reader* to transmit and still be able to energize the *TAG*. By using passive illuminated systems, one does not need to increase *Reader* energy to activate the *TAG*. This idea is presented in [30].

For relay attack specifically, the attacker may want to use an additional transmitter to activate a passive *TAG* (mimicking a passive illuminated system) which can improve the performance of the attack, however, this will make the attack more localized in terms of area.

When comparing passive illuminated and passive systems from the relay attack point of view, the following advantages and disadvantages can be pointed out.
Advantages of Passive Illuminated Systems

1. Increases the distance between victim and rogue *Reader* (*Victim Distance*)
2. Decreases the interference suffered by the *Reader* receiver when receiving the *TAG* signal

Disadvantages of Passive Illuminated Systems

1. Needs more hardware
2. Reduces the opportunity and window for attack due to the necessity of having the illuminator in close proximity of the victim.

**Active *TAGs***

Active *TAGs* carry a small battery so they do not need to receive energy from the *Reader* to be activated.

### 2.3.2 Hardware and firmware functionality

We begin this section by considering a general communications system, as shown in Figure 2.3. Using this general system and all its building blocks, we can then explain some of the existing *RFiD* protocols currently available in the marketplace. Most of them are developed using *NFC* (Near Field Communication) that uses both passive and active tags but others are based on *FFC* (Far Field Communications) and most of them only use active *TAGs*. Both systems (*FF* and *NF*) yield to similar analysis, with some modification to the requirements and assumptions. In this section we present some high level block diagrams that will used for the modeling that are described in details in Chapter 5.

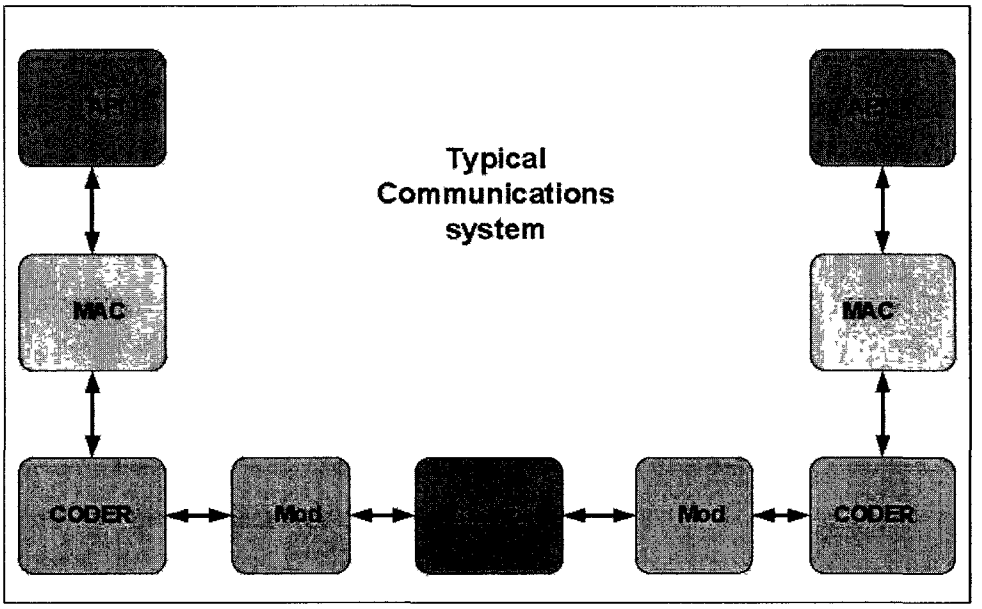


Figure 2.3: Typical communications system

#### Application Programming Interface (API)

In a general terms, the application software (**API**) is a simple piece of software designed to provide an interface to allow the end user to communicate with the *TAGs*, as well as possibly high-level software applications. In *OTS* (Off-The-Shelf) systems, the **API** is typically stored in the *Reader* only, as the cost of the *TAGs* and their simplicity make it prohibitive for them to support any software. In general, the intelligence contained in the *TAG* is resident in hardware because passive devices are designed with very

low power level requirements, and operate without the need of an internal battery. Thus this implies high power requirements for a valid *Reader* transmitter, although this transmitted power must be within the limits stated in [14]. If the system containing a rogue *TAG* and rogue *Reader* is designed for carrying out an attack the design is not limited by cost so we may assume the rogue *TAG* and rogue *Reader* have capabilities to store and run the amount of software that it is needed.

### Initialization and anti-collision protocol (MAC)

The *MAC* (Medium Access Controller) is also a simple layer that takes care of the initialization and anti-collision protocols. Figure 2.4 shows the state diagram for an ISO 14443 type *TAG*. When a *TAG* is placed close to a *Reader*, it receives power and it changes its state from OFF to IDLE. From time to time, the *Reader* sends a *REQA* (Request for Acknowledgement) command, and upon the acknowledgement of this command, the *TAG* will go into the *READY* state. If more than one *TAG* is present in the vicinity of the *Reader*, the *Reader* senses the presence of multiple cards and the anti-collision algorithm selects one of the cards, using a tree search algorithm, to put in an *ACTIVE* state. The *TAG* will go into *HALT* state either on *HALT* command [15]

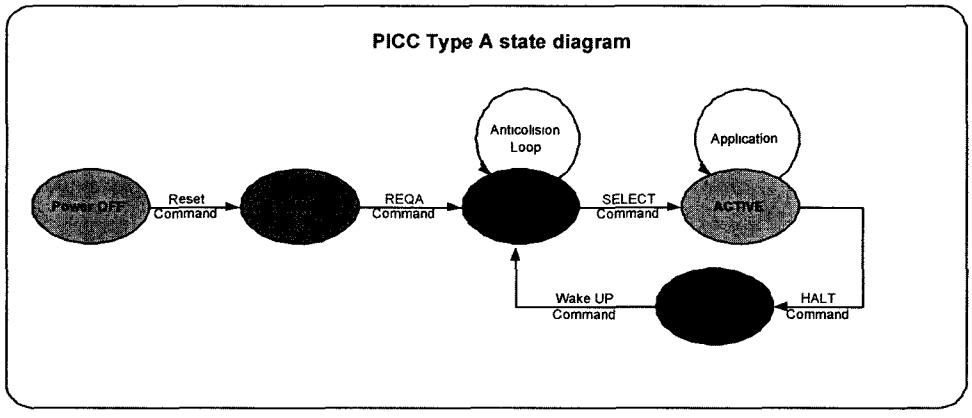


Figure 2.4: *PICC* type A state diagram (taken from [15])

or on an application-specific command. The *TAG* will need a *WAKE-UP* in order to get out of *HALT* state at a later time.

Figure 2.5 depicts the initialization process which includes an anti-collision protocol. To illustrate how the process works, let us assume that the passive *TAG* is positioned close to the *Reader* and it is already in the *IDLE* state. At this state, the

*TAG* is already energized and starts searching for a *REQA* message from the *Reader*. As long as it does not receive the *REQA* but is receiving energy from the *Reader*, it continues in this state. Once the *REQA* message is received, the *TAG* goes into *READY* state and sends back the channel conditions to the *Reader* using an Channel Condition Message (*ATQA*). The channel conditions message shall inform the *Reader* whether the communication between *TAG* and *Reader* can be established or not.

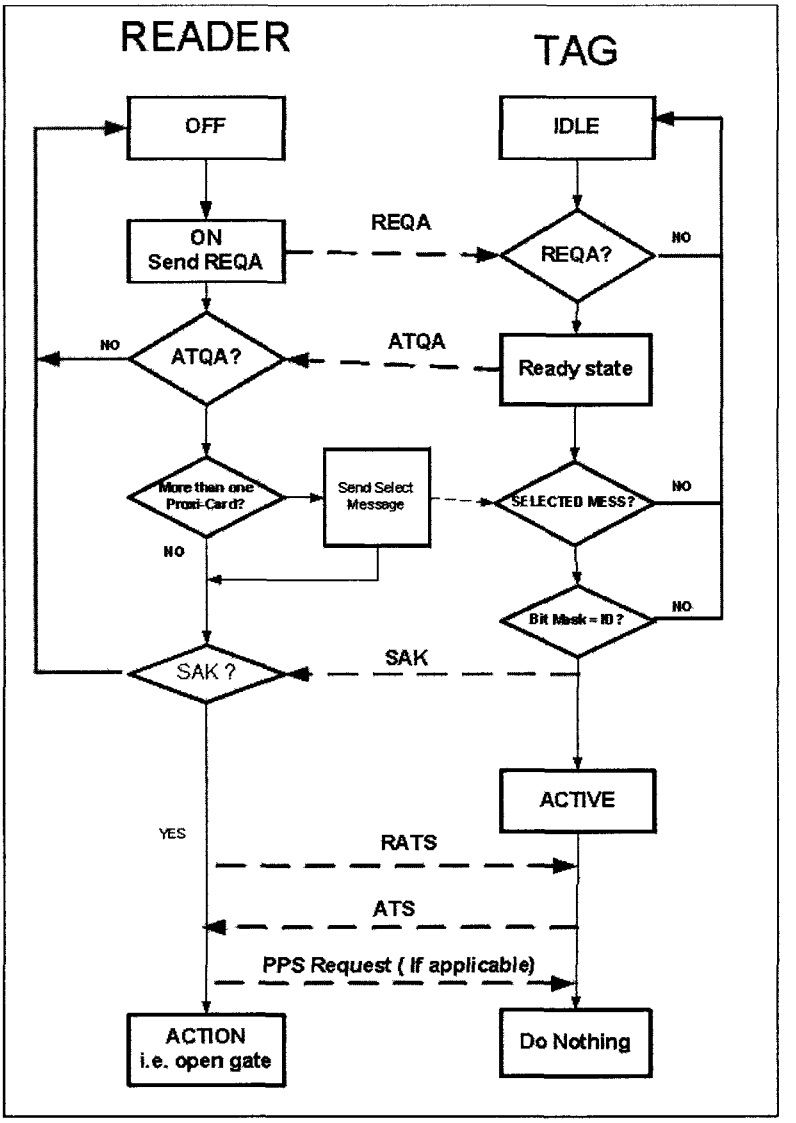


Figure 2.5: Initialization and anti-collision flow chart (Taken from [15])

If the channel condition is such that the communication can be started, the *Reader* will check to see whether it has received more than one *ATQA* message, in which case

it has to select one of the present *TAGs* to continue the communication process. The selection message is then broadcasted and only one *TAG* will be selected. If a particular *TAG* receives the *SELECT* message and it is not the one that has been selected by the *Reader*, it will go back to *IDLE* state. The chosen *TAG* will acknowledge the *Reader* by sending back a *SAK* (Select Acknowledge) message, and will move to *ACTIVE* state. The *Reader* then will send a *RATS* (Request to Answer Selected) message to the chosen *TAG*, asking for an *ATS* (Answer to Select) message. The *Reader* will send to the *TAG* a protocol parameter selection message, if there is more than one protocol available to be used. After the selection is done, standard protocol messages are exchanged between *Reader* and *TAG* [15]. It is driving this communication channel that the *TAG* authenticates itself to the *Reader* using possibly encrypted data.

### Modulation Used in *RFiD*

The modulation scheme used in *RFiD* is usually a very robust [1] modulation type. Even if there is no information to be sent, the *Reader* usually transmits pure carrier in order to provide power for the *TAG*. For *ISO14443A/B*, modulation and coding are described in Table 2.2.

To provide background information about the modulation schemes most used in *RFiD* systems, several modulation types and their characteristics are described in detail below.

[1] Very robust in the text means that the demodulator will be capable to demodulate the received signal without errors at very low sinal to noise channel environment when compared for example with multilevel modulations e.g., quadracture amplitude modulation (QAM)

| Direction | Characteristic | Type A | Type B |
|---|---|---|---|
| *Reader* to *TAG* | Modulation | ASK | ASK |
| | Modulation Index | 100% | 10% |
| | Coding | Modified Miller | *NRZ* |
| | Transmission Rate | 106Kbps | 106 Kbps |
| *TAG* to *Reader* | Modulation | *OOK* | *BPSK* |
| | Modulation Index | 100% | NA |
| | Coding | Manchester | *NRZ* |
| | Transmission Rate | 106Kbps | 106 Kbps |

Table 2.2: ISO 14443 A and B differences (Information taken from [15])

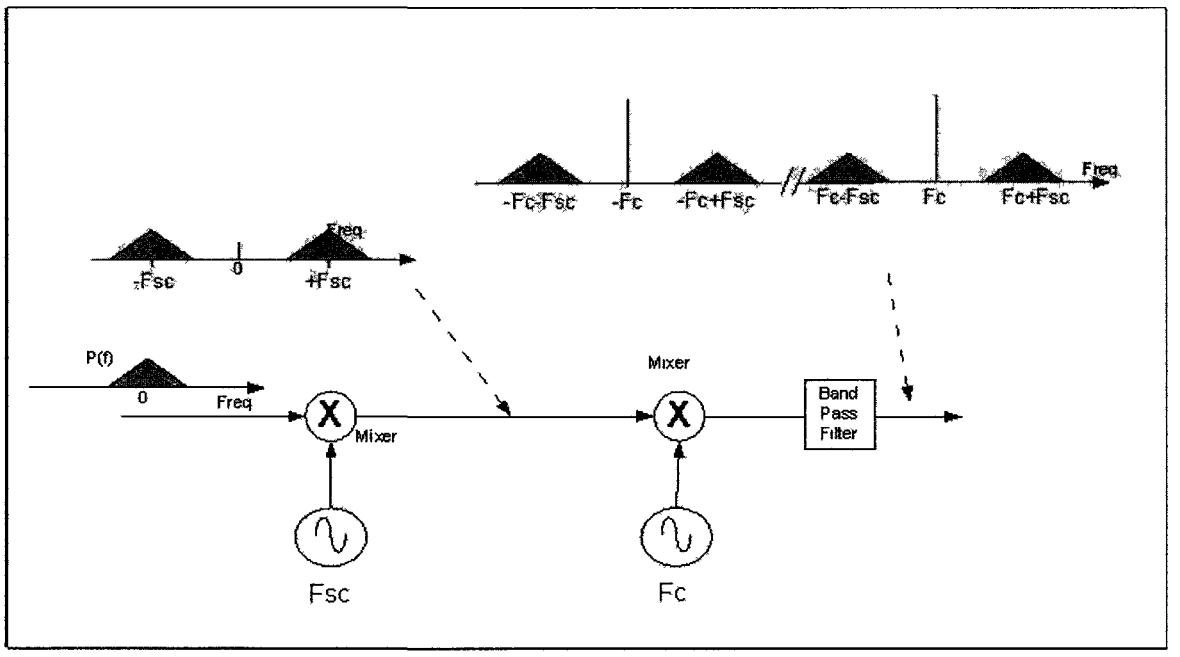


Figure 2.6: Modulator model

Figure 2.6 depicts a typical modulator model and a superheterodyne up-converter. The first mixer moves the serial stream $p(t)$ into the sub-carriers' frequencies and the second step is to move the signal to the carrier frequency (in this case, $f_c$ = 13.56MHz). For communication between the *TAG* and *Reader* for either type A or B, the standard *ISO14443-2* states that the sub-carrier frequencies $f_{sc}$ shall satisfy $f_{sc} = f_c/16$ (about 847KHz).

The use of the mixer is only for modeling purposes. In an actual design, the mixer function may be designed not as explicitly as in the model depicted by Figure 2.6. Instead it may be built in a such way that the designer takes advantage of the non linearity of some components to perform the mixer function. Also notice that there is no base-band filter or amplifier in this diagram; these blocks will be shown in detail in Chapter 4.

Let us now give an overview of the different modulation types used in *ISO14443*.

***OOK* - On Off Keying** This type of modulation is implemented by turning the carrier on and off in accordance with the data to be transmitted. During the demodulation process, it is very robust to *SNR* (signal to noise ratio), phase noise and *RF* non-linearity effects that otherwise usually generate degradation of communication systems, see Chapter 4 for details.

Figure 2.7 depicts an *OOK* modulation constellation. Notice that in the signal space, there are only two positions in which the carrier will be landing (indicated by dark dots in Figure 2.7: either at the origin or at maximum amplitude. Mathematically, the modulated *OOK* signal $s(t)$ can be represented by

$$s(t) = p(t)\cos(2\pi f_c t + \Phi) \tag{2.1}$$

where $f_c$ denotes the carrier frequency, $\Phi$ is a given arbitrary constant representing the phase and $p(t)$ is the multiplicative coefficient function of the coded bitstream which will define the value of the carrier frequency for a given bit to be transmitted. This multiplicative factor will assume only two different values during the transmission before the base-band filter and it is defined as per

$$p(t) = \begin{cases} 1 & \text{if logic state} = 0; \\ 0 & \text{if logic state} = 1. \end{cases} \tag{2.2}$$

For random transmitted signals, using *BSC* (Binary Symmetric Channel) type com-

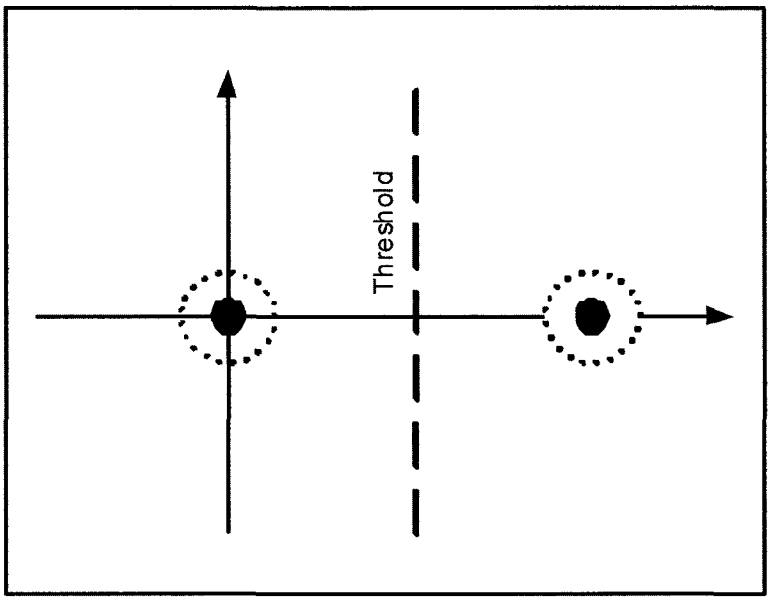


Figure 2.7: On Off Keying constellation ($s(t)$)

munications systems and under *AWGN* (Additive White Gaussian Noise), the threshold value used by the decoder is usually half of the bit energy transmitted [40, Ch4].

***BPSK* - Bipolar Phase Shift Keying** *BPSK* is another type of modulation and it is used for ISO 14443 type B. This modulation scheme modulates the carrier by changing its phases into two values as a function of the input serial data stream. Let $\phi_1$ and $\phi_2$ denote two distinct phases; these are usually chosen to be either zero and 180 degrees. Let $A$ be the maximum amplitude of the signal, $f_c$ be the carrier frequency, $p(t)$ be the coded information bitstream and $\Phi$ be the carrier phase function, which is defined by

$$\Phi(p(t)) = \begin{cases} \phi_1 & \text{if logic state} = 0; \\ \phi_2 & \text{if logic state} = 1. \end{cases} \tag{2.3}$$

Then the modulated *BPSK* signal can be represented by

$$s(t) = A\cos(2\pi f_c t + \Phi(p(t))). \tag{2.4}$$

Figure 2.8 shows the constellation for *BPSK* and the threshold values used by the detector on the received side for a hard decision decoder type. Decoder details are not in the scope of this chapter but the interested reader can refer to [40, Ch4].

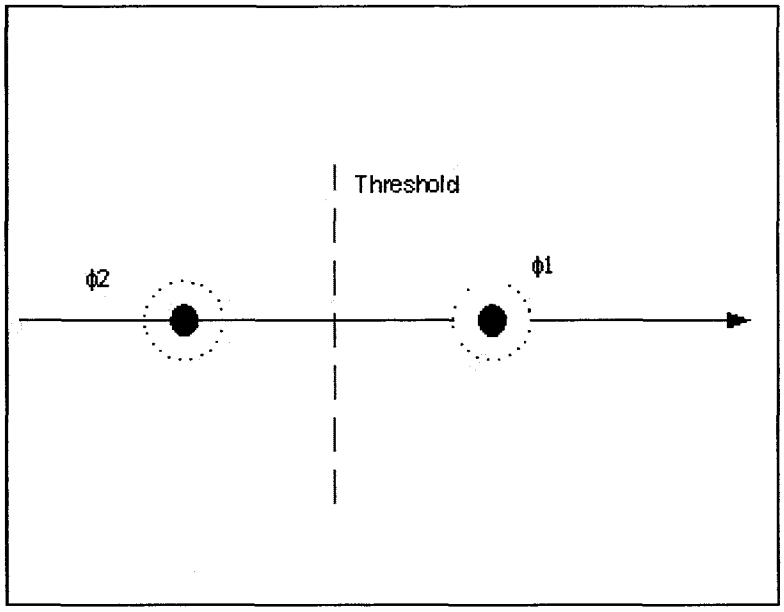


Figure 2.8: BPSK Constellation

***ASK* - Amplitude shift keying** This type of modulation can be thought as bi-level AM (Amplitude Modulation). The carrier assumes two distinct values of amplitude as a function of the input signal. In contrast, the phase of the transmitted signal does not change as a function of the input serial bitstream. Figure 2.9 depicts the constellation for this type of modulation.

Let $k$ be a constant, $0 < k < 1$, that determines the ASK modulation depth, $f_c$ be the carrier frequency, $\Phi$ represents the phase (a constant) and $p(t)$ is the multiplicative coefficient function of the coded bitstream, which is assumed to take on only two values.

Mathematically, the modulated ASK signal can be represented by

$$s(t) = [1 + kp(t)]\cos(2\pi f_c t + \Phi). \tag{2.5}$$

### Demodulation

All three types of modulation (*OOK*, *BPSK* and *ASK*) can be detected using a non-coherent demodulator. These types of demodulators are of simple implementation but there will be performance degradation if compared with coherent demodulation, see [40, Ch4].

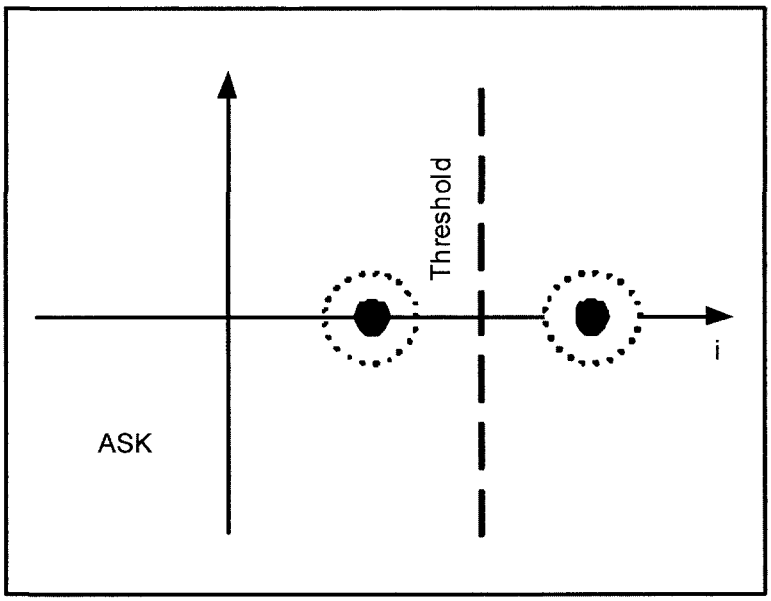


Figure 2.9: ASK constellation

Figure 2.10 shows a simplified demodulator for *ASK*. The received signal is integrated over the period $T$ and squared. Notice that neither carrier nor timing recovery has been included in this demodulator block diagram. As a result, the received signal can be directly multiplied by in-phase and in-quadrature local oscillator and then be integrated over the symbol period $T$ and squared. A threshold value is used for the detector in order to estimate the symbol value that was received. [40, Ch4] provides detailed analysis of the threshold detection for general purpose demodulators.

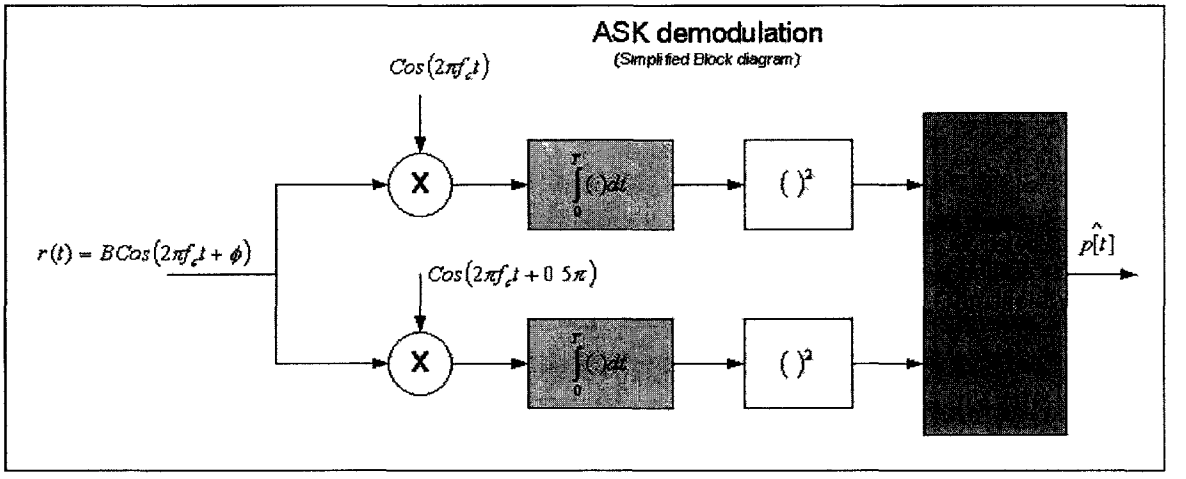


Figure 2.10: *ASK* demodulator

## 2.4 Modeling

*RFiD* is a mature technology that many Integrated Circuit companies have included as part of their portfolio. Consequently many *RFiD* models for systems, subsystems and circuits already exist. However, these *RFiD* models are not available in the public domain due to intellectual property (IP) protection rules. Models that are available in the public domain, some of which are listed below, serve as the foundation for this thesis. The model developed during this work is based on a legacy system (*ISO14443*) and it is developed for the purpose of verifying the feasibility of a relay attack and identifying security measures to protect the system from this attack. Even if the model is targeted for security it can also be used for activation and reading range simulations as well as considering impairments such as RF imperfections, noise and interference. By applying small modifications, the model can be used for *ISO18000-6*, also called *EPCglobal*[2] Gen2, the newly adopted standard that operates in the ultra high frequency (UHF) band.

The model presented here can also be easily modified to target different standards as they evolve. The tool used to develop it is Matlab/Simulink[3], which is a tool widely used in universities, research centers and industry. Many engineers are familiar with this tool and it is the tool of choice.

Depending on the level of accuracy that we are trying to achieve, the system can be modeled in several different ways. A vast amount of literature is available showing generalized *RFiD* system model implementation techniques; however, none tackle relay attack. Most of the related work, such as [12], [34] and [51], describe the different methodologies of modeling *RFiD* with the purpose of circuit level design targeting functionality risk mitigation. There are other works, such as [21], [3], [55], [53], that target *RFiD* antenna design and [24] that presents a model for *RFiD* low power integrated circuit. In the channel model area we find the paper from Malison [52]. A number of network simulators have been developed in the past including [9] and [13], that present a simulation engine that implements *ISO18000-6C* protocol and supports path loss backscattering. It is more suitable for relative comparison of different medium access protocols, transmission control strategies and settings in *ISO18000-6C*. There is also the network simulator Ns2 [10], which has been long used for wireless network protocols simulation and is in the same class of simulators as the

[2]EPCglobal Inc is a global not-for-profit standards organization for Electronic Product Code.

[3]The Mathworks, Inc.

GloMoSim [4][1], which is written in Parsec [31] and has been extensively used in adhoc networks.

These simulators have been successfully used in simulating networking, routing and protocols, which differ from the purpose of simulating the physical layer. The *RFiD* simulation model from Auto-ID Labs [18] addresses the physical level model; however, the simulator form Auto-ID Labs is limited to an specific standard (*ISO18000*). None of the available simulators could take in account the system delay, standardized handshaking messages, RF impairments and other factors necessary to mimic the relay attack system simulation. Thus, we had to develop the model presented in this section.

### 2.4.1 *Simulink* Model

In this section we present details of the model developed in *Simulink* and the boundaries (Rogue *Reader* to Victim's *TAG*) of the model for the relay attack. Figure 2.11 depicts the relay attack as well as the section of the attack that is simulated by the model. One observes that the model was developed to mimic the communication between rogue *Reader* and Victim's *TAG*. The relay attack system is divided into three parts: The rogue *TAG* to *Reader*, relay system and rogue *Reader* to victim's *TAG*. Only the rogue *Reader* to Victim's *TAG* section has been modeled because it is the only part of the system with unknown performance. The rogue *TAG* to reader and relay sections are existing systems of known performance.

The *Reader* and *TAG* top block diagrams are depicted by Figures 2.12 and 2.13 respectively.

[4]GloMoSim: Global Mobile System Simulator.

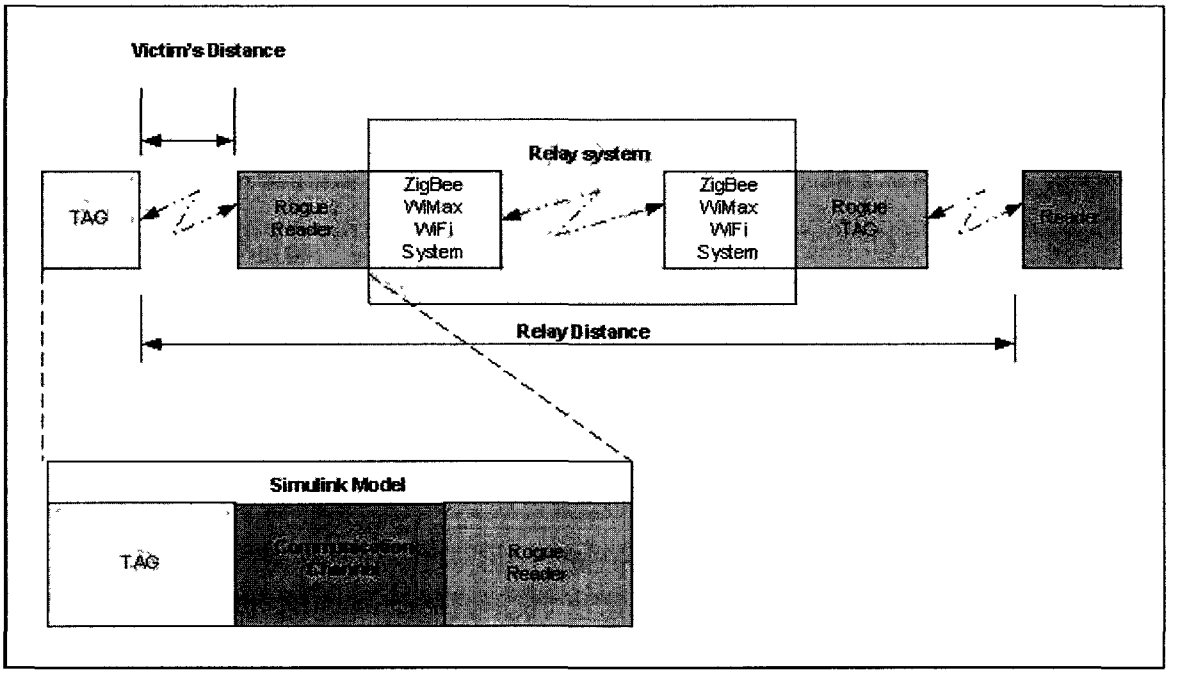


Figure 2.11: Relay Attack Model

The following list presents a brief description of each of the blocks that make up the *Reader* top level block diagram in Figure 2.12.

- PHY Tx
- Miller Encoder
- Up-Converter
- Down-Converter
- Detector
- Manchester Decoder

**PHY Tx**

This block will initiate the activation process by transmitting unmodulated carrier and polling message. As soon it receives the response from the *TAG*, it will generate another message that will continue the handshaking betwing *Reader* and *TAG*. The PHY TX block is built by the following sub-blocks:

- Message Generation
- Message detection
- Message Selection
- Start bit enable block
- Message selector

**Miller Encoder**

Encodes the message bit stream using modified Miller coding technique prior to Up-Conversion to *RF*. This block was designed using embedded Matlab and clock generators from *Simulink*.

### Up-Converter

Modulates the encoded message at 13.56MHz. The Up-Conversion is done done by using a mixer (ideal multiply from *Simulink*). Phase noise can be added directly by setting the *Simmulink* sine wave block.

### Down-Converter

It receives the modulated message embedded in noise from the *TAG* and down converts it to analog baseband. The down conversion process from 13.56Mhz to analogue base band is done in two steps: First the input input signal is down-converted to 836KHz by using mixers followed by an energy detector and a analogue filter (Elliptic filter). In the second step the subcarrier is removed by using a mixer followed by a digital low pass filter (FIR Finite Impulse Response) with bandwidth of 200KHz.

### Detector

Demodulates the *TAG's* received signal and it has the following blocks:

- Delay chain
- Hysteresis block
- Hard Detector

This block will receive the analogue base-band signal and will transform the analogue signal into digital (still Manchester encoded coded) signal. The decode of the analogue to digital is done by the hard detector.

### Manchester Decoder

Decodes the Manchester encoded signal and delivers it to the PHY Tx. Inside the PHY Tx, the message will be recognized if there is no error present. This sub-system uses basic *Simulink* blocks such as: delays, multipliers, adders and others.

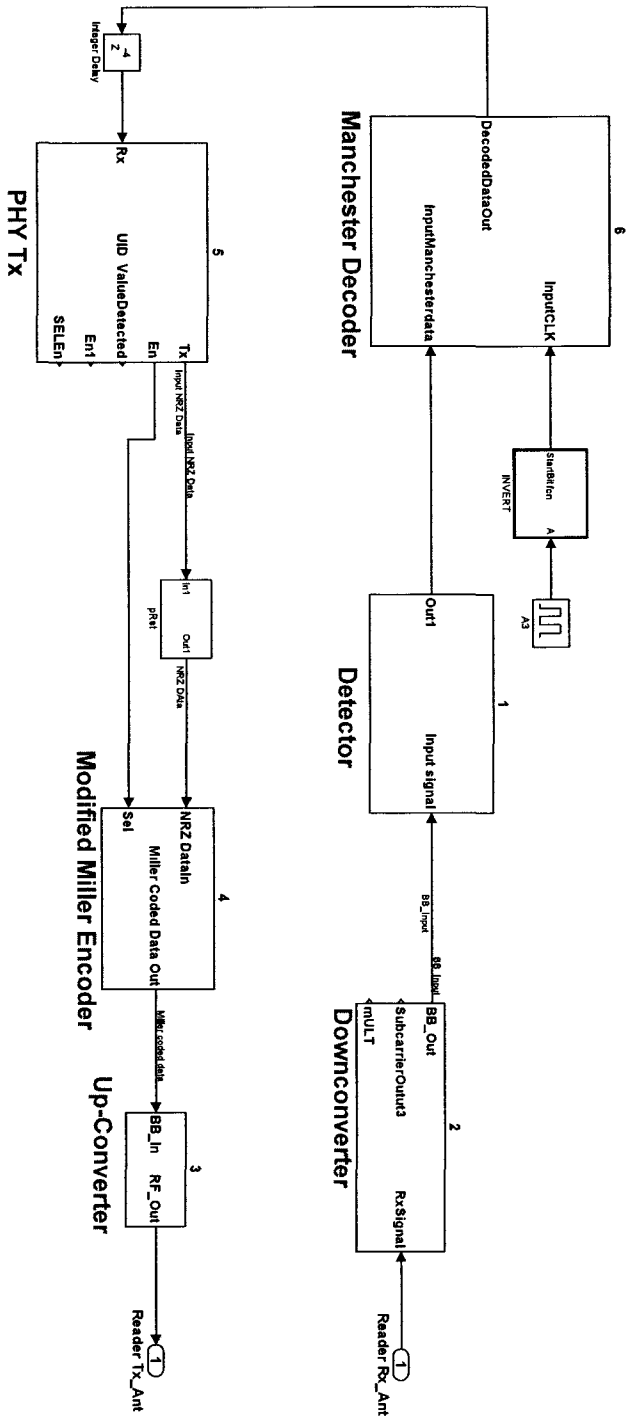


Figure 2.12: *Reader* Model Block Diagram

The following list presents a brief description of each of the blocks that make up the *TAG* top level block diagram in Figure 2.13.

- Down-Converter
- Miller Decoder
- Message Processor
- Manchester Encoder
- Up-Converter

### Down-Converter

Direct down conversion of the modulated signal to baseband. It also demodulates the signal. The demodulation method used is non-coherent, which is the same method recommended by *ISO14443*. The following blocks belong to this sub-system:

- Mixer
- Analogue filter (200KHz Tchebychev)
- Moving average filter with 8 delays
- Hard decoder
- RSSI

The *RSSI* (Receiver strength Signal Indicator) will measure the input power and is use to indicate the energy received by the *TAG*. Therefore will be use to indicate when the *TAG* is activated.

### Miller Decoder

Decodes the base band Miller encoded signal from the Down-Converter and delivers it to the message processor sub-system.

### Message Processor

This is the biggest block inside the system. It receives the decoded message, detects it and generates the response message to be transmitted to the *Reader*. This block has the following sub-systems that compose it:

- SEL timing generator
- SEL Detector
- WAKE Detector
- REQA Detector
- ATQA processor

### Manchester Encoder

Encodes the message bit stream generated by the Message Processor.

### Up-Converter

Converts the baseband coded message to *RF* (13.56MHz). The conversion process is done in two steps: Firstly the base band signal is up-converted to subcarrier frequency (836KHz) followed by a second up-conversion to the carrier frequency.

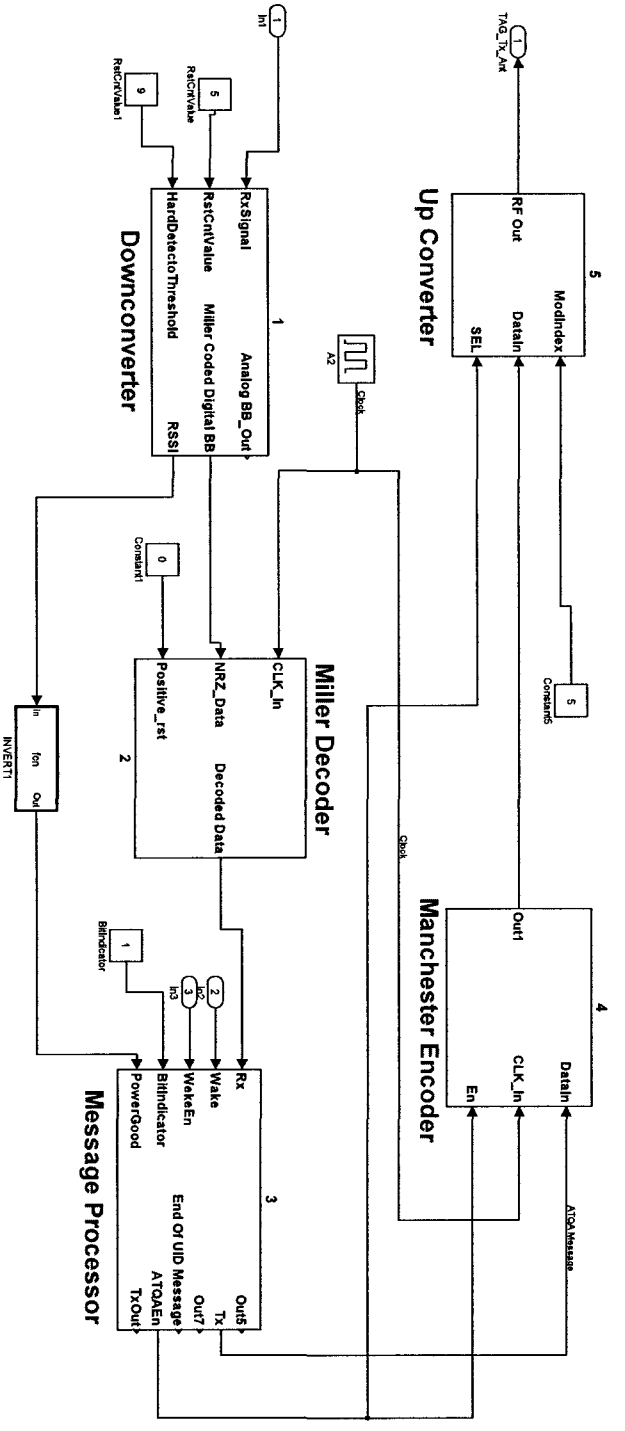


Figure 2.13: *TAG* Model Block Diagram

## 2.5 Conclusions

In this chapter we described how the relay attack is conducted in *RFiD* systems, as well as the operation of a general *RFiD* system (message exchange between *Reader* and *TAG*). We also described the anti-collision protocol process that happens in environments where multiple *TAGs* are in the presence of one *Reader* as well as details of the physical implementation of the system. We offered justification for the use of coding - such as Manchester and Miller - during the transmission of a bitstream signal, and several types of modulation used in *RFiD* system were reviewed in detail. Finally we presented the model of an *RFiD* system under *ISO14443*, which is currently unavailable in the literature. This will be used in Chapter 5 during the *RFiD* system analysis and to provide simulations of the relay attack.

# Chapter 3

# Communication Channel

## 3.1 Introduction

The attenuation of the communication channel that is located between the *TAG* and the rogue *Reader* depends on factors such as the distance between these devices, the operating frequency and antenna design. Communications carried out in the *NF* (Near Field) region is called *NF* communications, and communication outside the *NF*, is called *FF* (Far Field) or free space communications [22, Ch10] [57, Ch3]. The problem now that we face is how to estimate the boundary between these two fields for *RFiD* systems. This is the subject of the Section 3.2. This boundary will establish the region where Friis Equation can be used to determine the free space loss and *Victim Distance*. This is extremely important for the analysis and formulation of the complete *RFiD* system in Chapter 5, as well as to better understand the limits [1] of relay attack. In Section 3.3 we summarize other *NF/FF* boundaries available in the literature, and in Section 3.4 we provide equations describing the channel attenuation and free space loss that will be required in Chapter 5.

It has been shown in the literature [35], [36] and [46, Ch1] as well as in practical experiments that, depending on the application, *NF/FF* boundaries can differ. The approach adopted in this chapter is to calculate the boundary based on the dipole antenna equations found in [46, Ch1] and [47, Ch3]. We believe this approach gives the best approximation in *RFiD* systems under consideration here.

The *ISO* (International Standards Organization) has standardized the usage of *RFiD*

[1] Here limits mean the maximum distance that the attacker can be positioned away from the victim and successfully carry out a relay attack without being noticed.

devices operating in both regions (*NF* and *FF*), making them suitable for widespread adoption in a range of applications.

## 3.2 Near Field and Far Field

This section is focused primarily on defining the boundary between the *FF* and *NF* for an antenna or electromagnetic source. Detailed definitions of FF and NF can be found in [26, Ch5].

### 3.2.1 Near Field and Far Field Boundary

Let us assume an *RF* source (transmit antenna) and another *RF* sink (receive antenna) are placed with a distance $r$ between them. If $r$ is large enough that the energy that radiates from the transmit antenna is received only in a radial direction by the receive antenna, the receive antenna is said to be located in the FF region of the transmit antenna. In the *FF* region, the electrical $\vec{E}$ and magnetic $\vec{H}$ fields are perpendicular to the direction of propagation and also to each other forming a right-hand orthogonal basis. Angular variation in the $\vec{E}$ and $\vec{H}$ is essentially independent of the distance from the antenna. Another characteristic of this region is that the ratio of the magnitudes of the $\vec{E}$ and $\vec{H}$ fields equals the free space impedance, $\eta_0 = 377\Omega$ Ref [22, Ch10].

A receive antenna is located in the *NF* of the transmit antenna when the electrical $\vec{E}$ and magnetic $\vec{H}$ fields and direction of signal propagation are not perpendicular to each other.

### 3.2.2 Dipole Antenna

The dipole antenna, depicted in Figures 3.1 and Figure 3.2, are widely used in practice and is typically found in *RFiD TAGs*. In this section we present the equations for the electric and magnetic fields for the electric and magnetic dipole antennas. We present the standard equations (3.1 to 3.6), which may be found in [46, Ch1] and [47, Ch3] for example, where a very detailed dipole antenna analysis is given.

**Fields for Electrical Dipole** Let $\vec{a}_r$, $\vec{a}_\phi$ and $\vec{a}_\theta$ be unit vectors of a basis in a spherical coordinate system. Let the electrical dipole have an element of length $L$, see Figure 3.1. Let $f$ be the frequency, $c$ the speed of the light, $\lambda$ the wavelength, $i$ the antenna wire

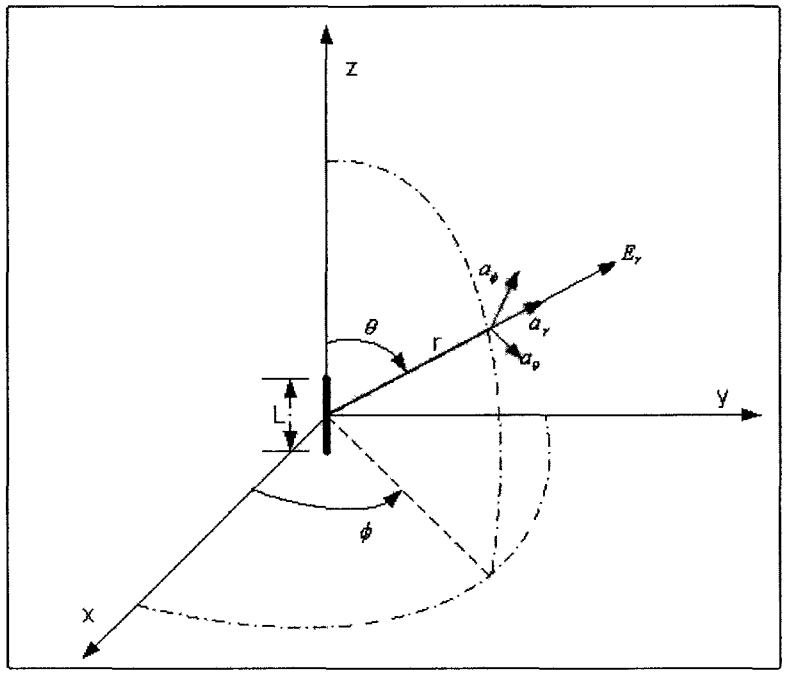


Figure 3.1: Electrical Dipole Field Source

current in Amperes, $j = \sqrt{-1}$, $\beta$ [2] the electrical length per meter, $\omega$ the angular velocity in rad/s, $\epsilon_0$ the permittivity of free space,( that is, $\epsilon_0 = \frac{1}{36\pi 10^9}$F/m), $\mu_0$ the permeability of free space (that is $\mu_0 = 4\pi 10^{-7} H/m$), and $\eta_0$ the free space impedance $\eta_0 = \sqrt{\frac{\mu_0}{\epsilon_0}} = 377\Omega$. The magnetic field $H$ has units of Ampere per meter $(A/m)$ and the electric field $E$ has units of Volts per meter $(V/m)$.

The nonzero projection of the electrical and magnetic fields of the electrical dipole antenna are given by Equation 3.1, 3.2 and 3.3.

$$\vec{E}_\theta = \frac{iL\beta^3}{4\pi\omega\epsilon_0}\left[\frac{j}{\beta r} + \frac{1}{(\beta r)^2} - \frac{j}{(\beta r)^3}\right]\sin(\theta)\, e^{-j\beta r}\vec{a}_\theta \quad V/m \tag{3.1}$$

$$\vec{H}_\phi = \frac{iL\beta^2}{4\pi}\left[\frac{-1}{j\beta r} + \frac{1}{(\beta r)^2}\right]\sin(\theta)\, e^{-j\beta r}\vec{a}_\phi \quad A/m \tag{3.2}$$

$$\vec{E}_r = \frac{iL\beta^3}{4\pi\omega\epsilon_0}\left[\frac{1}{(\beta r)^2} - \frac{j}{(\beta r)^3}\right]\cos(\theta)\, e^{-j\beta r}\vec{a}_r \quad V/m \tag{3.3}$$

[2] In the free space, the wave propagation $\beta = \frac{\omega}{c} = \frac{2\pi f}{c}$. With $c = \lambda f$, $\beta = \frac{2\pi}{\lambda}$.

**Fields for Magnetic Dipole** The antennas of *RFiD* devices used in Near Field Communication (*NFC*) are classified as magnetic dipoles and the nonzero projection of the fields for a magnetic dipole are given by equations 3.4, 3.5 and 3.6

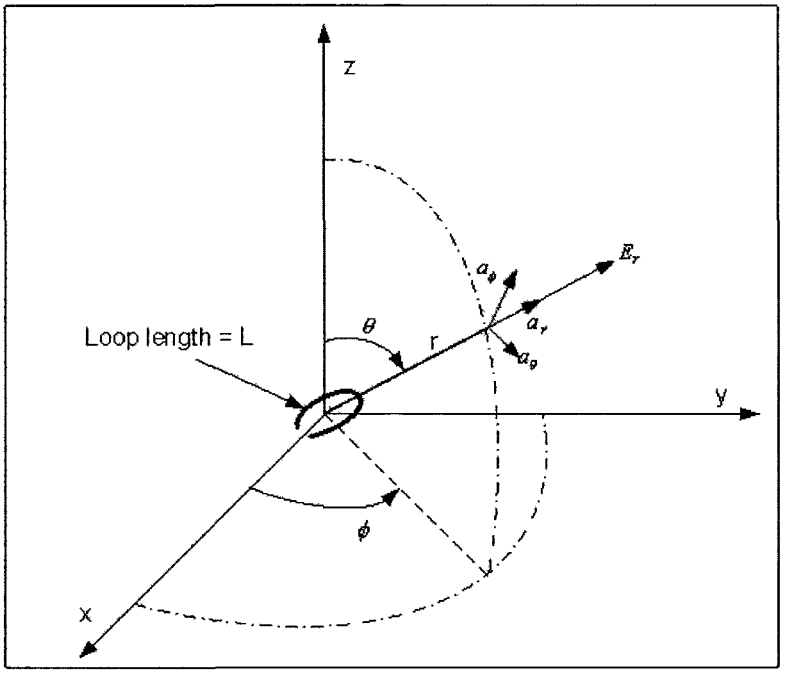


Figure 3.2: Magnetic Dipole Field Source

$$\vec{E}_\phi = -j\frac{\omega\mu m\beta^2}{4\pi}\left[\frac{-1}{j\beta r} + \frac{1}{(\beta r)^2}\right]\sin(\theta)\, e^{-j\beta r}\vec{a}_\phi \quad V/m \tag{3.4}$$

$$\vec{H}_r = j\frac{\omega\mu_0 m\beta^2}{2\pi\eta_0}\left[\frac{1}{(\beta r)^2} - \frac{j}{(\beta r)^3}\right]\cos(\theta)\, e^{-j\beta r}\vec{a}_r \quad A/m \tag{3.5}$$

$$\vec{H}_\theta = j\frac{\omega\mu_0 m\beta^2}{4\pi\eta_0}\left[\frac{j}{\beta r} + \frac{1}{(\beta r)^2} - \frac{j}{(\beta r)^3}\right]\sin(\theta)\, e^{-j\beta r}\vec{a}_\theta \quad A/m \tag{3.6}$$

### 3.2.3 Methodologies for Determining the NF and FF Boundary

The fields radiating from a transmit antenna are said to be inductive fields in the region of zero distance to the near field boundary from the antenna. Outside the Near Field boundary the wave front of the electric and magnetic fields propagate radially away from the transmit antenna [57, Ch3] this is called Far Field (*FF*). This section presents the wave impedance method of calculating the boundary between the *NF* and *FF*.

### Defining the NF/FF Boundary using Wave Impedance Method

The wave impedance method states that the point away from the radiating antenna where the magnitude of the ration between the $E$ field and $H$ fields approximates of the free space wave impedance $\eta_0 = 377\Omega$ is *NF/FF* boundary. Furthermore, Ref [22, Ch10] [47, Ch3] show that the wave impedance $Z$ can be calculated as follows:

$$Z = \frac{|E|}{|H|} \tag{3.7}$$

This method finds the point $r$ in space where the electromagnetic wave becomes constant. For the electrical dipole, the ratio $\vec{E}_\theta$ and $\vec{H}_\phi$ Equations 3.1 and 3.2 can be used in equation 3.7 to give 3.8 .

$$Z_E(r) = \left|\frac{E_\theta}{H_\phi}\right| = \eta_0 \left|\frac{1 + \frac{1}{j\beta r} + \frac{1}{(j\beta r)^2}}{1 + \frac{1}{j\beta r}}\right|. \tag{3.8}$$

Similarly, for the magnetic dipole the wave impedance is the ratio of equations 3.4 and 3.6, gives the equation 3.9 below.

$$Z_H(r) = \left|\frac{E_\phi}{H_\theta}\right| = \eta_0 \left|\frac{1 + \frac{1}{j\beta r}}{1 + \frac{1}{j\beta r} + \frac{1}{j(\beta r)^2}}\right|. \tag{3.9}$$

Figure 3.3 depicts the behavior of wave impedance Equations 3.8 and 3.9 as a function of the product $\beta r$, the distance per wavelength, where $r$ is the distance in meters.

#### Criterion for Choosing the Boundary

Figure 3.3 shows the impedance as function of the product $\beta \times$ radius. Looking at this figure, it is hard to select a precise point where the wave impedance is close enough to $377\Omega$ to satisfy the wave impedance criterion. However, it is known from basic electronics that maximum energy is transferred from a source to a load when the source and load impedances are equal. Let $RL$ be Return Loss [39, Ch2] which quantifies how close source and load impedances are to each other. Return Loss is defined by equation 3.10.

$$RL = 20 * \log\left|\frac{Z_0 - Z}{Z_0 + Z}\right| \tag{3.10}$$

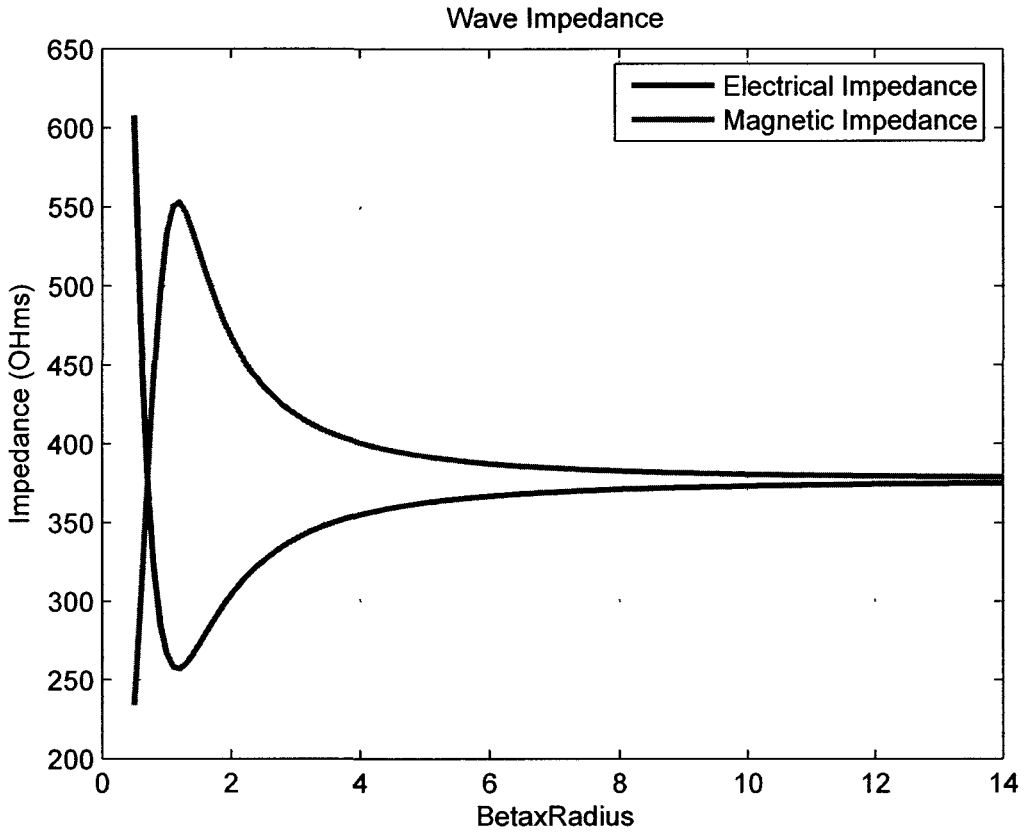


Figure 3.3: Wave impedance

Where $Z = Z_0 \pm \Delta Z$ and for simplicity we assume that $Z > Z_0 \Rightarrow Z = Z_0 + \Delta Z$. Substitute these into Equation (3.10), we find the value of $\Delta Z$ as function of $RL$ from equation 3.11.

$$\Delta Z = \frac{2 \times 10^{0.05RL} Z_0}{1 - 10^{0.05RL}}. \tag{3.11}$$

In similar manner when $Z < Z_0 \Rightarrow Z = Z_0 - \Delta Z$ we have equation 3.12

$$\Delta Z = \frac{2 \times 10^{0.05RL} Z_0}{1 + 10^{0.05RL}} \tag{3.12}$$

A $RL$ of 15dB has been chosen here as the test limit. This limit, although arbitrary, ensures that more than 97% of the source energy will be transferred to the load. Here the value of $\Delta Z = 111\Omega$ for the case $Z < Z_0$, which results in $Z = 266\Omega$; and $\Delta Z = 159\Omega$ for this case for $Z > Z_0$, which results in $Z = 530\Omega$. Now looking at Figure 3.3. We see that $Z = 260\Omega$ and $Z = 536\Omega$ correspond to a point $\beta \times r = 1.3$ radians. This gives the

boundary $r = \frac{1.3}{\beta} = \frac{1.3\lambda}{2\pi}$. These values are provided in Table 3.1 and one can observe that for $\beta \times r > 1.3$ the values of $RL$ are better than 15dB for both Electric and Magnetic dipole impedances. This will translate into a good match between antenna and air impedance.

| $\beta r = 1.3$ | Impedance ($\Omega$) | $\Delta$ Z($\Omega$) | Return Loss ($dB$) |
|---|---|---|---|
| Magnetic Field | 260 | 111 | 15 |
| Electric Field | 530 | 159 | 15 |

Table 3.1: Wave Impedance Boundary

For the *RFiD* system in consideration in this thesis we have $\lambda = 22.1m$ and so our estimate of the *NF/FF* boundary is $r = 4.57m$.

## 3.3 Boundaries from the Literature

The dipole antenna can be either the transmitter or receiver antenna. Table 3.2 lists NF/FF boundaries from literature. The second column gives the value of this boundary for $\lambda = 22.1m$ and the third column represents the absolute value of the difference between our boundary in Section 3.2.3 and the given boundaries.

| Distance | Distance (m) | Difference | Remarks | References |
|---|---|---|---|---|
| $\frac{1.3\lambda}{2\pi}$ | 4.57 | 0 | Wave Impedance method | Section 3.2.1 |
| $\frac{\lambda}{16}$ | 1.38 | 3.19 | Measurement error $\leq 0.1dB$ | [26, Ch5], [56] |
| $\frac{\lambda}{8}$ | 2.77 | 1.81 | Measurement error $\leq 0.3dB$ | [26, Ch5], [56] |
| $\frac{\lambda}{4}$ | 5.53 | 0.95 | Measurement error $\leq 1.0dB$ | [26, Ch5], [56] |
| $\frac{\lambda}{2\pi}$ | 3.52 | 1.06 | Rayleigh Criteria | [2] |
| $\frac{3\lambda}{16}$ | 4.15 | 0.43 | For dipoles $\leq 1.0dB$ | [56] |

Table 3.2: Definitions of NF/FF Boundaries

Table 3.2 shows a range of published values for the *NF/FF* boundary. This range occurs because each author has used different hypotheses and assumptions to determine this boundary. With no consensus *NF/FF* boundary, it was decided to select the criterion of $RL \geq 15dB$ (i.e., > 97% power transfer) and used this with the wave impedance method to determine a *NF/FF* boundary. The Wave Impedance method is a straight forward process that can be applied to any type of antenna. It presents strong agreement (less than 1m difference for *ISO14443*) between the method presented in Section 3.2.3 and many of the other methods in this table.

## 3.4 Free Space Loss

This section defines the channel attenuation that will be used in Chapter 5 for the analysis of the relay attack link budget. It is assumed that the victim's *TAG* is located in the *FF* region of the attacker's rogue *Reader* antenna. Let $d$ be the distance between victim's *TAG* and attacker's rogue *Reader*, $c$ the speed of light in (m/s), $f$ the frequency in *Hz* and $0 \leq l(d,f) \leq 1$ the attenuation factor or Free Space Loss with $FSL(d,f)$ as the equivalent value in $dB$. By [11] we have the free space loss given by Equation 3.13.

$$l(d,f) = \left(\frac{c}{f 4\pi d}\right)^2 \tag{3.13}$$

$FSL$ [1] in $dB$, is:

$$FSL(d,f) = 10\log_{10}\left(\frac{1}{l(d,f)}\right). \tag{3.14}$$

After some calculations Equation 3.14 can be re-written as:

$$FSL(d,f) = -147 + 20\log_{10}(d) + 20\log_{10}(f) \tag{3.15}$$

If the frequency is measured in *MHz* and keeping the distance in meters, the free space loss will be:

$$FSL(d,f) = -27 + 20\log_{10}(d) + 20\log_{10}(f) \tag{3.16}$$

[1] Notice that for $l(d,f) \leq 1 \Rightarrow \log(l(d,f)) \leq 0$. Values of attenuation are normally positive; therefore, we uses $\log(1/l(d,f))$ to make $FSL(d,f)$ positive.

## 3.5 Conclusion

In this chapter, using the Wave Impedance method, we estimated the bound between *NF* and *FF*. This is very important factor for the design of *RFiD* relay attack system because it determines where the *FSL* equation can be used. We can now also state that the attacker is working in the *FF*. This boundary determined here was used in the design and analysis of the results obtained from the simulation of the *RFiD* system model presented in Chapter 5. This result is in accordance with many references [57, Ch3],[26, Ch5] and [2, Ch2]. The conclusion obtained by this analysis is for ISO14443 it is safe to assume that the *NF/FF* boundary will be located approximately 4.5 meters from the *Reader* antenna. Therefore, the Friis free-space equation [5, Ch3] for attenuation in the *FF* is valid for distances greater than 4.5 meters and can be used to predict the maximum *Victim Distance*. For *Victim Distance* less than 4.5 meters the attack can still be carried out; however, this *Victim Distance* cannot be determined using Friis' equation.

# Chapter 4

# End to End *RFiD* System Analysis

In this chapter we present the effects of the imperfections at *RF* and baseband in the electronic components. These imperfections will contribute to the overall *SNR* of the system. Therefore, it will degrade the performance of the system and it will affect the success of the attacker carrying out a relay attack.

In Section 4.1 we present the analysis of the some of these imperfections (e.g, noise figure, phase noise, second and third order intermodulation, quantization noise and others). In Section 4.2 we calculate the total *EVM* of the system taking in account all the the contributions presented in Section 4.1. In Section 4.3 we present the sensitivity analysis of the receiver and in Section 4.4 we present the *RFiD* system budget analysis.

Understanding these imperfections is of high importance when the attacker is building the relay attack system in order to make the attacker's rogue *Reader* to operate at optimum performance. Today there are a variety of *RFiD* standards that allow devices to operate in many frequency bands (e.g, 13.56MHz, 900MHz, 2.4GHz, 5GHz and others).

*RFiD* systems that one can buy in the marketplace usually use very robust and simple modulation schemes that makes the system immune to phase noise, carrier feedthrough, $I$ and $Q$ imbalance and other imperfections. During a relay attack, the attacker may want to design and build his own attack system, to be able to carry out the relay attack with his system operating at optimum performance. Thus, the attacker will be able to position himself as far as possible from the victim; see Chapter 5 for details.

## 4.1 Transmitter and Receiver Imperfections

When information is transmitted from a point $A$ to a point $B$, there are many factors that could cause imperfection in the *RF* signal and consequently in the message. Such imperfections thus increase the probability of error in the detector.

In this section we analyze the causes and the impact of some of these imperfections (e.g, noise figure, phase noise, second and third order intermodulation, quantization noise and others) into the demodulated signal. In most cases, the imperfections at the *RF* section of the transmitter and/or receiver will cause degradation in the performance of the system. The degradation in performance of a communication system can be measured using several metrics including *BER, Phase Noise* and *Noise Figure*, but the most common metric used to measure digital communication system performance is *BER*.

During the design of front end *RFiD* communication systems, many engineers are faced with the difficult task of either selecting the electronic *OTS* components or designing the *RFiC* (Radio Frequency Integrated Circuit) that meets the cost target imposed by the application of the technology. To minimize the design effort while maintaining the overall system performance, the designer needs to answer the following question: What imperfection of the *RF* block can be relaxed without having major impact on the system performance? The purpose of this section is to provide a detailed analysis about the effects of *RF* imperfections. These imperfections will be considered during the relay attack system analysis in *RFiD* presented in Chapter 5.

### 4.1.1 Non Linearities

Indeed the modulation types used in *ISO14443* are not sensitive to non linearities for normal operating distances. During attack the rogue *Reader* will be as far as possible from the *TAG*. Therefore, the attacker will need to consider all the effects that may possibly cause the attack to fail.

**Linear System** A system with impulse response $h(t)$ is said to be linear if and only if the superposition theorem is applicable [37, Ch4]. Namely, suppose that when the system is excited by the input signal $v_1(t)$, the output signal is $y_1(t)$ and when the input is $v_2(t)$ the output is $y_2(t)$. When the input is $v_1(t) + v_2(t)$ , the output is $y_1(t) + y_2(t)$ so

the system is said to be linear.

For dynamic systems, the following differential equation applies, for some $m, n > 0$ [37, Ch4].

$$\frac{d^n v_{out}}{dt^n} + a_{n-1}\frac{d^{n-1} v_{out}}{dt^{n-1}} + \cdots + a_1\frac{dv_{out}}{dt} = b_m\frac{d^m v_{in}}{dt^m} + \cdots + b_1\frac{dv_{in}}{dt} + b_0 v_{in} \tag{4.1}$$

If the parameters $a_i$ and $b_i$ are constants, the system is called linear time-invariant [38, Ch1], [58, Ch2].

Any system to which we cannot apply the superposition theorem is said to be non-linear. If the system is memoryless (i.e, the present output does not depend on past inputs) the power series applies to calculate the output signal $v_{out}$ [58, Ch2]:

$$v_{out} = k_0 v_{in}(t) + k_1 v_{in}^2(t) + k_2 v_{in}^3(t) + \ldots \tag{4.2}$$

The values of $[k_0, k_1, k_2 \ldots]$ need to be modeled for each non-linear electronic device.

When an electronic device is operating in non-linear region, equation 4.2 is applied and there will be undesired frequency components that will cause interference in other frequency bands. Non-linearities could also cause self interference which is the case of two tone beats see Table 4.2. Mitigation of the non-linearities problem can be achieved using techniques either during the design of the components (Integrated Circuits) [27] or pre-distortion applied at baseband [29] [6][1].

Nonlinearities are present in all electronic devices. They commonly occur on transmitter and receiver front-ends. Nonlinearities can have a devastating impact on the performance a system. In a communication system, the main electronic devices or subsystems that are very susceptible to non-linearities are the PA (Power Amplifier) and *LNA* (Low Noise Amplifiers).

In this section we describe the effect of non-linearities in electronic devices. We begin by analyzing the meaning of $P1dB$ ( $1dB$ compression point) and explaining the two tone testing. This will walk us through in the calculation of the frequency components (second and third order components) resulting from the intermodulation distortion and finally lead to the effects of the resulting non-desired frequency components in the system design.

[1]Since ISO14443 uses a much simpler modulation scheme compared with OFDM (i.e., AM versus phase plus AM) it is safe to assume that these analysis can be applied to these systems.

### Single Tone Test (P1dB)

Let us consider the electronic circuit depicted by Figure 4.1 and the ideal input voltage described by $v_{in} = A\cos\omega t$; where $A$ is the maximum amplitude, $\omega$ is the angular frequency and $t$ is time. We substitute the input voltage $v_{in}$ into Equation 4.2. For simplicity only the first, second and third terms of the output voltage are considered. The output voltage of the electronic device can be written as:

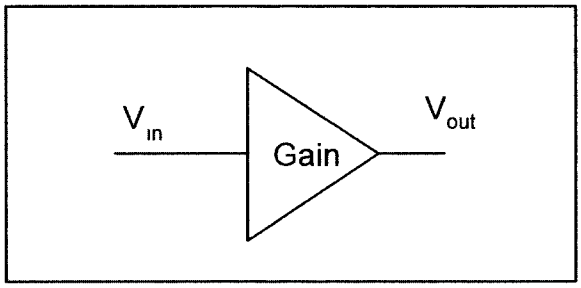


Figure 4.1: Single tone input

$$V_{out} = k_0 v_{in} + k_1 v_{in}^2 + k_2 v_{in}^3 \tag{4.3}$$

Expanding Equation 4.3 it is possible to better visualize the terms that appear at the output of the electronic device and this voltage can be represented as follows.

$$V_{out} = \frac{k_1 A^2}{2} + \left(k_0 A + \frac{3k_2 A^3}{4}\right)\cos\omega t + \frac{k_1 A^2}{2}\cos 2\omega t + \frac{k_2 A^3}{4}\cos 3\omega t \tag{4.4}$$

Observe that the second and third harmonic terms appear at the output. These undesirable signal components may be removed by using a band-pass filter centered at $\omega$. Table 4.1 shows the amplitude of the output signal components.

Let $n$ be the frequency component index. Then Equation 4.3 can be written as

$$v_{out} = \sum_{n=0}^{2} K_n \cos\left((n+1)\omega t + \theta\right) \tag{4.5}$$

where $\theta$ is the phase. When the electronic circuit operates in the linear region, $P_{out} = P_{in} + Gain$. For each $dB$ of increasing at the input power at the circuit, it will correspond a one $dB$ increase in power at the output. When the output power is 1dB lower than the expected value ($P_{out} = P_{in} + Gain - 1$), the circuit is in the non-linear region and this point is named $P1dB$. This point is depicted by Figure 4.2.

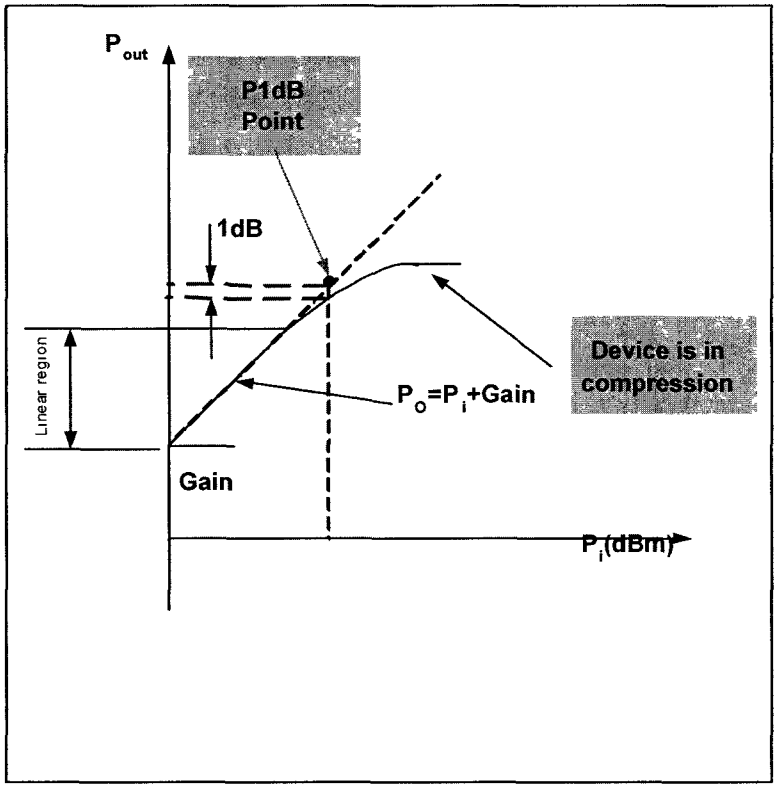


Figure 4.2: P1dB point

Table 4.1: Frequency composition at $V_{out}$

| Frequency | Amplitude | Comments |
|---|---|---|
| 0 | $\frac{k_1 A^2}{2}$ | DC component |
| $f_1$ | $k_0 A + \frac{3k_2 A^3}{4}$ | Fundamental |
| $2f_1$ | $\frac{k_1 A^2}{2}$ | $2^{nd}$ Harmonic |
| $3f_1$ | $\frac{k_2 A^3}{4}$ | $3^{rd}$ Harmonic |

### Intermodulation

Intermodulation or *IMD* (intermodulation distortion) is the loss of the characteristics of the transmitted information caused by the non-linearity of electronic devices. Intermodulation occurs as result of the mixing of two or more tones that are present in the input of the electronic circuit. This mixing effect will generate other undesired frequencies at the output of the circuit.

**Multiple Tones Test** In communication systems, the great majority of the transmitted signals are composed of more than one tone. Let us first focus on the case where two tones are present at the input of an amplifier, as shown in Figure 4.3. Let $\omega$ be the angular frequency, $f_n$ a frequency component, $n \in \Re^+$ and $t$ is time. Let $v_1(t) = A_1 \cos(\omega_1 t)$ and $v_2(t) = A_2 \cos(\omega_2 t)$ where $\omega_n = 2\pi f_n$ be the two tones present at the input of the amplifier. For simplicity, let us consider that both signals have the same amplitude $A_1 = A_2 = A$. Therefore, the input signal can be written as $V_{in} = A\cos(\omega_1 t) + A\cos(\omega_2 t)$.

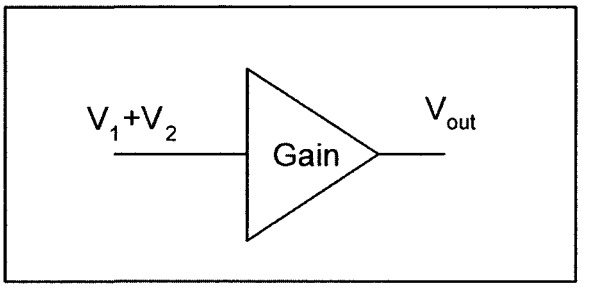


Figure 4.3: Two tones input

The power series has an infinite number of terms [38, Ch1], but for simplicity only to the cubic terms are considered. The output voltage at the electronic device can be described as follows:

$$V_{out} = k_0 v_{in}(t) + k_1 v_{in}^2(t) + k_2 v_{in}^3(t) \tag{4.6}$$

The values of $[k_0, k_1, k_2 \ldots]$ need to be adjusted (modeled) for each non-linear electronic device. The second and third order products from equation 4.6 are discussed in in the next paragraphs.

**Second Order Intermodulation Products** Let $v_{2nd}$ be the output signal of the amplifier considering only the first and second order terms of the power series. Removing the third order terms from Equation 4.6 yields

$$V_{2nd} = k_1 v_{in}^2(t) = K_1 \left[v_1(t) + v_2(t)\right]^2 \tag{4.7}$$

When substituting the input signals $v_1(t)$ and $v_2(t)$ into $V_{2nd}$, the result is:

$$\begin{aligned} v_{2nd} = & \underbrace{k_1 A^2}_{DC} + \underbrace{\frac{k_1 A^2}{2}\cos\left(\omega_1 + \omega_2\right)t + \frac{k_1 A^2}{2}\cos\left(\omega_1 - \omega_2\right)t}_{Second\ Order\ Intermodulation} \\ & + \underbrace{\frac{k_1 A^2}{2}\cos 2\omega_1 t + \frac{k_1 A^2}{2}\cos 2\omega_2 t}_{Second\ Harmonics} \end{aligned} \tag{4.8}$$

The second order intermodulation products will not generate fundamental frequency components. Therefore one method of removing or attenuating these undesired signals is using filter techniques such as *BPF* (Band Pass Filter).

Let $P_{in}$ and $P_{out}$ be respectively the input and output power of the amplifier in watts and $G$ be the linear gain. One can write the output power of the amplifier as function of its input power and the gain will be: $P_{out} = P_{in} * G$. If $P_i$ and $P_0$ are respectively the input and output powers expressed in *dBm* and *Gain* be the gain in *dB* one can write the expression in log form. Therefore, $P_0$ can be written as:

$$P_0 = P_i + Gain \quad (\text{dBm}) \tag{4.9}$$

Let $P_{2nd}$ be the power of the second intermodulation terms and $I_2$ be the intercept of the linear equation 4.9 with vertical power axis $P_{out}$.

$$\begin{aligned} P_{2nd} &= 10\log_{10}\left(\frac{k_1 A^2}{2}\right)^2 \\ &= \underbrace{10\log_{10}\left(\frac{k_1}{2}\right)^2}_{I_2} + \underbrace{2 * 10\log_{10} A^2}_{2P_i} \\ &= I_2 + 2 * P_i \end{aligned} \tag{4.10}$$

Equation 4.10 shows that for every $dB$ in increase at the input power, the value of the power of the second order intermodulation will increase by $2dB$.
Once $Gain > I_2$, these two lines Equations 4.9 and 4.10 are going to intersect at a point called *Second Order Intercept Point*. The input power level is given as *IIP2* (Input IP2) and will generate the second order intermodulation components at the output *OIP2* (Output IP2). Figure 4.4 details this point and the slope of the lines.

**Third Order Intermodulation Products** Now let us consider only the third order element of Equation 4.6. Let us proceed by expanding this term and calculate the components generated by the third order non-linearities when the circuit is excited by two tones. Let $v_{3rd}$ be the output of the amplifier only considering the third order components.

$$v_{3rd} = k_2 V_{in}^3(t) = K_2 \left[v_1(t) + v_2(t)\right]^3 = K_2 \left[v_1(t) + v_2(t)\right]^2 \left[v_1(t) + v_2(t)\right] \tag{4.11}$$

Applying simple trigonometry equation 4.11 can be expressed as

$$\begin{aligned}
V_{3rd} = & \underbrace{\frac{3k_2A^3}{2}\left[\cos\omega_1 t + \cos\omega_2 t\right]}_{Fundamental} + \\
& \underbrace{\frac{k_2A^3}{2}\cos\left(2\omega_1 + \omega_2\right)t}_{Out\ of\ band\ Intermodulation} + \underbrace{\frac{k_2A^3}{2}\cos\left(2\omega_1 - \omega_2\right)t}_{In-band\ Intermodulation} + \\
& \underbrace{\frac{k_2A^3}{2}\cos\left(2\omega_2 + \omega_1\right)t}_{Out\ of\ Band\ Intermodulation} + \underbrace{\frac{k_2A_1^2A_2}{2}\cos\left(2\omega_2 - \omega_1\right)t}_{In-band\ Intermodulation} + \\
& \underbrace{\frac{k_2A^3}{4}\left[\cos 2\omega_1 t + \cos 2\omega_2 t\right]}_{Second\ Harmonics} + \\
& \underbrace{\frac{k_2A^3}{4}\left[\cos 3\omega_1 t + \cos 3\omega_2 t\right]}_{Third\ Harmonics}
\end{aligned}$$

This equation shows that third order intermodulation produces additional frequency components. From Table 4.2 we see that some of these components fall within the operating frequency band and therefore cannot be removed by filtering. The only

way to mitigate this in-band interference is to operate the device in its linear region.

Let $I_3$ be the intercept point on the $P_{out}$ axis depicted in Figure 4.4. If we apply the same methodology as used in the second order intermodulation analysis, we can find the following equation

$$P_{3rd} = I_3 + 3 * P_i \tag{4.12}$$

Equation 4.12 shows that for each $dB$ in power increase at the input, the value of the power of the third order intermodulation will increase by $3dB$.

Once $Gain > I_3$, these two equations 4.9 and 4.12 intersect in a point named *Third Order Intercept Point*, where the input power is named *IIP3* (Input IP3) and will generate the third order intermodulation component *OIP3* (Output IP3). More details are shown in Figure 4.4.

Table 4.2: Second and third order intermodulation products for Two Tones test

| Freq | Amplitude | Comments |
|---|---|---|
| 0 | $k_1A^2$ | DC component due to second order products |
| $f_1$ | $\frac{3k_2A^3}{2}$ | 2nd and 3rd Order |
| $f_2$ | $\frac{3k_2A^3}{2}$ | 2nd and 3rd Order |
| $2f_1$ | $\frac{k_1A^3}{2}$ | 2nd and 3rd Order |
| $2f_2$ | $\frac{k_1A^3}{2}$ | 2nd and 3rd Order |
| $f_1 + f_2$ | $\frac{k_1A^2}{2}$ | Second Order |
| $f_1 - f_2$ | $\frac{k_1A^2}{2}$ | Second order |
| $2f_1 + f_2$ | $\frac{k_2A^3}{2}$ | Third order |
| $2f_1 - f_2$ | $\frac{k_2A^3}{2}$ | Third order |
| $2f_2 + f_1$ | $\frac{k_2A^3}{2}$ | Third order |
| $2f_2 - f_1$ | $\frac{k_2A^3}{2}$ | Third order |
| $3f_1$ | $\frac{k_2A^3}{4}$ | Third order |
| $3f_2$ | $\frac{k_2A^3}{4}$ | Third order |

In Table 4.2, we observe that the third order products occur and generate $\left(2f_i \pm f_j\right)$ frequency components, which may end up being located inside the pass-band of the

transmitted signal. Therefore, these components cannot be filtered. The second order products and some of third order can be remove using filter techniques.

### Computation of Undesired Power

Figure 4.4 depicts equations 4.8, 4.9 and 4.12. The input power is on the horizontal axis and the output power on the vertical. The curve $P_0 = f(P_i)$ intercepts the other two curves at two important points, called the third order and second order intercept points. At these points the output power and the power of the intermodulation products are equal.

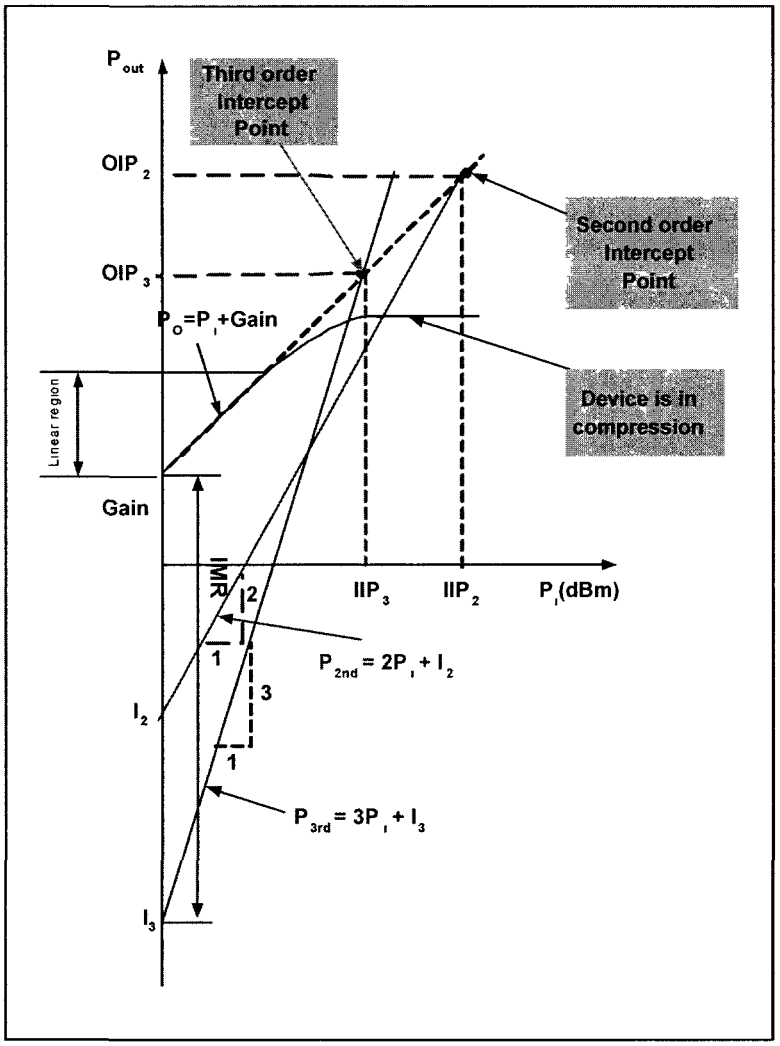


Figure 4.4: Relationship between the second and third order intercept points

Looking at Figure 4.4, we see that if the input signal has power equal to *IIP3* the output power will be *OIP3* therefore the following equation holds:

$$P_{3rd} = OIP_3 = P_0 \tag{4.13}$$

Re-arranging this last equation, $OIP_3$ can be written as

$$OIP_3 = \frac{IMR}{2} + Gain \tag{4.14}$$

where *IMR* is the intermodulation ratio, and $P_o$ is the output power at the operation point (for a given input power).

When operating in the linear region, the output power $P_0 = P_i + Gain$ and $IMR = 2(OIP_3 - P_0)$. The undesired power (harmonic distortion power) can be calculated by using

$$P_u = 3(P_i + Gain) + 2OIP_3. \tag{4.15}$$

These numbers are available in most data sheets published by the components manufacturers . Second and third order intercept points provide great valuable information and applying simple geometry, greatly simplify the calculation of the undesired power generated by intermodulation production in a given system.

**Example of Distortion due to Nonlinearity**

For illustration purpose only, let us uses *QPSK* modulation for this example. Figure 4.5 depicts the constellation of a *QPSK* (Quadrature Phase Shift keying) modulated signal. In an ideal system the constellation points will be located at the crosses. The red points show the actual position of the constellation for a real system. When the Euclidean distance between any two ideal points (crosses) decrease, the error probability [2] increases. The decrease in the Euclidean distance occurs because the amplifier is in compression and cannot reach the desired output power.

[2]Equation 5.4 calculates the error probability for a *PAM* signal. The respective *BER* function of *SNR* is depicted by Figure 5.2

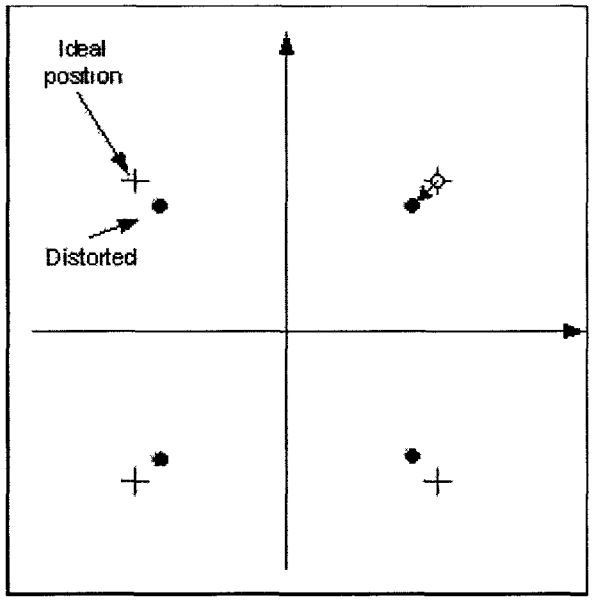


Figure 4.5: Amplitude distortion in *QPSK* signal

### 4.1.2 Effects of Phase Noise

One very important imperfection is *PN* (Phase Noise). This imperfection contributes to the degradation of the system by rotating the constellation points (phase rotation) of the modulated signal and therefore increasing the *BER*. Coherent demodulation is the aspect that suffers most from the presence of phase noise in the *LO* (Local Oscillator). The presence of *PN* increases the *EVM* (Error Vector Magnitude) and consequently the bit error rate (BER).

Many papers have covered phase and frequency fluctuations in great detail [8], [32], [45]. They cover this from the perspective of circuit design (how to apply techniques at circuit level to minimize the phase noise) then they consider system performance. In this section, we present the topic looking at the system level performance degradation, which is of interest during the design of the *RFiD* rogue *Reader*.

#### Formulation

Let us assume that we desire to design an oscillator that produces an amplitude $A$, an angular frequency $\omega_0$ and a constant phase $\phi$. Ideally this oscillator would generate an output signal that would have the following mathematical description: $v(t) = A\cos(\omega_0 t + \phi)$. In practice, there will be fluctuations in the amplitude and phase. These fluctuations occur due to many noise factors that are present in the transistors, include power supply, grounding, substrate. Taking in account these imperfections, the output of an oscillator can be represented by: $v(t) = A(t)\left[\cos\left(\omega_0 f(t) + \phi(t)\right)\right]$ where $f[.]$ is a periodic function with period $2\pi$, $A(t)$ and $\phi(t)$ are now the amplitude and phase fluctuation function of time respectively.

The output of an oscillator can be characterized by the short-term stability. It is usually done in terms of the single side band noise spectral density (*PN*) that is mathematically given [17] by

$$\pounds_{total}(\Delta\omega) = 10\log\left[\frac{P_{sideband}(\omega_0 + \Delta\omega, 1Hz)}{P_{carrier}}\right] \tag{4.16}$$

and graphically approximated by Figure 4.6. Indeed, there are many ways to characterize the stability of a signal. In [45] the author provides in details many of these techniques.

Also there is the famous equation based on the model proposed by [8] and [28] known as Leason-Cutler. It is mathematically given as: Let $F$ be an empirical parameter, $K$ be Boltzmann's constant, T be the temperature in Kelvin, $P_s$ be the real dissipated power, $\omega_0$ be the oscillator frequency, $Q_L$ is the effective quality factor of the tank also know as loaded $Q$, $1/f^3$ is the corner between $1/f^3$ and $1/f^2$ slopes [49] then

$$\pounds_{total}(\Delta\omega) = 10\log\left[\frac{2FKT}{P_s}\left[1+\left(\frac{\omega_0}{2Q_L\Delta\omega}\right)^2\right]\left(1+\frac{\Delta\omega 1/f^3}{\|\Delta\omega\|}\right)\right]. \tag{4.17}$$

This equation has many equally valid variations.

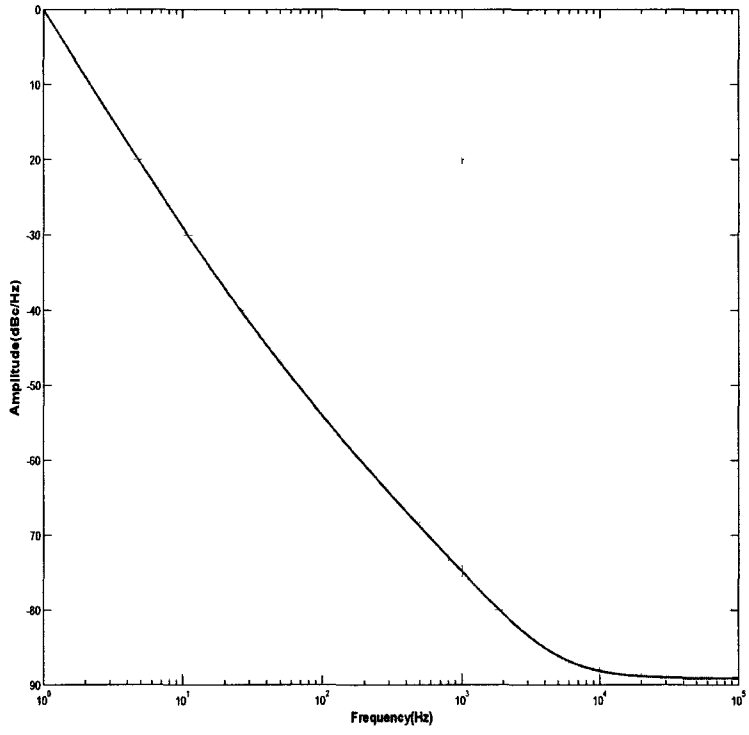


Figure 4.6: Leason-Cutler phase noise model Q=100, F=1MHz,T=27C,Ps=1mW

Figure 4.6 shows an example of a local oscillator noise, which will be added to the overall system noise. To calculate the local oscillator noise contribution, the area below the curve (noise density function) will need to be integrated into the used bandwidth. For example if the bandwidth is 100Kz, the noise needs to be integrated until 50KHz and added 3dB to consider the double sided noise, 50KHz for each side.

The advantage of short-term stability analysis is that is very simple. The disadvantage is that because the phase and amplitude variations are analyzed together they

cannot be separately investigated. In [7] Costa and Pupolin provide a discrete model for phase noise which can also be modeled as Winner-Lèvi process.

### 4.1.3 I and Q Imbalance and carrier feedthrough

In the previous sections we analyzed the intermodulation effects and *PN* in oscillators. In this section we analyze the up and down-converter imperfections, excluding the non-linearity and phase noise that already have been covered. This analysis is important during the total *EVM* calculation for the end-to-end system, and will serve to support the considerations used during the design of the Simulink model presented in Chapter 5. Our analysis will be made using a zero IF up-converter. This type of up-converter presents the following *RF* imperfections

- I and Q imbalance (*In Phase* and *In Quadrature*)
- Carrier feedthrough
- Phase noise
- Non-Linearities

Since the last two have been discussed in previous sections, we will concentrate the analysis on *I and Q* imbalance and carrier feedthrough.

#### System

In general, the baseband signal is composed of many frequency components and it can be represented as

$$s(t) = \sum_{i=1}^{K} A_i \cos(\omega_i t + \theta_i) \tag{4.18}$$

To simplify the analysis, let us assume that the modulated baseband signal is composed by the *In Phase* $S_Q(t)$ and *In Quadrature* $S_I(t)$ signals and each one of these signals ($S_I(t)$ and $S_Q(t)$), have only one frequency component. Let $A_I$ and $A_Q$ be their amplitudes, $\theta_Q$ and $\theta_I$ be the their phases, $t$ time and $\omega$ the angular frequency. The signals can be defined as

$$S_Q(t) = A_Q \cos\left(\omega t + \theta_Q\right) \tag{4.19}$$

$$S_I(t) = A_I \cos(\omega t + \theta_I) \tag{4.20}$$

and are depicted in Figure 4.7

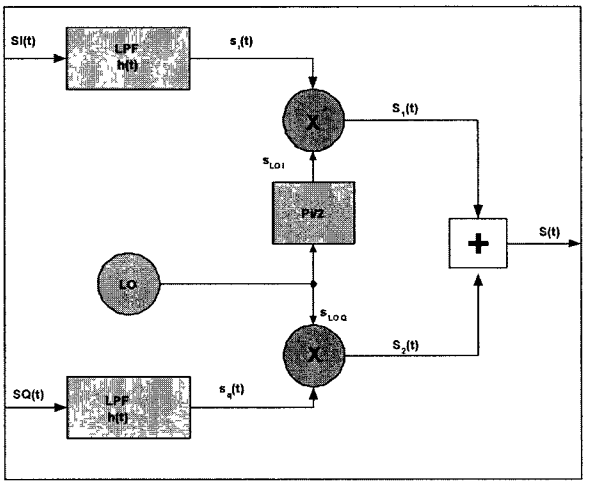


Figure 4.7: Up-Converter block diagram

Figure 4.7 shows a zero *IF* (Intermediate Frequency) up-converter that is designed using two baseband filters, one filter for the $S_I(t)$ and the other one for $S_Q(t)$ signals respectively. It has the *LO* that is responsible for generating the output frequency to be transmitted, the ninety degree phase rotator for the carrier, two mixers and an adder. We assume the filter is ideal. Therefore the impulse response of the filter in the frequency domain is given as [48, Ch3]

$$H(j\omega) = \begin{cases} 1e^{j\omega}, & \text{if } \omega < \Omega_{max}; \\ 0, & \text{otherwise.} \end{cases} \tag{4.21}$$

Here $\Omega_{max}$ is the maximum baseband frequency used by the system and $h(t) = F[H(j\omega)]$, where $F[.]$ is the Fourier transform.

The base-band signals at the input of the mixers are given as

$$s_I(t) = \int S_I(t)h(t-\tau)d\tau = S_I(t) * h_I(t) = A_I \cos(\omega t + \Theta_I) \tag{4.22}$$

and

$$s_Q(t) = \int S_Q(t)h(t-\tau)d\tau = S_Q(t) * h_Q(t) = A_Q \cos\left(\omega t + \Theta_Q\right) \tag{4.23}$$

where $(*)$ is the convolution operation between the input signal and impulse response of the Linear Time Invariant *(LTI)* system. The angle variation in the output with

relation to the input is given as

$$\Theta_x = \theta_x + \phi_x \tag{4.24}$$

Let $S_{LOI}$ and $S_{LOQ}$ be the input of the carrier generated at the input of each $LO$ port of the mixers, $A_{LOI}$ and $A_{LOQ}$ be their respective amplitudes and $\Theta_{LOI}$ and $\Theta_{LOQ}$ be their phases. The equations that represent the input signals at the $LO$ port of the mixers are given as

$$S_{LOI} = A_{LOI}\cos\left(\omega_0 t + \Theta_{LOI}\right) \tag{4.25}$$

$$S_{LOQ} = A_{LOQ}\cos\left(\omega_0 t + \Theta_{LOQ}\right) \tag{4.26}$$

If the mixers are not ideal, there will be carrier feedthrough in both mixers. Let $\alpha_I$ and $\alpha_Q$ be the coefficients of the carrier feedthrough for the *In Phase* and *In Quadrature* signals respectively.

The value of $\alpha$ is usually in the order of $10^{-2}$ *to* $10^{-4}$, see [59]. Looking at Figure 4.7, we find that at the input of the adder/output of the mixers, both signals are given as

$$s_1(t) = s_{LOI}(t)s_I(t) + \underbrace{\alpha_I s_{LOI}(t)}_{Carrier\,feedthrough} \tag{4.27}$$

$$s_2(t) = s_{LOQ}(t)s_Q(t) + \underbrace{\alpha_Q s_{LOQ}(t)}_{Carrier\,feedthrough} \tag{4.28}$$

Solving the trigonometric relationships for Equation 4.27 and 4.28 one finds the following solutions:

Let $\Theta_1 = \Theta_{LOI} + \Theta_I$, $\Theta_2 = \Theta_{LOI} - \Theta_I$ and $K_1 = 0.5A_I A_{LOI}$. Then

$$s_1(t) = K_1\left[\cos\left(\left(\omega_0 + \omega\right)t + \Theta_1\right) + \cos\left(\left(\omega_0 - \omega\right)t + \Theta_2\right)\right] + \alpha_I s_{LOI}(t) \tag{4.29}$$

Let $\Theta_3 = \Theta_{LOQ} + \Theta_Q$, $\Theta_2 = \Theta_{LOQ} - \Theta_Q$ and $K_2 = 0.5A_Q A_{LOQ}$. Then

$$s_2(t) = K_2\left[\cos\left(\left(\omega_0 + \omega\right)t + \Theta_3\right) + \cos\left(\left(\omega_0 - \omega\right)t + \Theta_4\right)\right] + \alpha_I s_{LOQ}(t) \tag{4.30}$$

Observe that the up-converter uses an ideal adder. Therefore the up converted signal will be given by

$$s(t) = s_1(t) + s_2(t) \tag{4.31}$$

For the particular case where: $\Theta_I = \pi/2$, $\Theta_Q = 0$, $\Theta_{LOI} = \pi/2$, $\Theta_{LOQ} = 0$, $\alpha = \beta = 0$, $A_I = A_Q = A_{BB}$ (where $A_{BB}$ is the amplitude of the baseband input signal) and $A_{LOI} = A_{LOQ} = A_{LO}$, the signal at the output of the up-converted is given as

$$s(t) = A_{BB}A_{LO}\cos(\omega_0 - \omega)t \tag{4.32}$$

Observe that the sign of the angular frequency $\omega$ is negative. This means that there is spectrum inversion of the signal. [3] This can be avoided if instead of adding both signals they are subtracted. The output signal of the ideal up-converter is depicted in Figure 4.8.

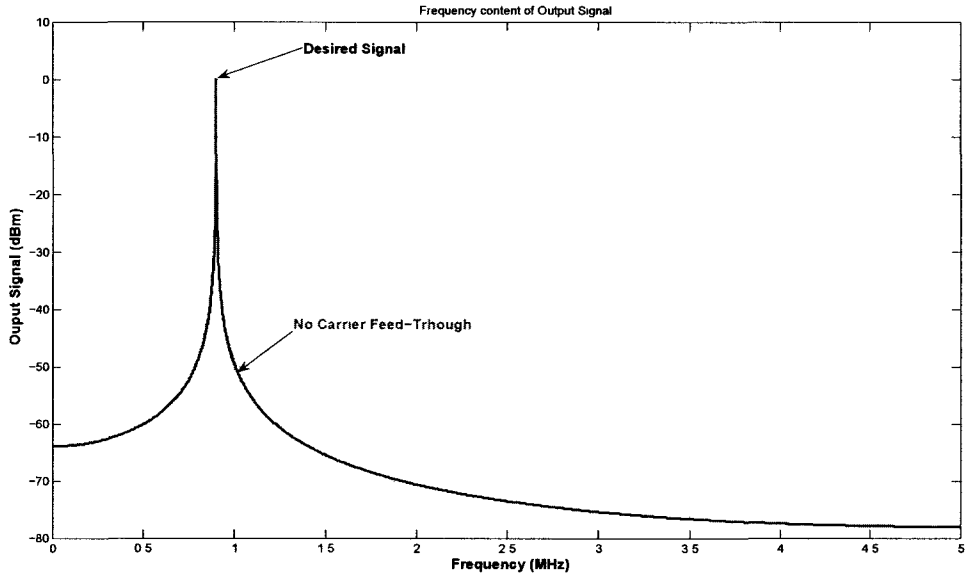


Figure 4.8: Output signal without imperfections

**Example** This example shows the output imperfections of the spectrum generated by carrier feedthrough, $I$ and $Q$ imbalance and nonlinearity in the mixers. Figure 4.8

[3]Spectrum inversion occurs during the transmission when the low part of the baseband signal is up converted for higher band and the higher part of the baseband is up converted to low band. This phenomenon is common in transmitters and when it does occur, it needs to be corrected at the demodulator; the correction takes place by applying another spectrum inversion.

depicts the output signal in the frequency domain for a single tone test applied at the baseband inputs (*I and Q*) of the modulator that is shown in Figure 4.7. For this example, a 1MHz carrier is used and the baseband frequencies are at 100KHz. (In *ISO14443* its a 13.56MHz carrier and the bandwidth is 100KHz)

The signal below shown by Figure 4.9 was obtained using the sum of Equations 4.33 and 4.34. These equations include more details and represents more practical implementation than Equation 4.31. During the discussion about non-linearity, the effects of non-linearities in devices were discussed. Therefore there will be generation of undesired frequencies at the output of the device. The effect of non linearity and *I and Q* imbalance are non-correlated so they can be treated independently. Now let us introduce non-linearity in the equations and show the effect mathematically and graphically. To consider the second and third order non-linearities, let us define their coefficients $K_{nd}$ and $K_{th}$ for second and third order respectively. The superior branch in Figure 4.7, the output signal after the mixer when introducing the effect of non-linearities is given as

$$s_1(t) = s_{LOI}(t)s_I(t) + \underbrace{K_{nd}\left[s_{LOI}(t)s_I(t)\right]^2 + K_{th}\left[s_{LOI}(t)s_I(t)\right]^3}_{Non-linearities} + \underbrace{\alpha_I s_{LOI}(t)}_{Carrier\,feedthrough} \tag{4.33}$$

For the inferior branch the output of the mixer is given as

$$s_2(t) = s_{LOQ}(t)s_Q(t) + \underbrace{K_{nd}\left[s_{LOQ}(t)s_Q(t)\right]^2 + K_{th}\left[s_{LOQ}(t)s_Q(t)\right]^3}_{Non-linearities} + \underbrace{\alpha_Q s_{LOQ}(t)}_{Carrier\,feedthrough} \tag{4.34}$$

Let us assume an *AWGN* $\eta(t)$ with zero mean and variance $\sigma^2$ added in the local oscillator. Using Equations 4.33 and 4.34 to define $s_1(t)$ and $s_2(t)$ in 4.31 with $A_q - A_i = 0.1$, and $\alpha_I = \alpha_Q = 1e^{-2}$, we obtain Figure 4.9 which depicts the plot the *FFT* calculated with 4196 points for the up-converter output time domain signal $s(t)$.

One sees in Figure 4.9 the output signal at 900KHz (Frequency value chosen arbitrarily) together with carrier feedthrough at 1MHz and side-band suppressed signal at 1.1MHz. Other signals present at the output represent second and third order non-linearities , as illustrated.

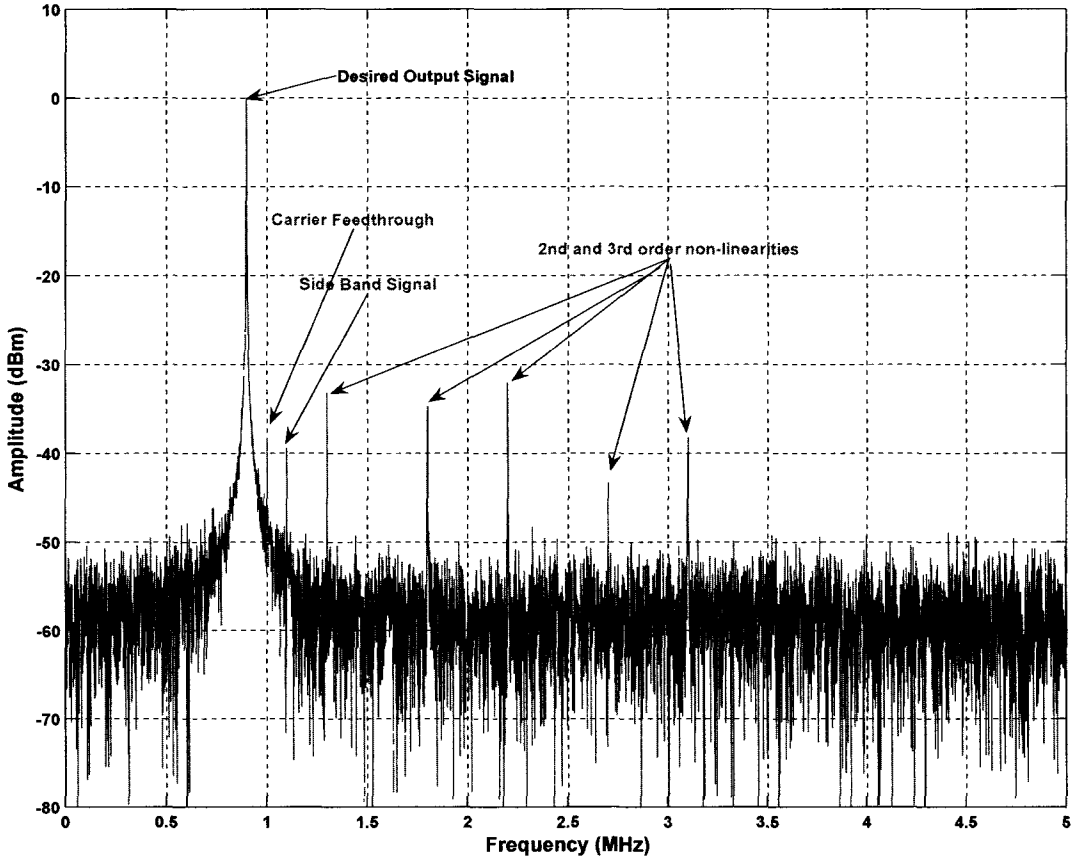


Figure 4.9: Imperfections in output signal

### 4.1.4 *ADC* Imperfections and Impact in *SNR*

All digital demodulators have analog to digital converters (*ADCs*) just after the down converters. *ADCs* are responsible for transforming the analog down converted *I* and *Q* signals into digital quantized signals. In this section we analyze the effects of the imperfections generated by the *ADCs* in the quantized signal and estimate the *SNR* degradation caused by this type of imperfection. This analysis will provide a process for the designer to be able to select of either an *OTS* integrated circuit or predict the best fit *ADC* during the system design specifications.

The number of levels during quantization is a function of the number of bits built in the *ADC*. There are two major questions that arise during the design of the baseband system:

- What is the minimum sample rate that can be used and still meet the system requirements?
- How many bits are required in order to fulfil the design requirements?

The answer to the first question is based on the Nyquist theorem that bounds the minimum sampling rate to twice of the maximum frequency $f_{max}$. This is a lower bound and if the *DAC*'s sampling rate is increased, it will improve the performance of the system because it will reduce the *SNR* effect. On the other hand, the power consumption and the price of the device will increase as well, which is really undesirable. The second question is harder to answer and it will be discussed in detail throughout this section.

#### Analysis

An *ADC* with $N$ bits can produce $2^N$ coded outputs. Let the operational voltage range be from -V to +V. Then the total voltage allowed at the input of the *ADC* is 2V. This is the maximum input voltage or dynamic range of the *ADC*. For simplicity, let us assume a uniform quantizer with $N = 2$ bits output. The possible output code set for this device is then [00 01 10 11] and the output code is a function of the input voltage

is coded as

$$Code = \begin{cases} 11, & \text{if } V_{in} > V_1; \\ 10, & \text{if } 0 < V_{in} < V_1; \\ 01, & \text{if } -V_1 < V_{in} < 0 \\ 00, & \text{if } V_{in} < -V_1 \end{cases} \tag{4.35}$$

Figure 4.10 shows the output code set as function of the input continuous voltage $v_{in}$. Since the number of bits is finite, an estimation error (quantization error) or quantization noise will appear at the output because not all input levels of the continuous signal can be represented by the set of codes available. This quantization noise is function of the step $\Delta$. The quantization error ($e$) is defined as $e = v_{in} - v_{coded}$ where $v_{coded}$ is the equivalent analog voltage of the coded output.

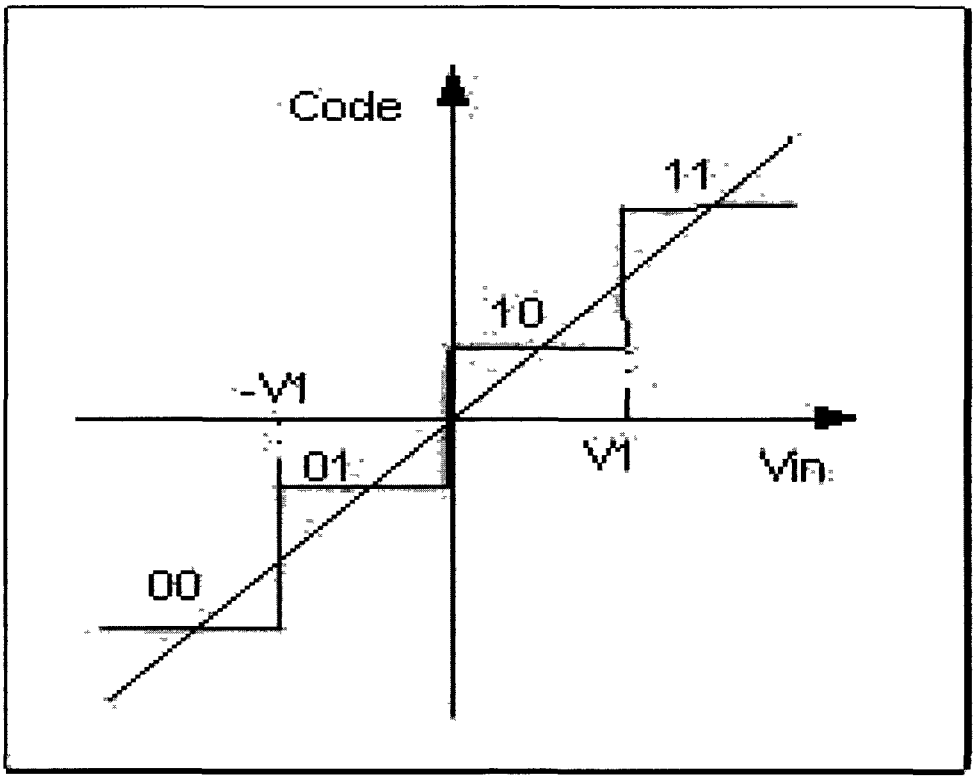


Figure 4.10: Quantization

Let $\Delta$ be the size of the voltage steps for an *ADC* with $2^N$ possible codes and input voltage range $2V$. The *ADC* output error is bounded by: $-\frac{\Delta}{2} \leq e \leq \frac{\Delta}{2}$ and the quantized noise, which is a function of the number of steps is given by Equation 4.40. The

occurrence in the input levels is assumed to have equal probability.

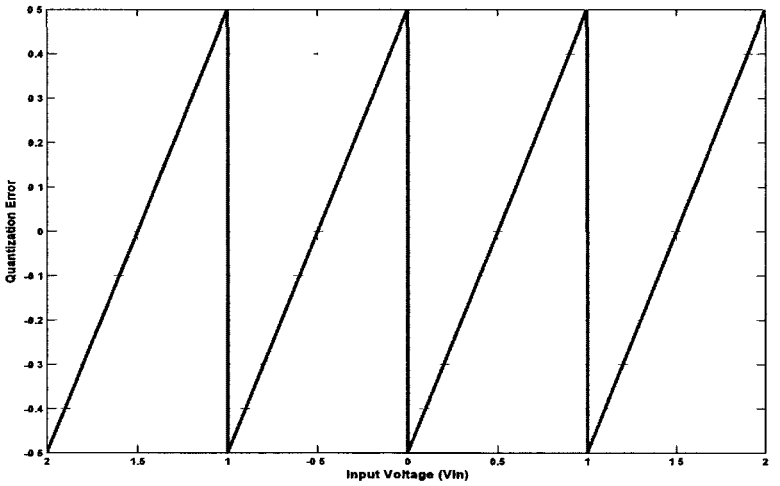


Figure 4.11: ADC Quantization error

Figure 4.11 depicts the quantization error function $e$ and it has a sawtooth shape. Let us assume that our quantizer is uniform [4]. Let $p(e)$ be the quantization error probability and can be described as

$$p(e) = \begin{cases} \frac{1}{\Delta}, & \text{if } \frac{-\Delta}{2} \leq e \leq \frac{\Delta}{2}; \\ 0, & \text{otherwise} \end{cases} \tag{4.36}$$

Since this is a probability density function, we must have [33, Ch3]

$$\int_{\frac{-\Delta}{2}}^{\frac{\Delta}{2}} p(e)de = 1 \tag{4.37}$$

Let $E(.)$ be the expected value of a function. The root mean squared error (*rms*) is the expected value of the square of the error, $e_{rms} = E(e^2)$ [25, Ch2] and here it can calculated as

[4] A uniform quantizer is one such that every change in the *LSB* (least significant bit) at its output, it represents the same variation on the input voltage, independent of the voltage input value. Another way to define the uniform quantizer is to say it is a quantizer such that the quantization steps $\Delta$ do not change with input level.

$$E(e^2) = \int_{-\infty}^{+\infty} e^2 p(e) de = \frac{\Delta^2}{12} \tag{4.38}$$

If the sampling frequency is $f_s$, the power spectrum density of the quantization noise will appear between $+f_s/2$ and $+3f_s/2$ and it folds into the band from 0 to $f_s/2$.

The power spectrum density of the quantization error is a function of the frequency $f$ denoted $e^2(f)$. Assuming that the band of interest is $f_s/2$, its value per Hz is given as:

$$e^2(f) = \frac{e^2_{rms}}{f_s/2} = \frac{\Delta^2}{6f_s} \tag{4.39}$$

The quantization noise can be calculated using the spectrum density of the *rms* error. Let $f_{max}$ be the maximum frequency such that $f_s \geq 2f_{max}$ (Nyquist theorem). Then one can calculate the total noise in the interest band $[0 \ to \ f_{max}]$ as follows.

Let $OSR = f_s/2f_{max}$ be the over-sampling [5] rate

$$\eta_0^2 = \int_0^{f_0} e^2(f) df = \int_0^{f_0} 2Te^2_{rms} df = \frac{\Delta^2}{12OSR} \tag{4.40}$$

For an *ADC* with $N$ bits the full scale voltage which does not saturate it is $V_{max} = 2^N - 1$, From this, the signal power and *SNR* can be calculated.

To calculate the power, let us assume that the signal is loaded with $Z_{load} = 1\Omega$ load. Therefore the power is given as

$$P = \left(\frac{V_{max}}{2\sqrt{2}}\right)^2 \frac{1}{Z_{Load}} = \frac{(2^N - 1)^2 \Delta^2}{8} \tag{4.41}$$

For $N$ greater than 6 we [6] can approximate $(2^N - 1)^2 \approx 2^{2N}$ and the *SNR* is given as

$$SNR_{dB} = 10log_{10}\left(\frac{P}{\eta_0^2}\right) \approx 6.02N + 3log_2(OSR) + 1.76 \tag{4.42}$$

Consequently, having the number of bits $N$ and over-sampling factor ($OSR$) one can calculate the *SNR*. We plot *SNR* as a function of the *OSR* for various values of N in Figure 4.12, and *SNR* as a function of N for various values of *OSR* in Figure 4.13.

[5]Over-Sampling: It is the sampling rate above the minimum from Nyquist theorem. For example, for a signal that has a maximum frequency of 10MHz, if it is sampled at 30MHz the over-sampling rate is 1.5, 50% more than the minimum requirement.

[6]Due to *SNR* and dynamic range requirements for the systems, it is impractical to use *ADC* with less than 6bits.

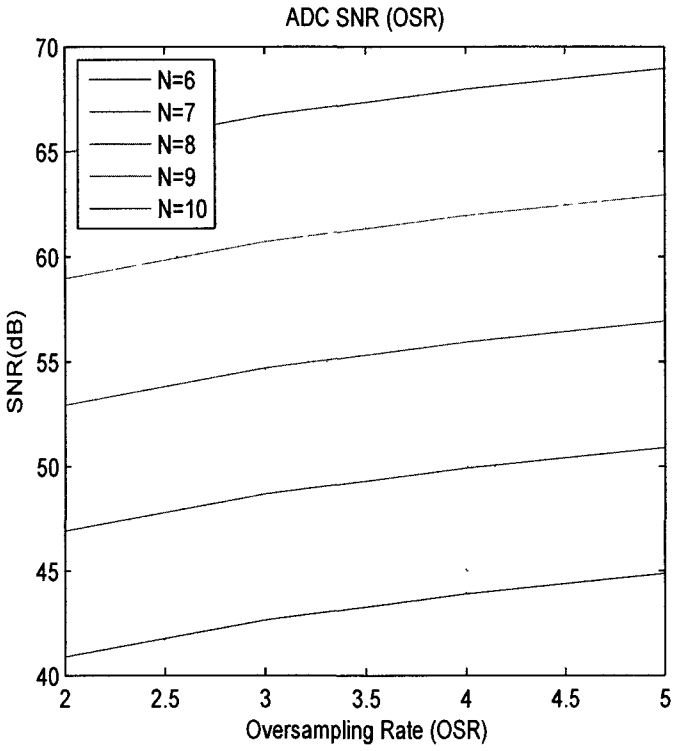


Figure 4.12: SNR function of over-sampling rate

Let us now consider Figures 4.12 and 4.13. One observes that by increasing the number of bits N, the *SNR* increases linearly as shown by Equation 4.42. Increasing *OSR* does not increase *SNR* at the same rate as the number of bits does. To conclude, the best practical approach to increase *SNR* at the output of the *ADC* is to increase the number of bits. Due to cost constraints, however, the designer may be required to apply a trade off between the number of bits and *OSR*.

So far we have presented many component imperfections that affect the performance of the communication between *TAG* and rogue *Reader*. These imperfections were presented independently. In the next section, the combined effect of the imperfections.

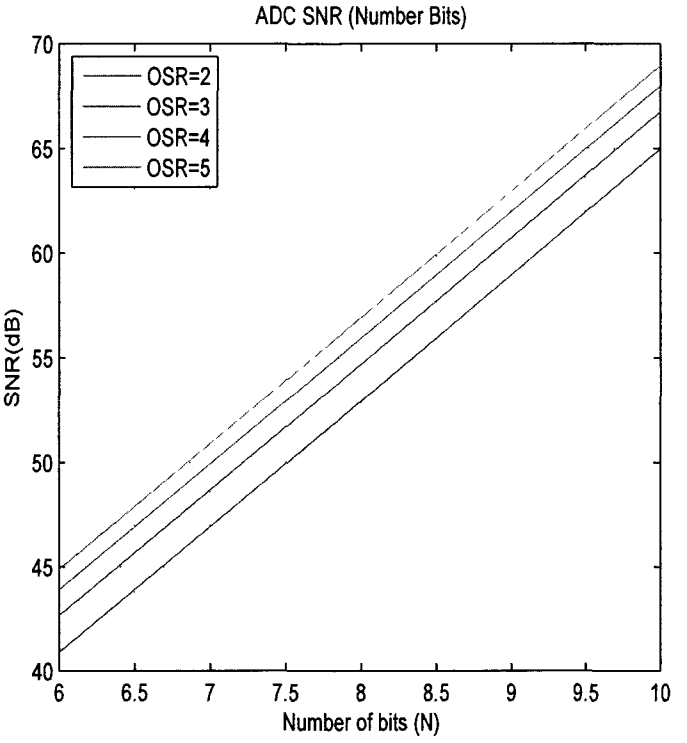


Figure 4.13: SNR as function of the number of bits

## 4.2 Error Vector Magnitude - EVM

One way to analyze the quality of a signal is the *EVM* which is an indirect measurement of the *SNR*. In digital communication transmitters, *EVM* measures how precisely the transmitter has reproduced the vectors $I$ and $Q$. This type of measurement characterizes the performance of the transmitters. For receivers, *BER* is more frequently used. In this section, we analyze how the imperfections affect the *EVM*:

- Phase Noise
- I and Q Imbalance
- Carrier feedthrough
- Intermodulation

We begin by carefully defining *EVM*. Let us denote by $\Re[.]$ and $\Im[.]$ respectively the real and imaginary parts of a complex number, which in this analysis is the modulated base band signal that will be upconverted to radio frequencies. Let $s$ be a reference ideal complex modulated signal that contains In-phase and In-quadrature components $s = \Re[s] + j\Im[s]$ where $j = \sqrt{-1}$. An observed non ideal signal $s_o(t)$ contains In Phase and In Quadrature components. Consequently, the observed signal has an error that is expressed by $e(t) = s(t) - s_o(t)$. Let the observed signal at instantaneous sample time $t_i$ be $s(t_i) = A(t_i)\left[\cos \omega t_i + \phi(t_i)\right]$. Then the *EVM* can be defined as

$$EVM(t_i) = \frac{|e(t_i)|}{|s(t_i)|} = \frac{\left|s(t_i) - s_{opt}(t_i)\right|}{|s(t_i)|} \tag{4.43}$$

Graphically, the *EVM* is shown by Figure 4.14

For K samples of the signal, the root mean squared *EVM* can be calculated as per [44]

$$EVM_{rms} = \sqrt{\frac{1}{K}\sum_{i=1}^{K}\left(\frac{|s(t_i) - s_o(t_i))|}{|s(t_i)|}\right)} \tag{4.44}$$

We have seen in previous sections that there are many sources of imperfections in the system. These imperfections are translated into *EVM* so the total *EVM* can be calculated as [44]

$$EVM_{total} = \sqrt{EVM_1{}^2 + EVM_2{}^2 + \cdots + EVM_L{}^2} \tag{4.45}$$

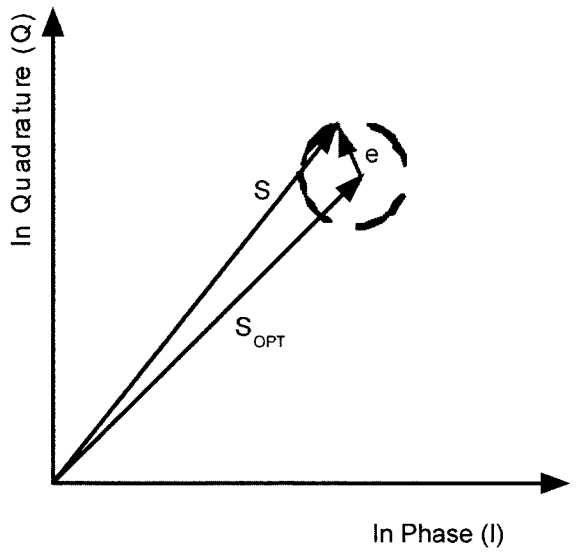


Figure 4.14: Graphical representation of *EVM*

One very useful characteristic of the *EVM* is that it represents the quality of the signal, in the sense that it can be related to the *SNR* through the following equation [41]

$$SNR \approx 20\log_{10}\left(\frac{1}{EVM(\%)}\right) \tag{4.46}$$

Thus system engineers can verify the values of the resulting *SNR*. We now show how to calculate the *EVM* contribution for each imperfection independently.

**Phase Noise** In [44], Plett shows that the *EVM* is a function of the integrated phase noise over the band of interest. Let $e_{PN}(t_i)$ be the error due to *PN* at instant $t_i$. The error vector is defined as $|e_{PN}(t_i)| = \left|s(t_i)\sin(\int(PN_{rms}))\right|$. For small angles $\sin(angle) \approx angle$, and so we may approximate $|e_{PN}(t_i)| \approx s(t_i)\int PN_{rms}$.

Let $EVM_{PN}$ be the *EVM* contribution due to *PN*. Applying Equation 4.43, the *EVM* due to phase noise is given as

$$EVM_{PN} = \frac{s(t_i)\int PNdf}{s(t_i)} = \int PNdf \tag{4.47}$$

**I and Q Imbalance** I and Q imbalance can occur due to two different practical implementations: 1) Phase difference due to the LO $\theta_{LO}$ 2) Amplitude difference due to I

and Q mismatch at the base-band.

Let us analyze the first case where the phase difference is in the LO ($\theta_{LO}$). In this case [44] provides the *EVM* function of the LO phase imbalance. which is simply

$$EVM_{LO} = \theta_{LO} \tag{4.48}$$

Let us analyze the effect of amplitude mismatch. Equation 4.22 and 4.23 provide the base-band signals. Ideally the amplitudes of these signals are equal and $A_I = A_Q = A$ holds. Let $\delta$ be the magnitude error of I and Q respectively. The error vector is given as

$$e = \sqrt{(\delta I)^2 + (\delta Q)^2} = \delta\sqrt{(I)^2 + (Q)^2} \tag{4.49}$$

Thus the *EVM* can be calculated as

$$EVM = \frac{|e|}{|s|} = \delta \tag{4.50}$$

**Carrier Feedthrough** Let $C_{FT}$ be the Carrier feedthrough, which is defined as the residue carrier that passes through the mixer and appears at its output. Ideally this value should be zero but generally it of the order of 30dBc (see [44]). This usually occurs due to imperfections/tolerances of the radio frequency Integrated circuit process used. Recalling the up-converter Equations 4.33 and 4.34, we have that the contribution of the $C_{FT}$ is given as

$$C_{FT}(t) = \alpha_I s_{LOI}(t) + \alpha_Q s_{LOQ}(t) \tag{4.51}$$

If we consider the $C_{FT}$ as an independent effect, we can assume that the absolute value of the in-phase and quadrature signals are equal and we can write $|s_{LOI}(t)| = \left|s_{LOQ}(t)\right|$. Then the function $C_{FT}$ can be written as

$$C_{FT}(t) = \sqrt{\alpha_I^2 + \alpha_Q^2}\,|s(t)|\,e^{j\omega t} \tag{4.52}$$

Let $A_{BB}$ be the baseband amplitude such that $A_{BB} \in \left[A_I, A_Q\right]$. Let $C_s$ be the carrier suppression value which is defined as the ratio between $C_{FT}$ power ($P_{cft}$) and channel power $P_c$. Therefore, the carrier suppression is given as

$$C_s = \frac{P_{cft}}{P_c} = \frac{\alpha_I^2 + \alpha_Q^2}{A_{BB}^2} \tag{4.53}$$

In [44] the author states that the *EVM* resulting from the carrier feedthrough in the output of the transmitter is the square root of the carrier suppression. Consequently one has

$$EVM_{cft} = \sqrt{\frac{P_{cft}}{P_c}} = \frac{\sqrt{\alpha_I^2 + \alpha_Q^2}}{A_{BB}}. \tag{4.54}$$

**Intermodulation** Non-linearity in the transmitter can cause *EVM*. As we saw earlier, third order intermodulation can cause in-band terms. From [44] we have the *EVM* as function of the triple bit tones power $P_{3rd}$; the *EVM* can be calculated as a ratio of the power of the triple bit tones to the power of the channel:

$$EVM_{lin} = 10^{\frac{1}{20}[2P_{3rd} - 2OIP_3 + 6 + 10log10(\frac{3}{8}N^2)]} \tag{4.55}$$

## 4.3 Sensitivity Study

Throughout this chapter we have analyzed many factors that contribute for the degradation of the performance of the communication system between rogue *Reader* and *TAG*. This section focus on the sensitivity study of this system. The study will include the degradations caused by the component imperfections seen so far throughout this chapter. We begin by defining the noise factor and thermal noise and then calculate the calculation the sensitivity of the system.

### 4.3.1 Thermal Noise, Noise Factor and Noise Figure

During the system sensitivity analysis, noise figure is one dominant factor that degrades the system performance. This section is the background for the sensitivity analysis in Chapter 5. We also discuss the meaning of noise figure $N_f$ in a specific device and the overall effect of $N_f$ in the performance of a system.

*Thermal* noise is also known as Johnson noise, is caused by the random variation of electrons inside the devices. The Nyquist's function for thermal noise is given as:

$$\eta = kTB \tag{4.56}$$

where $k = 1.3810^{-23} J/^oK$ is Boltzmann's constant, T is the absolute temperature Kelvin and $B$ is the bandwidth in Hz.

Let $SNR_{in}$ be the input signal-to-noise ratio and $SNR_{out}$ be the output signal-to-noise ratio. The noise figure measures how much noise a given electronic device adds to the input noise. This characteristic gives a very important criterion for selecting a low noise amplifier (*LNA*).

Let $F$ be the noise factor of a device. It is defined as

$$F = \frac{SNR_{in}}{SNR_{out}}. \tag{4.57}$$

The noise figure $N_f$ is given as

$$N_f = 10 \log_{10} F. \tag{4.58}$$

**Noise Factor of Cascading devices**

Let us assume we have three electronic devices (e.g., amplifiers, filters,etc.), each one of which has linear gain $G_i$ and thermal noise $\eta_i$ where $i = 1, 2, 3$. Now let us cascade these three devices and apply at the input a signal with strength $S_{in}$ and noise $\eta_{in} = kT$ that has a bandwidth equal to 1Hz. The system will produce an output signal with strength $S_{out}$ and noise $\eta_{out}$. One has

$$S_{out} = S_{in} G_1 G_2 G_3. \tag{4.59}$$

Observe that the noise at the output of the first device is generated by the first device only. It appears at the output of the chain multiplied by the gains of the second and the third devices. The noise at the output of the second device is generated only by the second device, and appears at the output of the chain multiplied by $G_3$. The total noise at the output of the chain is given as the sum of the input noise multiplied by the cascaded gain, plus each of the devices' noises multiplied by the gain of the following elements (if any). That is, the total noise at the output is:

$$\eta_{out(total)} = \underbrace{\eta_{in} G_1 G_2 G_3}_{\eta_{out(Source)}} + \underbrace{\eta_{o1} G_2 G_3 + \eta_{o2} G_3 + \eta_{o3}}_{\eta_{out(Syst)}} \tag{4.60}$$

Here $\eta_{out}(source)$ is the noise contribution at the output of the chain due to the input signal noise only and $\eta_{out}(syst)$ represents the noise contribution at the output of the chain by the noise generated by the electronic components used in the system.

Substituting Equation 4.59 and Equation 4.60 into Equation 4.57 one finds the total noise factor $F_{total}$ is given by

$$\begin{aligned} F_{total} &= \frac{SNR_{in}}{SNR_{out}} = \frac{S_{in}}{\eta_{in}} \frac{\eta_{out(total)}}{S_{out}} \\ &= \frac{\eta_{in}G_1G_2G_3 + \eta_{o1}G_2G_3 + \eta_{o2}G_3 + \eta_{o3}}{\eta_{in}G_1G_2G_3} \\ &= 1 + \frac{\eta_{o1}}{\eta_{in}G_1} + \frac{\eta_{o2}}{\eta_{in}G_1G_2} + \frac{\eta_{o3}}{\eta_{in}G_1G_2G_3} \end{aligned} \tag{4.61}$$

The first noise factor is given by

$$\begin{aligned} F_1 &= \frac{SNR_{in}}{SNR_{o1}} = \frac{S_i}{\eta_{in}} \frac{(\eta_{in}G_1 + \eta_{o1})}{S_i n G_1} \\ &= \frac{\eta_{in}G_1}{\eta_{in}G_1} + \frac{\eta_{o1}}{\eta_{in}G_1} \\ &= 1 + \frac{\eta_{o1}}{\eta_{in}G_1} \end{aligned} \tag{4.62}$$

Similarly, three cascaded devices the noise factor is given as

$$F_{total} = F_1 + \frac{F_2 - 1}{G1} + \frac{F_3 - 1}{G_1G_2} \tag{4.63}$$

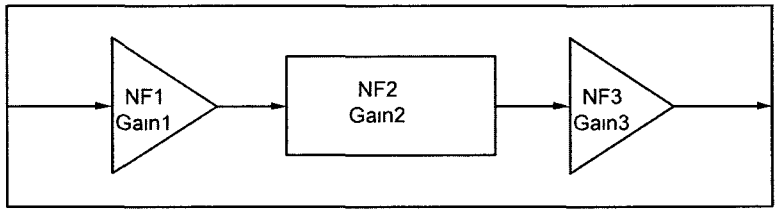


Figure 4.15: System with several components

For $n$ cascading devices, [5, Ch4] shows that the total noise factor is given as per 4.64

$$F_{Total} = F_1 + \frac{F_2 - 1}{G1} + \frac{F_3 - 1}{G_1G_2} + \cdots + \frac{F_n - 1}{G_1G_2G_{n-1}} \tag{4.64}$$

Looking carefully at this equation, we deduce a couple of important factors:

- The noise figure of the total system is dominated by the noise figure of the first device in the chain.

- The noise figure of the total system decreases with the gain of the first device. This means that we need to avoid the use of passive (lossy) elements at the front of the chain.

### 4.3.2 System Sensitivity

For a given receiver, the *BER* at the output of the demodulator is a function of the *SNR* at the input of the demodulator. Let $P_{Rx}$ be the received power at the *LNA*, $P_{Tx}$ the transmitted power, $G_{Tx}$ and $G_{Rx}$ the gain of the transmitter and receiver antennas and *FSL* the channel attenuation (Free space loss or path loss); all in log form (*dBm* and *dB*) The received signal level at the input of the receiver is given by

$$P_{Rx} = P_{Tx} + G_{Tx} + FSL + G_{Rx} \tag{4.65}$$

The signal-to-noise ratio in the receiver is the ratio of the received power and total noise $\eta_t$. The total noise $\eta_t$ is the sum of the thermal noise (4.56) and noise factor

$$\eta_t = \eta + N_f = -174dBm/Hz + 10\log_{10}(B) + N_f \tag{4.66}$$

## 4.4 Channel Link Budget

In this section we present the link budget calculation for a communication system where the transmit and received antennas are located in the far field region. Figure 2.1 represents a typical system architecture, although many variations on this architecture are possible. In Chapter 2 the relay attack system is composed of a rogue *Reader*, communication system, a rogue *TAG* and a legitimate *Reader*. The link budget dictates the maximum distance over which the system will operate for a given *BER*. The activation range analysis is provided in Chapter 5.

Let *FSL* be the path loss attenuation in free space, $d$ be the distance between *TAG* and rogue *Reader* and $\lambda$ be the wavelength. In free space the path loss of the channel is defined as in Equation 3.16.

The next step is to determine the link budget based on Figure 4.16. Observe that the rogue *Reader* has a transmitter and a receiver. By analyzing the link budget we can determine which device is more critical in this system.

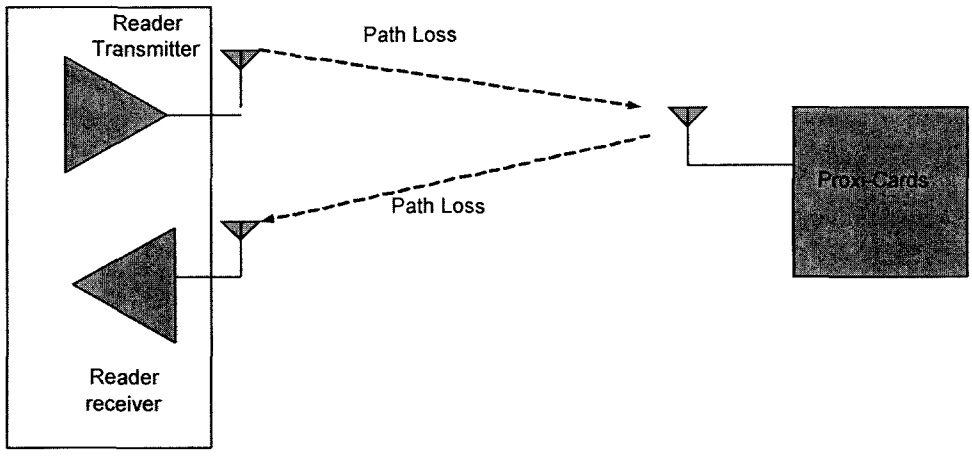


Figure 4.16: Attack system

In this section we present the link budget analysis for the system shown by Figure 4.16. As starting point let us assume we have a *SISO* (Single Input Single Output) communications system as depicted by Figure 4.17.

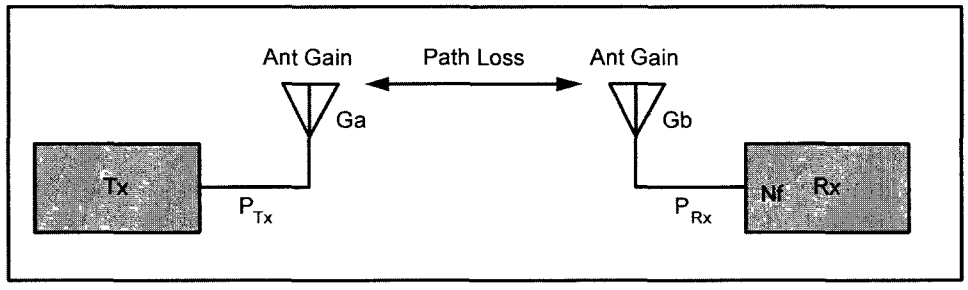


Figure 4.17: Link budget

The system is composed of a transmitter (Tx), the transmit antenna with a gain $G_{RTx}$, a receive antenna with gain $G_{TRx}$ and receiver circuitry that includes a *LNA* (Low Noise Amplifier), down converter and demodulator.

### Received Power

In the absence of any additional interference[7], the receiver power $P_{Rx}$ (measured in *dBm*) is the transmitter isotropic irradiated power (measured in *dBi*) minus the channel

[7]Here we refer to additional interference such as that created by any telecommunications equipment transmitting in a given frequency that is interfering with the given device. Details about interference during *TAG* and *Reader* communications is covered in detail in Chapter 5.

attenuation. For this type of communications there is no need to consider selective fading because this is a narrow band communication protocol. The received power can be thus calculated as 4.65 where *FSL* is defined in Section 3.4 and measured in *dB*. For simplicity, we use *dB* and *dBm* for power measurements rather than *W* or *mW*.

In its multiplicative form, one can write the received power as $P_{Rx} = P_{tx} g_a l(d, f) g_b$. Notice that in the multiplicative form (linear form), $P_{Rx}, P_{tx}$ are measured in Watts or submultiple, $g_a$ and $g_b$ are factors usually greater than one and $l(d, f)$ is a factor less than one. For a given system the $N_f$ is defined as the ratio of input and output *SNR*. The lower the noise figure (or noise contribution) the better the *LNA* is.

The required *SNR* is dependent on the modulation type used by the system and the maximum acceptable *BER*. Using Table 2.2, the *SNR* can be selected according to the type of modulation in use. For a given receiver performance, the *SNR* can be estimated as function of the total noise of the receiver and the input power, via

$$SNR(dB) = P_{Rx} - \eta_t. \tag{4.67}$$

In other words, Equation 4.67 says that if we minimize the total noise $\eta_t$ while keeping the distance constant, the performance at the receiver will improve. On the other hand, for a given performance — for example $BER = 10^{-6}$ (see Section 5.3.1 for details) — the transmitter can be located farther away.

## 4.5 Conclusion

In this chapter we presented tools for estimating the performance of a communication system focusing on *RFiD Relay attack* requirements. We discussed how to estimate the contribution of each main circuit imperfection. The effects of Intermodulation is presented in Section 4.1.1, phase noise contribution of an oscillator to the overall system noise was analyzed in Section 4.1.2, *ADC* quantization noise was introduced in Section 4.1.4, in Section 4.3.1 we analyzed the noise figure and we also presented the link budget calculation in Section 4.3.2.

All topics covered by this chapter are relevant for the system level design but one topic that deserves special attention is the contribution in *SNR* by *ADCs* and how the over-sampling ratio plays a role in increasing the *SNR* for a fix number of bits. This chapter presents a method of calculating the contributions in the *SNR* for each relevant *RF* imperfection. The summed effect of these imperfections will degrade the *SNR*. Therefore, they will contribute with the reduction of the maximum *Victim Distance* Equation 5.3.

# Chapter 5

# Relay Attack Analysis and Model

## 5.1 Introduction

The first four chapters of this thesis provide the basis for the considerations and assumptions made throughout this chapter. Chapter 2 covered the basics of the relay attack, Chapter 3 presented the channel model defining the Far Field/Near Field bound, and Chapter 4 presented how component imperfections such as intermodulation (Section 4.1.1), the noise figure (Section 4.3.1), phase noise (Section 4.1.2) and ADC quantization and oversampling (Section 4.1.4) impact the system performance.

In this chapter, we present an *RFiD* system analysis and use it to estimate the maximum delay that a relay attack system may introduce and the maximum distance at which the rogue Reader may be located relative to the victim's TAG. We then apply the *Simulink* model to simulate the relay attack operation and thus demonstrate its feasibility within these constraints.

An *RFiD* system specifies the maximum delay that is permitted to occur during any component of the interaction between the TAG and Reader, before the communication is terminated. We determine a bound on this delay in Section 5.2, and then calculate and compare the minimum delay introduced by a relay attack, to demonstrate the feasibility of carrying out a relay attack within the time permitted.

The maximum distance $d_{max}$ at which an attacker may locate the rogue Reader from the victim is a significant factor in determining the feasibility of a relay attack. In Section 5.3, we compute the factors which limit $d_{max}$, and verify that local interference is the most confounding factor. Thus, a crucial aspect of mounting a successful relay attack will be the inclusion of an interference canceller in the design, as discussed in

Section 5.3.1. The resulting bound on $d_{max}$ is illustrated in Figure 5.4; we see that for reasonable values of interference cancellation, one can obtain a value of $d_{max}$ of greater than 10 meters.

Finally, in Section 5.4.3 we present our successful simulation of the communication between a rogue Reader and the victim's TAG for an SNR of 11dB, which is a noise level equivalent of BER = $10^{-6}$, and represents the maximum distance achievable. The simulation includes graphs representing each interchange of communication between the rogue Reader and victim's TAG.

## 5.2 Relay System Delay

The maximum time a TAG has to respond to the Reader after the Reader has initiated communication during the authentication process is called the maximum TAG response time, or frame delay time. We illustrate this in Figure 5.1. The *ISO14443* standard specifies this time to be

$$FrameDelayTime = \begin{cases} \frac{n*180+84}{f_c} = RT_1, & \text{Last transmitted bit was equal to '1'} \\ \frac{n*180+20}{f_c} = RT_0, & \text{Last transmitted bit was equal to '0'} . \end{cases}$$

For the *REQA* and *SELECT* commands defined in Chapter 2, ISO14443 recommends $n \geq 9$ [15]. To give the most conservative bound, we choose the smallest delay, and thus set $n = 9$. This gives

$$FrameDelayTime = min\,[RT_o, RT_1]_{(n=9)} = \frac{n * 128 + 20}{f_c} = 86.5\mu s \tag{5.1}$$

The reader may note that we do not consider any time constraint for the *WAKEUP* message. The reason this is not considered is because a *TAG* will only enter the *HALT* state by the *HALT* command after authentication is complete (See Figure 2.4). During the relay attack it is expect that the victim's *TAG* will be authenticated by rogue *Reader*.

### 5.2.1 *RFiD* System Delay Analysis for Relay Attack

Recall that Figure 2.1 shows a typical *RFiD* system under relay attack. The signal must travel from the legitimate Reader to the rogue TAG, then to the rogue Reader, then to the victim's TAG, and then back again. Furthermore, at each *TAG* or rogue Reader,

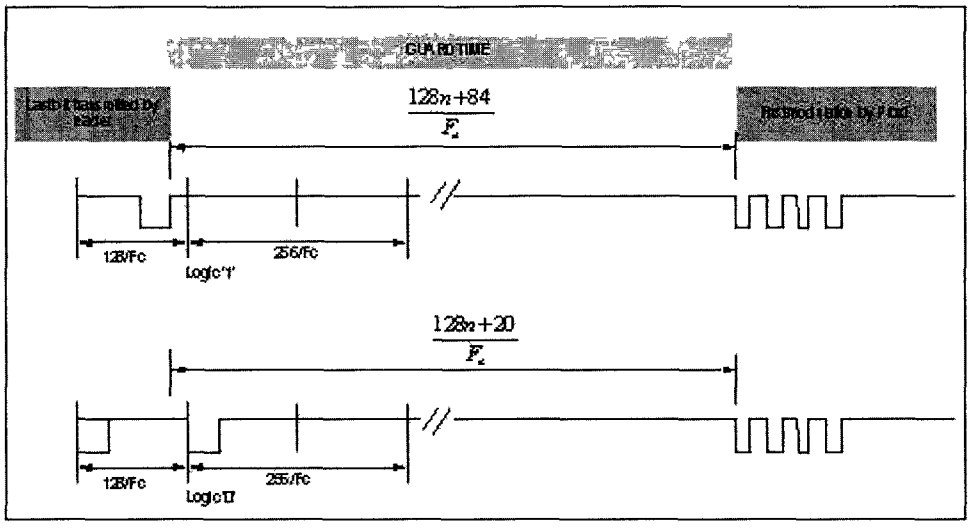


Figure 5.1: ISO14443 frame delay time (taken from [15])

the signal undergoes some processing. Let us analyze the maximum total delay that an attacking system will introduce, $\tau_{max}$.

Let $d_{Vd}$ and $\tau_{Vd}$ be the *Victim Distance* and its propagation delay, $d_{Rd}$ and $\tau_{Rd}$ be the distance between rogue *Reader* and rogue *TAG* and its propagation delay, $d_{RtLr}$ and $\tau_{RtLr}$ be the distance between the rogue *TAG* and legitimate *Reader* and its propagation delay, $\tau_{RtP}$ the rogue *TAG* processing delay, $\tau_{RrP}$ the rogue *Reader* processing delay and $\tau_{TAG}$ the victim's *TAG* delay.

$$\tau_{max} = 2 \times (\tau_{Vd} + \tau_{Rd} + \tau_{RtP} + \tau_{RrP} + \tau_{RtLr}) + \tau_{TAG} \leq 86.5\mu s \tag{5.2}$$

The propagation delay of a signal through space is given by

$$\tau = \frac{d}{c}$$

where $d$ is the distance traveled and $c = 3 \times 10^8$ m/s is the speed of light. Our target is to achieve $d_{Vd} \sim 10$ m, and we may assume that $d_{RtLr} < 0.5$m. In [19], Hancke claims to have performed the relay attack with $d_{Rd} = 50$ m. Thus the total distance traveled should be at least 121 m; let us take $d = 300$ m for a generous upper bound. This gives a total propagation delay of

$$\tau_{prop} = 2(\tau_{Vd} + \tau_{Rd} + \tau_{RtLr}) = \frac{300}{c} = 1\mu s.$$

We see that the contribution of the total relay distance to the delay which is introduced by the relay attack is minimal for this order of magnitude of distances. The delay of the electronic system used in the relay attack is the more serious consideration.

The delay $\tau_{TAG}$ of an RFiD tag was measured by Karthaus and Fisher in [27] to be $10\mu s$. It follows that the maximum delay is given by

$$\tau_{max} = \tau_{prop} + 2(\tau_{RtP} + \tau_{RrP}) + \tau_{TAG} = 2(\tau_{RtP} + \tau_{RrP}) + 11\mu s.$$

Since $\tau_{max} \leq 86.5\mu s$ by (5.1), we deduce that

$$\tau_{RtP} + \tau_{RrP} \leq 37.7\mu s.$$

We see that if our rogue TAG and rogue Reader operate with a delay comparable to a legitimate TAG, that is, if $\tau_{RtP}$ and $\tau_{RrP}$ are about $10\mu s$, then the relay attack can be successfully carried out within the maximum allowed delay time.

## 5.3 Victim Distance Link Budget analysis

Now the analysis will focus on the relay attack system. Our goal with this analysis is to find the *Victim Distance*, which will take several steps.

The maximum *Victim Distance* is dependent on the following factors:

- Minimum energy to power the *TAG* ,$P_{min}$
- Performance of the local interference canceler
- *FSL* between *TAG* and *Rogue Reader*

Let $d_{activ}$ and $d_{ReadRange}$ be the activation and read range distances respectively. The *Victim Distance* ($d_{max}$) will be the minimum of the reading range and the activation range:

$$d_{max} = min\left[d_{activ}, d_{ReadRange}\right]. \tag{5.3}$$

**Activation and reading range steps** To calculate both distances, we will divide the analysis into two paths: the activation range and the reading range.

To calculate the reading range in Section 5.3.1 we perform the following steps:

1. Establish operating *BER* and *SNR*
2. Provide a detailed estimate of the interferences
3. Provide a method of mitigating the interference
4. Estimate the *TAG* received signal strength
5. Calculate $d_{ReadRange}$ using a closed form solution

To calculate the activation range in Section 5.3.2 we establish the minimum power $P_{min}$ that the *TAG* needs to operate, the transmit output power and free space attenuation *FSL*.

### 5.3.1 Reading Range

#### *BER* and *SNR* Requirements

*ISO14443* [14] recommends that the modulated signal type be Pulse Amplitude Modulation (PAM) with 100% of modulation index during communication between *Reader* and *TAG* and 10% for the communication between *TAG* and *Reader*. During the sensitivity analysis it is necessary to establish the maximum Bit Error Rate (*BER*) that the system is allowed to have and still perform the communication properly. *BER* will consequently establish the relation between signal and noise levels present in the input of the detector. Let $P_{err}$ be the error probability of the received *PAM* signal, $M$ the number of levels of the modulation, and *SNR* the average signal-to-noise per symbol. In [40, Ch4], Proakis provides the the error probability relationship for a *PAM* modulated signal as:

$$P_{err} = \frac{M-1}{M} erfc\left(\sqrt{\frac{3}{M^2-1} SNR}\right) \tag{5.4}$$

where $erfc(x)$ is the complementary error function defined as:

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt. \tag{5.5}$$

When a *TAG* transmits a modulated signal, it will be *PAM* with 2 levels, so we may take $M = 2$ in this case. Figure 5.2 shows the theoretical *BER* values for $M = 2$ as a function of the the *SNR* for a signal containing *AWGN*. In this case we assume that this is the only source of impairment.

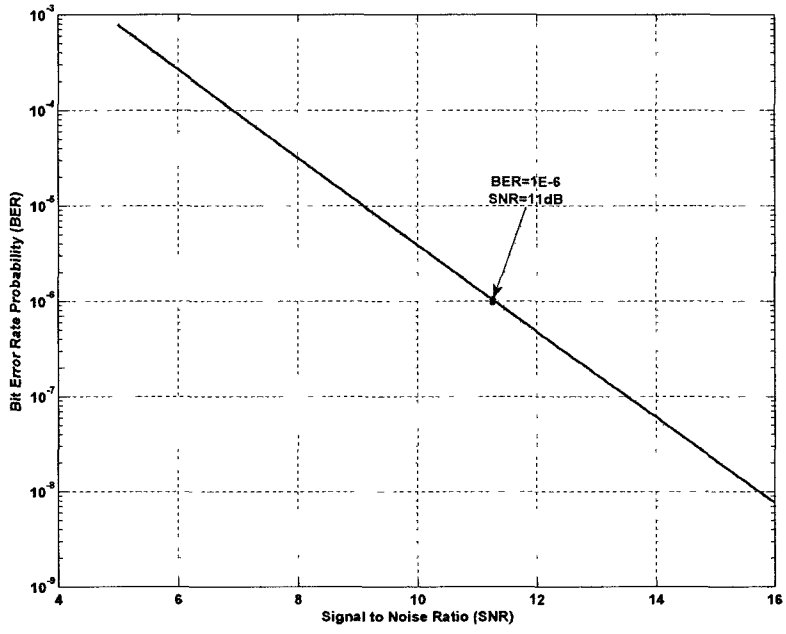


Figure 5.2: Error probability for *PAM* signal

Figure 5.2 shows that for a $BER = 10^{-6}$ a $SNR$ of 11dB is required. This value is the minimum $BER$ for this $SNR$. This $BER$ value will be used to calculate the maximum *Victim Distance*.

To justify the usage of $BER$ equal to $10^{-6}$, let us assume a typical *RFiD* message with 8 bytes. During the identification of the *TAG* let us assume that it needs to exchange 7 messages until it is identified by the *Reader*. The number of transmitted bits during the exchange of the messages will be 448. Let $NBE$ be the percentage of erroneous bits that was received that is

$$NBE = 448 * BER * 100 < 0.05\% \tag{5.6}$$

Using this $BER$ value, the result shown by Equation 5.6 assures that 99.95% of the messages will produce a *CRC* equal to zero. Consequently, the system will achieve more than 99% success during the communication between the two devices.

### Local Interference

*ISO 14443* operates at 13.56MHz. This is low frequency compared with *LAN* networks operating at 2.4 and 5.0 GHz frequencies and other *RFiD* standards using frequencies of 450 and 900MHz. The spectrum at the 13.56MHz frequency band is contaminated by household appliances, and other types of manmade electromagnetic interference. However, the biggest interference in *RFiD* systems is the unmodulated carrier that is being transmitted simultaneously by the *Reader*. This interference can cause two major problems: First the level of the interference signal will decrease the *SNIR;* second the strong transmitted signal induced into the receiver antenna will generate intermodulation distortion that will corrupt the message. [1]. The *Reader* can mitigate this interference by using interference cancelation techniques such as the one described in Section 5.3.1.

Let $i_j(t)$ be an interference component in Watts and $I_k(t)$ its value in dBm. Let $n$ be the total number of interferences components present at the antenna and $k = 1, 2, 3 \ldots m$ be the index of each interference component. The total interference at the receiving antenna can be described as the sum of all **m** interferences present:

$$i_{Total}(t) = \sum_{k=1}^{m} i_k(t) \tag{5.7}$$

### Calculating the Interference

To be able to estimate the minimum received signal required by the rogue *Reader*, it is necessary to estimate the total interference power which is mostly dominated by the unmodulated transmitted carrier. If the rogue *Reader* uses one antenna for transmission and another for reception, there will be a finite signal path isolation (dB) between these two antennas, which can written as $Ant_{rej}$. Therefore, the interference power (dBm), at the receive antenna, generated by the local transmitted carrier is:

$$I_{fc} = P_T - Ant_{rej} \tag{5.8}$$

Let us now assume that the attacker uses the interference cancelation described in Section 5.3.1. Let $Att_{canc}$ be the amount of interference power in (dBm) reduced by the

[1] IIP3, P1dB and other nonlinearities characteristics are covered in Chapter 4

usage of the canceler. Therefore, the total interference power will be reduced by the canceler as follows:

$$I_{fc} = P_T - \left(Ant_{rej} + Att_{canc}\right) \tag{5.9}$$

Now let us analyze what happens with the local interference when the output power varies. Let $v$ be the output voltage and $Z_{ant}$ the output impedance. The output power can be represented as:

$$P_{out} = \frac{v^2}{Z_{ant}}. \tag{5.10}$$

From (5.9) we notice that if the output power increases the interference power level will increase proportionally. This happens because the antenna isolation and interference cancelation mechanisms are independent of the output power.

### A Method to Mitigate the Local Interference

One method to reduce the local interference generated by the *Reader* carrier is to use the well known method of interference cancelation. In this section we present such a method that will minimize the local transmit carrier interference power that couples into the receiver. This will optimize the received *SNR*.

The rogue *Reader* transmitted signal $s(t)$ - that has power $P_t$ - will be coupled into in the receive antenna. The external path between the power amplifier (*PA*), Tx antenna, Rx antenna and the Low Noise Amplifier (*LNA*) will introduce attenuation $\alpha$ as well as a delay that will introduce the change in phase $\phi$. Internally the electronics that compose the interference canceler will intentionally introduce an attenuation $\hat{\alpha}$ and phase $\hat{\phi}$. For more details about the system see Figure 5.3.

The rogue *Reader* receive antenna receives the signal from the *TAG* plus a fraction of $s(t)$ and other interferences present in the spectrum. Let $j = \sqrt{-1}$, let $I_m(t)$ be the local interference and $P_r(t)$ be the received desired power at the rogue *Reader* receive antenna. The total received signal $r(t)$ can be mathematically represented as:

$$r(t) = P_r(t) + \underbrace{\alpha s(t) e^{j\phi}}_{i_m(t)} + \sum_{k=1}^{(m-1)} i_k(t). \tag{5.11}$$

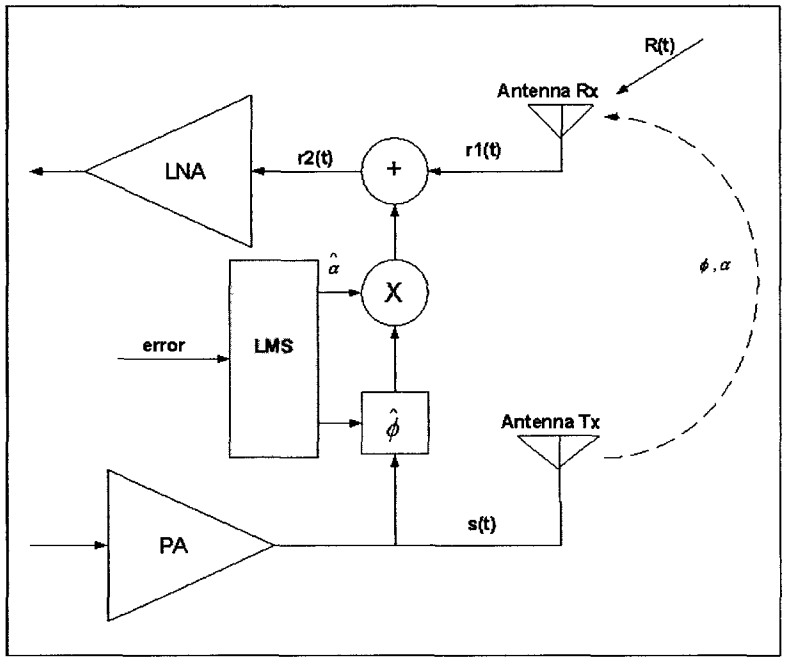


Figure 5.3: Proposal for an interference canceler

For simplicity, let us assume that the dominant interference at the rogue *Reader* receive antenna is the local carrier so one has

$$i_m(t) \gg \sum_{k=1}^{(m-1)} i_k(t) \tag{5.12}$$

The input signal at the *LNA*, denoted $r(t)_{LNA}$, is represented by the sum of the received antenna signal minus the output signal from the interference canceler:

$$r(t)_{LNA} = P_r(t) - \hat{\alpha}s(t)e^{j\hat{\phi}} + \alpha s(t)e^{j\phi}. \tag{5.13}$$

Let $E\left(\hat{\alpha}, \alpha, \hat{\phi}, \phi\right)$ be the error, function defined by

$$E\left(\hat{\alpha}, \alpha, \hat{\phi}, \phi\right) = \left[\alpha e^{j\phi} - \hat{\alpha}e^{j\hat{\phi}}\right]. \tag{5.14}$$

The received signal can be rewritten as

$$r(t)_{LNA} = P_r(t) + s(t)E\left(\hat{\alpha}, \alpha, \hat{\phi}, \phi\right) \tag{5.15}$$

The next step will be to minimize the value of $E(\hat{\alpha}, \alpha, \hat{\phi}, \phi) = E_{Min}$ which will yield $r(t)_{LNA} = r_{opt}$.

A direct form to find the value of $E_{min}$ is the zero forcing the error:

$$\alpha e^{j\phi} = \hat{\alpha} e^{j(\hat{\phi}+\frac{\pi}{2})}. \tag{5.16}$$

After removing the interference of the local carrier as much as the internal electronics is capable of, it is necessary to know by how much the interference signal power is attenuated (dB). To do this we use the following analytic expression to compare with the transmitted signal: Let $I_m(t) = I_{fc}$ be the interference in $dBm$ due to the local carrier, $Pt$ the output power of the rogue *Reader* in dBm when transmitting pure carrier and $Att_{canc}$ be the carrier cancelation in dB done electronically. then we have

$$Ant_{rej} + Att_{canc} = 10\log_{10}\left|\frac{s(t)\left[\alpha e^{j\phi} - \hat{\alpha} e^{j\hat{\phi}}\right]}{s(t)}\right| \tag{5.17}$$

$$Ant_{rej} + Att_{canc} = 10\log_{10}\left|\alpha e^{j\phi} - \hat{\alpha} e^{j\hat{\phi}}\right|. \tag{5.18}$$

In practice, to solve the optimization problem, there are many iterative methods available; a common one is least mean square *(LMS)* algorithm. The algorithm can be trained while neither the rogue *Reader* nor the *TAG* are responding to any message. During this time interval the system channel between rogue *Reader*'s transmitter and receive antenna can be estimated.

In the discrete time domain let $T_s$ be the sampling time and $k = [1, 2, 3, 4, \dots]$ be the sampling index. Given the received signal $r(kT_s)$ and let $\mu$ be a positive scalar, the *LMS* algorithm error function is defined by Campos in Ref [4] the updates are based on the error function in the discrete time domain as follows:

$$E(kT_s) = r(kT_s) - \hat{\alpha}\cos\left(2\pi f_c kT_s + \hat{\phi}\right) \tag{5.19}$$

So shows in [50] that the updates for $\hat{\alpha}$ and $\hat{\phi}$ can be calculated as :

$$\hat{\alpha}((k+1)T_s) = \hat{\alpha}(kT_s) - \frac{\mu_\alpha}{2}\frac{\partial e^2(kT_s)}{\partial \hat{\alpha}(kT_s)} \tag{5.20}$$

$$\hat{\phi}((k+1)T_s) = \hat{\phi}(kT_s) - \frac{\mu_\phi}{2}\frac{\partial e^2(kT_s)}{\partial \hat{\phi}(kT_s)}. \tag{5.21}$$

The coefficients $\mu_\alpha$ and $\mu_\phi$ are positive scalars that controls the convergence rate to ensure the algorithm stability. See [50] for details.

### TAG Received Signal Calculation

We need to understand how much power the *Reader* needs to transmit in order for the received signal at the *TAG* to be greater than the minimum requirement. Passive *TAGs* backscatter the unmodulated carrier received by the *Reader*. The mismatch coefficient $\gamma$ determines how much power the *TAG* sends back to the *Reader* and how much power is left for the *TAG* to remain energized. Passive *TAGs* generally get energized by the unmodulated carrier frequency energy transmitted by the *Reader*. Using the load modulation the *TAG* will reflect back to the *Reader* a portion of the received signal.

Let us assume that during the attack, both antennas rogue *Reader* and *TAG* are static [1] and located in two parallel planes [2] in space. Let $0 \leq \gamma \leq 1$ be the value of the backscattering factor or mismatch factor at the *TAG* antenna and $\Gamma$ its value in *dB*, let $Ag_{RTx}$ and $Ag_{RRx}$ be the transmission and receiver *Reader*'s antennas gains, $Ag_{TAG}$ the *TAG* be antenna gain in *dB*, $P_t$ be the rogue *Reader* output power in watts and $P_T$ be its equivalent power in *dBm*, $P_{Tout}$ be the *TAG* output power in watts and $P_r$ be the rogue *Reader* received power and $P_R$ its equivalent power in *dBm*. Then $P_{RxTAG}$, the *TAG* received power in *watts*, is given as

$$P_{RxTAG} = P_t l(d, f) Ag_{RTx} Ag_{TAG}. \tag{5.22}$$

The transmitted power at the *TAG* antenna is the product of the received power and the mismatch factor $\gamma$

$$P_{Tout} = P_t l(d, f) \gamma Ag_{RTx}. \tag{5.23}$$

The received power at the *Reader* in *watts* is the product of the transmitted power from the *TAG* and the free space loss *l(d,f)*.

$$P_r = P_t l(d, f)^2 \gamma Ag_{RTx} Ag_{RRx}. \tag{5.24}$$

One observes that Equations 5.22 and 5.24 do not include explicitly the *TAG* antenna gains. These gains are included in the reflected power calculation to the rogue *Reader* using the factor $\gamma$. Notice that if $0 \leq \gamma \leq 1$ then $\Gamma = 10 \log\left(\frac{1}{\gamma}\right) \geq 0$. Therefore the received power from the *Reader* can be expressed in logarithm form as:

[1] To exchange all the messages required for the authentication the system will need to exchange approximately 500 bits $\Rightarrow$ *5ms*. Assuming delay and pause within the messages, the system will require around 20ms for the process to end. If the attacker is static and the victim is in movement at 20Km/h the displacement of the *TAG* will be less then 1 cm

[2] If transmit and receive antennas are not located in parallel planes, corrections must be applied to compensate the loss due to the angle of arrival. This situation is not covered by this analysis

$$P_R = P_T - 2FSL(d, f) - \Gamma + 10\log_{10}(Ag_{RTx}Ag_{RRx}). \tag{5.25}$$

The rogue *Reader* is assumed to have two antennas, one for transmission and another for reception. This reduces the interference in the received signal that is generated by the transmitted carrier. See Section 5.3.1 for more details about this topic. If transmit and receive rogue *Reader* antennas have unit gain, Equation 5.25 reduces to:

$$P_R = P_T - 2FSL(d, f) - \Gamma \tag{5.26}$$

**Calculating the Reading Range ($d_{ReadRange}$)**

To calculate the *Reading Range*, first we will need to quantify the amount of noise plus interference present in the receiver. Equation 4.66 provides the total noise at the output of the *LNA*. The signal to noise ratio is 11dB for this application. Let $I_{Total}$ be the total interference at the *Reader* receive antenna. The local interference is a sinusoidal signal. Let *npi* be the noise plus interference value in *dBm* calculated over the signal band $B$ that is given as

$$npi = 10\log_{10}\left[\frac{10^{0.1\left(-174+20\log_{10}(B)+N_f\right)} + 10^{0.1(I_{Total})}}{1mW}\right]. \tag{5.27}$$

The value in *dBm* of the minimum received signal that assures proper communication is given as:

$$Rx_{Min} = SNR + npi. \tag{5.28}$$

Let $rx_{min}$ be the value of $Rx_{min}$ in watts. In linear form, using Equation 5.41 and the received power at rogue *Reader* in *dBm*, the minimum received power at rogue *Reader* can be written as:

$$rx_{Xmin} = 10^{0.1R_{Xmin}(dBm)} = P_{RxTAG}\gamma l(d, f) \tag{5.29}$$

$$10^{0.1R_{Xmin}(dBm)} = P_t l(d, f)^2 \gamma A g_{RTx} A g_{RRx}. \tag{5.30}$$

Isolating the free space attenuation ones we have,

$$l(d,f) = \sqrt{\frac{10^{0.1R_{Xmin}(dBm)}}{P_t \gamma A g_{RTx} A g_{RRx}}}. \tag{5.31}$$

Finally, by inserting equation 5.31 into 3.13 the reading range can be calculated as:

$$d_{ReadRange} = \frac{c}{4\pi f} \sqrt[4]{\frac{P_t \gamma A g_{RTx} A g_{RRx}}{10^{0.1R_{Xmin}(dBm)}}}. \tag{5.32}$$

Now let us calculate the reading range when the interference is much higher than the total noise $\eta_t$. This situation happens when either the isolation between antennas (transmit and receive) is low or when when there is no interference canceler or both. Let us assume that the only independent variable that is going to change is the output power of the transmitter. The total noise plus interference $np_i$ given by Equation 5.33 can be rewritten as:

$$npi \approx 10 \log_{10} \left[ \frac{10^{0.1(I_{Total})}}{1mW} \right] = I_{total} \tag{5.33}$$

The minimum value for the received signal can be calculated from Equation 5.34

$$Rx_{Min} \approx SNR + I_{total} \tag{5.34}$$

The next step is to calculate the read range distance. From Equation 5.32 one can write

$$d_{ReadRange} \approx \frac{c}{4\pi f} \sqrt[4]{\frac{\gamma A g_{RTx} A g_{RRx}}{10^{0.1SNR}}} \sqrt[4]{\frac{P_t}{10^{0.1I_{total}}}} \tag{5.35}$$

$$d_{ReadRange} \approx K \sqrt[4]{\frac{P_t}{i_{total}}} \tag{5.36}$$

where the constant K is given as

$$K = \frac{c}{4\pi f} \sqrt[4]{\frac{\gamma A g_{RTx} A g_{RRx}}{10^{0.1SNR}}} \tag{5.37}$$

Let $\epsilon$ be the linear value that represents the sum $Att_{rej} + Att_{can}$. These values are attenuation so $0 < \epsilon < 1$. From Equation 5.9, one can write it in linear form as

$$i_{total} = i_m(t) = \epsilon P_t \tag{5.38}$$

If we substitute

$$d_{ReadRange} \approx \frac{K}{\sqrt[4]{\epsilon}} \tag{5.39}$$

Therefore one can see that the value of the reading range is constant. This value represents the portion in Figure 5.4 where the distance is constant even as the rogue *Reader* transmit power increases. It follows that $d_{max}$ exists and cannot be increased by increasing power.

### 5.3.2 Activation Range ($d_{activ}$) Calculation

To calculate the activation range, it is required to know the power consumption of the *TAG*, transmitted power and the free space attenuation, Equation 3.13.

Let $P_{TAG_{suppmin}}$ be the minimum power required by the *TAG* to be energized. The total power received at the *TAG* antenna $P_{RxTAG}$ is given at Equation 5.22 and is re-written below:

$$P_{RxTAG} = P_t l(d, f) A g_{RTx} A g_{TAG} \geq P_{TAG_{suppmin}}. \tag{5.40}$$

The *TAG* will reflect some of this power back to the rogue *Reader* and the remainder is used to power the *TAG*, which can be calculated as:

$$P_{TAG_{suppmin}} \geq P_{supp} = P_{RxTAG}(1-\gamma). \tag{5.41}$$

In *dBm* the power the equation can be represented as:

$$P_{supp} = 10\log_{10}\left(\frac{P_{RxTAG}(1-\gamma)}{1mW}\right). \tag{5.42}$$

The energy captured by the *TAG* can be re-written as

$$P_{RxTAG}(1-\gamma) = P_t(l, d) A g_{RTx} A g_{TAG}(1-\gamma) \geq P_{TAG_{suppmin}}. \tag{5.43}$$

Assuming the equality holds and solving for $l(d, f)$ we have

$$l(d_{activ}, f) = \frac{P_{TAG_{suppmin}}}{P_t A g_{RTx} A g_{TAG}(1-\gamma)} = \left(\frac{c}{4\pi f d_{activ}}\right)^2. \tag{5.44}$$

so the activation distance can be calculated as:

$$d_{activ} = \frac{c}{4\pi f}\sqrt{\frac{P_t A g_{RTx} A g_{TAG}(1-\gamma)}{P_{TAG_{min}}}}. \tag{5.45}$$

### 5.3.3 Relay attack link budget - Example

Figure 5.4 depicts the general system analysis budget, which was generated using the data shown in Table 5.1 below. This figure shows that by increasing the rogue *Reader* output power, the *TAG* can be energized at greater distances from the rogue *Reader* ($d_{max}$ will increase). This is true until the *SNR* at the rogue *Reader* receive antenna is degraded below the minimum value (11dB). When the *SNR* reaches this minimum value by increasing the output power, the distance remains constant (flat region of the curve) at a value depending on the reductions or the local interference using an interference cancelation method.

| Item | Description | Comments |
|---|---|---|
| Standard | ISO14443 | [15] |
| Frequency | 13.56MHz | [15] |
| Modulation | PAM | See Figure 5.2 |
| SNR | 11dB | See 5.4 |
| $P_{out}$ | 10 to 36dBm | |
| Interference Cancelation | 5 to 35dB | |
| Bandwidth | 200KHz | Compatible with Model |
| $\gamma$ | 0.002 | 4 dB worse than [30] |
| $P_{supp}$ | 60 mW | |
| Nf | 6dB | [54] |
| Antenna rejection | 25dB | |

Table 5.1: System data example

Figure 5.4 shows that the distance $d_{max}$ can be significantly improved either by improving the capability of the interference cancelation function or by arranging the rogue *Reader* antennas for better isolation. Antenna isolation cannot be increased if the attacker uses an *OTS* rogue *Reader* with one antenna for both transmit and receive. We see that with a moderate interference canceler of 30dB to 35dB , the relay attack may be carried out at a maximum distance of approximately 10m.

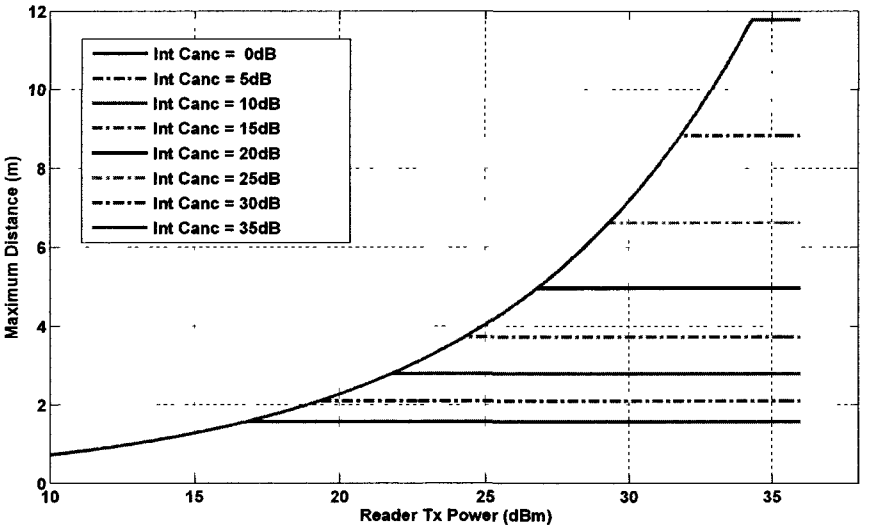


Figure 5.4: Maximum Distance Between *TAG* and *Reader Victim Distance*

## 5.4 Model Setup and Simulation

The previous sections covered the analysis of an *RFiD* relay attack system. Equation 5.6 shows that when the input signal has an *SNR* of 11dB or better, 99% of the communication in a relay attack will be successful. In this section we show simulation results that support this analysis. We also define a process to calibrate the noise and run the simulation using the system modeled in *Simulink*. The following steps need to be performed to run the simulation:

1. Initialize the simulator parameters
2. Calibrate the SNR
3. Run the simulator

The simulator is composed of two similar models that run independently. One model is used exclusively for noise calibration (*SNR*) and the other one is used to model the communication system between the rogue *Reader* and the victim's *TAG* during the relay attack. The reason for using two steps and two different models is that the calibrating of the *SNR* require the signal power to be continuously present in the path from *TAG* to *Reader*, but since the *RFiD TAG* is not continuously transmitting, the attack model does not allow this calibration method. This capability can be built into a future system.

### 5.4.1 Initialize the Simulator parameter

Before running the noise calibration, one initializes the system by running the *Matlab* script *StartSystem.m*. This script initializes the model variables with values from the *ISO14443* standard. It sets frequency, symbol rate, the sampling rate used by the model, as well as other parameters.

### 5.4.2 Calibrating the *SNR*

This section details the procedure used to calibrate the *SNR*. All the values set during this procedure are used to run the relay attack simulation.

Figure 5.5 represents the *TAG's* output signal excluding *AWGN*. One observes that the modulated signal is composed of the carrier at 13.56MHz, the side band (subcarriers) and the baseband signal. Figure 5.6 shows the output signal now with embedded noise; observe that the signal to average noise power density ratio is approximately 11dB. The noise is generated using a random number generator block in *Simulink* and is added to the signal. The modulated signal is kept constant while the noise is increased until required *SNR* is reached. The subcarrier is the signal of interested for the rogue *Reader*, therefore the *SNR* is calibrated to be 11dB for the subcarrier signal.

The noise and signal before added, they pass trough two independent amplifiers one for the noise and the other one for the modulated signal. When setting the gain of either amplifier to zero, its output will be zero. To allow the adjustment of the noise power and the signal power at the output of the channel block, they need to be adjusted as follows:

**Step 1** Remove the noise (Setting the value of the gain at the noise amplifier to zero) and measure at the output of the down-converter, the modulated signal power.

**Step 2** Remove the modulated signal (Setting the value of the gain at the signal amplifier to zero) and measure the noise power at the output of the down-converted. The user should either increase or decrease the noise power by increasing the gain at the noise amplifier until it reaches 11dB below the signal power measured at step 1.

Due to the low modulation index (10%), there is a strong undesired carrier present in the modulated signal from the *TAG*. This will cause the *SNIR* to be low at the rogue *Reader* receiver.

To verify that this approach correctly calibrates the *SNR* the simulator was run and the result displayed in the Figure 5.7. Figure 5.7 clearly shows that the noise is approximately 11dB below the desired signal. The next step is to run the simulator, (Section 5.4.3) and observe the result displayed in the *Simulink* oscilloscope during the communication between *TAG* and rogue *Reader*.

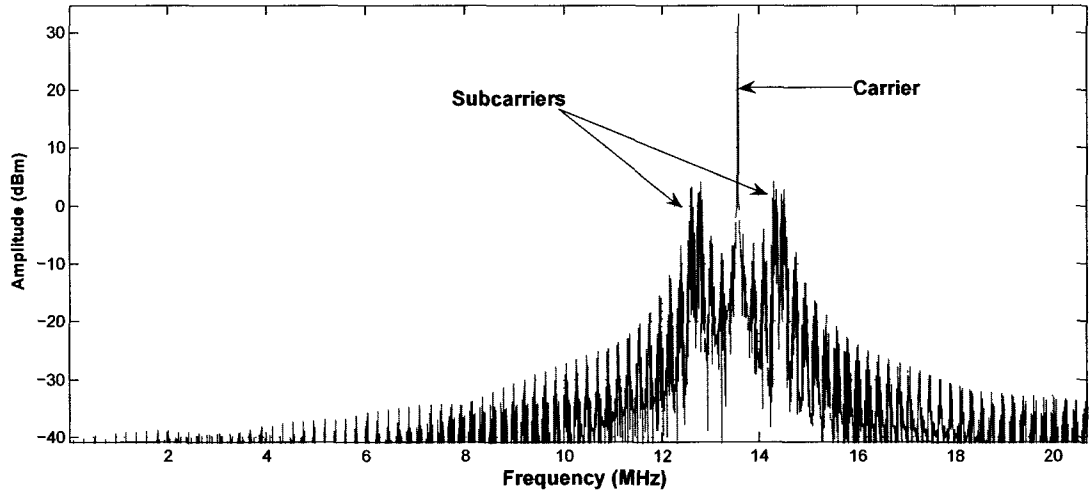


Figure 5.5: Spectrum of the transmitted signal from *TAG*

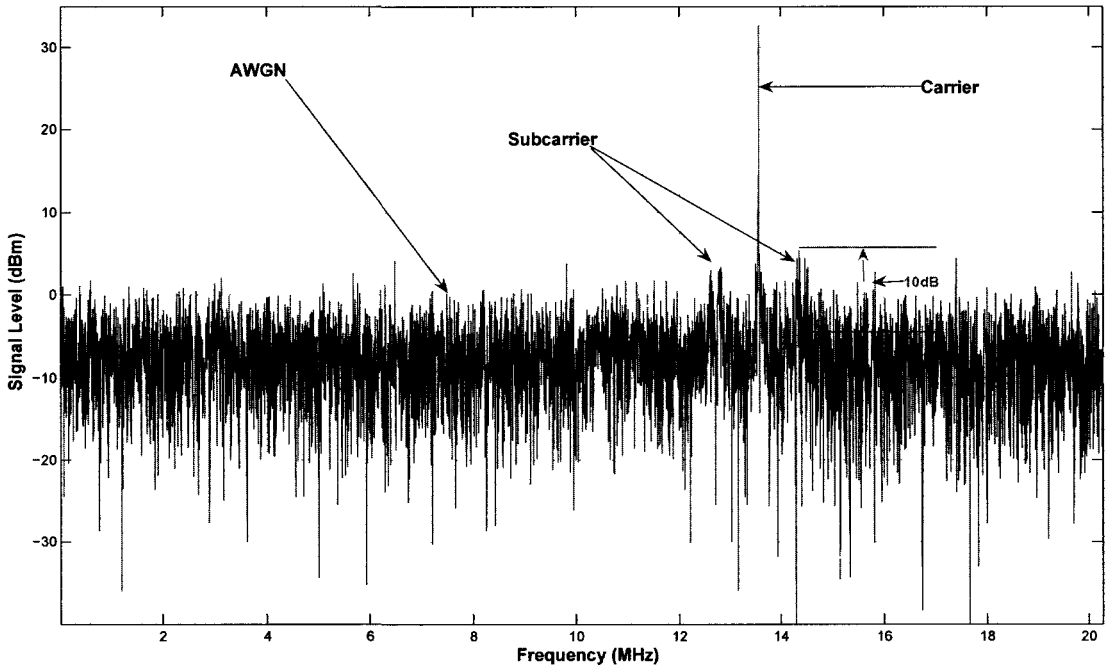


Figure 5.6: Spectrum of the transmitted signal from *TAG* plus *AWGN*

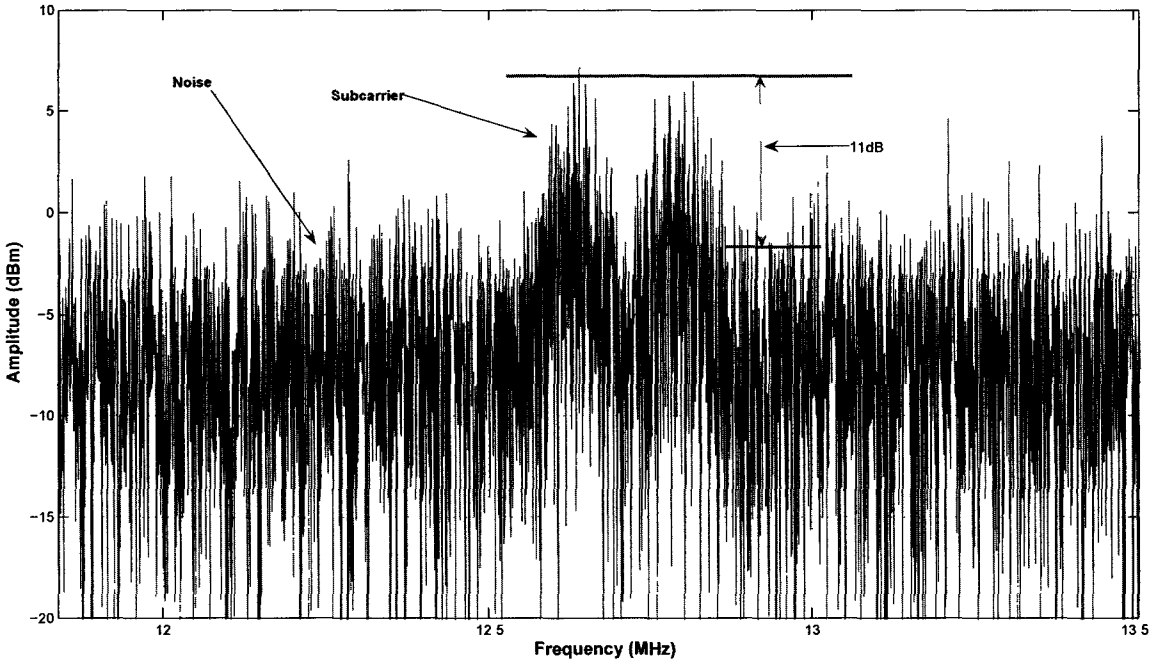


Figure 5.7: Zoom of transmitted signal from *TAG* plus noise

### 5.4.3 Running the Simulator

In this section we describe how to run the simulator and how to interpret the simulation results. After the *SNR* calibration is done, the same *SNR* value used during the noise calibration must be used during the attack simulation. During the attack simulation the model will exchange three messages between rogue *Reader* and *TAG*. First the rogue *Reader* sends *REQA*, then the *TAG* responds with *ATQA* and finally the rogue *Reader* will send *SELECT* messages. These messages happen in sequence and the next message is sent if and only if the previous message has arrived without error. The simulation results are displayed on a *Simulink* scope where the user will see if the three messages were exchanged properly. If the rogue *Reader* sends *SELECT*, we conclude that all three messages were exchanged without error and it is assumed that the system will work for any other message that is required to be exchanged between *TAG* and rogue *Reader*.

#### Simulation results of the system without Noise

To serve as base line, we first show the simulation results for a system without noise. The purpose of this is to familiarize the reader with the desired results so the simulation results may be interpreted more easily in the noise-added case.

Figure 5.8 depicts the three messages being exchanged by the rogue *Reader* and the *TAG*. At approximately $t = 0.5$, the rogue *Reader* sends *REQA*. The *TAG* receives this and at time $t = 0.65$ sends back *ATQA* to the rogue *Reader*. Finally, at time $t = 1.0$ the rogue *Reader* sends *SELECT*, which implies that all previous messages have been sent and decoded without errors.

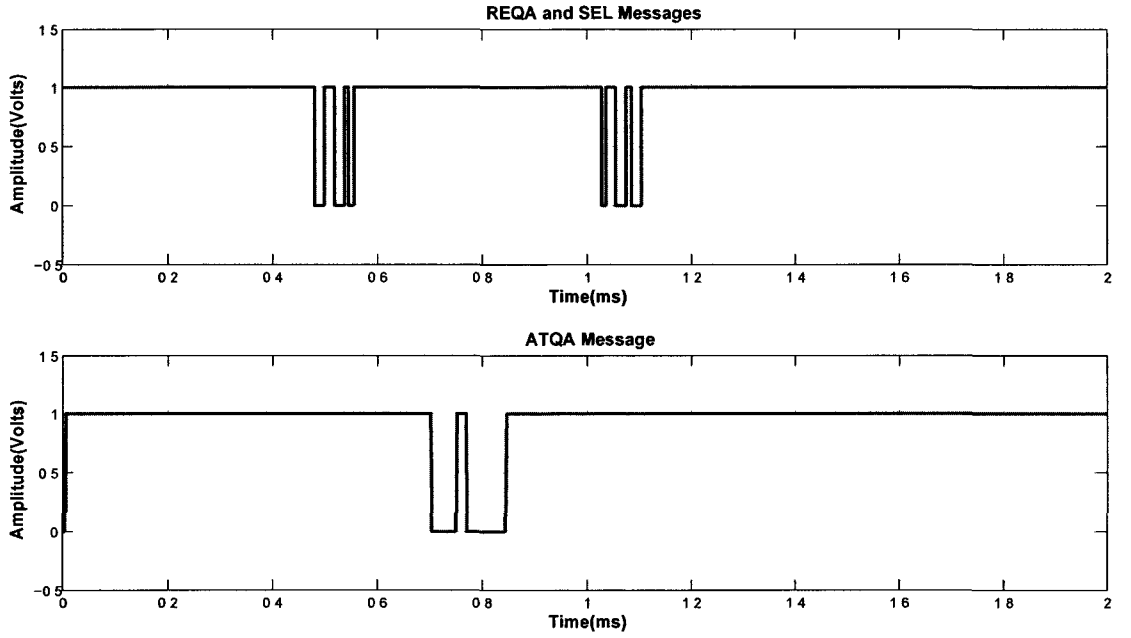


Figure 5.8: Messages Exchanged Between Rogue *Reader* and *TAG*

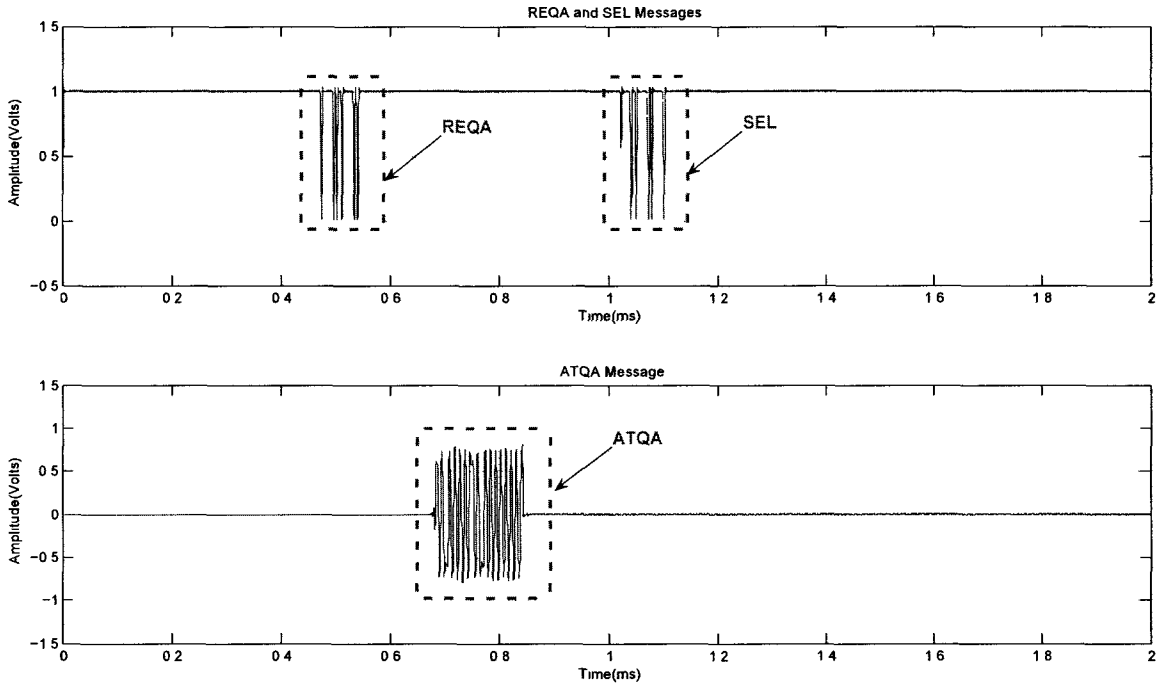


Figure 5.9: Baseband Messages Exchanged Between the Rogue *Reader* and the *TAG*

In Figure 5.9 we show the same message interchange as in Figure 5.8. Here, however, the signal is shown in the analog domain before being demodulated. This means that these messages must be demodulated and decoded to produce the signals shown in Figure 5.8.

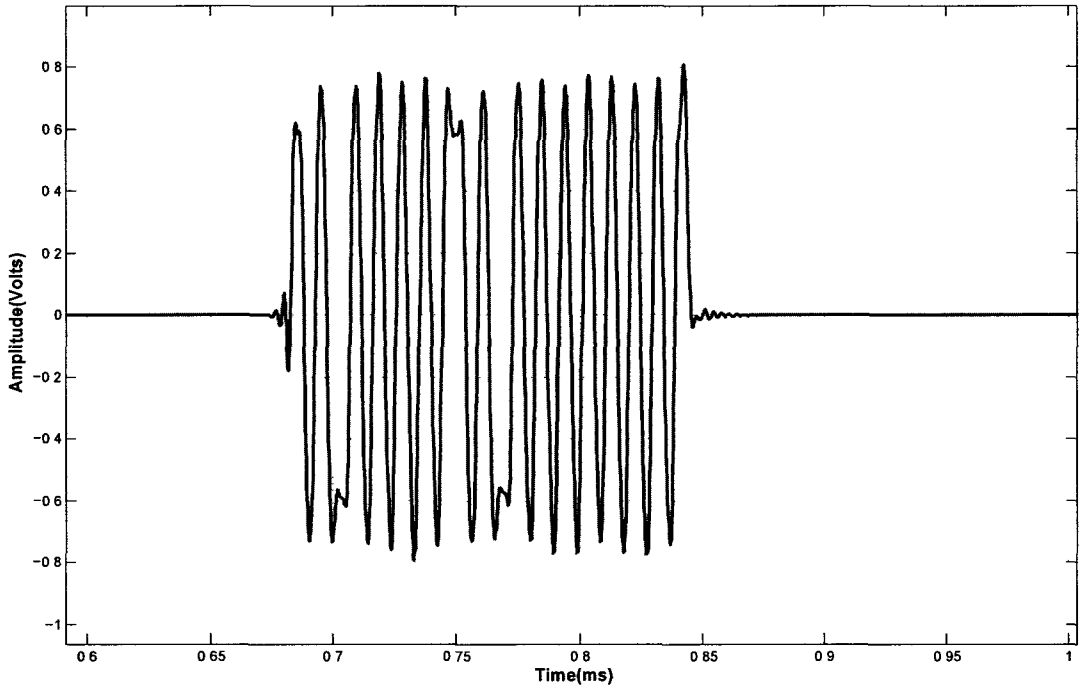


Figure 5.10: Baseband Signal at the Rogue *Reader*

In Figure 5.10, we give a close-up view of the analog baseband message corresponding to the *ATQA* message; this is the signal presented at the bottom of Figure 5.9.

### Simulation Results for a system with Noise (*AWGN*)

Figures 5.11 to 5.13 depict the simulation results where noise is added to the system. The values used for noise density are the ones obtained during the noise calibration procedure.

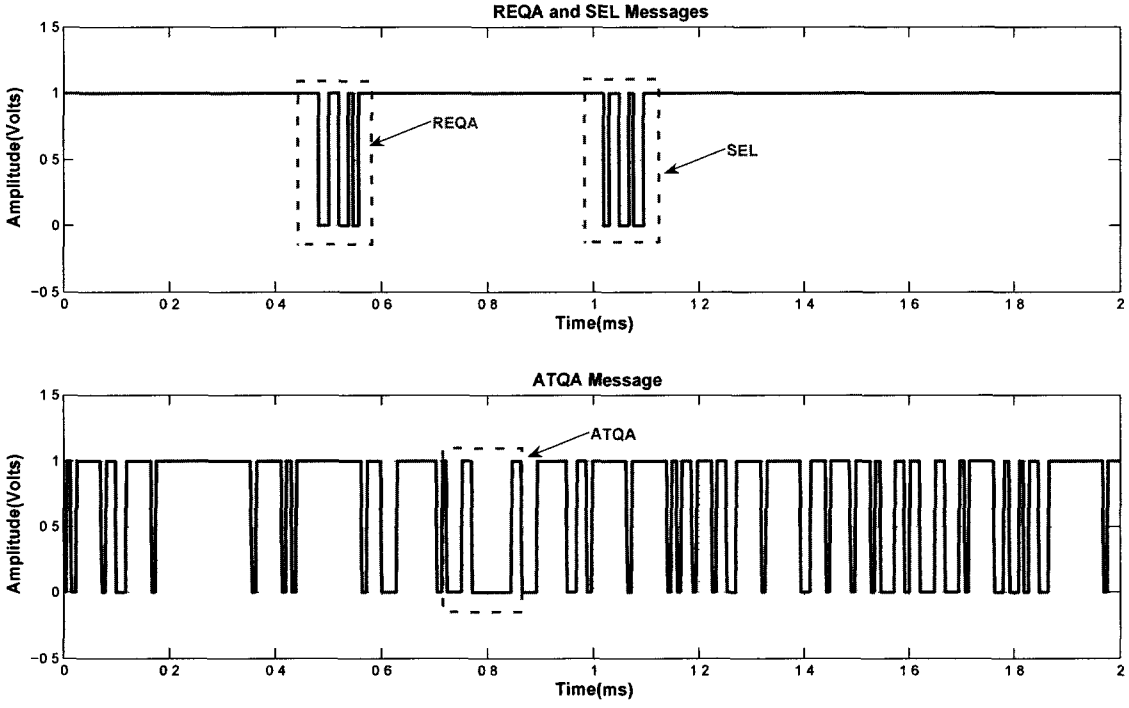


Figure 5.11: Decoded Messages in the Presence of *AWGN*

Figure 5.11 shows the three messages exchanged between the rogue *Reader* and the *TAG*. Observe that due to the noise present at the rogue *Reader* input, there are many rogue detections but the message is still present at approximately $t = 0.8$. Despite the many rogue detection pulses during the occurrence of the message, when the input signal is present the message is detected properly. This is evident by the response of the *Reader* with the *SEL* message that happens at approximately $t = 1$.

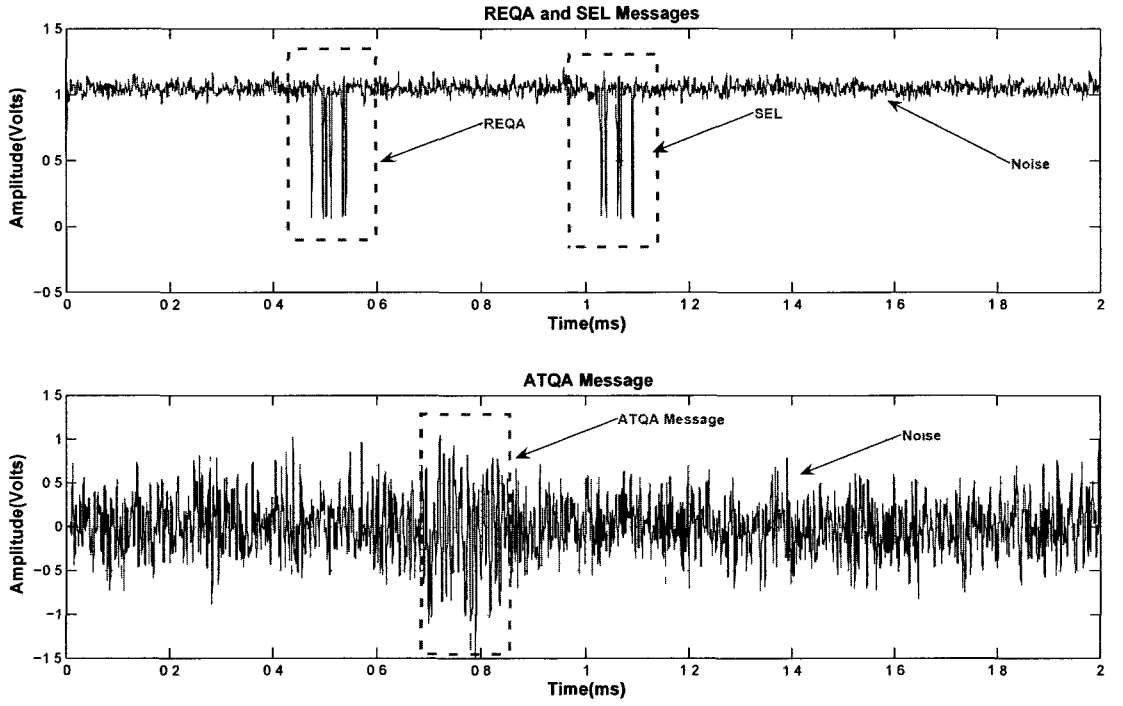


Figure 5.12: Base band Messages in the Presence of *AWGN*

Figure 5.12 shows the signal of Figure 5.9plus *AWGN*. Here the noise can be seen in both directions - from the rogue *Reader* to the *TAG* and vice versa. One observes that the *SNR* at the *TAG* receiver (top) is higher than the *Reader* (bottom). This is because the rogue *Reader* power is much greater than the *TAG* transmit power and the rogue *Reader* receive signal is very weak compared to the *TAG* received signal.

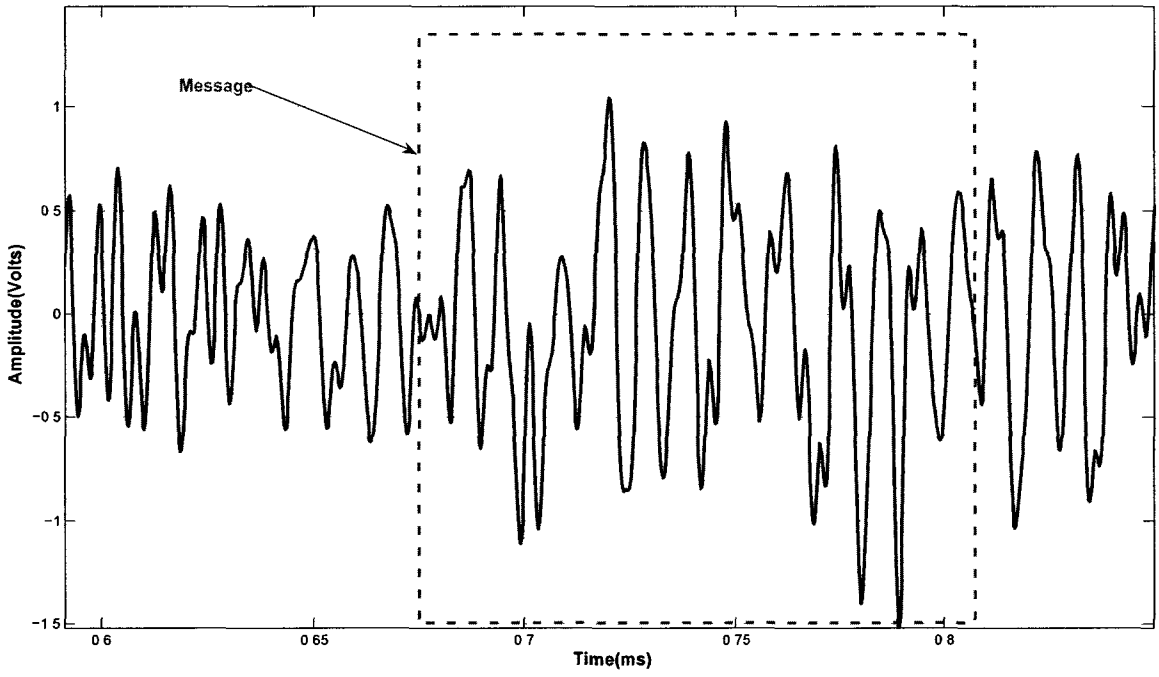


Figure 5.13: Baseband Signal at the *Reader* in Presence of *AWGN*

Figure 5.13 is similar to Figure 5.10; it depicts a close-up baseband signal corresponding to the *ATQA* message contaminated by noise.

## 5.5 Conclusion

In this chapter we discussed two majors aspects of the relay attack analysis: the first one is the maximum delay ($\tau_{max}$) introduced by the system used by attacker; and the second aspect is the maximum distance ($d_{max}$) between attacker (rogue *Reader*) and victim's *TAG* (*Victim Distance*). This work presents the analysis and methodology to calculate the *Victim Distance* ($d_{max}$) using *OTS* electronic subsystems to calculate these factors.

The maximum delay allowed for the relay attack to be successfully performed was determined in Section 5.2.

The *Victim Distance* estimation is in based on an *SNR* that has been verified to be adequate for reliable communication from the simulation results obtained by running the *Simulink* model created in this thesis. Improvements in this distance can be obtained by applying well known algorithms used to reduce the local interference generated by the unmodulated transmitted carrier (Section 5.3.1). During this work, a *Simulink* model was created to allow the user to simulate the communication between attacker and victim. This model provides an easy to use tool that allows the user to run the *ISO14443* protocol. Engineers can easily modify the model as needed for applications of *RFiD* standards other than *ISO14443*.

In summary, this chapter provides a closed form solution for estimating the *Victim Distance* ($d_{max}$). Using the *Simulink* model the *RFiD* communications can be simulated to verify the calculations done using the closed form solution. Also presented are options to improve the *Victim Distance* by using an interference canceler (Section 5.3.1).

# Chapter 6

# Countermeasures to Relay Attacks in RFiD Systems

## 6.1 Introduction

In the last chapter, we saw how a relay attack can be successfully conducted against an *RFiD* system. In this chapter we present countermeasures design to protect *RFiD* systems against these attacks. There are methods that use software protocols that are either implemented at MAC or physical layers, and others that simple use hardware to protect the systems.

In [20] Hancke and Kuhn propose modifying the Medium Access Controller *MAC* by adding a time dependent protocol. These types of protocols will reduce the choice of equipment to be utilized by the attacker but, they do not completely eliminate the threat of relay attack. Another point to mention about these methods is that the majority of software solutions proposed in the literature are incompatible with existing systems.

We present three hardware solutions. Within these, two are new and novel. All of these three solutions are backwards compatible with existing systems.

## 6.2 Preventing Relay Attacks

There are hardware and software methods to protect *RFiD* systems against relay attacks. In [20], Hancke and Kuhn state that the only effective methods to avoid relay attack are distance-bounding and secure-positioning protocols. Distance bounding is

based on limiting the response time from the *TAG*. Therefore the implementation of this type of countermeasure will require the modification of the existing systems.

### 6.2.1 Hardware Methods

The purpose of this section is to present solutions that are robust against relay attack and compatible with existing *RFiD* systems. These solutions are intended to make the existing and new systems immune to relay attack and in addition to this, for the new *TAGs* will be backwards compatible. This section also presents the comparison between three hardware solutions to protect *RFiD* systems against relay attack. These solutions are as follows:

1. Shielding
2. Positioning
3. Pressure

Within the methods mentioned above, the shielding (tempering) is well known but the other two methods are new. Before starting our discussion let us reinforce that during relay attack, the attacker does not have possession of the *TAG* and also he/she wants to be as far away as possible from the victim.

#### Shielding (Tempering)

This method is already in use by industry. It consists of a metal cover that will shield the *TAG*. The system requires the user to remove the shield prior to using the *TAG* and to put it back inside the metal case after using it. The shield will keep the *TAG* inactive and will thwart any unwanted communication. However, at any time that the user removes the cover the *TAG* is unprotected and it can be exposed to a relay attack.

**System Analysis for Shielding** We begin by estimating the isolation provided by a metal cover. We will consider that this isolation is equivalent to a semirigid cable, [1] we may take this value to be 80dB (20 dB worse than MCJ142A cable).

[1]Semirigid cable are largely used for connections that require high isolation between the center connector of the cable and external metal that shields the center connector e.g MicorCoax MCJ142A provides a shield effectiveness greater than 100dB at 1GHz

Let $P_{supp}$ be the power required for the *TAG* be activated, $P_{RxTAG}$ be the power present at *TAG* antenna, $l(d, f)$ the attenuation between *Reader* and *TAG*, $a_{shield}$ the isolation provided by the tempering and $\gamma$ the reflection factor or mismatch coefficient. Then we have

$$P_{supp} = P_{RxTAG}(1 - \gamma) \tag{6.1}$$

$$P_{supp} = P_t l(d, f) Ag_{RTx} Ag_{TAG} a_{shield}(1 - \gamma) \tag{6.2}$$

Assuming that antennas have unit gain, $Ag_{RTx} = Ag_{TAG} = 1$, equation 6.2 becomes:

$$P_{supp} = P_t l(d, f) a_{shield}(1 - \gamma) \tag{6.3}$$

Let $A_{shield}$ and $P_{SUPP}$ be the values in $dB$ and $dBm$, $0 \leq a_{shield} \leq 1$ and $P_{supp}$ is measured in watts

$$P_{SUPP} = P_T - A_{shield} - FSL_T(d, f) + 10 \log 10(1 - \gamma) \tag{6.4}$$

If $d = 0$, that is, the worst case scenario when rogue *Reader* is situated at zero distance from the *TAG*, then $FSL(d, f) = 0$ and we have

$$P_{supp} = P_T - A_{Shield} + 10 \log 10(1 - \gamma) \tag{6.5}$$

If we assume that the *TAG* requires 60mW of power to be active, ($P_{supp} = 60mW = +17.8dBm$) the required transmitted power will be $P_t = +97.8dBm$. Transformed in watts this is approximately $10^6 Watts$. It is thus impractical to build a system with this power to attack an *RFiD* card protected by a shield.

### Positioning

This new solution will allow the *TAG* to send messages to the *Reader* if and only if it is positioned properly with respect to the *Reader*. The user will be required to position the *TAG* properly during authentication process, with the help of visible indication about how the user will position the *TAG*. This hardware solution requires a *MEM* [1] device to provide position information to the *TAG*. *MEM* devices are widely used in iPhones and iPODs and are thus strong candidates for this application. As soon as the *TAG* is activated, the *MEM* device will provide information about its position and an

[1] Microelectromechanical systems (MEMS)

electronic circuit will verify if it is positioned properly. If the position is correct, the *TAG* will respond to the *Reader* polling and subsequently authentication process of the *TAG* will proceed normally. This situation is depicted in Figure 6.1.

Let $\theta_0$ be the maximum range of angle, where the *TAG* circuitry will still detect that the *TAG* is in the proper position. During the attack the probability that the *TAG* will respond to a polling from the rogue *Reader* is:

$$P_v = \frac{\theta}{\pi}. \tag{6.6}$$

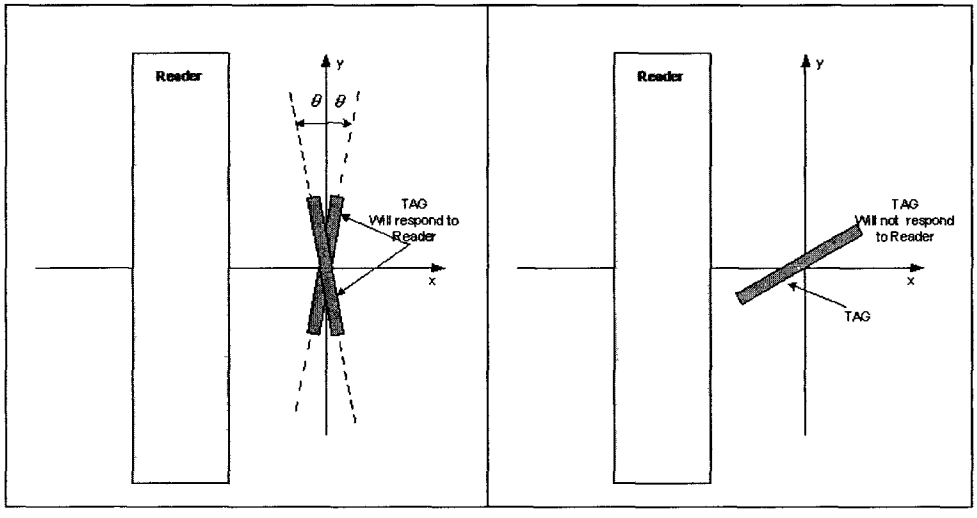


Figure 6.1: Position for the *TAG* to respond to *Reader* polling

Due to price constraints, it is expected that the $\Theta$ will not be very small.

### Detector

Figure 6.2 shows a possible control system to be used by the *TAG* during position detection. The transducer *MEM* will transform the angle position $\Theta$ into voltage $v_i(\theta)$. The feedback loop (denoted G for Gain and $H(s)$ for the feedback transfer function) will control the response time of the system. The detector will use a hardware threshold to decide if the *TAG* is correctly positioned.

### Pressure

This third solution uses a device embedded into the *TAG* such that it will respond to the reader polling when a small force/pressure is applied to a specific region that is

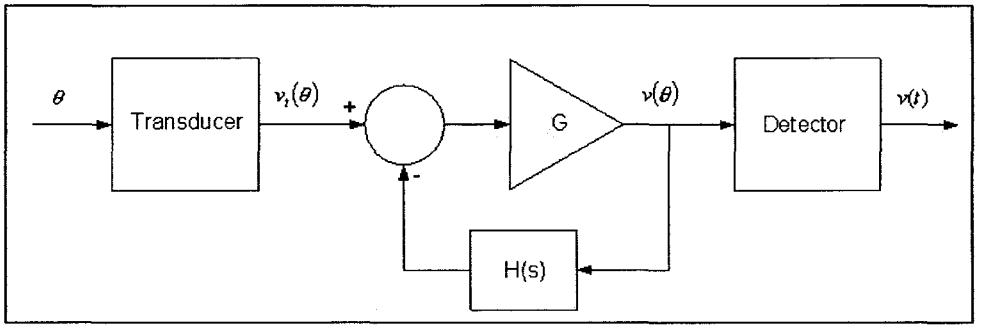


Figure 6.2: System model for positioning detector

pre-defined on the *TAG* exterior. This solution will eliminate the relay attack threat because the *TAG* can only be activated when the pressure is applied to the *TAG*.

This solution can use a similar control system as the one shown in Figure 6.2. The transducer will need to be changed for a pressure transducer instead. It will generate at its output, a voltage that is proportional to the amount of pressure applied instead of a function of the position, as in the case of position detection.

### 6.2.2 Relay attack success probability analysis

Let us analyze the probability of successful *Relay Attack* when one of the three methods above is used to protect the system.

Let $P_{act}$ be the probability of an unprotected *TAG* being activated during an attack, $P_{RR}$ the probability for a *TAG* to be in the reading range ($BER \leq 10^{-6}$) and $P_{success}$ be the probability for the attack to succeed.

#### Shielding

Let $P_f$ be the probability that the user forgets to replace the *TAG* inside the shield after using it. $P_{RR}$, $P_{act}$ ad $P_f$ are random variable independent distributed therefore, the probability of success during the attack will be:

$$P_{success} = P_{RR}P_{act}P_f \tag{6.7}$$

#### Pressure

Let $P_p$ be the probability that the *TAG* is under the correct pressure. For example when the *TAG* is loose inside the pocket, handbag, etc. $P_{RR}$, $P_{act}$ and $P_p$ are independent

random variables. The probability of success during the attack will be:

$$P_{success} = P_{RR}P_{act}P_p \tag{6.8}$$

**Position**

With positioning protection, for the *Relay Attack* to be successful, the device will need to be in the proper position. let $P_v$ be the probability that the device is positioned correctly. Since these events ($P_v$, $P_{act}$ and $P_{RR}$), are independent, the probability of success will be:

$$P_{success} = P_v P_{RR} P_{act} = \frac{\theta}{\pi} P_{RR} P_{act} \tag{6.9}$$

The attacker up to certain level will be able to control the probabilities $P_{act}$ and $P_{RR}$ but the remaining probabilities are completely out of control of the attacker. $P_v$ is random because the position of the *TAG* is function of what the victim is doing at the moment of the possible attack happens. $P_f$ totaly depends on the *TAG* user. Also, during the attack, the victim does not want to use the *TAG*, therefore $P_f$ is considered random as well.

## 6.3 Conclusion

When comparing the three methods presented above we need to address four important points for *RFiD* systems: Cost, effectiveness, device lifetime and user convenience.

**Cost** The cost of the *MEM* is comparable with the cost of the pressure device. The metal foil is more expensive than the other two solutions. The first two solutions are integrated into the access card but the foil is manufactured as a separate component. Costs of manufacturing and material management must be accounted for the calculation of the total cost of the system.

**Effectiveness** The usage of a shield device is the solution that presents medium effectiveness between the three methods. The vulnerability occurs when the user forgets the cover, having the *TAG* unprotected against attack. The integrated methods have similar effectiveness between themselves but both require the user to either position the *TAG* correctly or apply pressure.

**Lifetime/MTBF** Within the three options, the only one that presents a risk of decreasing the lifetime (Mean Time Before Failure - *MTBF*) of the system is the pressure element. The user may unintentionally apply more pressure than required, decreasing the lifetime of the device and therefore causing reduction in the *MTBF* of the system.

**Convenience** This is a very important point because even if a system may be "bullet proof" to relay attack, it may not be accepted by the users if it is too awkward to use. Therefore when this happens, the optimum technical solution gets superseded by the customer requirements and it is not put in production. These considerations are summarized in Table 6.1

| Item | Shielding | Pressure | MEM |
|---|---|---|---|
| Cost | High | Low | Low |
| Effectiveness | Low | High | High |
| MTBF | No effect | Decreases | No effect |
| Convenience | Highly inconvenient | Neutral | Neutral |

Table 6.1: Countermeasures Consideration Summary

The great advantage of the solutions presented in this sections is that none of them require modification to the existing standards. They simply enhance the *TAG*'s behavior against relay attack.

# Chapter 7

# Conclusions and Future Work

## 7.1 Summary of Results

In Chapter 3, the boundary between *NF* and *FF*is estimated using the wave impedance method. The results obtained by this method is compared with other methods in the literature and presented in Table 3.2. The boundaries presented in the literature vary case by case depending on the communication systems considerations and applications. The estimations done in this chapter show that for *RFiD* (*ISO14443*) the *NF* to *FF* boundary is 4.5 meters. This value is depicted by Figure 3.3 and Table 3.2 is in accordance with most of the values published. This chapter also presents two methods of estimating the *FSL*.

Chapter 4 presents methods to estimate the contribution of imperfections such as *EVM* to the *BER* of and *RFiD* systems. This chapter discusses the most important imperfections that occur in oscillators, down converters and other components such as the *LNA* and the *PA*.

Chapter 5 discusses the impact of the relay system delay on the success of the relay attack. It shows that the maximum delay that the attacker's system can add to the *RFiD* system communication and still be successful is 86.5$\mu s$ including *TAG* processing delay. This chapter also presents the analysis of the communication system between the attacker and victim. It estimates the *Victim Distance*. This chapter shows the simulation results obtained by using the *Simulink* model that was built for this purpose. The results obtained during this simulation match the results obtained during the mathematical analysis of the communication system. It was shown that an attacker can be located far enough from a victim (see Figure 5.4) and successfully carry out a

relay attack.
In Chapter 6 three methods of relay attack countermeasures are presented and an estimation of the probability of success was determined for each method. For the newer two methods (positioning and pressure) the corresponding electronic control system was described.

## 7.2 Contribution of the Thesis

This thesis includes the following contributions:

- A *Simulink* model has been designed for relay attack focusing on the communication channel between rogue *Reader* and victims' *TAG*. This model was designed based on *ISO14443* recommendations. It includes all the authentication hand shaking messages that occur between *TAGs* and *Reader*. This model can be easily modified for other *RFiD* protocols.

- A complete analysis of the communication channel between rogue *Reader* and victim's *TAG* was presented. This analysis is a fundamental tool for estimating the maximum distance between attacker and victim during a successful attack.

- Two new countermeasures against relay attack are introduced for *RFiD* systems. These methods are backwards compatible with the authentication process of the existing systems.

## 7.3 Future Work

A few possible extensions to the work presented in this thesis are described below.

1. In chapter 3, we considered dipole antennas. Relay attack can be carried out in high frequency *RFiD* systems, which usually use a variety of different types of antennas. To be able to estimate the maximum distance between attacker and victim for these systems, it is necessary to know the Near-Far field bound. For future work it is suggested to analyze this bound for other types of *RFiD* antennas.

2. The model built in *Simulink* only covers the messages used by *ISO14443*. This *Simulink* model could be extended to cover more standards than *ISO(14443)*.

This work will require the review of the analysis done in Chapter 5 and the consideration of impairments such as non-flat fading.

3. Chapter 6 presents three types of hardware implementations that reduce the probability of successful for relay attack. Each one of the newer solutions (pressure and positioning) presents opportunities for more detailed study. For positioning, *MEMs* are mentioned as potential solution. An in depth study will be required of the implementation tradoffs and cost increase in the *TAG*.

# Appendix A

# Standards

The *RFID* established standards are ISO 14443 [15] and ISO 15693 [16]. Both use a 13.56 MHz band, and are in widespread use in the marketplace.

Different groups, such as ISO/IEC JTC/SC3/WG4/SG 3 *RFID*, are currently working in new standards for *RFID* systems. See TableA.1 for a partial list of these new standards.

| Standard | Description |
|---|---|
| ISO 18000-1 | Generic Parameters for Air Interface for Global Interfaces |
| ISO 18000-2 | Parameters for Air Interface frequency band < 135 KHz |
| ISO 18000-3 | Parameters for Air Interface frequency band 13.56 MHz |
| ISO 18000-4 | Parameters for Air Interface frequency band 2.45 GHz |
| ISO 18000-5 | Parameters for Air Interface frequency band 5.84 GHz |
| ISO 18000-6 | Parameters for Air Interface frequency band 860 to 930 MHz |
| ISO 18000-7 | Parameters for Air Interface frequency band 433.92 MHz |

Table A.1: RFID Technical Standards

# Bibliography


[1] X. Zeng; R. Bagrodia and M. Gerla. GloMoSim: A library for parallel simulation of large-scale wireless networks. *Twelfth Workshop on Parallel and Distributed Simulation, 1998. PADS 98. Proceedings.*, (5):154–161, 1988.

[2] Bernard Berkowitz. *Basic Microwaves*. Book Company Inc., 1966.

[3] L. Matts; J. T. Cain and M. H. Mickle. The In-Situ Technique of Measuring Input Impedance and Correction Effects of RFiD Tag Antenna. *IEEE Trnas. Automation Science and Engineering*, 6(1):4–8, 2009.

[4] Patricia Fernandes Campos. Interference cancellation system based on the LMS algorithm. *IEEE International Conference on Acoustics, Speach, and Signal Processing*, 4:237–240, 1992.

[5] Johathon Y. C. Cheah. *Practical Wireless Data Modem Design*. Artech House Publishers, 1999.

[6] Hong Chen and Gregory J. Pottie. An Orthogonal Projection-Based Approach for PAR Reduction in OFDM. *IEEE Communications Letters*, 6(5):169–171, 2002.

[7] E. Costa and S. Pupolin. M-QAM-OFDM system performance in presence of a monlinear amplifier and phase noise. *IEEE Trnasactions on Communications*, 50(3):462–472, March 2002.

[8] L. S. Cutler and C. L. Searle. Some aspects of the theory and measurement of freqnecy fluctuations in frequency standards. *Proceeding on the IEEE*, 54(2):136–154, Feb 1966.

[9] S. Dominikus and M. Aigner. Petra Software. *[Online]. Available: http : //www.jce.iaik.tugraz.at/sic/products/rfid_components/petra_software_1*, 2009.

[10] K. Fall and K Varadhan. The ns Manual (formerly ns Notes and Documentation). *[Online]. Available: http://www.isi.edu/nsnam/ns/ns-documentation.html*, pages 1–430, 2010.

[11] Kamilo Feher. *Digital Communications*. Nobel Publishing Corporation - Atlanta, 1997.

[12] Christian Floerkemeier and Ravikanth Pappu. Evaluation of RFIDSim - a Physical and Logical Layer *RFiD* Simulation Engine. *IEEE International Conference on RFiD April 2008 Las Vegas USA*, pages 350–356, 2008.

[13] Christian Floerkemeier and Sanjay Sarma. RFIDSim - A Physical Layer Simulation Engine for Passive RFID. *IEEE Transactions on Automation and Engineering*, 6(1):33–43, 2009.

[14] ISO/IEC 14443-2 Work Group. Identification cards - Contactless integrated circ-cards - Proximity cards. *ISO/IEC FCD*, 2:1–6, 06 1999.

[15] ISO/IEC 14443-3 Work Group. Identification cards - Contactless integrated circ-cards - Proximity cards. *ISO/IEC FCD*, 2:1–38, 06 1999. [Online]. Available: *http : //www.iso.org/iso/iso$_c$atalogue/catalogue$_t$c/catalogue$_d$etail.htm?csnumber* = 45146.

[16] ISO/IEC Work Group. Identification cards Contactless integrated circuit(s) cards - Vicinity cards Part 3: Anti-collision and transmission protocol. *ISO/IEC FCD*, 2:1–44, 03 2000. [Online]. Available: *http : //www.iso.org/iso/iso$_c$atalogue/catalogue$_t$c/catalogue$_d$etail.htm?csnumber* = 39695.

[17] Ali Hajimiri and Thomas H. Lee. A General Theory of Phase Noise in Electrical Oscillators. *IEEE Journal of Solid-State Circuits*, 33:179–194, Feb 1998.

[18] Yifeng Han and Hao Min. System Modeling and Simulation of RFID. *[Online]. Available: http://www.autoidlabs.org*, 1988.

[19] Gerhard Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. *University of Cambridge, Computer laboratory*, pages 1–12, 2005. [Online]. Available: http://www.cl.cam.ac.uk/~gh275/relay.pdf.

[20] Gerhard Hancke and Markus G. Kuhn. An RFiD Distance Bounding Protocol. *First International Conference on Security and Privacy for Emerging Areas in Commu-*

*nications Networks, 2005. SecureComm 2005.*, pages 67–73, Sept 2005. Athenens, Greece.

[21] Christian Reinold; Peter Scholz; Werner John and Ulrich Hilleringmann. Efficient Antenna Design of Inductive Coupled RFID-Systems with High Power Demand. *IEEE Journal of Communications*, 2(6):14–23, 2007.

[22] Carl T.A. Jonk. *Engineering Eletromagnetic Fields & Waves.* Wiley International Edition, 1975.

[23] Thomas S. Heydt-Benjamin; Daniel V. Bailey; Kevin Fu; Ari Juels and Tom O'Hare. Vulnerabilities in First-Generation RFID-enabled Credit Cards. *rfid-cusp.org*, pages 67–73, Oct 2006. [Online]. Available: URL: www.rfid-cusp.org.

[24] Udo Karthaus and Martin Fisher. Fully Integrated passive UHF RFID Transponder IC With 16.7-$\mu$W Minimum RF Input Power. *IEEE JOURNAL OF SOLID-STATE CIRCUITS*, 38(10):1602–1608, 2003.

[25] Walt Kester. *Data Conversion Handbood.* Elsevier, 2005.

[26] John Krause. *Antennas.* McGraw Hill, 1950.

[27] Peter M. Asbeck; Lawrence E. Larson and Ian G. Galton. Synergistic Design of DSP and Power Amplifiers for Wireless Communications. *IEEE Tansactions on Microwave Theory and Techniques*, 49(11):2163–2169, 2001.

[28] E.J. Baghdady; R. N. Lincoln and B. D. Nelin. Short-term frequency stability: Characterization, theory, and measurement. *Proceedings of the IEEE*, 53(7):704–722, July 1965.

[29] Aldo N. D'Andrea; V. Lottici and R. Reggiannini. Nonlinear Predistortion of OFDM Signals over Frequency-Selective Fading Channels. *IEEE Transactions on Communications*, 40(5):837–843, 2001.

[30] G. Marrocco. Emerging Technologies for Radio Frequency Identification. Research Report RR-08-69, Dipartimento di Infomatica Sistemi e Produzione, Universit di Roma Tor Vergata, june 2 2008.

[31] R. L. Bargrodia; R. Meyer; M. Takai; Y. Chen; X. Zheng; J. Martin and H. Y. Song. Parsec: AParallel Simulation Environment for Complex Systems. *IEEE Computer*, 31:77–85, Oct 1998. [Online] Available: http://citeseerx.ist.psu.edu/viewdoc/summary/doi=10.1.1.21.3738.

[32] J. McNeil. Jitter in Ring oscillators. *Proc. ISCAS*, 16:201–204, June 1994.

[33] George J. Miao and Mark A. Clements. *Digital Signal Processing and Statistical Classification*. Artech House, 2002.

[34] Kin S. Leong; Mun Leng Ng and Peter H. Cole. The Reader Collision Problem In RFiD Systems. *IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications Proceedings*, 1:658–661, 2005.

[35] Department of Defense MIL 449. Measurement of eletromagnetic interference characteristics. *MIL-STD*, (449), 1977.

[36] Department of Defense MIL 462. Measurement of Eletromagnetic Interference Characteristics. *MIL-STD*, (462), 1977.

[37] Katsuhiko Ogata. *Modern Control Engineering*. Prentice-Hall Inc, 1970.

[38] Jose C. Pedro and Nuno B. Carvalho. *Intermodulation Distortion in Microwave and Wireless Circuits*. Artech House, 2003.

[39] David M. Pozar. *Microwave Engineering*. John Wiley & Sons, Inc., 2004.

[40] John G. Proakis. *Digital Communications*. McGraw Hill, 1989.

[41] R. A. Shafik; Md. S. Rahman and AHM R. Islam. On the Extended Relationships Among EVM, BER and SNR as Performance Metrics. *4ht International Conference of Electrical and Computer Engineering.*, pages 408–411, December 2006.

[42] Hannes Riedenbauer. Rfid - epc and security mechanisms. *Graz University of Technology, Austria*, pages 1–11, 2006.

[43] Stephen A. Weis; Sanjay E. Sarma; Ronald L. Rivest and Daniel W. Engels. Security and privacy aspects of low-cost radio frequency identification systems. pages 201–212, 2003.

[44] John W. M. Rogers and Calvin Plett. Noise, Linearity, and Signals. *Classe Notes*, pages 1–52, 2009.

[45] J. Rutman. Characterization of phase and frequency instabilities in precision frequency sources; Fifteen years of progress. *Proceeding of the IEEE*, 66(9):1048–1175, 1978.

[46] Sergey A. Shelkunoff. *Advanced Antennas Theory*. Wiley, 1952.

[47] Sergey A. Shelkunoff. *Antennas Theory and Pratice*. Chapman & Hall, Limited, 1952.

[48] Belle A. Shenoi. *Introduction to Digital Signal Processing and Filter Design*. Wiley-Interscience, 2006.

[49] Keliu Shu and Edgar Sanches-Sinencio. *CMOS PLL Synthesizers Analysis and Design*. Springer, 2005.

[50] H.C. So. Adaptive algorithm for sinousoidal interference cancellation. *Electronic Letters*, 33(22):1910–1912, 1997.

[51] Vojetech Derbek; Josef PreishuberPfluegl; Chritian Steger and Markus Pistauer. Architecture for Model-Based UHF RFID System Design Verification. *Proceedings of the 2005 European Conferencen on Circuit Theory and Design*, 2:II/181–II/184, 2005.

[52] Phissanu Malison; Sathaporn Promwong; Nikon Sukutamatanti and Thanawat Banpotjit. Indoor Measuret and Modeling of RFiD Transmission loss at 5.8GHz with human body. *5th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2008. ECTI-CON 2008.*, pages 421–424, 2008.

[53] Wim Aerts; Elke De Mulder; Bart Preneel; Guy A. E. Vandenbosch and Ingrid Verbauwhede. Dependence of RFID Reader Antenna Design on Read Out Distance. *Antennas and Propagation, IEEE Transactions on*, 56:3829–3837, 12 2008.

[54] F. Gatta; E. Sacchi ; F. Svelto; P. Vilmercati and R Castello. A 2-dB noise figure 900-MHz differential CMOS LNA. *IEEE Journal of Solid-State Circuits*, 36(10):1444–1452, 2001.

[55] V. Beroulle; R. Khouri; T. Vuong and S. Tedjini. Behavioral Modeling and Simulation of Antennas: Radio-Frequency identification case study. *IEEE Xplorer - Proceedings of the 2003 International Workshop on BMAS 2003*, pages 102–106, Oct 2003. Valence.

[56] Don White. *EMI Control Methods and Techniques*. Don White Consultants.

[57] Edward A. Wolff. *Antenna Analysis*. John Wiley & Sons, Inc., 1966.

[58] J. Wood and D.E.Root. *Fundamentals of Nonlinear Behavioral Modeling for RF and Microwave Design*. Artech House, 2005.

[59] P. J. Sullivan; B. A. Xavier and W. H. Ku. Low Voltage Performance of a Microwave CMOS Gilbert Cell Mixer. *IEEE Journal of Solid-State Circuits*, 32(7):1151–1155, 1997.

[60] Yan Zhang and Paris kitsos. *Security IN RFID and Sensors Networks*. Auerbach Publications, 2009.