Physical Layer Approach for Securing RFID Systems

by

Muhammad Khizer Kaleem

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2013

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Radio Frequency IDentification (RFID) is a contactless, automatic identification wireless technology primarily used for identifying and tracking of objects, goods and humans. RFID is not only limited to identification and tracking applications. This proliferating wireless technology has been deployed in numerous securities sensitive applications e.g. access control, e-passports, contactless payments, driver license, transport ticking and health cards.

RFID inherits all the security and privacy problems that are related to wireless technology and in addition to those that are specific to RFID systems. The security and privacy protection schemes proposed in literature for wireless devices are mostly secured through symmetric/asymmetric keys encryption/decryption and hash functions. The security of all these cryptographic algorithms depends on computationally complex problems that are hard to compute using available resources. However, these algorithms require cryptographic operations on RFID tags which contradict the low cost demand of RFID tags. Due to limited number of logic gates in tags, i.e., 5K-10K, these methods are not practical. Much research effort has done in attempt to solve consumer's privacy and security problem. Solutions that prevent clandestine inventory are mostly application layer techniques.

To solve this problem, a new RFID physical layer scheme has been proposed namely Direct Sequence Backscatter Encryption (*DSB Enc*). The proposed scheme uses level generator to produce different levels before transmitting the signal to the tag. The tag response to the signal sent by the reader using backscatter communications on the same signal which looks random to the eavesdropper. Therefore eavesdropper cannot extract the information from reader to tag and tag to reader communication using passive eavesdropping. As reader knows the different generated levels added to the carrier signal, it can remove the levels and retrieve the tag's messages.

We proposed a lightweight, low-cost and practically secure physical layer security to the RFID system, for a supply chain processing application, without increasing the computational power and tag's cost. The proposed scheme was validated by simulations on GNU Radio and experimentation using SDR and a WISP tag. Our implementation and experimental results validate that *DSB Enc* is secure against passive eavesdropping, replay and relay attacks. It provides better results in the presence of AWGN channel.

Acknowledgements

First and foremost, I am thankful to Allah Almighty for providing me knowledge and strength for doing this research.

I express my most sincere gratitude, hearty sentiments and thanks to my supervisor Professor Guang Gong for her excellent supervision, encouragement, knowledge delivering. This work would not have been completed without her supervision. Her sweet behaviour, keen interest, personal involvement and criticism for the betterment were all the real source of courage, inspiration and strength during the completion of this research.

I would also like to thank my committee members, Professor Mark Aagaard and Professor Liang-Liang Xie, for their constructing feedback and comments on this thesis.

I express my deep gratitude to Dr. XinXin Fan, Dr. Zilong Wang, Dr. Yin Tan, Yang Yang, Roy Feng, Yao Chen, Gangqiang Yang and Nusha Zidaric. I specially like to thank Bo Zhu, Fei Huo, Kalikinkar Mandal, Teng Wu and Shasha Zhu for their help and support. I want to thank all members of Communication Security (ComSec) lab of the University of Waterloo for providing friendly behaviour and atmosphere in the lab during my stay here.

Last but not least, I am deeply indebted to my family for their unconditional love, care, support and trust in me. Especially my mother, who always believed, encouraged and supported me for doing research. She is a real source of motivation for during a graduate studies.

Dedication

This thesis is dedicated to my parents, Kaleem Arshad and Samia Arshad, and my family, Muhammad Wahab Kaleem; Hira Wahab; Muhammad Mannal Kaleem and Marium Mazhar, and teachers for leading me into intellectual persuade and who inspired me toward the sacred task of learning.

Table of Contents

List of Tables **xi**

List of Figures **xii**

1 Introduction **1**

1.1 Contribution 2

1.2 Organization 2

2 Background and Fundamentals **4**

2.1 RFID Architecture 4

2.1.1 Tags 4

2.1.2 Readers 5

2.1.3 Back-end Database: 6

2.1.4 Physical Layer 6

2.2 Vulnerability of RFID System Security 11

2.2.1 Privacy and Security Issues 11

2.2.2 Privacy 11

2.2.3 Security 11

3 Preliminaries **13**

3.1 Notations 13

3.2 Backscatter Communications 14
3.3 Power Distance Relationship 14
3.4 Pseudorandom Sequence Generator 15
3.4.1 Linear Feedback Shift Register with Maximum Period 15
3.5 Complexity of Finite Sequences 16
3.6 Definitions 17
3.6.1 Histogram 17
3.6.2 Quantization 17
3.6.3 Central Limit Theorem 17
3.6.4 Extension Field 17
3.6.5 WG Transformation 18

4 Software Defined Radio, GNU Radio and USRP 19
4.1 Introduction 19
4.1.1 An Ideal Software Radio 20
4.1.2 Practical Software Defined Radio 21
4.2 Need for SDR 21
4.3 Evolution of SDR 22
4.4 SPEAKeasy 23
4.4.1 SPEAKeasy Phase I 23
4.4.2 SPEAKeasy Phase II 24
4.5 GNU Radio 25
4.5.1 GNU Radio Architecture 25
4.5.2 GNU Radio Companion (GRC) 26
4.6 Universal Software Radio Peripheral (USRP) 26
4.6.1 Features of USRP-1 26
4.7 Wrap-up 27

5 Literature Review **28**

5.1 Security and Privacy 28

5.2 Exploitation of Channel Characteristics 29

5.2.1 Blocker Tag 30

5.2.2 Noisy Tag Protocol 31

5.2.3 Noisy Reader 32

5.2.4 RFID Guardian 32

5.2.5 BUPLE 32

5.3 Authentication and Distance Checking 33

5.3.1 Distance Bounding Protocol 33

5.3.2 Hancke and Kuhn's Protocol 34

6 Direct Sequence Backscatter Encryption for Low Cost RFID Systems **36**

6.1 System Model 36

6.2 Finite State Machine for Tag 38

6.2.1 Discharging of Passive Tag 39

6.3 Direct Sequence Backscatter Encryption 40

6.4 Simulation Using GNU Radio 41

6.4.1 Design of Level Generator 42

6.4.2 Continuous Wave 43

6.4.3 Throttle 45

6.4.4 Modulation/Demodulation 45

6.4.5 AWGN Channel 46

6.4.6 Quantizer 46

6.4.7 Simulation Results and Analysis 46

6.5 Implementation Using SDR 49

6.5.1 Merits of Software Defined Radio 49

6.5.2 RFID Reader 50

6.5.3 Passive RFID Tag . . . 51
6.5.4 Experimental Environment . . . 51
6.6 Experimental Results . . . 51
6.6.1 Reader to Tag communication . . . 51
6.6.2 Channel Response . . . 53
6.6.3 Tag to Reader communication . . . 54

7 Security Analysis and Robustness Against Existing Attacks 58
7.1 Adversary Model . . . 58
7.2 Security Model . . . 59
7.3 Level Generators implemented by LFSRs and NLFSRs . . . 59
7.3.1 Combinatorial Generator using Multiple LFSRs . . . 60
7.3.2 Nonlinear Feedback Shift Register (NLFSR) . . . 61
7.3.3 Span n Sequences Generated from NLFSR . . . 61
7.3.4 Security Analysis of Level Generator using (N)LFSRs . . . 63
7.4 Level Generation Using Extension Field $GF(2^p)$ . . . 65
7.4.1 LFSR over $GF(2^3)$ . . . 65
7.4.2 Security Analysis . . . 66
7.5 Multilevel of Amplitude using FSRs . . . 66
7.5.1 Encoder . . . 67
7.5.2 Decoder . . . 68
7.5.3 Security Analysis . . . 68
7.6 Mutual Authentication . . . 69
7.6.1 Trade-off between Low Cost and High Security . . . 70
7.7 Robustness Against Different Attacks . . . 70
7.7.1 Test of Passive Eavesdropping . . . 70
7.7.2 Secure Against Replay Attack . . . 74
7.7.3 Secure Against Relay Attack . . . 74
7.8 Summary and Comparisons . . . 75

8 Conclusion and Future Work **76**

8.1 Contributions 77

8.2 Future Work 78

References **80**

List of Tables

6.1 Levels generated using two LFSRs 43

7.1 Levels generated using 2-PRSGs 64
7.2 Levels generated using 3-PRSGs 64
7.3 Levels generated using 4-PRSGs 65
7.4 Encoding of 2 bits 67
7.5 Encoding of 3 bits 68
7.6 Decoding of 3 bits 68
7.7 Example 73

List of Figures

2.1 General Architecture of RFID System 5
2.2 Signal and data flow in digital communication 6
2.3 Signal Coding in Baseband 7
2.4 Baseband waveform of Pulse Interval Encoding [53] 9
2.5 (a) Amplitude Shift Keying (*ASK or OOK*) (b) Frequency Shift Keying (*FSK*) (c) Phase Shift Keying (*PSK*) 10
2.6 UHF C1 Gen2 standard RFID communications [5] 10

4.1 An ideal Software Defined Radio 20

5.1 Wiretap Channel 29
5.2 Hancke and Kuhn's Protocol 34

6.1 Combinatorial generator with n PRSGs 37
6.2 Time samples of Binary bits of a PRSG 37
6.3 Finite State Machine (FSM) for tag 38
6.4 Charging and Discharging Phase of Passive Tag's Capacitor 39
6.5 Principle of level generator 41
6.6 Block diagram of simulation model 42
6.7 Time samples of generated three levels 43
6.8 Time samples of generated four levels 44
6.9 Time samples of generated five levels 44

6.10 Time samples of generated multi-levels 44
6.11 (a) Amplitude distribution (b) FFT of the received signal in simulation model (c) Amplitude distribution of decoded signal (d) FFT of the received data after decoding 47
6.12 Amplitude of added levels are higher than actual data 48
6.13 (a) Amplitude distribution (b) FFT of the received signal in simulation model (c) Amplitude distribution of decoded signal (d) FFT of the received data after decoding 49
6.14 System model 50
6.15 Complex time samples of levels generated and added constant continuous wave 52
6.16 FFT plot of the transmitted signal by Reader 52
6.17 Amplitude distribution plot of received signal 53
6.18 Tag's response at the receiver side 55
6.19 Tag's decoded messages 56
6.20 14-bit Tag's ID. The high amplitude signal represents **1** and low amplitude signal represents **0** 57

7.1 The block diagram of span n sequence from NLFSR of degree 20 62
7.2 The block diagram of span n sequence from NLFSR of degree 23 63
7.3 The block diagram of an 11-stage LFSR over $\mathbb{F}_{2^3}$ 66
7.4 The block diagram of i.i.d level generator using FSR 67
7.5 Passive Eavesdropping 70
7.6 Signal received by passive eavesdropper in scenario-I 71
7.7 Signal received by passive eavesdropper in scenario-II 72
7.8 Message decoded by passive Eavesdropper 72

Chapter 1

Introduction

Radio Frequency IDentification (RFID) is a contactless, automatic identification wireless technology primarily used for identifying and tracking of objects, goods and humans. This proliferating wireless technology is not only limited to identification and tracking applications but has been deployed in numerous securities sensitive applications, e.g., access control, e-passports, contactless payments, driver license, transport ticking and health cards as well [51, 66].

Conventionally, barcodes are used for keeping track of large number of objects, but they have been replaced by RFID tags in some products. RFID has superiority over bar-codes as they can detect massive objects individually, without line of sight (LOS), through non-conducting materials and contain much more information than merely a unique identifier for an object. Despite these benefits RFID devices (tags) are under threat of clandestine inventory.

RFID inherits all the security and privacy problems that are related to wireless technology in addition to those that are specific to RFID systems. The security and privacy protection schemes proposed in literature for wireless devices are mostly secured through symmetric keys encryption/decryption, hash functions and asymmetric keys encryption/decryption. The security of all these cryptographic algorithms depends on computationally complex problems that are hard to compute using available resources. However, these algorithms require cryptographic operations on RFID tags which contradicts the low cost demand of these tags. Due to limited number of logic gates in tags, i.e., 5K-10K, these methods are not practical. Much research has been done in attempt to solve consumer's privacy and security problem [12]. Solutions that prevent clandestine inventory are mostly application layer techniques [28, 35, 64].

Considering different security encryption/decryption schemes proposed by scholars at the expense of tag cost, the de facto standard for passive RFID systems, called EPCglobal UHF Class-1 Generation-2 (C1 Gen2) [53], doesn't include encryption/decryption as a part. They do not prevent other attacks that are specifically targeted to passive RFID tags. All these protocols have shown some weakness over the time [28]. Many attacks have shown that these application layer security can be by passed easily using relay attack, replay attack, brute-force attack, passive eavesdropping as well as active eavesdropping [10, 50, 17, 19].

1.1 Contribution

To solve this problem, a new RFID physical layer scheme has been proposed. The proposed scheme uses level generator to produce different levels before transmitting the signal to the tag. The tag responds to the signal sent by the reader using backscatter communications on the same signal which looks random to the eavesdropper. Therefore eavesdropper cannot extract the information from reader to tag and tag to reader communications using passive eavesdropping. As only the legitimate reader knows the different generated levels added to the carrier signal, it can remove the levels and retrieve tag's messages.

We propose a lightweight, low-cost and practically secure physical layer security to the RFID system, for a supply chain processing application, without increasing the computational power and tag's cost. The proposed scheme is validated by simulations on GNU Radio and experimentation using software defined radio (SDR) and a WISP tag. Our implementation and experimental results validate that *DSB Enc* is secure against passive eavesdropping, replay and relay attacks. It provides better results in the presence of AWGN channel.

1.2 Organization

The rest of the thesis is organized as follow. Chapter 2 gives an overview of fundamentals and background knowledge required for this thesis. Notation used in the thesis and preliminaries are defined in Chapter 3. Chapter 4 gives an review the historical background and evolution of Software Defined Radio, GNU Radio and Universal Software Radio Peripheral (USRP). Related work is discussed in Chapter 5. In Chapter 6, we introduce our physical layer approach for securing RFID systems using levels generator. It includes experimental setup, simulation and proof-of-concept. Section 6 discusses robustness of the proposed

scheme against existing attacks. Chapter 7 provides the security analysis of the level generator; other methods of implementing level generator; results of passive eavesdropping and measures against known existing attacks on low cost RFID passive tags. Chapter 8 concludes the thesis with the summary of the thesis and potential future applications.

Chapter 2

Background and Fundamentals

In this chapter, we will give the overview of the RFID system architecture and the physical layer characteristics used in different RFID standards. We will also discuss various privacy and security concerns in RFID systems.

2.1 RFID Architecture

An RFID system consists of RFID devices (*Tags*), Readers or *interrogators* and Back-end system or *database*. The general RFID architecture is shown in Figure 2.1.

2.1.1 Tags

Tags are embedded in all objects that are to be identified in RFID systems. Modern tag contains an Integrated Circuit (IC) chip with computational and storage capabilities and an antenna coil or coupling element for communications. The resources available to the tag varies depending on its power source and type. Tags can be mainly categorized into three types depending on the power source, i.e., active, passive and semi-passive tags.

- ***Active Tags*** have on board power source and much higher computational and storage capabilities, e.g., NFC enabled cell phones and an embedded RFID wireless sensor nodes.

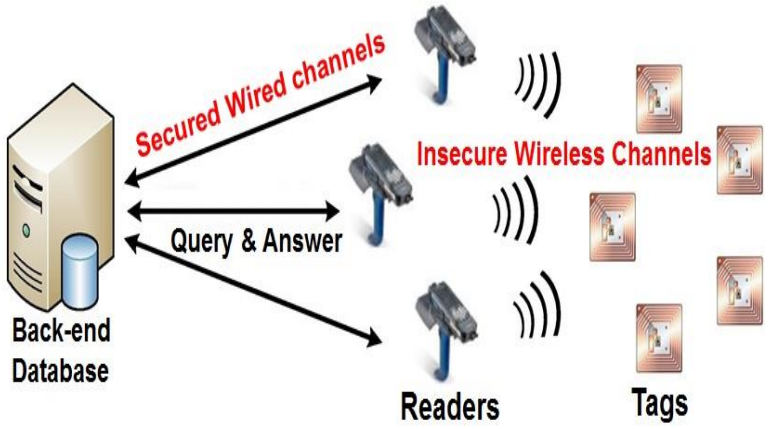


Figure 2.1: General Architecture of RFID System

- ***Passive Tags*** do not have internal power source. They harvest power from the reader's signal. These tags cannot perform complex computations due to power limitation. They harvest power when they come in the vicinity of reader's signal and store that power which depletes very rapidly. The power used for transmitting signal, from tag to reader communication, is inversely proportional to the square of the distance between the reader and the tag.
- ***Semi-passive Tags*** lie between the active and passive tags. They use battery power for computation and harvest energy from reader's signal for communications, e.g., Automated toll payment tags

2.1.2 Readers

An RFID reader or *interrogator* is a transceiver which sends commands to the tags and receives data from them. There are two types of readers:

1. *Portable readers*, i.e., NFC enabled cell phones acts as RFID reader's mode. These readers have power limitation which restricts their operation range.
2. *Fixed readers* have much higher capability of storage and processing range. Both readers talk to the database through a secured link which is not considered as part of RFID security vulnerability.

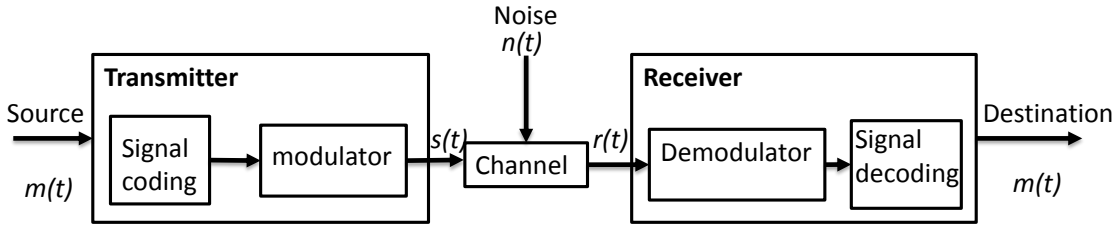


Figure 2.2: Signal and data flow in digital communication

2.1.3 Back-end Database:

Reader queries the tags for public IDs and then retrieve the private data corresponding to that ID from a secure database. This reduces the tag cost and helps in managing the data.

2.1.4 Physical Layer

Digital communication system consists of three main components, i.e., *signal processing* (*line coding*), *communication channel* and *modulator/demodulator* as shown in Figure 2.2. Similarly for an RFID system, in order to communicate on a physical layer it must have these three basic functional blocks. To transmit message over an RF channel the message source must be first encoded. The encoded signal influences the electromagnetic waves of a particular carrier depending on type of modulation used in a system. In digital communications, the signal can be represented as '1' and '0' in various line codes. RFID systems use one of the following schemes: Non-Return-Zero (NRZ), Manchester, Unipolar RZ, Differential Bi-Phase (DBP), Miller, Modified Miller, differential coding on Pulse Pause (PP) coding. Line coding (signal coding) used in an RFID system greatly depend on the boundary conditions.

Line Coding

Line coding is used for clock synchronization, elimination of DC component and can help in data recovery. Various line coding schemes used in RFID systems are shown in Figure 2.3.

- ***Non-Return-to-Zero (NRZ):*** Binary bits '1' and '0' are mapped onto high signal '+1' and low signal '-1' respectively for one bit period. If NRZ encoding is used with

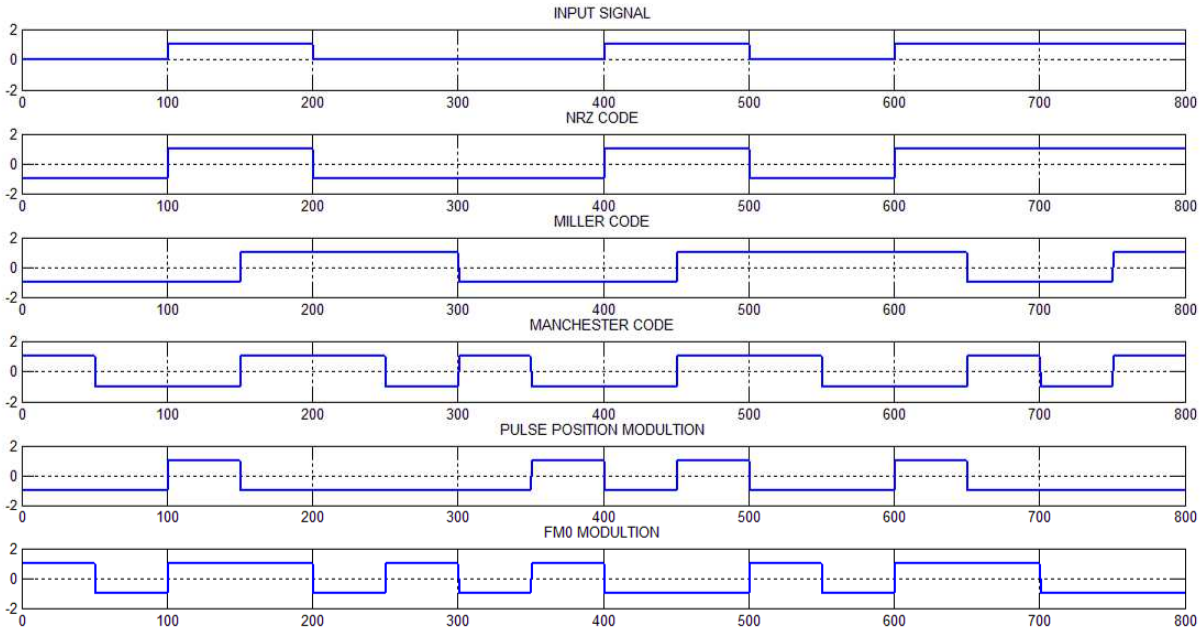


Figure 2.3: Signal Coding in Baseband

100% ASK the tag can not harvest the power through the carrier. Even if 33% ASK is used with long zero run sequence, it would interrupt the power. Therefore, it is used with FSK and PSK modulations.

- ***Miller:*** A binary bit '1' is encoded to half bit positive/negative edge transition and bit '0' is represented by the continuance of the preceding signal level of a bit period. An initial reference is taken for starting bit of the sequence and the following bits are mapped onto high signal and low signal depending on the combinations of preceding and current bits. If '1' bit is followed by '1', the half bit edge transition would be converted to its inverse transition. If '0' bit is followed by '0', inverse transition occurs at the start of bit period.

  In EPC Class-1 Generation-2 UHF RFID protocol tag to reader communication uses a modified miller sub-carrier coding [53]. A bit '0' is always encoded with low pulse at the start of a bit period and bit '1' is encoded with low pulse with a delay of half bit period. Miller modulated sub-carrier encoding uses 2, 4 or 8 cycles of a sub-carrier square wave for each bit period. The modified Miller encoding transitions are indicated by phase shifts of 180° in the sub-carrier. Each sub-carrier is modulated with ASK or PSK on another carrier.

- ***Manchester:*** A low to high transition and high to low transition represents bits '1' and '0' receptively. All these transitions occurs in the middle of a cycle at each transition, which helps in data clock recovery. Manchester coding techniques utilizes twice the bandwidth of NRZ with exclusively no DC component.

- ***Pulse Position:*** Pulse Position Modulation (PPM) encodes m message bits in one of the 2^m time slots. PPM is suitable for reader to tag communications since the decoding circuit is extremely simple, which results in small and light weight tags.

- ***Pulse Interval Encoding:*** In Pulse Interval Encoding (PIE), also known as pulse-pause coding, a bit '1' is represented by a pause of $2t$ before the next bit period and a bit '0' is represented by a pause of t before the next bit period where t is a unit time duration varying from 6.35μs to 25μs also known as Tari (Type A reference interval) as shown in Figure 2.4. PIE is used in EPC C1 Gen2 UHF RFID protocol from reader to tag communications [53]. The advantage of using PIE from reader to tag data communication is that there is a continuous flow of power supply to the tag.

- ***FM0 Encoding:*** FM0 encoding is a bi-phase-space encoding. In FM0 encoding, a bit '1' encodes to a constant signal level and a bit '0' encodes to transition in the middle of a bit period. FM0 inverts the phase at the boundary of each bit period.

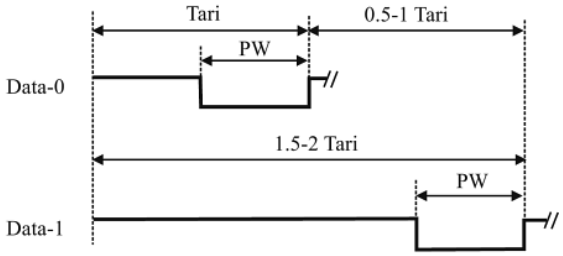


Figure 2.4: Baseband waveform of Pulse Interval Encoding [53]

FM0 encoding is used in tag to reader communications in EPC C1 Gen2 UHF RFID protocol [53]. Since there is transition in each bit period in FM0, data clock is embedded in it and can be recovered easily.

Modulation

Modulation is a process of sending the baseband data signal by varying the characteristics of a periodic electromagnetic wave (*carrier signal*). A sinusoidal carrier can be characterized by

$$x(t) = A_i \sin(2\pi f_c t + \phi_i) \tag{2.1}$$

From equation (2.1), the different carriers can be generated by varying the carrier's amplitude A_i, frequency f_c and phase ϕ_i to represent the baseband data signal. In HF and UHF RFID systems, digital modulations schemes are used, i.e., *Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK) and Phase Shift Keying (PSK)*. Examples of modulation schemes used in ISO 14443 and EPC UHF C1 Gen2 are shown in Figure 2.5.

In ISO 14443 framework, type A uses 100% ASK modulation at 13.56 MHz and a subcarrier at 847 kHz with a modified miller encoding. Type B uses BPSK modulation at same frequency as type A with NRZ-L encoding. In UHF C1 Gen2 standard, reader to tag communications use 30% to 100% ASK (*DSB-ASK, SSB-ASK, PR-ASK*) at 902-928 MHz divided into channels (200kHz, 500kHz) with PIE encoding. Tag to reader communications use ASK or PSK with FM0 or Modified Miller encoding. For conducting experiments, we have chosen 100% ASK with NRZ-L encoding.

Figure 2.6 shows the UHF C1 Gen2 standard RFID reader and tag communications.

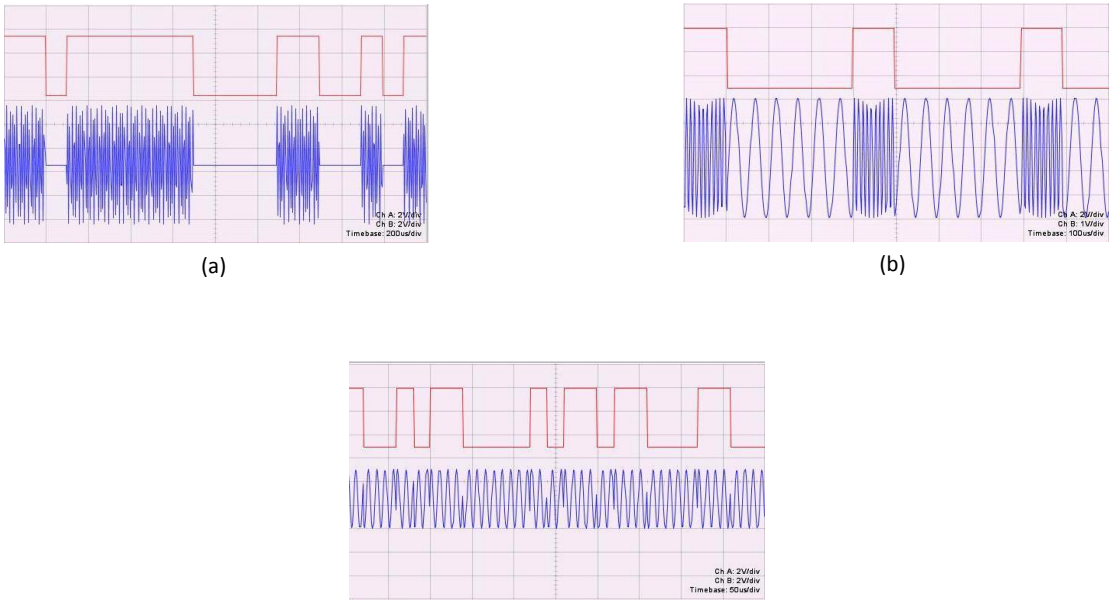
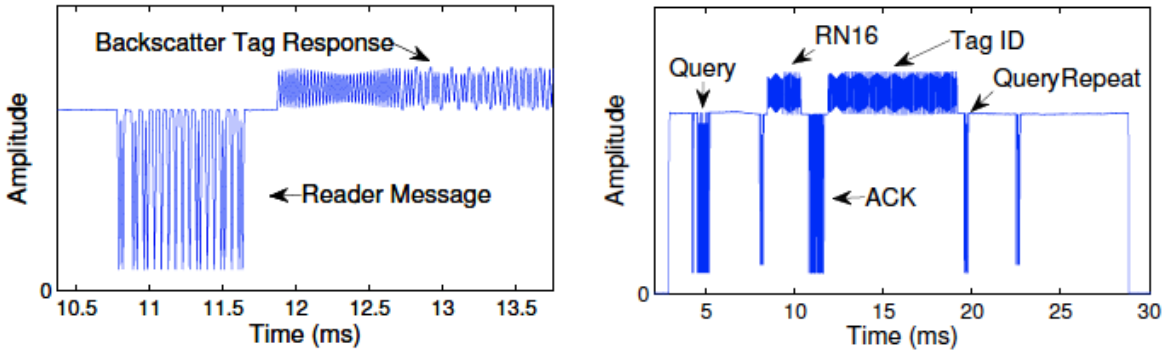


Figure 2.5: (a) Amplitude Shift Keying (*ASK or OOK*) (b) Frequency Shift Keying (*FSK*) (c) Phase Shift Keying (*PSK*)



(a) Reader command and tag response

(b) Message exchage between reader and tag

Figure 2.6: UHF C1 Gen2 standard RFID communications [5]

2.2 Vulnerability of RFID System Security

2.2.1 Privacy and Security Issues

RFID system is still passing through its developing phase. Many concerns have been expressed regarding the risks and threats of RFID systems. With the wide adoption of RFID technology, it has raised many security and privacy issues.

2.2.2 Privacy

- ***Tracking Problem:*** Adversary À can send beacon signals to query tag multiples time through different locations and distances, keeps a record of all the data sets it received from tag at particular time t and further using these data points to trace/track the movements of an individual while keeping his identity secret. These patterns can also be used for backward/forward tracing/tracking. Backward tracing reveals the secret information before time t. Similarly, forward tracing provides secret information after time t.

- ***Inventory Problem:*** As RFID tags also carry personal information of the user, e.g., mental health record in health card, confidential information in driving license, e-passport and credit cards, an adversary Á can get all the stored personal information apart from unique identification number of tag. EPC tag has four memory banks carrying additional information. They are Tag Identification (TID), Reserved, EPC and User [60]. Therefore a person carry EPC tag is subjected to inventory problem.

2.2.3 Security

- ***Passive Eavesdropping:*** Eavesdropper (ξ) listens to the communications between legitimate reader and the tag without participating in the conversation hence securing its identity. Such kinds of attacks are the biggest threat to RFID systems. As the system cannot detect the presence of an ξ. These attacks give rise to many other attacks.

- ***Active Eavesdropping:*** Espionage is not only passive it can also be active. In an active eavesdropping, ξ actively sends query to the tag from a longer distance. Such kind of attacks can be used in different scenarios.

- ***Replay Attack:*** ξ listen to the communication between reader and the tag for many sessions. This eavesdropping can be passive/attack. Later replay the previously collected data to the legitimate reader to breach the security of the system.

- ***Relay Attack:*** The most strongest and unavoidable attack in RFID systems is a relay attack. Relay attack by passes all forms of authentication and authorization protocols. Even the most secured cryptographic protocols and primitives cannot avoid this attack. In relay attack an adversary relays the messages between the reader and the tag. RFID challenge-response protocol can easy be relayed using two NFC-enabled cell phones [17, 19].

- ***Man-In-The-Middle Attack:*** Unlike relay attack, ξ not only relays the messages between the reader and the tag in MITM attack. Instead he modifies the relayed messages to recover the secret information or may harm the tag by sending the kill command to the tag. Such kind of attacks can be used to attack the back-end system, e.g., database injection.

- ***Denial of Service:*** Á tries to desynchronize/sabotage the communication by jamming the signals from the reader or by sending fake messages to the system. As a result, the system would not give access to the legitimate tag. Such kind of attacks are serious threat to military/medical applications.

- ***Side channel Attack:*** Á gets hold of the RFID device physically and tries to get the secret information/key by analyzing the power traces and exploiting the physical implementation weakness in the cryptographic algorithms. Side channel attacks are mainly divided into four categories, i.e., timing attack, fault attack, power analysis attack and electromagnetic attack.

- ***Brute force Attack:*** Most of the securing techniques in RFID systems involve application layer cryptography, i.e., symmetric/asymmetrical keys. But due to storage and computational limitation of these devices brute force attack are practical. ξ searches for the required key by looking through a whole search space.

Ideally, an RFID system should be able to prevent all of above mentioned attacks. But such a system does not exists in reality. There is no solution that can prevent all of these security and privacy issues all together. Therefore, we expect a security model which could mitigate as many problems as possible. In Chapter 7, we would compare different attacks against our proposed scheme.

Chapter 3

Preliminaries

This chapter defines the list of notations, definitions and fundamental background information essential for later chapters.

3.1 Notations

We will use the following notions throughout the thesis

- Á represents an Adversary in the system.
- Ř represents legitimate Reader.
- Ť represents legitimate passive Tag.
- ξ represents passive Eavesdropper in the system.
- É represents passive eavesdropper's receiver in the system.
- $\mathbb{F}$ represents finite field.
- $F_2 = GF(2)$ represents finite field with 2 elements: **0** and **1**.
- $F_{2^p} = GF(2^p)$ represents extension field of $GF(2)$ with 2^p elements. Each element in this field is represented as a p bit binary vector.

3.2 Backscatter Communications

The basic principle on which passive RFID system works is similar to radar principle in which the reader sends RF signal to the passive tag. Passive tag harvests power from the incident continuous wave sent by the reader to communicate in both directions. The readers send amplitude modulated carrier given by

$$CW(t) = A(t)\cos(2\pi f_i t + \theta) \tag{3.1}$$

where $A(t)$ is the amplitude of the carrier wave, f_i is the carrier frequency $\in \{f_1, ..., f_k\}$ and θ is a phase of a carrier signal.

This CW is rectified at the tag and supplies power to the tag. Tag decodes the reader's command if any using envelope detector. After transmitting the command, the reader keeps $A(t)$ at high amplitude while waiting for the tag response. In EPC C1 Gen2 [53], tag could reply on the same CW with ASK or PSK modulations using FM0 or Miller sub-carrier encoding schemes with clock recovery information embedded in it. Tag backscatters the encoded responses mixed with CW by changing the reflection coefficient of the antenna. The received signal is detected using matched filter and the backscattered signal's amplitude is compared to a threshold.

3.3 Power Distance Relationship

The power received at the input of receiver antenna is expressed in terms of transmitted power of transmission antenna separated at a distance of R in free space model by Friis equation:

$$P_r = P_t G_r G_t \left(\frac{\lambda}{4\pi R}\right)^2 \tag{3.2}$$

where
P_r is the received power
P_t is the transmitted power
G_r is the receiver antenna gain
G_t is the transmitter antenna gain
λ is the carrier wavelength and
R is the distance between transmitter and receiver.

Eq.(3.2) is the simplest form of Friis equation when there is no polarization mismatch between transmitter and receiver.

Two Path Model: Far field communications can be modeled with two path propagation model in which there is one line of sight (LOS) path and other is the reflected path [65]. At small distance the received power P_r is proportional to $\frac{1}{R^2}$, in symbol $P_r \propto \frac{1}{R^2}$. Above some critical distance R_c, the received power is given by

$$P_r \approx P_t G_r G_t \left(\frac{h_t h_r}{R^2}\right)^2 \tag{3.3}$$

where h_t and h_r are the transmitter antenna and receiver antenna heights with respect to ground. *Remark:* Above R_c, $P_r \propto \frac{1}{R^4}$ and independent of the carrier frequency.

3.4 Pseudorandom Sequence Generator

A sequence in which the complete knowledge of previous output bits does not assist in predicting the next bit with a probability better than half is called *truly random sequence*. A random sequences are produced by using two different approaches. The first approach to generate random bits is from truly random source, i.e., tossing a coin or extracting information from noise process in communication system. The other approach is to produce random bits by using deterministic algorithms. The binary sequences generated by deterministic algorithm are called *pseudorandom sequences* and the deterministic algorithm is called a *pseudorandom sequence generator* (PRSG).

The sequence produced by using truly random source does not guarantee the required statistic characters and mathematical properties which are essential for reliable and secure communications.

3.4.1 Linear Feedback Shift Register with Maximum Period

A shift register whose feedback function is a linear function is called linear feedback shift register (LFSR). If the feedback function $f(x_0, x_1, ..., x_{n-1})$ is a linear function, i.e., if it can be expressed as

$$f(x_0, x_1, ..., x_{n-1}) = c_0 x_0 + c_1 x_1 + ... + c_{n-1} x_{n-1}, c_i \in F, \tag{3.4}$$

then the recursive relation becomes the following linear recursive relation

$$a_{k+n} = \sum_{i=0}^{n-1} c_i a_{k+i}, k = 0, 1, ... \tag{3.5}$$

Thus feedback shift register is called *linear feedback shift register* (LFSR) and the output sequence is called a *linear feedback shift register (LFSR) sequence*.

A sequence with period $2^n - 1$ generated by an n-stage LFSR is called a *maximal length sequence*, or m-sequence [20].

3.5 Complexity of Finite Sequences

Complexity of the given finite sequence depends on the randomness or uncertainty/entropy of the sequence. Kolmogorov in [31] has proposed an algorithm for shortest Turing machine program in which when fed with an object x produces the exact same sequence y as a measure of complexity of that sequence. The entropy of the sequence is measured by the amount of information conveyed by the produced sequence y about the object x (initial seed) which generates the specific sequence. Lempel and Ziv in [33] has proposed an approach for measuring the complexity of finite sequences.

Let S be a sequence of production process with m steps, i.e., $S(1, h_i)$, $i = 1, 2, ..., m$ which are the states of the process. The parsing of S is given by

$$H(S) = S(1, h_1)S(h_1 + 1, h_2), ..., S(h_{m-1}, h_m) \tag{3.6}$$

which is called the production of S and m initial states $S(1, h_i)$ are called the *components* or *history* of $H(S)$. Let $c(S)$ define the complexity of production a sequence (S) and $c_H(S)$ denotes the number of components in the history $H(S)$ of S. Then

$$c(S) = \min\{c_H(S)\} \tag{3.7}$$

where minimization is over the complete history of S. Therefore, $c(S)$ is the minimum number of steps in a process required to generate the S according to the rule of production.

The aforementioned notion of complexity of finite sequence can be linked with pseudo-random sequences. In feedback shift registers the complexity of a sequence is defined in term of *linear span* or (*linear complexity*). *Linear complexity* defined as a shortest linear feedback shift register (LFSR) which generates the same sequence.

According to (3.6), in this case, the entropy of a finite sequence is the same as the least number of bits required to produce the specific sequence, which is equal to the length of the shortest LFSR which produces the sequence. In other words, the entropy of a finite sequence is equal to the linear span of the sequence. Thus the entropy of variable x is given by

$$H(x) = \log_2 N \ , \qquad x \in X, \, |X| = N. \tag{3.8}$$

Example: For an m-sequence of length $2^m - 1$, the complexity of the sequence will be $H(x) = \log_2(2^m - 1) \approx m$.

3.6 Definitions

3.6.1 Histogram

Histogram is defined as the graphical representation of distributed data that is an estimate of probability distribution of continuous variable.

3.6.2 Quantization

The process of mapping the large range of values of a wave into finite set of values. Each level in the finite range set is called *level of quantization*. The device that converts the analogue signal into digital is called *quantizer*. The difference between the actual value and quantized value is known as the *quantization error*. Quantization error occurs due to the finite level of quantizations and cannot be more accurate than $\pm \frac{1}{2}$ quantization step because of the resolution of the device. High resolution devices have less quantization error.

3.6.3 Central Limit Theorem

Let $X_1, X_2, ..., X_n$ be independent, identically distributed (i.i.d) random variables having mean μ and a non-zero variance σ^2. If $S_n = X_1 + X_2 + ... + X_n$, Then

$$\lim_{n\to\infty} P\left(\frac{S_n - n\mu}{\sigma\sqrt{n}} \leq x\right) = \phi(x) \tag{3.9}$$

where $\phi(x)$ is the probability that standard normal random variable is less than x.

3.6.4 Extension Field

$GF(p^n)$, $n > 1$ is called an extension field of $GP(p)$. If $p = 2$, we called it a binary extension field. In symbol it is represented as $\mathbb{F}_{p^n}$.

3.6.5 WG Transformation

Let

$$t(x) = x + x^{r_1} + x^{r_2} + x^{r_3} + x^{r_4}, \qquad x \in \mathbb{F}_{2^n} \tag{3.10}$$

where $r_i's$ are defined by

$r_1 = 2^k + 1$	$r_1 = 2^{k-1} + 1$
$r_2 = 2^{2k-1} + 2^{k-1} + 1$	$r_2 = 2^{2k-2} + 2^{k-1} + 1$
$r_3 = 2^{2k-1}2^{k-1} + 1$	$r_3 = 2^{2k-2}2^{k-1} + 1$
$r_4 = 2^{2k-1} + 2^k 1$	$r_4 = 2^{2k-1} + 2^{k-1} + 1$
for $n = 3k - 1$	for $n = 3k - 2$

Then a function

$$f(x) = \mathrm{Tr}(g(x + 1) + 1), \qquad x \in \mathbb{F}_{2^n} \tag{3.11}$$

where f(x) is a function from $\mathbb{F}_{2^n} \to \mathbb{F}_2$ and is called the *WG Transformation* of $\mathrm{Tr}(g(x))$. The WG transformation only exits if n $(mod\ 3) \neq 0$ [20].

Chapter 4

Software Defined Radio, GNU Radio and USRP

In this chapter we will give an overview of Software Defined Radio and its applications, GNU Radio (an open source software toolkit used for signal processing on a host computer) and USRP (a hardware device use as a transceiver for radio signals and feeds the DSP or host embedded PC with sampled signals for processing).

4.1 Introduction

Radio is a science of communicating over a distance by converting sounds or signals to electromagnetic waves and radiating these through space in a radio frequency band in a range of about 10kHZ to 300GHz [21]

With the evolution of communications technology, its rapid change from analog to digital has made it possible to implement most of the radio functions in software in modern radio systems leading to software defined radio. The term software defined radio (SDR) or software radio (SR) was first coined by Joseph Mitola in 1991. According to the latest definition recently coordinated between the IEEE and the SDR Forum:

> *A software defined radio is radio in which some or all of the Physical Layer Functions are software-defined*

An extensive definition is given by Joseph Mitola:

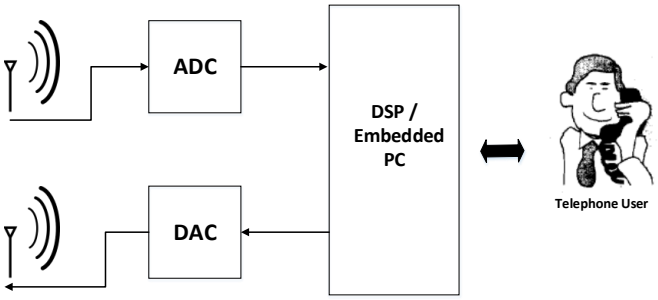


Figure 4.1: An ideal Software Defined Radio

> *A software radio is a radio whose channel modulation waveforms are defined in software. That is, waveforms are generated as sampled digital signals, converted from digital to analog via a wideband DAC and then possibly upconverted from IF to RF. The receiver, similarly, employs a wideband Analog to Digital Converter (ADC) that captures all of the channels of the software radio node. The receiver then extracts, downconverts and demodulates the channel waveform using software on a general purpose processor. Software radios employ a combination of techniques that include multi-band antennas and RF conversion; wideband ADC and Digital to Analog conversion (DAC); and the implementation of IF, baseband and bitstream processing functions in general purpose programmable processors. The resulting software-defined radio (or software radio) in part extends the evolution of programmable hardware, increasing flexibility via increased programmability* [39].

The convergence of SDR is made conceivable due to advancement in software and digital signal processor (DSP) that allows digital processing of radio frequency signals. A software radio uses digital signal processing and software communications radio system functions (mixers, filters, amplifiers, modulators/demodulators, detectors, channel model etc) on a targeted processor and memory to host it for real time communications.

4.1.1 An Ideal Software Radio

An ideal software Radio consists of an Antenna, Analog to Digital converter (ADC)/ Digital to Analog Converter (DAC) and embedded processor to handle all digital processing for

the received/transmitted signals. An ideal SR is shown in Figure 4.1.

In the receiver chain, an antenna receives the signals and passes it on to the ADC. Digital samples are then passed through the DSP or embedded PC for further processing. Similarly, in the transmitter chain, digital samples are taken from DSP or embedded PC and passed on to the DAC which feeds analog signals to the antenna for transmission. In a transceiver path, the processing block and an antenna may be shared between receiver and transmitter.

4.1.2 Practical Software Defined Radio

SDR presented in the previous section is simple and extremely flexible but it is not practical. The practical software defined radio includes many non-DSP hardware components like anti-aliasing filters, power handling, frequency up/down converters, etc. as the current ADC/DAC and DSPs does not support direct sampling of wideband RF signals.

As technology is ever evolving, the digital signal processors (DSP) are becoming faster, the conversion rates and the dynamic range are increasing, ADC/DAC are getting closer to the antenna. Due to this reason software defined radio is replacing the analogue circuitry in conventional radio systems by taking up additional processing tasks in the software part.

4.2 Need for SDR

In the past, the radio was used for military purposes and each one could only perform the particular task it has been designed and optimized for. If ever a need was evolved to use the radio for a different task, the complete hardware had to be re-designed. This was of course a costly and less flexible solution which led to compatibility issues as well. This problem was addressed by Velcro radios [23] who presented a solution for reducing the hardware that had to be carried around. The solution was developed on the basis of common architecture involved in all radios. They proposed to use a common motherboard and attached different peripherals (silicon chips) to it. For example if an army commander wants to talk to another on a particular frequency, he would use a specific peripheral and connect with his motherboard. He can replace the chip if he wants to use another frequency and protocol related to it. This reduced the total hardware involved in the conventional military radio systems but there was limited cross-functionality when a specific chip would only be compatible to the motherboard provided by the same manufacturer. An open

modular hardware architecture was developed to address this problem but communicating with simultaneously different radios were still not feasible [42].

As technology advanced rapidly, flexible software implementation of analog circuits in digital processing took over more tasks that were initially accomplished in less flexible programmable and special purpose hardware devices. The flexibility of software implementation of digital components of radio allows adaptive transitions to waveforms and RF frequencies not possible in previous technologies. SDR allows easy and simple enhancement to the existing system without replacing or modifying the hardware.

4.3 Evolution of SDR

Software Defined Radio has been originated by defense sector of US and Europe in late 1970s [23, 40]. By the end of the 1980s, emerging standards and incompatible protocols had made the radio technology evaluation process stagnant [42]. There were compatibility and cross-functional limitation problems in communicating on different RF frequency bands using different encoding methods and waveforms. Conventional radios were not keeping up to the rapid change in technology adoption. Similarly, the commercial use of radio systems were passing through the same dilemma. Each manufacturer wanted to provide new features on minimized cost layout by keeping the legacy system architecture. This limited the radio systems to specific geographic locations around the world. The proponents of radio technology were looking for a *MultiBand MultiMode Radio* (MBMMR) systems [32, 38].

Initially, MBMMR was implemented by encapsulating different RF bands and modes in a single package that could change their configuration by changing the parameters and were known as Velcro radios. By packing all these peripherals in the same system tremendously increased its size.[1].

To reduce the size of Velcro radios, Programmable Digital Radios (PDRs) were introduced in which programmable ROMs and ASIC processors replaced small hardware components. A prominent increase in efficiency, flexibility and reduction in size, weight and cost intrigued the manufacturers and researcher to shift more hardware functionality to software processing which gave birth to software defined radios. With the increase in conversion rate and dynamic range of AD/DA converters, the RF components got closer to the software processing independent of analog hardware, which provided more flexibility in generating different waveforms without modifying the hardware.

[1]Moree's law does not apply to RF components [42]

4.4 SPEAKeasy

SPEAKeasy was the first publicly announced military software radio initiated by US Department of Defense. The rationale behind SPEAKeasy program was to develop a modular, reprogrammable, reconfigurable, modem with open architecture. SPEAKeasy program was into two phases. The Phase I was aimed to demonstrate a proof-of-concept for the feasibility of software radios and its ability to inter-operate with more than 15 existing radios using MBMMR's envision.

4.4.1 SPEAKeasy Phase I

The Phase I was researched from 1992 to 1995, which was conducted by Hazeltine as the major contractor, and TRW as software subcontractor [32]. The Phase I was designed and implemented to provide the basic architecture for software radio and have the following capabilities:

- Interoperability between military radios
- Adaption of emerging new technology
- More flexibility without compromising the performance and power consumption
- Aim to cover single wide-band range from 2 MHz to 2 GHz
- Incorporating information security as well as transmission security using programmable INFOSEC processor, Cryptographic Reduced instruction Set (CYPRIS) and software implementation of the cryptographic algorithms in the multichannel SPEAKeasy INFOSEC Module (SIM)

The first practical demonstration of SPEAKeasy Phase I carried out successfully in June 1995. The interoperability was presented by connecting multiple existing radios applying different protocols. New protocols were programmed into software and were exhibited by two units of SPEAKeasy. The technology available then did not permit to have a single wide band RF channel of range 2MHz-2GHz, so they divided the range into 3 sub-bands. The first was High Frequency (HF) ranging from 2-30MHz. The second was Very High Frequency (VHF) ranging from 30-400MHz. The last is Ultra High Frequency (UHF) ranging from 400MHz-2GHz. Only VHF band was implemented in Phase I for feasibility

demonstration. It was observed that software radios are feasible for interoperability functions of radios and are compatible with new features of evolving technology. The general architecture of SPEAKeasy was same as conventional radios but all the blocks were digital except for the front end antennas. The common hardware was reprogrammable, multichip module (MCM) was employed for basic signal processing and CYPRIS was used for INFOSEC and TRANSEC for transmission security.

4.4.2 SPEAKeasy Phase II

The Phase II of SPEAKeasy was a 4 year project initiated in 1995. Motorola was the prime contractor and designed a white band RF transceiver. Its main features included open architecture for the entire radio and a more formalized software structure as compared to Phase I. Security was incorporate in its software structure in the single architecture as two modules, *BLACK* (secure) and *RED* (unsecure). The primary objectives of Phase II are as follows:

- Implementing a reconfigurable architecture
- Open and modular architecture for the entire radio system
- Cross Channel Connectivity
- Emphasis on more commercial off-the-shelf (COTS) and incorporating standards
- CYPRIS was improved to handle many different algorithms of INFOSEC and TRANSEC simultaneous
- Reduce radio size to improve practicality in the field

Though it was a 4 year project but it was ready for demonstration within 15 months. The exhibit was successful and manufacturing was started immediately. The Land Mobile Radio (LMR) waveform was developed in less than two weeks to add to SPEAKeasy units. One of the units was repaired in the field using COTS [14]. Since this was the first demonstration of Phase II so only 4-400MHz was exhibited in it but it achieved all its primary objectives. The project was closed and no further research was carried out for SPEAKeasy.

The hardware and software of SPEAKeasy Phase I and Phase II was used by joint tactical radio system programs (JTRS) and SDR forum for defining their standards.

4.5 GNU Radio

The *GNU Radio* is software development toolkit provided with signal processing library for developing and experimenting with SDR concepts. GNU Radio works under GNU General Public License (GPL)[2]. The project was initiated in 2000 by Eric Blossom and now supported by large community of volunteers working for the development of SDR. GNU Radio is mainly supported for Linux operating system with partial support for Mac and Windows.

4.5.1 GNU Radio Architecture

Processing Blocks: Signal processing blocks take continuous data stream(s) at their input and generate data stream(s) at their output. Apart from signal processing blocks, GNU Radio also provides signal sources and sinks which only produce or consume data stream(s) respectively. GNU Radio processing library provide more than 100 signal blocks. User can also write his own processing block if needed[3]. GNU radio framework take care of each block's number of input samples it might requires to produce the required output samples by using **forecost()** method.

Data Buffers: Blocks can have different input streams rate in flow graph but all output streams must be generated at the same rate.Blocks have input and output buffer associated with them to keep synchronization among different stream rates.

Flow Graph: GNU Radio applications are written using flow graph. The vertices in flow graph represent the processing blocks and edges constitute the data flow between them. The signal processing blocks are written in C++ language and are connected using Python. Each block primarily written for performing only one task to enable open and modular software architecture. Processing block takes infinite stream(s) of data flow from the input and after processing provides the output stream(s). GNU Radio uses Simplified Wrapper and Interface Generator (SWIG) to interface signal processing block written in C++ to be accessible from Python.

Data Type: The data types of signal processing blocks' stream can be of any kind. But the most common data types used in GNU Radio are

- c - complex(float)

[2]The GNU General Public License is a free, copyleft license for software [59].

[3]Further information about how to write a signal processing block can be found at [46, 47]

- f - single precision float
- s - short integer (2-byte)
- i - integer (4-byte)

These data types also exist as vector type. The data flows from one block to another in the form of bits or samples.

4.5.2 GNU Radio Companion (GRC)

GRC is graphical tool for creating signal flow graphs by connecting different processing blocks written in GNU Radio and generates a Python script to create and control signal flow graphs using visual programming language for signal processing via GNU Radio libraries. It provides easy and editable drag and drop flow graph environment to work without worrying about the underlying processes. GRC was developed by Josh Blum [3].

4.6 Universal Software Radio Peripheral (USRP)

USRP provides hardware interface for GNU Radio to build software defined radio using UHD. UHD is a hardware host driver and API for Ettus Research products i.e. all USRP devices, compatible with Linux, Windows and Mac. Users are able to use UHD driver standalone or with third party applications such as GNU Radio, Simulink, OpenBTS, Iris and LabVIEW [57]. A typical USRP consists of one motherboard which supports several plug-on daughterboards of different RF bands. USRP with GNU radio provides a complete SDR platform. USRP connects to a host PC via USB2.0 (USRP1) [55] or Ethernet (USRPN210) [56].

4.6.1 Features of USRP-1

USRP-1 includes the following features.

- Four 64 MS/s 12-bit analog to digital Converters and four 128 MS/s 14-bit digital to analog Converters

- Four digital downconverters and two digital upconverters with programmable decimation rates and interpolation rates respectively
- High-speed USB 2.0 interface (480 Mb/s) and capable of processing signals up to 16 MHz wide
- Modular architecture supports wide variety of RF daughterboards
- Auxiliary analog and digital I/O support complex radio controls such as RSSI and AGC
- Fully coherent multi-channel systems (MIMO capability)

4.7 Wrap-up

GNU Radio with the USRP provide an inexpensive, flexible and powerful supporting tool in license free radio bands for learning and experimenting with software defined radio concepts. Most of the applications can be developed using GRC without even writing any code. With increasing number of available signal blocks, GNU radio is becoming more and more flexible.

Chapter 5

Literature Review

In this chapter, we will review the various physical layer approaches proposed in literature to secure the communications of RFID system.

5.1 Security and Privacy

RFID system security mainly depends on the privacy and authentication of $\check{\mathrm{R}}$ and $\check{\mathrm{T}}$ [28]. Conventionally, privacy and security is considered essentially as a part of the upper layers except physical layer. With advances in technology, most of the cryptographic protocols are implemented at application layer with an assumption that physical layer is already present for reliable transmission of the encoded information from sender to receiver. Even if Eve gets the encoded data, he could not decode the bits without some additional knowledge. Unfortunately, this principle holds for many of communication devices but not for all of them. Ultra-low power environment technologies like wireless sensor nodes and RFID are designed for low cost and long life applications. Due to real time data processing with power, time and computational constraints, these technologies are subjected to security and privacy problems [34, 41]. Recently, extensive research has been carried out on the physical characteristics of communication channel to secure ultra-low power technologies from various security and privacy threats.

5.2 Exploitation of Channel Characteristics

In the literature many physical layer techniques have been proposed. Most of them use noise generator as an additional hardware to produce noise from the reader [44] or from the RFID tag's side [7]. In this way the eavesdropper, who is unaware of the added noise to the signal cannot filter it out to retrieve the messages that are being exchanged between the reader and tag.

Adding noise to the wireless communication channel is not a novel technique, it has been around for many years derived from the Shannon's work [45]. Later in 1975, Wyner introduced the wiretap channel [49]. In his model, sender and receiver can securely communicate through a particular encoding and decoding pair in the presence of wiretapper without pre-shared key [27]. The goal of such communication channel is to send the message from source to legitimate receiver, while keeping an eavesdropper unaware of the messages that are being exchanged. The key element of wiretap channel is that the legitimate receiver and wiretapper have different channels from the source. The main channel is noiseless and only contains the communication channel noise, i.e., $\mathbf{N}'$ whereas Wiretap channel has significant noise, i.e., $\mathbf{N}''$ as shown in Figure 5.1.

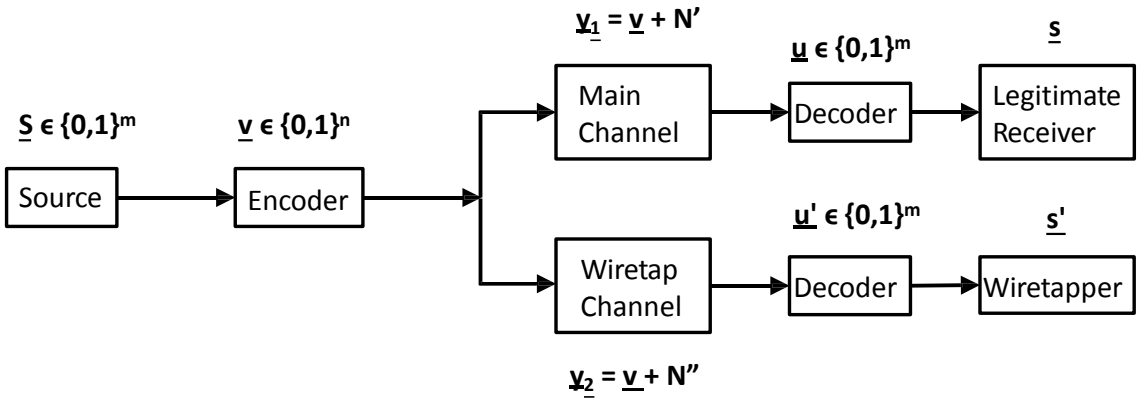


Figure 5.1: Wiretap Channel

The channel characteristics of main and wiretap channels can be expressed as

$$\underline{\mathbf{y}_1} = \underline{\mathbf{v}} + \mathbf{N}'$$

$$\underline{\mathbf{y}_2} = \underline{\mathbf{v}} + \mathbf{N}''$$

respectively where the power of $\mathrm{P}(\mathbf{N}') << \mathrm{P}(\mathbf{N}'')$.

The main idea in wiretap channel is to minimize the information gained by wiretapper and to maximize the information gained by the legitimate receiver. Based on information theory regarding noise and channel capacity, the legitimate receiver will recover the signal from added channel noise while wiretapper cannot.

Many ideas have been presented in theory based on Wyner's wiretap channel. The proof that wiretapper doesn't get any information from the shared channel is based on a strong assumption that wiretap channel is much noisier than main channel. This assumption is hard to fulfill in all cases which makes it less attractive to secure wireless communications in reality.

5.2.1 Blocker Tag

Juels *et al.* in [29] has proposed a conceptual scheme to protect consumer privacy problem that they called *blocking*. According to this scheme, a consumer has an additional tag that they call a *blocker tag*. Since the passive RFID tag has broadcast embedded in its nature, it will respond to a reader present in its vicinity without the knowledge of tag holder. This scheme has been proposed to prevent this type of unnecessary messaging and scanning. They have exploit the properties of an anti-collision protocol *singulation* which is already present in the RFID system. *Singulation* allows the reader to read many tags simultaneously at a time by first collectively communicating with all present in the vicinity of the system and then communicating with them individually later on.

Tree Walking is a type of *Singulation* protocol used for RFID tags. It is based on the binary tree structure with k depth. The root node is null. The node pointer progresses to its left child if a 0 bit is encountered for the identifier. Conversely, it progresses to the right child if the next bit in the identifier is 1. During simultaneous communication with multiple tags, the pointer can move to both child nodes if a 0 and 1 are encountered at the same time. If m bits of identifier value are sent by the tag, the pointer will traverse to the depth of m bits to identify the tag.

The first bit of the identifier is known as the *protected bit* with the help of which the *blocker tag* performs selective blocking. For example if it is 0, the tag will act normal and

the tree pointer will move to the right half of the root node. Whereas if the first bit is 1, the pointer moves to the right half which is declared as the privacy zone of the tree. Once the tree pointer has entered the privacy zone, the *blocker tag* will start transmitting random bits in pair irrespective of all other tag. The reader will not be able to identify any of the other tags present in its vicinity hence blocking the scanning.

5.2.2 Noisy Tag Protocol

A method for key exchange was proposed by Castelluccia and Avoine in [7] which is a similar idea as the *blocker tag discussed previously*. However, in this case a *noisy tag* is owned by the RFID system. The reader and *noisy tag* have the same pseudorandom generator with pre-shared key. This protocol is carried out in two phases, the *Exchange Phase* and the *Reconciliation Phase*.

Exchange Phase:

1. The reader sends nonce N to the *noisy tag*.
2. The *noisy tag* will generate its own pseudo random sequence using $f(k, N)$ where k is the pre-shared key between noisy tag and the reader and f is the pseudorandom generator function.
3. When the reader initiates the query, the legitimate as well as *noisy tag* will respond by transmitting the numbers generated by their pseudo random generators bit by bit. Since the channel is Additive White Gaussian Noise *AWGN*, bits generated by both tags will be added to one another.
4. If both tag transmit the same bit simultaneously, i.e., 00 or 11, the reader and eavesdropper will receive the same symbol, i.e., S_{00} or S_{11}. If both tags transmit a different bit i.e. S_{01} or S_{10}, the eavesdropper would not be able to distinguish which bit was sent by the *noisy tag*. This is referred to *bit blocking*.
5. Since the reader knows the pseudorandom sequence generated by the *noisy tag*, it will subtract the sequence from the received signal to retrieve the sequence sent by legitimate tag.

Reconciliation Phase:

1. The reader will discard the symbol sequence of the form S_{00} or S_{11} and will send the time instances of other symbols to the legitimate tag.

On average the reader needs $2n$ rounds to exchange the key since there is probability that n round are affected by collision if both tags transmit the same bit. This is known as the same bit problem. Another code based protocol presented in the same paper reduces the number of rounds to n by transmitting multiple bits from both tags to lessen the chances of collision. Based on this idea, Hancke in [26] and [25] proposed a new scheme called *Noisy Carrier Modulation* for key exchange.

5.2.3 Noisy Reader

Savry in [44] proposed a scheme after exploiting that the passive tag can send a reply to the reader on noisy carrier. This scheme involves a separate noise generating device synchronized with the reader. The reader sends an EPC C1 Gen2 command to the tag and triggers the noise generator to send a noisy signal into the channel. The tag replies on the same noisy signal which looks random to the passive eavesdropper. The legitimate reader already knows about the noise generated by the noise generator so it can cancel the effect of noisy signal from the tag's reply. This is called *Cooperative Jamming*.

5.2.4 RFID Guardian

Rieback *et al.* in [43] proposed a conceptual mobile battery powered device for privacy management of RFID systems which they named as *RFID Guardian*. It logs the RFID tags and readers and provides secure communication between the unknown reader and the customer's tag. *RFID Guardian* is owned by the customer and provides access control mechanism which enables the tag to communicate with legitimate readers and restrict the rogue readers.

5.2.5 BUPLE

Chai and Gong in [8] proposed a novel physical layer scheme for securing the low cost tag to reader communication in the presence of passive eavesdropper which they named as BUPLE (*Backscatter modulation- and Un-coordinated frequency hopping-assisted Physical Layer Enhancement*). In this scheme to hide the transmission from the eavesdropper, they used carrier wave amplitude along with periodically hopping frequency to transmit a message. They also used random sequence modulated to carrier's phase to prevent bit modifications. Their scheme provide security against passive eavesdropping and relay attacks.

5.3 Authentication and Distance Checking

The term *Authentication* means that at least one of the parties involved in communication is aware of the identity of the other. If all parties are assured about the identities of each other, then this is known as *Mutual Authentication*.

Distance Checking means that a party ensures the other parties involved in the communication that it is located at a specified distance to them.

All the cryptographic authentication protocols do not guarantee *distance checking* with *authentication*. Many such protocols were subjected to relay attacks [17, 19, 24, 18, 16].

There are two types of relay attacks. *Mafia Fraud Attack* and *Terrorist Fraud Attack*. *Mafia Fraud Attack* is similar to *Man-in-the-middle (MITM)* attack in which adversary tries to relay the communication between two legitimate parties. Desmedt *et al.* first demonstrated the *Mafia Fraud Attack* in [15]. He presented that even if cryptographically strong authentication protocols are not designed carefully, they can fall prey to *mafia fraud attack* based on *grandmaster chess problem* [13]. In the *Terrorist Fraud Attack* the prover is legitimate but dishonest, who with the help of an adversary tries to convince the verifier that he is within the range [2, 30].

There is another type of attack in which the deceitful tag tries to convince the verifier that it is close to it. It is called *Distance Fraud Attack* [30].

5.3.1 Distance Bounding Protocol

The countermeasures of aforementioned attacks were proposed by *Distance Bounding Protocol* [2]. The basic idea of this is based on cryptographic challenge response protocol with strict time constraints on the response time.

Brands and Chaum in [4] designed the first *Distance Bounding Protocol*. The protocol had three phases which work as follows:

Step 1: The verifier and prover generate a random binary sequence $V = v_1, v_2, ..., v_n$ and $P = p_1, p_2, ..., p_n$ respectively.

Step 2: The verifier sends one challenge bit v_i and starts the timer. Immediately, the prover upon receiving this bit replies with p_i which stops the timer at the verifier. The verifier calculates the distance based on the timer value which is the *Round Trip Time (RTT)* for each bit. This step is repeated k times.

Step 3: After n bits have been exchanged, the prover sends the authentication code/digital signature for the two binary sequences V and P.

Steps 1 and *3* are slow phases, whereas *Step 2* is a fast phase of this protocol which is repeated k times.

5.3.2 Hancke and Kuhn's Protocol

Hancke and Kuhn presented the first RFID protocol for distance bounding as shown in Figure 5.2. Their scheme was based on Brands and Chaum's protocol. They proposed in their own protocol that the last step can be omitted when used for RFID systems. Hence it has only two phases described as follows:

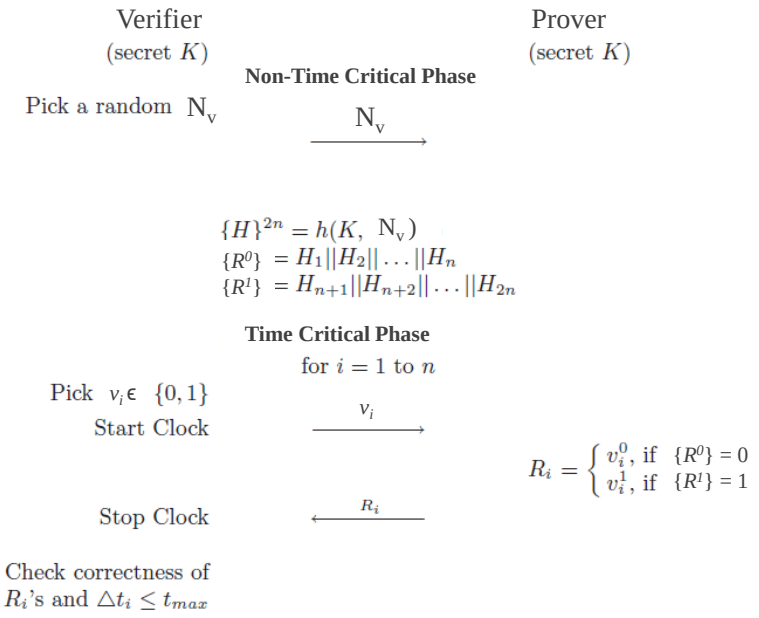


Figure 5.2: Hancke and Kuhn's Protocol

Non-Time Critical:

1. The verifier sends a random number N_v to the prover which is regenerated for each session.

2. The verifier and prover calculate two n-bit binary sequences R^0 and R^1 using the random number N_v, the secret key K and the cryptographic function h

$$R_1^0 R_2^0 ... R_n^0 || R_1^1 R_2^1 ... R_n^1 := h(K, N_v)$$

Time Critical

1. The verifier generates a random binary sequence $V = v_1, v_2, ..., v_n$, then sends one challenge bit v_i to the prover and starts the timer.

2. The prover upon receiving this bit replies with $R_i^{v_i}$ which stops the timer at the verifier. This step is repeated n times.

3. The verifier checks the reply with his computed $R_i^{v_i}$. If the reply matches and is received in sufficiently short period of time, then the verifier accepts the prover as the valid tag.

As there are only two states i.e. **0** or **1** in their protocol in *time critical* phase, an adversary could randomly choose the $v_i' = v_i$ with 0.5 probability of success and store the prover's response. After n rounds he could respond to the verifier with the prover's reply. In this case, adversary has $(\frac{3}{4})^n$ probability of success.

Later Kim and Avoine in [30] presented an enhanced version of Hancke and Kuhn's protocol in which they used multi-state with binary mixed challenges.

Chapter 6

Direct Sequence Backscatter Encryption for Low Cost RFID Systems

In this chapter, we present a new physical layer encryption scheme that we call Direct Sequence Backscatter Encryption (*DSB-Enc*), together with the simulation and experimental implementation for validating the scheme. Section 6.1 presents our system model for a proposed physical layer scheme. In Section 6.2, we discuss the FSM implemented on our tag. Section 6.3 introduces the principle of level generator and the scheme. In Section 6.4, we give the simulation model using GNU Radio and preliminary results of our new physical layer scheme for low cost RFID systems. In Section 6.5, we discuss in detail our experimental setup and its environment. Finally in Section 6.6, we validate our proposed scheme by implementing it on software defined radio and a WISP tag and conclude the chapter by providing the results.

6.1 System Model

We assumed two or more Pseudo Random Sequence (Number) Generators (PRSG) to produce bit streams $\boldsymbol{a_i}$, $\boldsymbol{b_i}$, $\boldsymbol{c_i}$ and so on. This is shown in Figure 6.1. Each bit $\boldsymbol{a_i}$, $\boldsymbol{b_i}$, $\boldsymbol{c_i}$ and so on is assumed to be independent, identical and uniformly distributed. The time samples of binary bits from a PRSG is shown in Figure 6.2.

Further, we also assumed that there is only one legitimate reader $\check{R}$ and one legitimate

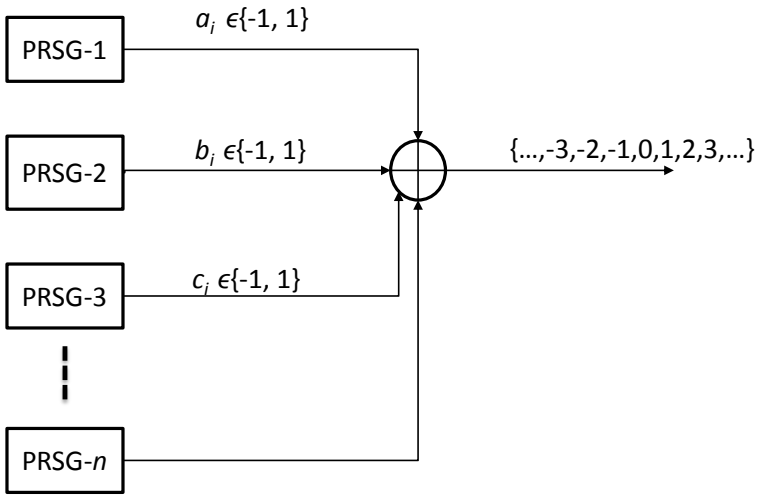


Figure 6.1: Combinatorial generator with n PRSGs

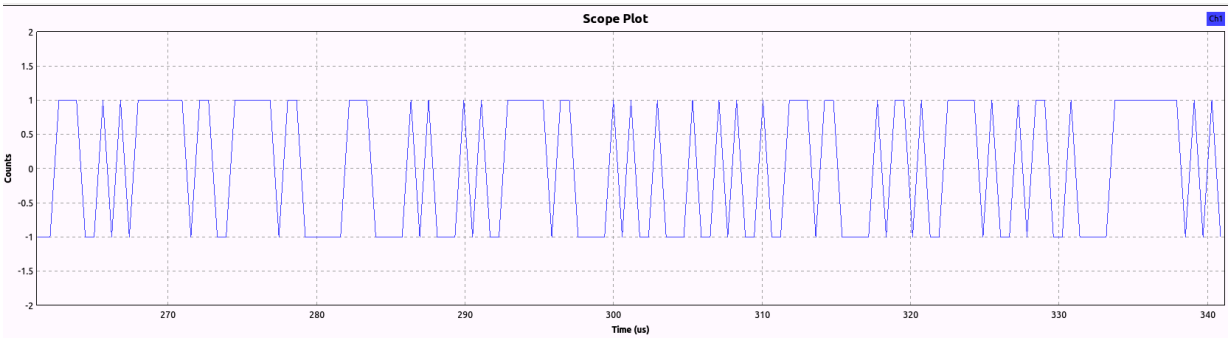


Figure 6.2: Time samples of Binary bits of a PRSG

tag $\check{T}$ in our system. $\check{R}$ and $\check{T}$ do trust each other and are not compromised. Signal collision and interference from simultaneous response produced by multiple tags are not considered in our system. Since our physical layer scheme is independent of upper layer protocols, we intentionally keep the functionally of the reader and the tag as simple as possible. We do not care much about the reader and a tag interaction at the logic layer.

In our system we only care about the physical layer and we intentionally keep the upper layers for $\check{R}$ and $\check{T}$ as simple as possible.

6.2 Finite State Machine for Tag

Tag in our system acts as a *Finite State Machine* (FSM) to transmit data by using backscatter communication. Different states of tag are shown in Figure 6.3.

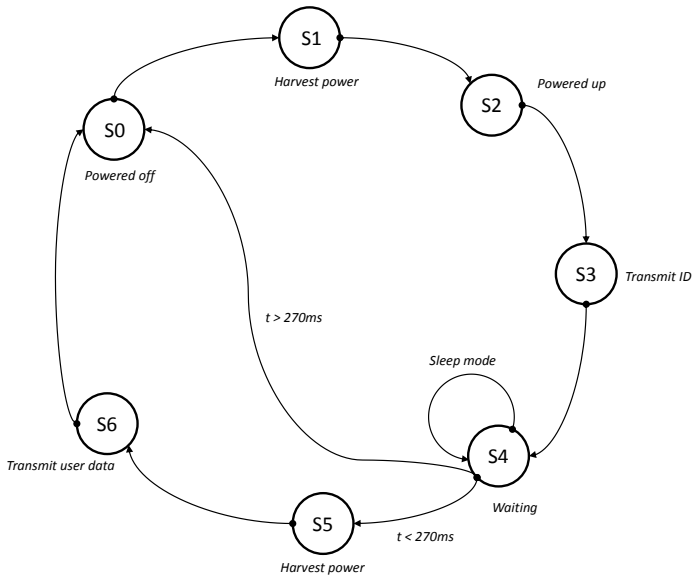


Figure 6.3: Finite State Machine (FSM) for tag

Initially, Tag is in powered off state S0. Reader sends the multilevel continuous carrier wave to tag. Tag harvests the ephemeral energy for computation from the carrier wave in state S1. Once the tag is fully charged (S2) it transmits 16-bit ID number by changing the impedance of an antenna in state S3. After sending the tag's ID it goes in waiting state

S4 in sleep mode. If it receives power while in state S4 it moves to state S5 and gets fully charged and transmits data in state S6 else it goes back to state S0. Finally, after sending data it comes back to its initial state.

6.2.1 Discharging of Passive Tag

We can exactly calculate the waiting time for state S4 for a passive tag. All passive tags harvest energy from the reader carrier wave and store it in a capacitor. We can model a capacitor in an RC circuit and calculate its discharging time after which the tag will discharge and goes back to its initial state.

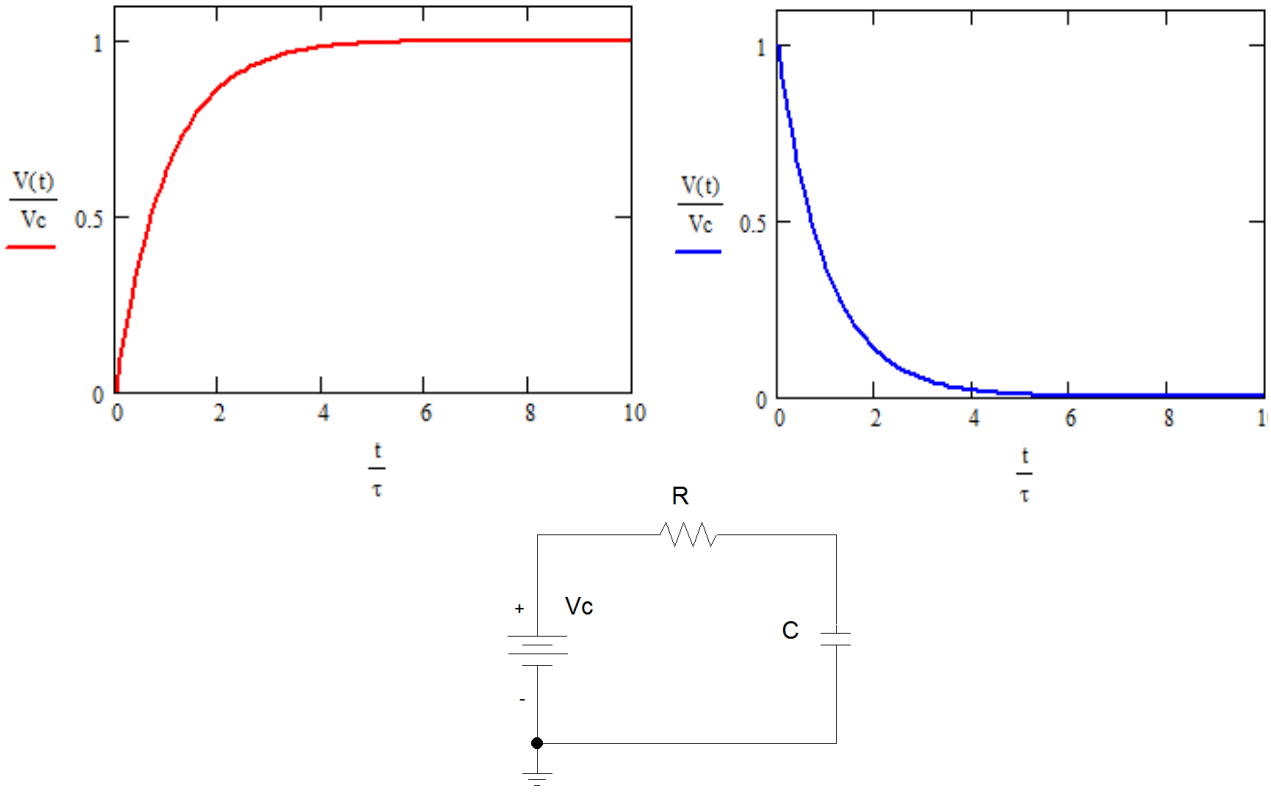


Figure 6.4: Charging and Discharging Phase of Passive Tag's Capacitor

According to circuit theory the charging of a capacitor can be written as

$$V(t) = V_{\circ}(1 - \mathbf{e}^{\frac{-t}{\tau}}) \tag{6.1}$$

and discharging of a capacitor as follows

$$V(t) = V_{\circ}(\mathbf{e}^{\frac{-t}{\tau}}) \tag{6.2}$$

where $\mathbf{e} = 2.71828$, $V_{\circ}$ is the initial voltage stored on a capacitor, t is the discharging time and τ is the time constant which is determined through RC parameters of a circuit. Charging/discharging phases are shown in Figure 6.4.

The Eq. (6.1) and (6.2) show that in charging and discharging phase the voltage across resistor grows and decays exponentially. When $t = \tau$, V(t) falls to $\mathbf{e}^{-1} = 0.368$ of its initial voltage.

We can calculate the discharging time for the passive tag's capacitor from Eq. (6.2) as follow. The resistor and capacitor used in Wireless Identification and Sensing Platform (WISP) 4.1 DL tag is 2.4kΩ and 100μF respectively [61]. The maximum voltage across a capacitor can be 5.5V and the minimum voltage required by the tag to retain its current state is 1.8V, we have t= 1.117τ where $\tau = 0.240$. Therefore, discharging time (t) for a capacitor is $0.240\tau \approx 270$ms [35].

Remark: If the reader does not send carrier signal to the passive tag for >270ms, the tag will go to its initial state otherwise it moves to the next state.

6.3 Direct Sequence Backscatter Encryption

The key component of *DSB Enc* scheme is a level generator. To understand the principle of level generator, we have to review the RFID communications standards. In ISO 14443 HF RFID and EPC UHF C1 Gen2 the reader encodes data using different line codes as mentioned in Section 2.1.4.

Our scheme works in the following way, the reader has been modified for signal generation by using multiple LFSRs which produce different signal levels and each level is encoded using NRZ-L. The encoded signal levels are discrete and are made continuous by adding them to a continuous wave. This will ensure that the tag never runs out of power supply. The resultant wave is modulated on a carrier frequency 902-928 MHz using MPSK as shown in Figure 6.5.

Level generator is implemented by multiple LFSRs, detail in Section 6.4 of this chapter, or other methods, which will be discussed in Section 7.3 in next chapter. Each sub-generator in level generator generators i.i.d random sequences with Gaussian distribution.

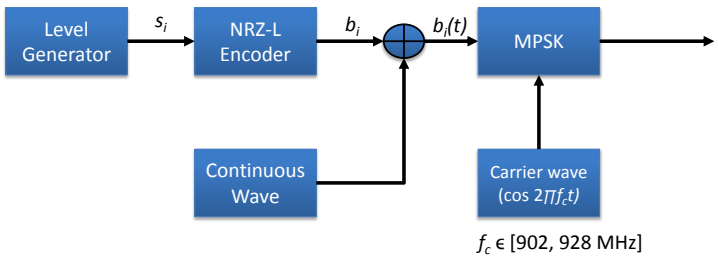


Figure 6.5: Principle of level generator

According to the central limit theorem (CLT) in Section 3.6.3, the sum of these subsequences, which is the output of level generator, is Gaussian. Therefore the transmitted signal becomes Gaussian.

To transmit the message to the reader, the passive tag modulates a resistive or capacitive load at its antenna and adds its response to the carrier signal using BASK or OOK. The resultant is still Gaussian. So if Eve picks the tag's reply, Eve will get a Gaussian signal which is hard to decode without a priori knowledge of the levels generated by the reader. Therefore only the legitimate reader can decode the tag's reply by subtracting the levels at the reader side. Another obstacle for an eavesdropper is the synchronization problem of levels generated at the time of transmission which we will discuss in detail in the next chapter.

Remarks: The goals of the *DSB Enc* is to provide secure physical layer link for tag to reader communications in the presence of a passive eavesdropper and defeat various attacks that exists in RFID systems, e.g., relay attack and replay attacks. This scheme works without requiring any pre-shared credentials by legitimate parties. *DSB-Enc* exploits physical layer resources of passive RFID systems and provides security functions while keeping the hardware cost of the reader and the tag almost unaffected, as required in many RFID applications.

6.4 Simulation Using GNU Radio

In this section, we will presented our simulation model and explain it in detail. We have implemented *DSB Enc* in GNU Radio using GRC *signal flow graph*. The block diagram of a simulation model is shown in Figure 6.6.

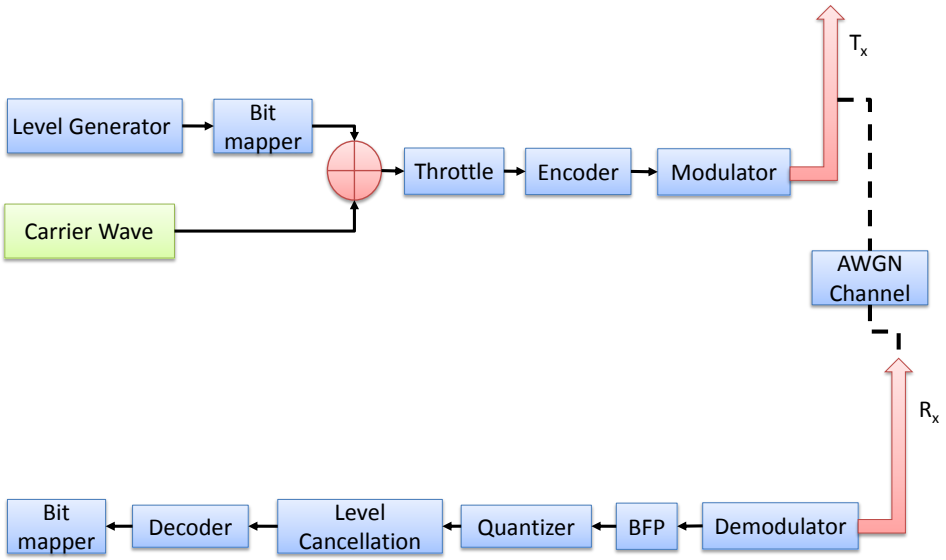


Figure 6.6: Block diagram of simulation model

6.4.1 Design of Level Generator

To produce different levels of amplitudes, we tested our system model with different signal sources. The levels were generated using a Gaussian random signal source. Theoretically, it gives better security in our system but it is over killing for the hardware. We have used LFSR with primitive polynomials to produce different levels. LFSRs are hardware as well as software efficient. The random bits of LFSR are mapped on BPSK and then added together to generate multiple levels. The resultant discrete levels are made continuous using continuous constant wave. This continuous wave gives power supply to the passive tag. To validate our concept of level generator we have built a simulation model using GNU Radio by creating a flow graph.

PRSGs for levels generator are realized using the LFSRs primitive polynomial of degrees 29 and 31 over $\mathbb{F}_2$. The characteristic polynomials of degrees 29 and 31 are given in Eqs. (6.3) and (6.4).

$$LFSR_1 = x^{29} + x^2 + 1 \tag{6.3}$$

$$LFSR_2 = x^{31} + x^3 + 1. \tag{6.4}$$

The primitive polynomials produce maximum length sequences also known as *m-sequences* [20]. The period of $LFSR_1$ and $LFSR_2$ are $2^{29} - 1$ and $2^{31} - 1$ respectively. As these two

primitive polynomials are co-prime and added together, therefore they generate sequence of linear span $LS = 60$[1]. Their respective linear recursive relations of Eqs (6.3) and (6.4) are given by

$$a_{k+29} = a_{k+2} + a_k \tag{6.5}$$

$$a_{k+31} = a_{k+3} + a_k, \quad k = 0, 1, ... \tag{6.6}$$

Table 6.1: Levels generated using two LFSRs

$LFSR_1$	$LFSR_2$	Levels
-1	-1	-2
-1	1	0
1	-1	0
1	1	2

The output bits $\{0, 1\}$ of an LFSR are mapped onto {-1,1}. In the simulation, shown in Section 6.4.1, we used bit rate of 500 kbps for producing LFSR bits in our simulation model and the symbol rate of 32k symbols/sec. Combinatorial generator structure is used to generate different levels. The generated levels from $LFSR_1$ and $LFSR_2$ are shown in Table 6.1

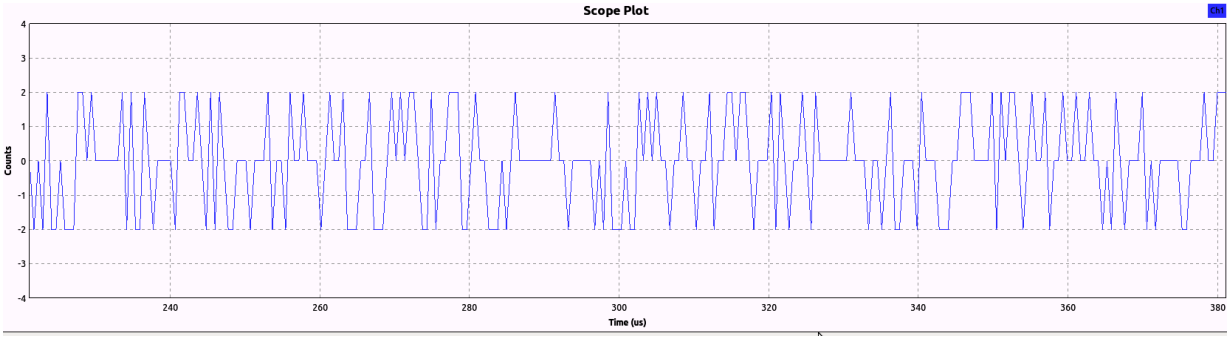


Figure 6.7: Time samples of generated three levels

6.4.2 Continuous Wave

The levels generated using PRSG (LFSR) are symmetric around x-axis which does not supply power to the passive tag due its periodic behavior. From Table 6.1, we can intu-

[1]The m-sequences with period $2^n - 1$ has linear span n

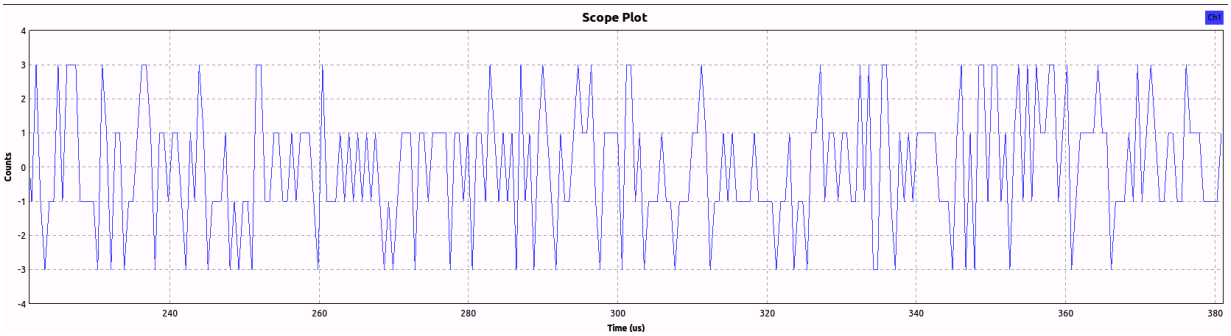


Figure 6.8: Time samples of generated four levels

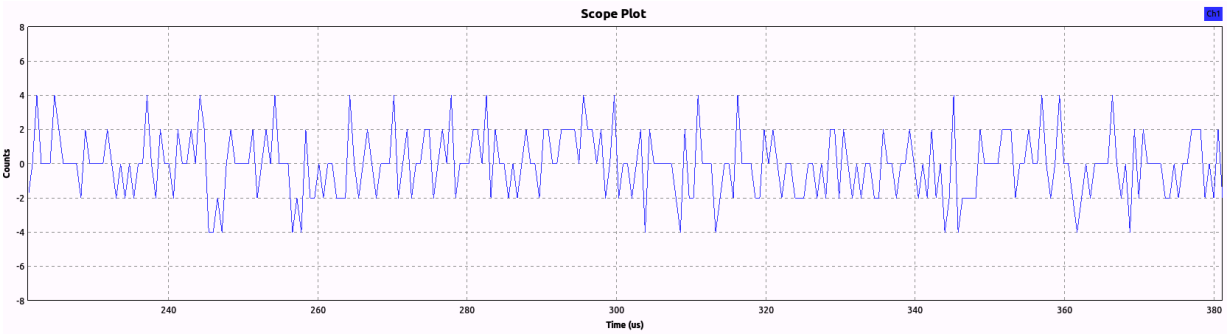


Figure 6.9: Time samples of generated five levels

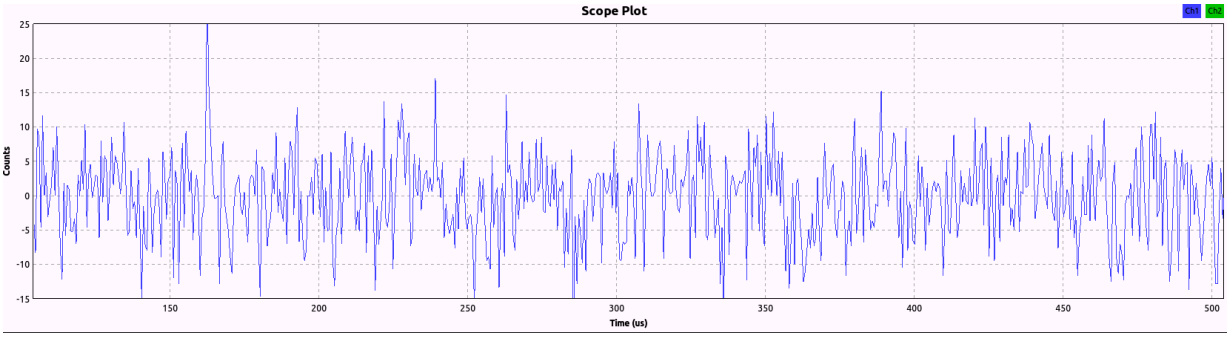


Figure 6.10: Time samples of generated multi-levels

itively say that the average energy of the level sequence is zero. Therefore, we need another method to power up the tag without compromising the properties of our level generator.

Periodic signals are the first choice to solve this problem. An essential class of continu-

ous time periodic signal are the *sinusoids*, which can be expressed in the following general form:

$$x(t) = A\sin(\omega t + \theta) \tag{6.7}$$

where A is an amplitude, ω is an angular frequency and θ is the phase of the signal.

The Average power of a continuous time periodic signal $x(t)$ with period T is given by

$$P = \frac{1}{T}\int_0^T |x(t)|^2\, dt. \tag{6.8}$$

According to Eq (6.8) the average power of a sinusoidal signal given in Eq (6.7) is

$$P = \frac{A^2}{2}. \tag{6.9}$$

By superimposing the generated level with sinusoidal carrier wave, we give sufficient power supply to the passive tag for transmitting random bits and data. The sample rate used for generating sinusoids baseband carrier signal was 100 kHz. To ensure the maximum uncertainty for our system, we have used higher sample rate for baseband carrier than level generated bits.

6.4.3 Throttle

Since we are generating levels, carrier signal and AWGN noise source, all on a same machine there is no threshold for sample rate, therefore we used a throttle block to slow down the sample rate to 100 kHz. This block is essential to keep the simulation model running smoothly and from overwhelming the PC.

6.4.4 Modulation/Demodulation

We modulated our base band signal using a carrier frequency of 2.712 MHz which is a scaled version of HF RFID standard frequency, i.e., 13.56 MHz by a factor 0.2. As modulation frequency does not affect the performance or analysis of our system and due to high data rate produced or processed by the PC, we reduced the modulation carrier frequency in our simulation model.

6.4.5 AWGN Channel

We modelled the channel between the reader and tag as AWGN (*Additive White Gaussian Noise*) channel. AWGN is considered as the best model for analyzing the performance of communication systems. According to central limit theorem the summation of many independent identically distributed random process tend to be close to the normal distribution which is best suited for most of the communication channels due to several noise sources[2].

6.4.6 Quantizer

We made a quantizer block to quantize received signal in the signal flow graph for simulating the real model. The levels generated at the transmission side were discrete. Therefore to cancel those levels from the received signal we quantized the analogue signal to convert it into discrete samples after which the system removed levels that were generated by the system. We quantized the signals using 4 bit to 9 bit quantizers.

6.4.7 Simulation Results and Analysis

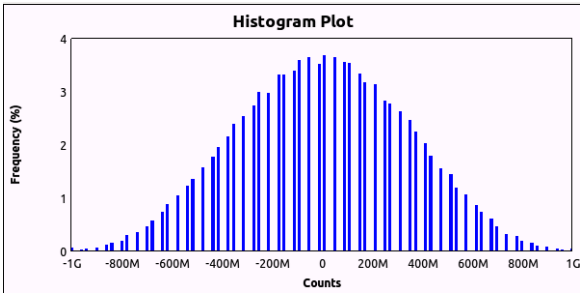
(1) Levels and Data Signal in the Same Frequency Band

Figure 6.11 shows (a) the transmitted signal amplitude distribution and (b) FFT plot of signal at the receiver end, when the levels and data carrier signal are in the same frequency band. The received signal is quantized with 4-bit quantizer and after passing through a level cancellation block we got the transmitted sinusoidal signal back. For our simulations we did not send any data with the signal. Instead of sending **1** and **0**, we sent the sinusoidal signal. Received signal histogram[3] and Fast Fourier Transform is shown in Figure 6.11−(c),(d).

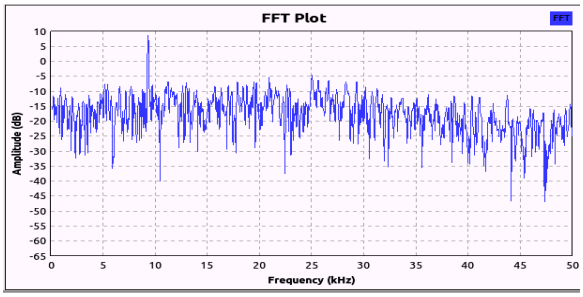
Result 1: From the simulation results shown in Figure 6.11 and 6.12, we have shown that we could recover the signal sent by a tag in the presence of AWGN channel as long as we know the levels of amplitudes added at the time of transmission. We can remove all the levels precisely at the receiver side regardless of the amplitudes of those levels.

[2]For more detail about Central Limit Theorem, reader is directed to [22]

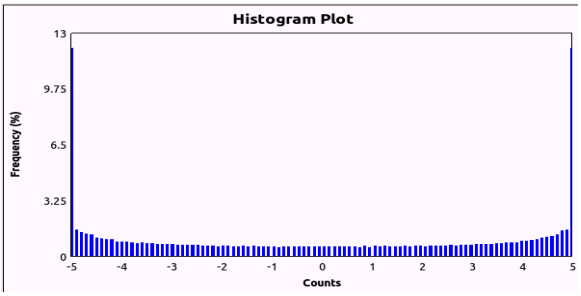
[3]Histogram is a graphical representation of a probability distribution of continuous variable data



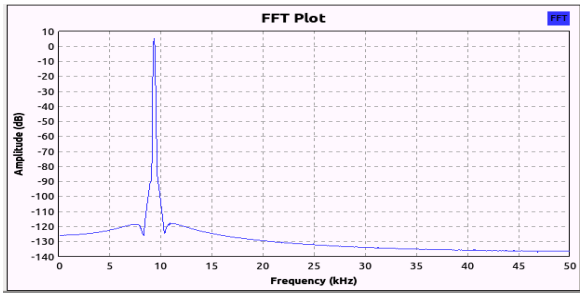
(a) Amplitude distribution of received Signal



(b) FFT of received signal



(c) Amplitude distribution after decoding



(d) FFT of decoded signal

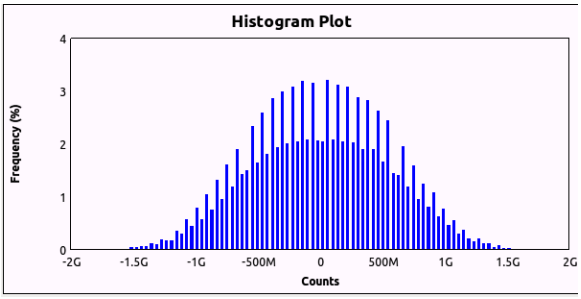
Figure 6.11: (a) Amplitude distribution (b) FFT of the received signal in simulation model (c) Amplitude distribution of decoded signal (d) FFT of the received data after decoding

(2) Levels and Data Signal in Different Frequency Bands

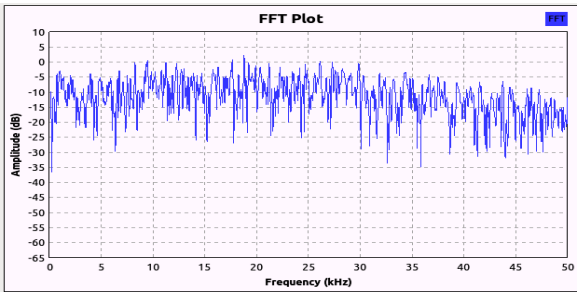
According to *Line Of Sight* (LOS) path loss model for reflected signal propagations, power loss in the free space is inversely proportional to the square of the distance ($\frac{1}{d^2}$) and is independent of the signal wavelength after some critical distance. To increase the distance between reader and tag, the following general methods can be applied.

- We can increase the received signal power by increasing the power of transmitted signal. This is applicable in most cases but involves the threshold for increasing power, i.e., antenna gain and receiver sensitivity.
- To solve the aforementioned problem, MIMO antennas can be used. However, it is an expensive method.

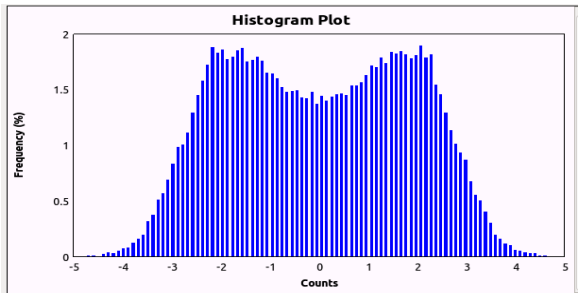
However, in Universal Software Radio Peripheral (USRP), we cannot increase the amplitude of baseband signal more than 1.0 without avoiding the RF clipping/rounding. To



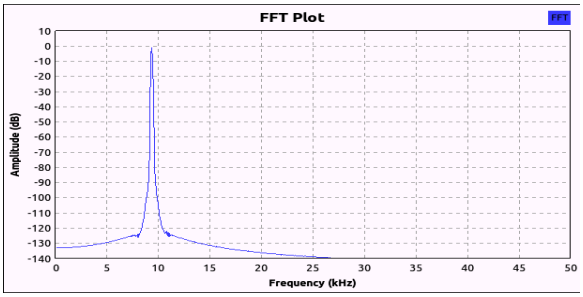
(a) Amplitude distribution of received Signal



(b) FFT of received signal



(c) Amplitude distribution before level cancellation

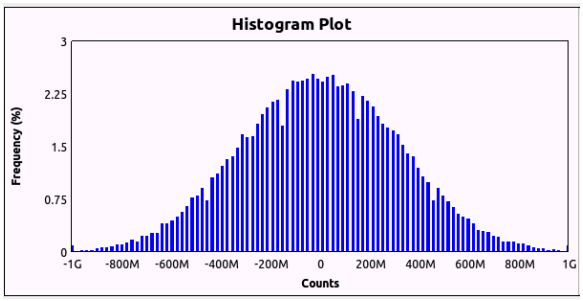


(d) FFT of decoded signal

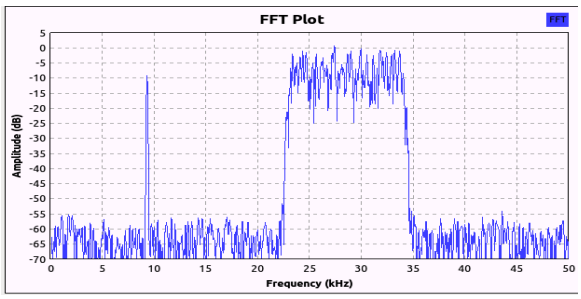
Figure 6.12: Amplitude of added levels are higher than actual data

tackle this problem, we have added the generated levels in the different frequency bands than the original signal. As RFID UHF C1G2 standards have large frequency spectrum ranging from 860-960 MHz [53], we can use the unused spectrum for adding levels of amplitude. The results for simulated model are shown in Figure 6.13.

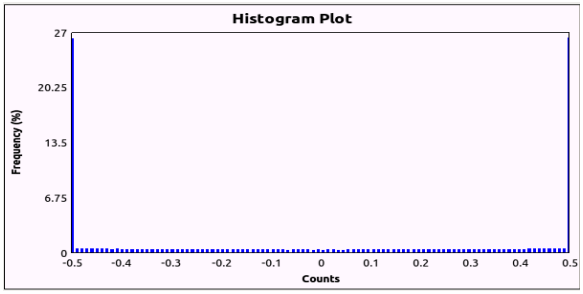
Result 2: From the simulation results, we have shown a method to increase the transmitted signal's power by adding the levels of amplitude and data signal in different frequency bands. This method follows the concept of double sideband large carrier (*DSB-LC*) amplitude modulation. Please note that DSB-LC is different from the Direct Sequence Backscatter (*DSB*) Encryption scheme. As added levels in different frequency band do not carry any information, therefore it a trade off between spectral efficiency and long range.



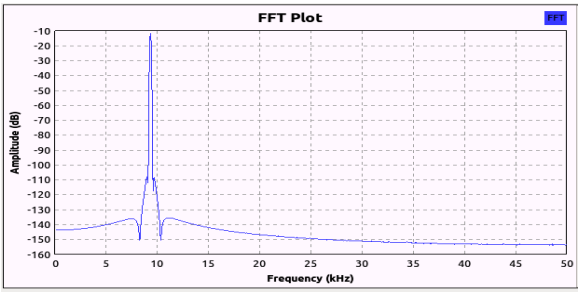
(a) Amplitude distribution of received Signal



(b) FFT of received signal



(c) Amplitude distribution after decoding



(d) FFT of decoded signal

Figure 6.13: (a) Amplitude distribution (b) FFT of the received signal in simulation model (c) Amplitude distribution of decoded signal (d) FFT of the received data after decoding

6.5 Implementation Using SDR

To validate our concept of *DSB Enc* scheme, we developed a prototype system. A system model consists of three parties, one legitimate reader $\check{R}$, one legitimate tag $\check{T}$, and one passive eavesdropper ξ, as shown in Figure 6.14. We are intentionally not sending any data from $\check{R} \rightarrow \check{T}$ to make this system as simple as possible.

6.5.1 Merits of Software Defined Radio

To allow flexibility, the Universal Software Radio Peripheral (USRP) is deployed for programmable RFID reader working at Ultra-High Frequency (UHF) band. USRP equipped with RFX900 *(flex-900)* daughterboard with effective frequency range between 750 - 1050 MHz [54] is used as transceiver which provides inexpensive RF transceiver with open source schematics and drivers for our experimental testbed.

Figure 6.14: System model

6.5.2 RFID Reader

We used an USRP-1 embedded with two RFX900 daughterboards carrying two *Left Hand Circularly Polarized* (LHCP) antennas effective in a range of 902 - 928 MHz [63]. We developed a signal flow graph on GNU Radio Companion[4] to enable this reader to send multilevel amplitude signals and provide sufficient power supply to the passive tag at 915 MHz.

1. In the transmission path, discrete signal levels are generated by GNU Radio and sent to USRP-1 via USB 2.0 [55]. USRP-1 interpolates the baseband signal to the intermediate frequency (IF) band and ultra high frequency(UHF) using digital upconverter (DUC) and finally sent to digital to analogue converter (DAC) and transmitted into the air via RFX900 and its antenna.

2. Similarly in the receiver path, an antenna captures the response signal from the tag and downconvert IF from UHF and further downconvert it to the baseband signal using digital downconverter (DDC) and sends it to GNU Radio running on our PC for further processing. We logged the response of passive tag in a file for decoding and analysis.[5]

[4]GRC is graphical tool for creating signal flow graphs by connecting different processing blocks written in GNU Radio and generates a Python script to create and control signal flow graphs using visual programming language for signal processing via GNU Radio libraries

[5]The decoding algorithm have been developed in MATLAB

The Python scripts *(signal flow graph)* run on Lenovo ThinkCentre M92p with Ubuntu 12.04 and communicates with the USRP-1 using the *USRP Hardware Driver*(UHD) [57] provided by Ettus[6].

6.5.3 Passive RFID Tag

We made use of a passive tag due to its unique properties that are important for our proof-of-concept. We used WISP v4.1 tag [61] to conduct our experiments. Unique features of WISP tag not only include wireless power harvesting, ephemeral energy storage and backscatter radiation but also allow re-programming [6, 48]. It comes with a firmware that supports most of the EPC C1 Gen2 standard protocols but for our experiment we did not use an EPC standard protocol. We re-programmed WISP in C language using IAR embedded workbench v5.40.7 and implemented a *Finite State Machine* (FSM) to transmit the data for tag to reader communications. WISP tag does not actively transmit RF signal instead it backscatters the incident carrier wave from the reader by modulating the impedance of the antenna. We initially sent 16-bit ID of the tag and demodulated it using the *DSB Enc* scheme as describe previously in the chapter.

6.5.4 Experimental Environment

We conducted all our experiments in an office environment to test proof-of-concept in real world settings. The multi-path effects and interference from nearby RF devices made it worst case scenario in possible real world problem test settings.

6.6 Experimental Results

In this section we present the experimental results of our proposed scheme.

6.6.1 Reader to Tag communication

During testing, we used UHF band frequency (915 MHz) for reader to tag communication.

[6]UHD is a hardware host driver and API for Ettus Research products i.e. all USRP devices, compatible with Linux, Windows and Mac. Users are able to use UHD driver standalone or with third party applications such as GNU Radio, Simulink, OpenBTS, Iris and LabVIEW

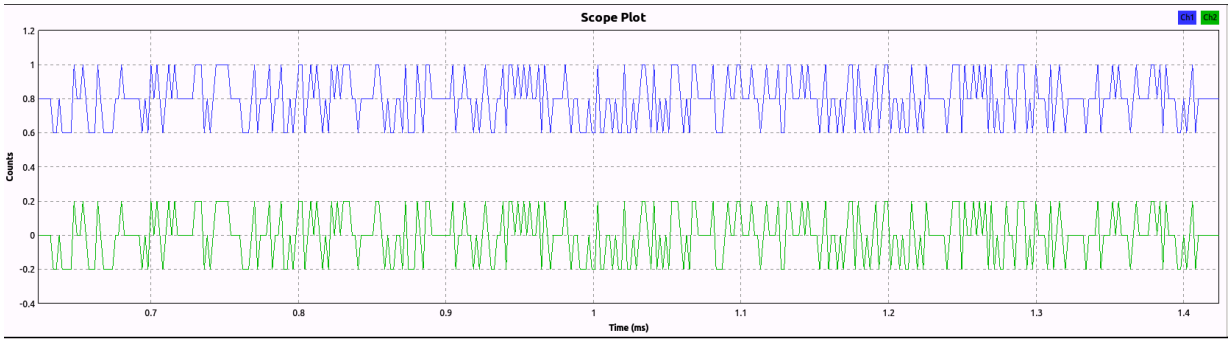


Figure 6.15: Complex time samples of levels generated and added constant continuous wave

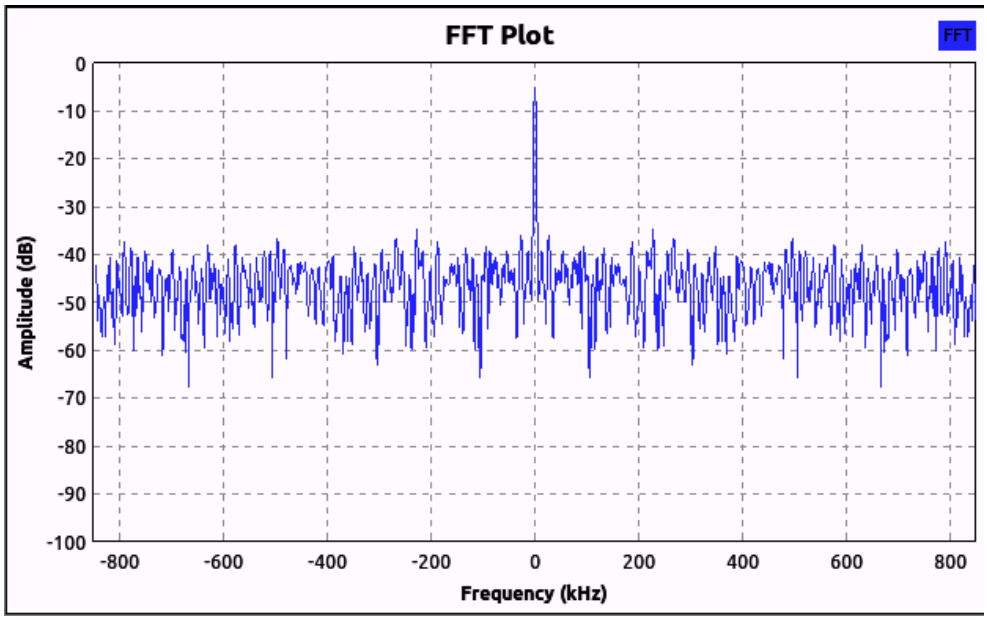


Figure 6.16: FFT plot of the transmitted signal by Reader

Figure 6.15 shows the output discrete signal levels of level generator in time domain. The amplitude scaling factor of generated levels were kept 0.1 *ampl*. FFT plot of the transmitted signal is shown in Figure 6.16.

Figure 6.17 shows the distribution of generated levels before transmission. Antenna gain of transmitter was 45 dB because we wanted to send a strong signal for testing. The generated signal is added to carrier whose amplitude was scaled to a factor of 0.8 *ampl*. The

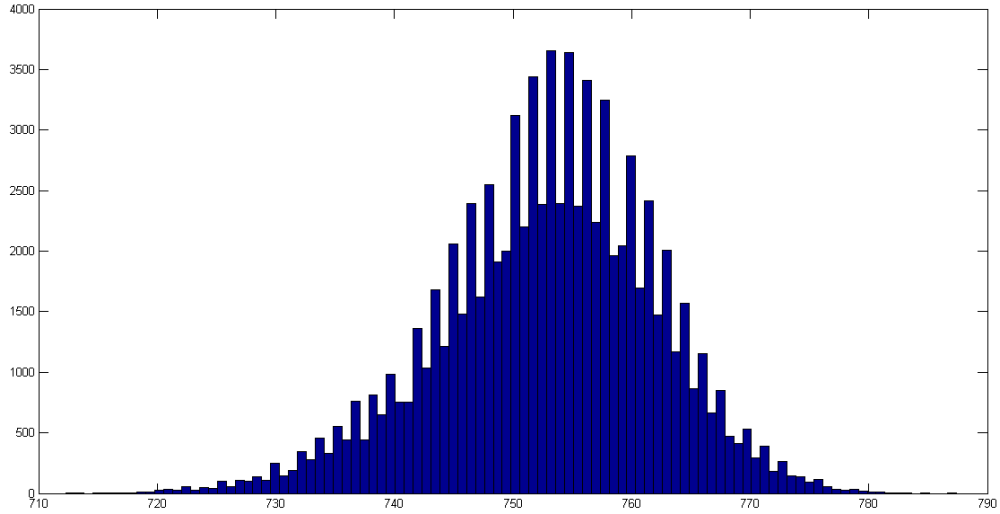


Figure 6.17: Amplitude distribution plot of received signal

overall signal amplitude was 0.9 *ampl*. It is scaled to this value to keep it lower than 1.0 in order to avoid clipping/rounding (we have tested this for different baseband amplitude levels of both carrier wave and level generator)[7]. The distance between the reader and tag was kept to be 1.5 meters.

6.6.2 Channel Response

The channel and tag's response is shown in Figure 6.18. The Figure 6.17 shows amplitude distribution of the received signals. The distribution follows Gaussian distribution. The unique property of Gaussian distribution is that adding and subtractive values to it does not affect the Gaussian distribution which hides the information about the bits that are being sent by the tag to reader communications. The communications from tag to reader were logged in a file for decoding and further processing.

[7]The *amplitude* parameter set above 1.0 in USRP is invalid and will cause clipping/rounding in the digital domain

6.6.3 Tag to Reader communication

The receiver's antenna gain for experiments was kept 20 dB to receive clean response from the tag. Figure 6.18 shows that the resultant received signal is a superposition of the varying amplitude levels generated carrier wave and the tag response[8]. As legitimate reader $\check{R}$ has the knowledge of multi levels that have been incorporated in the transmitted CW, they would be removed first and then decoded. The decoded signals of the tag is shown in Figure 6.19. The Tag decoded ID is shown in Figure 6.20. The high amplitude signal represents **1** and low amplitude signal represents **0**.

[8]For standard UHF RFID message exchange see Figure 2.6 in Section 2.1.4.

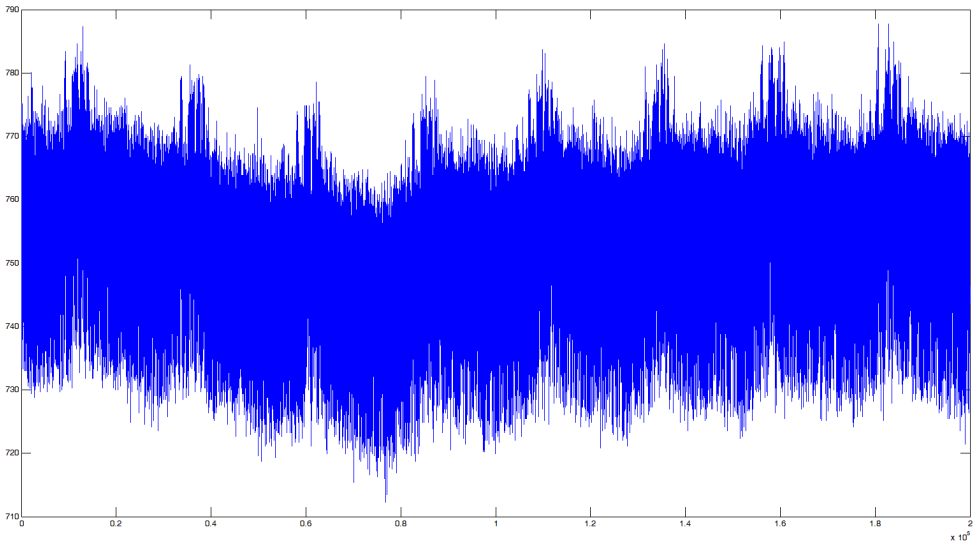


Figure 6.18: Tag's response at the receiver side

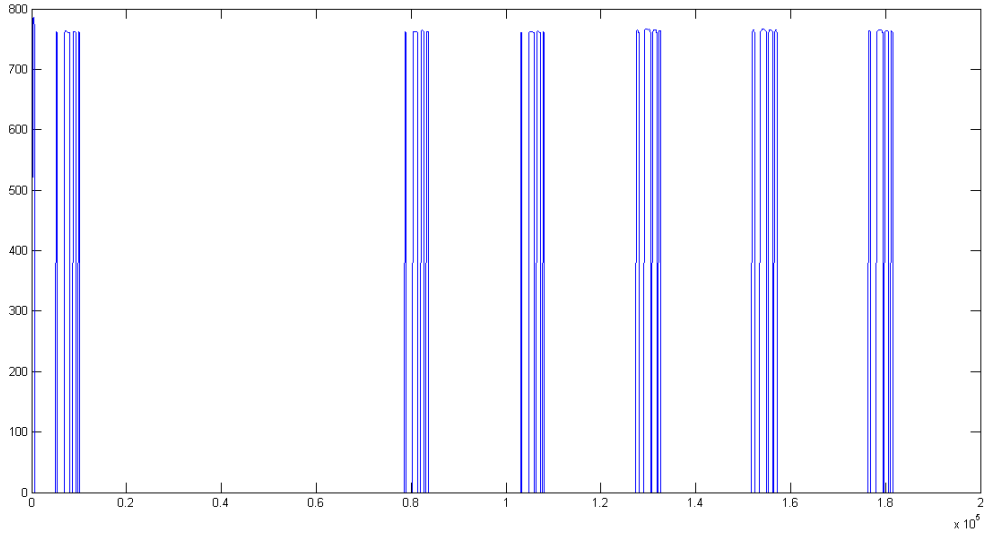


Figure 6.19: Tag's decoded messages

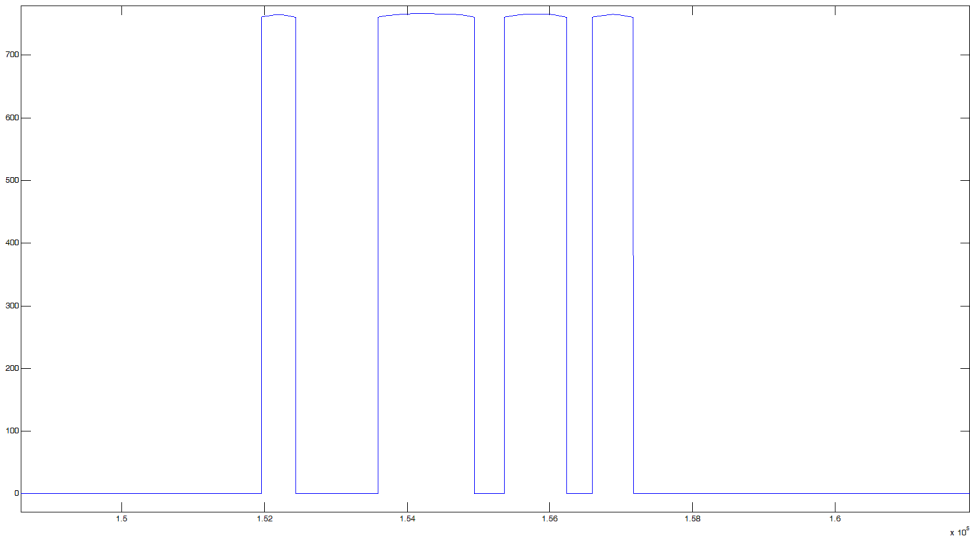


Figure 6.20: 14-bit Tag's ID. The high amplitude signal represents **1** and low amplitude signal represents **0**

Chapter 7

Security Analysis and Robustness Against Existing Attacks

In this chapter, we give a thorough security analysis for *DSB Enc* scheme. Section 7.1 defines the adversary model for our system. In Section 7.3, we present an implementation of level generator for generating multiple levels using LFSRs and NLFSRs and also provide a thorough security analysis for level generator. In Section 7.4 and 7.5, we provide two different methods of generating multi-levels using extension filed $GF(2^p)$ and and a feedback shift register. In Section 7.7, we provide a thorough cryptographic security analysis for *DSB Enc* scheme. We will also analyse the robustness of proposed scheme from different existing attacks and measures to prevent them.

7.1 Adversary Model

We assumed that the eavesdropper can listen to all the communications between the reader Ř and tag Ť. Eve has the knowledge of the channel and the carrier frequency and can acquire/intercept the transmitted data from tag to reader communication using passive eavesdropping. We do not consider active eavesdropper in our system who can either inject/modify messages in the channel or can jam the communications. The goal of a passive eavesdropper in our system is to acquire/intercept the messages transmitted from tag to reader and try to demodulate and decode them. He can move around or stay steady if he wants to. He can also exploit the level generator used in our system. We assume only one attacker in the system.

7.2 Security Model

We assume that the reader and tag are legitimate and are not compromised. Since Adversary Á can acquire/intercept the communication from tag to reader, we assume carrier frequency is known to the attacker. Therefore security of the system lies in the baseband signal. The security of our system is independent of the modulating carrier frequency, i.e., LF, HF and UHF. Á can control the communications which makes him capable of doing the following actions:

- **Passive Eavesdropping:** Á intercepts tag to reader signals, demodulates and decode to get transmitted messages.
- **Active Eavesdropping:** Á actively sends strong signal towards the tag and get the information as discussed in [10]. We implemented spectrum sensing in the reader so it can detect the presence of active eavesdropper in the system. This attack violates our assumptions made to *DSB-Enc* thus is not considered here.
- **Replay Attack:** Á listen to the communication between reader and the tag for many sessions. Later replay the previously collected data to the legitimate reader to breach the security of the system.
- **Relay Attack:** In relay attack an Á places an active relaying devices in between a reader and a tag, which generates new signals to answer the Ř according to the format of backscatter modulation after querying the Ť.
- **Brute force Attack:** Á searches for the required key by looking through a whole search space.

7.3 Level Generators implemented by LFSRs and NLFSRs

In this section, we will do the security analysis of the LFSRs used in *DSB Enc* for generating levels. We have consider that the attacker know the system's structure and the only thing that he does not know is the initial seeds (keys) of the LFSRs and the frequency at the particular time that has been used to communicate because we used frequency hopping to transmit the levels of amplitudes. In our system, we are updating the seeds (keys) and changing the carrier's frequency after every session.

For the proof-of-concept, we have used two LFSRs, i.e., $LFSR_1$ and $LFSR_2$ with primitive polynomials of degrees 29 and 31 respectively. We simulated our system model using many LFSRs in combinatorial generator fashion.

7.3.1 Combinatorial Generator using Multiple LFSRs

Period of Generated Sequence: Pseudorandom sequence generators (PRSG) are not truly random number generators. They generate random numbers based on deterministic algorithms. Their security lies in the repetition of the sequences they produce. Linear feedback shift registers ($LFSRs$) based on primitive polynomials of degree n produce long sequences of period 2^n-1. In our system, we had produced sequences from a combinatorial generator from $LFSR_1$ and $LFSR_2$ [20]. The produced sequence has a period of $(2^{29}-1)(2^{31}-1)$ which will repeat after $\approx$ 4633 years if clocked at 8 Mhz (USB 2.0 bus speed used in USRP-1). Based on our requirements for RFID communication, this sequence is long enough to secure all the communications without repeating.

Linear Span Attack: If we consider that Eve knows some information about the key streams bits k_i of the system. He can create a system of linear equations of multi-variables and try to solve a set of equations to get the initial seed (key)[1] of the system. The uncertainty or entropy of LFSRs used in the system is measured in term of numbers of bits of key κ in the internal stages of LFSRs. In level generator the total number of internal states are 60-bits. The internal stage of the system can be written in an algebraic form:

$$a_n = a_0 + f(a_1, a_2, a_3, ..., a_{n-1}) \tag{7.1}$$

where a_n is the feedback bit and f is the linear function. Higher degree polynomials are secure from linear span attack on LFSR.

Berlekamp Massey Algorithm: To find the short LFSR to produce the same sequence, an attacker needs twice the length of the key stream bits to launch Berlekamp Massey Algorithm [11]. In LFSR based level generator, attacker needs 120 consecutive bits to launch an attack.

Brute force Attack: In the worse case scenario, the time complexity of exhaustive search is 2^{60} and average time complexity is 2^{30} which can be considered secure for low cost RFID systems.

[1]According to Kerckhoffs' principle, the security of the system depends only on the secrecy of the key κ

Conclusion

- ***Advantages:*** LFSRs are efficient to implement in hardware as well as software. They can generate guaranteed maximum large sequences.
- ***Disadvantages:*** Since Linear Feedback Shift Registers are not very secure against different cryptanalytic attacks, hence we can use Non-Linear feedback Shift Registers for pseudorandom sequence generators with proven security against cryptanalytic attacks.

7.3.2 Nonlinear Feedback Shift Register (NLFSR)

NLFSR generators do not exhibit the same randomness properties as LFSRs do. Thanks to span n sequences generated from NLFSR. They have known randomness properties, i.e., maximum period $2^n - 1$, balanced sequence, ideal n-tuple distribution and have large linear span [37].

7.3.3 Span n Sequences Generated from NLFSR

In this section we present two different span n sequences which can be used to produce levels of amplitude. Furthermore, we analyse the span n sequences structure for security analysis. The following two span n sequences are discovered in [36, 37]

Span n sequences of stage $n = 20$: Span n sequences generated from NLFSR of degree 20 has a *period* of $2^{20} - 1$ and a *linear span* of $2^{20} - 2$. The recurrence relation of span n sequences of stage $n = 20$ is

$$a_{n+k} = a_k + WG(X_k^d), k \geq 0 \tag{7.2}$$

where n is the number of stages, WG is the WG transformation and d is the decimation of the sequence. The WG transformation as follows

$$WG(X_k^d) = f(x_{r_1}, x_{r_2}, x_{r_3}, x_{r_4}, x_{r_5}) \tag{7.3}$$

where r_1, r_2, r_3, r_4, r_5 are the tap positions and $(x_0, ..., x_{n-1})$ are variables for NLFSR.

For a span n sequence of stage $n = 20$ for nonlinear WG transformation with $d = 1$ and the tap positions are (5,10,12,18,19). The WG transformation is given by

$$\begin{aligned} f(x_5, x_{10}, x_{12}, x_{18}, x_{19}) = {} & x_5 + x_{18} + x_5x_{10} + x_5x_{12} + \\ & x_5x_{18} + x_5x_{19} + x_{10}x_{12} + x_{10}x_{18} + x_{10}x_{19} + x_{12}x_{19} + \\ & x_5x_{10}x_{18} + x_5x_{10}x_{19} + x_5x_{12}x_{18} + x_5x_{18}x_{19} + x_{10}x_{12}x_{19} \end{aligned} \tag{7.4}$$

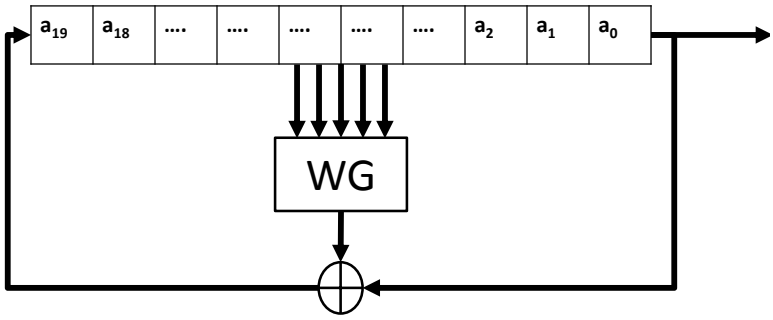


Figure 7.1: The block diagram of span n sequence from NLFSR of degree 20

By using Eq. (7.2) and (7.3)

$$a_{20+k} = a_k + f(a_{k+5}, a_{k+10}, a_{k+12}, a_{k+18}, a_{k+19}) \tag{7.5}$$

A Block diagram of span n sequence from NLFSR of degree 20 is shown in Figure 7.1.

Span n sequences of stage $n = 23$: The second NLFSR used in level generator for producing PSRG is Span n sequence generated from NLFSR of degree 23 having a *period* of $2^{23} - 1$ and a *linear span* of $2^{23} - 2$. The recurrence relation of span n sequences of stage $n = 23$ is given by [36]

$$a_{n+k} = a_k + WG_1(X_k^d) + WG_2(Y_k^d), k \geq 0 \tag{7.6}$$

where n is the number of stages, both WG_1 and WG_2 are WG transformations and d is the decimation of the sequence, given by (7.3).

For span n sequence of stage $n = 23$, WG_1 and WG_2 are given by

$$\begin{aligned} WG_1(x_{22}, x_{21}, x_{20}, x_{19}, x_{16}) = x_{22} + x_{21} + x_{20} + x_{19} + x_{16} + \\ x_{21}x_{20} + x_{21}x_{19} + x_{20}x_{16} \end{aligned} \tag{7.7}$$

$$\begin{aligned} WG_2(x_{15}, x_{11}, x_9, x_7, x_3) = x_{15} + x_7 + x_{15}x_{11} + x_{15}x_9 + \\ x_{15}x_7 + x_{15}x_3 + x_{11}x_7 + x_{11}x_3 + x_9x_7 + x_{15}x_{11}x_3 + \\ x_{15}x_9x_7 + x_{15}x_7x_3 + x_{11}x_9x_7 + x_{11}x_9x_3 + \\ x_{11}x_7x_3 + x_9x_7x_3 + x_{11}x_9x_7x_3 \end{aligned} \tag{7.8}$$

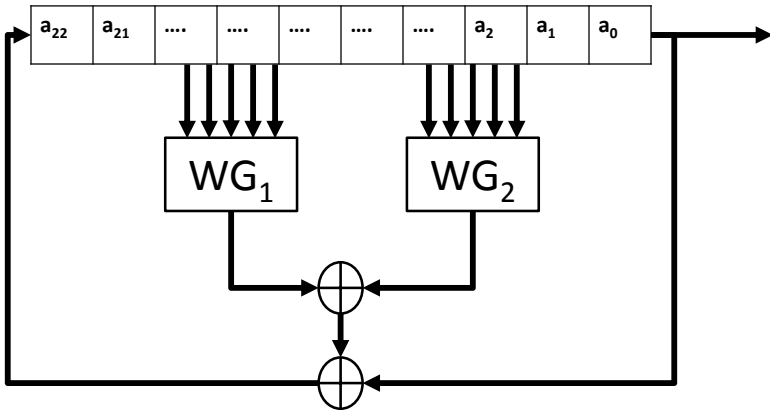


Figure 7.2: The block diagram of span n sequence from NLFSR of degree 23

where WG_1 corresponds d=15 and tap positions (16,19,20,21,22) and WG_2, d= 11 and tap positions (3,7,9,11,15). A Block diagram of span n sequence from NLFSR of degree 23 is shown in Figure 7.2. For details of span n sequences generated by WG transformations, see [37].

Security Analysis of NLFSRs: Replacing both the LFSRs in the level generator with aforementioned NLFSR in this section. We can generate the same levels with much better security. NLFSRs are more resistant to different types of attacks to which LFSRs are prone to.

Brute Force Attack: The time complexity of exhaustive search for the span n sequences generated from NLFSRs of degree 20 and 23 is 2^{43}.

Berlekamp Massey Algorithm: In NLFSRs based level generator an attacker need $2^{24.17}$ consecutive bits to launch an attack.

Algebraic Attack: The algebraic immunity of NLFSR span n sequences are very large. So they are immune to most of the known algebraic attacks.

7.3.4 Security Analysis of Level Generator using (N)LFSRs

Because of using decimal addition operator for combining the bits produced in level generator from each PRSG to create different levels of amplitudes, the fundamental property

of PRSG is destroyed. Bits produced from each LFSRs were independent and identically distributed random values but the generated levels are not equally distributed throughout the sequence.

Example

Table 7.1: Levels generated using 2-PRSGs

$PRSG_1$	$PRSG_2$	Levels
-1	-1	-2
-1	1	0
1	-1	0
1	1	2

Table 7.2: Levels generated using 3-PRSGs

$PRSG_1$	$PRSG_2$	$PRSG_3$	Levels
-1	-1	-1	-3
-1	-1	1	-1
-1	1	-1	-1
-1	1	1	1
1	-1	-1	-1
1	-1	1	1
1	1	-1	1
1	1	1	3

We can calculate the probabilities of each levels produced through multiple PRSGs given in Table 7.1, 7.2 and 7.3.

From Table 7.1, {-2,0,2} has probability distribution of $\{\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\}$. Similarly from Table 7.2 and 7.3, {-3,-1,1,3} and {-4,-2,0,2,4} has the probability distribution of $\{\frac{1}{8}, \frac{3}{8}, \frac{3}{8}, \frac{1}{8}\}$ and $\{\frac{1}{16}, \frac{4}{16}, \frac{6}{16}, \frac{4}{16}, \frac{1}{16}\}$ respectively.

Conclusion: An attacker can exploit this discrepancy to retrieve the information sent between $\check{\text{R}}$ and $\check{\text{T}}$. Though attacker still needs to overcome the synchronization problem to cancel the levels from the received signal.

Table 7.3: Levels generated using 4-PRSGs

$PRSG_1$	$PRSG_2$	$PRSG_3$	$PRSG_4$	Levels
-1	-1	-1	-1	-4
-1	-1	-1	1	-2
-1	-1	1	-1	-2
-1	-1	1	1	0
-1	1	-1	-1	-2
-1	1	-1	1	0
-1	1	1	-1	0
-1	1	1	1	2
1	-1	-1	-1	-2
1	-1	-1	1	0
1	-1	1	-1	0
1	-1	1	1	2
1	1	-1	-1	0
1	1	-1	1	2
1	1	1	-1	2
1	1	1	1	4

7.4 Level Generation Using Extension Field $GF(2^p)$

To secure the information sent in the channel, we need to generate multi-levels which are independent and identically distributed random variables.

We can produce the multi-levels using LFSR over the Extension Field $GF(2^p)$, p $\geq$ 2. The number levels produces are equal to 2^p. To demonstrate the feasibility of using LFSR over $GF(2^3)$, we present the simple structure of level generator over extension field.

7.4.1 LFSR over $GF(2^3)$

Let $GF(2^3)$ be defined by a primitive polynomial

$$f(x) = x^3 + x + 1 \quad over \quad \mathbb{F}_{2^3} \tag{7.9}$$

and let α be the root of $f(x)$. A feedback function of a 11- stage LFSR is given by

$$f(x) = x^{11} + \alpha x^{10} + x^8 + x^7 + x^6 + (\alpha^2 + 1)x^5 + x^4 + x^3 + \alpha^2 x + \alpha \tag{7.10}$$

Recurrence relation of Eq. (7.10) is given by

$$a_{k+11} = \alpha a_{k+10} + a_{k+8} + a_{k+7} + a_{k+6} + (\alpha^2 + 1)a_{k+5} + a_{k+4} + a_{k+3} + \alpha^2 a_{k+1} + \alpha a_k$$
$$k = 0, 1, ...$$

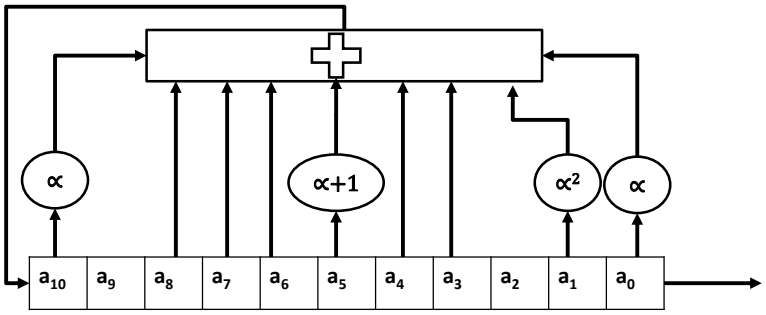


Figure 7.3: The block diagram of an 11-stage LFSR over $\mathbb{F}_{2^3}$

7.4.2 Security Analysis

- *Period* of the generated sequences of 11- stage LFSR over $\mathbb{F}_{2^3}$ is $2^{33} - 1$.
- *Linear Complexity* is 11.
- *Number of levels* generated are 8.

Conclusion: The levels of amplitude generated using extension field are independent and identically distributed random values but performing operations over extension field is expensive and slow.

7.5 Multilevel of Amplitude using FSRs

In this section we propose another method of producing levels in level generator using FSR(linear/non-linear) over $GF(2)$. The hardware efficient structure of producing independent and identically distributed levels through PRSG using single FSR with a buffer is shown in Figure 7.4 which can be extended to multiple LFSRs or NLSFR for better security.

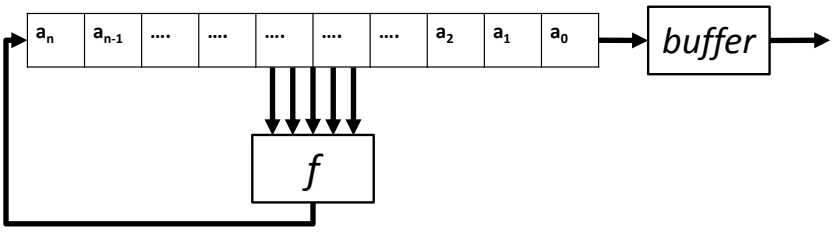


Figure 7.4: The block diagram of i.i.d level generator using FSR

7.5.1 Encoder

The 2-bit buffer can produce 4 i.i.d levels.

Table 7.4: Encoding of 2 bits

a_1	a_0	r	$f(r) = 2r - 3$
0	0	0	-3
0	1	1	-1
1	0	2	1
1	1	3	3

$$r(a_1, a_0) = 2.a_1 + a_0 \tag{7.11}$$

The probability distribution of levels is uniform. 2-bit buffer generate each level with a probability of $\{\frac{1}{4}\}$. Similarly, the 3-bit buffer produce 8 i.i.d levels. In general, for an n-stage FSR

$$r = \sum_{i=0}^{n-1} 2^i a_i \tag{7.12}$$

and the number of levels generated by FSR is given by

$$\text{number of levels} = 2^n \tag{7.13}$$

where n is the size of buffer in bits. A general encoding rule is given by

$$E(a_{n-1}...a_0) = 2r - (2^n - 1) \tag{7.14}$$

Table 7.5: Encoding of 3 bits

a_2	a_1	a_0	r	$f(r) = 2r - 7$
0	0	0	0	-7
0	0	1	1	-5
0	1	0	2	-3
0	1	1	3	-1
1	0	0	4	1
1	0	1	5	3
1	1	0	6	5
1	1	1	7	7

7.5.2 Decoder

Decoding of 4-levels is given by

$$r = \frac{f(r) + 3}{2} \tag{7.15}$$

Table 7.6: Decoding of 3 bits

Received Levels	r
-3	0
-1	1
1	2
3	3

A general decoding rule is given by

$$r = \frac{f(r) + (2^n - 1)}{2} \tag{7.16}$$

7.5.3 Security Analysis

- *Balanced Sequence*
- *Probability of each level*

  The levels produced though this method are uniformly distributed. The probability of each level is given by $\frac{1}{2^n}$.

Size of Buffer	*Number of* **1***'s*	*Number of* **0***'s*
$1-bit$	2^{n-1}	$2^{n-1}-1$
$2-bit$	2^{n-2}	$2^{n-2}-1$
$3-bit$	2^{n-3}	$2^{n-3}-1$
$x-bit$	2^{n-x}	$2^{n-x}-1$

- *Period*

  Period of generated level sequence is same as generating FSR.

Conclusion: The uniform multilevel generator using FSR are hardware efficient and low cost method to securely generate and transmit different level. The single FSR in the aforementioned method can be replaced with the NLFSRs described previously in this chapter. The general encoding and decoding rule presented in multilevel of amplitude using FSM could be used for uniformly distributing the levels produced using combinatorial structure of (N)LFSRs as shown in Table 7.1 and 7.2 by replacing the decimal addition operator with a n-bit buffer.

7.6 Mutual Authentication

For mutual authentication and data transmission between both legitimate parties, *DSB Enc* could be employed in two different ways.

- **EPC C1 Gen2 standard:** The overall communication is accomplished in two phases. In phase 1, the reader to tag communication follows EPC C1 Gen2 standard and sends query command without adding any levels of amplitudes to the carrier wave. Then, instead of sending the continuous wave followed by the reader command, the reader would add multiple levels to the carrier based on *DSB Enc*. In phase 2, the tag will decode the reader's command by again following the EPC C1 Gen2 standard but replies on *DSB Enc* scheme. The reader will decode tag's response using same *DSB Enc* scheme. No additional cost is required at reader's or tag's side.
- **Non-standard data transmission:** *DSB Enc* is used for secure reader to tag and tag to reader communication. A pre-shared master key or seed is required at both sides of the system for establishing a secure communication channel. Depending on

the tag's computational capability, the *DSB Enc* could be implemented on tag's side by using different level generation schemes that have been proposed previously in this chapter to interpret the reader's data. However to generate multiple levels for tag to reader communication and the tag requires additional hardware to support *DSB Enc*.

7.6.1 Trade-off between Low Cost and High Security

All methods and techniques described in this chapter are focused on low cost and efficient hardware as well as software implementation. For higher security, FSR for producing multilevel amplitudes can be replaced with stream cipher and block cipher in counter mode, i.e., 128-bit AES or Blum Blum Shub (BBS) [11].

7.7 Robustness Against Different Attacks

In this section, we will show the robustness of *DSB Enc* scheme against different attacks on RFID systems.

7.7.1 Test of Passive Eavesdropping

We transmitted the data from $\check{\mathrm{T}}$ to $\check{\mathrm{R}}$ in the presence of passive eavesdropper and tried to retrieve the UID sent by the $\check{\mathrm{T}}$. We considered two sceneries for the passive eavesdropping attack shown in Figure 7.5.

(a) When Eve ξ is near the $\check{\mathrm{R}}$ (b) When Eve ξ is near the $\check{\mathrm{T}}$

Figure 7.5: Passive Eavesdropping

Passive Receiver: We used an USRP N210 embedded with an RFX900 daughterboard carrying a *VERT900* vertical antenna effective in a range of 824 - 960 MHz [58]. We developed a signal flow graph on GNU Radio Companion to enable this receiver to passively receive the information at 915 MHz from the channel without being detected by the system. Furthermore, passive receiver É is connected to a Sony Vaio VPCEB33FD laptop using with UHD driver.

Scenario-I: In first scenario, we received the signal sent from the Ť to the Ř by placing passive eavesdropper É near the Ř.

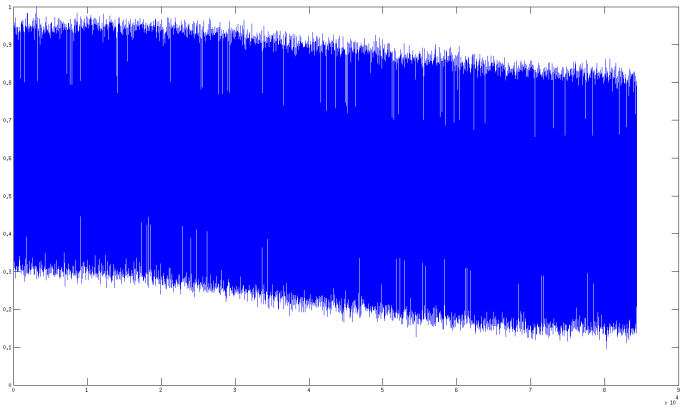


Figure 7.6: Signal received by passive eavesdropper in scenario-I

Scenario-II: We received the signal by placing passive eavesdropper É near the Ť.

Testing Results: In testing, we applied different filters and noise reduction techniques on passively receive data to retrieve the UID sent by the Ť but all attempts were unsuccessful in both scenarios. We were able to securely transmit and decode the UID on the legitimate Ř's side.

The signal received by the passive eavesdropper in scenario-I and II are shown in Figures 7.6 and 7.7. Both figures show that Eve gets constant (flat) power spectrum in the received signal which is a spectrum of a *white noise*. So passive eavesdropper gets nothing but a noise. The best retrieval(decoded) graph on the passive eavesdropper side is shown in Figure 7.8 in scenario-II. The decoded signal at the legitimate reader is shown in 6.19 in Chapter 6.

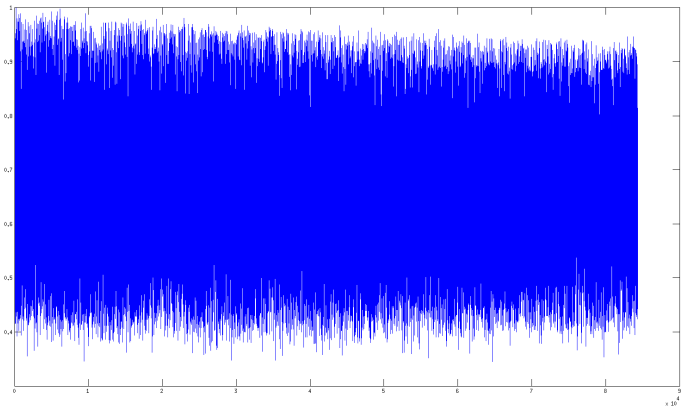


Figure 7.7: Signal received by passive eavesdropper in scenario-II

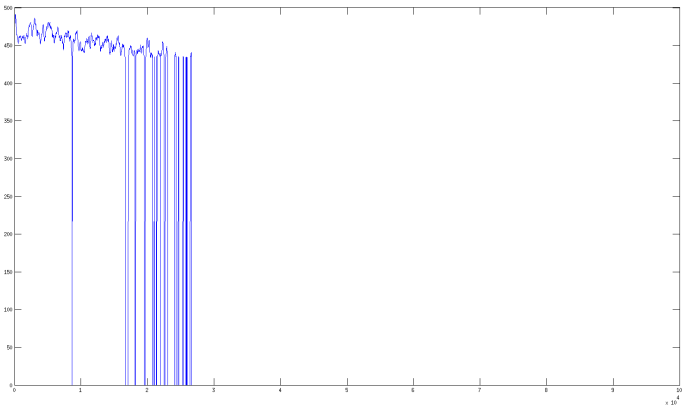


Figure 7.8: Message decoded by passive Eavesdropper

Security against Passive Eavesdropping

$\check{\text{R}}$ sent levels of amplitude s_i with continuous wave c_i towards $\check{\text{T}}$. $\check{\text{T}}$ received signal r_i which is given by

$$r_i(t) = (s_i(t) + c_i(t)) \cos(2\pi f_i t + \theta) + n(t) \tag{7.17}$$

where $n(t)$ is the channel noise and f_i is the UHF carrier hopping frequency. $\check{\text{T}}$ reply with the UID with ASK modulation given by

$$r_i'(t) = Ar_i(t) + n'(t) \tag{7.18}$$

Comments

Passive eavesdropper (ξ) gets signal r_i' , from the received signal. Eve (ξ) tries to recover the UID as well as levels of amplitudes. There are two major difficulties in launching passive eavesdropping.

1. To get the UID sent by the $\check{\text{T}}$ Eve first need to recover levels of amplitudes. For the ASK signal for RFID tag, **0** represents the same levels of amplitude and **1** increases all the levels. But it is hard to distinguish whether the resultant has been modified by **0** or **1**. The following example demonstrates this property.

   Example: We may assume that Eve has no knowledge of the generated levels.

   Levels generated by $\check{\text{R}}$ are S = {...,-3,-2,-1,0,1,2,3,...}. When $\check{\text{T}}$ responses with **0** all the levels will remain the same as sent by the reader $\check{\text{R}}$, i.e., S = {...,-3,-2,-1,0,1,2,3,...}. Otherwise the set S becomes {...,-2,-1,0,1,2,3,4,...}, which is obtained by adding 1 to each level of the transmitted signal S.

   As each transmitted symbol contains many set of generated levels. It hard for an Eve to distinguish where $\check{\text{T}}$'s response has been added to the send signal.

2. We may assume Eve recovers the levels of amplitude. However to get the UID Eve needs to remove all the levels in the same manner as they were added. The following example demonstrates this property.

   Example: Lets, from Table 7.7, $uid \neq (\xi)uid'$.

Table 7.7: Example

s	5	-2	1	7	-5	2	6	...	...
uid	2	5	4	3	1	2	7	...	...
r'	7	3	5	10	-4	4	13	...	...
$(\xi)s$			5	-2	1	7	-5	2	6
$(\xi)uid'$			10	8	3	11	8	...	...

Assume Eve gets s to recover *uid*. Eve needs to remove all levels from the same starting point as they were added with same data rate and timings. This is a synchronization problem. As Ř knows the staring point in the received signal's sample set, Ř can decode the *uid* by cancelling at the added levels. Hence *DSB Enc* scheme is secure from passive eavesdropping.

7.7.2 Secure Against Replay Attack

In replay attack, an adversary Á gets signal r' at time t which he tries to replay to the Ř at time $(t + \tau)$. As per *DSB Enc* scheme, we are continuously updating the key every session, so the key that has been used previously at time t would be different than the one used at time $(t + \tau)$ which makes *DSB Enc* scheme resistant to replay attacks.

7.7.3 Secure Against Relay Attack

NFC enabled devices: Most of the low cost relay attacks are initiated with NFC enabled phones using ISO 14443 [62]. ISO 14443 type A uses Manchester Coding with 10% ASK and Modified Miller with 100% ASK while type B uses NRZ-L encoding with 10% ASK [52]. These schemes are used in active and passive modes. According to ISO NFC standard, NFC devices can only capture and transmit two levels. NFC devices would map multi-levels to 1 or 0. Since NFC enabled devices cannot catch and transmit multilevel amplitudes, they can not initiate relay attacks those mentioned in [17, 19].

Expensive analogue devices: If Á uses an expensive device for such kind of attacks instead of NFC enabled phone, it would capture the analogue signal that has been transmitted. To retransmit the same signal to it other devices located near the vicinity of the tag, it must either re-sample it to the same digital sample rate as it was before or send the analogue signal directly. For the former case, since the sampling rate is unknown to the attacker, he cannot perform the re-sampling, i.e., the sample rate here is the bit-rate and symbol-rate of the produced levels of amplitudes using *DSB Enc* which can be standardized by randomly choosing the bit rate and symbol rate for each session. [2]. For the later case, it requires an expensive powerful antenna/amplifier.

Conclusion: This makes *DSB Enc* scheme secure against relay attacks from low cost NFC enabled devices, but it is somewhat secure against expensive analogue relay devices, which are neither practical nor can be detected easily.

[2]This sample rate is different and independent from the tag's symbol rate.

7.8 Summary and Comparisons

Conventional RFID systems suffer from various attacks. Many schemes and cryptographic algorithms have been proposed to secure RFID communication. But all of those schemes are prone to various types of attacks on different layers. Not any single scheme provides the solution against all existing attacks without increasing the cost or removing the salient features of RFID passive tags.

Savry *et al.* [1, 44] have proposed a physical layer scheme named RFID Noisy Reader in which they used a separate hardware for generating 8-bit noise level on the physical layer to secure tag to reader and reader to tag communications. In their scheme, the Eve can decode the tag's reply if Eve is closer to the tag or the reader and it creates a problem for the legitimate reader to decode the tag's reply if they are far apart due to tremendous increase in bit-error-rate (BER).

DSB Enc provides a lightweight, low-cost and practically secure physical layer security to the RFID system, for a supply chain processing application, without increasing the computational power and tag's cost. In comparison to Noisy Reader, we have generated different levels before transmission of the signal. Our implementation and experimental results validate that *DSB Enc* is secure against passive eavesdropping, replay and relay attacks. It provides better results in the presence of AWGN channel. *DSB Enc* scheme is a special case of [67].

Chapter 8

Conclusion and Future Work

This chapter summarizes the contributions of the thesis and provides potential future applications and directions for future work that are still need to be done.

In chapter 1, we have given the introduction of RFID and briefly describe the security and privacy concerns related to RFID systems. In Chapter 2, we presented fundamentals, and background information related to RFID systems. We have described the basic architecture of RFID system. Furthermore in the chapter, we have explained physical layer characteristics(encoding and modulation schemes) of RFID used in different standards. We also presented several attacks on RFID systems. In Chapter 3, we have defined the list of notations, definitions and fundamental background information essential for later chapters. In Chapter 4, we have given the historical background and evolution of software radio and software defined radio, GNU Radio and USRP. We also discussed the need and importance of SDR in the modern communication era. In Chapter 5, we have reviewed various physical layer techniques, that are present in literature and are used for securing RFID communications. In Chapter 6, we have introduced our new physical layer scheme named *DSB Enc* using multilevel generator. We provided the system model, simulation model, preliminary simulation results and illustrated the principle of level generator. Simulations were conducted on GNU Radio Companion. We have validated the feasibility of our new efficient scheme by conducting experiments using software defined radio (SDR) and a WISP tag. In Chapter 7, we have given a thorough security analysis and provided the results of passive eavesdropping on *DSB Enc* scheme.

8.1 Contributions

Proposed Scheme

In this thesis, we proposed a lightweight, low-cost and practically secure physical layer security to the RFID system, for a supply chain processing application, without increasing the computational power and tag's cost. The proposed scheme was validated by simulations on GNU Radio and experimentation using SDR and a WISP tag. Our implementation and experimental results validate that *DSB Enc* is secure against passive eavesdropping, replay and relay attacks. It provides better results in the presence of AWGN channel.

Simulation Results Part I

In first part of simulation results, we have shown that we could recover the sent signal in the presence of AWGN channel as long as we know the levels of amplitudes added at the time of transmission. We can remove all the levels precisely at the receiver side regardless of the amplitudes of those levels.

Simulation Results Part II

In second part of simulation results, we have shown a method to increase the transmitted signal's power by adding the levels of amplitude and data signal in different frequency bands. This method follows the concept of double sideband large carrier *(DSB-LC)* amplitude modulation. As added levels in different frequency band do not carry any information, therefore it is a trade off between spectral efficiency and long range.

Level Generator

In our proposed scheme, the reader has been modified for signal generation by using multiple LFSRs which produce different signal levels and each level is encoded using NRZ-L. The encoded signal levels are discrete and are made continuous by adding them to a continuous constant wave which tends to be a Gaussian distribution. This will assure that the tag gets uninterrupted power supply. The resultant wave is modulated on a carrier frequency 902-928 MHz using MPSK. The channel is an additive white Gaussian as well. Since the linear combination of two independent Gaussians is a Gaussian, therefore the transmitted signal becomes Gaussian.

To transmit the message to the reader, the passive tag modulates a resistive or capacitive load at its antenna and adds its response to the carrier signal using ASK. The resultant is still Gaussian. So if Eve picks the tag's reply, he will get a Gaussian signal which is hard to decode without a priori knowledge of the levels generated by the reader. Therefore only the legitimate reader can decode the tag's reply by subtracting the levels

at the reader side. Another obstacle for an eavesdropper is the synchronization problem of levels generated at the time of transmission.

Proof-of-Concept

We have given the proof-of-concept by practically implementing our proposed scheme using SDR and passive tag. From the experimental results, it can be concluded that the proposed scheme provides light weight,low cost and practically secure physical layer security to the RFID system.

Robustness Against Various Attacks

In Chapter 6, we have defined the adversary model for our system, presented cryptographic security analysis for the proposed scheme and provided several methods for generating multiple levels from level generator. We also analysed the robustness of proposed scheme against various existing attacks and suggested measures to prevent them.

8.2 Future Work

In future, we would like to perform active eavesdropping and colluded passive eavesdropper attack to further validate the feasibility of proposed scheme and use in real applications. In this thesis, we discussed the possibility of secure transmission at the physical layer for communication model comprising of one legitimate reader, one valid tag and a single passive eavesdropper. We would like to generalize this scheme with efficient encoding schemes and more complex communication models encompassing several passive eavesdropper with multi-user channel environment.

Our proposed scheme can be used for various future applications e.g. *key transportation* and *symmetric key distribution.*

1. ***Key transportation:*** As our proposed scheme provides secure physical layer protocol for sending UID of passive tag on vulnerable channel, we would like to extend the proposed scheme to securely transport the key from passive or active tag to reader channel using multi-level amplitudes in the future.

2. ***Symmetric key distribution:*** We would also like to enhance our proposed scheme to be used for symmetric key distribution which would be independent of the location and time invariant channel conditions and will be implemented on the physical layer of the OSI model.

The proposed scheme has verified potential of implementing many other applications but there is a lot of research that still needs to be done.

References

[1] F. Achard and O. Savry. A cross layer approach to preserve privacy in RFID ISO/IEC 15693 systems. *RFID-Technologies and Applications (RFID-TA)*, 2012 IEEE International Conference on , vol., no., pp.85,90, 5-7 Nov. 2012.

[2] S. Bengio, G. Brassard, Y.G. Desmedt, C. Goutier, and J.J. Quisquater. Secure implementation of identification system. *Journal of Cryptology*, vol. 4, no. 3, pp. 175-183, 1991.

[3] Josh Blum. GNU Radio Companion. `http://www.joshknows.com/grc`, 2013

[4] S. Brands and D. Chaum. Distance-bounding protocols. *Advances in Cryptology, EUROCRYPT'93*, LNCS 765, pp. 344-359, 1994.

[5] M. Buettner and D. Wetherall. A Gen 2 RFID monitor based on the USRP. *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 3, pp. 41-47, 2010.

[6] M. Buettner, R. Prasad, A. Sample, D. Yeager, B. Greenstein, J. R. Smith, D. Wetherall. RFID sensor networks with the Intel WISP. *Proceedings of the 6th ACM conference on Embedded network sensor systems*, Raleigh, NC, USA, November 05-07, 2008.

[7] C. Castelluccia and G. Avoine. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. *Proceedings of CARDIS 2006*, LNCS 3928, 289-299, 2006.

[8] Q. Chai and G. Gong. BUPLE: securing passive RFID communication through physical layer enhancements, to appear *In Proceedings of Workshop on RFID Security, RFIDSec'11*, Amherst, MA, USA, 2011.

[9] Q. Chai. Design and Analysis of Security Schemes for Low-cost RFID Systems. *PhD Thesis, University of Waterloo*, pp.93, 2012.

[10] Q. Chai, G. Gong, D. Engels. How to develop clairaudience-Active eavesdropping in passive RFID systems.*IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp.1-6, 2012.

[11] L. Chen and G. Gong. *Communication System Security*. CRC press, pp.28-33, 2012.

[12] C.L. Chen, and Y.Y. Deng, "Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection." *Engineering Applications of Artificial Intelligence* 22 (8), pp. 1284-1291, 2009.

[13] J.H. Conway. On numbers and games. *Number 6 in London Mathematical Society Monographs*, Academic Press, 1976.

[14] P.G. Cook and W. Bonser. Architectural overview of the SPEAKeasy system. *IEEE J. Select. Areas Commun.*, vol. 17, no. 4, pp.650 -661, 1999.

[15] Y. Desmedt. Society and group oriented cryptography : A new concept. *In C. Pomerance, editor, Advances in Cryptology, Proc. of Crypto87 (Lecture Notes in Computer Science 293), pages 120-127. Springer-Verlag, Santa Barbara, California, U.S.A., August 16-20*, 1988.

[16] W. Dullink and P. Westein. Remote relay attack on RFID access control systems using NFC enabled devices. *Technical report, University of Amsterdam*, 2013.

[17] A. Francillon , B. Danev and S. Capkun. Relay attacks on passive keyless entry andstart systems in modern cars. *Proc. NetworkDistrib. Syst. Security Symp.*, 2011.

[18] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. *Radio Frequency Identification:Security and Privacy Issues*, 2010.

[19] L. Francis , G. P. Hancke , K. E. Mayes and K. Markantonakis. Practical relay attack on contactless transactions by using NFC mobile phones. *Cryptology ePrint Archive, Report*2011/618, 2011.

[20] S.W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, New York, NY, 2004.

[21] Rudolf F. Graf. Modern Dictionary of Electronics (7th edition) pp.615-616, 1999.

[22] C.M. Grinstead and J.L. Snell. Introduction to Probability. *American Mathematical Society*, Providence, RI, 2nd Edition, pp. 325-356, 1997.

[23] S. Gultchev, K. Moessner, D. Thilakawardana, T. Dodgson and Rahim Tafazolli. Evaluation of Software Defined Radio Technology. *Centre of Communications System Research, University of Surrey*, February 2006.

[24] G. Hancke. A practical relay attack on ISO 14443 proximity cards. *Technical report, University of Cambridge Computer Laboratory*, 2005.

[25] G. Hancke. Modulating a noisy carrier signal for eavesdropping-resistant HF RFID. *Elektrotechnik und Informationstechnik*,pp. 404-408, November 2007.

[26] G. Hancke. Noisy carrier modulation for HF RFID. *First International EURASIP Workshop on RFID Technology*. pp. 63-66, 2007.

[27] M. E. Hellman and A. B. Carleial. A note on Wyner's wire-tap channel. *IEEE Trans. Inform. Theory*, vol. IT-23, pp.387 -390, 1977.

[28] A. Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication (J-SAC)* 24(2), 2006.

[29] A. Juels, R.L. Rivest and M. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. *In Proceedings of the 10th ACM Conference on Computer and Communication Security*, CCS'03, pp.103-111, 2003.

[30] C. Kim and G. Avoine. RFID distance bounding protocol with mixed challenges to prevent relay attacks. *Conference on Cryptology and Network Security, CANS'09*, LNCS 5888, pp 119-133, 2009.

[31] A. N. Kolmogorov. Three approaches to the quantitative definition of information. *Probl. Inform. Transmission*, vol. 1, pp. l-7, 1965.

[32] R. J. Lackey and D. W. Upmal. Speakeasy: The military software radio *IEEE Commun. Mag.*, vol. 33, pp.56-61, 1995.

[33] A. Lempel and J. Ziv. On the complexity of finite sequences. *IEEE Trans. Inform. Theory*, vol. IT-22, pp.75-81, 1976.

[34] Z. Li and G. Gong. A Survey on Security in Wireless Sensor Networks. ,*Department of Electrical and Computer Engineering, University of Waterloo, Canada*, CACR, 2008.

[35] Y. Luo, Q. Chai, G. Gong and X. Lai. WG-7, a lightweight stream cipher WG-7 for RFID encryption and authentication.*IEEE Global Telecommunications Conference, GLOBECOM'10*, pp.1-6, 2010.

[36] K. Mandal and G. Gong. Cryptographic D-morphic Analysis and Fast Implementations of Composited De Bruijn Sequences. *CACR technical report*, University of Waterloo, 2012.

[37] K. Mandal and G. Gong. Probabilistic Generation of Good Span n Sequences from Nonlinear Feedback Shift Registers. *CACR technical report*, University of Waterloo, 2012.

[38] J. Mitola, The software radio architecture, *IEEE Communications Magazine*, vol. 33, pp.26-38, 1995.

[39] J. Mitola. What is a Software Radio?. `http://web.archive.org/web/20050315234159/http://ourworld.compuserve.com/homepages/jmitola/whatisas.htm`, 2013.

[40] M. Nguyen. Software Radio (R) Evolution and Its Application to Aeronautical Mobile Communications. *Integrated CNS Conference* May 19-22, 2003.

[41] A. Perrig, J. Stankovic, and D. Wagner. Security in Wireless Sensor Networks. *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, June 2004.

[42] J. Reed and J. Neel *Software Radio: A Modern Approach to Radio Engineering*, chapter case studies in software radio design, Prentice Hall, 2002.

[43] M.R. Rieback, B. Crispo, and A.S. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. *Proc. 10th Australasian Conf. Information Security and Privacy (ACISP 05)*, LNCS 3574, Springer, pp. 184-194, 2005.

[44] O. Savry, F.P. Peyroula, F. Dehmas, G. Robert and J. Reverdy. RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? *9th International Workshop Cryptographic Hardware and Embedded Systems (CHES 2007), Springer-Verlag LNCS 4727*, pp 334-345, September 2007.

[45] C. Shannon, Communication theory of secrecy systems. *Bell Syst Tech. J.*, vol. 28, pp. 656-715, 1949.

[46] Dawei Shen. Tutorial 10: Writing A Signal Processing Block for GNU Radio - Part I, June 11, 2005. Available `http://www.snowymtn.ca/GNURadio/GNURAdioDoc-10.pdf`

[47] Dawei Shen. Tutorial 11: Writing A Signal Processing Block for GNU Radio - Part II, June 15, 2005. Available http://www.snowymtn.ca/GNURadio/GNURAdioDoc-11.pdf

[48] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy and A. Mamishev. A wirelessly powered platform for sensing and computation. *Proc. Ubicomp*, pp.495-506, 2006.

[49] A. Wyner. The wiretap channel. *Bell Syst Tech. J.*, vol. 54, pp. 1355-1387, Oct. 1975.

[50] D. Zanetti, P. Sachs, and S. Capkun. On the practicality of UHF RFID fingerprinting: how real is the RFID tracking problem? *In Proceedings of the 11th international conference on Privacy enhancing technologies (PETS'11), Simone Fischer-Hubner and Nicholas Hopper (Eds.)*. Springer-Verlag, Berlin, Heidelberg, 97-116, 2011.

[51] About Ontario's Enhanced Driver's Licence at http://news.ontario.ca/mto/en/2009/05/about-ontarios-enhanced-drivers-licence.html, May 5, 2009.

[52] Atmel Corporation. Requirements of ISO/IEC 14443 Type B Proximity Contactless Identification Cards, Application Note. Rev. 2056BRFID11/05.

[53] EPC Global, Class-1 Generation 2 specification for RFID air protocol standard v1.2.0, http://www.epcglobalinc.org/, 2008.

[54] Ettus Research LLC, RFX900 750-1050 MHz Rx/Tx. https://www.ettus.com/product/details/RFX900, 2013.

[55] Ettus Research LLC, USRP-1. https://www.ettus.com/product/details/USRPPKG, 2013.

[56] Ettus Research LLC, USRP-N210. https://www.ettus.com/product/details/UN210-KIT, 2013.

[57] Ettus Research LLC, Universal Software Radio Peripheral. https://ettus-apps.sourcerepo.com/redmine/ettus/projects/uhd/wiki, 2013.

[58] Ettus Research LLC, VERT900. https://www.ettus.com/product/details/VERT900, 2013.

[59] GNU GENERAL PUBLIC LICENSE, Version 3. http://www.gnu.org/licenses/gpl.html, 29 June 2007.

[60] GS1 EPC Tag Data Standard v1.6 http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf, 2011.

[61] Intel WISP, http://wisp.wikispaces.com, 2013.

[62] International Organization for Standardization. *ISO/IEC 14443-1, Identification cards - Contactless integrated circuit(s) cards - Proximity cards*, 2008.

[63] Laird Technologies, General Purpose Antenna. http://lairdtech.thomasnet.com/item/rfid-antennas/general-purpose-antennas/s9028-pcl?, 2013.

[64] RFID Security. *The Government of the Hong Kong special administrative region*, February 2008.

[65] Signal Propagation and Path Loss Models. *Lecture on Wireless Communications, Standford University*, Fall 2011.

[66] Smartrac-group web site Referenced 2013 at http://www.smartrac-group.com/en/applications.php

[67] F. Huo and J. Yang. A Framework to Securing RFID Transmissions by Varying Transmitted Reader's Power. Submitted to *RFIDSec Asia*, 2013.