QATAR UNIVERSITY

COLLEGE OF ENGINEERING

PHYSICAL LAYER SECUIRTY TECHNIQUES FOR RFID SYSTEMS

BY

GEHAD ESSAM DESOUKY

A Thesis Submitted to

the College of Engineering

in Partial Fulfillment of the Requirements for the Degree of

Masters of Science in Electrical Engineering

June 2020

COMMITTEE PAGE

The members of the Committee approve the Thesis of

Gehad Essam Desouky defended on 26th February 2020

Tamer Khattab
Thesis/Dissertation Supervisor

Aboelmagd Noureledin
Committee Member

Mazen Hasna
Committee Member

Amr Mohamed
Committee Member

Approved:

Khalid Naji , Dean, College of Engineering

ABSTRACT

DESOUKY, GEHAD E., Masters :

February: 2020 [Masters of Science/ Electrical Engineering]

Title: PHYSICAL LAYER SECURITY TECHNIQUES FOR RFID SYSTEMS

Supervisor of Thesis: Tamer M Khattab.

The deployment of RFID technology in various applications is delayed due to the increased concerns over possible security breaches, especially in healthcare applications. For medical devices and applications, RFID and IoT technologies can improve the wellbeing of patients and reduce errors at hospitals, but the deployment of RFID is obstructed by multiple barriers including the security concerns. Previous research and studies have proved that traditional cryptography methods cannot be applied on RFID, due to the limited computational, storage and power resources in RFID tags and readers. These constraints emerged the novel idea of exploiting the characteristics of the physical layer to achieve information secrecy in RFID systems.

In this thesis, two novel key-less physical layer based secrecy approaches have been developed and analyzed. In first approach a combined beamsteering and injected noise scheme is proposed, where beamsteering is exploited at the tag and the noise injection is exploited at the reader. The results show that this novel approach outperforms previous developed security scheme for RFID. Another novel approach is developed by implementing directional modulation (DM) techniques at the RFID reader while maintaining the simplicity of the tag's circuity and processing capabilities.

DEDICATION

This thesis is dedicated to my parents, my husband and my siblings

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor Dr. Tamer Khattab, for his continuous support of my Master study and related research. His guidance and mentoring helped during the time of research and writing this thesis.

Besides my supervisor, I would like to thank Dr. Khalid Abualsaud who provided me an opportunity to join his research project “NPRP10-1205-160012” team at Qatar University.

I would also like to thank my amazing parents, husband and siblings for their endless support and love.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

RFID	Radio Frequency Identification
CSI	Channel State Information
BER	Bit Error Rate
EVM	Error Vector Magnitude
LF	Low Frequency
HF	High Frequency
UHF	Ultra High Frequency
EPC	Electronic Product Code
RF	Radio Frequency
PLS	Physical Layer Security
BS	Beam Steering
DM	Directional Modulation
EMI	Electro Magnetic Interference
HIPAA	Healthcare Insurance Probability and Accountability Act
IoT	Internet of Things
SARS	Severe Acute Respiratory Syndrome
CW	Continuous wave
MIMO	Multiple Input Multiple out
SIMO	Single Input Multiple Output
ANI	Artificial Noise Injection
AFF	Artificial fast fading
SAR	Specific Absorption Rate
BAN	Body Area Network

FCC	Federal Communication Commission
AFA	Analogue Finger Print for Authentication
SINR	Signal to Interference Noise Ratio
SNR	Signal Noise Ratio
NFC	Near-Filed Coupling
FFC	Far-Filed Coupling
ISO	International Standards Organization
IEC	International Electrotechnical Commission
DAM	Direction Antenna Modulation
LOS	Line of Sight
BPSK	Binary Phase Shift Keying
QPSK	Quadrate Phase Shift Keying
FSK	Frequency Shift Keying
ASK	Amplitude Shift Keying
DSB	Double Side Band
PSK	Phase Shift Keying
EMI	Electromagnetic Interference
DOF	Degree Of Freedom
ASM	Antenna Subset Modulation
OFDM	Orthogonal Frequency Division Modulation
BS-NI	Beam Steering and Noise Injection

CHAPTER 1: INTRODUCTION

RFID is used in several applications such as inventory; biometric information, such as e-passports; drug tracking and medical devices that records patient's information; access control applications, such as access to sites; transports and event management by checking the authenticity of tickets for a concert or sports event or even a plane boarding ticket. Recently, RFID is widely adopted into healthcare applications, especially in patient tracking and identification as well as asset and equipment management and tracking [1]. The wide deployment of RFID technology in several applications has been delayed due to some lacking features such as the lack of security and confidentiality.

The increased presence of RFID systems has increased the likelihood of attacks against these systems. Due to the broadcast backscatter based nature of the communication technique in RFID, it is vulnerable to eavesdroppers attacks. The data is transmitted to the legitimate user through activating the tag from an access point. The tag's secret information sent over the backscatter channel can be overheard by an eavesdropper if it lies in the access point's air interference power coverage area [2]. Increasing the deployment of RFID in several applications at a commercial level mandates the development of robust security techniques that meets the target industry specifications.

Physical layer security (PLS) has recently emerged as a prominent method to secure wireless communication systems against eavesdropping; therefore, maintain the reliability of the information. The basic idea of PLS is to exploit the network characteristics including noise, fading, interference and diversity. The main design goal of PLS is to increase the performance of the legitimate channel while decreasing the performance of the eavesdropper’s channel. The performance is measured using the secrecy rate, which measures the difference between the intended receiver and the eavesdropper; it can also be assessed using the bit error rate (BER) and the error vector magnitude (EVM) metrics. There are several approaches for PLS, but the main approach is noise jamming (injection), which exploits the noise characteristics of the channel. In addition to noise injection, other characteristics of the physical layer can be exploited to enhance the performance of the system such as exploiting the degrees of freedom by using transmitter and/or receiver antenna arrays. PLS is used in several systems such as visual light communications (VLC), smart grids, power line communications (PLC), Internet of things (IoT), body area networks (BAN) and RFID. Focusing on RFID systems, there are several work and research studies to secure RFID systems using PLS [3]. An advanced technique that uses PLS is the directional modulation (DM) scheme, which exploits both noise and space (degrees of freedom) characteristics of the physical layer. Generally, DM is a transmitter side technology that is capable of directing the signal into pre-specified direction while simultaneously distorting the signal in any other direction. Practical representation of DM was first proposed in [4]. Prior work to [4] focused only on developing physical structures for DM. This lead to some practically challenged technologies in some applications, such as passive DM transmitter, direction antenna modulation (DAM) [5, 6], and sidelobe modulation [7]. Recently, the DM technology was combined with other technologies to produce more practical systems using active DM transmitters and phased arrays as presented in [4].

In the rest of this chapter, the motivations to carry this work are discussed, followed by stating the main objective (scope) of this thesis and describing the layout of the rest of the thesis.

1.1 Motivation

In the past few years, traditional cryptography techniques relying on secret key generation were adopted in any wireless system [8]. There are two main types in traditional cryptography methods; the public key and symmetric cryptography. These cryptography methods can be very challenging to use in backscatter, RFID and IoT technologies, due to their resource intensive requirements versus the limited resources in RFID systems. Cryptography requires complex processing and advanced mathematical algorithms while RFID tags are usually passive and do not have advanced processing capabilities. In addition, there are some limitations faced by cryptography techniques which are: 1) managing and maintain the secret key process for the intended users can be very challenging especially in a decentralized system such as RFID, which may have one reader and multiple tags; 2) since backscatter channels are vulnerable towards eavesdropping, increasing the key length can make the system more secure but it is a waste of resources; and 3) these techniques depend on the complexity of the mathematical fundamentals, but with the fast development in computing power devices, the assumption that the eavesdropper has limited computing capabilities is less valid and the eavesdropper can crack the key and obtain the information [3].

These complications in the traditional methods motivate a new approach for security aspects. PLS is an effective means to secure the wireless system by exploiting the physical layer characteristics of wireless networks. Hence, PLS is emerging as a high potential technique to secure RFID systems. Even though, PLS was deployed in several existing work, but all the existing work target the noise characteristic of the system. In some scenarios, the system performance was sufficient, and the desired secrecy level was achieved. However, exploiting the noise characteristics only showed some limitations in the power required and secrecy achieved in other scenarios [9]. Accordingly, this thesis will discuss addressing the security of RFID systems using Direction Modulation (DM) techniques, which is considered recently as one of the effective PLS techniques [3].

1.2 Thesis Scope

The overarching objective of this thesis is to develop a secure RFID system on the physical layer. Towards this objective, different techniques for securing RFID systems are surveyed. The survey is conducted by reviewing the literature including RFID privacy and security aspects, and physical layer security approaches. The limitations and challenges for each security method are highlighted and the proposed techniques are laid out. To test the performance of the proposed techniques, analysis of the BER and secrecy rate, as main performance metrics, are carried out and concluding remarks along with possible future directions are drawn.

1.3 Thesis objective

- Develop an adequate methodology to secure RFID system
- Reviewing several security techniques that was developed in the literature for RFID system
- Analyze the performance of the two proposed schemes

1.4 Thesis Outline

The organizational structure of this thesis proceeds as follows:

- Chapter 2 gives an overview of the RFID technology and its various applications and highlights the different protocols developed for commercial RFID technologies. In addition, it provides a general background on different physical layer secrecy methods along with an elaborate description of the direction modulation technique. The challenges in securing RFID systems are mentioned and different security methods are discussed. In addition, the state-of-the-art literature on physical layer security techniques in RFID are surveyed. Finally, the main working assumptions and the thesis contributions are highlighted.

- In Chapter 3, a novel combined beamsteering and noise injection PLS approach for RFID is proposed, which achieves security of the tag's signal by equipping the tag with multiple antennas. Further, the proposed system performance analysis is carried out, and the results are illustrated and discussed.
- In Chapter 4, another novel technique to secure RFID systems is developed using the DM technology applied at the reader transmitter. The system performance analysis is developed and the results are illustrated and discussed.
- Finally, in Chapter 5, conclusions are drawn, and new research challenges are identified for future work.

CHAPTER 2: BACKGROUND AND RELEVANT WORK

In this chapter, an overview of the state of the art of RFID technology and different security methodologies that can be applied to wireless systems are given. First, RFID technology, its network architecture and its applications are inclusively mentioned. Then, the different security techniques through physical layer are described in general. Further, an overview of the contributions of this thesis is highlighted.

2.1 RFID Technology

Radio frequency identification (RIFD) technology is a wireless communication technology that is mainly used to identify objects. It is a fast developing technology [10], where in 1960s and 1970s, research for RFID emerged and in July 1963, the first passive tag was developed by Richardson. Around 1967, a reader-tag system patent was developed and granted. European countries and the United States were interested in RFID technology when it was first developed and commercialized by several companies including Kongo, Sensoramtic and Checkpoint [11]. Different RFID applications were desired by the United States and European countries, where Europe was interested in animal tracking and industrial applications, while the US was interested in personal access and transportation applications. The increased requirement of the commercial use of RFID, emerged the need for standardizing the system. This led to several standards in 1990s. Most of the standardization activities were conducted by ISO (International Standards Organization) and IEC (International Electrotechnical Commission). More RFID applications were promoted in the late 1990s including supply chain management, which motivated a further series of standards. In 1999, GS1 which is European Article Number (EAN) International and the Uniform Code Council (UCC); adopted a UHF frequency band for RFID system and developed a global standard for product labeling called EPC (Electronic Product Code). In 2005, the first

EPC standard was released. Later, generations and classes were developed for EPCglobal. Currently, EPCglobal class-1 generation-2 is used for UHF RFID system. The RFID application areas massively increased to include inventory management, drug and human tracking, E-passports, automated libraries , livestock ID, access cards and healthcare applications. RFID is also widely used for auto-ID technologies [12-14]. RFID is an emerging technology used to provide unique identification code. An RFID system comprises fixed and remote components. The fixed components are the base station, the reader, and the coupling device. The remote components are tags, badges or smart cards. The remote components vary according to the application type [15]. The communication between the reader and the tag can be conducted through three types of coupling, which are capacitive, inductive and backscattering coupling [11] . In some applications, the system consists of multiple tags and a single reader such as in supply chain and inventory applications. RFID systems can operate under four different frequencies that lie in the ISM (Industrial-Scientific-Medical) range; low frequencies, high frequencies, ultra-high frequencies and microwave frequencies. Most of the RFID applications operate in the UHF range, and the work in this thesis assumes passive tags operating in UHF range only.

RFID tag consists of two main elements, the antenna to transmit and receive information from the reader and a chip where the tag's information is stored. Other elements such as batteries may be added to the tag depending on the tag type. There are three types of RFID tags: 1) passive tags: that rely on the continuous wave (CW) transmitted from the reader to power up as they do not have batteries, 2) active tags that contain an integrated circuit, antenna, battery and on-board transmitter and the on-board transmitter sends the signal directly to the reader instead of backscattering the signal, 3) semi-active tags that contain an integrated circuit, antenna and a battery and communicate with the reader by backscattering but the battery is used to maintain memory in the tag. Figure 1 illustrates the communication between the reader and passive tags in the case of single reader and single tag system [16].

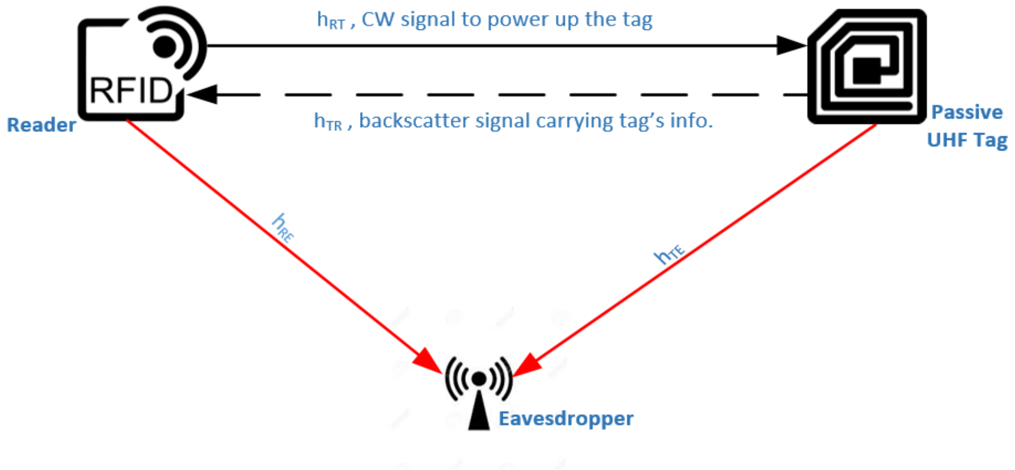

h_{RT} , CW signal to power up the tag
RFID
Reader
h_{TR} , backscatter signal carrying tag's info.
Passive
UHF Tag
h_{RE}
h_{TE}
Eavesdropper

Figure 1 Wirless backscatter model between a reader and a tag

RFID systems operate in different frequency bands ranging from the 50 kHz band up to the 2.5 GHz band [1]. The frequency ranges can be categorized into four categories; a) Low frequency (120-140 kHz), b) High frequency (13.56 MHz), c) UHF (860-960 MHz) and d) Microwave frequency (2.4 and 5.8 GHz). The LF and HF are used in Near-Field coupling, while UHF and microwave are used in Far-Field coupling.

In NFC, the passive tag relies on inductive coupling to harvest the energy from the reader and communicates back to the reader by a load modulation mechanism. Usually, NFC operates at LF and HF frequency band. Beyond that range, the wavelength of the signal is much smaller than the gap between the reader and the tag and the inductive coupling becomes very weak. In this case, at UHF and microwave frequencies, the signal required to power up the tag is harvested by the tag's antenna and a part of this power is reflected back to the reader. This process is known as backscatter coupling. Those different frequency bands have diverse applications and different reading ranges which are mentioned in Table 2 in section 2.4. In addition to that, the data rate is higher while using FFC in comparison with NFC due to the bandwidth of both methods.

The main protocol developed for RFID technology is EPCglobal generation-2 class-1. EPC Class-1 Gen-2 is the protocol used to initiate the identification between the reader and each tag. The reader receives the tag's information from a tag by transmitting a continuous wave (CW) to the tag and listening to the backscatter reply. In the backscatter signal, the tag sends its information back to the reader, while the tag does not need to demodulate the CW signal for backscattering.

In this thesis, the work focuses only on passive tags at UHF band that operate using backscatter coupling. A diagram that illustrates the backscatter coupling between the reader and the tag is presented in Figure 2. Moreover, to demonstrate a full picture, the equations of the reading range, absorbed power and reflected power are mentioned in the next section.

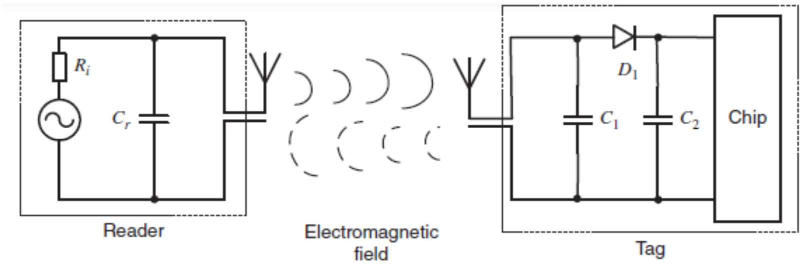


Figure 2 Backscattering coupling between reader and passive tags

2.2 RFID Communication Architecture

The communication between the reader and tag depends on the type of the tag and the operating frequency. Focusing on passive tags operating in UHF band, the communication between the reader and the tag is conducted through backscatter coupling. In backscattering, the RFID system is considered as a half-duplex system where the reader transmits a conventional continuous wave to the tag; the passive tag captures this signal to power up and uses the rest of the signal to transmit back its information to the reader. Since the communication is done in half-duplex mode, the channels between the reader and the tag can be divided into two links: forward and backward link, denoted as h^f and h^b, respectively. The forward link indicates the propagation of the signal from the reader to the tag and the backward link is the propagation of the backscatter signal from the tag to the reader. The total communication channel between the reader and the tag is denoted as $h = h^b \gamma h^f$, where γ is the backscatter coefficient of the tag [17]. In addition, the distribution of the channels may vary depending on which application the passive tags are deployed in. For applications of LF and HF, the RFID tags often have short distances and LOS (Line of Sight). Therefore, Rician distribution is used to model the fading of the links. While for UHF RFID tags that are deployed in long distance applications and thus are projected to multi-path fading, the channels can be represented by Rayleigh distribution. Since the RFID system has two communication links, the channel is modeled as a double Rayleigh channel. The performance of double Rayleigh using BPSK modulation for general wireless systems is analyzed in [18]. While, the performance of RFID with Rayleigh channel distribution was analyzed in [19]. In the latter work, FSK modulation was used to modulate the signal from the tag on the h^b link while the signal from the reader used ASK modulation on the h^f link. These modulation schemes are according to the EPC standards. The following part will analyze the analogue circuit of the tag while receiving the signal and backscattering it.

The CW is captured by the tag but divided into two parts which is controlled by the tag's antenna. The first part occurs at the matching state where the tag harvests some of the energy to power up. The second part occurs at the reflecting state where the tag backscatters the modulated signal to the reader. These two states are determined on the tag chip by using a transistor to switch between the two different values of the tag's impedance [20].

The backscattered signal received at the reader is composed of two different components: antenna mode and structure mode. Antenna mode scattering rely on the load impedance of the tag's antenna, the phase and amplitude of the signal is modified. Figure 3 illustrates the structure of passive RFID tag and Figure 4 illustrates the equivalent circuit of RFID tag.

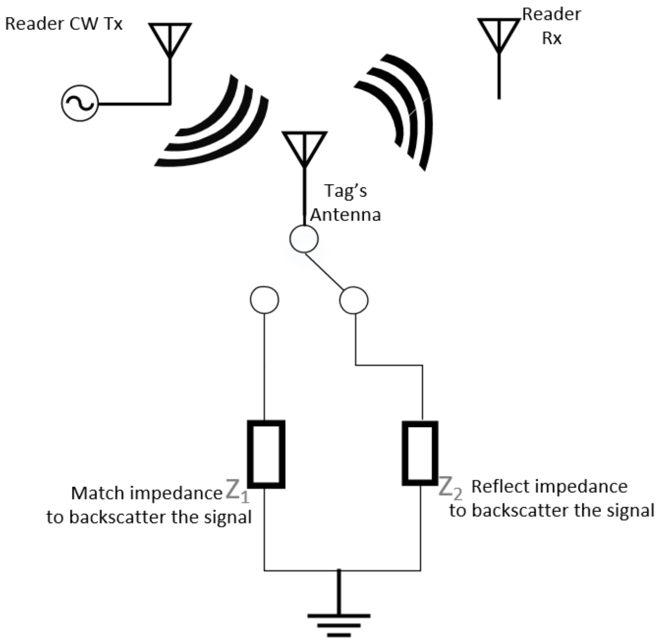

Reader CW Tx
Reader Rx
Tag's Antenna
Match impedance Z_1 to backscatter the signal
Z_2 Reflect impedance to backscatter the signal

Figure 3 General Circuit of Backscatter modulation between the reader and tag

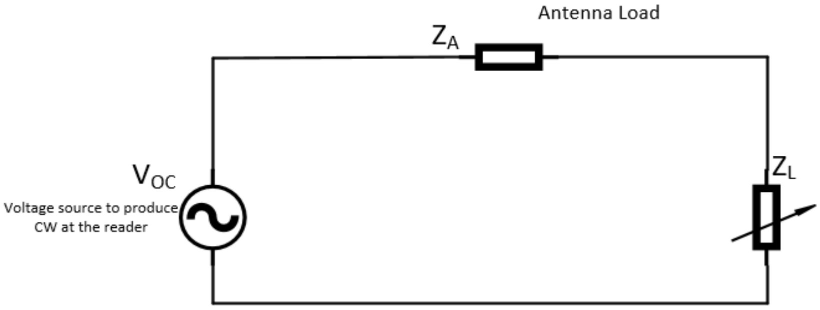


Figure 4 Equivalent Circuit to calculate the absorbed and reflected power at the tag

The backscatter field, $\xi_{scattered} = \xi_{scattered}^{M} - \Gamma I_M \frac{\xi_a}{I_a}$, where the equation indicates that the backscatter signal is degraded by the reflected signal from the tag. The reflection term, Γ is the combined reflection, which is the result of switching between Z_1 and Z_2. Moreover, the amount of power absorbed by the tag to power up depends on multiple variables such as the power of the signal at the reader side and the area of the tag antenna. The power absorbed by the tag can be analyzed using free space equations, where the power density of the electromagnetic wave at the tag's antenna following [17] is:

$$S = \frac{P_{RT} G_R}{4\pi r^2}, \tag{ 0-1}$$

where G_R is the gain of the reader's transmit antenna, P_{RT} is the transmitted power from the reader and r is the distance between the reader and the tag. Let the area of the tag's antenna be denoted by A_{Teff}, which is given by

$$A_{Teff} = \frac{\lambda^2}{4\pi} G_T, \tag{ 0-2}$$

where G_T is the gain of the tag antenna and λ is the wavelength of the CW. In this case, λ is taken at frequency in range of $860\ MHz - 960\ MHz$. The power received by the tag depends on the impedance of the antenna at that time. The antenna's impedance can have two different values; either Z_{match} or $Z_{reflect}$, denote $Z_{match} = Z_1$ and $Z_{reflect} = Z_2$. The switching between Z_1 and Z_2, determines the operating state of the tag; either absorbing or reflecting. The state can be determined by analyzing Figure 4 if $Z_A = Z_L$, then the power received by the tag is:

$$P_{TX} = SA_{Teff}. \tag{ 0-3}$$

When Z_A is connected to a different value of Z_L, then the tag is performing the reflection operation which is described as $Z_{reflect}$. In this operation, part of the power is re-radiated back to the reader, the reflected power is given by:

$$P_{TR} = KP_{TX} G_T, \tag{ 0-4}$$

where (0-5)

$$K = \frac{4R_a^2}{|Z_A + Z_L|^2}.$$

Similar to the received power at the tag, the received power at the reader also depends on the area of its antenna. Therefore,

$$P_{RX} = \frac{P_{TR}}{4\pi r^2} A_{Reff}. \quad (0\text{-}6)$$

where

$$A_{Reff} = \frac{\lambda^2}{4\pi} G_R \quad (0\text{-}7)$$

Thus, the backscattered power received by the tag is

$$P_{RX} = (\frac{\lambda}{4\pi r})^4 G_T^2 G_R P_{RT} \frac{4R_a^2}{|Z_A + Z_L|^2} \quad (0\text{-}8)$$

Switching between Z_1 and Z_2 is used to modulate the signal at the tag side, usually using BPSK modulation. This can be modified to achieve other modulation schemes such as QPSK modulation [21].

In general, the RFID reader communicates with the tag using modulation of Double Sideband (DSB) Amplitude Shift Keying (ASK) while the tag backsactters using ASK or Phase shift keying (PSK). Several research work have developed different modulation schemes at the backscatter link. In [22] BPSK modulator for RFID was developed, also QPSK was later developed in [23]. While developing any type of modulator other than the traditional ones, the designers must review the protocols [24]. In most applications, UHF tags are used and thus EPCglobal Class-1 Gen2 protocol is followed. EPCglobal Class-1 Gen2 protocol was developed for RFID with the objective of being lightweight and not requiring advanced computations as it only allows for simple passwords to secure the system. A brief description of the different protocols used in RFID is provided in the following section.

2.3 RFID Protocols and Standards

There are various types of protocols and standards developed for RFID systems. Those standards usually describe the physical and data link layers, covering different characteristics including the air interference, modulation schemes, anti-collision methodologies, communication protocols and security techniques. Despite that, the standards do not cover all the aspects required to deploy an RFID in different applications. Also, there is a clear absence in testing methods and application data.

Figure 5 [25] illustrates the different standards used for RFID systems and their main applications.

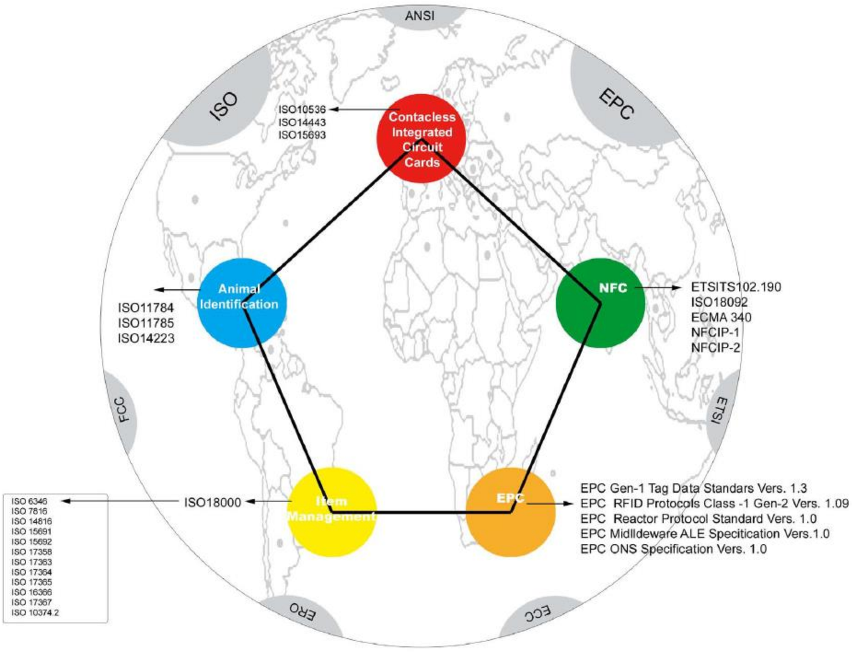


Figure 5 Standards for RFID systems

Some institutes develop their own standards for RFID based on the existing ones such as ISO/IEC, and modify them to meet the requirement of their applications. This is usually found in access control system, where each company modifies its system characteristics and database to comply with their requirements.

Most of the international standards are developed by International Organization for Standardization (ISO). Their standards cover the specifications for products, services and systems. While the International Electrotechnical Commission (IEC) prepares international standards for all electrical technologies. IEC provides assessment of compatibility to the standards in the field of electronic technologies such as RFID. A more specific standard for RFID, including item identification in general, is known as EPCglobal, which is a joint venture between the EAN international and UCC [26]. The EPC standard is commissioned for immediate reliable identification of any item in supply chain [27]. This has expanded to cover RFID in other applications. In this thesis, the review will focus on EPCglobal and its different classes for RFID tags.

Over the years, the EPCglobal standard has evolved and different versions were published. The most important standard proposed by EPCglobal is the EPCglobal generation-2 class-1 (EPCglobalC1G2) protocol. EPCglobalC1G2 defines the physical and logical requirements for passive backscatter components such as passive RFID tags that operates in $860 - 960\,MHz$ (the UHF range) [28] as described in pervious sections. The structure of EPCglobalC1G2 is presented in Figure 6. The network for EPCglobal consists of six essential components [29]: EPC code, tags or labels, readers, middleware, EPC information services, EPC discovery service and object naming service [30].

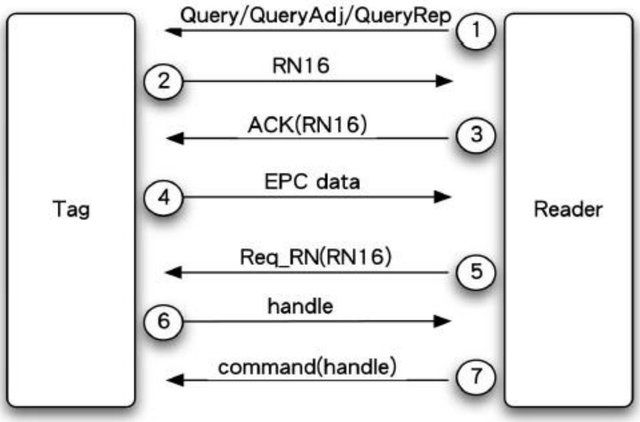


Figure 6 Structure of the EPCglobal G2C1 [31]

EPCglobal satisfies the industry requirement for an effective RFID network with its EPC infrastructure. Embedded in EPCglobal is the Hardware Action Group (HAG) which develops specifications for hardware components of any EPC network, including reader and tags in RFID system. The four classes of RFID are defined by the EPC system in Table 1 [17].

Table 1 The four classes of EPCglobal for UHF tags

Class	Passive/active	Features
Class 1	Passive	Tag identifier(TID), Kill function, Optional password protection
Class 2	Semi-active	TID,extended memory, authenticated access control,
Class 3	Semi-active	Integral-power-source, sensing circuity
Class 4	Active	T-T communication, active comm.,Ad-hoc and network capabilities

In the EPCglobalC1G2, the operating procedure includes some specific interfaces. These interfaces are divided into two types; physical interface and logic interface. The physical interface includes the following:

- Operational frequencies: The protocol is applied for UHF frequencies which operates in the range of $860 - 960\ MHZ$
- Reader to tag communications: The reader communicates with one or more tag by modulating an RF carrier signal using DSB-ASK, single sideband modulation (SSB)-ASK or Phase reversal (PR)-ASK. The modulation type shall be fixed during the transmission round.
- Tag to reader communications: The tag communicates with the reader using backscatter modulation, the procedure of backscatter coupling is described in section 2.2.

The logical interface includes the following:

- Tag memory: the memory shall be segregated into four banks: reserved memory, EPC memory, TID memory and user memory.
- Security timeout: Each tag may implement a security timeout after a failed access from the reader side.
- Tag states and slot counter: Each tag must implement a counter for its state and slot. From this counter, the reader will be able to obtain the state of the tag such as ready, open, acknowledged, secured or killed state.

Several researches have tried to develop a novel protocol to secure RFID system in various types of applications. Those developed protocols are usually designed to be lightweight for RFID authentication, especially for medical applications and IoT technologies. The work in [32] developed an authentication scheme for chip-less RFID in IoT applications. The protocol for chip-less RFID does not cover all the security attributes of the tag's privacy and security; where it only withstands tag impersonation and password decoding attacks. An advancement for this work was created in [33], where a lightweight RFID security protocol is developed based on Tian's protocol for medical privacy protection in IoT. This protocol achieves all the attributes required for the privacy of the tag. Moreover, in [34], an authentication scheme for cloud-based RFID healthcare system was developed. The security scheme in [34] is based on quadratic reSDuals and pseudo number generation. This protocol meets all the privacy and security requirements of a mobile RFID system with fewer resources in comparison with typical protocols. These protocols modify EPCglobalC1G2, to develop a secure network for different application but does not fully comply with the EPC protocol.

On the other hand, some protocols were developed that fully comply with the

EPC standard, but does not cover all the attributes of the tag's privacy and security. These protocols are: Chien protocol, Gossamer protocol, Xie protocol and Sarah protocol [33]. Although various protocols have been developed and tested, but none of them covered all the required aspects and complied with the EPC global standard, and thus, the practical deployment of RFID in multiple applications is still suspended. The different applications, where are RFID technology is employed, is discussed in the next section.

2.4 RFID Applications

Deploying RFID in several applications has been gaining popularity along the years. RFID technology is mainly meant for tracking applications. In addition to that, RFID is also used for payment, banking and access control by using contactless smart cards [35]. The applications listed below covers most of RFID applications either existing or emerging.

A. Supply chain

The use of RFID in supply chain management is actually one of the oldest applications of RFID, but the high cost of tags in contrast to barcodes has limited the use of tags to box or pallet tagging only. Despite the cost limitations, RFID in supply chain has regained the attention, especially after adoption by Walmart and other mass production warehouses. RFID tags provide lots of benefits for large warehouses considering the international shipping between countries, those benefits are [36]:

- Send advanced shipping notices to different branches of the warehouse.
- Mitigate goods loss by tracking all goods.
- Using real time monitoring of stock which improves the supply

management.

B. Access Control

RFID technology has been used to authenticate access to buildings, parkings, offices and safes in banks. Recently, most companies and institutes replaced conventional keys with card keys or electronic keys, which uses RFID passive tags [37]. These RFID cards are covered under the ISO/IEC 14443 standards and usually each company adds their cryptography layer to their card users database.

C. e-Payment and e-Passport

After the success and popularity of Visa cards and other forms of payment cards, the contactless smart cards technology has significantly developed. These cards deploy RFID technology to conduct the payment process by transmitting the data of the card by RF waves. Moreover, RFID is used in e-passports which are not technically a card but uses the same contactless IC chip found in smart cards. In e-passports, the information stored on the passport is transmitted to the RFID reader in places such as airports or any governmental institute [35].

D. Libraries

RFID can be used in libraries for tracking books and managing workflow between the staff. Other benefits of RFID in libraries include [36]:

- Perform books inventory without removing the books from their shelves, that is in contrast with barcode system.
- Check booking in and out.
- Maintain and monitor library inventory in real-time especially for borrowing and returning books.

The different applications of RFID are compared according to the tag type, frequency, reading range, and coupling method in Table 2 below.

Table 2 RFID technology categories and features [17, 35]

Frequency Band	Field Type	Reading Range	Coupling Method	Applications
LF (125 kHz)	NFC	0.1 m	Inductive coupling	Smart card, ticketing, access control, animal tagging and tracking
HF (13.56 MHz)	NFC	1 m	Inductive coupling	Secure ID cards (ePassport), credit and debit card payment, ePayment
UHF 865 – 868 MHz 902 – 928 MHz 433 MHz	FFC	2–20 m	Backscattering Coupling	Transportation vehicle ID, Inventory tracking, security, supply chain and healthcare devices
MF 2.4, 5.8 GHz	FFC	10 m	Electromagnetic coupling	Transportation vehicle ID, road toll, supply chain

The applications where RFID technology is used are not limited to those applications mentioned in the previous section. In fact, the applications of RFID are only limited by our imagination, as RFID tags can be deployed in a broad band of practical implementation scenarios. The reading range mentioned in Table 2 is for all types of tags, but for passive tags, the reading range is at the lower bound of the mentioned range. For example, the reading range for passive tags in UHF band is up-to 3m only.

Although, RFID is deployed in various applications in diverse disciplines, the deployment of RFID implementation within the framework of IoT and healthcare devices is strongly emerging, especially for implanted medical devices. The next section presents an inclusive review of RFID usage in healthcare applications.

2.4.1 RFID for Healthcare Applications

With the fast increase of population, patient's safety becomes a crucial concern in public health. Multiple hospitals claim that in 1 out of 300, there is a chance that the patient will be harmed due to medical errors. Usually the errors occur due to incorrect blood transfusion, inappropriate drug or even a misidentification of the patients and their records. RFID technology is considered the upcoming disruptive system in healthcare applications and offers multiple opportunities to increase patient's safety and cost savings [38]. However, RFID technology still lacks specific standards to be commercialized in hospitals, also it lags behind other wireless technologies in aspects of security and privacy [1, 39].

RFID technology can be deployed in several categories in healthcare applications. These categories include patient and drugs identification, monitoring and tracking, equipment and sensors tracking and blood transfusion [40]. In recent research, it is proposed to use RFID tags as implanted devices either implanted in the body or placed on the skin within the architecture of Body Area Networks (BAN). To develop implanted devices in the human body, the device should be small in size, passive, operate at low frequency to comply with the authorized SAR (Specific Absorption Rate) and most importantly to be secure and private [41]. All of these requirements are found in RFID systems as there are small passive tags and the system can operate at different frequencies including low frequency at range of (120-140kHz), the only missing requirement in RFID is the security and privacy especially when the tag is implanted in the body [42].

Some hospitals report errors of patient misidentification and is considered one of the main medical errors which are fatal if the patient is given an inadequate medicine. RFID can be used to assure positive identity of the patient by using a smart wristband with a passive RFID tag. The wristband can be scanned to present patient's information such as name, age, blood type and allergies. The wristband can also be used on surgical patients to ensure that the surgery will be performed on the correct patient [43]. RFID technology can also be used to track patients including elderly patients with chronic diseases or newborn babies to avoid baby snatching. In addition, RFID can be helpful in an epidemic to identify people who have been in contact with a carrier patient. In fact, RFID wristband was used during the Severe Acute Respiratory Syndrome (SARS) epidemic in Asian hospitals to determine people who contacted an infected patient [44, 45].

The research is currently emerging to integrate RFID technology with IoT based sensors to monitor and track patients. Collecting data from the sensors includes the patient's vitals such as blood pressure, temperature and heartbeat. Smart digital networks were developed by Show Chan hospital during the SARS epidemic [44]. The network used RFID active tags to monitor the patient’s temperature. Moreover, integrating RFID with wireless sensors can save a patient’s life in emergency scenarios as the physicians can monitor the patient’s vitals and if there is any irregular measure, help can be provided immediately. The benefits of RFID deployment in medical applications is described in Table 3.

Table 3. Benefits of RFID technology in healthcare applications [46-48]

Benefits	Examples
Mitigate medical errors and improves patient's safety	Reduce misidentification of patients and thus ensures that the patient will receive the right diagnosis and medication. Monitor drug dosage given for each patient.
Improved medical process	Monitor patient's waiting time, workflow of hospital staff, so that each patient will receive the required care
Real-time access	The Verichip has been approved recently which is implanted in patient's arm, by scanning the chip, the physician can obtain their medical records.
Time saving	Organize the workflow of the hospital, where the staff can know if a specific patient is receiving the care or not. And this reduces the time by 50% in the daily activities of the staff.
Cost saving	Monitor expiry date of drugs and thus reduce unnecessary waste. Reduce theft crimes of drugs and other components from the hospital.

Despite the benefits of RFID technology to healthcare applications, there are some challenges and limitations that obstruct the certification and adoption of RFID. These challenges are divided into different categories which are technological challenges as well as security and privacy challenges. Technological challenges include the EMI caused by RFID wireless transmission. EMI can interfere with other biomedical devices and impact their performance which might produce erroneous measures and cause a threat to patient's life. Moreover, the accuracy and reliability of RFID tags depend on several factors including the tag's placement, angle of rotation, read distance and if the object contains liquid or metal that might interfere with the measurement accuracy. Also, the material used to create the tag is not bio compatible. Moreover, the RFID technology still lacks multiple industrial standards and guidelines to be implemented in the healthcare industry [18, 4]. The barriers that is delaying the deployment of RFID in healthcare applications is mentioned in Table 4.

Table 4 Barriers obstructing deployment of RFID in healthcare applications [46]

Barriers	Examples
Privacy and security issues	Privacy concerns can include misuse of patient’s information due to the use of RFID technology. Security concerns include hacking patient’s medical records or attacking implanted devices such as pacemaker. From the ethical perspective, there are concerns regarding patients and institute privacy because of its tracking capabilities
Interference	RFID readers and tags may cause failure of electronic medical devices and sensors.
Ineffectiveness	Inaccurate read information, due to insufficient read range and existence of multiple tags.
Standardization	RFID deployment is mainly delayed due to lack of standards and protocols and it cannot be implemented in practical applications yet.
Other barriers	Lack of industrial support, no clear profit statistics from the investment, legal and ethical issues, current RFID systems are not compatible with hospitals requirements.

In healthcare sectors, security and privacy are crucial, while for RFID technology, security and privacy is the main challenging issue. Legally storing sensitive information about the patient violates the governmental regulations including Healthcare Insurance Portability and Accountability Act (HIPAA) as the tag will carry information about the patient insurance and other sensitive data. In addition, RFID tags are based on wireless communication which is vulnerable to eavesdropping. In fact, the security and privacy concerns are slowing down the deployment of RFID technology in healthcare sectors [49]. Even though, integrating RFID with IoT sensors will positively impact human wellbeing, but not enough researches addressed the security issues. In this thesis, the security and privacy concerns and approaches will be comprehensively reviewed, and a novel system model will be developed and analyzed.

2.5 RFID Security

RFID is rapidly developing and required for several applications in different industries. However, the deployment of RFID in some applications especially healthcare is delayed because of some limitations including operation and technical limitations such as security and privacy issues [50]. This section only focuses on privacy and security issues.

RFID tags are subject to different attacks including eavesdropping, hotlisting, replay attack, cloning, tag tracing, invading privacy, data frogging and denial of service [31, 51]. The most known attack is eavesdropping on the tag, where the eavesdropper can obtain the tag's information while the tag is backscattering to the reader. There are some traditional techniques developed to secure and ensure privacy in RFID tags including the kill technique. Killing the tag is successful at retail shops after the product is bought, the tag is killed or deactivated [51]. Although, the kill procedure assures privacy, it does not provide any post-purchase benefits for the customers. In addition to that, it can be used in object tracking such as borrowing books from library, the library should be able to track its books. To mitigate this issue, the sleeping technique was developed where the tag is deactivated temporary when the product is purchased. This solves the above-mentioned problem, but it does not really ensure customer's privacy [52]. In the sleeping technique, the reader can send a specific PIN to the tag which reactivates the tag. Development continues in [50], where the usage of tag password is discussed and the EPC protocol allows for simple password exchange between the reader and the tag. In this technique, the tag transmits its information only when it receives the correct password. However, the reader must know the tag identity to determine which password to send, hence this method is suitable in applications where the password is fixed; such as retail applications. Also, the password undermines the security of the system, because only simple passwords can be created with the RFID limited resources, which means they can be easily estimated by eavesdroppers. Advancement on this work was developed in [53], where tag pseudonyms method is used. The method is known as JP system, where a random pseudonym is generated and thus the communication between the reader and the tag is encrypted. The JP method was enhanced in [54], because RFID system requires multiple keys or pseudonym. The new method is known as universal key method. The universal key method requires encryption cipher text to ensure a secure system, which will cost beyond acceptable range for RFID systems. Also, to utilize a sophisticated cryptography techniques, a complex password and an advanced processors are needed, which are not suitable for inexpensive passive tags. In addition to that, traditional cryptography methods cannot be applied for RFID system due to the resources limitation of the system. These limitations are due to the fact that RFID tags are very constrained devices, with limitation in power consumption, storage and circuitry. As a result of these limitations, the traditional cryptography techniques including hash function such as MD5 and SHA-1 cannot be applied in RFID systems [8, 51]. These issues and constrains emerged a novel approach to secure RFID and backscatter systems through the physical layer. Several research works have used PLS to secure RFID systems by exploiting the nature and characteristics of backscattering systems. The work in [55] [56] developed PLS of MIMO RFID systems by proposing a noise injection mechanism to guarantee system security against eavesdropping, while considering the nature of backscatter systems. In [57], a novel and eavesdropping resilient method based on random modulation schemes and channels was developed to secure RFID systems by implementing multiple antennas.

The concept of PLS emerged from the limitations and constraints offered in cryptography and secret key generation methods. These constraints include the challenge of managing and distributing secret keys especially in a large decentralized wireless system. Also, high security is required in some applications which will require longer key lengths which is a waste of resources especially in a resource constrained system such as RFID and IOT [58, 59]. More importantly, traditional cryptography and encryption methods are not adequate with RFID and IoT systems because they require advanced processors and power which is limited in both systems. Therefore, the research on RFID communication security is focused on using physical layer security which provides key-less secure communication network. The first PLS research work used SINR to secure the system where its required for the legitimate receiver to have higher SINR than the eavesdropper [9]. The SINR approach provides a secure network under some conditions including that the eavesdropper has a degraded channel compared to the tag which cannot be guaranteed in practice due to uncertain locations of the receiver and the channel fading which may cause a better channel at the eavesdropper. Also, the SINR at eavesdropper (Eve) can be higher if its closer to the reader than the tag. Moreover, if the eavesdropper has an advanced and sensitive processor, it can detect the noise signal and eliminate it and thus decode the correct signal. PLS can be achieved using complex key-based approaches enabled by channel sharing via exploiting the channel reciprocity property. The survey in [3] offers more details about this approach. This thesis focuses on the SINR approach only.

The main concept of SINR approach is to provide secrecy when Eve's channel has lower SINR than the tag. The SINR technique can be enabled by injecting artificial noise signals. The advantages of SINR techniques include, system secrecy without the need for secret-key sharing and most of the processing occur at the transmitter side which is required in RFID system since tags are usually passive. The artificially noise injection can be implemented in time, frequency and space domains. This thesis will only discuss the noise injection in space domain, where noise injection is implemented using multiple antennas or antenna arrays in MIMO or MISO models. The first approach for AN (Artificial Noise) scheme was developed in [60, 61] where the signal is sent to the tag and an interference noise is sent in the direction of the eavesdropper. This method can be achieved by transmitting the noise in the null space of the reader-tag channel; thus it will only distort the signal at the eavesdropper. Also, in [62] another AN scheme was developed but in this case, it does not require using the null space; therefore, it can be called null-space independent scheme. Transmitting the noise in the null space of the legitimate channel has several merits including providing secure network in fading and non-fading channels. Also, the injected noise will not degrade the signal received at the tag, which means less processing at the tag side. On the other hand, the AN scheme has some drawbacks including the assumption that the transmitter knows the full CSI of the system and this is not always practical. The main drawback in AN scheme is that it requires the reader to have more Degrees of Freedom (DoF) than the tag and the eavesdropper. The DoF in this case is modeled as multiple antennas. This means that the number of antennas at the transmitter must be higher than that at the tag and eavesdropper. If the number of antennas at the eavesdropper is higher than the reader, the eavesdropper will be able to estimate the noise signal and cancel it and thus retrieve the correct signal. An inclusive description of various PLS techniques are presented in Figure 7.

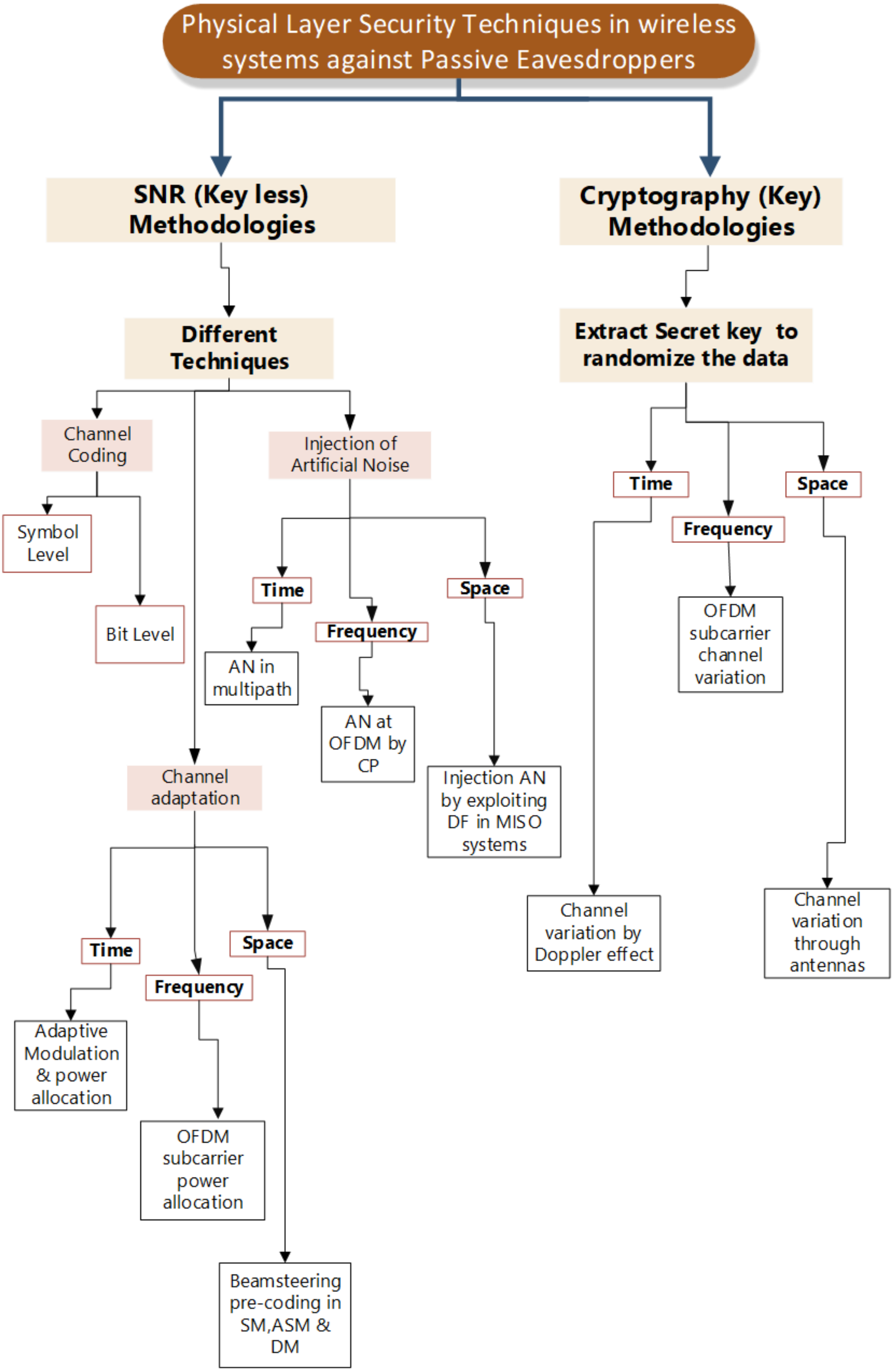

Physical Layer Security Techniques in wireless systems against Passive Eavesdroppers
SNR (Key less) Methodologies
Cryptography (Key) Methodologies
Different Techniques
Extract Secret key to randomize the data
Channel Coding
Injection of Artificial Noise
Symbol Level
Bit Level
Time
Frequency
Space
AN in multipath
AN at OFDM by CP
Injection AN by exploiting DF in MISO systems
Channel adaptation
Time
Frequency
Space
Adaptive Modulation & power allocation
OFDM subcarrier power allocation
Beamsteering pre-coding in SM,ASM & DM
Time
Frequency
Space
OFDM subcarrier channel variation
Channel variation by Doppler effect
Channel variation through antennas

Figure 7 Physical Layer security techniques

The different techniques mentioned in Figure 7 can be deployed for several applications through the three different resources domain of time, frequency and space. Two or more techniques can be combined to form a hybrid technique.

In this thesis, a hybrid technique is formed by using Beamforming and DM from channel adaptation and injecting artificial noise by exploiting a degree of freedom from AN injection.

There are several research works that developed secure systems through the physical layer for MIMO systems. In [63], the AN scheme was used alongside with a single antenna helper. This work was further advanced in [64] by using multiple antennas for jamming the signals. Also, the AN scheme was developed for the MISO model in [65], which is easier to construct because the transmitter has more antennas than the receiver and thus guarantee positive secrecy. The previous works assume CSI at the transmitter side to send the noise signal in the eavesdropper's direction, but this is not practical. So the work in [66] developed another AN scheme that only requires CSI of the legitimate receiver. All the previous work is based on the concept of injecting artificial noise that can only affect the eavesdropper, which is done by combining artificial noise and beamforming. In beamforming the signal is sent to the desired direction only and other directions would receive a distorted signal. Advancement of beamforming was carried in [67], where randomized beamforming was conducted and then developed under a different name called Artificial Fast Fading (AFF) in [68]. The results of this work showed that the AN scheme preforms better than AFF when the eavesdropper has less antennas than the transmitter. But AFF, preformed better when the eavesdropper has more antennas than the transmitter. For optimum results, AN and AFF schemes were combined. The drawback of beamforming, is that the noise is projected along all directions and thus if the eavesdropper is sensitive enough, it can eliminate the noise and retrieve the data [69, 70].

2.5.1 Directional Modulation

Directional modulation is an emerging technique for securing wireless systems from the transmitter side on the physical layer. The transmitter in DM is capable of projecting intentionally distorted signal along all directions except the direction of a prior selected desired direction. In this technology, the complex-domain antenna pattern is used to provide directional security where in the desired direction, the antenna pattern is set to have the same complex value of the transmitted symbol. Thus, the information signal is received correctly at the desired direction while other directions receives distorted signal. A basic scheme for DM is illustrated in Figure 8.

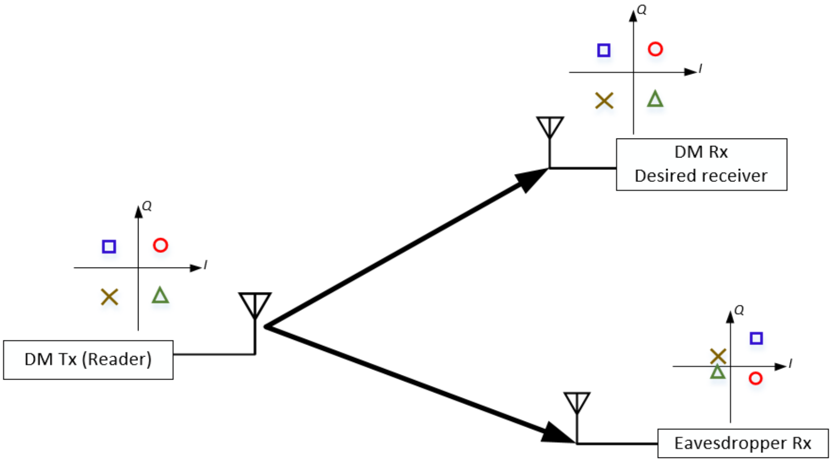


Figure 8 General system model of DM with QPSK modulation

The DM transmitter depends on having an antenna array and the element type as well as the structure of the antenna determine the type of the DM transmitter. Previous research work in [71] [5], designed the DM transmitter by using parasitic antenna array which includes passive reflectors that are coupled to the center of the antenna, this method is known as the Near-Field Direct Antenna Modulation (NFDAM). In NFDAM, the boundary of the near field antennas is manipulated using switches where the phase and amplitude of the antenna pattern is modulated at far-field which can be translated as constellation points in the IQ space. NFDAM DM transmitter is a time consuming and complicated method. It also requires a lot of passive reflectors which is a limitation for using DM in microwave. Also, using parasitic antenna arrays complicates the synthesis process in DM systems as trial and error methods are used to find the pattern of the elements or the electromagnetic characteristic of the elements to be used. As a result, the pattern calculations is complicated and consumes a lot of time.

In [72], active elements antenna array are used to produce a DM system. In this method each active element is activated by a CW and switches are added to change the phase and amplitude of the signal in the desired direction to match that of the symbol. Using active element arrays simplifies the synthesis calculation [5, 71], because once the pattern of the active elements are found, simple calculation are conducted to generate the adequate modulation scheme in a specific direction. The above two DM structures have some limitations in the case of various modulation schemes and multiple desired directions due to the limited number of antennas that can be implanted in the system [73].

To overcome the limitations mentioned in the above two structures, phased arrays are introduced to DM systems. In phased array topology, there are multiple radiating or active elements, where each element has a phase shifter of its own and the summed beam of all elements is directed in the desired direction. In conventional phased array systems, the information signal is transmitted in all directions but with higher SNR at the desired direction than that at other directions. This method achieves directional security but not at the physical layer, because the synthesis is conducted at baseband level. Also, since modulation is conducted at baseband and the signal only varies in power level, the eavesdropper can easily obtain the information from the modulated signal if it has higher sensitivity. In contrast with conventional beamforming, in DM the modulation occurs at the antenna level which steers the information beam, while in BS only the radiation pattern is steered [72, 73]. Hence, the digital modulation constellation diagram is distorted in undesired directions and it becomes hard for the eavesdropper to decode the information signal. Also, the complex weight vectors that scale the antenna array is changing based on the rate of change of the channel while in DM, it is changing according to the symbol rate.

Phased array topology for DM was developed in [4], where they created a multi-directional system using a QPSK scheme. In the efforts to optimize the synthesis of DM and reduce the complexity of multiple antenna schemes, the work in [69] used Antenna Subset Modulation (ASM) as a low complexity DM technique. Also, all research work about DM assumes perfect angle estimation which is not practical and this was analyzed in [74], where a robust low complex system that correct the angle estimation errors is developed. To optimize the synthesis process of DM transmitters, OFDM was exploited to produce direction sensitive pulse modulation in a US patent [75]. As an advancement to the work in [75], a vector representation for DM synthesis was developed in [76] to exploit the use of OFDM in DM systems. In [76], the destructive interference in the IQ space in undesired directions can be divided into two categories; static and dynamic interference, where static interference is constant during the whole transmission sequence and dynamic interference is updated according to the information symbol rate. The simulation results show that the dynamic interference achieves better system performance. The work in [77] combines both dynamic and static interference and shows that the combined interference in the undesired directions outperforms the output of dynamic interference only. The concept of interference is derived from the artificial noise injection scheme that was described in [78, 79] for multi-antenna passive eavesdroppers. Then the AN scheme was implemented in DM systems in [80], where the AN is projected in the null space of the desired direction channel; hence the noise is only received at the eavesdropper. In other work, the DM was transmitted in the null space of the eavesdropper which achieves the directional security, but it requires knowledge of the Channel State Information (CSI) of the eavesdropper, which is not practical. Hence, most work transmit the artificial noise vector in the null space of the desired direction channel. There are several DM synthesis methods developed in previous work that can be summarized as described in the next section.

2.5.1.1 DM Transmitter Synthesis Approaches

DM transmitter arrays are divided into two categories, either passive transmitters or active ones. The previous work for passive DM transmitter arrays did not develop any efficient DM synthesis process other than trial and error. On the other side, the research work on active DM transmitters have developed multiple techniques for DM synthesis process [81]. The main synthesis approach developed uses the orthogonal vector approach which is the difference vector between two vector paths picked to achieve the same standard constellation pattern in IQ space. The vector difference is defined as the orthogonal vector to the desired channel vector conjugant [76]. In addition to that, another concept related to orthogonal vector is artificial noise which is known as artificial orthogonal vector injection. The noise scheme has been developed to degrade the signal received by the eavesdropper by injecting artificial noise that is designed to be nulled in the legitimate receiver direction. The orthogonal vector approaches are compatible with both static and dynamic DM transmitters. There are subset categories under the orthogonal vector approach including BER-driven [82], Far-field radiation pattern and non-iterative synthesis [83]. Each subcategory has its own requirements and applications. In this thesis, the artificial orthogonal vector injection is used to develop the DM technique for RFID technology in 0.

In order to measure the performance of different DM techniques and compare them, there are various metrics to be used. The work in [84] describes the different metrics which are Error Vector Magnitude (EVM), Bit Error Rate (BER) and secrecy rate. The comparison done in [84] shows that BER and secrecy rate are the most appropriate for DM system [85].

In all of the above work, transmission was conducted in one direction and only using low order modulation schemes, mostly a QPSK scheme. The work in [70, 86] presents high order modulation and the work in [87, 88] provide multi-direction transmission by using DM techniques. In addition to that, DM technology was only developed for line of sight models (LOS), since applying DM in a multi-path fading channels is a complicated procedure. The work in [4] vaguely mentions the modifications required on the far-field pattern to be applied in multipath fading models. Moreover, the work in [89] provides an experimental work for multipath fading models facilitated by retrodirective antennas. All the related work developed for DM techniques focuses on classic wireless communication systems, and to the best of our knowledge, addressing DM for RFID systems is first done in this thesis.

In this thesis, a novel security method is proposed to secure RFID system through physical layer. Considering a generic RFID system, the main idea is to develop a DM technique to secure RFID systems considering the resources limitations in RFID. The novelty with respect to the state-of-the-art in DM technique is, on one hand , the deployment of DM in RFID applications and on the other hand, the ability to completely handle the DM technique from the reader side and eliminate any additional cost and complexity [90].

2.6 Assumptions in the thesis

The main assumptions considered in this thesis are the following:

- The RFID channels are independent and identically distributed following Rayleigh distribution.
- The eavesdropper is a passive device with a single antenna.
- The channel of the eavesdropper is independent from the channel of the legitimate tag and thus have different phases.
- Perfect estimation of the direction's angles at the transmitter.
- The eavesdropper's CSI is not known by neither, the reader nor the tag.

2.7 Relevant Work

In various cases, physical layer security mechanisms have been used to secure RFID systems against eavesdropping or any other attack. First in [9], the nature and characteristics of the backscatter network were investigated. Then by using the noise characteristic of the system, artificial noise was injected from the reader side to jam the eavesdropper and distort the signal received by it. This scheme achieves RFID tags security by distorting the signal received by the eavesdropper considering the tag is passive and that the reader is equipped with noise attenuation, which allows the reader to remove the injected noise while it will remain at the eavesdropper signal.. Thus, only the reader can retrieve the tag's information while eavesdropper will receive a noisy signal. In this work, the security of the RFID is achieved in limited cases including, the case where the reader is equipped with noise attenuation and assuming the eavesdropper is passive; however, the advantage is that the system remains secure even when the distance between the reader and tag increased. The system's security failed when the eavesdropper was equipped with directional antenna where it can direct all of its gain towards the tag only and thus will not receive most of the injected noise transmitted by the reader and in order to inject enough noise that can affect the eavesdropper, the reader must inject very high noise power which exceeds the power capabilities of the RFID, knowing that the reader's power is limited to $30dBm$. This problem was solved in [56], where the reader was equipped with multiple antennas, which guarantee system security even if the eavesdropper has a directional antenna. However, if the eavesdropper is capable of estimating the noise signal scheme, it can easily detect the tag's information. Also, multiple antenna techniques only works if the reader has more antennas than the eavesdropper, otherwise the system's security will fail. To enhance the security of RFID systems, [57] developed a novel and eavesdropping resilient scheme by randomizing the modulation scheme and channel using multiple antennas. Although randomizing the modulation scheme and channel improves the system security, the system still fails if the eavesdropper is equipped with more antennas than the reader. The performance in [9] and [56] can be improved by exploiting another DoF in the system by deploying the DM technique, which is the objective of this thesis.

2.8 Thesis Contributions

The main contributions of this thesis are briefed in the hereafter, and will be portrait in the following chapters.

2.8.1 Beam steering and Noise Injection for RFID

A novel security technique for RFID system is proposed in order to secure the tag's signal at the legitimate reader and distorting it at any other direction. It is a common technique to secure RFID by injecting artificial noise from the reader side but that showed inadequate performance due to RFID power limitations. In this design, the tag is equipped with beamsteering technology while the reader is injecting artificial noise. Using beamsteering alongside with injected noise guarantees power optimization. Numerical results are presented to show the effectiveness of the proposed technique, which outperforms the existing methods of securing RFID systems and reducing the power required by the reader. This contribution has been published in [91].

2.8.2 Directional Modulation for RFID

The thesis presents a more adequate and practical technique to secure RFID system by using DM at the reader side. This technique is more practical for most of the RFID applications since RFID tags are simple passive devices and usually are not equipped with any advanced equipment such as multiple antennas. More importantly, all the processing is conducted at one side, which is the reader, and that maintains the simplicity of the RFID system. In this design, the RFID reader is equipped with multiple antennas to transmit its signal correctly to the tag and scramble it at any other direction. Also, in DM, the injected artificial noise is designed to be in the null space of the desired channel, thus only the undesired direction will be affected by the noise. Numerical results are presented to show the performance of the DM technique in securing RFID systems.

2.8.3 Parameters used in both contribution chapters

There are some parameters that are common in both contribution chapters that include the number of elements of the antenna array, the number of symbols generated for simulation and the pattern of the beamsteering vector. Thus, the number of elements considered at the antenna array is 5 elements, the number of symbols used in simulation generation is 10^3 and the pattern of the beamsteering vector is illustrated in Figure 9 to Figure 11.

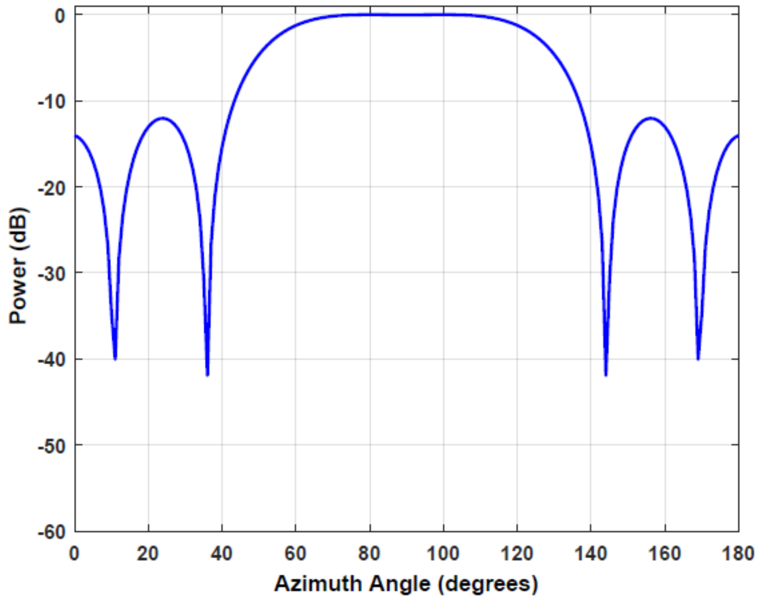


Figure 9 Magnitude power of Beamsteering vector at θ=80°

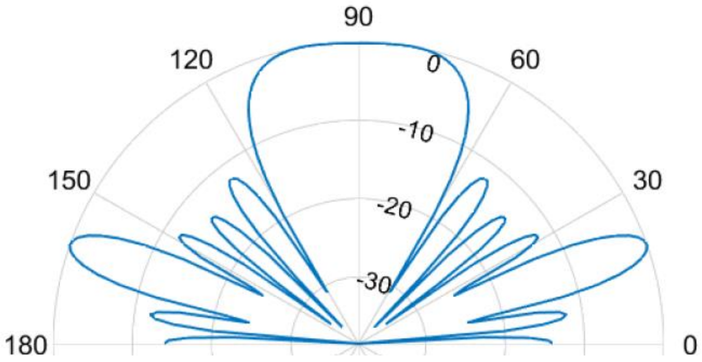


Figure 10 Beamsteering Pattern from antenna array

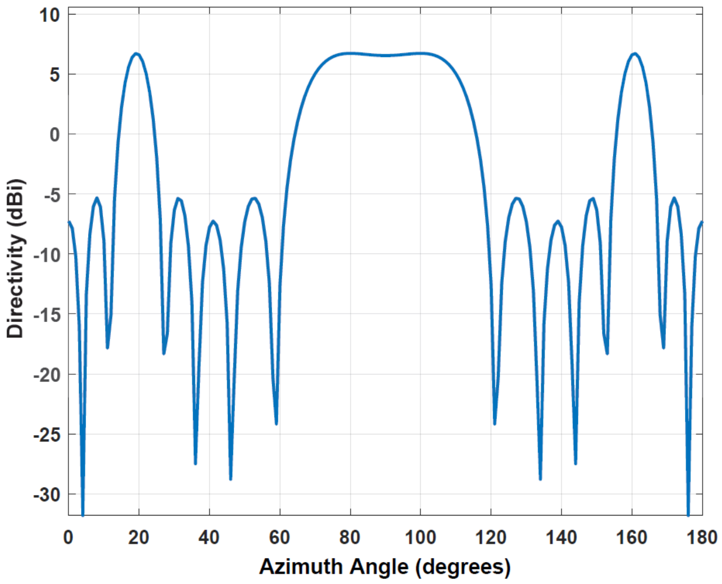


Figure 11 Directivity of the Beamsteering Vector

Figure 9 illustrates the magnitude of the beamsteering vector and it is shown that the magnitude is highest at the desired location $\theta = 80°$. The beam has the same magnitude from $\theta = 73° \; to \; \theta = 105°$ which complies with the BER values obtained in the results in the following chapters.

CHAPTER 3: BEAMSTEARING AND NOISE INJECTION FOR RFID

In this chapter, a novel physical layer security scheme is proposed to secure the information signal in RFID systems. In this scheme, a hybrid system is constructed where beam-steering and noise injection are utilized to secure an RFID system. The motivation for such a scheme is twofold as previously discussed. First, the processing and power limitation in RFID are conquered by using PLS. Second, the requirement on artificial noise power value is reduced by adding the beamsteering technique in the system. In this scheme, the signal is secure only at the intended direction and distorted in all other directions. The contributions in this chapter can be summarized as follows:

- Securing RFID at the physical layer by exploiting spatial characteristics at the tag and exploiting noise characteristics at the reader. This is accomplished by equipping the tag with multiple antennas and injecting artificial noise from the reader.
- The tag backscatters its secret signal correctly to the reader location only and scrambles it at any other direction. The reader is capable of eliminating the injected noise and thus the noise only affects the signal received at the eavesdroppers.

3.1 System Architecture for RFID with Beamsteering

Consider a backscatter RFID system with a single reader, single tag and single eavesdropper. The reader is equipped with a single transmit and single receive antenna, while the tag is deployed with a linear one dimensional (1-D) antenna array with N elements that are exploited for beamsteering (BS). The transmitted signal uses QPSK modulation. It is assumed that the eavesdropper has a single receive antenna and is located at θ_E from the tag. $\theta_E \in (0,180)$ but $\theta \neq \theta_R$, where θ_R is the spatial angle from tag to reader.

The RFID backscatter communication system is shown in Figure 12.The reader continuously transmits an excitation signal to power up the tag. The tag modulates the reader signal and backscatters its information to the reader. As assumed in this system, the tag is a passive device, but for this design it is assumed to have a special hardwired circuitry and antenna array to conduct the BS technique. BS at the tag is designed as follows: during backscattering, the BS signal results in a strong decodable information signal only in the direction of the reader at θ_R and weak/null in all other directions. Figure 13 shows the system, where the tag has multiple antennas and backscattering its signal through multiple channels to the reader. Since the tag has multiple antennas, in this design it has 5 antennas, each antenna receives a different version of the signal, which are shown in Table 5.

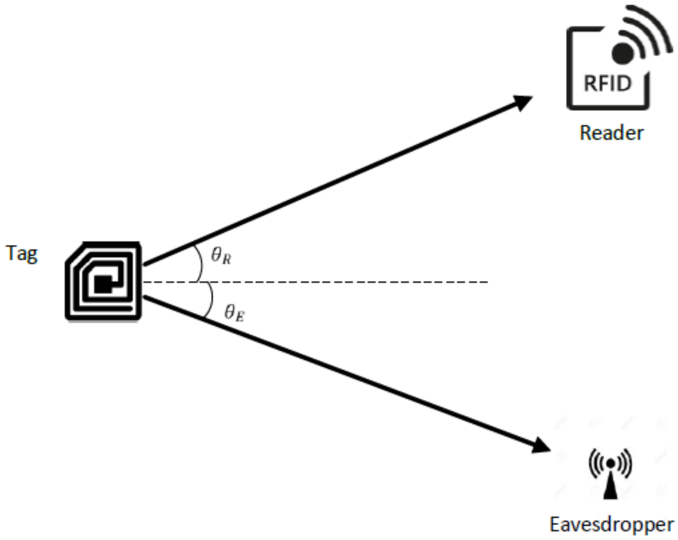


Figure 12 Communication links between reader, tag and eavesdropper

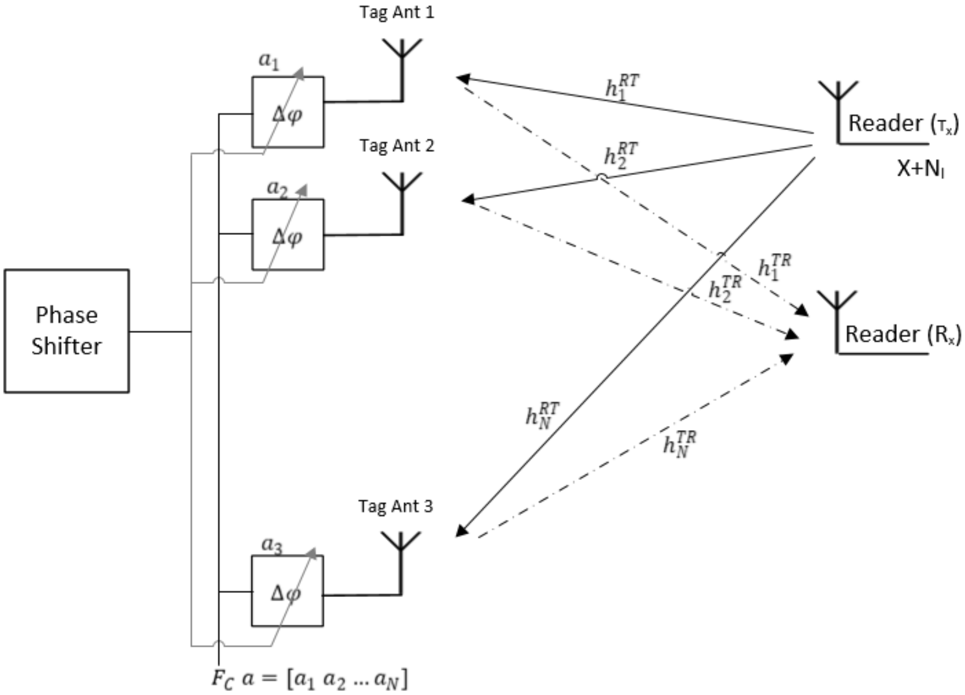
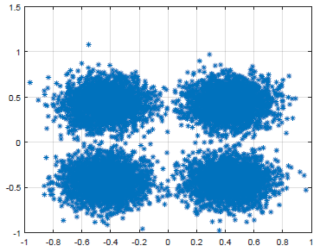
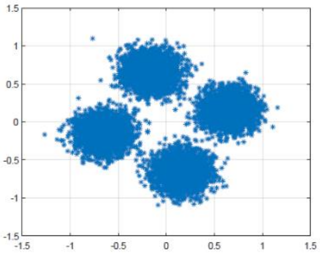
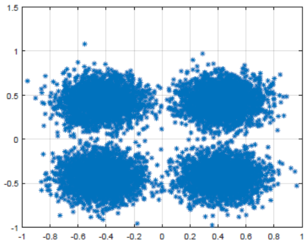
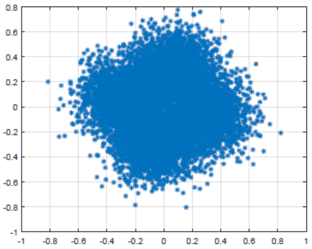
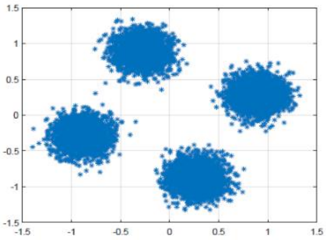


Figure 13 System model of BS exploited at the tag

Table 5 Constelation patterns at each element of the tag's antenna

Number of Tag’s antenna	Constellation pattern at that antenna
Constellation pattern received at Ant 1	
Constellation pattern received at Ant 2	
Constellation pattern received at Ant 3	
Constellation pattern received at Ant 4	
Constellation pattern received at Ant 5	

3.2 System Model for RFID with Eavesdropper

In general RFID system, the signal received at the reader following [9] is:

$$y_R = h_{RT}h_{TR}xs + N_R + N_T h_{TR}, \qquad (0\text{-}9)$$

where x is the signal sent from the reader, s is the confidential message from the tag carrying its secret information, h_{RT} is the channel from reader to tag, h_{TR} is the channel from tag to reader and N_R and N_T are the additive white Gaussian noise (AWGN) at the reader and tag receivers, respectively. The signal-to-noise ratio (SNR) at the reader following [9] is:

$$\gamma_R = \frac{P_x \Gamma G_{RT}^2 K^2 d_{RT}^{-4}}{\sigma_R^2 + \sigma_T^2 G_{RT} K d_{RT}^{-2}}, \qquad (0\text{-}10)$$

where P_x is the signal power from reader to tag. Γ is the coefficient of the reflected signal radiated from the tag side, G_{RT} is the combined antenna gain of the reader-tag link, d_{RT} is the distance between reader and tag, K is a constant which depends on the carrier wavelength λ, where $K = (\frac{\lambda}{4\pi})^2$, and σ_R^2 and σ_T^2 are the AWGN variances at the reader and tag receivers, respectively.

The signal received at the eavesdropper is:

$$y_E = h_{RT}h_{TE}xs + h_{TE}N_T s + N_E, \qquad (0\text{-}11)$$

where h_{TE} is the channel between the tag and the eavesdropper and N_E is the AWGN noise at the eavesdropper's receiver.

The SNR at the eavesdropper is:

$$\gamma_E = \frac{P_x \Gamma G_{RT} G_{TE} K^2 d_{RT}^{-2} d_{TE}^{-2}}{\sigma_E^2 + \sigma_T^2 G_{TE} K d_{TE}^{-2}} \qquad (0\text{-}12)$$

where G_{TE} is the combined antenna gain of the tag-eavesdropper link, d_{TE} is the distance between the tag and the eavesdropper and σ_E^2 is the AWGN noise variance at the eavesdropper’s receiver.

The artificial noise injection scheme for RFID was developed in [9]. let z be the noise injected from the reader side. The signal received at the tag is:

$$y_{RT} = h_{RT}x + h_{RT}z + N_T. \quad (0\text{-}13)$$

The backscattered signal from the tag to the reader is:

$$y_{TR} = h_{TR}y_{RT}s + N_R \quad (0\text{-}14)$$

$$y_{TR} = h_{TR}h_{RT}xs + h_{TR}h_{RT}zs + h_{TR}N_Ts + N_R. \quad (0\text{-}15)$$

The SNR at the reader is modified after adding the artificial noise following [9] and can be written as:

$$\gamma_R = \frac{P_x\Gamma G_{RT}^2K^2d_{RT}^{-4}}{\chi P_z\Gamma G_{RT}^2K^2d_{RT}^{-4} + \sigma_R^2 + \sigma_T^2G_{RT}Kd_{RT}^{-2}}, \quad (0\text{-}16)$$

where P_Z is the power of the injected noise from the reader side. The reader can attenuate the injected noise (since it is known to the reader) by a factor χ, where $0 \leq \chi \leq 1$, while the eavesdropper cannot eliminate the noise (unknown to eavesdropper) and therefore receives a distorted signal.

The tag's signal received at the eavesdropper after adding the artificial noise is:

$$y_E = h_{RT}h_{TE}xs + h_{TE}h_{RT}zs + n_E + n_Th_{TE}s \quad (0\text{-}17)$$

and the SNR received at the eavesdropper is:

$$\gamma_E = \frac{P_x\Gamma G_{RT}G_{TE}K^2d_{RT}^{-2}d_{TE}^{-2}}{P_z\Gamma G_{RT}G_{TE}K^2d_{RT}^{-2}d_{TE}^{-2} + \sigma_E^2 + \sigma_T^2G_{TE}Kd_{TE}^{-2}}. \quad (0\text{-}18)$$

3.3 System Model for RFID with Beamsteering

Adding the BS technique to RFID system allows the tag to transmit its secret information only at the desired direction at θ_R and attenuated/eliminates it at all other directions. In order to conduct BS, a beamforming vector can be constructed following the model in [76, 77] as described below:

Let the desired channel between the tag and the reader be:

$$H_{\theta_R} = \left[e^{j2\pi\cos\theta_R} \;\; e^{j\pi\cos\theta_R} \;\; e^{j0} \;\; e^{-j\pi\cos\theta_R} \;\; e^{-j2\pi\cos\theta_R}\right]. \tag{ 0-19}$$

Choose the beamforming vector to be:

$$P = \frac{h_{TR}(\theta_R)}{||h_{TR}(\theta_R)||}. \tag{ 0-20}$$

If the signal is received at any other direction other than θ_R, P will not be normalized and thus distorts the signal.

In the next section, the implementation of NI and BS combined will be analyzed.

3.4 BER Analysis for RFID with Beamsteering and Noise Injection

The novel proposed PHY layer security technique for RFID system, deploys combined NI and BS schemes. The BS scheme is exploited at the tag side, while the artificial noise is injected from the reader side. The BS technique assures that the signal is correctly received at the reader direction only and the injected noise assures that; even if the eavesdropper has knowledge of the reader location, the signal will still be distorted due to the injected AWGN noise. The injected noise does not affect the signal received at the reader, because the reader is equipped with noise elimination capability with factor χ where $0 \le \chi \le 1$ since it has knowledge of its own injected noise. By appending the combined technique to RFID system, the signals received at the reader and eavesdropper will be according to the following:

Signal received at the reader:

$$y_R = h_{RT}h_{TR}H_{\theta_R}Pxs + h_{RT}h_{TR}H_{\theta_R}Pzs + N_R + N_T h_{TR} \tag{ 0-21}$$

$$y_R = h_{RT}h_{TR}H_{\theta_R}\frac{H_{\theta_R}}{\| H_{\theta_R} \|}xs + h_{RT}h_{TR}H_{\theta_R}\frac{H_{\theta_R}}{\| H_{\theta_R} \|}zs + N_R + N_T h_{TR}. \tag{ 0-22}$$

Signal received at eavesdropper:

$$y_E = h_{RT}h_{TE}H_{\theta_E}Pxs + h_{RT}h_{TE}H_{\theta_E}Pzs + N_E + N_T h_{TE} \tag{ 0-23}$$

$$y_E = h_{RT}h_{TE}H_{\theta_E}\frac{H_{\theta_R}}{\| H_{\theta_R} \|}xs + h_{RT}h_{TE}H_{\theta_E}\frac{H_{\theta_R}}{\| H_{\theta_R} \|}zs + N_E + N_T h_{TE}, \tag{ 0-24}$$

where θ_E is any undesired direction from the tag where the eavesdropper is located. Accordingly, the SNR at the reader and eavesdropper are given according to the following:

The SNR of the signal received at the reader:

$$\gamma_R = \frac{\| Pxs \|^2 \, G_{RT}G_{TR}K^2 d_{RT}^{-4}}{\chi \| Pzs \|^2 \, G_{RT}G_{TR}K^2 d_{RT}^{-4} + \sigma_R^2 + \sigma_T^2 G_{RT}K d_{RT}^{-2}}. \tag{ 0-25}$$

The SNR of the signal received at the eavesdropper:

$$\gamma_E = \frac{\| Pxs \|^2 \, G_{RT}G_{TE}K^2 d_{RT}^{-2} d_{TE}^{-2}}{\| Pzs \|^2 \, G_{RT}G_{TE}K^2 d_{RT}^{-2} d_{TE}^{-2} + \sigma_E^2 + \sigma_T^2 G_{TE}K d_{TE}^{-2}}. \tag{ 0-26}$$

There are several metrics to measure the performance of the system, for this design, BER will be used to assess the performance of the system. BER for QPSK scheme is:

$$BER_{QPSK} = Q(\sqrt{2\gamma_b}) \tag{ 0-27}$$

where γ_b is the SNR per bit.

3.5 Numerical Result and Discussions

In this section some numerical results are presented, to show the performance of the proposed combined beamsteering and noise injection technique. Prior to discussing the results, the design parameters are defined as the following. The reader is on spatial direction $\theta_R = 80^0$ from the tag, the SNR along the desired direction is $15dB$, the injected noise is $10dBm$, the reader is able to cancel 90% of the injected noise (i.e $\chi = 0.1$) and the size of data stream is 10^3modulated symbols. The BER of the eavesdropper is evaluated at two different locations close to the reader; $\theta_{E1} = 90^0$ and $\theta_{E2} = 65^0$. The proposed approach beam steering/noise injection will be referred to by (BS-NI).

The presented results in Figure 14-Figure 19 have been obtained by averaging the BER over 100 runs with 10^3 symbols. The fading of the channels is not considered in this approach and thus, the performance is evaluated in free space (upper bound on fading channel performance). Moreover, quadrature phase shift keying (QPSK) modulation scheme is assumed.

Figure 14 compares the BER performance of the proposed approach of BS-NI at the eavesdropper side with the BS-only and the injected noise only techniques. The comparison is accomplished by evaluating the BER versus SNR for each technique. Also, the BER versus SNR is analyzed at different locations of the eavesdropper. The performance of the noise injection scheme does not depend on the location of the eavesdropper but on the value of P_z. This is why it is only shown at one arbitrary angle. The performance of NI is better than that of BS-only but worse than that of BS-NI with the same value of P_z. It shall be noted that, if the eavesdropper has more antenna than that of the tag, NI would fail as a securing technique [68].

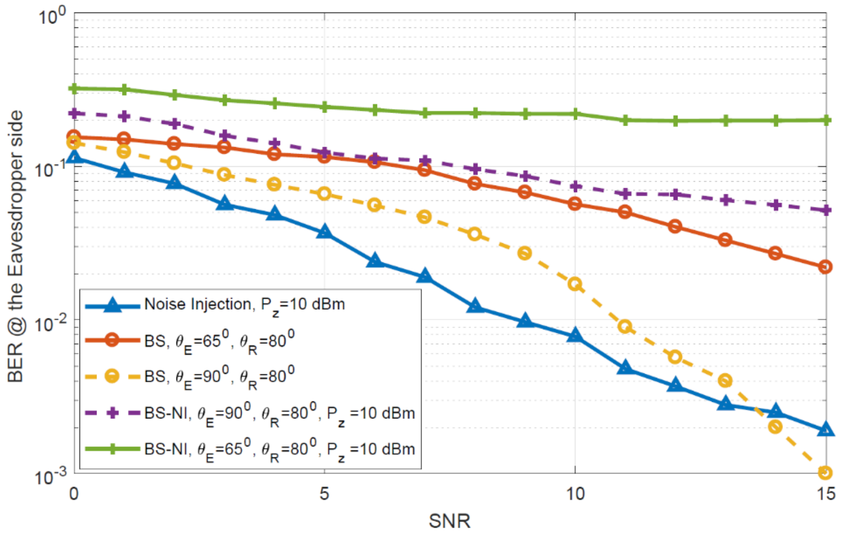


Figure 14 BER at Eavesdroppers vs SNR for different techniques and eavesdropper locations

Figure 15 illustrates the BER versus the spatial direction of the eavesdropper which complies with the results presented in Figure 14 and shows that even a close eavesdropper will not be able to retrieve the tag's signal.

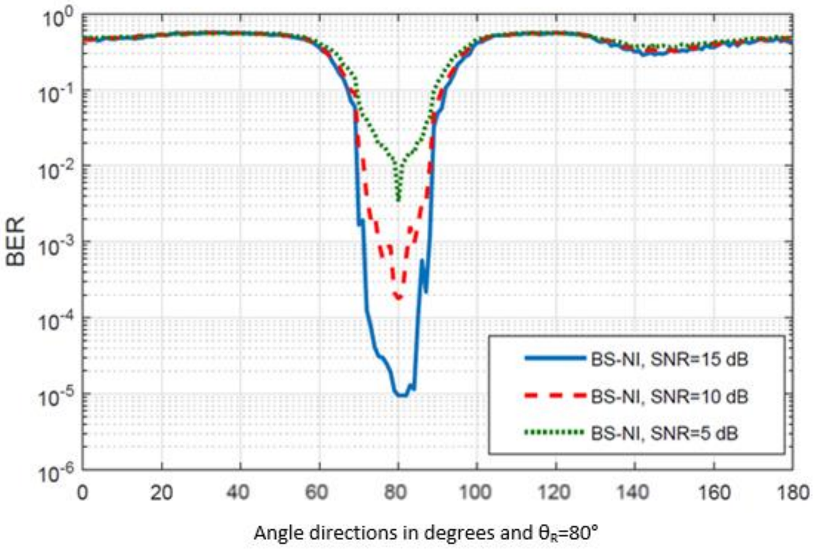


Figure 15 BER vs θ in degress for different SNR

Figure 16 illustrates the minimum required power level of the injected noise from the reader that keeps the tag's signal secret. As expected, the required power of the injected noise in the proposed BS-NI approach is less than the required power of the noise injection scheme and this verifies that the proposed system overcomes the power limitations faced in noise injection scheme [9].

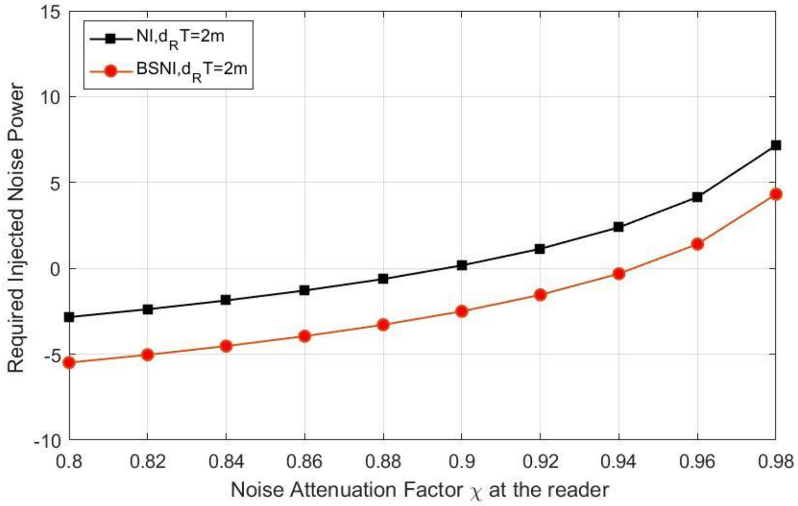


Figure 16 The minimum required noise power vs the attenuation factor χ for NI and BS-NI.

To investigate the benefit of the proposed BS-NI scheme, a comparison is conducted between two scenarios where the eavesdropper knows the location of the reader and tag. The comparison is developed for BS-only and BS-NI schemes. Figure 17 illustrates the BS-only technique in two cases; one where the eavesdropper is capable of determining the location of the reader and the tag, the second case is where the eavesdropper cannot detect the location of the reader and tag. As shown in the figure, if the eavesdropper is capable of tracking the location of the reader and tag, it can easily retrieve the tag's data. While in Figure 18, the performance of BS-NI has the advantage that even if the eavesdropper is capable of tracking the reader and the tag, it will not be able to retrieve the tag's data due to the presence of the injected noise.

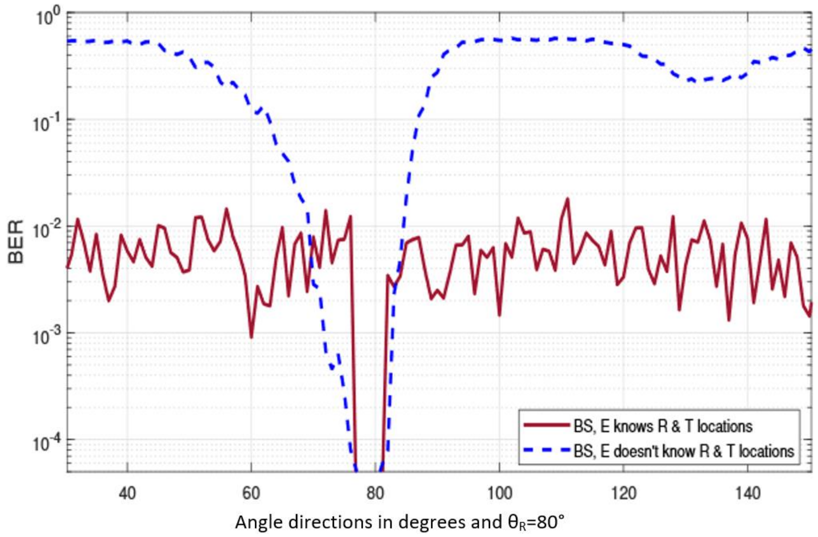


Figure 17 BER vs θfor BS technqiue

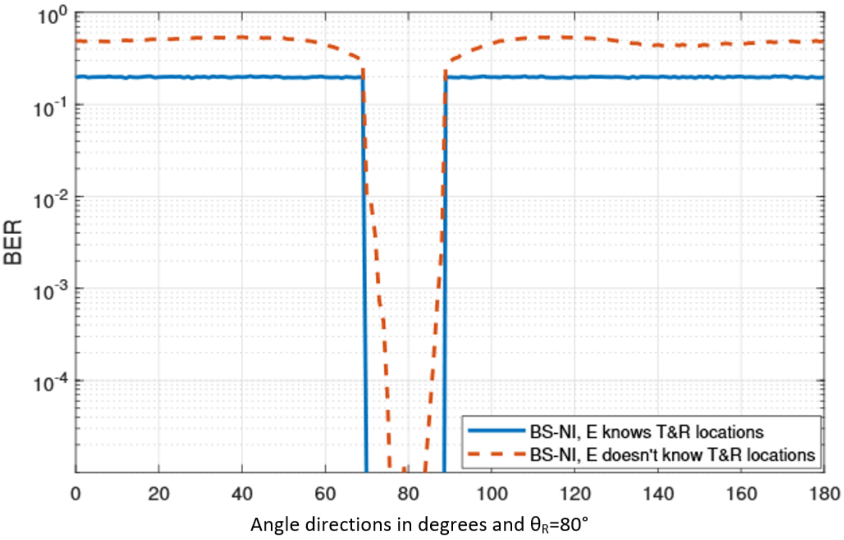


Figure 18 BER vs θfor BS-NI technique

Finally, Figure 19 presents the relation between the noise attenuation factor χ and the BER. As shown in the figure, the BER improves when the ability of the reader to attenuate the noise is higher, hence when the residual part of χ is lower.

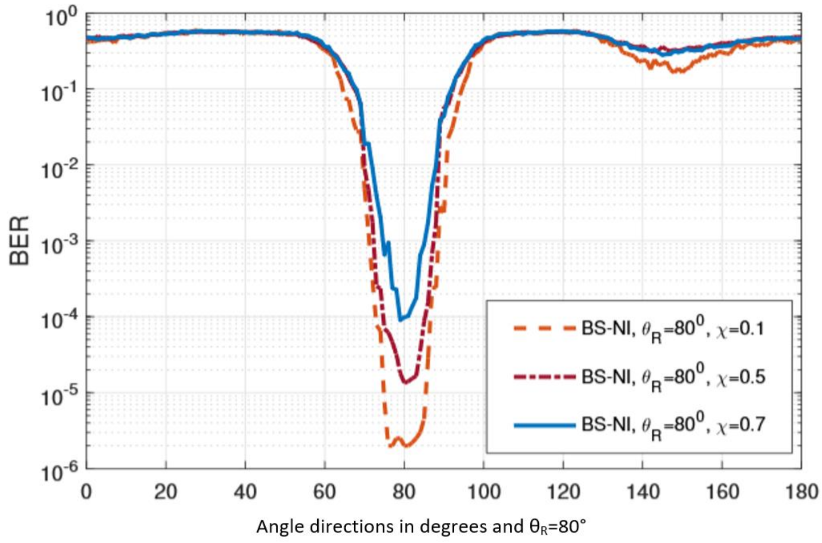


Figure 19 BER Vs theta for different χ

3.6 Applications for this approach

The proposed technology can be used in healthcare application to secure a network that deploys RFID systems. By using BS-NI, it is guaranteed that the tag's data is secure and used only by the legitimate receiver (reader). Due to the advanced processing and circuitry required to achieve BS-NI, its more adequate to be used for applications where the enhancement of tag’s characteristics will not affect the execution of the system, such as home assist sensors and components in healthcare applications. The devices used in such applications have relatively expensive resources and advanced processing capabilities and thus using an advanced tag will not be an issue in terms of cost. Also, in home assist applications, the devices are placed far from the patient, therefore, there will not be an issue in terms of space required to implement multiple antennas at the tag.

3.7 Conclusion

In this chapter, a novel PLS technique is developed to secure RFID systems. The approach consists of two parts, first, artificial noise is injected from the reader side and the second part deploys BS at the tag side. The proposed BS-NI technology overcomes the limitations of the already existing techniques such as injecting artificial noise only presented in [9]. The numerical results show that the proposed BS-NI technique outperforms the conventional noise injection scheme.

In the next chapter, another technique is developed to secure RFID systems. That technique is more adequate for all RFID tags including the implanted medical devices, because it does not require any modifications to tag circuitry or capabilities. This is achieved by designing the security attributes to be completely handled from the reader side.

CHAPTER 4: DIRECTIONAL MODULATION FOR RFID

This chapter presents another novel technique to secure RFID tags, aiming to exploit the reader capabilities to accomplish system security. In this system, DM technology is deployed to secure RFID passive tags while maintaining their simple circuity and processing nature. Specifically, the contributions of this chapter can be summarized as follows:

- The data of RFID tags is secured by exploiting the capabilities of the RFID reader. To achieve system security, Directional Modulation (DM) is implemented at the reader side. By using DM, the reader's signal is transmitted correctly to the legitimate tag only and other receivers will get a distorted signal due to the beam steering vector and the artificial noise which is designed to be orthogonal to the desired tag channel.
- The proposed approach maintains the simplicity of the tag's processing capabilities and circuity, which makes the approach suitable for any RFID tag.
- The performance of the proposed technique is analyzed, and numerical results are obtained to demonstrate the value of the proposed technique in terms of securing tag's data against eavesdropping readers.

4.1 Directional Modulation System Model

This section focuses on implementing DM technique in RFID system to secure the tag's signal. To illustrate, the DM methodology is exploited at the reader side, given that the reader already has a processor and is more likely to accommodate multiple antennas. In addition, this technique also embeds secrecy on the reader's signal which is transmitted with higher power and thus is subjected to eavesdropping even at large distances. As discussed in literature survey earlier, DM is developed using various synthesis methods. However, in this thesis the focus will be on the artificial orthogonal noise synthesis method is used to construct the DM system. This type of synthesis provides a noise signal that distorts the reader's signal at the eavesdropper's location but is null in the direction of the legitimate tag. In addition, there are two types of DM technique; Static and Dynamic. However, the dynamic method is considered in the proposed DM method, where the beamforming vector and the noise vector vary with each QPSK symbol [76].

Figure 20 illustrates the typical active DM transmitter array architecture that consists of baseband information controlled by phase shifters and attenuators. Also, Figure 21 illustrates how the signal is directed to the desired receiver and noise is nulled.

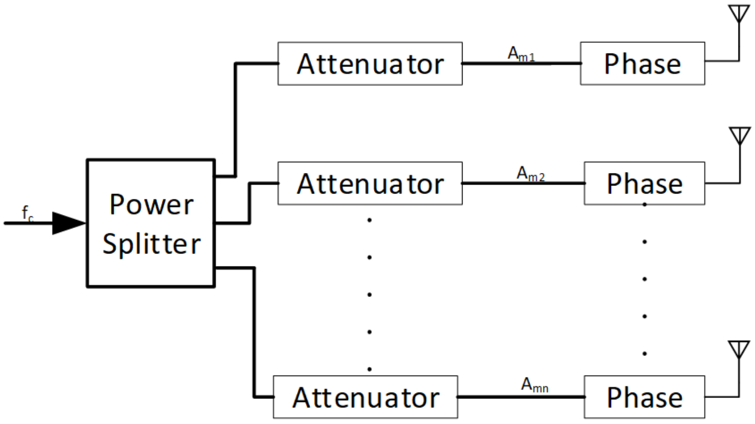


Figure 20 DM Transmitter array architecure

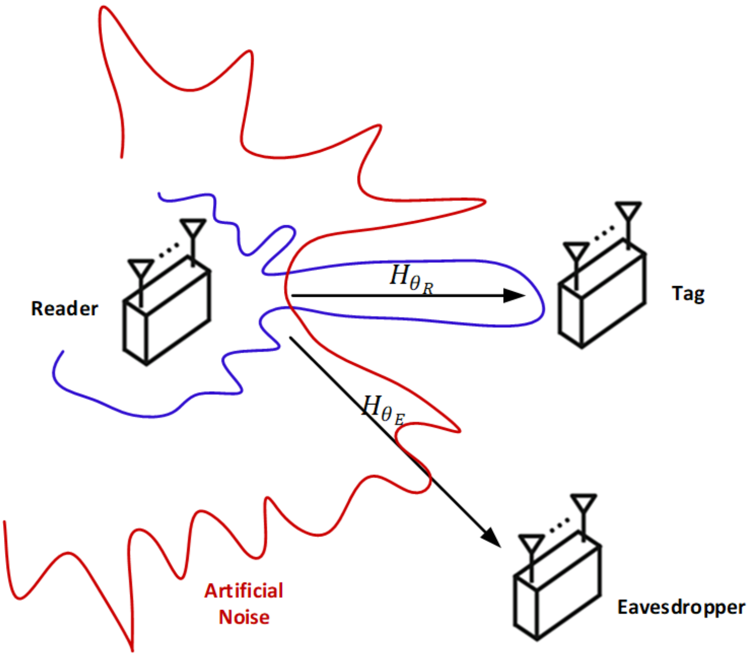


Figure 21 Secure DM modeled as beamforming with noise injection

The basic representation of DM using artificial orthogonal noise is [80],

$$S = PX + W, \tag{ 0-28}$$

where P is the beamforming vector and W is the noise signal that is constructed in the null space of the desired channel. The AWGN vector is assumed to have i.i.d distribution with zero-mean and unit variance, i.e, $W \sim CN(0, I_{nd})$. The signal delivered to any receiver is given by:

$$y = H_\theta S \tag{ 0-29}$$

$$y = H_\theta(PX + W), \tag{ 0-30}$$

where H_θ is the spatial communication channel described in the DM system. If the receiver is located at the desired direction of the system, then the noise term will be eliminated, and the beamforming vector will be normalized. Otherwise, the signal will be distorted by the injected noise.

The signal at the legitimate receiver located at θ_R can be represented as:

$$y = H_{\theta_R}(PX + W) \tag{ 0-31}$$

$$y = H_{\theta_R} \frac{H_{\theta_R}}{\parallel H_{\theta_R} \parallel} X + H_{\theta_R} W \tag{ 0-32}$$

$$y = \parallel H_{\theta_R} \parallel X. \tag{ 0-33}$$

The signal at undesired receivers located at θ, where $\theta \neq \theta_R$:

$$y = H_{\theta}(PX + W) \tag{ 0-34}$$

$$y = H_{\theta} \frac{H_{\theta_R}}{\parallel H_{\theta_R} \parallel} X + H_{\theta} W. \tag{ 0-35}$$

4.2 RFID with DM System Model

For DM in RFID, the communication links between reader, tag and eavesdropper are presented in Figure 22. In this thesis, X is considered as the signal sent from the reader. The equations described in the previous section represents the DM technique modeled in one-way communication systems and analyzed in free space. To introduce DM for RFID technology, the half-duplex communication mode is modeled by adding the forward and backward links of the RFID to the equations, where h^f and h^b are introduced denoting the forward and backward links for of the RFID system, respectively.

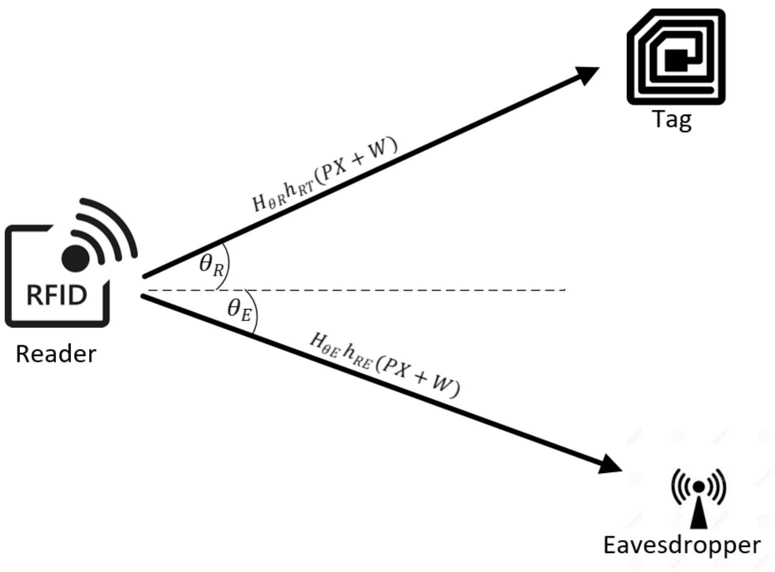


Figure 22 Communication links between reader, tag and eavesdropper

The desired channel between the reader and the tag is given as:

$$H_{\theta_R} = \left[e^{j2\pi\cos\theta_R}\ \ e^{j\pi\cos\theta_R}\ e^{j0}\ \ e^{-j\pi\cos\theta_R}\ \ e^{-j2\pi\cos\theta_R}\right]. \qquad (\ 0\text{-}36)$$

Therefore, $P = \frac{H_{\theta_R}}{\|H_{\theta_R}\|}$ will be normalized by the channel and W will be generated to be in the null space of H_{θ_R}.

The model of this system is presented in Figure 23, where DM is deployed at the reader. To achieve this, the reader is equipped with multiple antennas to transmit the signal to the tag, while the tag and the eavesdropper are passive devices with a single antenna. Noting that the eavesdropper has Channel State Information (CSI) about the channel between the reader and the eavesdropper h_{RE} and the combined channel $h_{RT}h_{TE}$. The eavesdropper is able to estimate h_{RE} channel since the power sent from the reader is standardized and can be easily estimated by any device. It is exactly the same way the eavesdropper can estimate the combined channel $h_{RT}h_{TE}$. Fortunately, the eavesdropper cannot estimate the channel between itself and the tag since it does not know the tag's circuit and how much it can reflect. The signal is received by both the tag and the eavesdropper but at different spatial communication directions. On the link between the reader and tag, the beamforming vector is normalized, and the injected noise is nulled. While on the link between the reader and eavesdropper, the beamforming and noise term remain present and cause signal distortion. Therefore, the tag will receive a decodable signal while the eavesdropper will receive a distorted (scrambled) signal.

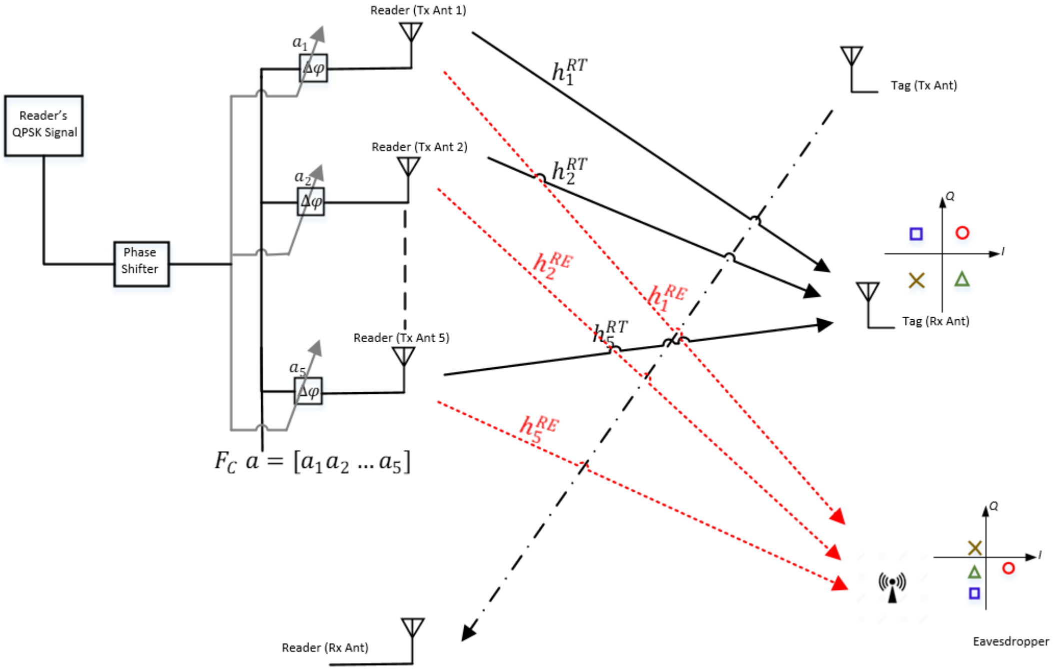


Figure 23 System model where DM is exploited at the reader

In general RFID system, the received signal at the reader is:

$$y_R = h_{RT} h_{TR} x s + n_R + n_T s h_{TR}, \qquad (\ 0\text{-}37)$$

where h_{RT} is the channel gain from reader to tag, h_{TR} is the backscatter channel gain from the tag to reader, s is the information signal generated by the tag and n_R and n_T are the AWGN at the reader and tag receivers, respectively. From practical point of view, the overall channel between reader and tag is an addition of i.i.d complex Guassian products [19]. Thus, the amplitude of each channel link follows Rayleigh distribution and the overall channel between reader and tag follows double Rayleigh distribution [17, 22]. The development of DM under fading channels effect is an interesting extend of this work and shall be addressed in future work, however, in this thesis, the RFID system will be modeled and analyzed in free space; hence, presenting an upper bound on performance in practical fading systems.

By adding the DM technique to RFID system, which is exploited at the reader side where the reader transmits a QPSK signal that is received correctly only by the tag located at θ_R and scrambled in any other direction. Hence, the eavesdropper cannot decode the reader's signal unless it is aligned on the same path of the tag. Figure 24 illustrates two constellation patterns of the reader signal received by the tag located at θ_R and the eavesdropper located at θ_E.

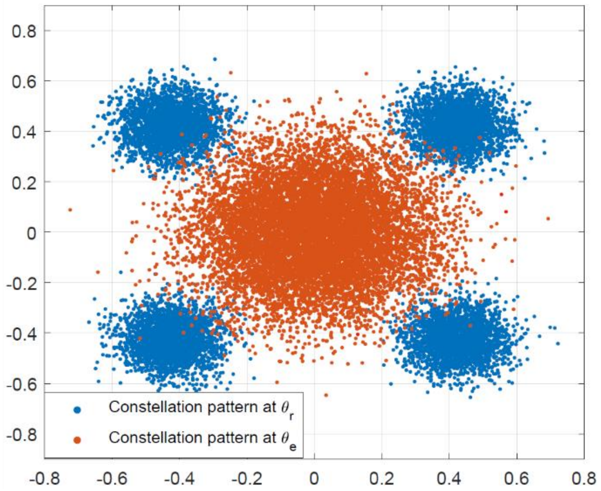


Figure 24 Constellation pattern at the desired tag and eavesdropper

The signals received from the reader to tag and eavesdropper are:

$$y_{RT} = H_{\theta_R} h_{RT}(PX + W) + N_T \qquad (0\text{-}38)$$

$$y_{RE} = H_{\theta_E} h_{RE}(PX + W) + N_E. \qquad (0\text{-}39)$$

Although DM is designed on the reader’s signal, the system security is evaluated from the tag’s signal perspective, since the secret information is carried by the tag’s signal. Therefore, the signal transmitted is analyzed from the signal transmitted from the tag to reader and from tag to eavesdropper.

The noiseless signal received from the tag located at H_{θ_R} is:

$$y_{TR} = h_{TR}(H_{\theta_R} h_{RT}(PX + W)s + N_T s) + N_R \qquad (0\text{-}40)$$

$$y_{TR} = h_{TR}(H_{\theta_R} h_{RT} PXs + H_{\theta_R} h_{RT} Ws + N_T s) + N_R \qquad (0\text{-}41)$$

$$y_{TR} = h_{TR}(\| H_{\theta_R} \| h_{RT} Xs + N_T s) + N_R \qquad (0\text{-}42)$$

$$y_{TR} = \| H_{\theta_R} \| h_{RT} h_{TR} Xs + h_{TR} N_T s + N_R. \qquad (0\text{-}43)$$

In (0-43), the signal is transmitted to a legitimate tag which is located at the desired direction θ_R, hence the artificial noise W is eliminated and the beamforming vector is normalized.

The distorted signal received at the eavesdropper can be presented as:

$$y_{TE} = h_{TE}h_{RT}H_{\theta_R}\,(PX + W)s + N_T h_{TE}s + N_E \qquad (\ 0\text{-}44)$$

$$y_{TE} = h_{TE}h_{RT}H_{\theta_R}PXs + h_{TE}h_{RT}H_{\theta_R}Ws + N_T h_{TE}s + N_E, \qquad (\ 0\text{-}45)$$

where θ_E is the direction of the eavesdropper from the reader, h_{TE} is the channel from tag to eavesdropper and N_E is the receiver noise generated at the eavesdropper.

Accordingly, the only way for the eavesdropper to obtain the secret signal transmitted by the tag is to divide the signal it received from the tag by the signal that is previously received from the reader. At this point, the eavesdropper has the signal Xs from the tag and is trying to estimate the signal X sent from the reader to obtain tag's secret signal s. However, the reader's signal received by the eavesdropper is a scrambled version of the actual signal X. Equation (0-46) describes the process where the eavesdropper is trying to obtain s.

In the first step, the eavesdropper attempts to estimate Xs from (0-45), where the eavesdropper knows the combined channel $h_{RT}h_{TE}$, thus $\widehat{Xs}$ can be presented as:

$$\widehat{Xs} = H_{\theta_R}PXs + H_{\theta_R}Ws + N_T s + N_E\frac{h_{TE}^*}{\|h_{TE}\|} \qquad (\ 0\text{-}46)$$

$$\widehat{Xs} = \|H_{\theta_R}\|Xs + s + N_T s h_{TE}\left(\frac{(h_{TE}h_{RT})^*}{\|h_{TE}h_{RT}\|^2}\right) + N_E\left(\frac{(h_{TE}h_{RT})^*}{\|h_{TE}h_{RT}\|^2}\right) \qquad (\ 0\text{-}47)$$

In the next step, the eavesdropper attempts to estimate the reader signal defined in (0-39), where the eavesdropper knows the channel h_{RE} ,thus $\hat{X}$ is given as:

$$\hat{X} = H_{\theta_E}PX + H_{\theta_E}W + N_E\frac{h_{RE}^*}{\|h_{RE}\|^2} \qquad (\ 0\text{-}48)$$

$$\hat{X} = H_{\theta_E}\frac{\|H_{\theta_R}\|}{H_{\theta_R}}X + H_{\theta_E}W + N_E\frac{h_{RE}^*}{\|h_{RE}\|^2} \qquad (\ 0\text{-}49)$$

The main aim of the eavesdropper is to detect the tag's secret signal s, to do so , it divides $\widehat{Xs}$ by $\hat{X}$ which follows:

$$\hat{s} = \frac{\widehat{Xs}}{\hat{X}} = \frac{\left\|H_{\theta_R}\right\|Xs + s + N_T s h_{TE}\left(\frac{(h_{TE}h_{RT})^*}{\|h_{TE}h_{RT}\|^2}\right) + N_E\left(\frac{(h_{TE}h_{RT})^*}{\|h_{TE}h_{RT}\|^2}\right)}{H_{\theta_E}\frac{\left\|H_{\theta_R}\right\|}{H_{\theta_R}}X + H_{\theta_E}W + N_E\frac{h_{RE}^*}{\|h_{RE}\|^2}} \qquad (\ 0\text{-}50)$$

The signal in (0-50) is received at the eavesdropper at undesired location θ_E, where W is not orthogonal to H_{θ_E} and hence the term $H_{\theta_E}W$ is nonzero, which distorts tag's secret information s. Thus, the eavesdropper cannot decode the tag's signal unless it is aligned with the tag at θ_R, where the signal will be the same as in (0-43).

From the above equations, the SNR term for the signal received at the reader and at the eavesdropper in free space can be derived and represented as:

The SNR received at the reader in free space is:

$$\gamma_R = \frac{\|Xs\|^2\left\|H_{\theta_R}\right\|^2 G_{RT}G_{TR}\,\Gamma\,K^2\,d_{RT}^{-4}}{\sigma_R^2 + \sigma_T^2\,G_{TR}\,d_{RT}^{-2}\,K}, \qquad (\ 0\text{-}51)$$

where K is a constant that depends on the carrier wavelength λ, where $K = \left(\frac{\lambda}{4\pi}\right)^2$, G_{RT} and G_{TR} are the antenna gain of the reader and tag, respectively,Γ is the partial of the power reflected back from the tag, d_{RT}^{-4} is the distance between the reader, and tag and σ_R^2 and σ_T^2 are the noise power at the reader and tag receivers, respectively.

The SNR at the eavesdropper is the same of that of the reader but with different channel annotation. The signal at the eavesdropper is degraded by the estimated reader's signal derived in (0-51). The SNR received at eavesdropper in free space is:

$$\gamma_E = \frac{\|\,Xs\|^2\left\|H_{\theta_R}\right\|^2 G_{TE}\,\Gamma\,K^2\,d_{TE}^{-2}}{\sigma_E^2 + \sigma_T^2\,G_{TE}\,d_{TE}^{-2}\,K} \qquad (\ 0\text{-}52)$$

There are several metrics to evaluate the performance of the DM technique in any wireless communication system [84]. For this system and to be inline with the previous proposed system model, BER will be used to evaluate the performance at the reader and eavesdropper. BER for QPSK modulation is:

$$P_b = Q\left(\sqrt{2\gamma}\right),$$

where γ is the SNR per bit.

4.3 Numerical Results and Discussions

This section presents the numerical results of the system to illustrate the performance of the DM technique applied in the RFID system. Prior discussing the results, the design parameters are defined as the following. The tag is on spatial direction $\theta_R = 80^0$ from the reader, the SNR along the desired direction is $15dB$ and antenna gains are assumed to be 1. The BER of the eavesdropper is evaluated at two different locations from the reader $\theta_{E1} = 90^0$and $\theta_{E2} = 45^0$.

Figure 25-Figure 27 present the obtained results following the same simulation parameters mentioned in Section 3.5 ,where a quadrature phase shift keying (QPSK) modulation scheme is assumed.

Figure 25 illustrates the performance of the proposed system by plotting the BER against θ ranging from $0^0\ to\ 180^0$. The results show that the BER is at its lowest value at the desired direction of the tag at $\theta = 80^0$, where the BER reaches a value below 10^{-4}, while the BER for other directions has an average value of almost 0.5 (perfect secure system).

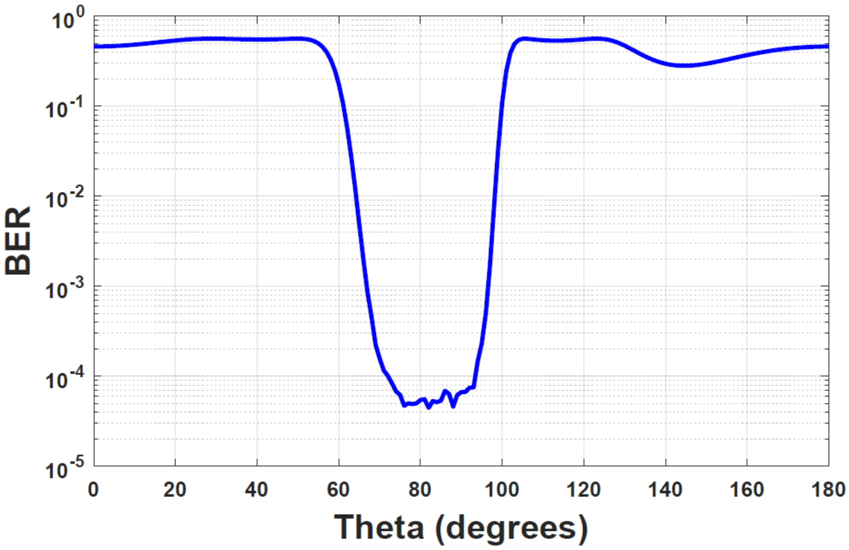


Figure 25 BER vs θ, tag at θ=80°

Figure 26 illustrates the BER versus the spatial direction of the eavesdropper at different SNR values. It can be seen from Figure 27 that even at high SNR of 15dB, the BER curve remains almost constant at the eavesdropper locations at value of 0.554. However, the BER value improves at the tag located at $\theta = 80^0$, where it reaches a value below 10^{-4} at 15 dB.

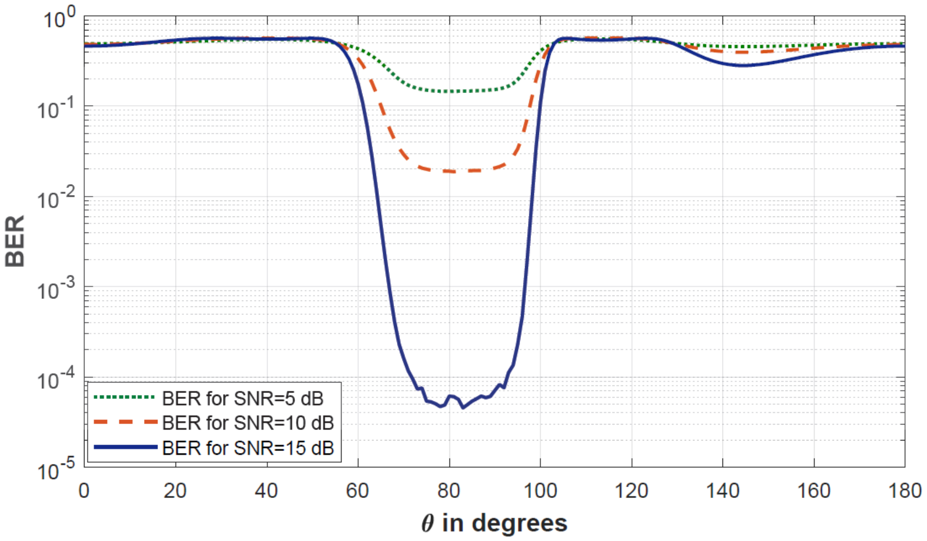


Figure 26 BER vs θ for different SNR values

Figure 27 presents the BER at eavesdropper located at different angles vs SNR values. The results show that even at high SNR, the eavesdropper still have high BER, which complies with the results obtained in Figure 26. However, it is important to mention that the eavesdropper located near the tag has better performance than others. This can be shown in Figure 27, where the eavesdropper located at angle $\theta = 45^0$, remains almost constant. While for the eavesdropper located at $\theta = 90^0$, its performance improves at higher SNR values.

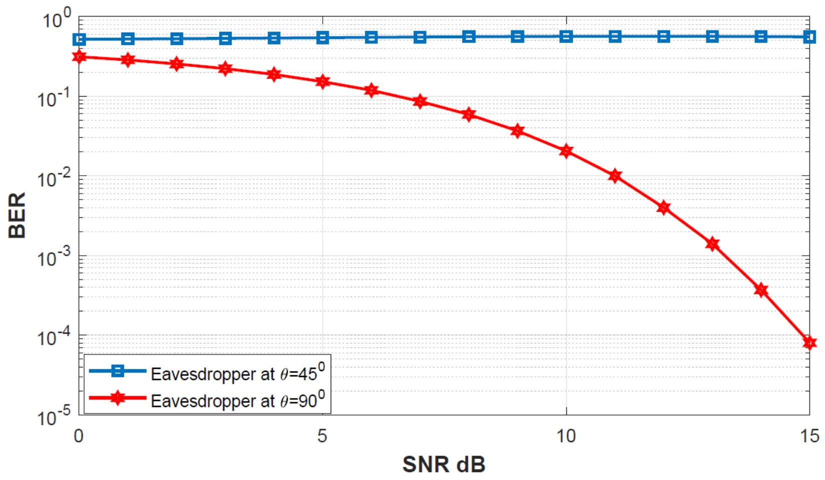


Figure 27 BER at eavesdropper Vs SNR for different eavesdropper locations

The results obtained in Figures 4-6 to 4-8 prove that the system is functional, and it can secure the tag's signal where the BER is high at eavesdropper location and low only at the legitimate tag's location. In addition, even at high SNR, the eavesdroppers still cannot decode the reader's signal which is one of the features of DM. On the contrary, the performance at the eavesdropper in conventional beamsteering improves as the SNR increases.

4.4 Application of the proposed Approach

This novel approach provides RFID security, where it ensures secrecy of the tag's information signal by using DM technique. Since this approach does not require any extra resources or advancement of the tag's capabilities, it can be easily deployed in multiple applications. Mainly in IoT technology and medi92cal devices, especially for implanted devices that require powerless, small size and secure tags. Moreover, it can be employed in inventory and supply chain applications. In fact, this approach is adequate for most RFID applications but presents more importance in applications that requires more security while maintaining the simple characteristics of passive tags, such as healthcare applications.

4.5 Conclusion

In this chapter, a novel DM technique has been proposed, aiming to secure RFID passive tags through the physical layer without any modification or enhancement of the tag's circuity or processing capabilities. The DM scheme used in this work is dynamic where the beamforming and injected noise are updated for each QPSK symbol. DM scheme is exploited at the reader side which is equipped with 5-element antennas, where the reader transmits a QPSK signal. This signal is received correctly at the tag's direction and distorted at any other locations. This distortion is caused by two factors, the first factor the beamforming vector that only normalizes in the desired direction, while the second factor is the injected artificial noise which is designed at the null space of the desired link between the reader and tag. The results obtained in the previous section show that the system achieve tag's signal security where, the BER is low only at the tag's direction.

CHAPTER 5: CONCLUSION AND FUTURE WORK

In this chapter, the main conclusions of this thesis are summarized, and the concerns for future work are determined and discussed. The main motivation of this thesis has been the investigation of novel security schemes suitable for RFID and backscatter systems, where related research is very limited in this area. In this context, the aim was to develop a novel robust security technique to secure RFID tags while considering the restricted resources of the RFID tags.

In the first contribution of the thesis, novel beamsteering and noise injection scheme has been proposed, in order to secure tag's secret information signal by exploiting BS technique at the tag side and exploiting the noise characteristic of physical layer at the reader side. To develop this technique, the tag was equipped with 5 element 1-D antenna array and the reader injected artificial noise while it had noise attenuation capabilities. This scheme requires the tag to have a specific hardwired circuit to accommodate multiple antenna technology. Also, this proposed approach was designed for single reader, single tag system model. The system analytical and performance model has been derived in the contribution. Moreover, numerical results have been presented, showing how the proposed scheme outperforms the state-of-the-art in RFID security techniques, in terms of the required power and the security rate while considering intelligent eavesdroppers. This contribution can be deployed in multiple healthcare applications. Due to the advanced processing and circuitry required to achieve BS-NI, its more adequate to be used for applications where the enhancement of tag's characteristics will not affect the execution of the system, such as home assist sensors. In order to deploy RFID system in various healthcare application, a more adequate scheme that maintains the simplicity of tag's circuit and processor is required, which is developed in chapter 4.

In the second contribution of the thesis, a novel DM technique has been proposed to secure tag's secret information while maintaining its simple circuitry and processing capabilities. This approach is constructed by exploiting DM technology at the reader which is equipped by 5 element 1-D antenna array and it is assumed that both the tag and the eavesdropper are passive devices. The approach was designed for single reader, single tag system model. The system mathematical model has been presented in this thesis. The proposed approach operates using dynamic DM based on combined beamsteering and orthogonal noise injection. The beamstearing is selected such that it is normalized by the tag's channel while the noise is in the null space of the tag's channel. Numerical results have been presented, showing how the proposed scheme is capable of securing the tag's secret information. Moreover, the results highlight the fact that even at high SNR values, the eavesdropper cannot detect the tag's signal. For an eavesdropper located at an angle that is relatively far from the tag's angle, the BER value remains almost constant across different values of SNR, while for eavesdropper located close by the tag, their performance slightly improves at high SNR values. In this contribution, the tag's signal is secured while maintaining the simplicity of tag's circuit and processing capabilities which facilitates the deployment of RFID system in various healthcare applications including implanted devices.

The work developed in this thesis can be extended in multiple different directions. The main concerns for future work are mentioned below:

- Design DM technique for RFID system while considering multi-path fading channels, where RFID channels are modeled by double Rayleigh distribution.
- Derive the BER equations for double Rayleigh distributed channels, and develop theoretical results.
- Develop advanced methods in DM such as adaptive beamforming technique .

- Inspect the performance of the proposed approaches by using different metrics schemes such as EVM and secrecy rate and determine if all the metrics are applicable for DM and BS-NI techniques.
- Investigate the robustness of the proposed schemes in the presence of intelligent eavesdroppers equipped with directional antennas.
- Designing secure network for RFID system in MIMO or SIMO model, where there will be multiple tags and single reader or multiple readers and multiple tags. Also, designing a secure network in the presence of multiple eavesdroppers.
- Develop secure network for active tags, while considering the collision between readers and tags among themselves, since active tags can communicate with each other.

REFERENCES

[1] M. Haddara and A. Staaby. (2018) RFID Applications and Adoptions in Healthcare: A Review on Patient Safety. *Procedia Computer Science*.

[2] G. L. Simson, A. Jules, and R. Pappu, "RFID Privacy: An Overvieew of Problems and Proposed Solutions," *IEEE Secuirty & Privacy,* 2005.

[3] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE,* 2018.

[4] M. Daly and J. Bernhard, "Direction Modulation Technique for phased Arrays," *IEEE Transactions of Antennas and propagation,* vol. 57, no. 9, 2009.

[5] A. Babakhani, D. Rutledge, and A. Hajumiri, "Transmitter Architectures Based on Near-Field Direct Antenna Modulation," *IEEE J. Solid State Circuits,* vol. 43, pp. 2674-2692, 2008.

[6] S. HongZhe and T. Alan, "Secure Physical-Layer Communication Based on Directly Modulated Antenna Arrays," presented at the Loughborough Antennas & Propagation Conference Loughborough, UK, 2012.

[7] S. HongZhe and T. Alan, "Characteristics of a Two Element Direction Dependent Antenna Array," presented at the Loughborough Antennas & Propagation Conference, Loughborough,UK, 2011.

[8] P. Danai and S. S.J., "Cryptographic Security Techniques for Wirless Networks ",

[9] W. Saad, X. Zhou, H. Zhu, and H. V. Poor, "On the Physical Layer Security of Backscatter Wireless Systems," *IEEE Transactions of Wireless communications,* 2014.

[10] A. Kamran, S. Hanifa, and K. Paul, "RFID Applications: An Introductory and

Exploratory Study," *International Journal of Computer Science,* vol. 7, no. 1, 2010.

[11] C. Vipul and S. H. Dong, "An Overview of Passive RFID," *IEEE Applications & Practice,* 2007.

[12] S. Harry, "Communication by Means of Reflected Power," *Proc. Institute of Radio Engineers,* 1948.

[13] R. Want, *RFID Explained: A Primer on Radio Frequency Identification Technologies*. Morgan & Claypool, 2006.

[14] P. V. Nikitin and S. Lazar, "An Overview of Near Field UHF RFID," in *IEEE International Conference RFID,* 2007.

[15] P. Davinder, K. Twinkle, and K. Preet, "The RFID Technology and its Applications : A Review," *International Journal of Electronics,* vol. 2, no. 3, pp. 109-120, 2012.

[16] "The Beginner's Guide To RFID Systems," Atlas RFID Store.

[17] F. Zheng and T. Kaiser, *Digital Signal Processing For RFID*. 2016.

[18] J. Salo, H. M. El-Shallabi, and P. Vainikainen, "Impact of Double-Rayleigh Fading on System Performance," *IEEE Wireless Pervasive Computer,* 2006.

[19] H. Chen and J. Wang, "Closed-Form BER Analysis of Non-Coherent FSK in MISO Double Rayleigh Fading/RFID Channel," *IEEE Communications Letters,* vol. 15, no. 8, 2011.

[20] D. Yvan and T. Smail, "RFID: A Key technology for Humanity," *Science Direct,* 2018.

[21] B. Colby and R. Sumit, "Backscatter Commmunication and RFID: Coding, Energy, and MIMO Analysis," *IEEE Transacations on communications,* vol. 62, no. 3, 2014.

[22] N. Amin, N. Wen Jey, and M. Othman, "A BPSK Backscatter Modulator Design for RFID Passive Tags," *IEEE International Workshop on Radio-Frequency Integration Technology,* 2017.

[23] M. S. Trotter, C. R. Valenta, G. A. Koo, B. R. Marshall, and G. D. Durgin, "Multi-Antenna Techniques for Enabling Passive RFID Tags and Sensors at Microwave Frequencies," *IEEE International Conference on RFID,* 2012.

[24] *EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID*, Epcglobal, Belgium, 2015.

[25] P. P. Lopez, "Lightweight Cryptography in Radio Frequency Identification (RFID)," UNIVERSIDAD CARLOS III DE MADRID, Madrid, 2008.

[26] "GS1-EAN International." http://www.ean-int.org (accessed.

[27] "EPCglobal." http://www.epcglobalinc.org (accessed.

[28] "Class-1 Generation-2 UHF air Interference Protocol Standard." http://www.epcglobalinc.org/standards (accessed.

[29] "EPCglobal Architecture Framework." http://www.epcglobalinc.org/ (accessed.

[30] "EPC ONS Standard." http://www.epcglobalinc.org/ (accessed.

[31] S. Hung-Min and T. Wei-Chih, "A Gen2-Based RFID Authentication Protocol for Security and Privacy," *IEEE TRANSACTIONS ON MOBILE COMPUTING,* vol. 8, no. 8, 2009.

[32] S. Vijay, A. Vithalkar, and M. Hashmi, "Lightweight Security Protocol for Chipless RFID in Internet of Things (IoT) Applications,"

[33] F. Kai, J. Wei, L. Hui, and Y. Yintang, "Lightweight RFID Protocol for Medical Privacy Protection in IoT," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 4, 2018.

[34] F. Kai, Z. Shanshan, Z. Kuan, and Y. Yintang. (2019) A Lightweight Authenication Scheme for Cloud-Based RFID Healthcare Systems. *IEEE Network.*

[35] I. Lacmanovie, R. Bilajana, and L. Dejan, "Contactless payment systems based on RFID Technology," *IEEE,* 2010.

[36] V. Chawla and S. H. Dong, "An Overview of Passive RFID," *IEEE Applications & Practice,* 2007.

[37] A.-Z. Malek, A. Ja'far, and A.-K. Omar, "Privacy and Security of RFID Access Control Systems," presented at the IEEE Jordon Conference on Applied Electrical Engineering and Computing Technologies Jordon, 2011.

[38] B. W. Podaima, M. Friesen, and R. D. McLeod, "A review of emerging smart RFID in healthcare," *CMBES Proceedings,* vol. 33, no. 1, 2018.

[39] L. Antti, "A short Overview of the RFID Technology in Healthcare," presented at the 2009 Fourth International Conference on Systems and Networks Communications, Portugal, 2009.

[40] D. Joseph, I. Chicco, P. Isabelle, and R. Silvano, "Using RFID Technologies to Reduce Blood Transfusion Errors ",

[41] A. Herve, "RFID technology for human implant devices," *Nanoscience and nanotechnologies: hopes and conerns,* pp. 675-683, 2011.

[42] "Radio-Frequency Identification: its Potential in Healthcare," *Health Devices,* vol. 34, pp. 149-160, 2005.

[43] L. S. Wauben, A. C. Guedon, K. De, and V. d. Dobbelsteen, "Tracking surgical day care patients using RFID technology," *BMJ Innovations,* 2015.

[44] S. Zalilami, M. Irammanesh, D. Nikbin, and J. K. C. Beng, "Determinants of RFID adoption in Malaysia's healthcare industry," *Journal of Medical systems,*

vol. 39, no. 1, 2015.

[45] W. Angela M., V. John k., and L. Suhong, "Radio Frequency Identification Applications in Hospital Environments," vol. 84, no. 3,

[46] A. Binita S. and F. Ann, "Radiofrequency Identification Technology in Healthcare: Benefits and Potential Risks,"

[47] A. Antonio, P. Wil, and M. Gerlad, "Positive Patient Identification using RFID and Wireless Networks," presented at the HISI 11th Annual Conference and Scientific Symposium, 2003.

[48] W. Fan, K. Frank, and L. Liu-Wei, "The Application of RFID on Drug Safety of Inpatient Nursing Healthcare," in *The 7th international conference on Electronic commerce*, 2005: Association of Computing Machinery

[49] B. P. Rosenbaum, "Radio frequency identification (RFID) in healthcare: privacy and security concerns limiting adoption," *Journal of Medical Systems*, vol. 38, no. 3, 2014.

[50] Y. Wen, H. C. Chao, and L. Zang, "The Use of RFID in Healthcare: Benefits and Barriers," presented at the IEEE International Conference on RFID-Technology and Applications China, 2010.

[51] X. Yang, S. Xuemin, S. Bo, and C. Lin. (2006) Security and Privacy in RFID and Applications in Telemedicine. *IEEE Communications Magazine*.

[52] S. Frank and A. Ross, "The Resurrecting Duckling Secuirty Issues for Ad-hoc Wireless Networks," in *Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science*, 1999: Springer.

[53] J. Ari and P. Ravilanth, "Privacy Protection in RFID-Enabled Banknotes," presented at the Financial Cryptography Newyork 2003.

[54] G. Philippe , J. Markus, J. Ari, and S. Paul, "Universal re-encryption for

mixnets," in *RSA Conf.-Cryptographers*, 2004, vol. 2964, pp. 163-178.

[55] Y. Qian, Z. Yi, W. Hui-Ming, and H. Zhu, "Transmit Optimization for Secure MIMO RFID Wireless Communication," presented at the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016.

[56] Q. Yang, H.-M. Wang, Y. Zhang, and Z. Han, "Physical Layer Security in MIMO Backscatter Wireless Systems," *IEEE Trans, Microw Theory Tech.*, 2016.

[57] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing RFIDs by Randomizing the Modulation and Channel," in *12th USENIX Symposium on Networked Systems Design and Implementation*, Oakland, Canda, 2015: USENIX Association.

[58] A. S. Thombre and T. Aditya, "Physical Layer Secrecy Solution for Passive Wireless Sensor Networks," *IEEE*, 2015.

[59] A. Jules, "RFID Security and Privacy: A Research Survey," *IEEE Journal On Selected Areas in Communications*, vol. 24, no. 2, 2006.

[60] N. Rohit and G. Satashu "Secret Communication using Artificial Noise," presented at the IEEE 62nd Veh. Technol. Conf., 2005.

[61] G. Satashu and N. Rohit, "Guaranteeing Secrecy Using Artifical Noise," *IEEE Transactions On Wireless Communications*, vol. 7, no. 6, 2008.

[62] C. Kanapathippillai *et al.*, "Physical Layer Security Jamming: Theoratical Limits and Practical Designs in Wirless Networks," *IEEE*, 2016.

[63] F. S.Ali A. and S. A.Lee, "Solutions for the MIMO Gaussian Wiretap Channel With a Cooperative Jammer," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, 2011.

[64] M. Amitav and H. Jing, "Deploying Multi-Antenna Energy-Harvesting Cooperative Jammers in the MIMO Wiretap Channel," in *Asilomar Conf.*, 2012, pp. 1886-1890.

[65] H. Jing and S. A.Lee, "Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization," *IEEE Transcations on Signal Processing* vol. 60, no. 4, 2012.

[66] K. Ashish and W. Gregory W, "Secure Transmission With Multiple Antennas-Part II: The MIMOME Wiretap Channel," *IEEE TRANSACTIONS OF INFORMATION THEORY* vol. 56, no. 11, 2010.

[67] L. Qiaolong, S. Huawei, and H. Kaizhi, "Achieving Secure Transmission with Equivalent Multiplicative Noise in MISO Wiretap Channels," *IEEE Communications Letters,* vol. 17, no. 5, 2013.

[68] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO Wiretap Channels with Multi-Antenna Passive Eavesdropper: Artifical Noise vs. Artifical Fast Fading," *IEEE Transactions on Wireless Communications*, 2013.

[69] V. Nachiappan, L. Angle, and H. W. Robert, "Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication," 2012.

[70] M. Hafez and H. Arslan, "On Directional Modulation: An Analysis of Transmission Scheme with Multiple Directions," *IEEE,* 2015.

[71] A. Babakhani, D. Rutledge, and A. Hajumiri, "A Near-Field Modulation Technique Using Antenna Reflector Switching," in *Proc., IEEE Intl. Solid State Circuits Conf. (ISSCC)*, 2008, pp. 188-605.

[72] D. P. Michael and B. T. Jennifer, "Beamsteering in Pattern Reconfigurable Arrays Using Directional Modulation," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 7, 2010.

[73] Y. Ding and V. F. Fusco, "Developments in Directional Modulation Technology," *FERMAT*, vol. 13, 2016.

[74] H. Jinsong, S. Feng, and L. Jun, "Robust Synthesis Method for Secure Directional Modulation With Imperfect Directional Angle," *IEEE Communications Letters*, vol. 20, no. 6, 2016.

[75] C. M. Elam and D. A. Leavy, "Secure Communication using Array Transmitter," Patent Appl. US06/788,617, 2001.

[76] D. Yuan and F. F. Vinecent, "A Vector Approach for the Analysis and Synthesis of Directional Modulation Transmitters," *IEEE Transacations on Antennas And Propagation*, vol. 62, no. 1, 2014.

[77] G. Bin and Y. Yu-hong, "Combinatorial Interference Directional Modulation for Physical Layer Security Transmission," *IEEE*, 2016.

[78] B. Qiu, J. Xie, L. Wang, and Y. Wang, "Artificial-Noise Aided Secure Transmission for Proximal Legitimate User and Eavesdropper Based on Frequency Diverse Arrays," *IEEE*, 2018.

[79] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO Wiretap Channels with Multi-Antenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading," *IEEE Transcations on Wireless Communications,* 2013.

[80] Y. Ding and V. F. Fusco, "A Vector Approach for the Analysis and Synthesis of Directional Modulation Transmitters," *IEEE Transactions of Antennas And Propagation*, vol. 62, no. 1, 2014.

[81] D. Yuan and F. Vincent, "Directional Modulation Transmitter Synthesis using Particle Swarm Optimization " presented at the Loughborough Antennas & Propagation Conference Loughborough, UK, 2013.

[82] D. Yuan and F. Vincent, "BER Driven Synthesis for Directional Modulation

Secured Wireless Communication " *International Journal of Microwave and Wireless Technologies* vol. 6, no. 2, 2013.

[83] D. Yuan and F. Vincent, "Directional Modulation Transmitter Radiation Pattern Consideration," *IET Microw. Antennas Propag.*, vol. 7, no. 15, pp. 1201-1206, 2013.

[84] D. Yuan and F. F. Vincent, "Establishing Metrics for Assessing the Performance of Directional Modulation Systems," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 5, 2014.

[85] S. Rishad, R. Shahriar, and I. Razibul, "On the Extended Relationships Among EVM, BER and SNR Performance Metrics," presented at the 4th International Conference on Electrical and Computer Engineering Dhaka, Bangladesh, 2006.

[86] C. Long, X. Xinyu, S. Leixin, and L. Shaoqian, "A Novel Approach for the Analysis and Synthesis of High Order Directional Modulation," *IEEE 4th Information Technology and Mechatronics Engineering*, 2018.

[87] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xianobo, "Artificial-Noise-Aided Secure Multicast Precoding for Directional Modulation Systems," *IEEE Transactions On Vehicular Technology*, vol. 67, no. 7, 2018.

[88] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure Spatial Multiple Access Usign Directional Modulation," *IEEE Trans. Microw Theory Tech.*, pp. 563-570, 2018.

[89] D. Yuan and F. Vincent, "Improved Physical Layer Secure Wireless Communications Using a Directional Modulation Enhanced Retrodirective array," presented at the 2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS), Beijing, China, 2014.

[90] K. Ashkan, S. Mojtaba, M. Sina, C. Symeon, and o. Björn, "Secure M-PSK

Communication VIA Directional Modulation," *IEEE*, 2016.

[91] E. Gehad, S. Heba, K. Tamer, A. Khalid, and G. Mohsen, "Novel Hybrid Physical Layer Security Technique in RFID Systems," *IEEE*, 2019.

[92] E. Katisri, K. Pramatani, A. Billiris, A. Kaiafas, A. Christodoulakis, and H. Karanikas, "An RFID Based Blood Bank/Healthcare Information Management System," in *Mediteranean Conference on Medical and Biological Engineering and Computing*, 2016.