

INTELLIGENT REFLECTING SURFACE ASSISTED PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATION

BY

ABRAHAM SANENGA
Registration Number: 18100191

MEng COMPUTER AND TELECOMMUNICATIONS

A thesis submitted to the Faculty of Engineering & Technology in partial fulfilment of the requirements for the award of the degree of Master of Engineering in Computer and Telecommunications of Botswana International University of Science & Technology

July 2021

BOTSWANA INTERNATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY

MASTERS THESIS

Intelligent Reflecting Surface Assisted Physical Layer Security in Wireless Communication

by

Abraham SANENGA
Registration Number: 18100191
sa18100191@studentmail.biust.ac.bw

A thesis submitted to the Faculty of Engineering & Technology in partial fulfilment of the requirements for the award of the degree of **Master of Engineering in Computer and Telecommunications** of Botswana International University of Science & Technology

Supervisor: Dr. Bokamoso BASUTLI
basutlib@biust.ac.bw, (+267) 493 1679

Signed: _____

Date: 16 August 2021

Co-supervisor: Prof. Joseph M. CHUMA
chumaj@biust.ac.bw, (+267) 490 0117

Signed: _____

Date: 16/08/2021

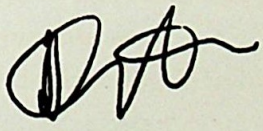
Faculty of Engineering & Technology
Department of Electrical, Computer and Telecommunications
Signal Processing, Networks & Systems Research Group

July 2021

Declaration of Authorship

I, Abraham SANENGA, declare that this thesis titled, "Intelligent Reflecting Surface Assisted Physical Layer Security in Wireless Communication" and the work presented in it are my own. I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University.
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
3. Where I have consulted the published work of others, this is always clearly attributed.
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
5. I have acknowledged all main sources of help.
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: 

Date: August 6, 2021

© This dissertation/thesis is copyright material protected under the Berne Convention, the Copyright Act of 1999 and other international and national enactments, in that behalf, on intellectual property. It must not be reproduced by any means, in full or in part, except for short extracts in fair dealing; for private researcher study, critical scholarly review or discourse with an acknowledgement, without the written permission of the office of the Deputy Vice Chancellor - Academic Affairs, on behalf of both the author and the Botswana International University of Science & Technology.

Certification

The undersigned certifies that they have read and hereby recommend for acceptance by the Faculty of Engineering & Technology, a thesis titled: **"Intelligent Reflecting Surface Assisted Physical Layer Security in Wireless Communication"**, in partial fulfilment of the requirements for the award of the degree of **Master of Engineering in Computer and Telecommunications** of Botswana International University of Science & Technology.

Signed: _____

Supervisor: Dr. Bokamoso BASUTLI
Department of Electrical, Computer and Telecommunications
Faculty of Engineering & Technology
basutlib@biust.ac.bw
(+267) 493 1679

Date: 16 August 2021

Signed: _____

Co-supervisor: Prof. Joseph M. CHUMA
Department of Electrical, Computer and Telecommunications
Faculty of Engineering & Technology
chumaj@biust.ac.bw
(+267) 490 0117

Date: 16/08/2021

BOTSWANA INTERNATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY

Abstract

Faculty of Engineering & Technology
Department of Electrical, Computer and Telecommunications

Master of Engineering in Computer and Telecommunications

Intelligent Reflecting Surface Assisted Physical Layer Security in Wireless Communication

by Abraham SANENGA

The open nature of radio propagation enables ubiquitous wireless communication, which allows seamless data transmission. However, unauthorized users may pose a threat to the security of the data being transmitted leading to network vulnerabilities such as hacking, eavesdropping, and jamming. Physical layer security (PLS) has been identified as one of the promising security approaches to safeguard the transmission in a wireless network. The intention is to augment the computationally demanding and complex cryptographic algorithms. Due to the random nature of the transmission channel such as scattering, it is possible for confidential and authentic signal transmission in the physical layer. The aim of this thesis is to propose and investigate mathematical optimization techniques for PLS. Firstly, optimal beamformers for the information signal and the jamming signal were designed with the aid of an intelligent reflecting surface (IRS) to significantly improve the secrecy rate of the legitimate transmission in the presence of an eavesdropper. Secondly, the problem of maximizing the energy harvested by energy receivers while satisfying the secrecy constraint at the legitimate receiver was considered. This was achieved through the use of an alternating algorithm to optimize the beamforming of information to the legitimate receiver and the manifold optimization approach to design optimal phase shifters of the IRS. The results shows that the use of both IRS and jamming offers an improvement in the secrecy rate by about 28 % to 33 % than in the conventional PLS schemes. It was also shown that increasing the number of IRS elements offers an improvement in the secrecy rate level. The second set of results showed that the use of IRS significantly improves the secrecy rate while achieving the minimum energy constraint set for the system.

Acknowledgements

I would like to thank my supervisors Dr. Bokamoso Basutli and Prof. Joseph Chuma for their guidance, assistance and support during the course of my studies at BIUST.

I would also like to thank my colleague Mr. Galefang Mapunda for his help and the discussions we had throughout our studies during the time we spent together both at BIUST and NARIT. In addition, my special thanks also goes to NARIT and their stuff for giving me an opportunity to gain experience while pursuing my studies.

Lastly, my most heartfelt gratitude goes to my family for their love, encouragement and unending support.

Contents

Declaration of Authorship iii

Certification v

Abstract vii

Acknowledgements ix

List of Figures xv

List of Abbreviations xvii

List of Symbols xix

1 Introduction to Physical Layer Security 1

1.0.1 Overview of PLS . . . 2
1.0.2 Problem Description . . . 3
1.0.3 Aim . . . 4
1.0.4 Research Objectives and Contributions . . . 4
1.0.5 Research Publications . . . 5
1.0.6 Motivation . . . 5
1.0.7 Thesis outline . . . 5

1.1 Background . . . 6

1.1.1 Overview of cryptography and PLS . . . 6
1.1.2 Information-theoretic security . . . 8
1.1.3 Mathematics Preliminaries . . . 12
Matrices . . . 12
Row space, column space & null space of a matrix . . . 13
Eigenvalues & eigenvectors . . . 13
Matrix Pencil . . . 13
Optimization . . . 13
1.1.4 Channel state information (CSI) . . . 15
1.1.5 Multiple-input multiple-output (MIMO) communication . . . 15

1.2 Performance metrics in PLS 17
Secrecy rate 17
Secrecy Outage Probability (SOP) 18
Quality of service (QoS)-related metrics 18

2 Technologies in PLS **19**
2.1 Secure multi-antenna techniques 19
2.1.1 Convex optimization 19
Quadratic programming (QP) 20
Semi-definite programming (SDP) 21
Fractional programming 21
2.1.2 Beamforming 22
Different beam forms 22
2.1.3 Artificial Noise (AN) precoding 28
2.1.4 Zero-Forcing 30
2.1.5 Space-time coding (STC) 32
2.1.6 Cooperative jamming 34
2.2 Emerging technologies 36
2.2.1 Wireless information and power transfer (WIPT) 36
2.2.2 Intelligent reflecting surface (IRS) 37
2.2.3 Visible light communication (VLC) 37
2.2.4 Unmanned aerial vehicle (UAV) 38
2.2.5 PLS in satellite communication 39

3 Information jamming and intelligent reflecting surface (IRS) scheme **43**
3.1 System model and problem formulation 43
3.1.1 System model 43
3.1.2 Secrecy maximization 45
3.2 Solution 45
3.2.1 Closed form solution for beamforming and jamming vectors, $\mathbf{w}$ and $\mathbf{v}$ given $\boldsymbol{\Theta}$ 46
3.2.2 Optimization of IRS phase shifting coefficients 48
3.3 Numerical results and simulations 50
Secrecy vs distance 51
Effect of increasing IRS elements 52
Transmit power vs distance and the secrecy rate 53
BER vs SNR 53

4 A physical layer security(PLS) scheme using wireless information and power transfer (WIPT) and intelligent reflecting surface (IRS) 55
4.1 System model and problem formulation 55
4.1.1 System model 55
4.1.2 Energy harvesting maximization 57
4.2 Numerical results and simulations 61

5 Summary and Future Directions 65
5.1 Conclusion 65
5.2 Future work 66
5.2.1 Machine learning-based channel estimation 66

List of Figures

1.1 PLS system model 3
1.2 The process of cryptography [15] 6
1.3 Wiretap channel 7
1.4 The difference between cryptography and physical layer security approaches [21] 8
1.5 Shannon information content 9
1.6 Shannon's wiretap channel 10
1.7 Wyner's wiretap channel 11
1.8 Wyner's transmission rate vs equivocation rate [7] 12
1.9 MIMO wiretap channel model [9] 17
1.10 MIMO channel capacity for different SNR values 17

2.1 Secure multi-antenna techniques 20
2.2 Beamforming 22
2.3 Transmit Beamformer 23
2.4 System model of multi-user and eavesdroppers pair with beamforming 25
2.5 Secrecy beamforming with AN 28
2.6 Zero forcing 31
2.7 BER and secrecy rate performance metrics simulations for different precoding schemes. 32
2.8 System block diagram 33
2.9 Secrecy with cooperative jamming 35
2.10 Secrecy rate against transmit power of Alice 36
2.11 WIPT system 37
2.12 Wireless communication system based on IRS. Adapted from [63]. . . 38
2.13 Power and illumination distribution against distance 39
2.14 Cooperative jamming using UAV 40
2.15 Multi-beam satellite communication network [71] 40

3.1 IRS system model 44
3.2 System setup 50
3.3 Secrecy rate vs distance. 51

3.4 Secrecy rate versus the number of reflecting elements. 53
3.5 Transmit power vs distance. 54
3.6 BER curves for Bob and Eve with transmit beamforming and IRS and artificial noise added 54

4.1 Energy harvesting system model 56
4.2 Transmit power vs Energy harvested with varying secrecy rate. . . . 62
4.3 Energy harvested with varying secrecy rate. 63

List of Abbreviations

AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CSI	Channel State Information
IRS	Intelligent Reflecting Surface
ITU	International Telecommunication Union
LTE	Long Term Evolution
MIMO	Multiple Input Multiple Output
MISO	Multiple Input Single Output
MRC	Maximum Ratio Combining
OFDM	Orthogonal Frequency Division Multiplexing
PLS	Physical Layer Security
QoS	Quality of Service
QP	Quadratic Program
SDP	Semi Definite Program
SIMO	Single Input Multiple Output
SINR	Signal-to- Interference-plus- Noise Ratio
STBC	Space- Time Block Code
SVD	Singular Value Decomposition
UAV	Unmanned Aerial Vehicle
URLLC	Ultra- Reliable Low Latency Communication
VLC	Visible Light Communication
WIPT	Wireless Information and Power Transfer
ZF	Zero Forcing

List of Symbols

$\mathbf{x}$	Bold-face and lower-case letters denotes a vector
$\mathbf{A}$	Bold-face and upper-case letters denotes a matrix
$\mathbf{I}$	Identity matrix
$\mathbb{R}$	A set of real numbers
$\mathbb{R}^n$	n-dimensional Real vectors
$\mathbb{C}$	A set of complex numbers
$\mathbb{C}^n$	n-dimensional complex vectors
$(\cdot)^T$	Transpose operation
$(\cdot)^H$	Hermitian operation
$\|\cdot\|$	The absolute value
$\|\cdot\|$	l_2 norm
$\text{diag}\{\cdot\}$	The diagonal elements of a square matrix
$\text{Tr}(\cdot)$	Trace operator
$\mathbf{A} \succeq 0$	A is PSD matrix
$\mathbb{E}\{\cdot\}$	Expectation operator
$\lambda_{max}(\cdot)$	The maximum eigenvalue of the matrix
$\Re\{\cdot\}$	Real part of a complex number
$\Im\{\cdot\}$	Imaginary part of a complex number
$\arg\{\cdot\}$	The phase of a complex number
$\text{rank}(\cdot)$	The rank operator
$\log_2(\cdot)$	Logarithm to base 2
$\log(\cdot)$	The natural logarithm
$[x]^+$	Positive part of x, that is $[x]^+ = \max(x, 0)$

In dedication to my beloved grandmother, and in memory of my mother.

Chapter 1

Introduction to Physical Layer Security

Wireless communication technology is a necessity for modern-day life because human beings depend on this technology for data transmission. In most cases, the said data contains confidential information such as banking transactions, military applications and multimedia. The International telecommunication organization approximated that 53.6 percent of the world population, which amounts to about 4.1 billion people were using the internet at the end of 2019 [1]. It is expected that this number will rise due to a rapid increase in active mobile subscribers as wireless networks continue to expand, and new applications are developed. However, it is reported in [2] that an increasing number of mobile and wireless devices are affected by cyber-criminal activities. Cyber security ventures [2], predicted that cyber crime costs will increase to more than six trillion US dollars annually by 2021 from three trillion US dollars recorded in 2015. Therefore, it is highly important to improve wireless networks against cyber-criminal activities.

Conventionally, upper layers of the open system interconnect model are utilized to handle any discrepancies related to the attributes of authenticity, confidentiality and privacy of data transmission. These attributes are mostly dependent on cryptographic algorithms which include secret-key distribution, public-key, and symmetric encryption. All these techniques function independently from the physical layer [3]. Based on the assumption that the eavesdropper has limited computing power ability, the above mentioned techniques are considered to be secure. Moreover, they rely on underlying computational complexity for their robustness. Recent advances in quantum computing, pose a serious threat to the currently used cryptographic schemes with its unlimited computational capacity [4]. Therefore, it is evident that the relevance of the conventional methods in secure wireless communication is becoming less reliable.

The open and superposition nature of wireless networks raises issues of confidentiality and security on the transmitted data when unintended users are present.

Difficulties which prevent the transmitted signal from reaching the unintended users are a result of the broadcast nature. On the other hand, the time-varying and fluctuations of the wireless channel results in the arrival of multiple copies of the transmitted signal at the receiver. With that being said, security attacks in wireless networks may be categorized as active and passive attacks [5]. Passive attacks involves eavesdroppers who listens to the ongoing transmission silently and tries to steal the transmitted information without interrupting legitimate transmission [6]. Under active attacks, the eavesdroppers use more aggressive and intrusion techniques which attempts to deteriorate the received signal quality at the intended user. The common examples of these aggressive techniques are the denial of service, routing, and node malfunction attacks [5]. With exposure to such many attacks, wireless networks are required to have certain capabilities that will enable them to withstand and mitigate these attacks. The desired characteristics of a secure network are shown in Table 1.1 include integrity, confidentiality & authentication, availability, and access control [5].

Table 1.1: Wireless security requirements

Security Requirement	Objective
Integrity	Defined to guarantee the accuracy of the transmitted information without any modifications.
Confidentiality	States that the transmitted message content should only be accessible to the sender.
Authentication	Establish proof of identities between authorized and unauthorized users.
Availability	Specifies that resources should be available to authorized parties at all times
Access control	Defines the ability to control and manage devices that are permitted to access the legitimate transmission process

1.0.1 Overview of PLS

PLS dates back from the 1970s with a mathematical description of a wiretap channel [7]. Following the advancements in massive MIMO and integration of technologies such as IEEE 802.11n and long term evolution (LTE) a major interest in PLS research was revived over the last decade. The current research is focused towards utilizing

the MIMO spatial degrees of freedom in order to leverage security benefits [8]. A typical network in which PLS is employed comprises of three nodes viz. a transmitter, a legitimate receiver, and an eavesdropper. With this setup, the transmitter under normal circumstances sends a private message to the receiver. The transmitted message is protected from any form of interception by the eavesdropper [9]. The adopted general convention is that the transmitter is named "Alice", whilst the eavesdropper and the legitimate receiver are referred to as "Eve" and "Bob", respectively. This model is illustrated in Figure 1.1.

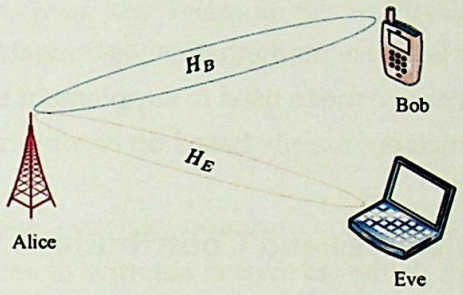


FIGURE 1.1: PLS system model

1.0.2 Problem Description

The open nature of radio propagation enables ubiquitous wireless communication. This allows for seaming less data transmission. However, unauthorized users may pose a threat to the security of the data which is being transmitted to the authorized users. This gives rise to network vulnerabilities such as hacking, eavesdropping, and jamming of the transmitted information. Physical layer security (PLS) has been identified as one of the promising security approaches to safeguard the transmission from eavesdroppers in a wireless network. It is an alternative to complement the computationally demanding and complex cryptographic algorithms and techniques. PLS is continually receiving exponential research interest owing to the possibility of exploiting the characteristics of the wireless channel. One of the main characteristics which PLS makes use of, is the randomness nature of the transmission channel. The aforesaid nature makes it possible for confidential and authentic signal transmission between the sender and the receiver in the physical layer. This field of study is called physical layer security. The conventional physical layer security multi-antenna techniques which includes but not limited to beamforming, zero-forcing, artificial noise and convex optimization has been well investigated in the literature. With the proliferation of wireless communication networks and the unending demand for higher bandwidths and data rates mobile operators have been

forced to migrate to millimeter frequencies to meet these needs. Due to high signal attenuation, fading and multi-paths which occurs at these frequencies, intelligent reflecting surfaces has recently been proposed to counter these downfalls. Most research on IRS has however been aimed at improving signal reception in a fading and multipath environment. This thesis will leverage the signal gains improvement provided by the IRS to implement physical layer security as it has been shown in the literature [10, 11, 12, 13, 14] that IRS will be at the core of 6G wireless networks.

1.0.3 Aim

The aim of this research is to use mathematical optimization to investigate physical layer security as an alternative mean used to supplement existing security measures in wireless networks which are mainly based on cryptographic algorithms.

1.0.4 Research Objectives and Contributions

1. Beamforming and AN have been well investigated as means of implementing security in the physical layer. One of the objective of this thesis is to develop optimal beamformers which maximizes the secrecy rate using a joint design of beamforming and jamming.

2. Recently, intelligent reflecting surfaces have been proposed as one of the key technologies for 5G wireless networks and beyond. Most of the existing works have studied and employed the IRS with beamforming as means of implementing PLS without including jamming. This has motivated another objective of this thesis which is to consolidate IRS with information jamming to find out whether using both jamming and IRS can have any significant impact on the level of secrecy rate of the wireless communication networks.

3. Information transmitting signals have been explored in the literature as a possibility for harvesting energy in wireless networks. However, high RF signals attenuation with increasing distance is a major drawback in the capacity of the energy that can be harvested. IRS offers an effective means for boosting the energy harvested by means of phase shifting. Therefore, this thesis is proposes an algorithm which can maximize the energy harvested by the energy harvesting receivers while ensuring the secrecy rate requirements are satisfied for the legitimate receiver in the wireless network.

4. The main contribution of this work is that the optimal solution for jamming beamforming vectors and IRS reflecting coefficients of the PLS optimization

problem are derived. The consolidation of both jamming and IRS created a problem which is non-convex and difficult to solve due to the non-convexity and unit-modulus constraints. This work proposed an alternating algorithm and show that this problem can be solved in an alternating manner and the optimal solutions to the problem can be achieved.

1.0.5 Research Publications

1. **A. Sanenga**, G. A. Mapunda, M. T. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, "An Overview of Key Technologies in Physical Layer Security," Entropy, vol. 22, no. 11, pp. 1–33, Nov. 2020.

1.0.6 Motivation

The inception of technologies such as quantum computing poses a major threat in existing security techniques in wireless networks, which means that wireless communication is not completely secure. PLS offers an additional solution to exploit the secrecy possibilities that the wireless channel offers. The main motivations behind PLS are; 1) to use the physical layer of the wireless network to supplement the existing security mechanisms in wireless networks which are based on cryptography algorithms implemented at the upper layer of the protocol stack, and 2) to find and develop new security technologies compatible with recent developments of the 5G and 6G wireless networks as well as MIMO communication.

1.0.7 Thesis outline

This thesis is organised into five chapters. The breakdown of each chapter is as follows:

Chapter 1 introduces the concepts of physical layer security, its underlying principles as well as the mathematical background. The motivation of this work, the objectives and contributions as well as the publication produced are also found in this chapter.

In Chapter 2, the conventional technologies as well as some of the emerging technologies in PLS are discussed.

The secrecy rate optimization problem in a MISO system is studied in Chapter 3. This is performed by optimizing of information beamforming and jamming vectors as well as optimizing the phase shifts of an intelligent reflecting surface.

In Chapter 4, energy harvesting maximization of energy harvesting receivers in the wireless network is studied. The maximization of the harvested energy is constrained to the satisfaction of the required secrecy rate of the system.

Finally, Chapter 5 covers the summary of the work and provide some of the open research problems for possible future works.

1.1 Background

1.1.1 Overview of cryptography and PLS

Cryptography is the method of transforming data into an unreadable format so that only the authorized recipient can understand and be able to decode it [15]. The main process of cryptography is shown in Figure 1.2. Encryption uses coding to transform plain text into a ciphertext, whereas decryption uses a decoding process to convert the ciphertext text back to a plain text using the shared public keys. Cryptography can be divided into three main types which are, hash functions, public-key cryptography and secret key cryptography [16]. The latter uses only one digital key to encrypt and decrypt data for both the sender and the receiver. Meanwhile, the first mentioned type utilizes a pair of public digital keys. In this case, one key is a public key used by the sender to encrypt the message, and the other key is a secret key used by the receiver to decrypt the information. Lastly, cryptographic hash functions map strings of different lengths to short, fixed size, outputs [16].

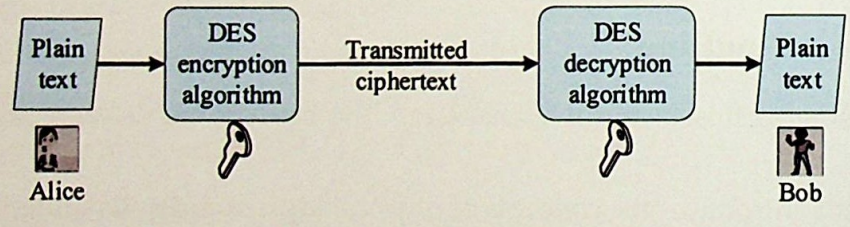


FIGURE 1.2: The process of cryptography [15]

In most cases, cryptography is the main technology which is being utilized to address security issues for conventional and some of the modern day electronic communication systems. From another perspective, some of the novel technologies, mainly quantum computing are a threat to systems that are based on cryptography. Quantum computers have close to unbounded computing capabilities such as the ease of breaking the encryption and decryption keys. The ability to guess the secret keys or perform a quick reverse calculation using a quantum computer enables breakage of such keys and this gives unauthorized or disguised network

users the ability to intercept the ongoing data transmission or access the data [4]. With that being said, it is worth noting that quantum computing is however limited to some extent as it cannot break all kinds of cryptographic algorithms. This means that it is one of the technologies which jeopardizes some of the existing systems based on cryptography. Furthermore, the processes involved in cryptography can impose some delays which can be unwelcome in some applications, such as the fifth generation (5G) ultra-reliable low latency communication (URLLC) [17]. Moreover, cryptographic methods are inefficient in terms of energy consumption as they require extra resources for performing computations. Therefore, this calls for the need to implement new measures with an effort to augment cryptography. One of the technologies directed towards augmenting cryptography is physical layer security (PLS) [6, 18, 19].

PLS is different from cryptography technology because it is based on the concept of information-theoretic security proposed by Wyner [7]. The concept of PLS describes communication between two authorized users in the presence of an unintended user by modeling a discrete memoryless wiretap channel [20]. Figure 1.3 shows the general case of the wiretap channel where two authorized users communicate over the main channel and are observed by an eavesdropper through a wiretap channel. Figure 1.4 illustrates the fundamental differences between cryptography and PLS. [21].

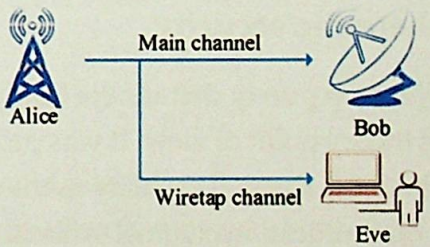


FIGURE 1.3: Wiretap channel

In contrast to cryptography, PLS schemes can seamlessly prevent the unintended users from intercepting data signals which are being transmitted. PLS is able to facilitate security without any form of encryption in the upper layers. The facilitation of key free encryption is made possible by the exploitation of some wireless channel characteristics through the application of suitable signaling and channel coding [9]. PLS techniques have been proved to be capable of realizing verifiable security even when the network intruders have almost limitless computational resources. Despite the unparalleled benefits of PLS, it is worth noting that there exist some shortfalls. It was shown in [22] that it is almost impossible to warrant maximal security with a probability of one since PLS relies mainly on the average information. In addition,

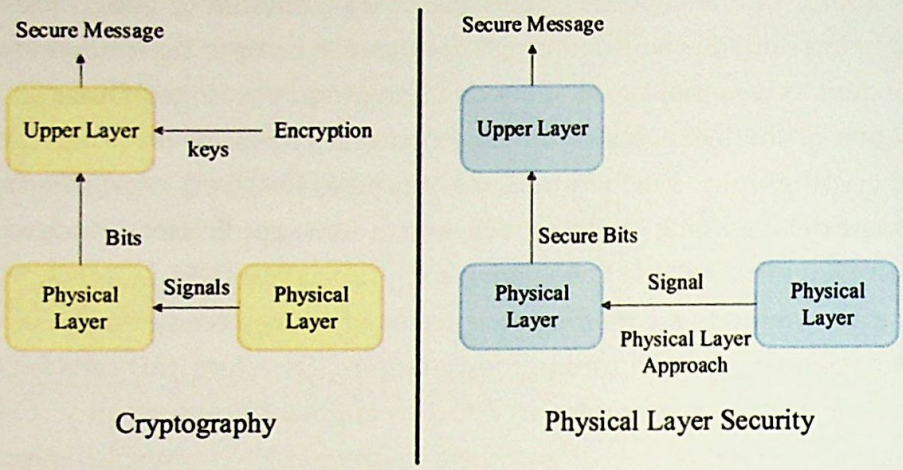


FIGURE 1.4: The difference between cryptography and physical layer security approaches [21]

most of the PLS schemes assume prior knowledge of the eavesdropper's wiretap channel, which is not feasible in practical applications. Having stated the aforementioned benefits of both technologies, investigations on the concurrent use of PLS and cryptography are worth looking into to provide elevated robustness of the communication network.

1.1.2 Information-theoretic security

This is the kind of security which purely defines the fundamental limits of PLS measures from an information theory point of view. It was proposed by Claude Shannon in 1949 [23]. Shannon defined the channel capacity as the maximum rate of information transmission over a communication channel with an arbitrarily low probability of error. For an additive white Gaussian noise (AWGN) channel, the channel capacity is given by [23]:

$$C = B \log_2(1 + \mathrm{SNR}), \tag{1.1}$$

where B represents the channel's bandwidth (fixed quantity) in Hertz (Hz), and SNR is the signal-to-noise ratio. The SNR is mathematically denoted by Equation 1.2. From Equation 1.1, it can be seen that the channel capacity is directly proportional to the power of the signal.

$$\mathrm{SNR} = \frac{P}{\sigma^2}, \tag{1.2}$$

where P denotes the power of the signal and σ^2 is the noise power.

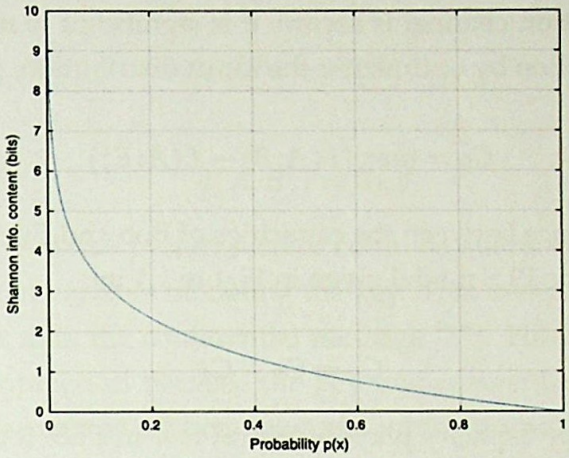


FIGURE 1.5: Shannon information content

The Shannon information content of an outcome, x_i, is defined as:

$$h(x_i) = \log_2 \left(\frac{1}{p(x_i)} \right) = -\log_2 p(x_i). \tag{1.3}$$

where the probability of the random variable, X is denoted by $p(x_i)$. Figure 1.5 shows a graph of Shannon information content versus the different probabilities and it illustrates that less probable or rare outcomes contain more information than common or high probable outcomes. The entropy function $\mathbf{H}(X)$ is the average of the Shannon information content and it is given by:

$$H(X) = \sum_{i=1}^{M} p(x_i) \log_2 \left(\frac{1}{p(x_i)} \right) = -\sum_{i=1}^{M} p(x_i) \log_2 p(x_i). \tag{1.4}$$

where M is the total number of possible outcomes. The mutual information, $I(X;Y)$, defines the amount of information X conveys about Y:

$$I(X;Y) = H(X) - H(X \mid Y). \tag{1.5}$$

Therefore this implies that the amount of information sent to Bob by Alice is given by Equation 1.6 whereas the same quantity between Alice and Eve is given by Equation 1.7.

$$I(A;B) = H(A) - H(A \mid B), \tag{1.6}$$

$$I(A;E) = H(A) - H(A \mid E), \tag{1.7}$$

where random variable A, represents the bit sent by Alice. B, denotes the bits received by Bob, and the outcome observed by Eve is denoted by E. In order to ensure

that the communication channel is secure, it is significant to maximize the achievable mutual information by optimizing the input distribution, $p_{(A)}$ such that [24]:

$$C_S = \max_{p_{(A)}} \left(I\left(A;B\right) - I\left(A;E\right) \right). \tag{1.8}$$

Therefore the difference between the capacities of Bob and Eve's channels gives the secrecy capacity of the PLS model given in Figure 1.1 by:

$$C_S = C_B - C_E. \tag{1.9}$$

The notion of secrecy capacity plays a central role in PLS. It's a metric which de-

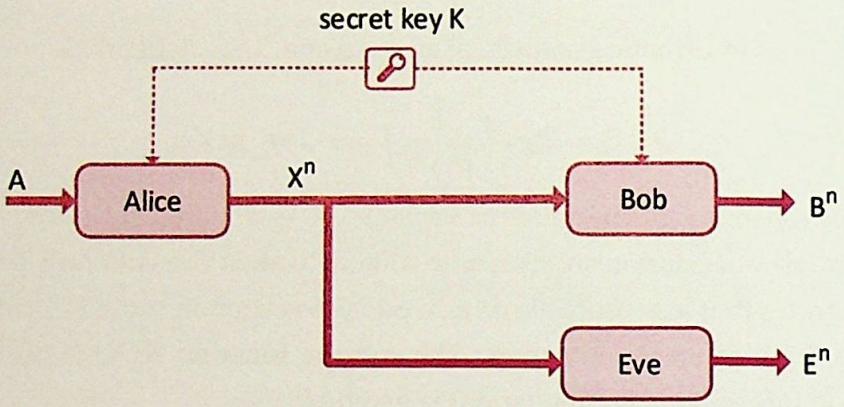


FIGURE 1.6: Shannon's wiretap channel

fines the rate at which the transmitted signal reaches the legitimate receiver without any form of invasion from the eavesdropper. To define perfect secrecy, we consider Shannon's wiretap channel model shown in Figure 1.6. In this model, Alice intends to transmit confidential information, A, to an authentic receiver, Bob, under a condition that there exist an eavesdropper, Eve. A is encoded into X^n which represents the information vector of length n. The received information vectors for Bob and Eve are given by B^n and E^n, respectively. Consequently, the source information entropy together with the amount of uncertainty of the message received by Eve are given by $H(A)$ and $H(A \mid E^n)$, respectively. Shannon showed that legitimate parties could achieve information-theoretically secure communication in a wireless communication environment by using the same random secret key which is unknown to the eavesdropper. This is known as perfect secrecy, and it is given by Equation 1.10 in terms of the entropy. Transforming Equation 1.10 into Equation 1.11 shows that the eavesdropper is not able to receive any of the transmitted information content.

$$H(A|E^n) = H(A) \tag{1.10}$$

$$I(A, E^n) = 0 \tag{1.11}$$

The theorem also proved that perfect secrecy could be guaranteed if $H(K) \geq H(A)$, where K is the random variable modeling the key. This means that the key should be equal to or longer than the confidential message [25]. However, perfect secrecy was proved to be impractical because the key management may be cumbersome for specific networks such as ad hoc networks which do not operate under fixed infrastructures [26].

To expand Shannon's information-theoretic secrecy theorem, Wyner proposed the concept of weak secrecy. Weak secrecy is defined by the Wyner's wiretap channel model shown in Figure 1.7. In this model, the encoder operates on blocks of k source bits $A^k = (A^1, A^2, ..., A^k)$ and produces an encoded sequence $X^n = (X^1, X^2, ..., X^n)$ of length n. The transmission rate, which is the proportion of infor-

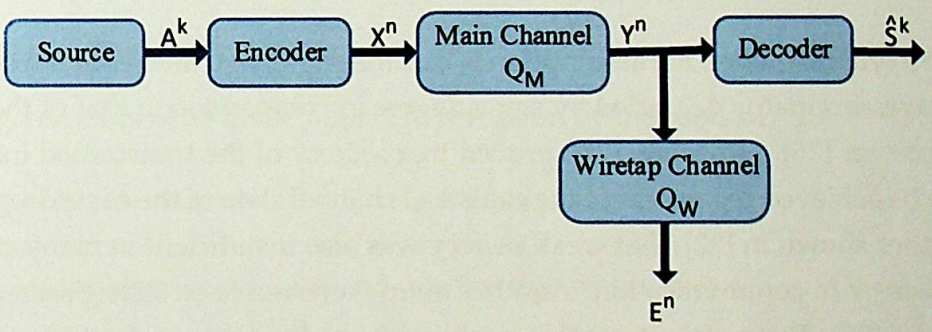


FIGURE 1.7: Wyner's wiretap channel

mation sent in each codeword, is given by Equation 1.12. The equivocation rate, defined as a measure of confusion at the eavesdropper, is employed to investigate the weak secrecy of transmitted information. The said rate is given by Equation 1.13.

$$R = k/n \qquad (bits/channel), \tag{1.12}$$

$$\Delta = \frac{1}{k} H(A^k|E^n), \tag{1.13}$$

where k is the total number of source bits in the code, and n is the code length. A scheme is considered to have weak secrecy in the event that,

$$\lim_{n\to\infty} \frac{1}{n} I(A, E^n) = 0. \tag{1.14}$$

Unlike the Shannon perfect secrecy metric, this metric proved that it is possible to obtain secrecy in a practical scenario [27]. Figure 1.8 illustrates the relationship between the transmission rate and equivocation. It shows the region of achievable pairs as (R, Δ) [7]. The highest rate that capable of achieving the complete equivocation, H_s i.e confusion at the eavesdropper, is the secrecy capacity, C_s of the channel.

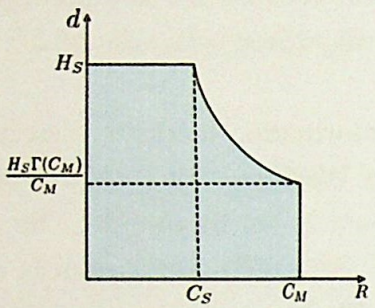


FIGURE 1.8: Wyner's transmission rate vs equivocation rate [7]

With Wyner's model, the assumption is that the signal that arrives at the receiver of the eavesdropper is degraded by some degree in comparison to that of the legitimate receiver [25]. However, [28], proved that secrecy of the transmitted information can be achieved regardless of the statistical channel state of the eavesdropper. It was further shown in [22], that weak secrecy was also insufficient in many cases to prove secrecy in communication. Another metric referred to as strong secrecy was defined by [29]. The metric states that a scheme is said to achieve strong secrecy if:

$$\lim_{n\to\infty} I(A, Z^n) = 0. \tag{1.15}$$

Subsequently, in [30], strong secrecy was proved to be inefficient for some applications. This is based on the assumption of random and uniformly distributed message symbols over the message alphabet at the input of the secrecy encoders. In practice, the limitation is caused by the unavailability of universal compression algorithms capable of providing messages that have the distribution mentioned above.

1.1.3 Mathematics Preliminaries

Matrices

Let **A** represent an $m \times n$ matrix;

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Row space, column space & null space of a matrix

The column space of $\mathbf{A}$ is the maximum number of linearly independent columns of $\mathbf{A}$. Similarly the row space of $\mathbf{A}$ is the maximum number of linearly independent rows of $\mathbf{A}$.

$$\begin{aligned} \textit{Row rank}(\mathbf{A}) &= \textit{Column rank}(\mathbf{A}) \\ &= \textit{Rank}(\mathbf{A}) \end{aligned} \tag{1.16}$$

The null space of any matrix $\mathbf{A}$, $\mathcal{N}(\mathbf{A})$, consists of all the vectors $\mathbf{x}$ such that $\mathbf{Ax} = 0$ and $\mathbf{x}$ is not zero. The null space of a matrix represents the solution obtained from $\mathbf{Ax} = 0$.

Eigenvalues & eigenvectors

The eigenvectors of a square matrix $\mathbf{A}$, are given by the roots of:

$$\mathbf{Ax} = \lambda \mathbf{x}, \tag{1.17}$$

where $\mathbf{x}$ is the eigenvector of $\mathbf{A}$ and λ is the eigenvalue of $\mathbf{A}$.

Matrix Pencil

The eigenvalue and eigenvector problem of the matrix pencil, $(\mathbf{A}, \mathbf{B})$ is given by;

$$\mathbf{B}^{-1}\mathbf{Ax} = \lambda \mathbf{x}. \tag{1.18}$$

Optimization

Mathematical optimization, specifically convex optimization are very crucial in facilitating the analysis and deriving numerical solutions of many wireless communication problems. Convex optimization is applied when given a cost function which is also called an objective function, which has to be maximized in order to find an

optimal value of a certain variable that gives the optimal value of the objective function. This means trying to minimize a cost function in particular a convex optimization problem. A convex optimization problem is one of the form [31];

$$\begin{aligned} \min_{\mathbf{x}} \quad & f_0(\mathbf{x}) \\ \text{s.t.} \quad & f_i(\mathbf{x}) \leq b_i, \quad i = 1, \ldots, m, \\ & h_i(\mathbf{x}) = 0, \quad i = 1, \ldots, n, \end{aligned} \tag{1.19}$$

where $\mathbf{x} \in \mathbb{R}^n$ is the optimisation variable, $f_0 : \mathbb{R}^n \to \mathbb{R}$ is the cost function or the objective function, $f_i : \mathbb{R}^n \to \mathbb{R}$ are the functions for the inequality constraints, and $h_i : \mathbb{R}^n \to \mathbb{R}$ are the functions for the equality constraint.

Convex sets: A set $S \subseteq \mathbb{R}^n$ is regarded as a convex set if when taking any two points $x_1, x_2 \in S$, the entire line segment joining x_1, x_2 belong to S. Mathematically, it is defined as;

$$\theta x_1 + (1-\theta)x_2 \in S, \quad \forall\, [0,1]. \tag{1.20}$$

In general, a convex set must be a solid body, containing no holes. Examples of convex sets include hypercubes, ellipsoids, polyhedral sets, and so on.

Affine set: A set S is said to be an affine set if for any two distinct points x_1, x_2, the line passing through these points lie in the set S, that is $x_1, x_2 \in S$. Mathematically, it is defined as;

$$\theta x_1 + (1-\theta)x_2 \in S, \ \forall\, \theta. \tag{1.21}$$

Every affine set is convex. An example of an affine set is a hyperplane.

Convex function: A function $f(\mathbf{x})$ is said to be convex if for any two points x_1, x_2;

$$f(\theta x_1 + (1-\theta)x_2) \leq \theta f(x_1) + (1-\theta) f(x_2). \tag{1.22}$$

The domain of f is a convex set.

Lagrangian function: The Lagrangian function is used to obtain solutions of the convex optimization problem by summing together the constraints and the objective function using Lagrangian multipliers. The Lagrangian function $\mathcal{L} : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}$ is defined as;

$$\mathcal{L}(\mathbf{x}, \boldsymbol{\lambda}, \mathbf{v}) = f_0(\mathbf{x}) + \sum_{i=1}^{m} \lambda_i f_i(\mathbf{x}) + \sum_{i=1}^{p} v_i h_i(\mathbf{x}), \tag{1.23}$$

where λ_i is the Lagrange multiplier associated with the inequality constraint, and v_i is the Lagrange multiplier associated the equality constraint [31].

1.1.4 Channel state information (CSI)

CSI defines the properties of a channel in a wireless communication link. CSI is used to describe the propagation of the transmitted signal in relation to the corresponding effects such as scattering, fading and power decay with distance. Wang et al. in [9], shows that the availability of CSI is one of the most important aspects to be taken into consideration when choosing an appropriate secrecy performance metric in order to design optimal transmission strategies in PLS. CSI can be categorized into two classes and they are referred to as perfect and imperfect CSI. The latter is concerned with the characterization of the statistical information only. Such information include the average channel gain, the type of fading distribution, the line-of-sight (LOS) component and the spatial correlation. The former involves the complete knowledge of the channel properties of a communication link.

In practice, CSI is initially not available at the transmitter and receiver terminals. It is gathered through some channel estimation methods such as those found in [32, 33]. The two channel estimation mechanisms commonly employed to acquire CSI are; the pilot-based channel training and channel state feedback. In pilot-based channel training, the transmitter distributes the total transmission time and energy such that some of the energy and time are allocated for the transmission of pilot symbols while the remaining portion is used for data transmission. In the channel state feedback method, the receiver is required to share its estimated channel knowledge with the transmitter prior to transmission. It is shown in [34] that the greatest level of security could be achieved if the transmitter has full knowledge of both the wireless channels to the intended user and the unintended user. This can be achieved by designing MIMO transmit precoders that minimize the information leaked to the eavesdropper's channels or to accurately direct jamming signals towards the eavesdroppers. However the exact CSI is not known in practise, only an estimate of the channel coefficient of CSI is known.

1.1.5 Multiple-input multiple-output (MIMO) communication

MIMO is a very powerful technology in wireless communication systems. A MIMO network structure consists of many antennas at the transmitter as well as at the receiver. MIMO technology has been well studied and developed for the past decade, mainly because of its capability to significantly enhance performance and widen the

coverage range of the wireless communication systems [35]. Some of its other important benefits that have been shown include but not limited to its, capability to provide higher data rates, improved reliability, and less noise and interference [36]. Even though MIMO technology was proposed many years back, it only came to reality in the practical world in 2018 [37]. This research work focuses on the relevance and application of MIMO technology in PLS rather than its traditional capacity benefits in the wireless communication networks. It was shown in [38] that MIMO systems are very robust against passive eavesdropping attacks since the secrecy capacity is directly proportional to the difference in capacities of the main and wiretap channels. Beamforming in massive MIMO was used in [39] to implement security in physical layer. In [40], artificial noise generation was used to demonstrate the application of PLS in MIMO orthogonal frequency division multiplexing (OFDM) systems. A typical MIMO system is shown in Figure 1.9 wherein the transmitter, the legitimate receiver, and the eavesdropper have multiple antennas N_A, N_B, N_E. This is referred to as MIMO multiple-antenna eavesdropper (MIMOME) [9], and in this case, the secrecy capacity can be expressed as;

$$C_s = \max_{K_x \succ 0, tr(K_x \preceq P)} \frac{\log_2|\mathbf{I} + \mathbf{H}_b \mathbf{K}_x \mathbf{H}_b^H|}{\log_2|\mathbf{I} + \mathbf{H}_e \mathbf{K}_x \mathbf{H}_e^H|}, \tag{1.24}$$

where $\mathbf{I}$ is the identity matrix, $\mathbf{K}_x$ is the covariance matrix of transmit signal, x, P is the maximum transmit power constraint, $\mathbf{H}_b \in \mathbb{C}^{N_B \times N_A}$ and $\mathbf{H}_e \in \mathbb{C}^{N_E \times N_A}$ are the MIMO complex Gaussian channel matrices of legitimate and wiretap channel, respectively. The signals received by the legitimate receiver and passive eavesdropper are given by Equation 1.25:

$$\begin{aligned} \mathbf{y}_b &= \mathbf{H}_b \mathbf{x}_a + \mathbf{n}_b, \\ \mathbf{y}_e &= \mathbf{H}_e \mathbf{x}_a + \mathbf{n}_e, \end{aligned} \tag{1.25}$$

where $\mathbf{x}_a \in \mathbb{C}^{N_A \times 1}$ is the transmit signal and $\mathbf{n}_b \in \mathbb{C}^{N_B \times 1}$, $\mathbf{n}_e \in \mathbb{C}^{N_E \times 1}$ are zero-mean complex white Gaussian additive noise vectors. Equation 1.25 is used as a fundamental tool in optimization techniques in PLS and also to demonstrate the application of MIMO in PLS.

The capacity of different MIMO channels against different SNR levels is plotted in figure 1.10. It can be seen that the capacity of the channel increases with the increasing number of transmitters at both the transmitter or receiver, and it is much higher for high SNR level.

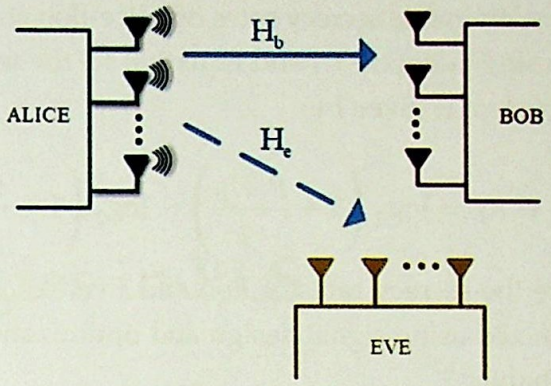


FIGURE 1.9: MIMO wiretap channel model [9]

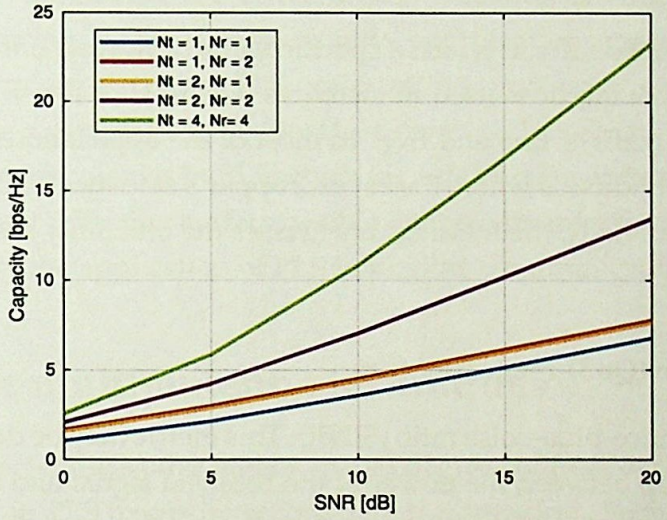


FIGURE 1.10: MIMO channel capacity for different SNR values

1.2 Performance metrics in PLS

The secrecy metrics from information-theoretic security are well established and they laid the foundation of secrecy coding in the physical layer. However, they are challenging to evaluate and measure especially when the coded sequence have a finite block length [34]. Therefore, different metrics which are much easier to work with were proposed. In this subsection, we discuss some of these metrics according to how they are used to evaluate performance in PLS.

Secrecy rate

The rate of transmission which can reliably be supported on the legitimate channel of transmission but not decodable on the channel of the eavesdropper is termed secrecy rate. The secrecy rate of the Gaussian channel is calculated as the maximum

difference between the attainable secrecy rates of Alice-Bob and Alice-Eve. Considering Figure 1.1, and using Equation 1.1 and Equation 1.9 the secrecy rate of a typical PLS communication system is given by;

$$R_s = R_B - R_E = \log_2\left(1 + \frac{P_T H_B}{\sigma_B^2}\right) - \log_2\left(1 + \frac{P_T H_E}{\sigma_E^2}\right), \tag{1.26}$$

where, R_B and R_E are the secrecy rates of Bob and Eve, respectively. The secrecy rate, R_s, can be maximized using signal design and optimization techniques, which will be discussed in chapter 2.

Secrecy Outage Probability (SOP)

SOP defines the probability at which a specific value of R_s for a particular system is not obtainable. This metric is used in instances where Alice has very little channel state information (CSI) of Bob and Eve. In most of the applications, the SOP is put to use under the conditions where the eavesdropper's statistical CSI is known to the transmitter. Additionally, the metric characterizes the reliability and the security of data transmission.

Quality of service (QoS)-related metrics

Signal-to-interference-plus-noise ratio (SINR): This metric may be described as quantitative relationship between the power of the received signal and power of the interference plus noise. The performance of a communication link is characterized by the QoS. SINR is directly related to the QoS and this can aid with the design of secrecy algorithms. A minimum value of SINR for transmission from Alice to Bob and a maximum value of SINR for Eve means a good receiving performance in terms of security and reliability. This paves way for a robust transmission capable of achieving the desired minimum and maximum error levels for Bob and Eve, respectively. Improvement of the SINR can be facilitated the use of PLS techniques such as beamforming.

Bit error rate (BER): This metric is defined as the ratio of the number of information bits received in error to the total number of bits transmitted. Different modulation and coding techniques have varying BER performance at the same SINR level. For the establishment of a communication link, the BER of a system must be above the minimum required level. Therefore, PLS techniques utilize optimization methods to improve the security of a communication system by degrading the BER of illegitimate users. Thus, the BER can be employed to measure the QoS and the security of a communication system.

Chapter 2

Technologies in PLS

In this section, the conventional and emerging PLS technologies are discussed. The chapter begin by discussing the conventional technologies which includes beamforming, zero-forcing, artificial noise, convex optimization, space-time coding and cooperative jamming. A typical PLS optimization problem of each scheme is presented as well as a comprehensive literature review. The second part discuss some of the emerging technologies in PLS which include wireless information and power transfer, intelligent reflecting surface, visible light communication, unmanned aerial vehicle and lastly the application of PLS in satellite communications.

2.1 Secure multi-antenna techniques

Multi-antenna techniques offer higher spatial degrees of freedom, which can be utilized effectively in PLS to ensure secure data transmission. Such techniques either attempt to degrade the eavesdropper's channel relative to the main transmission channel or enhance the quality of the received signal at the legitimate receiver. From the perspective of optimization, the four techniques which are representative of this area are; 1) beamforming, 2) zero-forcing (ZF), 3) convex optimization, and 4) artificial noise (AN). In Figure 2.1, from [8], each technique is described in terms of the transmission's orthogonality to Bob and Eve.

2.1.1 Convex optimization

Convex optimization can be used in PLS with other secure-multi antenna techniques to find the most favourable transmit solutions that can effectively make best out of the performance metrics of the wireless communication system. The objective function $f(x)$, to be maximized or minimized may be considered to be the performance metric, for example, secrecy rate, SINR and secrecy outage probability [19]. Several methods which are commonly used to solve optimization problems in PLS are widely available in the literature [41].

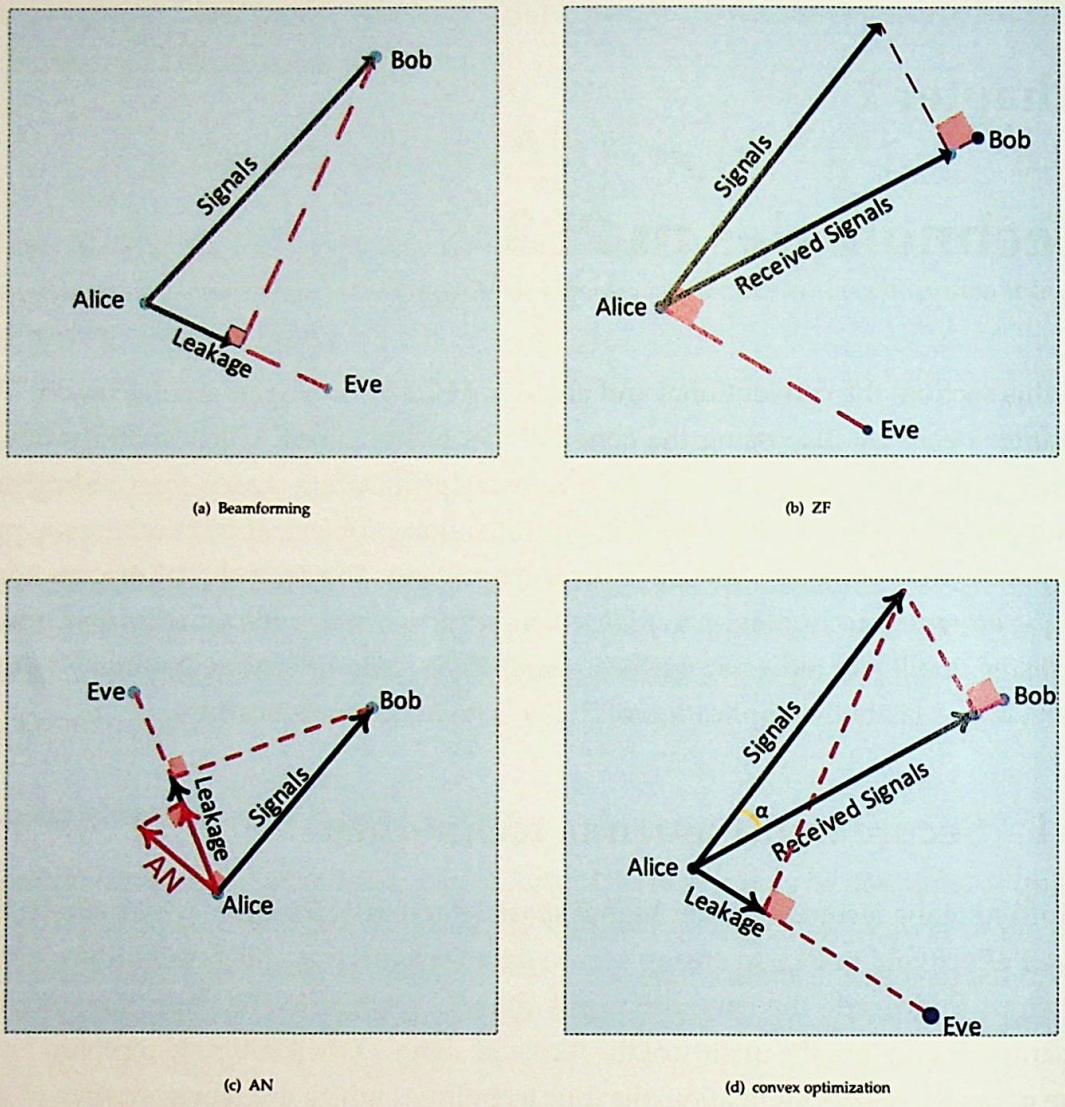


FIGURE 2.1: Secure multi-antenna techniques

Quadratic programming (QP)

QP is one of the convex optimization methods in which the objective function has quadratic terms and the constraint functions are affine. A quadratic is in standard form if written as [31];

$$\begin{aligned} \min_{x} \quad & c^T x + \frac{1}{2} x^T Q x \\ \text{s.t.} \quad & Ax = b \\ & x \geq 0, \end{aligned} \tag{2.1}$$

where $c \in \mathbb{R}^n$, $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$ and Q is a symmetric, PSD matrix. Quadratic programming is used in the design problems of nonlinear programming. Some of the common quadratic problems in PLS is that of power minimization, the secure power allocation and beamforming.

Semi-definite programming (SDP)

Another method used in PLS is the one of semi-definite programming (SDP). It is used to optimize a linear function of variables under linear equality constraints and a non-negativity constraint. An SDP problem is defined as follows [31];

$$\begin{aligned} \min_{x} \quad & c^T x \\ \text{s.t.} \quad & \sum_{j=1}^{n} F_j x_j \preceq F_0 \\ & Ax = b, \end{aligned} \tag{2.2}$$

where $F_j \in \mathcal{S}^d$ and $j = 0, 1, \ldots, n$. Most of the problems in PLS are usually non-convex and they must be converted into convex problems using SDP. In turn, an efficient algorithm that is easy to implement is developed in order to obtain optimal performance metrics.

Fractional programming

Fractional programming is one more method which is applied in optimization of a ratio of two nonlinear functions. The general fractional programming can be formulated as the following problem [31];

$$\begin{aligned} \min_{x} \quad & \frac{A(x)}{B(x)} \\ \text{s.t.} \quad & x \in \mathcal{X}, \end{aligned} \tag{2.3}$$

where $A(x)$ and $B(x)$ are continuous real-valued functions of $x \in \mathcal{X}$. The fractional programming problem is in general not convex. A typical example of its application in PLS is the energy efficiency maximization.

Even though convex optimization offers improved secrecy performance in the physical layer than the conventional precoding techniques such as beamforming or zero-forcing, it is more computationally expensive to implement.

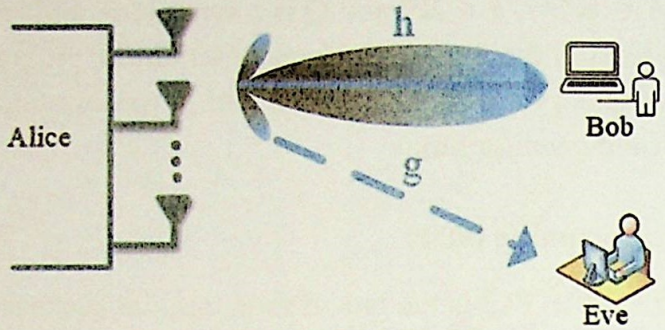


FIGURE 2.2: Beamforming

2.1.2 Beamforming

Beamforming is a signal processing technique that is used to transmit signals effectively in intended directions to give a maximum signals difference between the receiver in the intended direction and the one in the unintended direction. Beamforming forms a beam in the direction of the desired recipient to maximize the signal to noise power ratio while suppressing the reception or transmission in the direction of the unintended user, Figure 2.2. This significantly improves the energy efficiency of the system because the energy is transmitted or focused in a particular direction rather than being spread out in a diffused fashion.

Different beam forms

There are different configurations of beamforming that can be performed so that data can be sent to or received by the users in the communication network in order to achieve spatial diversity. The configurations are categorised according to the number of antennas used at the transmitter or receiver and they include but not limited to, multiple-input single output (MISO), single input multiple-output (SIMO) and MIMO [42].

- Transmit beamforming (MISO): It used to match the channel from multiple transmit antennas to the receiver [43]. This matching steers the transmitted signal towards the intended receiver by finding the best possible channel among all the transmit antennas. Figure 2.3 demonstrate transmit beamforming using two transmit antennas and a single receive antenna.

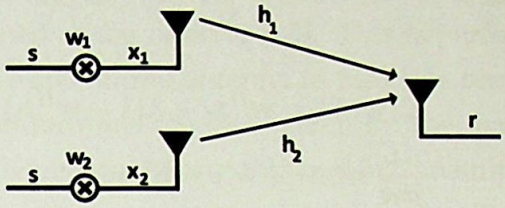


FIGURE 2.3: Transmit Beamformer

Then system model equation is given by:

$$\begin{aligned} r &= \mathbf{h}\mathbf{x} + n, \\ r &= \Big(\sum_{i=1}^{M_t} \mathbf{h}_i \mathbf{w}_i\Big)\mathbf{x} + n, \\ r &= h_1 x_1 + h_2 x_2 + n, \\ r &= h_1 w_1 s + h_2 w_2 s + n, \end{aligned} \tag{2.4}$$

where $M_t = 2$ is the number of transmit antennas. The beamforming problem is to choose the optimal beamforming vectors, w_1 and w_2 which maximizes the SNR. The SNR maximization can be performed by maintaining the signal gain constant, that is ensuring unity signal gain for the desired user and minimizing noise power. Assuming an AWGN noise model where we make an assumption that all the noises are independent and statistically identical, i.e they have zero mean, $\mathbb{E}\{\mathbf{n}_i \mathbf{n}_j\} = 0$ and noise power equals to $\mathbb{E}\{\mathbf{n}_i^2\} = \sigma^2$. Therefore the noise power reduces to;

$$\text{Noise power} = \sigma^2 \|\mathbf{w}\|^2.$$

Now the optimization problem for beamforming is to;

$$\begin{aligned} \min \quad & \sigma^2 \|\mathbf{w}\|^2 = \|\mathbf{w}\|^2 = \mathbf{w}^H \mathbf{w} \\ \text{s.t.} \quad & \mathbf{w}^H \mathbf{h} = 1. \end{aligned} \tag{2.5}$$

To solve this equation we use the concept of Lagrange multiplier from subsection 1.1.3 ;

$$\begin{aligned} \mathcal{L}(\mathbf{w},\lambda) &= \mathbf{w}^H\mathbf{w} + \lambda(1 - \mathbf{w}^H\mathbf{h}) \\ \frac{d\mathcal{L}}{d\mathbf{w}} &= 2\mathbf{w} + \lambda(0 - \mathbf{h}) = 0 \\ &\implies 2\mathbf{w} = \lambda\mathbf{h} \\ &\implies \mathbf{w} = \frac{\lambda}{2}\mathbf{h}. \end{aligned} \tag{2.6}$$

In order to determine λ we use the constraint;

$$\begin{aligned} \mathbf{w}^H\mathbf{h} &= 1 \\ &\implies \left(\frac{\lambda}{2}\mathbf{h}\right)^H \mathbf{h} = 1 \\ &\implies \lambda = \frac{2}{\|\mathbf{h}\|}. \end{aligned} \tag{2.7}$$

Therefore, the optimal transmit beamformer is given by;

$$\begin{aligned} \mathbf{w}^\star &= \frac{1}{2}\frac{2}{\|\mathbf{h}\|}\mathbf{h} \\ \mathbf{w}^\star &= \frac{\mathbf{h}}{\|\mathbf{h}\|}. \end{aligned} \tag{2.8}$$

This process of beamforming in the same direction as the channel is known as maximum ratio transmission (MRT) [44]. The signal from the transmitting antenna is multiplied with this optimal beamforming vector obtained from the derivation above such that the magnitude and phase of the signal is adjusted to form a beam in the desired direction and minimizes the output in other directions. The SNR at the output is given by;

$$\begin{aligned} \text{SNR} &= \frac{\mathbb{E}\{\mathbf{x}^2\}}{\sigma^2\|\mathbf{w}\|^2}\,; \quad \mathbf{w} = \frac{\mathbf{h}}{\|\mathbf{h}\|} \\ &= \frac{P}{\sigma^2\frac{\|\mathbf{h}\|^2}{\|\mathbf{h}\|^4}} \\ &= \frac{P\|\mathbf{h}\|^2}{\sigma^2}. \end{aligned} \tag{2.9}$$

where P is the symbol power.

- Receive beamforming (SIMO): In receive beamforming, the beamforming processing is performed at the receiver [43]. This is performed by matching the channel from the transmitting antenna to multiple receive antennas. The optimal receive beamforming vector is given by the maximal ratio combining (MRC) and is equivalent to the one obtained in transmit beamforming by MRT.

- Maximum eigenmode beamforming (MIMO): Both the transmitter and receiver form beams that are jointly matched to each other. The formed channel is equal to the maximum singular value of the channel and is given by the SVD of the channel matrix [42].

  The $M_t \times 1$ transmitted signal is given by $\mathbf{x} = \left(\sum_{i=1}^{M_t} \mathbf{w}_{tx,i}\right)\mathbf{x}_i$ and the $M_r \times 1$ transmitted signal is given by $y_i = \mathbf{H}\mathbf{w}_{tx,i}\mathbf{x}_i + \mathbf{n}$. After receive beamforming the resultant signal is given by

$$\mathbf{y} = \mathbf{w}_{rx}^T \mathbf{H} \mathbf{w}_{tx} \mathbf{x} + \mathbf{w}_{rx}^T \mathbf{n}$$

- Eigenmode beamforming (MIMO): This is applicable in MIMO system whereby both transmitter and receiver form multiple beams matched to the underlying structure of the channel. Each transmit beam is matched to a receive beam and the corresponding channel matrix is given by the SVD [42].

A beamforming problem in PLS involves steering the transmitted signal towards the desired user while taking into account an interfering user trying to decode the transmitted information, Figure 2.2. To demonstrate the beamforming optimization problem in PLS we consider a MISO system shown in Figure 2.4 in which the transmitter uses transmit beamforming to communicate with K users. We assume that

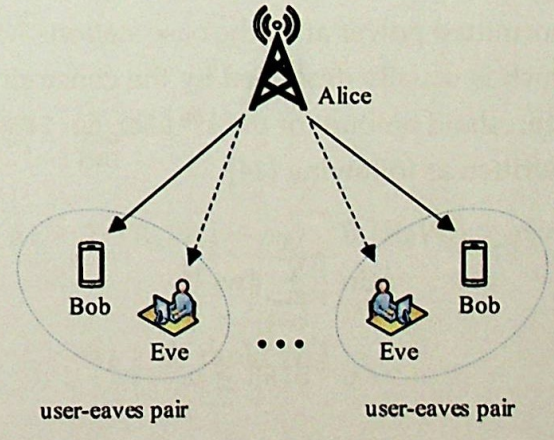


FIGURE 2.4: System model of multi-user and eavesdroppers pair with beamforming

the transmitter is equipped with N_t transmit antennas and the legitimate user and the eavesdropper each have a single receive antenna. Therefore the received signal at legitimate user k and their equivalent SINR are respectively given by:

$$\begin{aligned} y_k &= \mathbf{h}_k^H \mathbf{x}_k + \sum_{\substack{k=1 \\ k \neq i}}^{K} \mathbf{h}_k^H \mathbf{x}_i + n_k, \\ \text{SINR}_B &= \frac{|\mathbf{h}_k^H \mathbf{w}_k|^2}{|\sum_{\substack{k=1 \\ k \neq i}}^{K} \mathbf{h}_k^H \mathbf{w}_i|^2 + \sigma^2}. \end{aligned} \tag{2.10}$$

Similarly the signal received signal by the k^{th} eavesdropper and their equivalent SINR can be shown to be respectively given by:

$$\begin{aligned} z_k &= \mathbf{g}_k^H \mathbf{x}_k + \sum_{\substack{k=1 \\ k \neq i}}^{K} \mathbf{g}_k^H \mathbf{x}_i + m_k, \\ \text{SINR}_E &= \frac{|\mathbf{g}_k^H \mathbf{w}_k|^2}{|\sum_{\substack{k=1 \\ k \neq i}}^{K} \mathbf{g}_k^H \mathbf{w}_i|^2 + \sigma^2} \end{aligned} \tag{2.11}$$

where $\mathbf{x}_k \in \mathbb{C}^{N_T \times 1}$ is the transmitted signal symbol of the desired user k with corresponding beamforming vector $\mathbf{w}_k \in \mathbb{C}^{N_T \times 1}$, $\mathbf{h} \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{g} \in \mathbb{C}^{N_T \times 1}$ are the channel vectors of the desired user and eavesdropper respectively, and n_k, m_k are the corresponding AWG noise vectors for k^{th} user and eavesdropper with zero mean and noise power σ^2. The covariance matrix of the transmitted signal is given by $\mathbf{R}_k = \mathbb{E}\{\mathbf{x}_k \mathbf{x}_k^H\}$. The objective problem of a typical beamforming design scheme is to minimize the total transmitted power at all the base stations while ensuring desired QoS for each user, which is usually described by the constraint of the SINR greater or equal to the given threshold amount of the k^{th} user, i.e. $\text{SINR} \geq \rho_k$. Therefore the beamforming can be written as following [44]:

$$\begin{aligned} \min_{\mathbf{w}_k} \quad & \sum_{k=1}^{K} \|\mathbf{w}_k\|^2 \\ \text{s.t.} \quad & \text{SINR} \geq \rho_k. \end{aligned} \tag{2.12}$$

The solution to the beamforming problem in equation (2.12) provide an optimal vector $\mathbf{w}_i$ which maximizes the SNR of the desired user. This results in focusing the beam

in one direction, and the process is referred to as electronic steering. One beamforming vector is assigned to each legitimate user and is matched to their channel. In order to solve the problem in equation (2.12) we have to reformulate it as a convex problem. The cost function $\sum_{k=1}^{K}||\mathbf{w}_k||^2$ is a convex function of the beamforming vectors. However, the SINR constraint is non-convex which makes the problem in equation (2.12) non-convex. Therefore the SINR has to be reformulated as follows [44];

$$\frac{\mathbf{w}_k^H\mathbf{R}_k\mathbf{w}_k}{\sum\limits_{\substack{k=1\\k\neq i}}^{K}\mathbf{w}_i^H\mathbf{R}_k\mathbf{w}_i+\sigma^2}\geq\rho_k\Leftrightarrow\mathbf{w}_k^H\mathbf{R}_k\mathbf{w}_k-\rho_k\sum_{\substack{k=1\\k\neq i}}^{K}\mathbf{w}_i^H\mathbf{R}_k\mathbf{w}_i\geq\rho_k\sigma^2. \tag{2.13}$$

As a result the problem given by equation (2.12) can be expressed in its equivalent convex form as follows;

$$\begin{aligned}\min_{\mathbf{w}_k}\quad&\sum_{k=1}^{K}\|\mathbf{w}_k\|^2\\ \text{s.t.}\quad&\mathbf{w}_k^H\mathbf{R}_k\mathbf{w}_k-\rho_k\sum_{\substack{k=1\\k\neq i}}^{K}\mathbf{w}_i^H\mathbf{R}_k\mathbf{w}_i\geq\rho_k\sigma^2.\end{aligned} \tag{2.14}$$

The problem in equation (2.14) is classified as NP-hard problem because it is very difficult and challenging to solve in reasonable time in this form. One approach to solving this problem is by the use of semi-definite relaxation. This is done by defining the matrix $\mathbf{W}_k=\mathbf{w}_k^H\mathbf{w}_k$ such that $\mathbf{w}_i^H\mathbf{R}_k\mathbf{w}_i=\text{Tr}\left(\mathbf{R}_k\mathbf{W}_i\right)$. Then the problem in equation (2.14) can be transformed to given the problem given in equation (2.15). The problem in equation (2.15) can be easily solved using CVX solvers by relaxing the rank-one constraints.

$$\begin{aligned}\min_{\mathbf{w}_k}\quad&\sum_{k=1}^{K}\text{Tr}\left(\mathbf{W}_k\right)\\ \text{s.t.}\quad&\text{Tr}\left(\mathbf{R}_k\mathbf{W}_k\right)-\rho_i\sum_{\substack{k=1\\k\neq i}}^{K}\text{Tr}\left(\mathbf{R}_k\mathbf{W}_i\right)\geq\rho_i\sigma^2\\ &\mathbf{W}_k\succeq 0,\ \text{rank}(\mathbf{W}_k)=1\end{aligned} \tag{2.15}$$

2.1.3 Artificial Noise (AN) precoding

The notion of using artificial noise to enhance security in the physical layer was first proposed in [45]. They identified AN based transmission as an effective technique that can be deployed in PLS to ensure secure communication in wireless networks. The technique involves deliberately degrading the quality of the channel of the eavesdropper by generating an interference signal which is used to interrupt their eavesdropping capabilities. Basically, in the AN precoding scheme, the transmitter, Alice divides the transmission power between transmitting the information to the intended recipient, Bob, and transmitting the noise signal towards the eavesdropper, Eve is shown in Figure 2.5.

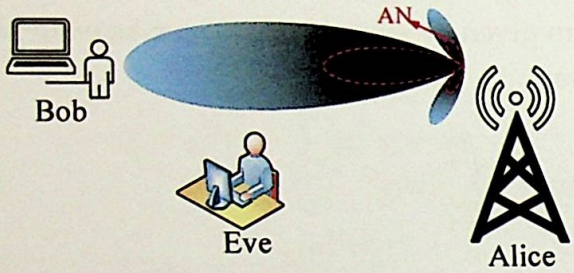


FIGURE 2.5: Secrecy beamforming with AN

Generating AN depends on the transmitter's knowledge of the eavesdroppers' channel state information. In a case where the eavesdropper's CSI is unknown, the isotropic AN is generated. The generated AN is designed such that it lies in the nullspace of the intended receiver and directed in the range space of the unintended receivers. This is done to cancel out its effect at the intended receiver such that only the eavesdropper's channel is degraded [45]. Another form of AN generation is called the spatially selective AN, which is applicable in the event that the transmitter knows the the eavesdropper's CSI [46]. The AN generation technique's major strength is that the secrecy provided scales well with the SNR since an increase in SNR at Eve will increase the received AN power along with the message power. The conventional AN scheme can be represented in general as follows;

$$\mathbf{x} = \mathbf{w}s_a + \mathbf{v}s_j, \tag{2.16}$$

where $\mathbf{x}$ is the signal transmitted by Alice. The source information is denoted by s_a and s_j denotes the AN jamming signal which is chosen to be independent of the source information, i.e $s_a \neq s_j$. Beamforming vectors for the information and jamming signals are represented by $\mathbf{w}$ and $\mathbf{v}$, respectively. Therefore the signals

received by Bob and Eve are given by Equation 2.17 and Equation 2.18, respectively.

$$\mathbf{y}_B = \mathbf{h}_B^H \mathbf{w} s_a + \mathbf{g}_B^H \mathbf{v} s_j + n_B, \tag{2.17}$$

$$\mathbf{y}_E = \mathbf{h}_E^H \mathbf{w} s_a + \mathbf{g}_E^H \mathbf{v} s_j + n_E \tag{2.18}$$

Where $\mathbf{h}_B^H$, $\mathbf{g}_E^H$ denotes the channel responses of Alice-Bob and Alice-Eve, respectively. The independent identically distributed complex Gaussian noise for Bob and Eve with zero mean and variance σ^2 are denoted by n_B and n_E, respectively. The corresponding secrecy rate is given by:

$$R = \log_2\left(1 + \frac{|\mathbf{h}_B^H \mathbf{w}|^2}{|\mathbf{g}_B^H \mathbf{v}|^2 + \sigma^2}\right) - \log_2\left(1 + \frac{|\mathbf{h}_E^H \mathbf{v}|^2}{|\mathbf{g}_E^H \mathbf{v}|^2 + \sigma^2}\right) \tag{2.19}$$

A novel approach of AN scheme which offers better secrecy rate performance where the jamming signal is generated to be dependent on the information signal was presented in [47]. The scheme significantly improves the signal strength at Bob and at the same time canceling the received signal at the eavesdropper. In the scheme the signal received by Bob and Eve can be shown to be given by:

$$\mathbf{y}_B = \mathbf{h}_B^H \mathbf{w} s_a + \mathbf{g}_B^H \mathbf{v} s_a + n_B, \tag{2.20}$$

$$\mathbf{y}_E = \mathbf{h}_E^H \mathbf{w} s_a + \mathbf{g}_E^H \mathbf{v} s_a + n_E. \tag{2.21}$$

Therefore the secrecy rate is now given by:

$$R = \log_2\left(1 + \frac{|\mathbf{h}_B^H \mathbf{w} + \mathbf{g}_B^H \mathbf{v}|^2}{\sigma^2}\right) - \log_2\left(1 + \frac{|\mathbf{h}_E^H \mathbf{v} + \mathbf{g}_E^H \mathbf{v}|^2}{\sigma^2}\right). \tag{2.22}$$

The optimization problem of AN precoding scheme is to find an optimal power allocation method for the artificial noise, which ensures maximum secrecy of the legitimate transmission. The classical AN injection schemes are investigated broadly in the literature, and their application in MIMO systems has been shown as promising to exploit in future wireless networks. In [48], the authors demonstrated an approach capable of guaranteeing secrecy without knowledge of the eavesdropper's CSI. The authors of the same paper proposed two schemes which employs AN generation to implement PLS. In the first scheme, they proposed a scheme which was based on MIMO technology while the second scheme used a single transmit antenna. For the latter scheme amplifying relays were used to mimic the effects of multiple antennas. Moreover, in the second scheme the transmitter and the intended

receiver both transmit independent AN signals to the helper nodes. The eavesdropper receives differently weighted versions of the AN signals from the transmitter and the receiver. The two transmission schemes proposed in the paper transmit both AN and information-bearing signals together. However, the paper does not necessarily find an optimal power allocation for the transmission of message signals and minimal power allocated to the AN.

To tackle the shortfall indicated in [48], researchers of [49] proposed an AN-assisted secure MIMO-OFDM system to improve the security of the legitimate transmission and find an optimal power allocation scheme. AN precoding scheme is proposed where Alice divides her power between transmitting a message to Bob and transmitting AN into Bob's nullspace. Assuming Bob and Eve's channels are independently faded, Eve will see some of the AN in her range space. The authors determined the minimum power consumption which satisfies the legitimate transmission quality with the largest residual power in generating AN. They use convex optimization solvers to find the optimal solution to this problem. This technique's major strength is that the secrecy provided scales well with SNR since an increase in SNR at Eve will increase the received AN power along with the message power [50].

AN precoding was also used in [40] to implement security in the physical layer. AN was used as a transmit strategy over Bob's null space with the intention of improving the secrecy of the Alice-Bob channel without affecting its quality. The authors examines three approaches of generating AN. Firstly, the minimum power was used for the information-bearing signal and the rest of the transmit power was distributed to the AN. Secondly, the power was evenly distributed between the transmit signal and the AN signal in order to maximize ergodic secrecy capacity. Lastly, the AN power was progressively varied in order to understand its effects on the secrecy confidence level. Eve was modeled to use the minimum mean square error (MMSE) as an optimal receiver structure to maximize the SNR. Eve's capability to compromise the secrecy of the main link was defined as the SNR difference between the intended receiver and the eavesdropper. It was shown in [40] that when an eavesdropper is using zero-forcing to mitigate the interference introduced by the artificial noise transmission with a large number of receiving antennas and knows some of the main channel's CSI, the secrecy of the system can be compromised.

2.1.4 Zero-Forcing

Zero-forcing (or null-steering) precoding is a method of spatial signal processing by which multiple antennas at the transmitter can cancel out (null) multiple user

interference signals in wireless communications. The basic idea of the ZF method is based on canceling out the interference at the intended receiver in multiple user communications. This can be done by using eavesdropper's CSI to transmit a message orthogonal to the eavesdropper, which is equivalent to steering a null in the direction of the eavesdropper, illustrated in Figure 2.6.

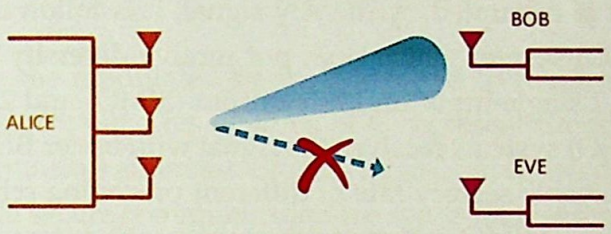


FIGURE 2.6: Zero forcing

To present the optimization problem for ZF precoding we consider the system model given by:

$$\mathbf{y} = \mathbf{h}x + \mathbf{g}x_i + \mathbf{n}, \tag{2.23}$$

where $\mathbf{h}$ is the channel of the desired user and $\mathbf{g}$ is the channel of the interfering user. Performing beamforming we now have the output given by:

$$\begin{aligned} \mathbf{y} &= \mathbf{w}^H(\mathbf{h}x + \mathbf{g}x_i + \mathbf{n}) \\ &= \mathbf{w}^H\mathbf{h}x + \mathbf{w}^H\mathbf{g}x_i + \mathbf{w}^H\mathbf{n}, \end{aligned} \tag{2.24}$$

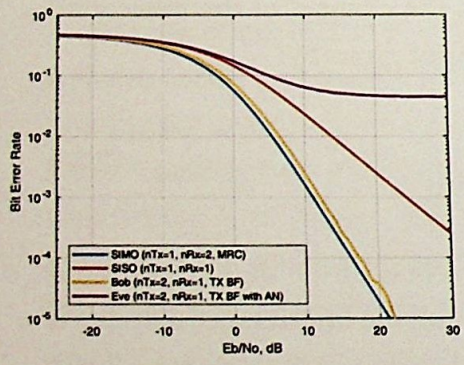
where $\mathbf{w}^H\mathbf{h}$ is the signal gain or the gain in the direction of the desired user and $\mathbf{w}^H\mathbf{g}$ is the gain of the interfering user. ZF intends to null the interference and this is done by forcing the interference term to zero. Therefore the optimization problem for the ZF beamformer is given by:

$$\begin{aligned} \min \quad & \sigma^2\|\mathbf{w}\|^2 = \|\mathbf{w}\|^2 = \mathbf{w}^H\mathbf{w} \\ \text{s.t.} \quad & \mathbf{w}^T\mathbf{h} = 1 \\ & \mathbf{w}^T\mathbf{g} = 0. \end{aligned} \tag{2.25}$$

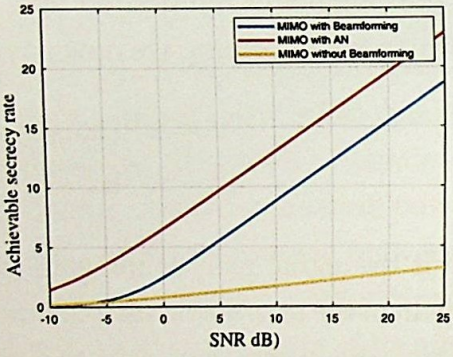
The design problem of ZF precoding has been presented in [51]. The iterative algorithm presented in [51] was developed to obtain the optimal transmit and receive filters to cancel out the interference. The designed filters minimizes the mean-square error (MSE) between the legitimate parties whilst guaranteeing and maintaining a certain eavesdropper MSE level, subject to the power constraint. Nonetheless, the ZF precoding methods presented have been demonstrated to perform well or

achieves the highest secrecy system capacity when full knowledge of CSI is available at the transmitter, which is a highly unlikely case. Therefore, with limited CSI at the transmitter, the performance of ZF-precoding is very poor, which makes it less applicable.

In 2.7a we demonstrate the BER performance of the beamforming and AN schemes.The figure illustrates that the eavesdropper's channel has the worst bit error rate because it is corrupted by the AN signal, it is followed by a single-input single-output (SISO) system which does not receive diversity from beamforming and lastly the 1×2 single-input multiple-output (SIMO) and 2×1 multiple-input single-output (MISO) systems receives the signal with better BER because of beamforming. The achievable secrecy rate of different precoding schemes are shown in 2.7b. In particular, a MIMO scheme with six transmit antennas, the intended receiver and eavesdropper each equipped with two receive antennas. In the figure we have the same MIMO configuration for no beamforming used and with beamforming introduced and lastly we introduce an AN signal. The figure confirms that the use of AN indeed improves the secrecy rate of the communication network compared to beamforming only or no beamforming used.



(a) BER vs SNR



(b) Comparison of the achievable secrecy rate for beamforming precoding with and without AN

FIGURE 2.7: BER and secrecy rate performance metrics simulations for different precoding schemes.

2.1.5 Space-time coding (STC)

Alamouti proposed a space-time block code (STBC) to achieve transmitter diversity in 1998 [52]. In the conventional transmit schemes, diversity techniques were applied at the receiver using algorithms such as the MRC. These techniques require the knowledge of the channel between the transmitter and the receiver to derive the optimal beamforming weights. However, Alamouti showed that it is possible to transmit data using multiple antennas and perform separation at the receiver using

a single receive antenna, which gives the same diversity gains. To provide diversity using the Alamouti scheme, the time and space blocks are used to encode the information signal. The Alamouti space-time encoder takes a block of two modulated symbols to create an encoding matrix denoted by;

$$\mathbf{C} = \begin{bmatrix} \mathbf{s}_1 & -\mathbf{s}_2^* \\ \mathbf{s}_2 & -\mathbf{s}_1^* \end{bmatrix}, \tag{2.26}$$

where s_1 and s_2 are the modulated symbols mapped to two transmit antennas in two transmit time slots [53]. The columns of C represent timeslots, and the rows represent different transmit antennas. Studies by [54, 55] showed that STBC may be employed to provide secure communication for space-time systems while lowering the eavesdropper's order of diversity. A technique depicted in Figure 2.8 to achieve a secure STBC without the need to estimate CSI at the transmitter was proposed in [54]. The proposed technique uses mutual received signal strength indicator measurement to generate a pseudo-random sequence used to secure communication. In this model, at each transmit antenna random phase rotations θ_1 and θ_2 are applied to the symbols. Each phase shift is applied for one code duration. For a single codeword, the transmitter encodes source information, s_1 and s_2 as:

$$\mathbf{X} = \begin{bmatrix} \mathbf{s}_1 e^{j\theta_1} & \mathbf{s}_2^* e^{j\theta_2} \\ -\mathbf{s}_2 e^{j\theta_1} & \mathbf{s}_1^* e^{j\theta_2} \end{bmatrix}. \tag{2.27}$$

Therefore Bob's receives the signal given by:

$$\begin{aligned} \mathbf{z} &= \mathbf{X}\mathbf{h} + \mathbf{n} \\ \mathbf{z} &= \mathbf{H}^{+}(\theta_1, \theta_2)\mathbf{s} + \tilde{\mathbf{n}} \\ \begin{bmatrix} \mathbf{z}_1 \\ -\mathbf{z}_2^* \end{bmatrix} &= \begin{bmatrix} \mathbf{h}_1 e^{j\theta_1} & \mathbf{h}_2^* e^{j\theta_2} \\ -\mathbf{h}_2 e^{j\theta_1} & \mathbf{h}_1^* e^{j\theta_2} \end{bmatrix} \begin{bmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{bmatrix} + \begin{bmatrix} \mathbf{n}_1 \\ -\mathbf{n}_2^* \end{bmatrix}. \end{aligned} \tag{2.28}$$

Using the MRC algorithm, the source information can be estimated to be given by:

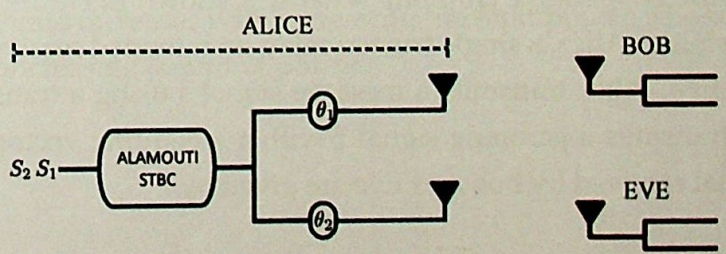


FIGURE 2.8: System block diagram

$$\tilde{\mathbf{s}} = \mathbf{H}^{+}(\theta_1, \theta_2)\mathbf{z}. \tag{2.29}$$

Eve's received signal is given by $\mathbf{y}$, which can be also be decomposed to $\tilde{\mathbf{y}}$ as:

$$\begin{aligned} \mathbf{y} &= \mathbf{X}\mathbf{g} + \mathbf{e}, \\ \tilde{\mathbf{y}} &= \mathbf{G}^{+}(\theta_1, \theta_2)s + \tilde{\mathbf{e}}, \end{aligned} \tag{2.30}$$

where $\mathbf{H}^{+}$ and $\mathbf{G}^{+}$ are the pseudoinverse of $\mathbf{H}$ and $\mathbf{G}$, respectively. The transmitter manipulates the transmitted symbols by generating and applying the maximum number of phase rotations so that the eavesdropper is completely denied access to the source information. The strength of this technique is that improved security is achieved without the knowledge of the CSI, unlike in the preceding security schemes which assumes that the CSI is available. However, it was shown in [55] that the security of the transmitted signal is compromised if the eavesdropper can obtain one of the space angles and is in close proximity to Bob. To avoid this compromisation, the authors proposed a technique which is able to achieve zero diversity for the eavesdropper even under enhanced receive diversity. This can be achieved through signal and space rotations.

2.1.6 Cooperative jamming

Cooperative jamming is also one of the techniques proposed to implement security in the physical layer to curb eavesdropping in wireless networks. A cooperative jamming network is comprised of the source which transmits its message to the intended receiver and a relay node which transmits a jamming signal to degrade the eavesdropper's channel and improve the secrecy rate [56, 57]. Cooperative jamming was derived from the conventional technique for user cooperation known as cooperative relaying. However cooperative relaying is distinctive from cooperative jamming by that it improves the security by enhancing channel quality between the transmitter and legitimate receiver. Some of the examples of cooperative relaying are decode-and-forward (DF) and amplify-and-forward schemes (AF). A system model of a typical cooperative jamming scheme is shown in Figure 2.9 which consist of the transmitter Alice, a single trusted relay, an intended receiver Bob and and eavesdropper, Eve. Alice transmits a message signal s using a transmit power PA and the relay transmits a jamming signal z with a weighting vector $\mathbf{w}$, simultaneously. The signal received by Bob and Eve are given by:

$$y_B = \sqrt{P_A}\mathbf{h}_{AB}s + \mathbf{w}^{H}\mathbf{h}_{RB}z + n_B, \tag{2.31}$$

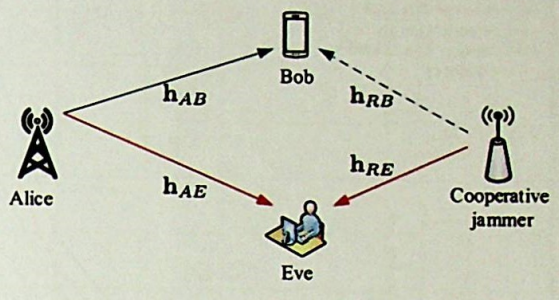


FIGURE 2.9: Secrecy with cooperative jamming

$$y_E = \sqrt{P_A}\mathbf{h}_{AE}s + \mathbf{w}^H\mathbf{h}_{RE}z + n_E, \tag{2.32}$$

respectively, where $\mathbf{h}_{AB}$ is the Alice-Bob channel, $\mathbf{h}_{RB}$ is the relay-Bob channel, $\mathbf{h}_{RE}$ is the relay-Eve channel, $\mathbf{h}_{AE}$ is the Alice-Eve channel and $\mathbf{n}_B$ and $\mathbf{n}_E$ are the AWG noise with variance σ^2 at both Bob and Eve respectively. The corresponding secrecy rate is given by:

$$R = \log_2\left(1 + \frac{P_A|\mathbf{h}_{AB}|^2}{\sigma^2}\right) - \log_2\left(1 + \frac{P_A|\mathbf{h}_{AE}|^2}{|\mathbf{w}^H\mathbf{h}_{RE}|^2 + \sigma^2}\right). \tag{2.33}$$

In equation (2.33), the effect of interference is neglected at the legitimate user because of the existing cooperation between the jammer node and the legitimate user [58]. The interference is only present at the eavesdropper do degrade their SNR hence improving the secrecy rate of the network. We demonstrate the secrecy rate performance of a cooperative jamming in Figure 2.10. The model considered is made of the legitimate receiver, Bob, a cooperative jammer and an eavesdropper all located at distance of 50m away from the transmitter, Alice. The transmitter and cooperative jammer lie in the same horizontal line. Bob and Eve also lie in the same horizontal line. The perpendicular distance between the two lines is equal to 2m. To evaluate the performance we vary the transmit power of Alice and plot against the secrecy rate. The result simulation plot is shown in Figure 2.10 and it shows that the secrecy rate increases with increasing transmit power. The secrecy rate also increases with increasing jamming power.

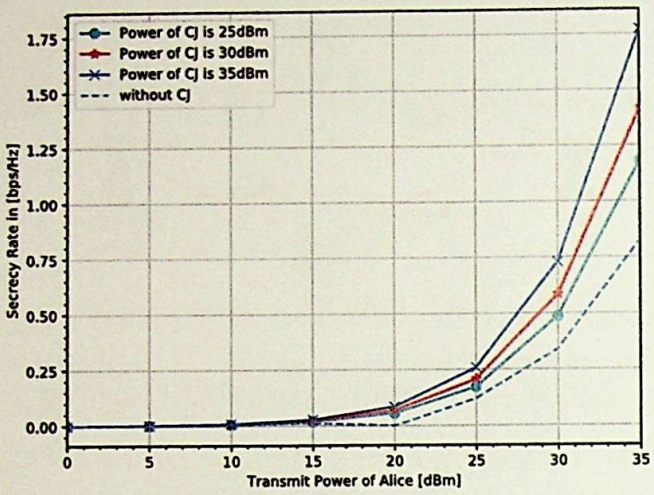


FIGURE 2.10: Secrecy rate against transmit power of Alice

2.2 Emerging technologies

In recent years, wireless communication networks have been proliferating to cope with the need for high demands in data transmission and reception. In addition, the advancement in technology has provided hackers with improved eavesdropping capabilities. All of this factors poses a major threat in the conventional PLS technologies. Hence, many different researchers have conducted studies to propose new technologies which can tackle this problems. We present some of this technologies in this section.

2.2.1 Wireless information and power transfer (WIPT)

WIPT has been identified as a sustainable proposition for harvesting of energy from the radio frequency (RF) signals which in-turn is supplied to finite-powered wireless communication devices including wireless sensors and electronic gadgets [59, 60]. The concept of WIPT, which is depicted in Figure 2.11, was shown to be beneficial in PLS precoding schemes, specifically the ones which uses AN technique. It was shown in Section 2.1.3 that the injection of AN into the communication network is an intriguing technique for improving the overall system secrecy performance. Therefore, using the concept of WIPT, the additional AN introduced in the system can be harvested at the receiver. This can offer a viable solution for the facilitation of sustainable and efficient wireless networks, especially when the receivers do not have enough energy to achieve their functionality.

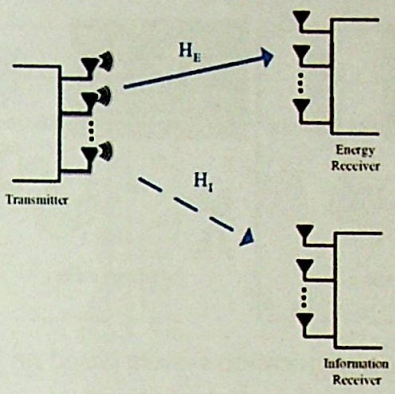


FIGURE 2.11: WIPT system

2.2.2 Intelligent reflecting surface (IRS)

Future wireless networks are expected to employ intelligent and software re-configurable functionalities to enable safe and secure communication [61]. Intelligent reflective surfaces have been identified as a solution to create a controllable wireless environment. According to [62], an IRS is a software-controlled artificial surface that can be programmed to alter its electromagnetic response. An IRS can change the attenuation and scattering of the incident electromagnetic wave so that it can propagate in the desired way towards the intended receiver by adjusting the reflecting coefficients. In [63], the two methods of deploying IRS, namely, (a) energy focusing and (b) energy nulling, which are graphically shown in Figure 2.12 are discussed. Energy focusing employs beamforming technique approach by using the IRS reflecting elements to adjust the phases of the signal coming from the transmitter so that it is focused towards one intended user. Meanwhile, energy nulling, uses the IRS to perform destructive reflection, by adjusting the phases of the scattered signals to null out the signal at the unintended recipients [63]. One application of IRS is in holographic beamforming, as described in [64]. Holographic beamforming is a dynamic beamforming technique that uses a software-defined antenna.

2.2.3 Visible light communication (VLC)

VLC is one of the technologies that has emerged with the potential of providing omnipresent access to wireless broadband for indoor settings [65, 66]. This is enabled by some of its unique characteristics which include line-of-sight propagation, inability of light waves to penetrate opaque surface, technological advancements and economical costs of lighting equipment such as solid-state light-emitting diodes

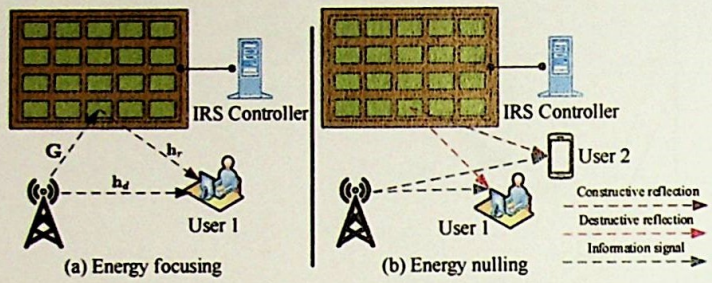


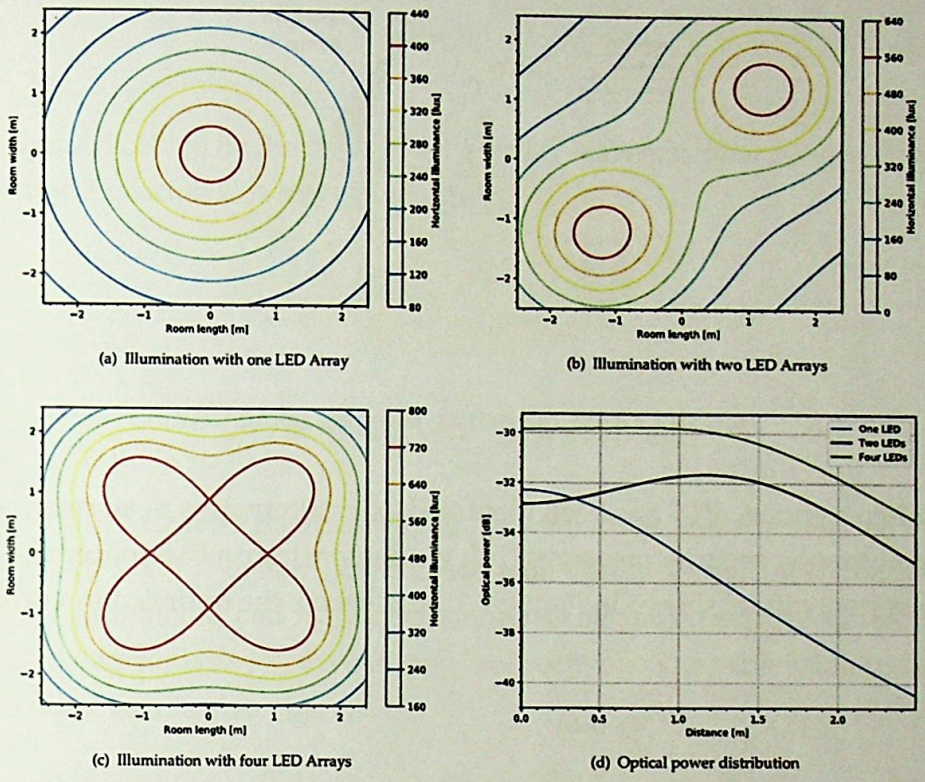
FIGURE 2.12: Wireless communication system based on IRS. Adapted from [63].

(LEDs). The aforementioned characteristics are highly useful in PLS since VLC signals are confined inside the building's walls, hence an inherently secure communication which prevents eavesdropping for outdoor eavesdroppers. VLC schemes are realized through the use of a number of LED arrays and photodetectors (PDs). The LED arrays serves a dual purpose of offering illumination and data transmission simultaneously while the PDs are used as receivers. The most common method of modulation in VLC is the intensity modulation and direct detection (IM/DD). Unlike in RF systems, the modulating signals in VLC systems must be real valued and non-negative [67]. To show the concept of VLC, Figure 2.13 depicts the illumination and power distribution using various arrays made up of red-green-blue (RGB) LEDs.

Horizontal illuminance of a light fixture made up of an LED array of 50×50 RGB LED chips with a semi-angle of 60° is depicted in Figure 2.13a. Each LED chip have a Lambertian radiation pattern and total luminous intensity of 33.74 cd. As seen in Figure 2.13b, increasing the number of LED arrays leads to an increased intensity and illuminance at all points of the room. Consequently, this results in elevated optical power as seen in Figure 2.13d. Optical power is crucial for data transmission because direct detection depends on the amount of power which impinges the PD. Due to incoherent distributed light intensity, the amount of optical power produced by the LED arrays decreases logarithmically with increasing distance.

2.2.4 Unmanned aerial vehicle (UAV)

Drones or UAV-based communication technology was thoroughly studied and adopted by the 3GPP standard [68]. A study on UAV systems that highlighted and gave an overview of the latest advances and state of the art in the field of PLS was conducted in [68]. UAV systems have been envisaged to form an integral part of future wireless communication applications due their dynamic, flexible and flying nature.



(a) Illumination with one LED Array

(b) Illumination with two LED Arrays

(c) Illumination with four LED Arrays

(d) Optical power distribution

FIGURE 2.13: Power and illumination distribution against distance

It was shown in [69] that due to their ability to reach higher altitudes, they usually have a dominant LOS channels with the ground nodes. This capability can be used to provide confidentiality to the legitimate receivers against the eavesdroppers. This can be done by deploying UAVs to launch more effective jamming signal attacks to the terrestrial eavesdroppers. Figure 2.14 depicts a scenario in which a UAV is equipped with an air-to-ground jammer and a ground communication network comprising of a legitimate transmitter-receiver pair and an eavesdropper. The mobile UAV-enabled jammer is used to opportunistically jam the eavesdropper.

2.2.5 PLS in satellite communication

Satellite communication is getting more incorporated into current terrestrial wireless communication networks mainly because of its features which include wide area coverage and high bandwidth. Some noteworthy applications of satellite communication include but not limited to, military operations, TV broadcast and internet access. However, their broadcast nature and ability to provide wide coverage area makes them more vulnerable to eavesdropping. Traditionally, security in satellite communication is implemented in the upper layers of the protocol stack by

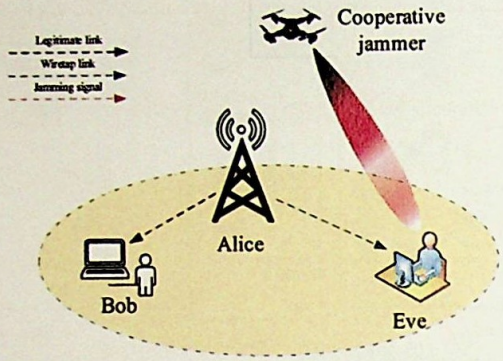


FIGURE 2.14: Cooperative jamming using UAV

means of encryption. PLS has been identified as an alternative to augment the current cryptography security measures [70]. We demonstrate a PLS concept in satellite using a system model shown in Figure 2.15 and derive the optimization problem.

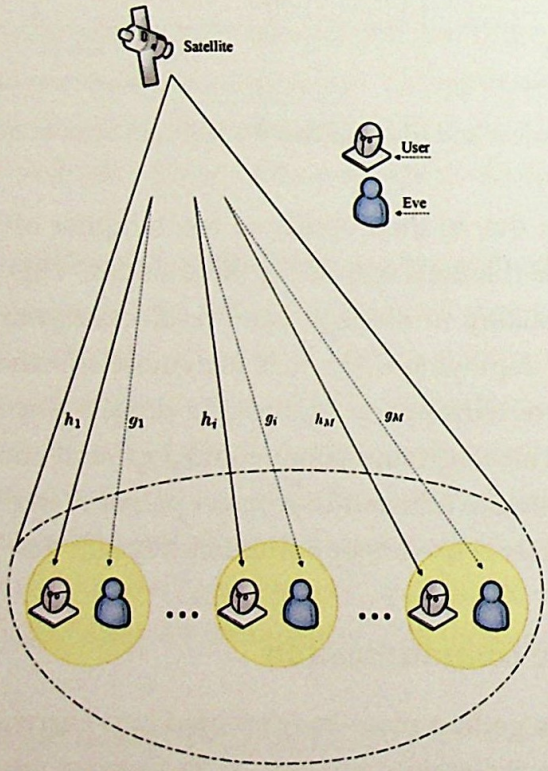


FIGURE 2.15: Multi-beam satellite communication network [71]

Suppose that the satellite transmit the signal s_i intended for the i^{th} legitimate user with average power $E\{|s_i|^2\} = 1$. The transmitted signal has a weighted beamforming vector given by $\mathbf{w}_i \in \mathbb{C}^{N\times 1}$. Therefore the overall transmitted signal is

given by:

$$\mathbf{x} = \sum_{i=1}^{M} \mathbf{w}_i s_i \tag{2.34}$$

The signal received by the i^{th}-legitimate and i^{th}-eavesdropper are given by Equation 2.35 and Equation 2.36 respectively.

$$y_{user-i} = \mathbf{h}_i^H \mathbf{w}_i s_i + \sum_{m \neq i}^{M} \mathbf{h}_i^H \mathbf{w}_m s_m + n_i \tag{2.35}$$

$$y_{e-i} = \mathbf{g}_i^H \mathbf{w}_i s_i + \sum_{m \neq i}^{M} \mathbf{g}_i^H \mathbf{w}_m s_m + n_{e-i} \tag{2.36}$$

where $\mathbf{h}_i \in \mathbb{C}^{N \times 1}$ denotes the channel gain vector between the i^{th}-intended user and the satellite, $\mathbf{g}_i \in \mathbb{C}^{N \times 1}$ denotes the channel gain vector between the i^{th} eavesdropper and the satellite, n_i and n_{e-i} are assumed to be zero-mean AWG noise of the i^{th}-intended user and the i^{th} eavesdropper, respectively. The achievable secrecy rate of i^{th}-intended user is given by:

$$R_s = \log_2 \left(1 + \frac{|\mathbf{h}_i^H \mathbf{w}_i|^2}{\sum_{m \neq i}^{M} |\mathbf{h}_i^H \mathbf{w}_m|^2 + \sigma_i^2} \right) - \log_2 \left(1 + \frac{|\mathbf{g}_i^H \mathbf{w}_i|^2}{\sum_{m \neq i}^{M} |\mathbf{g}_i^H \mathbf{w}_m|^2 + \sigma_{e-i}^2} \right) \tag{2.37}$$

The typical optimization problem of interest is the maximization of the achievable secrecy rate as per the minimum transmit power available constraints and this can be written mathematically as follows;

$$\begin{aligned} \max_{\mathbf{w}_i} \quad & R_s \\ \text{s.t.} \quad & \sum_{m=1}^{M} \|\mathbf{w}_i\|^2 \leq P_T, \end{aligned} \tag{2.38}$$

where P_T is the maximum transmit power of the satellite. The authors in [72] studied the problem of minimizing the transmit power on a multi-beam satellite while fulfilling the minimum per user secrecy rate. They further proposed an iterative algorithm to jointly optimize the transmission power and the beamforming vector by completely eliminating the co-channel interference and perfectly nulling out the received signal at the eavesdropper. Kalantari *et al.* in [73] also used PLS to address the issue of confidentiality in bidirectional satellite communication based on network coding. They designed the optimal beamforming weight vector which maximizes the sum secrecy rate by using semi-definite programming.

Chapter two presented a comprehensive overview and problem formulations of

physical layer security technologies. In the next two chapters the discussed technologies will be used to formulate and solve the PLS problems of this research work that were presented by the objectives in Chapter 1.

Chapter 3

Information jamming and intelligent reflecting surface (IRS) scheme

The first two chapters provided a comprehensive study of physical layer security in wireless communication networks by providing the underlying technologies and key concepts. In this chapter, the optimization of secrecy rate in a multiple-input single-output (MISO) system through the optimization of the information beamforming and jamming vectors is considered. Additionally, the optimization of the phase shifts of the intelligent reflecting surface is also investigated. This work specifically consider a benchmark model which was proposed by authors in [74]. However, this work introduce information jamming to the system and determine the impact of the jamming signal on the secrecy rate of the overall system compared to the benchmark model.

3.1 System model and problem formulation

3.1.1 System model

The MISO system equipped with an intelligent reflecting surface (IRS) as shown in Figure 3.1 is examined. The setup is made up of one transmitter (Alice), a single legitimate receiver (Bob), a single eavesdropper (Eve) and an IRS. It is assumed that Alice is equipped with N_T antennas for transmitting the information signal as well as the jamming signal, while Bob and Eve are equipped with single receive antenna nodes. The IRS has M passive reflecting elements. The channel between Alice and the IRS is denoted by $\mathbf{H}_{AI} \in \mathbb{C}^{M \times N_T}$ while $\mathbf{h}_{AB} \in \mathbb{C}^{N_T}$, $\mathbf{h}_{IB} \in \mathbb{C}^{M}$ denote the channel responses of Alice-Bob and IRS-Bob, respectively. The channel responses of Alice-Eve and IRS-Eve are respectively denoted by $\mathbf{h}_{AE} \in \mathbb{C}^{N_T}$ and $\mathbf{h}_{IE} \in \mathbb{C}^{M}$. The diagonal phase shift matrix modeling the reflecting elements of the IRS is given by $\boldsymbol{\Theta} = \text{diag}\{[\theta_1, \theta_2 \ldots, \theta_M]\}$, where $\theta_n = e^{j\phi_n}$ and $\phi_n \in [0, 2\pi)$ represents the phase shift coefficient of the n-th reflecting element of the IRS. The signal transmitted by

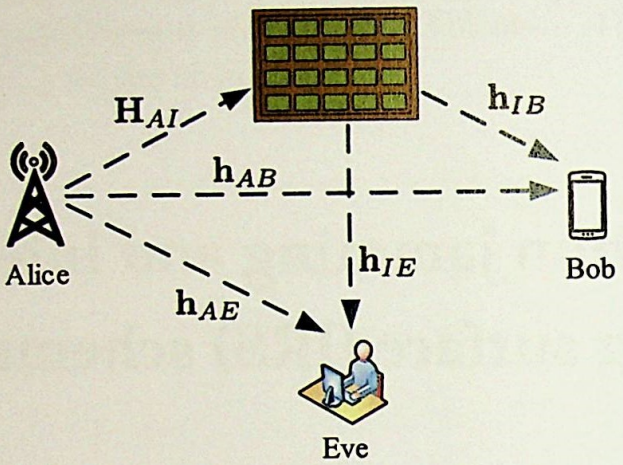


FIGURE 3.1: IRS system model

Alice is given by:

$$\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_1, \tag{3.1}$$

where $\mathbf{x}_0 \in \mathbb{C}^{N_T}$ is the information signal and $\mathbf{x}_1 \in \mathbb{C}^{N_T}$ is the jamming signal. The information jamming scheme proposed in [47] is adopted. In the said scheme the friendly jammer transmits the source message rather than the Gaussian noise as in the conventional schemes. The benefit of this approach is that the signal strength at Bob is significantly enhanced while at the same time canceling the received signal at Eve. Therefore, the transmitted signal in equation (3.1) can be expressed as $\mathbf{x} = \mathbf{w}s + \mathbf{v}s$, where, $s \sim \mathcal{CN}(0,1)$ is the information bearing signal and $\mathbf{w} \in \mathbb{C}^{N_T}$ and $\mathbf{v} \in \mathbb{C}^{N_T}$ are beamforming vectors for the information and jamming signals, respectively. Therefore, the signal received by Bob is given by:

$$\begin{aligned} y_B &= \mathbf{h}_{AB}^{\mathsf{H}}\mathbf{x} + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{x} + n_B \\ &= \mathbf{h}_{AB}^{\mathsf{H}}(\mathbf{w}s + \mathbf{v}s) + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}(\mathbf{w}s + \mathbf{v}s) + n_B \\ &= \mathbf{h}_{AB}^{\mathsf{H}}(\mathbf{w} + \mathbf{v})s + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}(\mathbf{w} + \mathbf{v})s + n_B, \end{aligned} \tag{3.2}$$

where n_B is an independent identically distributed (i.i.d.) complex Gaussian noise with zero mean and variance σ_B^2 for the intended receiver. Therefore, the signal received by Bob is comprised of the signal from the direct path channel, $\mathbf{h}_{AB}$ as well as the signal reflected by the IRS composite channel, $\mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}$. similarly, the signal received by Eve is given by:

$$y_E = \mathbf{h}_{AE}^{\mathsf{H}}\mathbf{x} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{x} + n_E, \tag{3.3}$$

where n_E is an i.i.d. complex Gaussian noise with zero mean and variance σ_E^2 for the eavesdropper. The secrecy of Bob and Eve, respectively can be expressed as:

$$R_B = \log_2\left(1 + \frac{|\mathbf{h}_{AB}^H(\mathbf{w}+\mathbf{v}) + \mathbf{h}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI}(\mathbf{w}+\mathbf{v})|^2}{\sigma_{n_B}^2}\right) \tag{3.4}$$

$$R_E = \log_2\left(1 + \frac{|\mathbf{h}_{AE}^H(\mathbf{w}+\mathbf{v}) + \mathbf{h}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI}(\mathbf{w}+\mathbf{v})|^2}{\sigma_{n_E}^2}\right) \tag{3.5}$$

3.1.2 Secrecy maximization

The scope of the first optimization problem is to maximize the achievable secrecy rate through a joint design of the information beamforming vector $\mathbf{w}$, jamming vector $\mathbf{v}$ and the diagonal phase shift matrix $\boldsymbol{\Theta}$ subject to the total transmit power constraint at Alice. Therefore, the optimization problem is defined as **P1** and it is mathematically given by:

$$\begin{aligned} \textbf{P1:} \quad \max_{\mathbf{w},\mathbf{v},\boldsymbol{\Theta}} \quad & R_s(\mathbf{w},\mathbf{v},\boldsymbol{\Theta}) \\ \text{s.t.} \quad & \|\mathbf{w}\|^2 + \|\mathbf{v}\|^2 \leq P_T \\ & |\theta_n| = 1 \quad \forall n = 1,\ldots,M, \end{aligned} \tag{3.6}$$

where the achievable secrecy rate, $R_s(\mathbf{w},\mathbf{v},\boldsymbol{\Theta}) = R_B - R_E$ and P_T denotes the maximum transmit power available at the transmitter.

3.2 Solution

The transmit power budget constraint, given by $\|\mathbf{w}\|^2 + \|\mathbf{v}\|^2 \leq P_T$ in equation (3.6) is convex. However, problem **P1** is difficult to solve because the objective function is non-concave and also due to the non-convex unit modulus constraint, $|\theta_n| = 1$ introduced by the IRS phase shifting implementation. **P1** can be broken down into sub-problems which can be efficiently solved when one of the optimization variables $(\mathbf{w},\mathbf{v})$ and $\boldsymbol{\Theta}$ is fixed. Hence, an alternating optimization (AO) algorithm is proposed for solving $(\mathbf{w},\mathbf{v})$ and $\boldsymbol{\Theta}$ by iteratively optimizing a single variable at a time while fixing one until convergence. AO algorithm has been used in [75, 76, 77] to successfully solve a wide range of problems in wireless communication design for IRS-enabled devices and resource allocation.

3.2.1 Closed form solution for beamforming and jamming vectors, w and v given Θ

In the first sub-problem, the value of Θ is fixed to solve for $\mathbf{w}$ and $\mathbf{v}$. Hence, the second constraint can be ignored. Without loss of generality, the assumption is that the variance of Bob and Eve's noise are equal. Therefore, the secrecy rate defined in equation (3.6) can be expressed in this form;

$$R_s(\mathbf{w},\mathbf{v}) = \log_2\left(\frac{\sigma^2 + |(\mathbf{h}_{AB}^{\mathrm{H}} + \mathbf{h}_{IB}^{\mathrm{H}}\Theta\mathbf{H}_{AI})(\mathbf{w}+\mathbf{v})|^2}{\sigma^2 + |(\mathbf{h}_{AE}^{\mathrm{H}} + \mathbf{h}_{IE}^{\mathrm{H}}\Theta\mathbf{H}_{AI})(\mathbf{w}+\mathbf{v})|^2}\right). \tag{3.7}$$

Suppose we now let $\mathbf{h}_B = \mathbf{h}_{AB}^{\mathrm{H}} + \mathbf{h}_{IB}^{\mathrm{H}}\Theta\mathbf{H}_{AI}$ and $\mathbf{h}_E = \mathbf{h}_{AE}^{\mathrm{H}} + \mathbf{h}_{IE}^{\mathrm{H}}\Theta\mathbf{H}_{AI}$. Then the first sub-problem of **P1** is given by;

$$\begin{aligned} \textbf{P1.1:} \quad \max_{\mathbf{w},\mathbf{v}} \quad & \log_2\left(\frac{\sigma^2 + |\mathbf{w}\mathbf{h}_B + \mathbf{v}\mathbf{h}_B|^2}{\sigma^2 + |\mathbf{w}\mathbf{h}_E + \mathbf{v}\mathbf{h}_E|^2}\right), \\ \text{s.t.} \quad & \mathbf{w}^{\mathrm{H}}\mathbf{w} + \mathbf{v}^{\mathrm{H}}\mathbf{v} \leq P_T. \end{aligned} \tag{3.8}$$

The goal of this sub-problem is to:

i. Design the information signal beamforming vector, $\mathbf{w}$ which maximizes the information transmitted towards Bob. In this way the energy is focused towards Bob hence significantly improving Bob's SNR compared to Eve. Since the intention is to maximize the transmission to only one user, the transmitter can employ the MRT strategy to design the information signal beamforming vector, $\mathbf{w}$ [44]. This implies that the optimal value of $\mathbf{w}$ is given by

$$\mathbf{w}^\star = \sqrt{P_T}\frac{\mathbf{h}_B}{\|\mathbf{h}_B\|}. \tag{3.9}$$

ii. The second part of sub-problem one is to solve for the optimal value of the jamming vector $\mathbf{v}$. The assumption made to solve this problem is that, the optimal value of $\mathbf{w}$ is given by equation (3.9), hence it is fixed in the optimization problem. The log function is discarded in order to make **P1.1** more tractable. Therefore, the optimization problem can be reformulated as;

$$\begin{aligned} \textbf{P1.2:} \quad \max_{\mathbf{v}} \quad & \frac{|\mathbf{w}\mathbf{h}_B + \mathbf{v}\mathbf{h}_B|^2 + \sigma^2}{|\mathbf{w}\mathbf{h}_E + \mathbf{v}\mathbf{h}_E|^2 + \sigma^2} \\ \text{s.t.} \quad & \|\mathbf{v}\|^2 \leq P_T - \|\mathbf{w}\|^2. \end{aligned} \tag{3.10}$$

Due to the design the jamming beamforming vector, $\mathbf{v}$ which strengthen the signal received by Bob and eliminates the signal leaked to Eve, it implies that $\mathbf{v}\mathbf{h}_E = 0$. Therefore, **P1.2** reduces to;

$$\begin{aligned} \textbf{P1.3:} \quad & \max_{\mathbf{v}} \quad |\mathbf{w}\mathbf{h}_B + \mathbf{v}\mathbf{h}_B|^2 \\ & \text{s.t.} \quad \mathbf{v}\mathbf{h}_E = 0 \\ & \qquad \|\mathbf{v}\|^2 \leq P_T - \|\mathbf{w}\|^2. \end{aligned} \tag{3.11}$$

In order to provide a closed form solution to **P1.3**, the following analysis and simplifications are made. Applying the triangle inequality to the objective function of **P1.3** yields;

$$|\mathbf{w}\mathbf{h}_B + \mathbf{v}\mathbf{h}_B|^2 \leq (|\mathbf{w}\mathbf{h}_B| + |\mathbf{v}\mathbf{h}_B|)^2. \tag{3.12}$$

The LHS of equation (3.12) is equal to the RHS if and only if, they have the same phase angle i.e., $\angle \mathbf{w}\mathbf{h}_B = \angle \mathbf{v}\mathbf{h}_B$. It is important to notice that if $\mathbf{v}$ satisfies the two constraints of **P1.3**, then so does $\mathbf{v}e^{j\phi}$ for any arbitrary ϕ. Hence it implies that $|\mathbf{v}\mathbf{h}_B| = |\mathbf{v}e^{j\phi}\mathbf{h}_B|$ always holds. Thus the equality in equation (3.12) is always true for maximizing the objective function of **P1.3** when the optimal solution is achieved. This implies that, **P1.3** is equivalent to the following problem;

$$\begin{aligned} & \max_{\mathbf{v}} \quad |\mathbf{v}\mathbf{h}_B|^2 \\ & \text{s.t.} \quad \mathbf{v}\mathbf{h}_E = 0 \\ & \qquad \|\mathbf{v}\|^2 \leq P_T - \|\mathbf{w}\|^2. \end{aligned} \tag{3.13}$$

The Lagrangian of equation (3.13) can be expressed as

$$\begin{aligned} \mathcal{L}(\mathbf{v}, \lambda, \mu) &= \mathbf{v}^{\mathrm{H}}\mathbf{h}_B^{\mathrm{H}}\mathbf{h}_B\mathbf{v} - \lambda(\mathbf{v}^{\mathrm{H}}\mathbf{v} - P_T + \mathbf{w}^{\mathrm{H}}\mathbf{w}) - \mu\mathbf{v}\mathbf{h}_E \\ &= \mathbf{v}^{\mathrm{H}}(\mathbf{h}_B^{\mathrm{H}}\mathbf{h}_B - \lambda\mathbf{I})\mathbf{v} + \lambda(\mathbf{w}^{\mathrm{H}}\mathbf{w} - P_T) - \mu\mathbf{v}\mathbf{h}_E, \end{aligned} \tag{3.14}$$

where $\lambda \geq 0, \mu \geq 0$ are the Lagrange multipliers for each constraint. Let S_v be a set specified by the two constraints in **P1.3**, then the Lagrange dual function can be defined as

$$f(\lambda, \mu) = \max_{\mathbf{v} \in S_v} \quad \mathcal{L}(\mathbf{v}, \lambda, \mu), \tag{3.15}$$

it then follows that the Lagrangian dual problem is defined as

$$\min_{\lambda, \mu \geq 0} \quad f(\lambda, \mu). \tag{3.16}$$

To solve equation (3.14) the stationarity KKT conditions are employed. These conditions states that $\frac{\partial \mathcal{L}}{\partial \mathbf{v}} = 0$, which implies that;

$$\begin{aligned} \mathbf{v}(\mathbf{h}_B^{\mathsf{H}}\mathbf{h}_B - \lambda \mathbf{I}) - \mu \mathbf{h}_E &= 0 \\ \mathbf{v} &= \frac{\mu \mathbf{h}_E}{\mathbf{h}_B^{\mathsf{H}}\mathbf{h}_B - \lambda \mathbf{I}}. \end{aligned} \tag{3.17}$$

$$\frac{\mu \mathbf{h}_E^{\mathsf{H}}}{(\mathbf{h}_B^{\mathsf{H}}\mathbf{h}_B - \lambda \mathbf{I})^{\mathsf{H}}} \cdot \frac{\mu \mathbf{h}_E}{\mathbf{h}_B^{\mathsf{H}}\mathbf{h}_B - \lambda \mathbf{I}} \leq P_T - \|\mathbf{w}\|^2 \tag{3.18a}$$

$$\frac{\mu \mathbf{h}_E}{\mathbf{h}_B^{\mathsf{H}}\mathbf{h}_B - \lambda \mathbf{I}} \mathbf{h}_E = 0, \tag{3.18b}$$

Using equation (3.17), as well as equations (3.18a) and (3.18b), which are derived from the stated constraints of our problem, equation (3.19) is obtained.

$$\mathbf{v}_1^* = \left(\sqrt{P_T} - \mathbf{w}\right) \frac{(\mathbf{I} - \hat{\mathbf{h}}_E \hat{\mathbf{h}}_E^{\mathsf{H}})\mathbf{h}_B}{\|(\mathbf{I} - \hat{\mathbf{h}}_E \hat{\mathbf{h}}_E^{\mathsf{H}})\mathbf{h}_B\|}, \tag{3.19}$$

where $\hat{\mathbf{h}}_E = \frac{\mathbf{h}_E}{\|\mathbf{h}_E\|}$. The optimal solution to **P1.3** is now given by

$$\begin{aligned} \mathbf{v}^\star &= \mathbf{v}_1^* e^{j\hat{\phi}^*} \\ &= \left(\sqrt{P_T} - \mathbf{w}\right) \frac{(\mathbf{I} - \hat{\mathbf{h}}_E \hat{\mathbf{h}}_E^{\mathsf{H}})\mathbf{h}_B e^{j\hat{\phi}^*}}{\|(\mathbf{I} - \hat{\mathbf{h}}_E \hat{\mathbf{h}}_E^{\mathsf{H}})\mathbf{h}_B\|}, \end{aligned} \tag{3.20}$$

where $\hat{\phi}^* = \angle \mathbf{w}\mathbf{h}_B - \angle \mathbf{v}_1^* \mathbf{h}_B$.

3.2.2 Optimization of IRS phase shifting coefficients

In the second sub-problem of **P1**, the intention is to optimize the phase shift of the IRS using the optimal beamforming and jamming vectors, $\mathbf{w}$ and $\mathbf{v}$ obtained in equation (3.9) and equation (3.20), respectively. Therefore, the equivalent optimization problem is given by

$$\begin{aligned} \textbf{P2:} \quad \max_{\boldsymbol{\Theta}} \quad & \frac{|(\mathbf{h}_{AB}^{\mathsf{H}} + \mathbf{h}_{IB}^{\mathsf{H}} \boldsymbol{\Theta} \mathbf{H}_{AI})(\mathbf{w} + \mathbf{v})|^2 + \sigma^2}{|(\mathbf{h}_{AE}^{\mathsf{H}} + \mathbf{h}_{IE}^{\mathsf{H}} \boldsymbol{\Theta} \mathbf{H}_{AI})(\mathbf{w} + \mathbf{v})|^2 + \sigma^2} \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M. \end{aligned} \tag{3.21}$$

Let $\mathbf{b}_i = \mathbf{h}_{Ai}^{\mathsf{H}}(\mathbf{w}+\mathbf{v})$, $\mathbf{a}_i = \text{diag}\{\mathbf{h}_{Ii}^{\mathsf{H}}\}\mathbf{H}_{AI})(\mathbf{w}+\mathbf{v})$ for $\forall i \in (B,E)$ and $\boldsymbol{\theta} = [\theta_1, \theta_2, \ldots, \theta_M]^T$. Therefore, **P2** is transformed into;

$$\begin{aligned} \max_{\boldsymbol{\theta}} \quad & \frac{|b_B + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_B|^2 + \sigma^2}{|b_E + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_E|^2 + \sigma^2} \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M. \end{aligned} \tag{3.22}$$

Using the Dinklebach's transform [78], equation (3.22) can be expressed as follows ;

$$\begin{aligned} \min_{\boldsymbol{\theta}} \quad & \frac{|b_E + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_E|^2 + \sigma^2}{|b_B + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_B|^2 + \sigma^2} \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M. \end{aligned} \tag{3.23}$$

The corresponding parametric equation of equation (3.23) is given by [79];

$$\begin{aligned} \min_{\boldsymbol{\theta}} \quad & |b_E + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_E|^2 + \sigma^2 - \mu(|b_B + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_B|^2 + \sigma^2) \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M. \end{aligned} \tag{3.24}$$

The objective function of equation (3.24) can be simplified into;

$$\begin{aligned} f(\mu) &= |b_E + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_E|^2 + \sigma^2 - \mu(|b_B + \boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_B|^2 + \sigma^2) \\ &= (\boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_E + b_E)^{\mathsf{H}}(\boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_E + b_E) + \sigma^2 \\ &- \mu[(\boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_B + b_B)^{\mathsf{H}}(\boldsymbol{\theta}^{\mathsf{H}}\mathbf{a}_B + b_B) + \sigma^2] \\ &= \boldsymbol{\theta}^{\mathsf{H}}(\mathbf{a}_E\mathbf{a}_E^{\mathsf{H}} - \mu\mathbf{a}_B\mathbf{a}_B^{\mathsf{H}})\boldsymbol{\theta} - 2\Re\{\boldsymbol{\theta}^{\mathsf{H}}(\mu b_B^*\mathbf{a}_B - b_E^*\mathbf{a}_E)\} \\ &+ |b_E|^2 - \mu|b_B|^2 + (1-\mu)\sigma^2. \end{aligned} \tag{3.25}$$

Therefore, the optimization problem for the phase shifts can be written as;

$$\begin{aligned} \min_{\boldsymbol{\theta}} \quad & \boldsymbol{\theta}^{\mathsf{H}}(\mathbf{a}_E\mathbf{a}_E^{\mathsf{H}} - \mu\mathbf{a}_B\mathbf{a}_B^{\mathsf{H}})\boldsymbol{\theta} - 2\Re\{\boldsymbol{\theta}^{H}(\mu b_B^*\mathbf{a}_B - b_E^*\mathbf{a}_E)\} \\ & + |b_E|^2 - \mu|b_B|^2 + (1-\mu)\sigma^2 \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M. \end{aligned} \tag{3.26}$$

Applying the triangle inequality on the objective function of equation (3.26), the following expression is obtained;

$$\begin{aligned} \min_{\boldsymbol{\theta}} \quad & \lambda_{max}(\boldsymbol{\Phi})\|\boldsymbol{\theta}\|^2 - 2\Re\{\boldsymbol{\theta}^{\mathsf{H}}\beta\} \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M, \end{aligned} \tag{3.27}$$

where $\mathbf{\Phi} = \mathbf{a}_E\mathbf{a}_E^{\mathsf{H}} - \mu\mathbf{a}_B\mathbf{a}_B^{\mathsf{H}}$ and $\beta = \left(\lambda_{max}(\mathbf{\Phi})\mathbf{I} - \mathbf{\Phi}\right)\tilde{\theta} + \mu b_B^*\mathbf{a}_B - b_E^*\mathbf{a}_E$. The optimal solution to (3.24) is given by [80];

$$\theta^\star = \left[e^{jarg(\beta_1)}, \ldots, e^{jarg(\beta_M)}\right]^T. \tag{3.28}$$

The AO algorithm for solving problem **P1** is given by algorithm 1. It is implemented in section 3.3 in the numerical analysis to achieve the optimal secrecy rate level through optimizing the beamforming and jamming signal and the IRS phase shifts in the alternating manner.

Algorithm 1 : Proposed algorithm for **P3**

Input: P_T, f_o, $\mathbf{H}_{AI}$, $\mathbf{h}_{AB}^{\mathsf{H}}$, $\mathbf{h}_{IB}^{\mathsf{H}}$, $\mathbf{h}_{AE}^{\mathsf{H}}$, $\mathbf{h}_{IE}^{\mathsf{H}}$, convergence factor
1: **Initialization**
2: Compute the initial phase shifts based on the IRS configuration and Transmitter and Receiver locations, $\tilde{\mathbf{\Theta}}$.
3: **repeat**
4: Set $\mathbf{\Theta} = \tilde{\mathbf{\Theta}}$ and compute the beamforming vectors, $\mathbf{w}$ and $\mathbf{v}$ using equation (3.9) and equation (3.20).
5: Set $\mathbf{w}^\star = \mathbf{w}$ and $\mathbf{v}^\star = \mathbf{v}$, and calculate $\theta^\star$ using equation (3.28)
6: **until** convergence
Output: $\mathbf{w}^\star$, $\mathbf{v}^\star$, $\theta^\star$

3.3 Numerical results and simulations

An IRS with operational frequency of 30 GHz which implies a 1 mm of wavelength is taken into consideration. To avoid scattering of the wave and ensure maximization of the beam, the dimensions of the meta plate are chosen to be $\frac{\lambda}{5} \times \frac{\lambda}{5}$. The simulation setup is shown in Figure 3.2. The simulation parameters are shown in Table 3.1. The path loss is modeled as $\mathrm{PL} = \left(\mathrm{PL}_0 - 10\varsigma \log\left(\frac{d}{d_0}\right)\right)$ dB where, PL_0 denotes the path loss at a reference distance, d_0, ς is the path loss exponent and d is

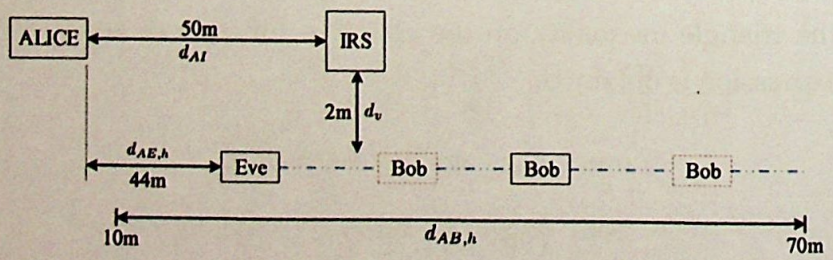


FIGURE 3.2: System setup

Table 3.1: Simulation Parameters

Parameter	Value
Carrier Frequency	30 GHz
IRS Configuration	Metal plate dimensions of $\frac{\lambda}{5} \times \frac{\lambda}{5}$
Path loss at 1m	$PL_0 = -30$dB
Path loss exponents	$\varsigma_{AI} = 2.2$, $\varsigma_{IB} = 2.5$, $\varsigma_{IE} = 2.5$, $\varsigma_{AB} = 3.5$ and $\varsigma_{AE} = 3.5$
Other parameters	$N_T = 4$, $P_T = 15$ dBW and $\sigma = -75$ dBW, L = 32

the given distance between the transmitter and the receiver. The distance between the transmitter Alice and the IRS is given by $d_{AI} = 50$m. The horizontal distance between Alice and Eve is denoted by $d_{AE,h} = 44$m. Furthermore, both Bob and Eve lie in a horizontal line which is parallel to the one between Alice and the IRS and the vertical distance between these two lines is $d_v = 2$m. The secrecy rate performance of the system is analysed by varying the horizontal distance between Alice and Bob, $d_{AB,h}$.

Secrecy vs distance

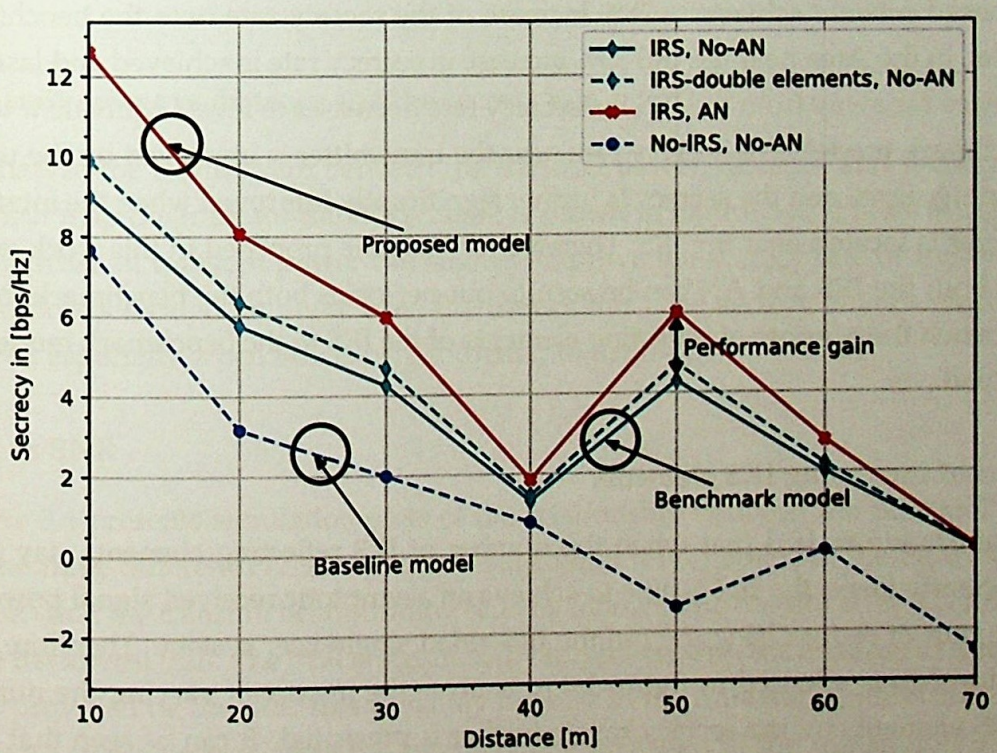


FIGURE 3.3: Secrecy rate vs distance.

The relationship between the secrecy rate versus distance for the different schemes is shown in Figure 3.3. In the figure the plot with the dashed blue line is for the baseline system which has no IRS and no AN, and it can be seen that the secrecy rate reduces as Bob moves away from the transmitter. The secrecy rate drastically reduces to below zero after Bob passes a distance of 44m away from the transmitter because after this point, Eve is more close to the transmitter than Bob which implies that Eve is receiving a much better signal gain compared to Bob which poses a great threat in the security of the legitimate transmission of the scheme. The second plot in the figure is of the benchmark scheme from [74] which is comprised of the IRS with just information beamforming with no AN. This model proves that the introduction of IRS significantly enhances the secrecy rate compared to the baseline model and this is due to the reflect beamforming gain provided by the IRS. A further improvement of the secrecy rate can be made by doubling the number of reflecting elements to 64 which is shown by the double-elements plot on the figure. The simulation plot of our proposed scheme is depicted by the plot with a red color. To evaluate the performance of the models presented in the figure we divide the region into three parts; the region which is 10 meters near the transmitter which we call Area near transmitter, the region 10 meters near the IRS which we refer to as Area near IRS and lastly the region which is 20 meters away from the IRS which is referred to as Area far away from IRS. From the figure it can be seen that in the Area near transmitter the proposed scheme achieves a 28% increase of the secrecy rate over the benchmark model, in the Area near the IRS 33% increase in secrecy rate is achieved and lastly in the Area far away from the IRS the secrecy rate decreases to levels equivalent to the benchmark model. The secrecy rate near the transmitter is improved by the use of jamming signal and the secrecy is further significantly improved when the intended receiver is located near the IRS. Therefore the scheme proposed in this work which uses both the IRS and AN can be seen to out-performs both the benchmark model and when the number of reflecting elements of the IRS in the benchmark model are doubled.

Effect of increasing IRS elements

It was shown in [81] that when the number of IRS reflecting elements, say N, is sufficiently large, the IRS is able to achieve an asymptotic received signal power or SNR gain of order $\mathcal{O}(\log_2 N^2)$ in the IRS-aided single-user system. Therefore, this relationship is adopted in figure 3.4 to analyse the impact of varying the number of IRS elements on the secrecy rate is further is presented. It can be seen that with increasing the number of elements from 4 to 40 elements we are able to significantly increase the secrecy rate of the transmission scheme which only uses beamforming

from around 2 bps/Hz to almost 12 bps/Hz. It it worth noting that even though the secrecy is improved it comes at a cost of increased computations in the algorithm for optimizing the phase shifts of the IRS. This implies that a longer time will be required for the algorithm to converge to the optimal solution.

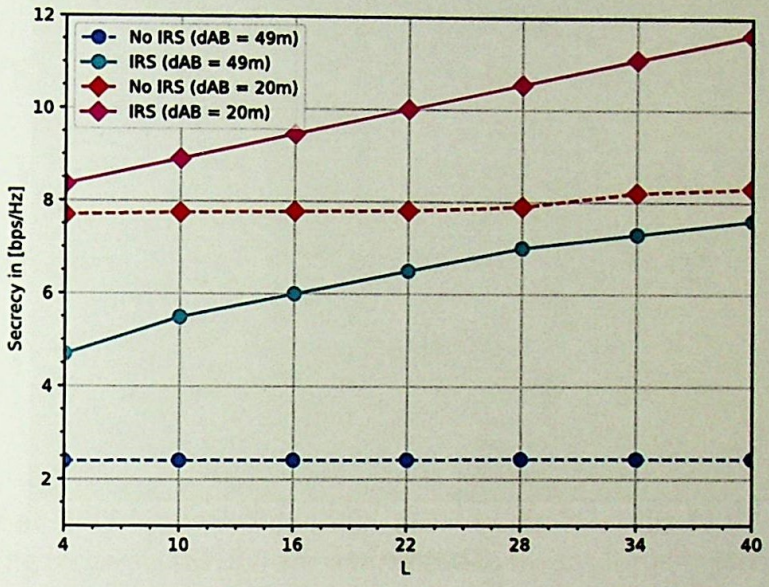


FIGURE 3.4: Secrecy rate versus the number of reflecting elements.

Transmit power vs distance and the secrecy rate

To analyze the relationship between the transmit power, distance and secrecy rate the heat map diagram for the IRS scheme is shown in Figure 3.5. It is showing that the increase in transmit power can slightly improve the secrecy rate of the system when Bob is located far away from the transmitter. The secrecy is very much improved especially when Bob is perpendicular to the IRS.

BER vs SNR

Figure 3.6 presents simulation plots of the relationship between the BER and SNR for the three different PLS schemes investigated in this chapter. In the figure it can be seen that the transmit beamforming scheme followed by the IRS with AN for Bob have the lowest BER. The BER is significantly improved with the increase in received SNR provided by the IRS. This is mainly because in the transmit beamforming Bob receive a diversity gain from the beamforming provided at the transmitter and in the IRS plus AN the SNR gain is improved which improves Bob's performance than

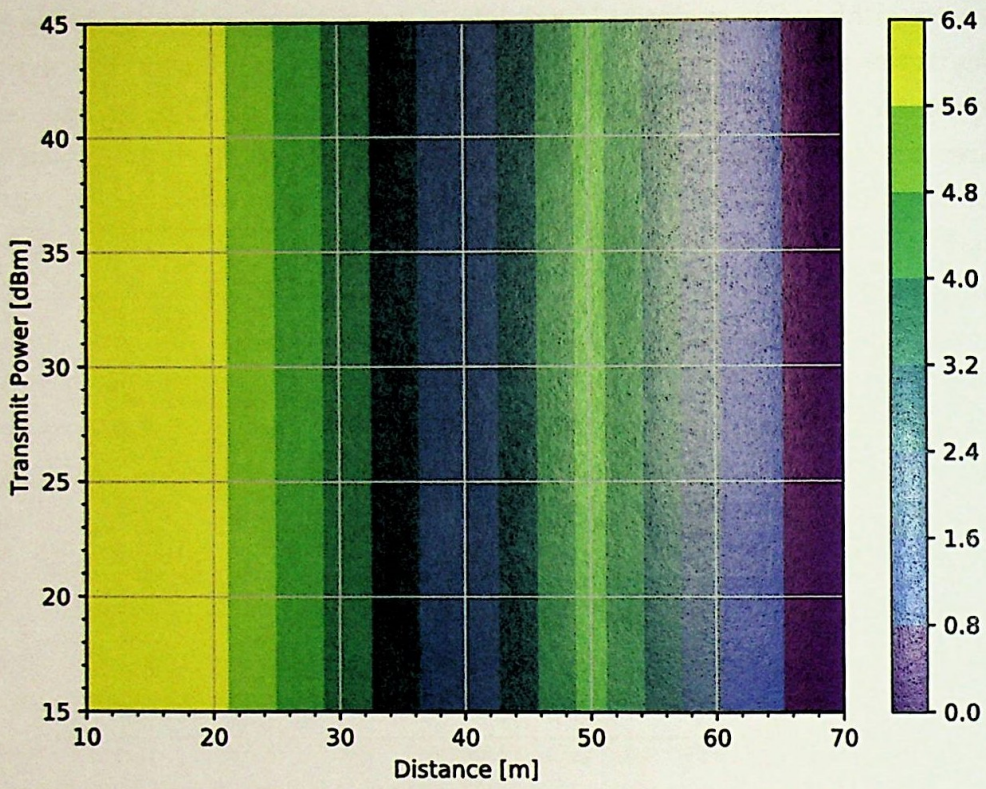


FIGURE 3.5: Transmit power vs distance.

Eve's. The plot also shows that with the use of IRS plus AN, Eve receives the worst BER because she experiences a poor channel compared to Bob.

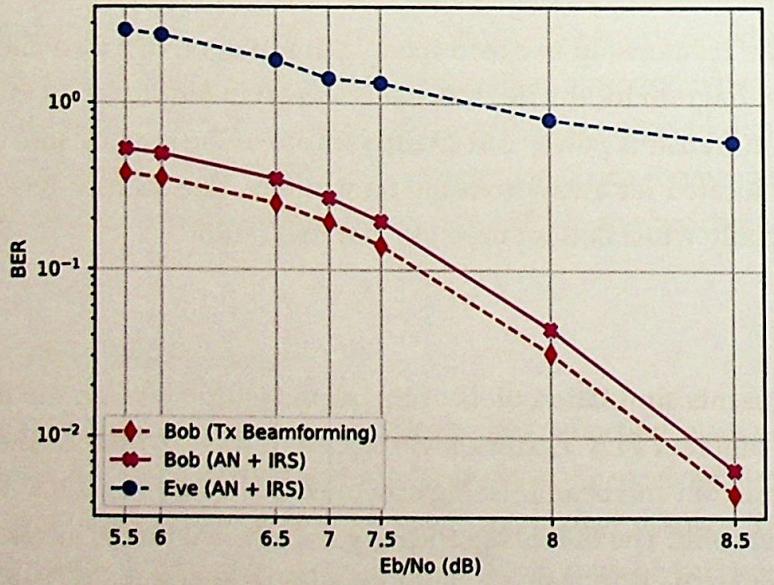


FIGURE 3.6: BER curves for Bob and Eve with transmit beamforming and IRS and artificial noise added

Chapter 4

A physical layer security(PLS) scheme using wireless information and power transfer (WIPT) and intelligent reflecting surface (IRS)

The previous chapter studied the optimization of secrecy rate, in this chapter, energy harvesting receivers (EHRs) are introduced to the multiple-input single-output (MISO) system similar to the one discussed in Chapter 3 to harvest some amount of power carried by the RF signal. Our objective is to maximize the energy harvested by the EH receivers while satisfying the constraints of the secrecy rate at Bob, the transmit power available at the transmitter, and the phase shifts of the IRS. It should however be noted that for this optimization problem does not take into account the jamming signal.

This work is motivated by the work in [82]. Unlike the system proposed in [82], this thesis considers the addition of an IRS to the model. The addition of IRS introduces unit-modulus constraints to the optimization problem, which makes the energy harvesting maximization problem non-convex and difficult to solve using the successive convex approximation (SCA). Furthermore, the proposed system does not incorporate AN and the formulated problem is solved in two parts using interior-point methods (IPM) and manifold optimization.

4.1 System model and problem formulation

4.1.1 System model

The system under consideration is a MISO system model as illustrated in Figure 4.1. The model is made of a transmitter with N transmitting antennas, an IRS with M reflecting elements, an information receiver, and an eavesdropper, both equipped with

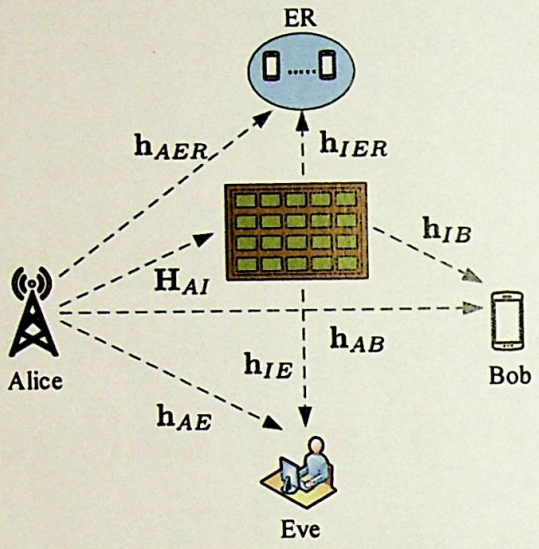


FIGURE 4.1: Energy harvesting system model

a single receiving antenna. In addition, there are $\mathcal{K} = \{1, \ldots, k\}$ energy harvesting receivers. The transmitter uses beamforming to steer the information signal towards the legitimate receiver in the presence of the eavesdropper. The work assumes both line-of-sight (LOS) and non line-of-sight (NLOS) signal propagation between the transmitter and the receivers. The LOS channel paths between the Alice-Bob, Alice-Eve and Alice-EHR are given by $\mathbf{h}_{AB} \in \mathbb{C}^N$, $\mathbf{h}_{AE} \in \mathbb{C}^N$ and $\mathbf{h}_{AER} \in \mathbb{C}^N$, respectively. The NLOS channel paths between Alice-IRS, IRS-Bob, IRS-Eve and IRS-EHR are denoted by $\mathbf{H}_{AI} \in \mathbb{C}^{M \times N}$, $\mathbf{h}_{IB} \in \mathbb{C}^M$, $\mathbf{h}_{IE} \in \mathbb{C}^M$ and $\mathbf{h}_{IER} \in \mathbb{C}^M$, respectively. The signal received by the legitimate user and the eavesdropper are given by:

$$y_B = \mathbf{h}_{AB}^{\mathsf{H}}\mathbf{x} + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{x} + n_B, \tag{4.1}$$

$$y_E = \mathbf{h}_{AE}^{\mathsf{H}}\mathbf{x} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{x} + n_E, \tag{4.2}$$

where n_B and n_E are i.i.d. complex Gaussian noise for each with zero mean and variance σ_B^2 and σ_E^2, respectively. The secrecy rate achieved at the legitimate user is expressed as:

$$R_s = \left[\log_2\left(1 + \frac{|(\mathbf{h}_{AB}^{\mathsf{H}} + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_B}^2}\right) - \log_2\left(1 + \frac{|(\mathbf{h}_{AE}^{\mathsf{H}} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_E}^2}\right)\right]^+. \tag{4.3}$$

The signal received at the $k-th$ EH receiver is given by:

$$y_{ER,k} = \mathbf{h}_{AER,k}^{\mathsf{H}}\mathbf{x} + \mathbf{h}_{IER,k}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{x} + n_{ER,k}, \quad k = 1, \ldots, K, \tag{4.4}$$

where n_{ER} is the i.i.d. complex Gaussian noise with zero mean and variance σ^2. According to the law of conservation of energy, the total harvested RF-power at the $k-th$ energy receiver is given by [83]:

$$E_k = \eta \cdot |(\mathbf{h}_{AER,k}^{H} + \mathbf{h}_{IER,k}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2, \quad \forall k, \tag{4.5}$$

where $\eta \in (0, 1]$ is the energy harvesting efficiency.

4.1.2 Energy harvesting maximization

This optimization problem is concerned with the maximization of the energy harvested by the energy harvesting receivers. The design objective is to maximize the energy harvested by EH receivers and this can be formulated mathematically as:

$$\begin{aligned}
\textbf{P4:} \quad & \max_{\mathbf{w},\boldsymbol{\Theta}} \quad \min_{k} \quad E_k && \text{(4.6a)}\\
& \text{s.t.} \quad \|\mathbf{w}\|^2 \leq P_T, && \text{(4.6b)}\\
& \quad\quad \min R_s \geq R, && \text{(4.6c)}\\
& \quad\quad |e^{(j\phi_n)}| = 1 \quad \forall n = 1, \ldots, M. && \text{(4.6d)}
\end{aligned}$$

The formulated problem given in **P4** is non convex due to the non-convex objective function and the secrecy constraints given by equation (4.6c) as well as the unit modulus IRS phase shifts constraints given by equation (4.6d). In order to tackle the non-convex objective function defined by the energy harvesting the method proposed in [82] is adopted, and the slack variable t for the minimum energy harvesting objective function is defined such that **P4** can be written as;

$$\begin{aligned}
\textbf{P5:} \quad & \max_{\mathbf{w},\boldsymbol{\Theta},t} \quad t && \text{(4.7a)}\\
& \text{s.t.} \quad \|\mathbf{w}\|^2 \leq P, && \text{(4.7b)}\\
& \quad\quad \min_{k} \quad E_k \geq E, && \text{(4.7c)}\\
& \quad\quad \min R_s \geq R, && \text{(4.7d)}\\
& \quad\quad |e^{(j\phi_n)}| = 1 \quad \forall n = 1, \ldots, M. && \text{(4.7e)}
\end{aligned}$$

Problem **P5** is still non-convex due to the constraints equations (4.7c) to (4.7e). The non-convexity of the minimum energy harvesting constraint in equation (4.7c) is tackled through the use of first order Taylor's approximation. Consider;

$$|(\mathbf{h}_{AER,k}^{H} + \mathbf{h}_{IER,k}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2 \geq E. \tag{4.8}$$

The real part of the LHS of equation (4.8) is defined as $x_k = \Re\{(\mathbf{h}_{AER,k}^{\mathsf{H}} + \mathbf{h}_{IER,k}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}\}$ and the imaginary part as $y_k = \Im\{(\mathbf{h}_{AER,k}^{\mathsf{H}} + \mathbf{h}_{IER,k}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}\}$, i.e., $x_k^2 + y_k^2 \geq E$, hence, $\mathbf{u}_k = \begin{bmatrix} x_k \\ y_k \end{bmatrix}$. This implies that;

$$\begin{aligned} |(\mathbf{h}_{AER,k}^{\mathsf{H}} + \mathbf{h}_{IER,k}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2 &= x_k^2 + y_k^2 \\ &= \begin{bmatrix} x_k & y_k \end{bmatrix} \begin{bmatrix} x_k \\ y_k \end{bmatrix} \\ &= \mathbf{u}_k^{\mathsf{H}}\mathbf{u}_k. \end{aligned} \tag{4.9}$$

Therefore, using the first order Taylor approximation equation (4.9) can be written as;

$$\mathbf{u}_k^{\mathsf{H}}\mathbf{u}_k \approx \|\mathbf{u}^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}^{(n)}(i)[\mathbf{u}(i) - \mathbf{u}^{(n)}(i)], \tag{4.10}$$

where i denotes the $i-th$ element of the vector $\mathbf{u}_k$ for the $n-th$ iteration. In order to deal with the non-concave secrecy rate constraint given by equation (4.7d) the secrecy rate constraint is re-written as;

$$\frac{1 + \frac{|(\mathbf{h}_{AB}^{\mathsf{H}} + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_B}^2}}{1 + \frac{|(\mathbf{h}_{AE}^{\mathsf{H}} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_E}^2}} \geq 2^R \tag{4.11a}$$

$$\frac{|(\mathbf{h}_{AB}^{\mathsf{H}} + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_B}^2} \geq (2^R - 1) + 2^R \cdot \frac{|(\mathbf{h}_{AE}^{\mathsf{H}} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_E}^2} \tag{4.11b}$$

$$\frac{|(\mathbf{h}_{AB}^{\mathsf{H}} + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_B}^2} \geq \begin{bmatrix} \frac{2^{R/2}}{\sigma_{n_E}^2}(\mathbf{h}_{AE}^{\mathsf{H}} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w} \\ (2^R - 1)^{1/2} \end{bmatrix}^{\mathsf{H}} \begin{bmatrix} \frac{2^{R/2}}{\sigma_{n_E}^2}(\mathbf{h}_{AE}^{\mathsf{H}} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w} \\ (2^R - 1)^{1/2} \end{bmatrix}. \tag{4.11c}$$

The Schur's complement of a matrix:

$$\mathbf{M} = \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^T & \mathbf{C} \end{bmatrix}, \tag{4.12}$$

is defined as [31]:

$$\mathbf{S} = \mathbf{C} - \mathbf{B}^T\mathbf{A}^{-1}\mathbf{B}. \tag{4.13}$$

Using equation (4.13), the secrecy rate constraint, which was re-formulated in equation (4.11) can be written as;

$$\begin{bmatrix} (\mathbf{h}_{AB}^{H}+\mathbf{h}_{IB}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}\mathbf{I} & \begin{bmatrix} \frac{2^{R/2}}{\sigma_{n_E}^2}(\mathbf{h}_{AE}^{H}+\mathbf{h}_{IE}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w} \\ (2^R-1)^{1/2} \end{bmatrix} \\ \begin{bmatrix} \frac{2^{R/2}}{\sigma_{n_E}^2}(\mathbf{h}_{AE}^{H}+\mathbf{h}_{IE}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w} \\ (2^R-1)^{1/2} \end{bmatrix}^{H} & (\mathbf{h}_{AB}^{H}+\mathbf{h}_{IB}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w} \end{bmatrix} \succeq 0, \tag{4.14}$$

therefore, **P5** can be re-formulated as;

$$\begin{aligned} \textbf{P6:} \quad & \max_{\mathbf{w},\boldsymbol{\Theta},t} \quad t \\ & \text{s.t.} \quad \|\mathbf{w}\|^2 \leq P \\ & \mathbf{S} \succeq 0 \\ & \|\mathbf{u}^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}^{(n)}(i)[\mathbf{u}(i)-\mathbf{u}^{(n)}(i)] \geq t \\ & |\theta_n| = 1 \quad \forall n = 1,\ldots,M, \end{aligned} \tag{4.15}$$

where $\mathbf{S}$ is given by equation (4.14). However, **P6** is still non-convex due to the unit modulus constraints and cannot be solved directly. An alternating optimization algorithm similar to the one used in chapter three is adopted to solve problem **P6** and as a result it is divided into two sub-problems. The two sub-problems are given by;

$$\begin{aligned} \textbf{P6.1:} \quad & \max_{\mathbf{w},t} \quad t \\ & \text{s.t.} \quad \|\mathbf{w}\|^2 \leq P \\ & \mathbf{S} \succeq 0 \\ & \|\mathbf{u}^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}^{(n)}(i)[\mathbf{u}(i)-\mathbf{u}^{(n)}(i)] \geq t, \end{aligned} \tag{4.16}$$

and

$$\begin{aligned} \textbf{P6.2:} \quad & \max_{\boldsymbol{\Theta}} \quad t \\ & \text{s.t.} \quad |\theta_n| = 1 \quad \forall n = 1,\ldots,M. \end{aligned} \tag{4.17}$$

The sub-problem **P6.1** is convex and can be solved by IPM. However, sub-problem **P6.2** is still non-convex because of the unit-modulus constraints. The principle of

manifolds optimization proposed in [84] is used to tackle the unit-modulus constraints. Firstly, **P6.2** is reformulated as a minimization problem defined by;

$$\begin{aligned} \min_{\boldsymbol{\Theta}} \quad & -t \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M. \end{aligned} \tag{4.18}$$

Using the exact penalty method [31], the problem in equation (4.18) can be written as;

$$\begin{aligned} \min_{\boldsymbol{\Theta}} \quad & -t + \lambda \Bigg(\mathrm{Tr}\left(\mathbf{w}\mathbf{w}^{\mathrm{H}}\right) - P_T + 1 - 2^R + \frac{|(\mathbf{h}_{AB}^{\mathrm{H}} + \mathbf{h}_{IB}^{\mathrm{H}} \boldsymbol{\Theta} \mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_B}^2} \\ & - \frac{|(\mathbf{h}_{AE}^{\mathrm{H}} + \mathbf{h}_{IE}^{\mathrm{H}} \boldsymbol{\Theta} \mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_E}^2} + \|\mathbf{u}^{(n)}\|^2 + 2 \sum_{i=1}^{2} \mathbf{u}^{(n)}(i)[\mathbf{u}(i) - \mathbf{u}^{(n)}(i)] - t \Bigg) \\ \text{s.t.} \quad & |\theta_n| = 1 \quad \forall n = 1, \ldots, M. \end{aligned} \tag{4.19}$$

Through the utilization the manifold optimization algorithm equation (4.19) can be expressed as [12];

$$\begin{aligned} \min_{\mathcal{M}} \quad & -t + \lambda \Bigg(\mathrm{Tr}\left(\mathbf{w}\mathbf{w}^{\mathrm{H}}\right) - P_T + 1 - 2^R + \frac{|(\mathbf{h}_{AB}^{\mathrm{H}} + \mathbf{h}_{IB}^{\mathrm{H}} \boldsymbol{\Theta} \mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_B}^2} \\ & - \frac{|(\mathbf{h}_{AE}^{\mathrm{H}} + \mathbf{h}_{IE}^{\mathrm{H}} \boldsymbol{\Theta} \mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_E}^2} + \|\mathbf{u}^{(n)}\|^2 + 2 \sum_{i=1}^{2} \mathbf{u}^{(n)}(i)[\mathbf{u}(i) - \mathbf{u}^{(n)}(i)] - t \Bigg), \end{aligned} \tag{4.20}$$

where $\mathcal{M}$ is the manifold space which is defined as;

$$\mathcal{M} = \left\{ \boldsymbol{\theta} \in \mathbb{C}^M \; : \; |\theta_1| = \ldots = |\theta_M| = 1 \right\}. \tag{4.21}$$

The method of manifold optimization functions by performing a gradient decent algorithm in the space defined by the manifold. It is shown in [84] that the Euclidean space gradient descent algorithm is very similar to the Riemannian manifold. However, in the manifold optimization the Riemannian gradient is calculated as a search direction. The Riemannian gradient of equation (4.20) is a vector field on $\mathcal{M}$ such that at each $\boldsymbol{\theta} \in \mathcal{M}$, $\mathrm{grad}_{\boldsymbol{\theta}} f(\boldsymbol{\theta})$ is a tangent vector on $\mathcal{T}_{\boldsymbol{\theta}}\mathcal{M}$. This can be expressed as;

$$\mathcal{T}_{\boldsymbol{\theta}}\mathcal{M} = \left\{ \mathbf{u} \in \mathbb{C}^M \; : \; \Re\left\{ \boldsymbol{\theta}^{\mathrm{H}} \odot \mathbf{u} \right\} = 0 \right\}, \tag{4.22}$$

where $\mathbf{u}$ is the set of all unit vectors which lies on the tangent space. Let $f(\boldsymbol{\theta})$ represents the objective function of equation (4.20), i.e.,

$$f(\boldsymbol{\theta}) = -t + \lambda\Bigg(\mathrm{Tr}\left(\mathbf{w}\mathbf{w}^{\mathsf{H}}\right) - P_T + 1 - 2^R + \frac{|(\mathbf{h}_{AB}^{\mathsf{H}} + \mathbf{h}_{IB}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_B}^2} - \frac{|(\mathbf{h}_{AE}^{\mathsf{H}} + \mathbf{h}_{IE}^{\mathsf{H}}\boldsymbol{\Theta}\mathbf{H}_{AI})\mathbf{w}|^2}{\sigma_{n_E}^2} + \|\mathbf{u}^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}^{(n)}(i)[\mathbf{u}(i) - \mathbf{u}^{(n)}(i)] - t\Bigg), \tag{4.23}$$

then, the Euclidean gradient of equation (4.20) at $\boldsymbol{\theta}$ is given by;

$$\Delta_{\boldsymbol{\theta}} f(\boldsymbol{\theta}) = \begin{bmatrix} \partial_1 f(\boldsymbol{\theta}) \\ \vdots \\ \partial_M f(\boldsymbol{\theta}) \end{bmatrix}, \tag{4.24}$$

hence, the Riemannian gradient is calculated based on the Euclidean gradient and it is given by;

$$\mathrm{Grad}_{\boldsymbol{\theta}} f(\boldsymbol{\theta}) = \Delta_{\boldsymbol{\theta}} f(\boldsymbol{\theta}). \tag{4.25}$$

The update rule for the current value of $\boldsymbol{\theta}$ in the tangent space is given by Riemannian gradient as follows;

$$\boldsymbol{\theta} - \delta\Delta_{\boldsymbol{\theta}} f(\boldsymbol{\theta}), \tag{4.26}$$

where $\delta > 0$ is the step size. The ability to move in the direction of a tangent vector, while at the same time staying on the manifold is achieved by the retraction operation. A retraction R at $\boldsymbol{\theta}$, denoted by $R_{\boldsymbol{\theta}}$, maps $\mathcal{T}_{\boldsymbol{\theta}}\mathcal{M}$ to $\mathcal{M}$ and is defined as;

$$R_{\boldsymbol{\theta}} = \frac{\boldsymbol{\theta} - \delta\Delta_{\boldsymbol{\theta}} f(\boldsymbol{\theta})}{\|\boldsymbol{\theta} - \delta\Delta_{\boldsymbol{\theta}} f(\boldsymbol{\theta})\|}. \tag{4.27}$$

The algorithm for implementing the manifold optimization method is presented in algorithm 2.

4.2 Numerical results and simulations

In this section, the simulation results are presented to evaluate the performance of the energy harvesting scheme proposed. All simulations were performed using Python 3.8.5 with the aid of CVXPY 1.1.10. The simulation model, is assumed to have one transmitter which has four transmit antennas for beamforming, a legitimate receiver, an eavesdropper and an energy harvesting receiver, both with a

Algorithm 2 : Proposed algorithm for **P4**

Input: P_T, f_o, R, E, $\mathbf{h}_{AB}$, $\mathbf{h}_{AE}$, $\mathbf{h}_{IB}$, $\mathbf{h}_{IE}$, $\mathbf{h}_{AER}$, $\mathbf{h}_{AER}$, $\mathbf{h}_{IER}^{H}$, accuracy ϵ.

Initialization
Choose arbitrary initial $\tilde{\Theta}$.
Set $t = 0$ and $\Theta^{(t)} = \tilde{\Theta}$.
while $\|\theta^{(t+1)} - \theta^{(t)}\| \leq \epsilon$ **do**
    Calculate the Euclidean gradient using equation (4.24).
    Calculate the step size using Armijo step size,
    Calculate the update $\tilde{\theta} = \theta - \delta\Delta_\theta f(\theta)$
    if $\tilde{\theta} \notin \mathcal{M}$ **then**
        Update $\tilde{\theta}$ using the retraction operation in equation (4.27).
    end if
    Set $t = t + 1$
end while
Output: Return the optimal phase shifts, $\Theta^{\star} = \text{diag}(\theta^{\star})$
end

single receive antenna. The transmitter performs beamforming of the information signal to the legitimate receiver in the presence of the eavesdropper and the energy harvesting receiver which harvest some of the transmit power at the receiver. The objective of the scheme is to maximize the energy harvested by the energy harvesting receiver while satisfying the secrecy rate level required for the information transmitted at the legitimate receiver.

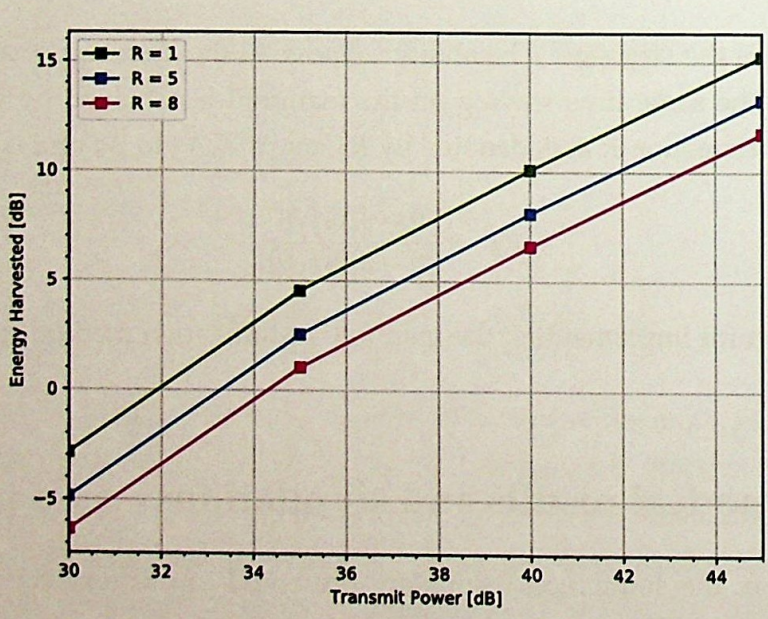


FIGURE 4.2: Transmit power vs Energy harvested with varying secrecy rate.

The simulation parameters for this model are similar to those stipulated in Table 3.1 with additional parameters, which include the secrecy rate R, the EHR path

loss and the transmit power. The secrecy rate values are set to 1 bit/s/Hz, 5 bit/s/Hz and 8 bit/s/Hz to evaluate the harvested energy with varying secrecy rate constraints, while the EHR path loss and the transmit power are varied from 15 m to 50 m and 15 dB to 50 dB, respectively. Figure 4.2, shows the impact of varying the secrecy rate of the system on the energy harvested by the EHRs. It is observed that the increase in the secrecy rate of the system results in the use of more transmit power requirements to achieve the desired secrecy rate level which implies that there will be low levels of the energy harvested by the EHRs.

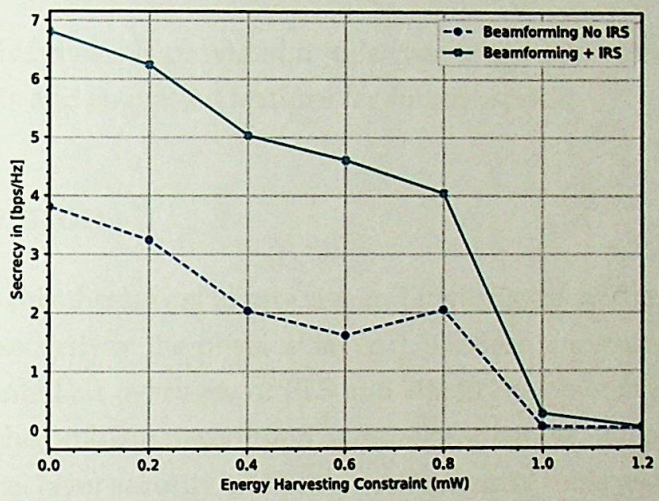


FIGURE 4.3: Energy harvested with varying secrecy rate.

In Figure 4.3, the secrecy rate versus the minimum energy harvesting constraint is demonstrated with the transmit power equal to 35 dBm and dAB = 20m, and the EHR placed also placed at 20m away from the transmitter. The secrecy rate for the two schemes is observed to decrease with increasing minimum energy harvesting requirement. It is also observed that for the same minimum energy requirement the proposed scheme which comprises of an IRS is able to achieve higher level of secrecy rate than the conventional RF network which has no IRS. The plot also shows that the secrecy rate level drops to almost zero when the minimum energy requirement becomes larger than 0.8mW.

Chapter 5

Summary and Future Directions

A summary of this thesis is provided in this chapter which includes the contributions of this thesis and suggested features for future work.

5.1 Conclusion

The main aim of this thesis was to propose and investigate mathematical optimization to improve security in the physical layer in wireless communication networks. Chapter 1, presented an overview of PLS and stated the objectives of this research work as well as the problem description and the motivation. It also covered a background of physical layer security and some mathematical tools used in PLS problem formulation and optimization.

In Chapter 2, the discussion of chapter was expanded with the focus in the conventional as well as new emerging technologies in PLS. The typical physical layer security optimizations problems for each technology were also presented.

In Chapter 3, a PLS scheme which uses a combination of information jamming and IRS was proposed. The optimal beamformers for both the information signal and jamming signal were designed and the work also provided an optimization of the phase shifts of the IRS to improve the level of secrecy rate of the system. The results analysis showed that the use of both jamming and IRS can improve the secrecy rate of the network. The simulation also showed that the secrecy rate can be improved by increasing the number of IRS elements at the cost of increasing the computation for the convergence of the optimization algorithm.

Chapter 4, considered the optimization problem of maximizing the energy which can be harvested by the energy receivers while satisfying the secrecy rate requirements in a wireless network. An alternating algorithm was proposed for solving for optimal beamforming vectors. Additionally, a gradient descent based on the manifold optimization technique was also proposed for designing optimal phase shifts of the IRS. The simulations showed that for the same minimum energy harvested

requirement the secrecy rate level is significantly improved with the introduction of the IRS than in the conventional schemes with no IRS.

5.2 Future work

In this work, the assumption made is that the initial CSI of the communication network is available at the transmitter in order to configure the phase shifts of the IRS. Future work will consider making practical measurements in the communication network with the IRS.

In order for the phase shifts of the IRS to be configured, channel estimation methods such as sending of pilot symbols from the transmitter to the receiver and, or machine learning based channel estimation methods can be used to learn the channel. This can used to adjust the IRS in real-time to measure different paths of the channel to find the phase shifts which maximizes the secrecy rate as well as the energy harvested by the energy harvesting receivers.

5.2.1 Machine learning-based channel estimation

The development of channel estimation techniques has been investigated in [85, 86, 87, 88]. From these investigations it's evident that tackling imperfect CSI in PLS is one of the problems still open for research. The conventional channel estimation methods based on channel modeling have been proved to be insufficient for providing accurate and timely CSI. There has been a recent surge in research directed towards the feasibility of tackling some of the various communication problems using ML [85]. Most of the research is devoted towards developing efficient and reliable algorithms for channel estimation in communication networks. The performance of the existing channel estimation algorithms can be augmented through the use of ML to achieve close-to-optimal algorithms with reduced complexity on the implementation [37]. ML has emerged as an effective tool for channel estimation in wireless communication systems, especially under some imperfect environments.

Bibliography

[1] International Telecommunication Union, "Statistics." [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2] S. Morgan, "Official Annual Cybercrime Report," Cybersecurity Ventures, Tech. Rep., 2019. [Online]. Available: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[3] M. Zorgui, "Wireless Physical Layer Security: On the Performance Limits of Secret-Key Agreement," Ph.D. dissertation, King Abdullah University of Science and Technology, apr 2015. [Online]. Available: https://repository.kaust.edu.sa/bitstream/handle/10754/552538/Zorgui-Thesis.pdf?sequence=1&isAllowed=y

[4] M. Campagna, A. L. Chen, Ö. Dagdelen, T. U. Darmstadt, J. Ding, J. K. Fernick, D. Hayford, T. Jennewein, N. Lütkenhaus, M. Mosca, D. Phil, B. Neill, M. Pecen, R. Perlner, J. M. Schanck, D. Stebila, N. Walenta, W. Whyte, Z. Zhang, S. Kaiser, and A. Petzold, "Quantum-Safe Cryptography and Security An introduction, benefits, enablers and challenges," European Telecommunications Standards Institute, Tech. Rep., 2015. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[5] H. Li and X. Wang, "Physical-Layer Security Enhancement in Wireless Communication Systems," Ph.D. dissertation, University of Western Ontario, Sep 2013. [Online]. Available: http://ir.lib.uwo.ca/etd

[6] A. Mukherjee, S. Ali, A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, 2014.

[7] Wyner A.D, "The Wire-Tap Channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[8] K. S. Ryland, T. C. Clancy, R. M. Buehrer, and C. B. Dietrich, "Software-Defined Radio Implementation of Two Physical Layer Security Techniques," Ph.D.

dissertation, Virginia Polytechnic Institute and State University in, Dec 2017. [Online]. Available: https://vtechworks.lib.vt.edu/bitstream/handle/10919/82055/Ryland_KS_T_2018.pdf

[9] L. Wang, *Physical Layer Security in Wireless Cooperative Networks*, ser. Wireless Networks. Ontario: Springer International Publishing, 2018.

[10] E. Björnson, Ö. Özdogan, and E. G. Larsson, "Reconfigurable Intelligent Surfaces: Three Myths and Two Critical Questions," *IEEE Communications Magazine*, vol. 58, no. 12, 2020.

[11] E. Björnson, H. Wymeersch, B. Matthiesen, P. Popovski, L. Sanguinetti, E. De Carvalho, . P. Popovski, and E. De Carvalho, "Reconfigurable Intelligent Surfaces: A Signal Processing Perspective With Wireless Applications," Feb 2021.

[12] Y. Xiu and Z. Zhang, "Secure Wireless Transmission for Intelligent Reflecting Surface-Aided Millimeter-Wave Systems," *IEEE Access*, vol. 8, pp. 192 924–192 935, 2020.

[13] Q.-U.-A. Nadeem, A. Kammoun, A. Chaaban, M. Debbah, and M.-S. Alouini, "Intelligent Reflecting Surface Assisted Wireless Communication: Modeling and Channel Estimation," King Abdullah University of Science and Technology, Tech. Rep., Dec 2019.

[14] P. Wang, J. Fang, X. Yuan, Z. Chen, and H. Li, "Intelligent Reflecting Surface-Assisted Millimeter Wave Communications: Joint Active and Passive Precoding Design," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14 960–14 973, 2020.

[15] R. Devi.T, "Importance of cryptography in network security," in *Proceedings - 2013 International Conference on Communication Systems and Network Technologies, CSNT 2013*, 2013, pp. 462–467.

[16] S. Vanstone, A. Menes, and P. Van Oorschot, *Handbook of Applied Cryptography*. CRC Press, 1996.

[17] Siddiqi, Yu, and Joung, "5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices," *Electronics*, vol. 8, no. 9, Sep 2019.

[18] L. Sun and Q. Du, "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions," *Entropy*, vol. 20, no. 10, Sep 2018.

[19] D. Wang, B. Bai, W. Zhao, and Z. Han, "A Survey of Optimization Approaches for Wireless Physical Layer Security," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1878–1911, Apr 2019.

[20] J. Li, "A Critical Review of Physical Layer Security in Wireless Networking," MPhil, University College London, 2015. [Online]. Available: https://discovery.ucl.ac.uk/id/eprint/1472248/1/MPhilThesis.pdf

[21] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.

[22] M. Bloch and J. Barros, *Physical-layer security : from information theory to security engineering*. Cambridge University Press, 2011.

[23] C. E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*, vol. 28, no. 4, 1949.

[24] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*, ser. SpringerBriefs in Computer Science. Singapore: Springer Singapore, 2016. [Online]. Available: http://link.springer.com/10.1007/978-981-10-1575-5

[25] A. Hyadi, Z. Rezki, and M. S. Alouini, "An Overview of Physical Layer Security in Wireless Communication Systems with CSIT Uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, 2016.

[26] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation," in *Proceedings - IEEE INFOCOM*, 2011, pp. 2165–2173.

[27] W. K. Harrison, D. Sarmento, J. P. Vilela, and M. Gomes, "Analysis of Short Blocklength Codes for Secrecy," *EURASIP Journal on Wireless Communications and Networking*, vol. 255, 2018.

[28] I. Csiszar and J. Kijrner, "Broadcast Channels with Confidential Messages," *IEEE TRANSACTIONS ON INFORMATION THEORY*, vol. 24, no. 3, pp. 339–348, 1978.

[29] J. L. Massey, R. E. Blahut, and C. Symposium on "Communications, *Communications and cryptography : two sides of one tapestry*. Kluwer Academic Publishers, 1994.

[30] R. Safavi-Naini and R. Canetti, *Advances in cryptology– CRYPTO 2012 : 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*. Springer, 2012.

[31] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge: Cambridge University Press, 2004.

[32] P.-H. Lin and E. Jorswieck, "Multiuser Channels with Statistical CSI at the Transmitter: Fading Channel Alignments and Stochastic Orders, an Overview," *Entropy*, vol. 19, no. 10, p. 515, Sep 2017.

[33] M. Migliore, D. Pinchera, M. Lucido, F. Schettino, and G. Panariello, "MIMO Channel-State Estimation in the Presence of Partial Data and/or Intermittent Measurements," *Electronics*, vol. 6, no. 2, p. 33, Apr 2017.

[34] X. S. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. CRC Press, 2016.

[35] "What Are MIMO, MRC, Beamforming, STBC, and Spatial Multiplexing? - WLAN Troubleshooting Guide - Huawei." [Online]. Available: https://support.huawei.com/enterprise/es/doc/EDOC1000060368/d9adbe5a/

[36] M. Mohaisen, Y. Wang, and . K. Chang, "Multiple Antenna Technologies," 2013. [Online]. Available: https://arxiv.org/pdf/0909.3342.pdf

[37] E. Björnson, L. Sanguinetti, H. Wymeersch, J. Hoydis, and T. L. Marzetta, "Massive MIMO is a Reality-What is Next? Five Promising Research Directions for Antenna Arrays," *Elsevier*, vol. 94, pp. 3–20, 2019.

[38] D. Kapetanovi, G. Zheng, and F. Rusek, "Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[39] E. Yaacoub and M. Al-Husseini, "Achieving physical layer security with massive MIMO beamforming," in *2017 11th European Conference on Antennas and Propagation, EUCAP 2017*. IEEE, May 2017, pp. 1753–1757.

[40] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO-OFDM systems by beamforming and artificial noise generation," *Physical Communication*, vol. 4, no. 4, pp. 313–321, Dec 2011.

[41] Z. Sheng, H. D. Tuan, Z. Sheng, H. D. Tuan, T. Q. Duong, and H. Vincent Poor, "Beamforming Optimization for Physical Layer Security in MISO Wireless Networks," *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3710–3723, 2018.

[42] R. Mohammadkhani, "Lecture 13: MIMO Transceivers Part II," University of Kurdistan, Tech. Rep., 2017. [Online]. Available: http://eng.uok.ac.ir/mohammadkhani

[43] A. Gershman, N. Sidiropoulos, S. Shahbazpanahi, M. Bengtsson, and B. Ottersten, "Convex optimization-based beamforming," in *IEEE Signal Processing Magazine*, vol. 27, no. 3. IEEE, 2010, pp. 62–75.

[44] E. Bjornson, M. Bengtsson, and B. Ottersten, "Optimal multiuser transmit beamforming: A difficult problem with a simple solution structure [Lecture Notes]," *IEEE Signal Processing Magazine*, vol. 31, no. 4, pp. 142–148, 2014.

[45] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 3. IEEE, 2005, pp. 1906–1910.

[46] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-aoise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, Mar 2011.

[47] H. Zhang and L. Duan, "Going beyond Secrecy Rate via Information Jamming," in *2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings*. IEEE, 2018.

[48] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun 2008.

[49] W. Liu, M. Li, X. Tian, Z. Wang, and Q. Liu, "Transmit Filter and Artificial Noise Design for Secure MIMO-OFDM Systems," 2017. [Online]. Available: https://arxiv.org/pdf/1704.08007.pdf

[50] Y.-S. SHIU, S. Y. CHANG, H.-C. Wu, S. HUANG, and H.-H. CHEN, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[51] H. Reboredo, V. Prabhu, M. R. Rodrigues, and J. Xavier, "Filter design with secrecy constraints: The multiple-input multiple-output Gaussian wiretap channel with zero forcing receive filters," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2011, pp. 3440–3443.

[52] S. M. Alamouti, "A Simple Transmit Diversity Technique for Wireless Communications," *IEEE JOURNAL ON SELECT AREAS IN COMMUNICATIONS*, vol. 16, no. 8, 1998.

[53] B. Sujatha, "Space-Time Block Coding (STBC) for Wireless Networks," *International Journal of Distributed and Parallel Systems (IJDPS*, vol. 3, no. 4, 2012.

[54] T. Allen, J. Cheng, and N. Al-Dhahir, "Secure space-time block coding without transmitter CSI," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 573–576, Dec 2014.

[55] P. O. Akuon and H. Xu, "Secure Signal and Space Alamouti Scheme," *SAIEE Africa Research Journal*, vol. 107, no. 4, pp. 237–244, Dec 2018.

[56] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *IEEE Workshop on Statistical Signal Processing Proceedings*. IEEE, 2009, pp. 417–420.

[57] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, Feb 2018.

[58] Y. Zhong, F. Zhou, Y. Wang, X. Deng, and N. Al-Dhahir, "Cooperative Jamming-Aided Secure Wireless Powered Communication Networks: A Game Theoretical Formulation," *IEEE Communications Letters*, vol. 24, no. 5, pp. 1081–1085, May 2020.

[59] F. Zhou, S. Member, Z. Li, S. Member, J. Cheng, Q. Li, J. Si, F. Zhou, Z. Li, J. Si, J. Cheng, and Q. Li, "Robust AN-Aided Beamforming and Power Splitting Design for Secure MISO Cognitive Radio With SWIPT," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2450–2464, 2016.

[60] E. Boshkovska, D. Wing, K. Ng, N. Zlatanov, A. Koelpin, and R. Schober, "Robust Resource Allocation for MIMO Wireless Powered Communication Networks Based on a Non-linear EH Model," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 1984–1999, 2017.

[61] C. Huang, S. Hu, G. C. Alexandropoulos, S. Member, A. Zappone, C. Yuen, R. Zhang, M. Di Renzo, and M. Debbah, "Holographic MIMO Surfaces for 6G Wireless Networks: Opportunities, Challenges, and Trends," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 118–125, 2019.

[62] X. Lu, E. Hossain, T. Shafique, S. Feng, H. Jiang, and D. Niyato, "Intelligent Reflecting Surface (IRS)-Enabled Covert Communications in Wireless Networks," *IEEE Network*, vol. 34, no. 5, pp. 148–155, 2019.

[63] J. Zhang, E. Björnson, M. Matthaiou, D. Wing Kwan Ng, H. Yang, and D. J. Love, "Prospective Multiple Antenna Technologies for Beyond 5G," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, 2020.

[64] E. J. Black, "Holographic Beam Forming and MIMO," Pivotal Commware, Tech. Rep., 2017. [Online]. Available: https://pivotalcommware.com/wp-content/uploads/2017/11/Holographic-Beamforming-and-MIMO-1.pdf

[65] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible Light Communication, Networking, and Sensing: A Survey, Potential and Challenges," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 17, no. 4, 2015.

[66] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. Assi, and H. Haas, "Physical Layer Security for Visible Light Communication Systems: A Survey," *IEEE Communications Surveys & Tutorials*, pp. 1–1, Apr 2020.

[67] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical wireless communications: System and channel modelling with MATLAB®*. CRC Press, Jan 2017.

[68] J. Hamamreh, "Physical Layer Security Against Eavesdropping in The Internet of Drones (IoD) Based Communication Systems," Jun 2019. [Online]. Available: https://figshare.com/articles/preprint/Physical_Layer_Security_Against_Eavesdropping_in_The_Internet_of_Drones_IoD_Based_Communication_Systems/8362385/1

[69] H. M. Wang, X. Zhang, and J. C. Jiang, "UAV-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 32–39, 2019.

[70] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, Jan 2020.

[71] W. Lu, K. An, and T. Liang, "Robust Beamforming Design for Sum Secrecy Rate Maximization in Multibeam Satellite Systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1568–1572, Jun 2019.

[72] J. Lei, Z. Han, M. A. Vázquez-Castro, and A. Hjørungnes, "Secure Satellite Communication Systems Design with Individual Secrecy Rate Constraints,"

IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 661–671, 2011.

[73] A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1862–1874, Sep 2015.

[74] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy Rate Maximization for Intelligent Reflecting Surface Assisted Multi-Antenna Communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, Sep 2019.

[75] W. Zhao and S. Wang, "Resource Allocation for Device-to-Device Communication Underlaying Cellular Networks: An Alternating Optimization Method," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1398–1401, Aug 2015.

[76] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*. IEEE, Dec 2019.

[77] X. Guan, Q. Wu, and R. Zhang, "Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not?" *IEEE Wireless Communications Letters*, pp. 1–1, Jan 2020.

[78] W. Dinkelbach, "On Nonlinear Fractional Programming," *Management Science*, vol. 13, no. 7, pp. 492–498, Mar 1967.

[79] J. Antoneta, "A parametric study for solving nonlinear fractional problems," *The European Digital Mathematics Library*, vol. 11, no. 2, pp. 87–92, 2003.

[80] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy Rate Maximization for Intelligent Reflecting Surface Assisted Multi-Antenna Communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, Sep 2019.

[81] E. Bjornson, O. Ozdogan, and E. G. Larsson, "Intelligent Reflecting Surface Versus Decode-and-Forward: How Large Surfaces are Needed to Beat Relaying?" *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 244–248, Feb 2020.

[82] Z. Chu, Z. Zhu, M. Johnston, and S. Y. Le Goff, "Simultaneous wireless information power transfer for MISO secrecy channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6913–6925, Sep 2016.

[83] S. Abeywickrama, R. Zhang, and C. Yuen, "Intelligent Reflecting Surface: Practical Phase Shift Model and Beamforming Optimization," in *IEEE International Conference on Communications*, vol. 2020-June. IEEE, Jun 2020.

[84] P.-A. Absil, R. Mahony, and R. Sepulchre, *Optimization Algorithms on Matrix Manifolds*. New Jersey: Princeton University Press, 2008.

[85] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. C. Chen, and L. Hanzo, "Machine Learning Paradigms for Next-Generation Wireless Networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98–105, apr 2017.

[86] M. Soltani, V. Pourahmadi, A. Mirzaei, and H. Sheikhzadeh, "Deep Learning-Based Channel Estimation," *IEEE Communications Letters*, vol. 23, no. 4, pp. 652–655, Apr 2019.

[87] H. Huang, S. Guo, G. Gui, Z. Yang, J. Zhang, H. Sari, and H. Adachi, "Deep Learning for Physical-Layer 5G Wireless Techniques: Opportunities, Challenges and Solutions," *IEEE Wireless Communications*, vol. 27, no. 1, pp. 214–222, 2019.

[88] B. Mashhadi and D. Gündüz, "Deep Learning for Massive MIMO Channel State Acquisition and Feedback," *Journal of the Indian Institute of Science*, vol. 100, pp. 369–382, 2020.