PhD-FSTC-2016-14
The Faculty of Sciences, Technology and Communication

DISSERTATION

Presented on 22/04/2016 in Luxembourg

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG
EN INFORMATIQUE

by

Ashkan KALANTARI
Born in Yazd, Iran

SIGNAL PROCESSING FOR PHYSICAL LAYER SECURITY WITH APPLICATION IN SATELLITE COMMUNICATIONS

Dissertation defense committee

Dr Björn Ottersten, dissertation supervisor

Professor and Director of SnT, University of Luxembourg

Dr Symeon Chatzinotas

Research Scientist, SnT, University of Luxembourg

Dr Francesco Viti, Chairman

Professor, University of Luxembourg

Dr Luc Vandendorpe

Professor, Université Catholique de Louvain, Belgium

Dr Jens Krause

Senior Manager, Satellite Telecommunications Systems at SES, Luxembourg

Abstract

Wireless broadcast allows widespread and easy information transfer. However, it may expose the information to unintended receivers, which could include eavesdroppers. As a solution, cryptography at the higher network levels has been used to encrypt and protect data. Cryptography relies on the fact that the computational power of the adversary is not enough to break the encryption. However, due to increasing computing power, the adversary power also increases. To further strengthen the security and complement the encryption, the concept of physical layer security has been introduced and surged an enormous amount of research. Widely speaking, the research in physical layer security can be divided into two directions: the information-theoretic and signal processing paradigms. This thesis starts with an overview of the physical layer security literature and continues with the contributions which are divided into the two following parts.

In the first part, we investigate the information-theoretic secrecy rate. In the first scenario, we study the confidentiality of a bidirectional satellite network consisting of two mobile users who exchange two messages via a multibeam satellite using the XOR network coding protocol. We maximize the sum secrecy rate by designing the optimal beamforming vector along with optimizing the return and forward link time allocation. In the second scenario, we study the effect of interference on the secrecy rate. We investigate the secrecy rate in a two-user interference network where one of the users, namely user 1, requires to establish a confidential connection. User 1 wants to prevent an unintended user of the network to decode its transmission. User 1 has to adjust its transmission power such that its secrecy rate is maximized while the quality of service at the destination of the other user, user 2, is satisfied. We obtain closed-form solutions for optimal joint power control. In the third scenario, we study secrecy rate over power ratio, namely "secrecy energy efficiency". We design the optimal beamformer for a multiple-input single-output system with and without considering the minimum required secrecy rate at the destination.

In the second part, we follow the signal processing paradigm to improve the security. We employ the directional modulation concept to enhance the security of a multi-user multiple-input multiple-output communication system in the presence of a multi-antenna eavesdropper. Enhancing the security is accomplished by increasing the symbol error rate at the eavesdropper without the eavesdropper's CSI. We show that when the eavesdropper has less antennas than the users, regardless of the received signal SNR, it cannot recover any useful information; in addition, it has to go through extra noise enhancing processes to estimate the symbols when it has more antennas than the users. Finally, we summarize the conclusions and discuss the promising research directions in the physical layer security.

Acknowledgements

Above all, I am grateful to have family members who supported me morally and economically during all of my studies and I would like to give them my sincerer thank for their great support. I wish to be able to always live with them and wish a happy and healthy life for them.

I would like to thank Professor Björn Ottersten, Dr Symeon Chatzinotas, Dr Sina Maleki, and Dr Gan Zheng for their supervision during my PhD research in the Interdisciplinary Centre for Security, Reliability and Trust (SnT) between the years 2012-2016. In addition, I would like to thank Professor Mojtaba Soltanalian, Professor Zhu Han, and Dr Zhen Gao for their collaboration. I would like to also thank the "*Fonds National de la Recherche*" of Luxembourg for fonding my PhD studies.

In addition, my special thanks go to my office mates, my colleagues, and the administrative staff at the University of Luxembourg and SnT who provided a great and friendly and cheerful environment for both enjoying life and carrying out research.

Ashkan Kalantari
Luxembourg, April 2016

Contents

List of Figures

List of Tables

Abbreviations

ACM	**A**daptive **C**oding and **M**odulation
AES	**A**dvanced **E**ncryption **S**tandard
AF	**A**mplify and **F**orward
AWGN	**A**dditive **W**hite **G**aussian **N**oise
BER	**B**it **E**rror **R**ate
CSI	**C**hannel **S**tate **I**nformation
DF	**D**ecode and **F**orward
ETA	**E**qual **T**ime **A**llocation
FL	**F**orward **L**ink
GW	**G**ate**W**ay
ISM	**I**ndustrial, **S**cientific and **M**edical
LDPC	**L**ow **D**ensity **P**arity **C**heck
LoS	**L**ine **o**f **S**ight
MAC	**M**ultiple **A**ccess **C**hannel
MIMO	**M**ultiple-**I**nput **M**ultiple-**O**utput
MIMOME	**M**ultiple-**I**nput **M**ultiple-**O**utput **M**ultiple-antenna **E**avesdropper
MIMOSE	**M**ultiple-**I**nput **M**ultiple-**O**utput **S**ingle-antenna **E**avesdropper
MISO	**M**ultiple-**I**nput **S**ingle-**O**utput
MISOME	**M**ultiple-**I**nput **S**ingle-**O**utput **M**ultiple-antenna **E**avesdropper
MISOSE	**M**ultiple-**I**nput **S**ingle-**O**utput **S**ingle-antenna **E**avesdropper
SIMOME	**S**ingle-**I**nput **M**ultiple-**O**utput **M**ultiple-antenna **E**avesdropper
M-PSK	**M**-ary **P**hase **S**hift **K**eying
MSE	**M**ean **S**quare **E**rror
OFDM	**O**rthogonal **F**requency **D**ivision **M**ultiple **A**ccess
OTA	**O**ptimal **T**ime **A**llocation

QoS	**Q**uality **o**f **S**ervice
Q-PSK	**Q**uadrature **P**hase **S**hift **K**eying
RF	**R**adio **F**requency
RL	**R**eturn **L**ink
SDP	**S**emi**d**efinite **P**rogramming
SER	**S**ymbol **E**rror **R**ate
SIC	**S**uccessive **I**nterference **C**ancellation
SIMO	**S**ingle-**I**nput **M**ulti-**O**utput
SINR	**S**ignal to **N**oise plus **I**nterference **R**atio
SISO	**S**ingle-**I**nput **S**ingle-**O**utput
SNR	**S**ignal to **N**oise **R**atio
SR	**S**ecrecy **R**ate
SATCOM	**S**atellite **C**ommunications
SVD	**S**ingular **V**alue **D**ecomposition
ZF	**Z**ero **F**orcing

Notations

$\mathbf{W}$, $\mathbf{w}$	Matrix, column vector
$(\cdot)^T$	Transpose
$(\cdot)^*$	Conjugate
$(\cdot)^H$	Hermitian
$(\cdot)^\dagger$	Moore-Penrose pseudo inverse
$\|\cdot\|$	Frobenius norm
$\|\cdot\|$	Absolute value
$\mathrm{Re}\,(\cdot)$	Real part of a complex number
$\mathrm{Im}\,(\cdot)$	Imaginary part of a complex number
$\arg(\cdot)$	Angle of a complex number
$\mathbf{I}_{M\times N}$	An M by N identity matrix
$\mathbf{A} \succeq \mathbf{0}$	The Hermitian matrix $\mathbf{A}$ is positive semidefinite
$\mathbf{a} \circ \mathbf{b}$	Element-wise Hadamard product
$\mathrm{diag}(\mathbf{a})$	Diagonal matrix where the elements of vector $\mathbf{a}$ are its diagonal entries
$\mathbf{a}_+$	A vector where negative elements of the vector $\mathbf{a}$ are replaced by zero
$\lambda_{max}(\cdot)$	Maximum eigenvalue
$sup(\cdot)$	Supremum
$inf(\cdot)$	Infimum
$A \underset{(2)}{\overset{(1)}{\gtrless}} 0$	$A > 0$ when the conditions of Case 1 hold and $A < 0$ when the conditions of Case 2 hold
$\mathcal{CN}(\mathbf{m}, \mathbf{K})$	Complex Gaussian distribution with mean vector $\mathbf{m}$ and covariance matrix $\mathbf{K}$
$\lambda_{\max}(\mathbf{A}, \mathbf{B})$	Maximum eigenvalue of the matrix pencil $(\mathbf{A}, \mathbf{B})$

I would like to dedicate this thesis to my parents who have always support me in my life.

Chapter 1

Introduction

1.1 Motivation and Scope

Wireless communications allows information flow through broadcasting; however, unintended receivers may also receive these information, with eavesdroppers amongst them. One way to enhance the security is by applying encryption on the information before transmission. Currently, security in communications is achieved at upper layers by means of encryption such as the Advanced Encryption Standard (AES) [1, 2]. Nevertheless, cryptography security is based on the assumption of limited computational capability of the malicious nodes, and thus there exists the risk that a malicious node can successfully break an encryption and get access to sensitive information [3]. As time goes on, the increasing computational power of the computers increases the probability of encryption interception.

In addition to the upper layer encryption techniques, recently, there has been significant interest in securing wireless communications at the physical layer using an information-theoretic approach. As a pioneer in information-theoretic physical layer security, Shannon mentioned that in order to have a perfectly secure communication, the length of the key has to be at least equal to the length of the message [4]. Later, Wyner introduced the concept of "*secrecy rate*" for discrete memoryless channels in his seminal paper [5] which initiated a research direction for keyless secure communications. Wyner noted that if the eavesdropper has a noisier channel than the legitimate receiver, we can achieve a perfectly secure communication with encoding and decoding at the transmitter and legitimate receiver, respectively. The main advantage of these approaches is that the malicious nodes cannot get access to the protected information regardless of their computational capabilities. The secrecy rate defines the bound for a perfectly secure transmission and coding is being developed to achieve this bound. However, this area

is still in its infancy, and the research effort at the moment is inclined in implementing practical codes [6–8]. Wyner's idea was later extended to broadcast channels with confidential messages [9], Gaussian [10], and fading channels [11–13]. We provide a detailed overview of the information-theoretic research in Chapter 2.

The first part of this thesis focuses on the information-theoretic secrecy rate in both satellite and terrestrial scenarios. In Chapter 3, we maximize the secrecy rate in a bidirectional satellite communication network to facilitate fast and secure satellite communications (SATCOM). SATCOM is becoming more and more integrated into communication networks to complement the current terrestrial communication systems [14]. Satellite services have to support increasing demands for data transfer. Traditionally, orthogonal resources either in frequency or time domain should be used to avoid interference between users. Bidirectional satellites where users exchange messages simultaneously can be one of the solutions to save the precious wireless resources. To realize bidirectional satellite communications, we use network coding as an efficient protocol to exchange information between two mobile satellite users. The basic principle is that the received information from users are combined at the gateway (GW), and then the mixed signal is simultaneously broadcast to the users using the same frequency. Because each user can subtract its own message, it can easily decode the message from the other user. Network coding can greatly improve the system throughput. However, the security it provides is largely unknown in SATCOM and is not yet compared with the conventional scheme, which does not use network coding. Due to the broadcast nature and immense area coverage, satellite communications systems, e.g., in military and commercial applications, are vulnerable to security attacks such as eavesdropping. We leverage the physical layer security approach to address the confidentiality issue in bidirectional SATCOM using the principle of network coding.

In Chapter 4, the effect of interference on the secrecy rate was studied in wiretap interference channels. Broadcasting information over the same frequency band in wireless networks leads to interference among users. Even in the systems where the spatial dimension is used to concentrate the signal towards the intended destination, the destination may receive interfering signals from other transmitters operating in the same frequency band. Also, due to the expansion and deployment of wireless services, the spectrum is becoming scarce [15]. As one possible solution, devices can share the same spectrum which results in interference and degradation of the signal quality. For instance, IEEE standards such as WiFi, Zigbee and Bluetooth share the same frequency band named the industrial, scientific and medical (ISM) band and they may interference with each other [16]. Furthermore, the wireless medium leaves the information vulnerable to unintended users who can potentially decode the message which was meant for other users. By intelligently tuning the system parameters using physical layer security

techniques, we can prevent the wiretappers from getting access to the information. Consequently, a specific rate can be perfectly secured for the users to transmit their data, so that the wiretapper is not able to decode the message. Potentially, the interference can improve the secrecy rate by introducing extra interference at the eavesdropper. To find a relation between the secrecy rate and energy efficiency, we study the secrecy energy efficiency in Chapter 5. Energy-efficiency, high data rates and secure communications are essential requirements of the future wireless networks. We consider a multiple-input single-output (MISO) and a single-input single-output (SISO) scenario while a single-antenna unintended receiver, which is part of the network, is listening. The secrecy rate over the power ratio, named "*secrecy energy efficiency*", is maximized with and without considering the minimum required secrecy spectral efficiency at the destination. For comparison, we derive the optimal beamformer when the zero-forcing (ZF) technique is used to null the signal at the eavesdropper with considering the minimum required secrecy spectral efficiency. Furthermore, we study the trade-off between secrecy energy efficiency and secrecy spectral efficiency.

The second part of this thesis focuses on enhancing the security through the signal processing paradigm. In Chapter 6, we employ the directional modulation concept [17, 18] to enhance the security for finite-alphabet signaling in a multi-user MIMO channel without relaying on the information-theoretic secrecy rate. In the directional modulation, the antenna weights are designed such that the desired data constellation is received only in a specific direction, and is distorted in other directions. Although the Gaussian distribution is optimal when the information-theoretic secrecy rate is the target, the Gaussian distribution assumption for the signals is rarely satisfied in practical communication systems. There are digital communication systems which use finite-alphabet signals such as M-PSK modulation which usually have a discrete uniform distribution [19]. Due to the non-Gaussian distribution, finite-alphabet signals are not optimal in terms of the developed secrecy rates in [5, 9–13]. Furthermore, although the physical layer security concept introduced in [5] provides perfect secrecy with the proper coding scheme, it also reduces the message transmission rate to the legitimate receiver. Primarily, the secrecy rate requires perfect or statistical knowledge of the eavesdropper's channel state information (CSI) [5, 20–22], however, it may not be possible to acquire the perfect or statistical CSI of a passive eavesdropper in practice. In addition, in the secrecy rate approach, the transmission rate has to be lower than the achievable rate, which may conflict with the increasing rate demands in wireless communications. In Chapter 6, we study and design the optimal precoder for a directional modulation transmitter in order to enhance the security in a quasi-static fading MIMO channel where a multi-antenna eavesdropper is present. Here, enhancing the security means increasing the SER at the eavesdropper. In directional modulation, users' channels and symbols meant for the

users are used to design the precoder. The precoder is designed to induce the symbols on the receiver antennas rather than generating the symbols at the transmitter and sending them, which is the case in the conventional transmit precoding [23, 24].

1.2 Thesis Organization

We mention the system model details of each chapter in this section. These explanations are followed by our contributions. Chapters 3, 4, and 5 span the first part of the thesis which is focused on the information-theoretic secrecy rate. The second part of the thesis focuses on enhancing the wireless security via signal processing paradigm. This approach is described in Chapter 6. Finally, Chapter 7 summarizes the main results of the thesis and proposes future possible research directions.

1.2.1 Chapter 2: Physical Layer Security

In this chapter, we mention the state of the art in physical layer security by dividing them into two major groups. The first group consists of the works which study the security based on the information-theoretic secrecy rate. We mention the information-theoretic secrecy rate literature in detail and classify them into direct link and cooperative communications subcategories. For the direct link communications, we divide the works into broadcast wiretap channels, broadcast channels with confidential messages, multiple-access channels, interference channels, and the works which jointly study the secrecy rate and energy efficiency. The cooperative works are divided into works which study the secrecy rate in networks with untrusted relays and the works which consider external eavesdropper.

The second group includes the works which improve the security through the signal processing paradigm by increasing the symbol/bit error rate or signal to noise ratio at the eavesdropper. We divide the literature of this group into two categories. The first category enhances the security using conventional precoding, which only uses the CSI of the legitimate link in the precoder design. The second category uses both the legitimate CSI and the symbols to design the precoder.

1.2.2 Chapter 3: Security in Bidirectional Multibeam Satellites

We study network coding based bidirectional SATCOM in this chapter. We consider a scenario where two mobile users exchange data via a transparent multibeam satellite in the presence of two eavesdroppers. There is an eavesdropper present for each user

who overhears the bidirectional communications. The users employ omnidirectional antennas and the communication is prone to eavesdropping in both the return link[1] (RL) and forward link[2] (FL). In the RL, two users send signals using two orthogonal frequency channels; the signals collected by the satellite are passed to the GW, where they are decoded, XOR-ed and then the produced stream is re-encoded. This combined stream is multiplied by the beamforming vector which contains the designed weight of each feed. The beamforming weights are designed to maximize the users' sum secrecy rate. Consequently, each element of the resultant vector is transmitted to the satellite using the feeder link. Each element which includes both the feed weight and the data signal is applied to the corresponding feed to adjust the beams for broadcasting to both users simultaneously in the FL. The content of this chapter is published in [22].

1.2.2.1 Contributions

The contributions of this chapter are as follows:

1. XOR network coding is introduced into SATCOM to enable both efficient and secure bidirectional data exchange.
2. The end-to-end sum secrecy rate is first derived, and then maximized by designing the optimal beamforming vector and the RL and FL time allocation. The optimization problem regarding the beamforming vector is solved using semi-definite programming (SDP) along with 1-D search.
3. Comprehensive simulation results are provided to demonstrate the advantage of the bidirectional scheme over the conventional scheme using realistic SATCOM parameters.

1.2.3 Chapter 4: Power Control in Wiretap Interference Channels

In this chapter, the secrecy rate is investigated in a two-user wireless interference network. Apart from the two users, one of the idle users (unintended user) in this network is a potential eavesdropper. Both nodes transmit in a way so that the secrecy rate is maximized for the first user (user 1), and the second user (user 2) maintains the quality of service (QoS) at its intended destination. Only user 1 needs to establish a secure connection and to keep its data secure. For example, in a network with ISM band users, user 1 and user 2 can be WiFi and ZigBee transmitters. The ZigBee can be used to send

[1]The return link denotes the data transmission from the user to the gateway via the satellite.
[2]The forward link denotes the data transmission from the gateway to the user via the satellite.

measurement data, which is one of its applications, so its data may not be necessarily important to the potential eavesdropper who is interested in WiFi messages. We study the effect of interference from user 2 on the secrecy rate of user 1 in two scenarios, namely altruistic and egoistic scenarios. In the altruistic scenario, we jointly optimize the transmission powers of both users in order to maximize the secrecy rate of user 1, while maintaining the QoS at user 2's destination equal or above a specific threshold. The incentives for user 2 to cooperate are twofold: 1) when positive secrecy rate cannot be granted for user 1, it can enjoy an interference-free transmission, 2) user 1 adjusts its transmission power to maintain the QoS of user 2's destination equal or above the threshold. In the egoistic scenario, the users' powers are still jointly optimized. However, user 2 is selfish and only tries to maintain the minimum QoS at the corresponding destination. The content of this chapter is published in [21].

1.2.3.1 Contributions

The contributions of this chapter are as follows:

1. It is shown that by appropriate control of user 1's power, we can make sure that the eavesdropper cannot decode the signal of user 2, and thus cannot employ successive interference cancellation (SIC).
2. It is shown that the transmitted power from user 2 has a crucial role in achieving a positive secrecy rate for user 1. According to the channel conditions, we define the proper power transmission for user 2 to maintain a positive secrecy rate for user 1
3. Closed-form expressions are developed to implement joint optimal power control for both users in both altruistic and egoistic scenarios.
4. Finally, a new metric called "secrecy energy efficiency" is defined, which is the secrecy rate over the consumed power ratio. Using the new metric, it is shown that the interference channel can outperform the single-user channel for specific values of QoS requirements.

1.2.4 Chapter 5: Secrecy Energy Efficiency Optimization for MISO and SISO Communication Networks

In this chapter, we consider a multiple-input single-output (MISO) and a single-input single-output (SISO) scenario while a single-antenna unintended receiver, which is part of the network, is listening. The secrecy rate over the power ratio, named "*secrecy energy*

efficiency" and denoted by ζ, is maximized with and without considering the minimum required secrecy spectral efficiency, denoted by η_0, at the destination. For comparison, we derive the optimal beamformer when zero-forcing (ZF) technique is used to null the signal at the eavesdropper with considering the minimum required secrecy spectral efficiency. Note that the ZF can only be used for the MISO scenario. Furthermore, the trade-off between ζ and secrecy spectral efficiency, denoted by η, is studied. The content of this chapter is published in [25].

1.2.4.1 Contributions

The contributions of this chapter are as follows:

1. A convex problem is formulated to derive the exact beamformer to maximize the secrecy energy efficiency in a MISO wiretap channel.
2. An iterative algorithm is proposed for optimal power allocation in SISO wiretap channel to maximize the secrecy energy efficiency.
3. The trade-off between the secrecy rate and energy efficiency is analyzed to figure out the optimal operating point.

1.2.5 Chapter 6: Security Enhancing Directional Modulation via Symbol-Level Precoding

In this chapter, the optimal precoder is designed for a directional modulation transmitter to enhance the security in a quasi-static fading MIMO channel where a multi-antenna eavesdropper is present. Here, enhancing the security means increasing the SER at the eavesdropper. In directional modulation, users' channels and symbols meant for the users are used to design the precoder. The precoder is designed to induce the symbols on the receiver antennas rather than generating the symbols at the transmitter and sending them, which is the case in the conventional transmit precoding [23, 24]. In other words, in the directional modulation, the modulation happens in the radio frequency (RF) level while the arrays' emitted signals pass through the wireless channel. This way, we simultaneously communicate multiple interference-free symbols to multiple users. Also, the precoder is designed such that the receivers antennas can directly recover the symbols without CSI and equalization. Therefore, assuming the eavesdropper has a different channel compared to the users, it receives scrambled symbols. In fact, the channels between the transmitter and users act as secret keys [26] in the directional modulation. Furthermore, since the precoder depends on the symbols, the eavesdropper

cannot calculate it. In contrast to the information theoretic secrecy rate paradigm, the directional modulation enhances the security by considering more practical assumptions. Particularly, directional modulation does not require the eavesdropper's CSI to enhance the security, furthermore, it does not reduce the transmission rate and signals are allowed to follow a non-Gaussian distribution. A part of the content of this chapter is published in [27], and all of the content is submitted to [28].

1.2.5.1 Contributions

The contributions of this chapter are as follows:

1. The optimal symbol-level precoder is designed for a security enhancing directional modulation transmitter in a MIMO fading channel to communicate with arbitrary number of users and symbol streams. In addition, we derive the necessary condition for the existence of the precoder. The directional modulation literature mostly includes LoS analysis with one or limited number of users, and multi-user works do not perform security enhancing optimization.

2. It is shown that when the eavesdropper has less antennas than the transmitter, regardless of the SNR level, it cannot extract useful information from the received signal and when it has more antennas than the transmitter, it has to estimate the symbols by extra processes which enhance the noise. We minimize the transmission power for the former case and maximize the SER at the eavesdropper for the latter case to prevent successful decoding at the eavesdropper. This is done while keeping the SNR of users' received signals above a predefined threshold and thus the users' rate demands are satisfied. The directional modulation literature do not analyze the abilities of a multi-antenna eavesdropper and rely on the fact that it receives scrambled symbols

3. It is shown that in conventional precoding, the eavesdropper needs to have more antennas than the receiver to estimate the symbols since the eavesdropper can calculate the precoder. In our design, the eavesdropper has to have more antennas than the transmitter since the precoder depends on both the channels and symbols. The transmitter, e.g., a base station, probably has more antennas than the receiver, hence, it is more likely to preserve the security in directional modulation, specially in a massive MIMO system.

4. The power and SNR minimization precoder design problems are simplified into a linearly-constrained quadratic programming problem. For faster design, we introduce new auxiliary variable to transform the constraint into equality and propose

two different algorithms to solve the design problems. In the first algorithm, we use a penalty method to get an unconstrained problem and solve it by proposing using an iterative algorithm. Also, we prove that the algorithm converges to the optimal point. In the second one, we use the constraint to get a non-negative least squares design problem. For the latter, there are already fast techniques to solve the problem.

1.3 Publications

The author has published his PhD research in the *IEEE* journals and international conferences. The publications are listed below with the acronyms "J" and "C" defining the journal and conference publications, respectively.

1.3.1 Journals

- J1: A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels", *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810–3823, Jul. 2015.
- J2: A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications", *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1862–1874, Sep. 2015.
- J3: A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Security enhancing directional modulation via symbol-level precoding", submitted to *IEEE Journal of Selected Topics in Signal Processing*.

1.3.2 Conferences

- C1: Sina Maleki, Ashkan Kalantari, Symeon Chatzinotas, Björn Ottersten, "Power Allocation for Energy-Constrained Cognitive Radios in the Presence of an Eavesdropper," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Florence, Italy, May 2014.
- C2: A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Feasibility of positive secrecy rate in wiretap interference channels", in *IEEE Global Conf. on Signal and Inf. Proces. (GlobalSIP)*, Atlanta, GA, Dec. 2014, pp. 1190–1194.

- C3: A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Secrecy energy efficiency optimization for MISO and SISO communication networks", in *IEEE Int. Workshop on Signal Proces. Advances in Wireless Commun. (SPAWC)*, Stockholm, Sweden, Jun. 2015, pp. 21–25.

- C4: A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secure M-PSK communication via directional modulation", in *IEEE Int. Conf. on Acoustics, Speech and Signal Proces. (ICASSP)*, Shanghai, China, Mar. 2016 (to appear).

- C5: A. Kalantari, S. Maleki, S. Chatzinotas, and B. Ottersten, "Frequency of arrival based interference localization using a single satellite", submitted to 8^{th} *Advanced Satellite Multimedia Systems Conference,* 14^{th} *Signal Processing for Space Communications Workshop*, Palma de Mollorca, Spain, Sep. 2016.

To keep the consistency of the thesis, the following publications are not included in the thesis:

- Sina Maleki, Ashkan Kalantari, Symeon Chatzinotas, Björn Ottersten, "Power Allocation for Energy-Constrained Cognitive Radios in the Presence of an Eavesdropper," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Florence, Italy, May 2014.

- Ashkan Kalantari, Sina Maleki, Gan Zheng, Symeon Chatzinotas, Björn Ottersten, "Feasibility of Positive Secrecy Rate in Wiretap Interference Channels," *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Atlanta, GA, Dec. 2014.

- A. Kalantari, S. Maleki, S. Chatzinotas, and B. Ottersten, "Frequency of arrival based interference localization using a single satellite", submitted to 8^{th} *Advanced Satellite Multimedia Systems Conference,* 14^{th} *Signal Processing for Space Communications Workshop*, Palma de Mollorca, Spain, Sep. 2016.

Chapter 2

Physical Layer Security

In this chapter, we review the physical layer security literature which relates to this thesis. Broadly speaking, we divide the related literature into two parts. For the first part, we mention the works which use the information-theoretic secrecy rate as a metric for establishing the security. In this part, we firstly elaborate on the secrecy rate concept and then classify the related literature into direct link and cooperative wireless networks. To go further into the literature depth, we discuss and classify each group into subgroups. For the second part, we review the works which rely on the signal processing paradigm to improve the security of wireless communication systems. A summary of the literature review of this chapter is given in Table 2.1. For a detailed review of the physical layer security state of the art, we refer the interested readers to [29]. Here, we use the word "unintended receiver" to refer to the eavesdropper.

2.1 Information-Theoretic Secrecy Rate Paradigm for Security

In his fundamental work [4], Shannon mentions the conditions for having perfect secrecy using a secret key. He shows that in order to have a perfectly secure transmission, the length of the secret key needs to be at least equal to the length of the message. Later, Wyner introduced the secrecy rate for the keyless secure transmission paradigm in his seminal paper [5]. Wyner considered a discrete memoryless channels and showed that it is possible to design a pair of encoder-decoder to establish a perfectly secure transmission when the eavesdropper has noisier channel than the legitimate receiver. The introduction of the keyless information-theoretic secrecy rate by Wyner opened up many research areas. In the following, we overview the works built upon the information-theoretic secrecy rate. Apart from the secrecy rate, another metric to measure the

TABLE 2.1: Classification of physical layer security literature

Category	Related research
Secrecy in wiretap broadcast channels: single-antenna nodes	[5, 10–12, 30–34]
Secrecy in wiretap broadcast channels: multiple-antenna nodes	[35–68]
Secrecy in broadcast channels with confidential messages	[9, 69–87]
Secrecy in multiple-access channels	[20, 70, 88–93]
Secrecy in interference channels	[21, 94–112]
Energy efficiency and secrecy rate	[25, 113–118]
Cooperative communication and secrecy rate: untrusted relay	[119–126]
Cooperative communication with external eavesdropper	[22, 127–150, 150, 151]
Signal processing paradigm for security: conventional precoding	[152–157]
Signal processing paradigm for security: directional modulation via symbol-level precoding	[17, 18, 23, 27, 28, 158–176]

physical layer security is the secrecy outage probability, which measures the probability that the secrecy rate goes below a predefined threshold rate.

2.1.1 Secrecy Rate in Non-cooperative Links

Since the introduction of the information-theoretic secrecy rate by Wyner for discrete memoryless channels, this concept has been extended to different types of direct link wireless networks. In this part, we categorize these works based on the wireless channel type and mention the related literature.

2.1.1.1 Secrecy in wiretap broadcast channels

In wiretap broadcast channels, the aim is to keep the message secret from external unintended receivers or eavesdroppers. A generalized wiretap broadcast channel is shown in Fig. 2.1. Here, we categorize the literature into single-antenna and multiple-antenna works.

- **Wiretap broadcast channel with single-antenna nodes:** Inspired by Wyner, [30] shows that for a noiseless legitimate channel and a binary symmetric channel, it is possible to establish a secure transmission at the rate of the legitimate link. To further push the limits, [10] extends Wyner's secrecy rate to Gaussian wiretap

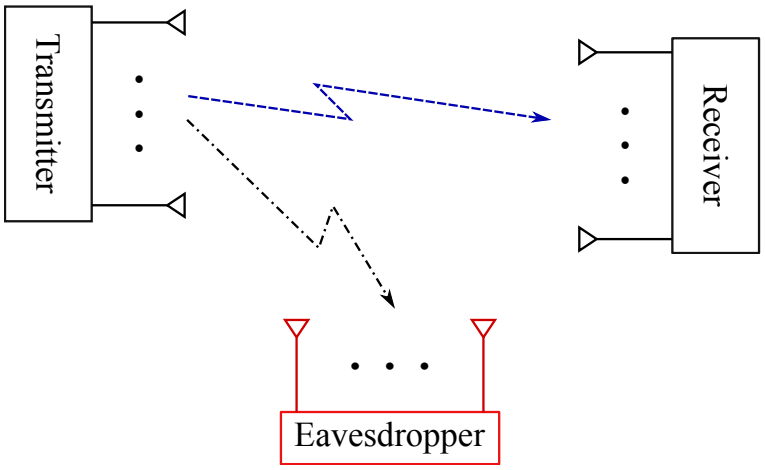


FIGURE 2.1: Broadcast MIMO communications over wiretap fading channels.

channels. The authors of [31] extend [10] by considering a Gaussian interference known at the encoder and propose the coding strategy to achieve the perfect secrecy rate. The authors of [12] analyze the secrecy rate when the main channel is additive white Gaussian noise (AWGN) and the wiretap channel is Rayleigh fading. They show that under artificial noise injection, positive secrecy rate is achievable even when the average channel gain of the legitimate receiver is worse than the eavesdropper. To analyze the secrecy rate in more general channels, the authors of [32] derive a closed-form expression for the secrecy capacity and an upper bound for the secrecy outage probability of α-μ fading wiretap channels. By taking into account more practical assumptions, the works in [11, 33] study the secrecy rate by assuming the absence of the eavesdropper's CSI. The work of [11] studies strategies to achieve the secrecy rate over fading channels by assuming both the availability and the absence of the eavesdropper's CSI at the transmitter. Assuming long coherence intervals for the eavesdropper's channel, the authors propose a on/off power allocation which gets close to optimal performance for asymptotically infinity SNR. Compound[1] wireless channels for the legitimate receiver and the eavesdropper are studied in [33]. It is shown that without the eavesdropper CSI knowledge at the transmitter and assuming limited states for it, it is possible to guarantee perfect secrecy. The work of [34] determines the sensing threshold, sensing time, and the transmission power to maximize the secrecy rate of a cognitive radio using the statistical CSI of the eavesdropper.

- **Wiretap broadcast channel with multiple-antenna nodes:** The work of [35]

[1]The compound channel models transmission over a channel that may take a number of states and reliable communication needs to be guaranteed regardless of which state occurs.

initiated the extension of Wyner's secrecy rate to multiple-antenna wiretap channel. In [35], space-time codes are used to initiate secure transmission in a multiple-input multiple-output multiple-antenna eavesdropper (MIMOME) Rayleigh fading channel. The secrecy rate for single-input multiple-output multiple-antenna eavesdropper (SIMOME) slow fading channel is derived in [36] and it is shown that reception diversity improves the secrecy rate. The authors of [37] derive the optimal transmit covariance matrix for a multiple-input single-output single-antenna eavesdropper (MISOSE) channel where they consider AWGN legitimate channel and Rayleigh fading and AWGN channels for the eavesdropper. The effect of beamforming on the secrecy rate is investigated in [38]. The authors determine the secrecy capacity of Gaussian MIMO wiretap channel with two antenna legitimate nodes and a single-antenna eavesdropper and show that applying beamforming on Gaussian signaling is the optimal strategy. The work of [39] derives the secrecy rate in terms of generalized eigenvalues for a multiple-input multiple-output single-antenna eavesdropper (MIMOSE) Rayleigh fading channels. The secrecy rate is extended to multi-user scheduling scenario in [47]. The authors derive the achievable secrecy sum-rate in a multi-user scenario where each user is wiretapped by multiple eavesdroppers. In a new paradigm, [49] calculates the optimal jamming covariance matrix for a full-duplex receiver in a SIMOME wiretap channel where the receiver can both receive the signal and jamm the eavesdropper at the same time. The advantage in [49] compared to cooperative jamming scenarios is the "*self-protection*" ability at the receiver, which is that the destination can remove the jamming from the received signal since it knowns the jamming pattern.

The secrecy rate of MIMOME network is studied in [40–42, 44, 45, 48]. To further study the MIMOME channel, [41] derives the exact secrecy capacity of a MIMOME AWGN wiretap channel. The analyzes of [39] are extended to include a multiple-antenna eavesdropper in [40] and the authors derive the optimal covariance matrix for Gaussian distributed inputs. The work of [42] characterizes the secrecy rate of a MIMOME wiretap channel by considering a more general transmit covariance matrix compared to [40, 41]. The achievable secrecy rate is studied while jointly minimizing the power received by the eavesdropper and maximizing the power received by the desired terminal. The precoding at the transmitter to maximize the secrecy rate in a MIMOME channel is studied for space shift keying transmission in [45]. Not all the research in the physical layer security is built from scratch, the cognitive communications has shown to be useful in the information-theoretic secrecy rate research. For example, a new relationship between the wiretap channel and the cognitive radio channel is set up in [48]. The authors derive the optimal covariance matrix of Gaussian input signal which maximizes the secrecy rate and

calculate the achievable rates in MIMOSE and MIMOME wiretap channels. The work of [44] designs the transmit precoding in a MIMOME channel.

The works of [43, 46] study the secrecy outage probability. To perform secrecy rate analysis on other channel types, [43] studies the secrecy outage probability over MISOME generalized K-fading channels. The frequency domain analysis is employed in [46] to derive a unified communication-theoretic approach in order to analyze the probability of nonzero secrecy capacity, the secrecy outage probability, and the secrecy capacity over MIMO fading channels.

The security of the systems with finite-alphabet inputs is considered in [50, 51]. The authors in [50] study the information-theoretic secrecy rate for a multiple-antenna transmitter, receiver, and eavesdropper when finite-alphabet signal is used. The authors assume that the eavesdropper CSI is available at the transmitter. An external helper generating interference in the form of fine-alphabet signal is considered in [51]. Information-theoretic secrecy rate expressions are derived by approximating the beneficial interference distribution as sum of Gaussian distributions and assuming the availability of the eavesdropper's CSI.

As a way to exploit the diversity and reduce the amount of radio frequency (RF) chains, antenna selection at the transmitter/receiver can be employed. The physical layer security research also incorporates antenna selection to reduce the transceiver complexity while improving the security. The work of [52] derives the secrecy outage probability in a MISOME channel using transmitter antenna selection. As an extension of [52], the authors of [53] derive a closed-form expression for the secrecy outage probability when transmit antenna selection is used in a MIMOME wiretap channel to maximize the SNR at the receiver. In [54], the authors perform transmit antenna section to improve the secrecy outage probability in MIMO wiretap channel with multiple multiple-antenna eavesdroppers. The work of [55] considers optimal and suboptimal antenna selection at the transmitter in a MIMOME wiretap channel. The authors maximize the secrecy rate and derive the secrecy diversity order.

The usage of artificial noise to enhance the secrecy rate is studied in [56–62]. The work of [56] considers a MIMOME channel where it proposes using external helpers to jamm the eavesdropper. This work derives the noise covariance matrix to improve the secrecy rate. The authors of [57] calculate the optimum power allocation strategy between the transmitted information and artificial noise to guarantee a specific secrecy outage probability. The authors of [58] extend [57] by defining a "*Protected Zone*" around the transmitter and study it by statistical modeling. The work of [59] analyzes the secrecy rate in a slow flat fading MISO wiretap channel where multiple eavesdroppers are present. The authors jointly

optimize the transmit and artificial noise covariance matrices. The work of [60] considers a MISOSE wiretap channel in fast fading channels. The optimal transmit and artificial noise matrices to maximize the secrecy rate are designed using perfect CSI of the legitimate link and the statistics CSI of the eavesdropper. The power splitting between the data and artificial noise transmission is proposed in [61] to prevent the energy collector nodes to intercept the message. Secrecy rate is extended to green wireless communications in [62], where the authors consider a two-phase communication procedure. In the first phase, the source sends power to the jammer through wireless channel. Then, the source communicates with the destination in the second phase while the jammer creates interference at the eavesdropper. The authors maximize the average rate and minimize the secrecy outage probability.

To move toward practical scenarios and considering system errors, the physical layer security research society has tried to study the effect of imperfect and partial CSI on the secrecy rate. The authors of [63] minimize the secrecy outage probability in a MISOSE flat fading wiretap channel where perfect CSI of the legitimate and partial CSI of the wiretap channel is considered. To further improve the secrecy, artificial noise is injected in the null direction of the legitimate receiver. The authors of [64] follow a robust design approach along with Taylor series approximation to minimize the power and secrecy rate maximization over MIMOME wiretap channel using imperfect global CSI. Robust design of transmit and receiver filters over a MIMOME wiretap channel is studied in [65]. Considering the imperfect CSIs of the legitimate link and the eavesdropper, the authors minimize the mean square error (MSE) at the legitimate receiver, whereas keeping the MSE at the eavesdropper above a threshold. The secrecy rate of a MISO transceiver in the presence of multiple single-antenna eavesdroppers is studied in [66]. The secrecy rate constrained to secrecy rate outage probability and power is maximized by designing a robust beamformer using the imperfect CSI of the eavesdroppers. The secrecy rate in a MIMOME channel is analyzed in [67] using the distribution of the eavesdropper's channel at the transmitter and the effect of the channel estimate feedback. Stochastic geometry is used in [68] to minimize the secrecy outage probability in a MISO wiretap channel in the presence of multiple randomly located single-antenna eavesdroppers. The authors maximize the throughput constrained to outage of the legitimate link by designing the transmit beamformer with the eavesdropper's channel state distribution while the quantization error is considered.

2.1.1.2 Secrecy in broadcast channels with confidential messages

In broadcast channels with confidential messages, the goal is to keep the message of each user secret from the other users, and a common message is usually transmitted to the users. As a pioneer, the work of [9] considers a two-user network where a secret message is transmitted to the first user and a common message to both of the users. The secret and common messages are transmitted using different rates over discrete memoryless channels. Works [69, 70] study a similar scenario as in [9] for Gaussian and fading channels, respectively. The authors of [70] minimize the secrecy outage probability using optimal power allocations and derive the secrecy capacity region. Broadcast channels with one-sided interference are studied in [71, 72]. In [71], an easier way is proposed to derive an outer bound for secrecy capacity region of a two-user one-sided interference channel where the message of one user needs to be kept confidential while message of other user is assumed to be alway transmitted securely. In [72], a two-user network with one-sided interference where each destination is a potential eavesdropper for the other one is studied. Using game theory, it is concluded that depending on the objective of each pair, the equilibrium can include or exclude the self-jamming strategy. The work of [69] characterizes the capacity region of the broadcast channel with confidential messages by decomposing the legitimate receiver into two virtual receivers. The authors of [73] derive the inner and outer bounds of the secrecy capacity region for a memoryless interference MIMO broadcast channels where artificial noise is used to enhance the secrecy of the private message. To further generalize the scenario, [74, 75] consider transmitting two private messages to the users. The authors of [74] derive the secrecy rate region for a two-user MIMO network where the transmitter wants to transmit private message to each of the receivers. The work of [75] derives the secrecy capacity for a two-user MIMO channel where each user should receive a private message and both users need to receiver a common message. Later, [76] extended [73] to the case where both users transmit artificial noise along with data. Outer bounds on sum secrecy rate of a two-user Gaussian interference channel are studied in [77] where message confidentiality is important for users. Secrecy capacity region for a two-user MIMO Gaussian interference channel is investigated in [78] where each receiver is a potential eavesdropper. The authors show that larger secrecy rate region can be achieved when one or both destinations are considered as eavesdropper. The work in [177] analyzes a two-user interference channel with one-sided noisy feedback where a common message is sent to users and a confidential message to both users. The authors derive the rate-equivocation region when the message of one user needs to be kept secret. As a generalization, [79–81] consider sending a private message to each of the users in a multi-user network. A multi-user interference channel where only one user as a potential eavesdropper receives interference is considered in [81]. The sum secrecy rate is derived

using nested lattice codes. The work of [79] derives he optimal precoder to maximize the sum secrecy rate in a large multi-user MIMO channel. The authors of [82] derive closed-form optimal beamformers for two MIMO transmitters where each of them wants to communicate a private message with its own receiver. The work of [83] studies the secrecy rate competition. The authors study the rank of the optimal input covariance matrix that achieves the secrecy capacity in a Gaussian interference channel with two MISO links where each transmitter tries to maximize its own secrecy rate compared to the secrecy rate of the other transmitter. The authors of [84] analyze a two-user MISO Gaussian interference channel where each destination is a potential eavesdropper. Game theory is used to tackle the scenario where each user tries to maximize the difference between its secrecy rate and the secrecy rate of the other user. Beamformers under full and limited channel CSI are designed at each transmitter to achieve this goal. A two-user MISO interference channel is considered in [85] where each users may decode the message of the other user. The beamforming is performed to jointly optimize the secrecy rates of the users. The broadcast channels with confidential messages is extended to multi-user case in [86]. The authors consider a communication network comprised of multiple-antenna base stations and single-antenna users. The total transmit power is minimized while the signal-to-interference plus noise ratio and equivocation rate for each user is satisfied. The extension of broadcast channel with confidential messages to finite-alphabet input is considered in [87]. The authors maximize the secrecy rate in a two-user channel where the transmitter sends a common message to both users and private message to each of them.

2.1.1.3 Secrecy in wiretap multiple-access channels

As a natural extension, the Wyner wiretap channel was also extended to multiple access (MAC) channel with external eavesdroppers, which can be seen in Fig. 2.2. As the first work, [88] considers a MAC channel with an external eavesdropper where the authors derive the outer bounds for the secrecy rate region and the power allocation to maximize the secrecy sum rate. The upper bound for the secrecy sum rate of the MAC channel is derived in [89]. In another scenario, [70] considers a two-user MAC channel where each user is a potential eavesdropper for other users. The authors derive the rate-equivocation pair for each user. The secrecy analysis of MAC channel is extended to two-way communications in [20]. The authors consider two-way MAC channel where an eavesdropper wiretaps the communication between two users. The work of [90] derives the secrecy capacity region for a two-user MAC channel where both users transmit a common message to the destination while one of them has a private message to transmit. As a new approach, [91] uses uplink training to hide the CSI from eavesdroppers and

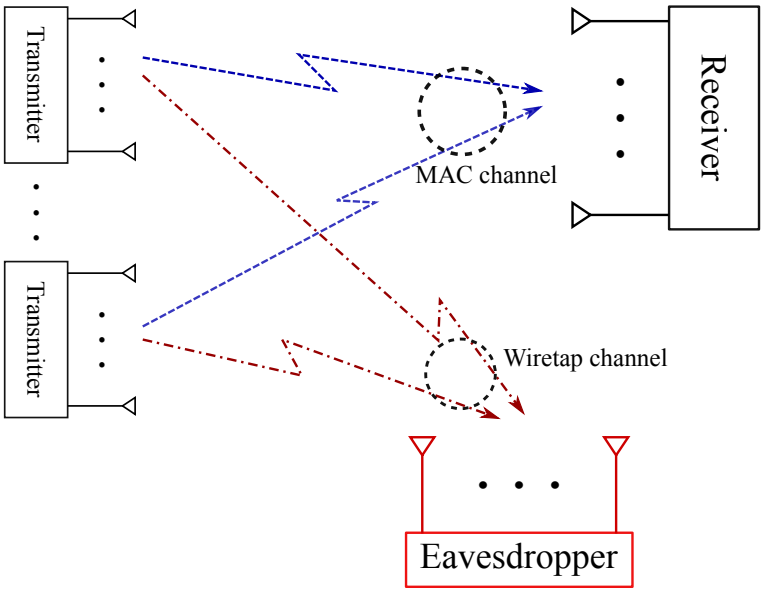


FIGURE 2.2: A MIMO multiple access channel over wiretap fading channels.

designs codes to create high decoding error at the eavesdropper. The security analysis of a two-user MAC channel is extended to multiple-antenna nodes in [92] where an external eavesdropper wiretaps the channel. The work of [93] characterizes the secrecy rate region for discrete and Gaussian memoryless channels for a two-user MAC channel in the presence of an external eavesdropper where individual secrecy rate constraints are considered.

2.1.1.4 Secrecy in wiretap interference channels

Wireless transmission in the same frequency band causes interference at the receivers. Physical layer security researchers have tried to study the interference effect on the secrecy rate and calculate the secrecy rate in the presence of interference. Secrecy rate in a two-user interference channel is studied by [94–97]. The authors of [94] investigate the secrecy rate in a two-user interference channel with an external eavesdropper. They show that the structured transmission results in a better secrecy rate compared to randomly generated Gaussian codebooks. The authors of [95] study the secrecy capacity region for a two-user interference channel in the presence of an external eavesdropper. The users jointly design randomized codebooks and inject noise along with data transmission to improve the secrecy rate. The work of [96] considers a user who gets helping interference in order to increase its confidentiality against an eavesdropper. The achievable secrecy rate for both discrete memoryless and Gaussian channels is derived. The possibility of secure transmission in a multi-user interference channel using interference alignment and secrecy precoding is investigated in [98]. A two-user symmetric linear deterministic interference channel is investigated in [99]. The achievable secrecy rate is

investigated when interference cancellation, cooperation, time sharing, and transmission of random bits are used. It is shown that sharing random bits achieves a better secrecy rate compared to sharing data bits. The authors in [100] consider a wireless network comprised of users, eavesdroppers and interfering nodes. It is shown that interference can improve secrecy rate. A transceiver pair is studied in [101] where they try to increase the secrecy rate using an external interferer when a passive eavesdropper is present. The authors of [102] consider a user and an eavesdropper where known interference which only degrades the decoding ability at the eavesdropper is used to enhance the secrecy capacity. The secrecy capacity and secrecy outage capacity when closest interfering node and multiple interfering nodes are separately employed to prevent eavesdropping is studied in [103]. It is demonstrated that multiple interferes method is superior to the closet interfering method. The exact secure degrees of freedom for different types of Gaussian wiretap channels are discussed in [104] where cooperative jamming from helpers is used. A scenario in [105] considers two sources where each of them communicates with its own destination and each of them is wiretapped by a specific eavesdropper. The authors investigate the effect of interference caused by sources transmission on the secrecy rate.

As an application of interference channels, the effect of interference on the secrecy rate is also investigated in cognitive radio systems. In cognitive radios, secondary user transmits in the primary user's operating frequency band when it is not in use. Stochastic geometry is used in [106] to analyze physical layer secrecy in a multiple node cognitive radio network where an eavesdropper is present. The secrecy outage probability and the secrecy rate of the primary user is derived while secondary user produces interference. The equivocation-rate for a cognitive interference network is analyzed in [107] where the primary receiver is a potential eavesdropper and should not decode the secondary message. The authors of [108] maximize the secrecy rate for a multiple-antenna secondary user in the presence of an external eavesdropper while considering the QoS at the primary receiver. In [109], a cognitive radio network with single-antenna nodes is considered. The secondary user causes interference to both primary destination and eavesdropper. The primary user is interested in maintaining secrecy rate while the secondary is aiming to increase its transmission rate. The achievable pair rate for both users is derived and then the interaction is modeled as a game. Similar problems to maximize the secrecy rate through beamforming design in cognitive radio are studied in [110–112].

Our contributions in [21, 97] fall into the categories of secrecy in interference channel. We consider a two-user interference channel with an external eavesdropper in [21] where one user tries to maximize its secrecy rate while the other user is interested in keeping the QoS at its destination. We derive closed-form expressions for the optimal power control of the users to maximize the secrecy rate and preserving the QoS while preventing

the SIC at the eavesdropper. Depending on the channel conditions, bounds on the transmission power of the interfering user are derived such that a positive secrecy rate is sustained for the other user.

2.1.1.5 Secrecy rate and energy efficiency

While security is a concern, power consumption is also another important issue in wireless communications since some wireless devices rely on limited battery power. Recently, researchers have shown interest to jointly optimize the secrecy rate and the power consumption. In [113], sum secrecy outage probability over the consumed power is studied where multiple layer optimization is used. The optimal power allocation is carried out for each user on a specific subcarrier in a scalar manner in a MISO channel. The work of [114] uses switched beamforming to maximize the secrecy outage probability over the consumed power ratio, while delay and power constraints are considered. The optimal beamformer a wiretap channel with multiple-antenna nodes is designed in [115] using first-order Taylor series expansion and Hadamard inequality are used to maximize secrecy rate over power ratio. The work of [116] maximizes the secrecy energy efficiency in a cooperative network with multiple decode-and-forward (DF) relays. The secrecy energy efficiency is extended to cooperative networks in [117, 118]. Power consumption for a fixed secrecy rate is minimized in [117] for an AF rely network. The work of [118] maximizes the secrecy outage probability over the consumed power subject to power limit for a large scale AF relay network.

Our contribution in [25] falls into the secrecy rate and energy efficiency category. The work of [25] derives the exact solution for the optimal beamformer which maximizes the secrecy rate over power, denoted by "*secrecy energy efficiency*", for a MISO channel wiretapped by a single-antenna eavesdropper. In addition, we propose an efficient iterative algorithm to calculate the closed-form expression for maximizing the secrecy energy efficiency in a SISO channel where a single-antenna eavesdropper is present.

2.1.2 Cooperative Communication and Secrecy Rate

Relay-aided cooperative communications helps improving the transmission coverage without increasing the transmission power. Keeping a sufficiently low transmission power prevents interference in other adjacent wireless networks. Furthermore, reducing the interference improves the overall capacity [178]. While cooperative networks improve the communications, similar to direct link communications, the security is sill an issue since the information can be wiretapped by unintended receivers and the encryption can be compromised. A typical wiretap relay channel in the presence of a helper is shown in

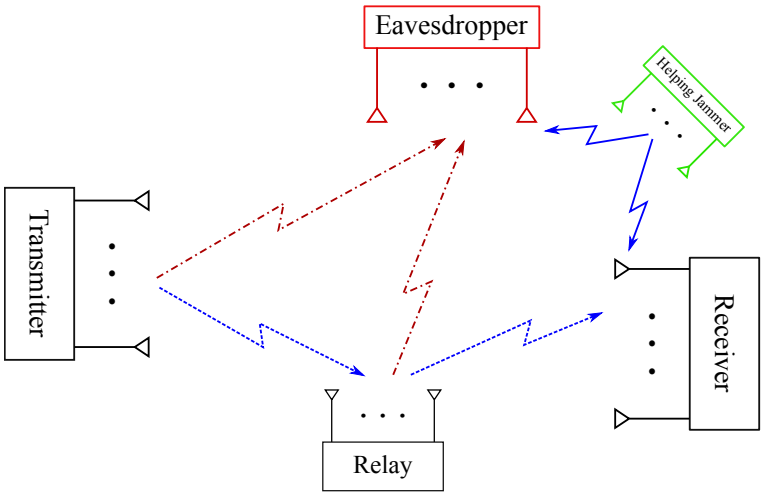


FIGURE 2.3: A cooperative relay link over wiretap fading channels in the presence of a helper.

Fig. 2.3. In this part, we review the physical layer security literature in the cooperative communications networks. We divide the literature into two parts. In the first part, we review the works where the unintended node is the relay, which is regarded as the "*untrusted relay*" in the literature. In the second part, we mention the research which consider scenarios where external eavesdroppers wiretap the cooperative network.

2.1.2.1 Untrusted relay

Analyzing the security for untrusted relays in a cooperative network is a more practical scenario. This is due to the fact that the relay node is part of the network and is used to complete the transmission process; hence, its perfect of partial CSI is probably available at the transmitter. As one of the first works, [119] studies the security performance of a cooperative network by considering different malicious behaviors from the DF relays and proposing a trust-assisted communication protocol. The Wyner's secrecy rate is developed to the untrusted relay channel in [120] where achievable secrecy rate is derived for the relay channel. The source and untrusted AF relay beamformers are jointly designed in [121] to maximize the secrecy rate. The work of [121] is extended to a two-way network with an untrusted AF relay in [122] where the beamformer of the two sources and the relay are jointly designed to maximize the secrecy rate. The secrecy outage probability for a single-antenna and multiple-antenna AF untrusted relay is studied in [123]. Furthermore, as the first work, the authors investigate the effect of antenna selection at the relay on the secrecy outage probability. The work of [124] introduces the destination-based jamming to handle single or multiple untrusted AF relays. To evaluate the security, the authors derive the achievable secrecy rates. In a novel approach, [125] applies beamforming at the transmitter so that the untrusted relay

only receives the real valued part of the signal, whereas the receiver gets both the real valued and imaginary valued parts of the signal. To perform a global optimization over the cooperative network, [126] designs the precoder for the source, relay and destination. The authors consider a cooperative network with multiple-antenna nodes where the relay is a potential eavesdropper. The precoding is applied at the source and relay for message transmission and at the destination to jamm the relay such that the secrecy rate is maximized.

2.1.2.2 Cooperative communication with external eavesdropper

As a extension to secrecy in broadcast wiretap channels, Wyner's secrecy rate can be analyzed in cooperative communications where the source/relay is being intercepted by one or multiple eavesdroppers. Wyner's secrecy rate concept was first extended to cooperative networks with external eavesdropper in [127]. The achievable rate-equivocation region of the network is characterized when the relay transmits artificial noise. The average secrecy outage probability is optimized in [128] for a cellular network with multiple-antenna base station, relays, and eavesdropper where multiple single-antenna users communicate with the base station. The work of [129] considers a cooperative network consisting of multiple relays which are wiretapped by multiple eavesdroppers. The relay weights are designed under total and individual power constraints to maximize the secrecy rate or null the information at the eavesdroppers. Upper and lower bounds for the secrecy capacity of a diamond wiretap channel is derived in [130] where a source communicates with a destination through two relays in the presence of an eavesdropper. As an application of full-duplex radios, [131] considers single-antenna source, destinations, and eavesdroppers where they communicate through a multiple-antenna full-duplex relay. The beamforming at the relay is designed to cancel self-interference and satisfying different SINRs at the destination and eavesdroppers. Works [132, 133] incorporate large arrays in cooperative networks and study the secrecy rate. A large array MIMO relay is studied in [132] where it is powered by the signal from the source and can freely change its location to improve the secrecy. The secrecy outage probability is derived for both AF and DF relaying protocols. A cooperative network with single-antenna source and destination along with a large array relay is studied in [133]. The authors study the secrecy of AF and DF protocols at the relay in the presence of a single-antenna eavesdropper. To move toward more practical scenarios, [134, 135] study the robust design when the eavesdroppers' imperfect CSI is available. The work of [134] follows robust design to calculate the relay weights using the eavesdropper's imperfect CSI for a multiple relay cooperative network with single-antenna nodes in the presence of a single-antenna eavesdropper. The work of [135] proposes a robust beamforming

design for a multiple-antenna relay using eavesdropper's imperfect CSI to maximize the secrecy rate. The secrecy analysis when the satellite works as a relay is studied in [22]. In this work, two users exchange messages using XOR network coding protocol while each of them is being wiretapped by a specific eavesdropper. The authors derive the satellite antenna weights to maximize the sun secrecy rate.

The effect of jamming and artificial noise in the secrecy of cooperative communications is studied in [136–142]. The maximum number of eavesdropper for maintaining a secure communication in a multiple relay cooperative network is studied in [136] where a set of relay nodes are selected to transmit artificial noise in order to improve the secrecy rate. The work of [137] studies the achievable secrecy rate in the cases where the relay performs jamming or artificial noise generation from a known codebook to improve the secrecy rate. A similar scenario as [127] is considered in [138] where the relay improves the secrecy by jamming the eavesdropper. The authors derive the optimal power allocation for the source and relay to maximize the secrecy rate. Cooperative jamming along with interference aliment are used in [139] to improve the secrecy rate in a cooperative network with multiple antenna nodes where the communication is wiretapped by a multiple-antenna eavesdropper. Multiple scenarios where multiple relays perform AF, DF, or jamming are considered in [179]. The authors derive the relay weights to maximize the secrecy rate in the presence of one or more single-antenna eavesdroppers. The work of [140] designs linear precoding and proposes using inactive DF relays of the cooperative network as jammers to improve the secrecy where a multiple-antenna eavesdropper can intercept the transmission in both hops. Similar as in [140], [141] considers cooperative jamming by inactive nodes of a cooperative network consisting of multiple single-antenna DF relays and single-antenna source and destination to counteract a single-antenna eavesdropper. The authors propose optimal relay section and optimal power allocation for signal transmission and jamming to improve the secrecy rate. As a usage of full-duplex radios, a cooperative network including a full-duplex relay with the jamming ability is considered in [142] to counteract a single-antenna eavesdropper.

As the relay selection can be used to improve the rate, it can be used to improve the secrecy rate. Relay selection in cooperative networks to improve the secrecy is employed in [143–148]. The authors of [143] propose relay selection and cooperative beamforming to improve the secrecy. Optimal AF and DF relay selection is investigated in [144] for a cooperative network with single-antenna nodes in the presence of single-antenna eavesdropper. It is shown that the probability of interception for the proposed scheme outperforms the conventional approach. Opportunistic relay selection in a cooperative network with single-antenna nodes is employed in [145] to lower the probability of interception at the eavesdropper and outage probability at the destination. Relay selection

between multiple DF relays is carried out in [146] and the resulting secrecy rate is derived. The authors in [147] consider a cooperative network consisting of multiple DF relays and destinations. The relays perform collaborative beamforming to send the message to the destination with the strongest link to the relays to maximize the secrecy rate. The work of [148] considers a cooperative network with multiple AF relays and users. The selected user jamms the transmission from source to relay and subtracts the jamming after receiving the signal from the relay in order to improve the secrecy rate.

A part from two-hop cooperative networks, the secrecy rate in multi-hop networks is studied in [149, 150, 150, 151]. A multi-hop cooperative network with full-duplex DF relays is considered in [149] where a single-antenna eavesdropper wiretaps each hop. The secrecy rate is evaluated when the relay receives the message and jamms the eavesdropper at the same time. As another study in multi-hop relays, [150] performs security analysis of a multi-hop DF relay network where the eavesdropper can wiretap all the hops. The authors perform optimal power allocation/beamforming for single/multiple antenna relay nodes to improve the secrecy rate. The work of [151] considers a cooperative network with multiple AF relays with single-antennas nodes which is wiretapped by a single-antenna eavesdropper. The authors derive the secrecy outage probability using the CSI feedback.

Our contribution in [22] falls into the category of Cooperative communication with external eavesdropper. The secrecy analysis when the satellite works as a relay is studied in [22]. In this work, two users exchange messages using XOR network coding protocol while each of them is being wiretapped by a specific eavesdropper. The authors derive the satellite antenna weights to maximize the sun secrecy rate.

2.2 Signal Processing Paradigm for Security

In the information-theoretic secrecy rate, the perfect, imperfect, or statistical CSI knowledge of the eavesdropper or specific assumptions on the eavesdropper's CSI are required at the transmitter. The transmitter uses these information to design the system parameters in order to maximize the secrecy rate. Moreover, when using the secrecy rate, the secrecy rate is lower than the achievable rate of the channel. As an alternative, a signal processing approach can be followed at the transmitter to improve the security. Here, we divide these signal processing-based works into two groups. The first group enhances the security by designing the precoding using the legitimate CSI. The second group enhances the security by designing the precoding using both the legitimate CSI and the symbols, which is referred to as "directional modulation". In the following, we mention these two groups.

2.2.1 Conventional precoding

As the first work, [152] mentions the concept of enhancing the security using artificial noise, which deviates from the information-theoretic secrecy rate concept introduced by Wyner [5]. This approach relys on the signal processing at the transmitter to design the artificial noise in the null space of the legitimate receiver. One major advantage of this technique is that the eavesdropper's CSI is not required for the system design. In a similar approach, the work of [153] designs a Robust beamformer in a MIMOME wiretap channel. The beamformer is designed to maximize the jamming power, which is in the null direction of the legitimate receiver, and sustains a predefined SINR at the legitimate receiver without the eavesdropper's CSI and imperfect CSI of the legitimate link. The authors of [154] use the artificial noise in the null space of the legitimate channel to prevent decoding at the eavesdropper over a MIMOME channel. The perfect secrecy is achieved when the number of antennas of the legitimate receiver goes to infinity. Linear precoding to transmit data and artificial noise is studied in [155] to improve the security in a multi-cell environment without eavesdropper's CSI where the number of antennas and users increase asymptotically.

Although the Gaussian distribution is optimal when secrecy rate is the target, the Gaussian distribution assumption for the signals cannot be always satisfied in practical communication systems. There are digital communication systems which use finite-alphabet signals such as M-PSK modulation which usually have a discrete uniform distribution [19]. Due to having a non-Gaussian distribution, finite-alphabet signals are not optimal in terms of the developed secrecy rates in [5, 9–13]. Furthermore, although the physical layer security concept introduced in [5] provides perfect secrecy, i.e., zero bit leakage, it also reduces the message transmission rate to the legitimate receiver. There have been research interests in investigating the security issues when finite-alphabet signal is used in a communication system [156, 157]. The authors in [156] devote some of the available power in order to add a randomly scaled version of the finite-alphabet data to itself to create induced fading without optimal beamforming and preserving the phase of the symbol at the receiver. This way, the channel seen by the eavesdropper will be different. If the added random part rotates the M-PSK constellation enough, the eavesdropper decodes the wrong symbol. In [157], suboptimal random beamforming is used to assure the security without requiring the eavesdropper channel state information (CSI) when finite-alphabet signal is used.

2.2.2 Directional modulation via symbol-level precoding

Recently, there has been growing research interest on directional modulation technology and its security enhancing ability for finite-alphabet input signals. As a pioneer, [17] implements a directional modulation transmitter using a parasitic antenna. This system creates the desired amplitude and phase in a specific direction by varying the length of the reflector antennas for each symbol while scrambling the symbols in other directions. The authors of [18] suggest using a phased array at the transmitter and employ a genetic algorithm to derive the phase values of a phased array in order to create symbols in a specific direction. The directional modulation concept is later extended to directionally modulate symbols to more than one destination. In [158], the singular value decomposition (SVD) is used to directionally modulate symbols in a two user system. The authors of [159] derive the array weights to create two orthogonal far field patterns to directionally modulate two symbols to two different locations and [160] uses least-norm to derive the array weights and directionally modulate symbols towards multiple destinations in a multi-user multiple-input multiple-output (MIMO) system.

Array switching at the symbol rate is used in [161, 162, 176] to induce the desired symbols without using actively driven elements, phase shifter and amplifier, in the RF chain. The work of [161] uses an antenna array with a specific fixed delay in each RF chain to create the desired symbols by properly switching the antennas. The authors in [162] use an array where each element can switch to broadside pattern[2], endfire pattern[3], or off status to create the desired symbols in a specific direction. Switched phased array to enhance the security is proposed in [176].

In the second group, a parasitic antenna is used to create the desired amplitude and phase in the far field by near field interactions between a driven antenna element and multiple reflectors [17, 163, 164]. In [17, 163], transistor switches or varactor diodes are used to change the reflector length or its capacitive load, respectively, when the channel is line of sight (LoS). This approach creates a specific symbol in the far field of the antenna towards the desired direction while randomizes the symbols in other directions due to the antenna pattern change. In connection with [17], [164] studies the far field area coverage of a parasitic antenna and shows that it is a convex region. The first group employs amplifiers and/or phases shifters to create an array with actively driven antennas to directionally modulate the data [18, 27, 28, 158–160, 165–175], where [27, 158, 174] consider fading channels. The authors of [18] use a genetic algorithm to derive the phase values of a phased array and create symbols in a specific direction. The technique of [18] is implemented in [165] using a four element microstrip patch array where symbols are

[2]Maximum radiation of an array directed normal to the axis of the array.
[3]Additional maxima radiation directed along the axis.

directionally modulated for Q-PSK modulation. The authors of [166] propose an iterative nonlinear optimization approach to design the array weights which minimizes the distance between the desired and the directly modulated symbols in a specific direction. In [167], baseband in-phase and quadrature-phase signals are separately used to excite two different antennas so that symbols are correctly transmitted only in a specific direction and scrambled in other directions. In another paradigm, [168] uses random and optimized codebook selection, where the optimized selection suppresses large antenna side lobes, in order to improve the security in a millimeter-wave large uniform linear antenna array system. The authors of [169] derive optimal array weights to get a specific bit error rate (BER) for Q-PSK modulation in the desired and undesired directions. The work of [170] uses the Fourier transform to create the optimal constellation pattern for Q-PSK directional modulation, while [171] uses the Fourier transforms along with an iterative approach for Q-PSK directional modulation and constraining the far field radiation patterns. The Fourier transform is used in [170, 171] to create the optimal constellation pattern for Q-PSK directional modulation. In [158, 172–174] directional modulation is employed along with noise injection. The authors of [172, 173] utilize an orthogonal vector approach to derive the array weights in order to directly modulate the data and inject the artificial noise in the direction of the eavesdropper. The work of [172] is extended to retroactive arrays[4] in [174] for a multi-path environment. An algorithm including exhaustive search is used in [175] to adjust two-bit phase shifters for directly modulating information. Since the location of the eavesdropper is unknown, the transmitting angle of the interference is changed randomly. The directional modulation literature do not analyze the abilities of a multiple-antenna eavesdropper and rely on the fact that it receives scrambled symbols. In addition, the works of [158, 173] also transmit interference to degrade the signal quality at the eavesdropper. However, depending on the eavesdropper's number of antennas, it can remove the interference and estimate the symbols. They show that compared to the conventional zero-forcing (ZF) at the transmitter [23], directional modulation is more secure.

On top of the works in the directional modulation literature where antennas excitation weight change on a symbol basis, the symbol-level precoding to create constructive interference between the transmitted symbols has been developed in [180–183] by focusing on the digital processing of the signal before being fed to the antenna array. The main difference between directional modulation and the digital symbol-level precoding for constructive interference is that the former focuses on applying array weights in the analog domain such that the received signals on the receiving antennas have the

[4] A retroactive antenna can retransmit a reference signal back along the path which it was incident despite the presence of spatial and/or temporal variations in the propagation path.

desired amplitude and phase, whereas the latter uses symbol-level precoding for digital signal design at the transmitter to create constructive interference at the receiver. Furthermore, directional modulation was originally motivated by physical layer security, whereas symbol-level precoding by energy efficiency.

Our contributions in [27, 28] fall into the the category of directional modulation via symbol-level precoding. In [27, 28], we design the array weights of a directional modulation transmitter in a single-user MIMO system to minimize the power consumption while keeping the signal-to-noise ratio (SNR) of each received signal above a specific level.

2.3 Conclusion

In this chapter, we reviewed the physical layer security literature by dividing it into the works based on the keyless information-theoretic secrecy rate and signal processing paradigms in Sections 2.1 and 2.2. The signal processing paradigm handles one of the most important shortcomings of the keyless information-theoretic secrecy rate, which is the requirement of the eavesdropper CSI at the transmitter, which may not be possible to acquire in practice.

We divided the information-theoretic research into non-cooperative and cooperative categories in Sections 2.1.1 and 2.1.2. We further divided the secrecy rate analysis of the non-cooperative category into: 1) wiretap broadcast channels, 2) broadcast with confidential messages, 3) wiretap multiple access channels, and 4) secrecy rate and energy efficiency. We divided the literature of the cooperative part into: 1) Untrusted relay, and 2) cooperative communication with external eavesdropper. The information-theoretic secrecy rate literature considers the secrecy rate and the secrecy outage probability as the security metric. These metrics along with the perfect, imperfect or partial CSI of the legitimate and wiretap CSIs are used to design the transmitter, receiver, and/or the relay, e.g., deriving the precoding at the transmitter.

The signal processing paradigm works were divided into two major categories: 1) conventional precoding in Section 2.2.1, and 2) directional modulation via symbol-level precoding in Section 2.2.2. In the conventional precoding literature, the transmitter is designed only using the legitimate CSI knowledge. On the other hand, in the directional modulation via symbol-level precoding, the transmitter is designed using both the symbols and the legitimate CSI. The directional modulation shows to outperform the conventional precoding in terms of the imposed BER at the eavesdropper.

Chapter 3

Security in Bidirectional Multi-beam Satellites

Network coding is an efficient means to improve the spectrum efficiency of satellite communications. However, its resilience to eavesdropping attacks is not well understood. This chapter studies the confidentiality issue in a bidirectional satellite network consisting of two mobile users who want to exchange message via a multibeam satellite using the XOR network coding protocol. We aim to maximize the sum secrecy rate by designing the optimal beamforming vector along with optimizing the return and forward link time allocation. The problem is non-convex, and we find its optimal solution using semidefinite programming together with a 1-D search. For comparison, we also solve the sum secrecy rate maximization problem for a conventional reference scheme without using network coding. Simulation results using realistic system parameters demonstrate that the bidirectional scheme using network coding provides considerably higher secrecy rate compared to that of the conventional scheme. The contributions of this chapter are published in [22].

3.1 Introduction

Satellite communications (SATCOM) is getting more and more integrated into communication networks to compliment the current terrestrial communication systems. Satellite services have to support increasing demands for data transfer. To realize bidirectional satellite communications, traditionally orthogonal resources either in frequency or time domain should be used to avoid interference between users. To save the precious wireless resources, network coding has been used in this work as an efficient protocol to exchange information between two mobile satellite users. The basic principle is that the received

information from users are combined on the satellite or gateway (GW), and then the mixed signal is broadcast to users at the same time and using the same frequency. Because each user can subtract its own message, it can easily decode the message from the other user.

However, due to the broadcast nature and immense area coverage, satellite communications systems, e.g., in military and commercial applications, are vulnerable to security attacks such as eavesdropping. Currently, security in SATCOM is achieved at upper layers by means of encryption such as the Advanced Encryption Standard [1, 2]. Nevertheless, traditional security is based on the assumption of limited computational capability of the malicious nodes, and thus there exists the risk that a malicious node can successfully break an encryption, and get access to sensitive satellite data [3]. In contrast to the upper layer encryption techniques, recently there has been significant interest in securing wireless communications at the physical layer using an information-theoretic approach named "*secrecy rate*" [5]. The main advantage of this approach is that the malicious nodes cannot even get access to protected information regardless of their computational capabilities.

While network coding can greatly improve the system throughput, whether it is more secure than the conventional scheme, which does not use network coding, is largely unknown in SATCOM. In this work, we will leverage the physical layer security approach to address the confidentiality issue in bidirectional SATCOM using the principle of network coding. Below, we provide an overview on the applications of network coding to SATCOM and the related work in the physical layer security literature.

3.1.1 Literature Review

3.1.1.1 Network coding related works

Network coding technique, first introduced in [184], can considerably reduce delay, processing complexity and power consumption, and can significantly increase the data rate and robustness [185]. In the popular XOR network coding scheme, the received signals at an intermediate node are first decoded into bit streams, and then XOR is applied on the bit streams to combine them. The processed bits are re-encoded and then broadcast. Utilization of network coding has been studied in both terrestrial and satellite networks. The authors in [186] apply superposition coding and XOR network coding to a bidirectional terrestrial relay network. A multi-group multi-way terrestrial relay network is considered in [187] where superposition coding and XOR network coding are investigated and compared to each other. Network coding can also considerably improve the spectral

efficiency in bidirectional SATCOM in which two mobile users exchange information via the satellite. The work in [188] compares the amplify-and-forward (AF) method with the XOR network coding scheme in a satellite scenario. A joint delay and packet drop rate control protocol without the knowledge of lost packets for mobile satellite using network coding is studied in [189]. In [190], buffers are designed for satellites when the network coding scheme is employed. Random linear network coding is used in [191] to minimize the packet delivery time. Satellite beam switching for mobile users is tackled in [192] where the network coding scheme increases the robustness in delivery of the packets when mobile terminals move from beam to beam. The XOR network coding protocol is demonstrated in a satellite test bed in [193].

3.1.1.2 Physical layer security related works

Wyner in [5] first showed that secure transmission is possible for the legitimate user given the eavesdropper receives noisier data compared to the legitimate receiver. Inspired by Wyner's work, [10] extended the idea of physical layer secrecy rate from the discrete memoryless wiretap channel to Gaussian wiretap channel. The Wyner's wiretap channel was generalized in [9] to the broadcast channel. After the seminal works done in [5, 9, 10], there have been substantial amount of works in physical layer secrecy. Here, we only review those most relevant to network coding and bidirectional communications. The authors in [194] consider a relay utilizing the XOR network coding protocol where joint relay and jammer selection is done to enhance the secrecy rate. A bidirectional AF relay network with multiple-antenna nodes is considered in [195] where the relay beamforming vector is designed by the waterfilling method to improve the secrecy rate. The authors in [196] consider random relay selection in a bidirectional network in which the relay performs both data transmission and jamming the eavesdropper at the same time to increase the secrecy. The work in [139] performs selection over AF relays and jammers in a bidirectional network for the single-antenna case, and precoding in the multiple-antenna case to enhance the secrecy. To maximize the secrecy in a bidirectional network, the authors in [197] consider the location and distribution of nodes while joint relay and jammer selection is performed. Distributed beamforming along with artificial noise and beamforming is studied in [198] for a bidirectional AF relay network. The work in [199] designs the distributed beamforming weights for a bidirectional network where one intermediate node acts as a jammer. In contrast to the terrestrial literature, there are very few works in physical layer security for SATCOM. The problem of minimizing the transmit power on a multibeam satellite while satisfying a minimum per user secrecy rate is studied in [200]. Iterative algorithms are used to joint optimize the transmission power and the beamforming vector by perfectly nulling the received signal at the eavesdropper.

Both optimal and suboptimal solutions are developed in [201] where the use of artificial noise is also studied.

Despite the physical layer security and network coding works in the terrestrial and SATCOM scenarios, some unaddressed issue are left. In [186], only downlink bottlenecks are considered when designing the beamforming weights for the XOR network coding case. The uplink bottlenecks also need to be considered when optimizing the uplink-downlink time allocation. In [187], the authors consider the decoding-re-encoding and designing the beamforming vector separately. The works in [196, 197] consider single-antenna relay where the AF protocol is used in a bidirectional network. The authors in [195, 198, 199] use the analog network coding protocol in a two-way relay network to facilitate secure information exchange between two users. Furthermore, the mentioned terrestrial works in physical layer security for bidirectional communications assume one eavesdropper in the environment. The works in [200, 201] design the beamforming weights for unidirectional service for fixed users in the forward link (FL).

3.1.2 Our Contribution

In this work, we study the network coding based bidirectional SATCOM in which two mobile users exchange data via a transparent multibeam satellite in the presence of two eavesdroppers. There is an eavesdropper present for each user who overhears the bidirectional communications. The users employ omnidirectional antennas and the communication is prone to eavesdropping in both the return link (RL) and FL. In the RL, two users send signals using two orthogonal frequency channels; the signals collected by the satellite are passed to the GW, where they are decoded, XOR-ed and then the produced stream is re-encoded. This combined stream is multiplied by the beamforming vector which contains the designed weight of each feed. Consequently, each element of the resultant vector is transmitted to the satellite using the feeder link. Each element which includes both the feed weight and the data signal is applied to the corresponding feed to adjust the beams for broadcasting to both users simultaneously in the FL. This scheme is more power-efficient than the conventional method where network coding in not utilized and the power is splitted into two data streams. This benefit is extremely vital for SATCOM because of the limited on-board power.

Our main contributions in this work are summarized below to differentiate it from the prior work:

1. XOR network coding is incorporated into SATCOM in to enable both efficient and secure bidirectional data exchange.

2. The end-to-end sum secrecy rate is first derived, and then maximized by designing the optimal beamforming vector and the RL and FL time allocation. The optimization problem regarding the beamforming vector is solved using semi-definite programming (SDP) along with 1-D search.

3. Extensive simulation results are presented to demonstrate the advantage of the bidirectional scheme over the conventional scheme using realistic SATCOM parameters.

3.2 System Model

Consider a satellite communication system comprised of two users denoted by U_1 and U_2 who exchange information with each other, one multibeam transparent satellite denoted by S, one GW, two eavesdroppers denoted by E_1 and E_2 as depicted in Fig. 4.1. Users are located in different beams of the satellite, and they transmit the RL signals using different frequency channels simultaneously. We assume that each user and each eavesdropper is equipped with a single omni-directional antenna. Because of the long distance between the users, there is no direct link between them; furthermore, eavesdroppers cannot cooperate and E_i can only overhear U_i for $i = 1, 2$. Contemporary orbiting satellites such as *ICO*, *SkyTerra*, and *Thuraya* have limited power, here defined as P_S, and some of them do not have the on-board processing ability to decode the received messages or perform on-board beamforming, so they have to forward the received signal to the GW to get it processed [202–204]. Using the GW to process the signal and designing the feed weights is referred to as the ground-based beamforming technique. The ground-based beamforming technique is perceived as the most convenient and economical approach [204]. In this chapter, we consider a commercial satellite without digital processing ability and follow the ground-based beamforming paradigm.

In our satellite network model, we assume that the eavesdropper is a regular user which is part of the network. However, it is considered as an unintended user, potential eavesdropper, which the information needs to be kept secret from it. Due to the fact that the eavesdropper is part of the network, it is possible to estimate the channels to it. Hence, similar to the works [20, 42, 179, 205, 206], we assume that the eavesdropper's channel state information (CSI) is known. Based on the mentioned assumption, we assume that the users and eavesdropper know all the CSIs. Further, all communication channels are known and fixed during the period of communication. It is worth mentioning that in the secrecy rate analysis of XOR network coding, only the CSI of the eavesdroppers in the RL is required. Although we assume the availability of the eavesdropper's CSI, there are methods such as null-space artificial noise transmission [207],

random beamforming [51, 157, 208], or effective channel coding design to strengthen the cryptography [209] in order to sustain secrecy without having the knowledge of the eavesdropper's CSI. Another alternative can be using the statistical knowledge of the eavesdropper's CSI in order to improve the secrecy [210–213]. Also, the interference alignment technique can be used along with statistical knowledge of the eavesdropper's CSI to enhance the secrecy [95]. In the situations when the geographical area of the eavesdropper is known, the worst-case scenario can be considered. In this scenario, the best CSI from the user to the eavesdropper's area is considered for the design. One possible example for the worst-case scenario can be when the occupied zone by the enemy is known. This example can be one of the applications of this chapter.

To acquire the RL channel state information (CSI) at the GW, the users send the pilot signals along with the data toward the satellite. For the FL CSI, the GW sends pilots to the users. Afterwards, the estimated CSI by the users is sent back to the GW. Therefore, getting the FL CSI takes more time compared to the RL CSI [214]. The GWs are equipped with advanced transceivers and antennas and because of this reason, the communication link between the GW and the satellite (feeder link) is modeled as an ideal link. Hence, similar to the works [203, 215–218] which are carried out in the satellite communications literature, we assume that the channel between the satellite and the GW, which is referred to as the feeder link, is ideal with abundant bandwidth.

The complete communication phases of the network coding based scheme are summarized in Table 3.1. The conventional scheme without using network coding is also included for comparison and details are given in Section 3.2.2. The first two phases for the RL are the same for both schemes while the main difference lies in the FL transmission. In the conventional scheme, signals are sent in different time slots for each user in the FL, so this scheme has less available transmission time for each user. In the bidirectional scheme, signal streams are combined, and then sent in the FL using the XOR network coding protocol, therefore, the spectral efficiency is significantly improved compared to the conventional scheme.

3.2.1 Network coding based bidirectional SATCOM

3.2.1.1 Signal model

In this case, the whole communication takes place in four phases. In Phase I, both users transmit signals using different frequencies simultaneously. The signals received at the

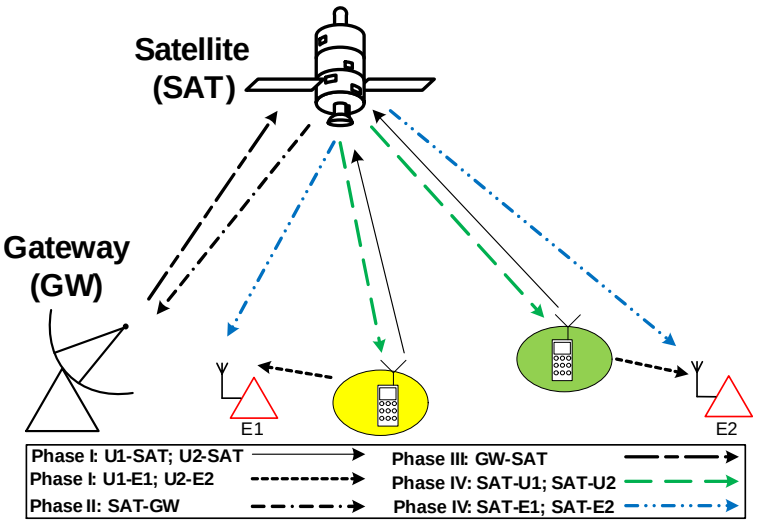


FIGURE 3.1: Bidirectional satellite communication network.

satellite and the eavesdroppers are

$$\mathbf{y}_{S_1} = \sqrt{P_{U_1}}\mathbf{h}_{U_1,S}\, s_1 + \mathbf{n}_{S_1}, \tag{3.1}$$

$$\mathbf{y}_{S_2} = \sqrt{P_{U_2}}\mathbf{h}_{U_2,S}\, s_2 + \mathbf{n}_{S_2}, \tag{3.2}$$

$$y_{E_1}^{RL} = \sqrt{P_{U_1}} h_{U_1,E_1} s_1 + n_{E_1}, \tag{3.3}$$

$$y_{E_2}^{RL} = \sqrt{P_{U_2}} h_{U_2,E_2} s_2 + n_{E_2}, \tag{3.4}$$

where P_{U_i} is the transmitted power by the users for $i = 1, 2$, h and $\mathbf{h}$ represent the user-eavesdropper and user-satellite channels, respectively, and the corresponding source and destination are denoted by the subscript. The channel for the satellite is a $N_S \times 1$ vector where N_S is the number of the satellite feeds. Additive white Gaussian noises (AWGN) are denoted by n and $\mathbf{n}$ with $n \sim \mathcal{CN}(0, \sigma^2)$ and $\mathbf{n} \sim \mathcal{CN}(0, \sigma^2 \mathbf{I}_{N_S \times N_S})$, respectively. We consider the noise power for users, satellite and eavesdroppers as KTB, where K is the Boltzman's constant which is -226.8 dBW/K/Hz, T is the on-board temperature and B is the carrier bandwidth. We assume that s_1 and s_2 are independent and identically distributed (i.i.d.) Gaussian random source signals with zero mean and unit variance. For convenience, we use the noise variance, σ^2, instead of KTB and omit the bandwidth, B, in the rate expressions throughout the chapter. Note that we consider different temperatures for ground nodes and the satellite. The satellite forwards the received signal to the GW using the feeder link in Phase II and thanks to the ideal link between the satellite and the GW, the same signals as (3.1) and (3.2) are present at the GW to be processed.

At the GW, the received signal is filtered and users' data are separated and decoded into two bit streams denoted by x_1 and x_2, respectively. The GW applies the bit-wise XOR algebraic operation to the decoded bit streams of the users to get the combined

TABLE 3.1: Communication stages for the XOR network coding and the conventional schemes.

<table>
<tr><th>Conventional reference scheme</th><th>XOR network coding scheme</th></tr>
<tr><td colspan="2">Phase I: U_1 and U_2 simultaneously send their signals, s_1 and s_2, to the satellite while they are overheard by E_1 and E_2, respectively.</td></tr>
<tr><td colspan="2">Phase II: The satellite passes the received signal to the GW for processing. At the GW, the users' signals are separately decoded.</td></tr>
<tr><td>Phase III: The intended signal for U_1, decoded s_2, is re-encoded at the GW and the corresponding feed weights are designed. Then, the feed weights multiplied by the data signal are sent to the satellite.</td><td rowspan="2">Phase III: The GW applies XOR operation on the decoded streams from s_1 and s_2 to create a merged stream of bits and the feed weights are designed. Then, the feed weights multiplied by the data signal are sent to the satellite.</td></tr>
<tr><td>Phase IV: The satellite passes the re-encoded signal through the corresponding beam to U_1 while E_1 is listening to it.</td></tr>
<tr><td>Phase V: The intended signal for U_2, decoded s_1, is re-encoded at the GW and the corresponding feed weights are designed. Then, the feed weights multiplied by the data signal are sent back to the satellite.</td><td rowspan="2">Phase IV: The satellite broadcasts the merged stream toward the users through the corresponding beams which is wiretapped by both E_1 and E_2.</td></tr>
<tr><td>Phase VI: The satellite passes the re-encoded signal through the corresponding beam to U_2 while E_2 is listening to it.</td></tr>
</table>

stream

$$x_{GW} = x_1 \oplus x_2. \tag{3.5}$$

Note that before applying the XOR network coding, the GW uses zero-padding to add zeros to the shorter bit stream in order to make equal length bit streams out of the two different bit streams sent by the users [219, 220]. In Phase III, x_{GW} is encoded into s_{GW} with unit power, and then multiplied by the beamforming vector, $\mathbf{w}$. Using the ideal feeder link, each element, $w_i s_{GW}(t)$, of the produced vector, $\mathbf{w}s_{GW}$, at the GW which both includes the feed weight, w_i, and the data signal, s_{GW}, is transmitted from the GW to the satellite. Since the codebook used at the GW to encode x_{GW} can

be different in the XOR network coding scheme, the RL and FL transmission times are generally different for the XOR network coding. This enables optimum RL and FL time allocation for the XOR network coding. The received signal by satellite is denoted as $\mathbf{s}_S = \mathbf{H}_{GW,S}\mathbf{w}s_{GW}$. The model $\mathbf{s}_S = \mathbf{H}_{GW,S}\mathbf{w}s_{GW}$ encapsulates the process of transmitting each element of the vector $\mathbf{w}s_{GW}$ from the GW to the satellite. Since the feeder link is considered to be ideal, $\mathbf{H}_{GW,S}$ is a $N_S \times N_S$ identity matrix. Finally, in Phase IV, each feed weight designed at the GW, which includes the data signal, is applied to the corresponding feed at the satellite. Hence, the beams are adjusted and the signal $\mathbf{s}_S$ is broadcast through the antennas. The received signals at two users are, respectively,

$$y_{U_1}^{FL_{XOR}} = \mathbf{h}_{S,U_1}^T \mathbf{s}_S + n_{U_1}, \tag{3.6}$$

$$y_{U_2}^{FL_{XOR}} = \mathbf{h}_{S,U_2}^T \mathbf{s}_S + n_{U_2}. \tag{3.7}$$

Similarly, the received signals at the eavesdroppers in Phase IV are, respectively,

$$y_{E_1}^{FL_{XOR}} = \mathbf{h}_{S,E_1}^T \mathbf{s}_S + n_{E_1}, \tag{3.8}$$

$$y_{E_2}^{FL_{XOR}} = \mathbf{h}_{S,E_2}^T \mathbf{s}_S + n_{E_2}. \tag{3.9}$$

In the following, we shall define the sum secrecy rate. We first introduce the users' rates and eavesdroppers' channel capacities.

3.2.1.2 Users' RL rates

Consider t_1 and t_2 for the RL (Phase I) and FL (Phase IV) transmission time, respectively. In Phase I, we can characterize the RL rates $(R_{U_1}^{RL}, R_{U_2}^{RL})$ by the following equations [221, Chapter 5]:

$$R_{U_1}^{RL} \leq I_{U_1}^{RL} = t_1 \log\left(1 + \frac{P_{U_1}\left\|\mathbf{h}_{U_1,S}\right\|^2}{\sigma_S^2}\right) \tag{3.10}$$

$$R_{U_2}^{RL} \leq I_{U_2}^{RL} = t_1 \log\left(1 + \frac{P_{U_2}\left\|\mathbf{h}_{U_2,S}\right\|^2}{\sigma_S^2}\right), \tag{3.11}$$

where I denotes channel capacity or the maximum supported rate and R is the maximum achievable rate.

3.2.1.3 Users' FL rates

After receiving the FL signal, users decode $\mathbf{s}_S$. As each user knows its own transmitted bits, it can use the XOR operation to retrieve the intended bits. Subsequently, using (3.6) and (3.7), the FL rates can be expressed as

$$R^{FL_{XOR}} = \min\left\{I_{U_1}^{FL_{XOR}}, I_{U_2}^{FL_{XOR}}\right\}, \tag{3.12}$$

$$I_{U_1}^{FL_{XOR}} = t_2 \log\left(1 + \frac{|\mathbf{h}_{S,U_1}^T \mathbf{w}|^2}{\sigma_{U_1}^2}\right), \tag{3.13}$$

$$I_{U_2}^{FL_{XOR}} = t_2 \log\left(1 + \frac{|\mathbf{h}_{S,U_2}^T \mathbf{w}|^2}{\sigma_{U_2}^2}\right). \tag{3.14}$$

Since the data for both users have gone through a bit-wise XOR operation at the GW and a combined signal is broadcast, the GW has to adjust the combined signal's data rate to match both users' channel capacities. This rate should be equal to the minimum FL channel rate between the satellite and the users in Phase IV before sending $\mathbf{s}_S$ to the satellite.

3.2.1.4 Eavesdroppers' channel capacities

Using (3.3) and (3.8), the channel capacity from U_1 to E_1, $I_{E_1}^{RL}$, and from satellite to E_1, $I_{E_1}^{FL_{XOR}}$, can be expressed, respectively, as

$$I_{E_1}^{RL} = t_1 \log\left(1 + \frac{P_{U_1}|h_{U_1,E_1}|^2}{\sigma_{E_1}^2}\right), \tag{3.15}$$

$$I_{E_1}^{FL_{XOR}} = t_2 \log\left(1 + \frac{|\mathbf{h}_{S,E_1}^T \mathbf{w}|^2}{\sigma_{E_1}^2}\right). \tag{3.16}$$

The channel capacities for E_2 can be derived in a similar way.

3.2.1.5 Secrecy rate definition

First, we derive the secrecy rate for the RLs and FLs, and then the end-to-end secrecy rate. In [13], the result of [5] is extended to fading channels with multiple-antenna transmitter, receiver, and eavesdropper. Using the special case of the result in [13] for single-antenna transmitter, multiple-antenna receiver, and single-antenna eavesdropper along with employing (3.10) and (3.15), the secrecy rate for the RL of U_1 is calculated

as

$$SR_{U_1}^{RL} = I_{U_1}^{RL} - I_{E_1}^{RL}, \tag{3.17}$$

where the notation "SR" means "secrecy rate". To calculate the secrecy rate in the FL, first, we derive the information that E_1 can recover during the RL transmission in Lemma 3.1.

Lemma 3.1. *Independent of getting a positive or zero secrecy rate defined for the RL of U_1 in (3.17), E_1 cannot recover any bits from U_2 transmitted message using the FL transmission.*

Proof. To recover bits from U_2, E_1 has to apply XOR operation between the bits recovered from U_1 in the RL transmission and the bits derived from the satellite broadcast in the FL transmission. Hence, the information detected by E_1 in the FL depends on the bits recovered from U_1 in the RL transmission. The recovered bits from U_1 in the RL depend on the sign of the secrecy rate defined in (3.17). The sign of the RL secrecy rate in (3.17) has the following possibilities:

1. If $I_{U_1}^{RL} - I_{E_1}^{RL} > 0$, then U_1 can establish a perfectly secured connection so that the eavesdropper cannot get any bits from U_1 in the RL [13]. Hence, E_1 does not have the bits transmitted by U_1 in the RL and it cannot recover any bits from U_2 using the FL transmission.

2. If $I_{U_1}^{RL} - I_{E_1}^{RL} \leq 0$, then the secrecy rate is zero. Therefore, U_1 cannot establish a secure connection in the RL. In this case, U_1 remains silent during the corresponding time slot. In this time slot, GW generates random bits instead of the bits from U_1 and applies XOR between them and the bits from U_2. As a result, E_1 cannot recover any bits from U_2 using the FL transmission.

Note that since the RL time, t_1, is always positive and all the channels are known, the sign of the expression $I_{U_1}^{RL} - I_{E_1}^{RL}$ is known prior to the beamformer design. □

A similar argument as in Lemma 3.1 can be applied to E_2. Consequently, using Lemma 3.1, the secrecy rate for the FL is given in Lemma 3.2.

Lemma 3.2. *Assume that there exists at least one RL with a positive secrecy rate. Then, the secrecy rate in the FL is given as below:*

$$SR^{FL_{XOR}} = \begin{cases} \min\left\{I_{U_1}^{FL_{XOR}}, I_{U_2}^{FL_{XOR}}\right\} & SR_{U_1}^{RL} > 0, \\ & SR_{U_2}^{RL} > 0, \\ I_{U_1}^{FL_{XOR}} & SR_{U_1}^{RL} = 0, \\ & SR_{U_2}^{RL} > 0, \\ I_{U_2}^{FL_{XOR}} & SR_{U_1}^{RL} > 0, \\ & SR_{U_2}^{RL} = 0. \end{cases} \tag{3.18}$$

Proof. Excluding the case that both RLs have zero secrecy rate, i.e., the total secrecy rate is zero, the secrecy rate for the FL transmission for different signs of the secrecy rate in the RL is given as follows:

1. If $SR_{U_1}^{RL} > 0$ and $SR_{U_2}^{RL} > 0$, then according to Lemma 3.1, E_1 and E_2 cannot wiretap any bits from U_2 and U_1, respectively, using the FL transmission. Therefore, using (3.12), the secrecy rate in the FL is $\min\left\{I_{U_1}^{FL_{XOR}}, I_{U_2}^{FL_{XOR}}\right\}$.
2. If $SR_{U_1}^{RL} > 0$ and $SR_{U_2}^{RL} = 0$, then according to Lemma 3.1, E_1 cannot wiretap any bits from U_2 using the FL transmission. Further, since the RL of U_2 is not secure, U_2 does not transmit and E_2 does not get any bits from U_2. Hence, E_2 cannot recover bits from U_1 using the FL transmission. Since U_1 is not expected to receive any message because of $SR_{U_2}^{RL} = 0$, the FL secrecy rate is $I_{U_2}^{FL_{XOR}}$.
3. If $SR_{U_1}^{RL} = 0$ and $SR_{U_2}^{RL} > 0$, similar to the procedure as in Case 2, the secrecy rate in the FL is $I_{U_1}^{FL_{XOR}}$.

According to the results in Cases 1, 2, and 3, the secrecy rate of the FL is derived as in (3.18). □

According to Lemma 3.2, when the XOR protocol is used, the FLs are totally secured. Note that for the Cases 2 and 3, the GW creates random bits instead of the message from the user with insecure link, i.e., zero secrecy rate in the RL. Then, the GW applies XOR between the received message from the user which has a positive secrecy rate in the RL and the randomly generated bits. This way, the eavesdropper still receives a combined message when the secrecy rate is zero in one of the RLs.

To derive the end-to-end secrecy rate for U_1, we invoke Theorem 1 in [222], which states that, when decoding and re-encoding is performed by an intermediate node, the secrecy

rate of each hop needs to be taken into account as a bottleneck to derive the end-to-end secrecy rate. Since decoding and re-encoding is performed at the GW, the result of Theorem 1 in [222] can be applied. Consequently, using the mentioned theorem and the secrecy rate derived in (3.17) and the result of Lemma 3.2 in (3.18), the end-to-end secrecy rate for U_1 is calculated by

$$SR_{U_1}^{XOR} = \min\left\{SR_{U_1}^{RL}, SR_{U_1}^{FL_{XOR}}\right\}. \tag{3.19}$$

The end-to-end secrecy rate for U_2 can be derived in a similar way. The sum end-to-end secrecy rate is expressed as

$$SR^{XOR} = SR_{U_1}^{XOR} + SR_{U_2}^{XOR}. \tag{3.20}$$

3.2.2 Conventional SATCOM

A conventional scheme without using network coding is described here as a performance benchmark.

3.2.2.1 Signal model

As shown in Table 3.1, the Phases I and II are the same for the conventional and the XOR network coding schemes, which result in the same signal model for both schemes. In Phases III and V, the GW sends back each element of the processed $\mathbf{s}_2$ and $\mathbf{s}_1$ to the satellite, respectively, using the ideal feeder link where $\mathbf{s}_1$ and $\mathbf{s}_2$ are $N_S \times 1$ vectors containing both the feed weights and the users' data signals. $\mathbf{s}_1$ and $\mathbf{s}_2$ are defined as $\mathbf{s}_1 = \mathbf{w}_1\hat{s}_1$ and $\mathbf{s}_2 = \mathbf{w}_2\hat{s}_2$, where $\hat{s}_1$ and $\hat{s}_2$ are the decoded and re-encoded versions of the data signals received from U_1 and U_2 at the GW with unit power, and $\mathbf{w}_1$ and $\mathbf{w}_2$ are beamforming vectors to be designed at the GW. Note that since different Gaussian codebooks are used at the GW to re-encode the signals for U_1 and U_2, the generated signals at the GW are different from those received from the users. Therefore, generated signals at the GW are shown by $\hat{s}_1$ and $\hat{s}_2$.

The satellite applies each component of the vector $\mathbf{s}_2$, containing the feed weight multiplied by the data signal, to the corresponding feed. Then, the beam is adjusted and $\hat{s}_2$ is sent toward U_1 in Phase IV, and the received signals at U_1 and E_1 are, respectively,

$$y_{U_1}^{FL_{Con}} = \mathbf{h}_{S,U_1}^T\mathbf{s}_2 + n_{U_1}, \tag{3.21}$$

$$y_{E_1}^{FL_{Con}} = \mathbf{h}_{S,E_1}^T\mathbf{s}_2 + n_{E_1}. \tag{3.22}$$

Similarly, at the end of Phase VI, the received signals at U_2 and E_2 are, respectively,

$$y_{U_2}^{FL_{Con}} = \mathbf{h}_{S,U_2}^T \mathbf{s}_1 + n_{U_2}, \tag{3.23}$$

$$y_{E_2}^{FL_{Con}} = \mathbf{h}_{S,E_2}^T \mathbf{s}_1 + n_{E_2}. \tag{3.24}$$

The beamformer weights in the conventional scheme are exclusively designed at the GW for each user. Hence, when data is being transmitted for U_1, the satellite's main lobe is focused toward U_1. Since E_2 is outside the beam directed toward U_1 and the beamformers are designed to maximize the signal strength toward U_1, E_2 receives the signal from side lobes. As a result, the signal received by E_2 is weak. Similar conditions hold for E_1 when transmitting to U_2. To make the derivation tractable, we neglect these weak signals received by E_2 and E_1 in Phases IV and VI, respectively. As a result, the sum secrecy rate derived for the conventional scheme shall be an upper-bound.

3.2.2.2 Users' rates

The RL rates for the conventional SATCOM are the same as the XOR network coding scheme in (3.10) and (3.11). Using (3.21) and (3.23), the FL rates to U_1 and U_2 after self-interference cancellation can be derived, respectively, as

$$I_{U_1}^{FL_{Con}} = t_2 \log_2 \left(1 + \frac{\left| \mathbf{h}_{S,U_1}^T \mathbf{w}_2 \right|^2}{\sigma_{U_1}^2} \right), \tag{3.25}$$

$$I_{U_2}^{FL_{Con}} = t_3 \log_2 \left(1 + \frac{\left| \mathbf{h}_{S,U_2}^T \mathbf{w}_1 \right|^2}{\sigma_{U_2}^2} \right). \tag{3.26}$$

In order to make the conventional method comparable to the bidirectional one, we assume that the total available transmission time for both the network coding and the conventional schemes are the same. In other words, the RL time for the users is t_1 and the FL for U_1 and U_2 are t_2 and $t_3 = 1 - t_1 - t_2$, respectively.

3.2.2.3 Eavesdroppers' channel capacities

The RL capacities for E_1 and E_2 in the conventional SATCOM are the same as the ones derived for the XOR network coding scheme. Using (3.22) and (3.24), the FL capacity from the satellite toward E_1 and E_2 to overhear the signals sent in Phases IV and VI,

respectively, are

$$I_{E_1}^{FL_{Con}} = t_2 \log_2 \left(1 + \frac{\left| \mathbf{h}_{S,E_1}^T \mathbf{w}_2 \right|^2}{\sigma_{E_1}^2} \right), \tag{3.27}$$

$$I_{E_2}^{FL_{Con}} = t_3 \log_2 \left(1 + \frac{\left| \mathbf{h}_{S,E_2}^T \mathbf{w}_1 \right|^2}{\sigma_{E_2}^2} \right). \tag{3.28}$$

3.2.2.4 Secrecy rate definition

The RL secrecy rate for U_1 and U_2 are the same as the XOR network coding scheme in Section 3.2.1.5. In the conventional scheme, the messages that E_1 receives in the RL and FL are different and can be decoded independently. Hence, the FL secrecy rate for U_1 can be defined using (3.25), (3.27) and the result from [13] as

$$SR_{U_1}^{FL_{Con}} = I_{U_1}^{FL_{Con}} - I_{E_1}^{FL_{Con}}. \tag{3.29}$$

Utilizing (3.17), (3.29), and Theorem 1 in [222], the end-to-end secrecy rate for U_1 is derived as

$$SR_{U_1}^{Con} = \min \left\{ SR_{U_1}^{RL}, SR_{U_2}^{FL_{Con}} \right\}. \tag{3.30}$$

The end-to-end secrecy rate for U_2 can be defined in a similar way. Like in Section 3.2.1.5, the sum secrecy rate is

$$SR^{Con} = SR_{U_1}^{Con} + SR_{U_2}^{Con}. \tag{3.31}$$

3.3 Problem Formulation and the Proposed Solution

In this section, we study the problem of maximizing the sum secrecy rate by optimizing the precoding vectors at the GW to shape the satellite beams along with the RL and FL time allocation, given the maximum available power P_S at the satellite. We consider both the XOR network coding and the conventional schemes. For the XOR network coding, we just solve the optimal beamformer design for the secrecy rate derived from the first case of the FL secrecy rate in (3.18). The solutions for the optimal beamformer design for the other two cases of (3.18) are similar to the first case of (3.18).

3.3.1 Network coding for bidirectional SATCOM

Using the sum secrecy rate defined in (3.20), the optimization problem for the XOR network coding scheme is defined as

$$\begin{aligned}
\max_{\mathbf{w},t_1,t_2} \quad & \min\left\{I_{U_1}^{RL}-I_{E_1}^{RL},\min\left\{I_{U_1}^{FL_{XOR}},I_{U_2}^{FL_{XOR}}\right\}\right\} \\
& +\min\left\{I_{U_2}^{RL}-I_{E_2}^{RL},\min\left\{I_{U_1}^{FL_{XOR}},I_{U_2}^{FL_{XOR}}\right\}\right\} \\
\text{s.t.} \quad & t_1+t_2=1, \\
& \|\mathbf{w}\|^2 \le P_S.
\end{aligned} \tag{3.32}$$

To transform (3.32) into a standard convex form, we apply the following procedures. First, we assume that t_1 and t_2 are fixed and study the beamforming design. After designing the optimal beamformer, the optimal time allocation is found by performing 1-D search of t_1 over the range $(0,1)$. Second, after considering a fixed transmission time for the RL and FL, the RL secrecy rate expressions in (3.32) are fixed and can be dropped without loss of generality. Hence, (3.32) boils down into

$$\begin{aligned}
\max_{\mathbf{w}} \quad & \min\left\{I_{U_1}^{FL_{XOR}},I_{U_2}^{FL_{XOR}}\right\} \\
\text{s.t.} \quad & \|\mathbf{w}\|^2 \le P_S.
\end{aligned} \tag{3.33}$$

Next, we introduce the auxiliary variable u to remove the "min" operators. Then, (3.33) yields

$$\begin{aligned}
\max_{\mathbf{w},u>0} \quad & u \\
\text{s.t.} \quad & \|\mathbf{w}\|^2 \le P_S, \\
& \sigma_{U_1}^2\left(2^{\frac{u}{t_2}}-1\right) \le \left|\mathbf{h}_{S,U_1}^T\mathbf{w}\right|^2, \\
& \sigma_{U_2}^2\left(2^{\frac{u}{t_2}}-1\right) \le \left|\mathbf{h}_{S,U_2}^T\mathbf{w}\right|^2.
\end{aligned} \tag{3.34}$$

The last two constraints in (3.34) are not convex. By introducing $\mathbf{W}=\mathbf{w}\mathbf{w}^H$, we rewrite (3.34) as

$$\begin{aligned}
\max_{\mathbf{W}\succeq 0,u>0} \quad & u \\
\text{s.t.} \quad & \mathrm{tr}\left(\mathbf{W}\right) \le P_S, \\
& \sigma_{U_1}^2\left(2^{\frac{u}{t_2}}-1\right) \le \mathrm{tr}\left(\mathbf{W}\mathbf{A}\right), \\
& \sigma_{U_2}^2\left(2^{\frac{u}{t_2}}-1\right) \le \mathrm{tr}\left(\mathbf{W}\mathbf{B}\right),
\end{aligned} \tag{3.35}$$

where $\mathbf{A} = \mathbf{h}_{S,U_1}^{*}\mathbf{h}_{S,U_1}^{T}$ and $\mathbf{B} = \mathbf{h}_{S,U_2}^{*}\mathbf{h}_{S,U_2}^{T}$. The rank constraint, $\text{rank}(\mathbf{W}) = 1$, in (3.35) is dropped. The optimal beamforming weight in (3.35) is designed for the FL transmission. However, since the RL secrecy rates, which can be bottlenecks for the total end-to-end secrecy rate, are not considered in (3.35), extra unnecessary power at the satellite may be utilized. To fix this, one last constraint is added to (3.35) to get

$$\begin{aligned}
\max_{\mathbf{W}\succeq 0, u>0} \quad & u \\
\text{s.t.} \quad & \text{tr}(\mathbf{W}) \leq P_S, \\
& \sigma_{U_1}^2\left(2^{\frac{u}{t_2}}-1\right) \leq \text{tr}(\mathbf{W}\mathbf{A}), \\
& \sigma_{U_2}^2\left(2^{\frac{u}{t_2}}-1\right) \leq \text{tr}(\mathbf{W}\mathbf{B}), \\
& u \leq \max\left\{I_{U_1}^{RL}-I_{E_1}^{RL}, I_{U_2}^{RL}-I_{E_2}^{RL}\right\}.
\end{aligned} \tag{3.36}$$

Problem (3.36) is recognized as a SDP problem, thus convex and can be efficiently solved. According to Theorem 2.2 in [223], when there are three constraints on the matrix variable of a SDP problem such as (3.36), existence of a rank-1 optimal solution for $N_S > 2$ is guaranteed. Hence, if the solution to (3.36) happens not to be rank-one, we can use Theorem 2.2 in [223] to recover the rank-one optimal solution out of a non-rank-1 solution. According to [224], the complexity of problem (3.36) is

$$\text{O}\left(\left(3+N_S^2\right)\left(\frac{N_S^2\left(N_S^2+1\right)}{2}\right)^3\right). \tag{3.37}$$

Solving (3.36) is accompanied along with a 1-D exhaustive search over the time variable t. We assume that the time variable is divided into m bins between 0 and 1. The overall computational complexity for designing the beamformer for the XOR network coding scheme is m times the complexity mentioned in (3.37). This is typically affordable since the optimization is performed at the GW on the ground.

3.3.2 Conventional SATCOM

According to the secrecy rate defined in (3.31), the optimization problem for the conventional scheme is

$$\begin{aligned}
\max_{\mathbf{w}_1,\mathbf{w}_2,t_1,t_2} \quad & \min\left\{I_{U_1}^{RL}-I_{E_1}^{RL}, I_{U_2}^{FL_{Con}}-I_{E_2}^{FL_{Con}}\right\} \\
& + \min\left\{I_{U_2}^{RL}-I_{E_2}^{RL}, I_{U_1}^{FL_{Con}}-I_{E_1}^{FL_{Con}}\right\} \\
\text{s.t.} \quad & \|\mathbf{w}_1\|^2+\|\mathbf{w}_2\|^2 \leq P_S.
\end{aligned} \tag{3.38}$$

Assume that the power split between the beamforming vectors $\mathbf{w}_1$ and $\mathbf{w}_2$ is βP_S and $(1-\beta)P_S$ where β is a given parameter with $0 \leq \beta \leq 1$. Using the parameter β, the beamforming vectors $\mathbf{w}_1$ and $\mathbf{w}_2$ in the power constraint of (3.38) can be separated. Hence, (3.38) can be rewritten as

$$\begin{aligned}
&\max_{\mathbf{w}_1,\mathbf{w}_2,t_1,t_2} \quad \min\left\{I_{U_1}^{RL}-I_{E_1}^{RL}, I_{U_2}^{FL_{Con}}-I_{E_2}^{FL_{Con}}\right\} \\
&+\min\left\{I_{U_2}^{RL}-I_{E_2}^{RL}, I_{U_1}^{FL_{Con}}-I_{E_1}^{FL_{Con}}\right\} \\
&\quad \text{s.t.} \qquad \|\mathbf{w}_1\|^2 \leq \beta P_S, \\
&\qquad\qquad \|\mathbf{w}_2\|^2 \leq (1-\beta)P_S.
\end{aligned} \tag{3.39}$$

The problem (3.39) can be expanded as

$$\begin{aligned}
&\max_{\mathbf{w}_1,\mathbf{w}_2,t_1,t_2} \min\left\{SR_{U_1}^{RL}, t_2\log\left(\frac{\sigma_{E_2}^2}{\sigma_{U_2}^2}\frac{\sigma_{U_2}^2+|\mathbf{h}_{S,U_2}^T\mathbf{w}_1|^2}{\sigma_{E_2}^2+|\mathbf{h}_{S,E_2}^T\mathbf{w}_1|^2}\right)\right\} \\
&+\min\left\{SR_{U_2}^{RL}, t_3\log\left(\frac{\sigma_{E_1}^2}{\sigma_{U_1}^2}\frac{\sigma_{U_1}^2+|\mathbf{h}_{S,U_1}^T\mathbf{w}_2|^2}{\sigma_{E_1}^2+|\mathbf{h}_{S,E_1}^T\mathbf{w}_2|^2}\right)\right\} \\
&\quad \text{s.t.} \qquad \|\mathbf{w}_1\|^2 \leq \beta P_S, \\
&\qquad\qquad \|\mathbf{w}_2\|^2 \leq (1-\beta)P_S.
\end{aligned} \tag{3.40}$$

Before further simplifying (3.40), we first mention the following theorem.

Theorem 3.3. *If the achievable secrecy rate is strictly greater than zero, the power constraints in (3.40) are active at the optimal point $\mathbf{w}_1^\star$ and $\mathbf{w}_2^\star$, i.e., $\|\mathbf{w}_1\|^2 = \beta P_S$ and $\|\mathbf{w}_2\|^2 = (1-\beta)P_S$.*

Proof. The proof is given in Appendix A. □

Using Theorem 3.3, we can show that the constraints in (3.40) are active which enables us to write (3.40) as

$$\begin{aligned}
&\max_{\mathbf{w}_1,\mathbf{w}_2,t_1,t_2} \quad \min\left\{I_{U_1}^{RL}-I_{E_1}^{RL}, t_2\log\left(\frac{\sigma_{E_2}^2}{\sigma_{U_2}^2}\frac{\mathbf{w}_1^H\mathbf{U}_2\mathbf{w}_1}{\mathbf{w}_1^H\mathbf{E}_2\mathbf{w}_1}\right)\right\} \\
&+\min\left\{I_{U_2}^{RL}-I_{E_2}^{RL}, t_3\log\left(\frac{\sigma_{E_1}^2}{\sigma_{U_1}^2}\frac{\mathbf{w}_2^H\mathbf{U}_1\mathbf{w}_2}{\mathbf{w}_2^H\mathbf{E}_1\mathbf{w}_2}\right)\right\} \\
&\quad \text{s.t.} \qquad \|\mathbf{w}_1\|^2 = \beta P_S, \\
&\qquad\qquad \|\mathbf{w}_2\|^2 = (1-\beta)P_S,
\end{aligned} \tag{3.41}$$

where $\mathbf{U}_1 \triangleq \frac{\sigma_{U_1}^2}{(1-\beta)P_S}\mathbf{I}+\mathbf{h}_{S,U_1}^*\mathbf{h}_{S,U_1}^T$, $\mathbf{U}_2 \triangleq \frac{\sigma_{U_2}^2}{\beta P_S}\mathbf{I}+\mathbf{h}_{S,U_2}^*\mathbf{h}_{S,U_2}^T$, $\mathbf{E}_1 \triangleq \frac{\sigma_{E_1}^2}{(1-\beta)P_S}\mathbf{I}+\mathbf{h}_{S,E_1}^*\mathbf{h}_{S,E_1}^T$, $\mathbf{E}_2 \triangleq \frac{\sigma_{E_2}^2}{\beta P_S}\mathbf{I}+\mathbf{h}_{S,E_2}^*\mathbf{h}_{S,E_2}^T$. The benefit of (3.41) is that given β, $\mathbf{w}_1$ and $\mathbf{w}_2$ can be optimized

separately. To be specific, the optimal $\mathbf{w}_1$ and $\mathbf{w}_2$ corresponds to the eigenvectors associated with the maximum eigenvalues of matrices $\mathbf{C} = \mathbf{L}_1^{-1}\mathbf{U}_1\mathbf{L}_1^{-H}$ and $\mathbf{D} = \mathbf{L}_2^{-1}\mathbf{U}_2\mathbf{L}_2^{-H}$ where $\mathbf{E}_1 = \mathbf{L}_1\mathbf{L}_1^H$ and $\mathbf{E}_2 = \mathbf{L}_2\mathbf{L}_2^H$, respectively. As a result, (3.41) can be simplified into

$$\begin{aligned}\max_{\substack{0<t_1<1\\0<t_2<1}} \ & \min\left\{I_{U_1}^{RL} - I_{E_1}^{RL}, t_2\log\left(\frac{\sigma_{E_2}^2}{\sigma_{U_2}^2}\lambda_{\max}\left(\mathbf{C}\right)\right)\right\} \\ & + \min\left\{I_{U_2}^{RL} - I_{E_2}^{RL}, t_3\log\left(\frac{\sigma_{E_1}^2}{\sigma_{U_1}^2}\lambda_{\max}\left(\mathbf{D}\right)\right)\right\}. \end{aligned} \tag{3.42}$$

Note that the constraints of (3.41) are dropped in (3.42) due to the homogeneity of the objective function. To solve (3.42), we introduce auxiliary variables as u_1 and u_2 to remove the "min" operators as

$$\begin{aligned} \max_{t_1,t_2,u_1,u_2} \quad & u_1 + u_2 \\ \text{s.t.} \quad & u_1 \le t_1 c, && \text{(3.43a)} \\ & u_1 \le t_2\log\left(\frac{\sigma_{E_2}^2}{\sigma_{U_2}^2}\lambda_{\max}\left(\mathbf{C}\right)\right), && \text{(3.43b)} \\ & u_2 \le t_1 d, && \text{(3.43c)} \\ & u_2 \le t_3\log\left(\frac{\sigma_{E_1}^2}{\sigma_{U_1}^2}\lambda_{\max}\left(\mathbf{D}\right)\right), && \text{(3.43d)} \\ & u_1, u_2 \ge 0, && \text{(3.43e)} \\ & 0 < t_1 < 1, 0 < t_2 < 1, && \text{(3.43f)} \end{aligned}$$

where

$$c \triangleq \log\frac{1+\frac{P_{U_1}\|\mathbf{h}_{U_1,S}\|^2}{\sigma_S^2}}{\left(1+\frac{P_{U_1}\left|h_{U_1,E_1}\right|^2}{\sigma_{E_1}^2}\right)}, \ d \triangleq \log\frac{1+\frac{P_{U_2}\|\mathbf{h}_{U_2,S}\|^2}{\sigma_S^2}}{\left(1+\frac{P_{U_2}\left|h_{U_2,E_2}\right|^2}{\sigma_{E_2}^2}\right)}, \tag{3.44}$$

and $t_3 = 1 - t_1 - t_2$. Clearly, it is a linear programming problem and can be optimally solved. After that, we use 1-D search to find the optimal power allocation parameter $\beta^\star$.

3.4 Simulation Results

In this section, we present numerical results to evaluate the secrecy rate of the XOR network coding based SATCOM protocol and compare it with the conventional scheme. We consider both i) equal RL and FL time allocation (ETA), and ii) optimized time

allocation between the RL and the FL (OTA). We use labels "XOR-ETA" and "XOR-OTA" to denote equal time allocation and optimal time allocation policies, respectively.

In our simulations, B denotes the carrier bandwidth, 41.67 kHz, for both RL and FL transmissions. Since there is a main direct link from the satellite to the users as well as some diffuse components, the channel from the satellite to the users can be modeled as Rician [225]. The K-factor for the FL is determined by the multipath average scattered power and random log-normal variable using the values provided by [225]. Due to the "scintillation" effect [226], we have multipath in the RL. Moreover, there exists a direct link like the FL case. Therefore, the RL can be considered to follow Rician distribution with a higher K-factor which is assumed to be 15 dB. The rest of the link parameters are summarized in Table 3.2 [227]. The satellite's FL transmission power in Table 3.2 shows the carrier power used in the following transmissions: 1) the broadcast in Phase IV of the XOR scheme or, 2) the transmissions in Phases IV and V of the conventional reference scheme. If the satellite's FL transmission power is not a variable in a simulation scenario, its value provided by Table 3.2 is used.

The ground channels between the users and the eavesdroppers are assumed to follow a Rayleigh distribution with the pathloss calculated by

$$L = 10 \log \left[\left(\frac{4\pi}{\lambda} \right)^2 d^{\gamma} \right], \tag{3.45}$$

where γ is the pathloss exponent which we assume to be $\gamma = 3.7$. The maximum Doppler shift is calculated using the following relation as

$$f_{D_{max}} = \frac{v}{\lambda} = \frac{v f_c}{c}, \tag{3.46}$$

where v is the user's speed, f_c is the maximum frequency used and c is the light speed.

Since the carrier bandwidth is 41.67 kHz, we assume that the RL operating bandwidth is $1616-1616.04167$ MHz for U_1, $1616.04367-1616.08534$ MHz for U_2 and the FL operating bandwidth is $1616 - 1616.04167$ MHz which is common between the users. Each user is supposed to move in a random direction with a 10 m/s speed. If not explicitly mentioned, each eavesdropper's distance to the user is randomly changed between 2 to 2.5 km.

We first show the average sum secrecy rate in Fig. 3.2 when the number of feeds used on the satellite varies from 3 to 10. As we can see, the XOR network coding scheme can achieve over 54% higher average sum secrecy rate than the conventional one. It can be observed that optimizing the RL and FL communication times improves the average sum secrecy rate for both schemes considerably, especially for the conventional scheme in higher number of feeds. The effect of time allocation is further illustrated in

TABLE 3.2: Link budget and parameters

Parameter	Value
Satellite orbit type	LEO
Operating band (1∼2 GHz)	L-band
RL and FL frequency band, MHz	1616-1626.5
Beams on the Earth	48
Number of antenna arrays	318
Frequency reuse factor (FRF)	12
Number of carriers per beam	20
Carrier bandwidth, B_c, kHz	41.67
Guard bandwidth, kHz	2
Satellite's antenna gain per beam, dBi	24.3
Total power at the satellite, dBW	31.46
Satellite noise temperature, K	290
Terminal noise temperature, K	321
Satellite's FL transmission power, dBW	7.65
Mobile device radiation power, dBW	0
Mobile device antenna gain, dBi	3.5
Return and forward link pathloss, dB	151
Doppler shift due to satellite velocity, Hz	270
Envelope mean of the direct wave, m_s	0.787
The variance of the direct wave, σ_s^2	0.0671
The power of the diffuse component	0.0456

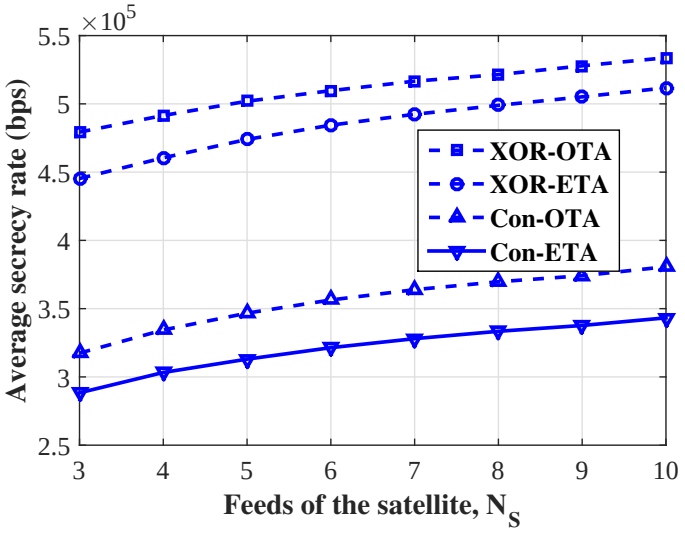


FIGURE 3.2: Average sum secrecy rate versus different number of feeds on the satellite for the XOR network coding and conventional schemes.

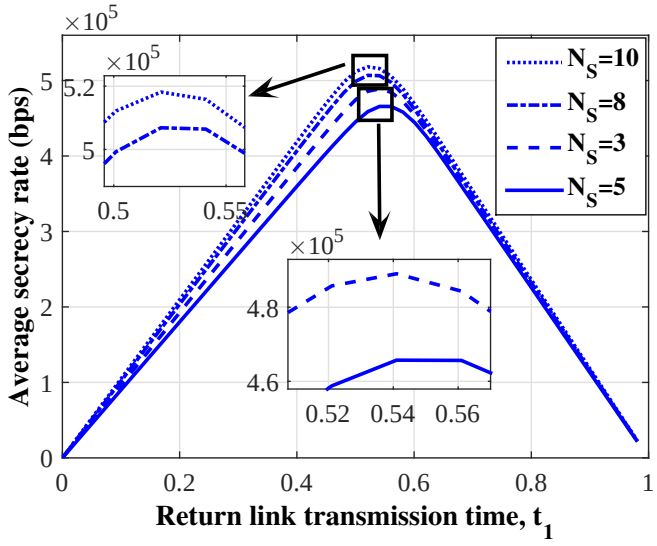


FIGURE 3.3: Average sum secrecy rate versus the RL time allocation t_1 in the XOR network coding scheme.

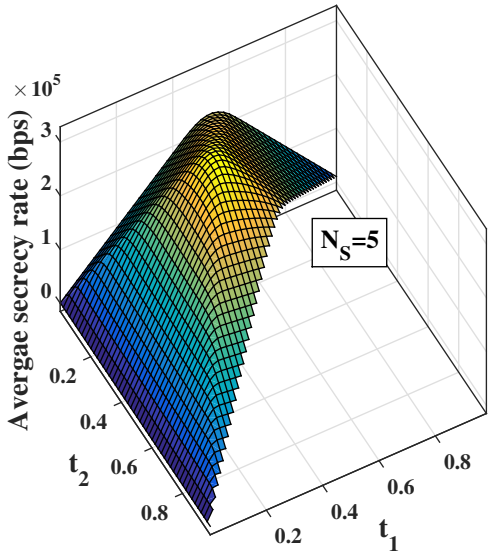


FIGURE 3.4: Average sum secrecy rate versus different RL, t_1, and FL, t_2 and $t_3 = 1 - t_1 - t_2$, time allocation in the conventional scheme.

Figs. 3.3 and 3.4 for the XOR network coding and the conventional schemes, respectively. It is observed in Fig. 3.3 that for different number of feeds, the average sum secrecy rate first increases, and then then decreases with the RL time allocation t_1. Here, more time is allocated to the RL transmission which means that the FL transmission rate is a bottleneck for the end-to-end rate. The time split between the RL and FL depends on the number of feeds at the satellite. As the number of feeds increases, the time devoted to the FL transmission increases. This shows that the FL acts as a bottleneck for the end-to-end communications. The change in the RL and FL time allocation makes the channel secrecy rates closer to each other so that the overall average secrecy

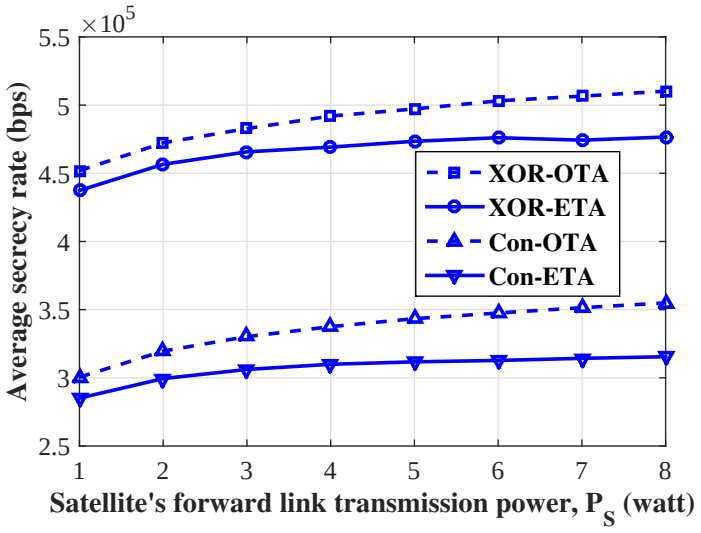


FIGURE 3.5: Average sum secrecy rate versus the satellite's forward link transmission power.

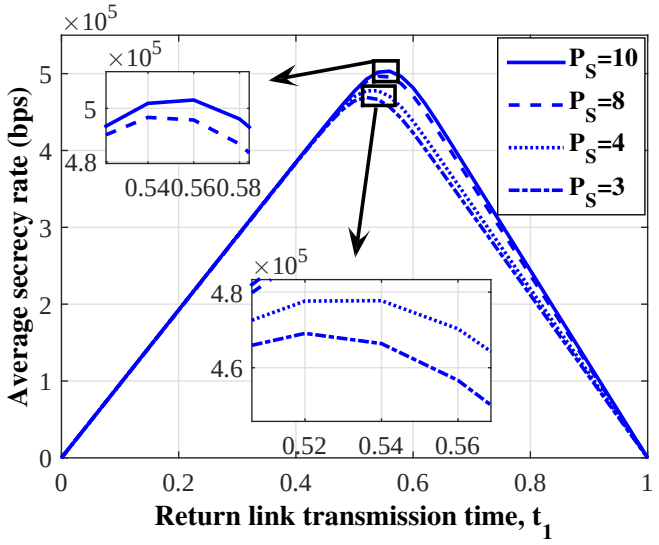


FIGURE 3.6: Average sum secrecy rate versus RL time allocation for different satellite's forward link transmission powers.

rate increases. The optimal time allocation for one RL slot and two FL slots in the conventional scheme can be seen in Fig. 3.4.

The effect of the satellite's FL transmission power on the average secrecy rate is investigated in Figs. 3.5 and 3.6. In Fig. 3.5, we see that the average secrecy rate for the equal time allocation approach in both schemes starts to saturate as the available power for the FL transmission increases. This can be explained by the fact that as the available power increases, the RL becomes a bottleneck for the end-to-end secrecy rate and hinders the overall improvement. On the other hand, while performing optimal time allocation over RL and FL, the average secrecy rate keeps growing for both the conventional and the

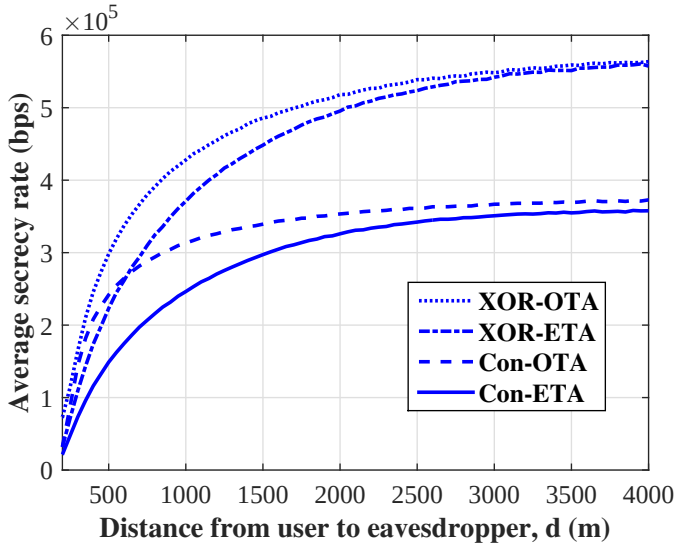


FIGURE 3.7: Average sum secrecy rate versus the distance between the user and the eavesdropper for XOR network coding and conventional schemes while equal and optimal time allocation are employed.

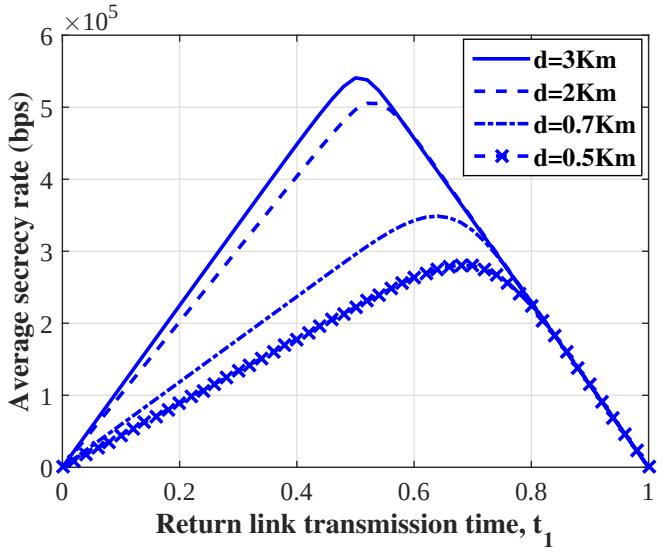


FIGURE 3.8: Average sum secrecy rate versus different RL and FL time allocation in XOR network coding scheme for different distances between the user and eavesdropper.

XOR network coding schemes. It is seen in Fig. 3.6 that by increasing the power at the satellite, more time is allocated to the RL transmission in order to balance the RL and FL secrecy rates and sustaining the secrecy rate growth. However, after increasing the satellite's power beyond a specific point, the effect of the optimal time allocation fades out, and the average secrecy rate in the optimal time allocation scheme also saturates due to RL being a bottleneck. This fact can be observed in Fig. 3.6. As the power of the FL transmission increases, less time is exchanged between the RL and FL transmission and the average secrecy rate saturates. The effect of the distance between each user and the corresponding eavesdropper is investigated in Figs. 3.7 and 3.8. As is seen in

Fig. 3.7, the average secrecy rate for equal time allocation in both schemes saturates as the distance between the user and eavesdropper increases. This is because increasing the distance to the eavesdropper improves the secrecy rate in the RL, leaving the FL as a performance bottleneck. When the time allocation is optimized, the average secrecy rate shows notable gain in both schemes. However, after a specific distance, the secrecy rate for the optimal power allocation also saturates. Increasing the distance to the eavesdropper increases the secrecy rate for the RL, but this increment is going to be quite small at some point and consequently vanishes. Consequently, as the distance increases, less time exchange is required between the RL and FL transmission. This fact can be seen in Fig. 3.8. Due to this limit in the RL secrecy rate, the secrecy rate can be improved using optimal time allocation up to a limited distance. Furthermore, as it is observed in Fig. 3.7, the average sum secrecy rate of the XOR network coding saturates in a much longer distance compared to the conventional scheme. Interestingly, when the user and the eavesdropper are close, the conventional scheme using the optimal time allocation outperforms the XOR network coding scheme using equal time allocation. This originates from the fact that there are more degrees of freedom in terms of optimal time allocation in the conventional scheme compared to the XOR network coding scheme. Hence, when it comes to picking up a secure protocol, distance plays an important role.

The results in Fig. 3.8 illustrate that as the distance between the user and the eavesdropper decreases, more time is allocated to the RL transmission of the XOR network coding scheme in order to balance the secrecy rates in RL and FL. It is observed that as the distance to the eavesdropper increases, less change is required in the RL and FL times. This is due to the fact that as the distance increases, the improvement rate in the secrecy rate of the RL is reduced and less regulation is required in the transmission times.

3.5 Conclusion

In this chapter, we studied the sum secrecy rate of SATCOM network where XOR network coding is used for bidirectional information transmission. We designed the satellite's antenna beamforming weights at the GW and transmit them to the satellite via an ideal feeder link. The beamforming weights as well as the RL and FL time allocations were designed to maximize the sum secrecy rate of the users. We also designed the beamformer as well as the optimal time allocation for RL and FL to maximize the sum secrecy rate for the one way conventional SATCOM scheme. Simulations showed that the sum secrecy rate of the network coded SATCOM is considerably more than the conventional SATCOM in most of the scenarios, especially when the legitimate users and

the eavesdroppers are not close. We observed that increasing the satellite's transmission power will saturate the sum secrecy rate for equal RL and FL time allocation, whereas it increases the sum secrecy rate of the optimal time allocation.

Chapter 4

Power Control in Wiretap Interference Channels

Interference in wireless networks degrades the signal quality at the terminals. However, it can potentially enhance the secrecy rate. This chapter investigates the secrecy rate in a two-user interference network where one of the users, namely user 1, requires to establish a confidential connection. User 1 wants to prevent an unintended user of the network to decode its transmission. User 1 has to transmit such that its secrecy rate is maximized while the quality of service at the destination of the other user, user 2, is satisfied, and both user's power limits are taken into account. We consider two scenarios: 1) user 2 changes its power in favor of user 1, an altruistic scenario, 2) user 2 is selfish and only aims to maintain the minimum quality of service at its destination, an egoistic scenario. It is shown that there is a threshold for user 2's transmission power that only below or above which, depending on the channel qualities, user 1 can achieve a positive secrecy rate. Closed-form solutions are obtained in order to perform joint optimal power control. Further, a new metric called secrecy energy efficiency is introduced. We show that in general, the secrecy energy efficiency of user 1 in an interference channel scenario is higher than that of an interference-free channel. The contributions of this chapter are published in [21].

4.1 Introduction

Broadcasting information over the same frequency band in wireless networks leads to interference among users. Even in the systems where the spatial dimension is used to concentrate the signal towards the intended destination, the destination may receive interfering signals from other transmitters operating in the same frequency band. Also, due

to the expansion and deployment of wireless services, the spectrum is getting scarce [15]. As one possible solution, devices can share the same spectrum which results in interference and degradation of the signal quality. For instance, IEEE standards such as WiFi, Zigbee and Bluetooth share the same frequency band named the industrial, scientific and medical (ISM) band and they may interference with each other [16]. Furthermore, the wireless medium leaves the information vulnerable to unintended users who can potentially decode the message which was meant for other users. Throughout this chapter, the words "wiretapper", or "eavesdropper" refer to the unintended users. While there are higher layer cryptography techniques to secure the data, it is yet possible that a malicious agent breaks into the encryption and gets access to the data [3]. By intelligently tuning the system parameters using physical layer security techniques, we can prevent the wiretappers from getting access to the information and this way, and further improve the system security along other techniques. Consequently, a specific rate can be perfectly secured for the users to transmit their data, so that the wiretapper is not able to decode the message. There are efficient coding schemes which can achieve this rate. However, this area is still in its infancy, and the research effort at the moment is inclined in implementing practical codes [6].

Potentially, the interference can improve the secrecy rate by introducing extra interference at the eavesdropper. The possibility of secure transmission in a multi-user interference channel using interference alignment and secrecy pre-coding is investigated in [98]. The authors of [94] investigate the secrecy rate in a two-user interference channel with an external eavesdropper. They show structured transmission results in a better secrecy rate compared to randomly generated Gaussian codebooks. The authors of [95] study the secrecy capacity region for a two-user interference channel in the presence of an external eavesdropper. The users jointly design randomized codebooks and inject noise along with data transmission to improve the secrecy rate. The authors of [96] consider a user who gets helping interference in order to increase its confidentiality against an eavesdropper. The achievable secrecy rate for both discrete memoryless and Gaussian channels is derived. A two-user interference network with an unintended user is considered in [97]. Depending on the channel conditions, bounds on the transmission power of the interfering user is derived such that a positive secrecy rate is sustained for the other user.

As an example of the interference channel, the effect of interference on the secrecy rate is also investigated in cognitive radio systems. In cognitive radios, secondary user transmits in the primary user's operating frequency band when it is not in use. Stochastic geometry is used in [106] to analyze physical layer secrecy in a multiple node cognitive radio network where an eavesdropper is present. The secrecy outage probability and the secrecy rate of the primary user is derived while secondary user produces interference.

The authors of [108] maximize the secrecy rate for a multiple-antenna secondary user in the presence of an external eavesdropper while considering the quality of service (QoS) at the primary receiver. Similar problems to maximize the secrecy rate through beamforming design in cognitive radio are studied in [110–112].

4.1.1 Contributions and main results

In this work, we investigate the secrecy rate in a two-user wireless interference network. Apart from the two users, one of the idle users (unintended user) in this network is a potential eavesdropper. Both nodes transmit in a way so that the secrecy rate is maximized for the first user (user 1), and the second user (user 2) maintains the QoS at its intended destination. Only user 1 needs to establish a secure connection and to keep its data secure. For example, in a network with ISM band users, user 1 and user 2 can be WiFi and ZigBee transmitters. The ZigBee can be used to send measurement data, which is one of its applications, so its data may not be necessarily important to the potential eavesdropper who is interested in WiFi messages.

The effect of interference from user 2 on the secrecy rate of user 1 is studied in two scenarios, namely altruistic and egoistic scenarios. In the altruistic scenario, we jointly optimize the transmission powers of both users in order to maximize the secrecy rate of user 1, while maintaining the QoS at user 2's destination equal or above a specific threshold. The incentives for user 2 to cooperate are twofold: 1) when positive secrecy rate cannot be granted for user 1, it can enjoy an interference-free transmission, 2) user 1 adjusts its transmission power to maintain the QoS of user 2's destination equal or above the threshold. In the egoistic scenario, the users' powers are still jointly optimized. However, user 2 is selfish and only tries to maintain the minimum QoS at the corresponding destination. The contributions of our work are as follows. It is shown that by appropriate control of user 1's power, we can make sure that the eavesdropper cannot decode the signal of user 2, and thus cannot employ successive interference cancellation (SIC). Also, it is shown that the transmitted power from user 2 has a crucial role in achieving a positive secrecy rate for user 1. According to the channel conditions, we define the proper power transmission for user 2 to maintain a positive secrecy rate for user 1. We develop closed-form expressions to implement joint optimal power control for both users in both altruistic and egoistic scenarios. Finally, a new metric called "secrecy energy efficiency" is defined, which is the secrecy rate over the consumed power ratio. Using the new metric, it is shown that the interference channel can outperform the single-user channel for specific values of QoS requirements.

4.1.2 Related Work

Inner and outer bounds for the secrecy capacity regions in a two-user interference channel with destinations as eavesdroppers are investigated in [73]. They showed that the secrecy capacity can be enhanced when one user transmits signal with artificial noise. Later, [73] was extended to the case when both users transmit artificial noise along with data in [76]. As a result, they achieve a larger secrecy rate region when one or both destinations are considered as eavesdropper. In [71], an outer bound for secrecy capacity region is calculated for a two-user one-sided interference channel. Outer bounds on sum rate of a two-user Gaussian interference channel are studied in [77] where message confidentiality is important for users. Secrecy capacity region for a two-user MIMO Gaussian interference channel is investigated in [78] where each receiver is a potential eavesdropper. A two-user symmetric linear deterministic interference channel is investigated in [99]. The achievable secrecy rate is investigated when interference cancelation, cooperation, time sharing, and transmission of random bits are used. It is shown that sharing random bits achieves a better secrecy rate compared to sharing data bits. A two-user MISO interference channel is considered in [85] where beamforming is performed to maintain fair secrecy rate. The work in [177] analyzes a two-user interference channel with one-sided noisy feedback. Rate-equivocation region is derived when the second user's message needs to be kept secret. The secrecy rate constrained to secrecy rate outage probability and power is maximized by designing robust beamformer in [66] where a transceiver pair and multiple eavesdroppers constitute a network.

A multiple-user interference channel where only one user as a potential eavesdropper receives interference is considered in [81]. The sum secrecy rate is derived using nested lattice codes. The authors in [100] consider a wireless network comprised of users, eavesdroppers and interfering nodes. It is shown that interference can improve secrecy rate. A communication network comprised of multiple-antenna base stations and single-antenna users is considered in [86]. The total transmit power is minimized while the signal-to-interference plus noise ratio and equivocation rate for each user is satisfied.

In [72], a two-user network with one-sided-interference where each destination is a potential eavesdropper for the other one is studied. Using game theory, it is concluded that depending on the objective of each pair, the equilibrium can include or exclude the self-jamming strategy. The authors of [84] analyze a two-user MISO Gaussian interference channel where each destination is a potential eavesdropper. Game theory is used to tackle the scenario where each user tries to maximize the difference between its secrecy rate and the secrecy rate of the other user. Beamformers under full and limited channel information are designed at each transmitter to achieve this goal.

A transceiver pair is studied in [101] where they try to increase the secrecy rate using an external interferer when a passive eavesdropper is present. The authors of [102] consider a user and an eavesdropper where known interference which only degrades the decoding ability at the eavesdropper is used to enhance the secrecy capacity. The secrecy capacity and secrecy outage capacity when closest interfering node and multiple interfering nodes are separately employed to prevent eavesdropping is studied in [103]. It is demonstrated that multiple interferes method is superior to the closet interfering method. The exact secure degrees of freedom for different types of Gaussian wiretap channels are discussed in [104] where cooperative jamming from helpers is used.

The equivocation-rate for a cognitive interference network is considered in [107] where the primary receiver is a potential eavesdropper and should not decode the secondary message. A MISO transceiver along with multiple single-antenna eavesdroppers are considered in [48]. The relationship of the mentioned network with interference cognitive radio network is used to design the transmit covariance matrix. In [109], the secondary user causes interferes to both primary destination and eavesdropper. Primary user tries to maintain its secrecy rate while the secondary aims to increase its rate. The achievable pair rate for both users is derived.

4.2 System model

4.2.1 Signal Model

We consider a wireless interference network consisting of two users denoted by U_1 and U_2, two destinations denoted by D_1 and D_2, and one user as the eavesdropper denoted by E. E is assumed to be passive during U_1 and U_2 transmission and active outside the mentioned period. All nodes employ one antenna for data communication. We denote by x_1 and x_2, the messages which are sent over the same frequency band from U_1 and U_2 to D_1 and D_2, respectively. Sharing the same frequency band by the users leads to cross-interference. While the users send data, their signals are wiretapped by the eavesdropper, E. The network setup is depicted in Fig. 4.1. Here, we consider a scenario where E is only interested in the data sent by one of the users, namely U_1. As a result, x_2 is considered as an interfering signal at both D_1 and E.

There are two ways in order to carry out the joint power allocation: 1) users send their channel information to a fusion center. At the fusion center, the optimal power values are calculated and sent back to the users separately, 2) one of the users sends its channel information to the other user who calculates the optimal power values and sends the optimal power value to the corresponding user. It can be seen that the first

approach consumes more time and number of transmissions compared to the second one. Since U_1 is interested in sustaining a positive secrecy rate, it is fair if this user pays the computational cost. Hence, we assume that U_2 sends the channels data to U_1 and then U_1 calculates the optimal power values and sends back the related optimal power value to U_2. To perform channel estimation in the network, one approach is that the destinations, including the unintended user, send pilots and the transmitters are then able to estimate the required CSIs. After estimating the channels, U_2 forwards the required CSIs to U_1. U_1 is then responsible to perform the power control and inform U_2 of the optimal power that it can transmit. Note that in practice, it is often optimistic to have such a model, as the eavesdroppers are often totally passive. But here, we assume that the eavesdropper is momentarily active, and thus its channel can be estimated and remains unchanged for the optimal power control usage. One practical example of such a scenario is when the eavesdropper is a known user in a network such that U_1's messages should be kept confidential from it.

The received signals at D_1 and D_2 are as follows

$$y_{D_1} = \sqrt{P_1} h_{U_1,D_1} x_1 + \sqrt{P_2} h_{U_2,D_1} x_2 + n_{D_1}, \tag{4.1}$$

$$y_{D_2} = \sqrt{P_2} h_{U_2,D_2} x_2 + \sqrt{P_1} h_{U_1,D_2} x_1 + n_{D_2}, \tag{4.2}$$

where P_1 and P_2 are the power of the transmitted signals by U_1 and U_2, and h_{U_i,D_j} is the channel gain from each user to the corresponding destination for $i = 1, 2$ and $j = 1, 2$. The transmission signal from the i-th user, and the additive white Gaussian noise at the i-th destination are shown by $\sqrt{P_i} x_i$ and n_{D_i} for $i = 1, 2$, respectively. The random variables x_i and n_{D_i} are independent and identically distributed (i.i.d.) with $x_i \sim \mathcal{CN}(0, 1)$ and $n_{D_i} \sim \mathcal{CN}(0, \sigma_n^2)$, respectively, where $\mathcal{CN}$ denotes the complex normal random variable. In practice, some signals follow Gaussian distribution such as the amplitude of sample distributions of OFDM signal [228]. Using a Gaussian distributed signal may not always be optimal, however, our focus is on maximizing the secrecy rate by designing joint optimal power allocation in a specific system model. The wiretapped signal at E is

$$y_E = \sqrt{P_1} h_{U_1,E} x_1 + \sqrt{P_2} h_{U_2,E} x_2 + n_E, \tag{4.3}$$

where $h_{U_i,E}$ is the channel coefficient from the i-th user to the eavesdropper for $i = 1, 2$, and n_E is the additive white Gaussian noise at the eavesdropper with the same distribution as n_{D_i}. The additive white Gaussian noise at different receivers are assumed to be mutually independent.

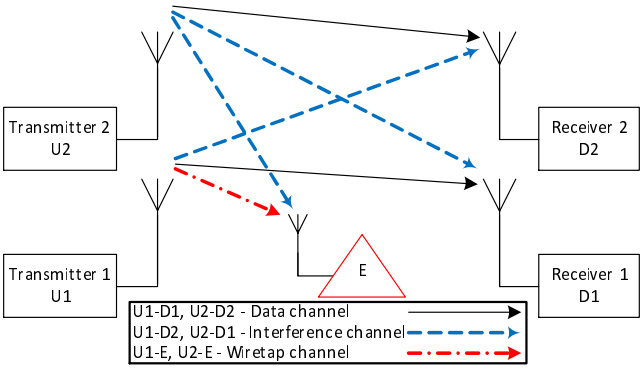


FIGURE 4.1: Two-user wireless interference network.

4.2.2 Secrecy rate of U_1

In order to calculate the secrecy rate of U_1, we need to first find the rate of U_1 without considering the secrecy, and then the rate in which the eavesdropper wiretaps U_1. In this chapter, we assume that U_1 and U_2 do not employ SIC. Therefore, using (4.1) and (4.2), the rates for each user to the corresponding destination can be calculated as

$$I_{U_1-D_1} = \log_2\left(1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}\right), \tag{4.4}$$

$$I_{U_2-D_2} = \log_2\left(1+\frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2+\sigma_n^2}\right). \tag{4.5}$$

The eavesdropper simultaneously receives signals from U_1 and U_2 which are transmitting in the same frequency band. Hence, the channel from users towards the eavesdropper can be modeled by a multiple-access channel. Assume that the transmission powers of U_1 and U_2 in a specific time slot are P_1 and P_2. Then, considering that users employ Gaussian codebooks and the eavesdropper tends to achieve the maximum wiretapping rate from U_1, the rate pairs achieved at the eavesdropper are shown in Fig. 4.2 [229] which lie on the line from point "$\mathcal{A}$" to point "$\mathcal{D}$". To wiretap U_1 with the maximum achievable rate, the eavesdropper can employ the SIC method [221]. Using SIC, the eavesdropper first decodes the signal from U_2 while considering U_1's signal as interference. Then, considering the fact that the signal from U_2 is decoded and known, eavesdropper deducts U_2's signal from the received signal and gets an interference-free signal from U_1. In this approach, the rate pairs on the line "$\mathcal{CD}$" are achieved at the eavesdropper if the transmission rate of U_2, defined by R_2, is lower than the decode-able rate defined at point "$\mathcal{G}$". To prevent the eavesdropper from achieving the maximal wiretapping rate, U_2's transmission rate needs to be higher than the decode-able rate at point "$\mathcal{G}$". Since users do not coordinate in order to implement time-sharing or rate-splitting, U_1's signal cannot be decoded with the rates which are on the line "$\mathcal{DE}$", and thus it needs to

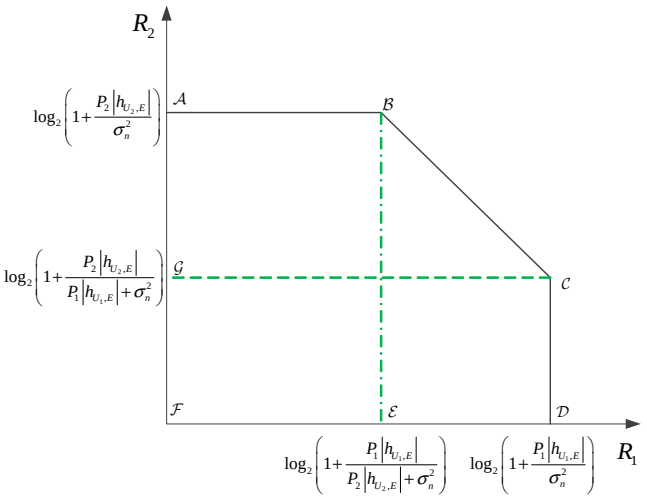


FIGURE 4.2: Maximum achievable rate pairs of a two-user multiple-access fading channel.

decode U_1 considering U_2 as the interference with a rate equal to the rate at point "$\mathcal{E}$". Therefore, to disable the eavesdropper from performing SIC (i.e., achieving rate at point "$\mathcal{D}$"), the following condition needs to hold:

$$\begin{aligned} R_2 =& \log_2\left(1+\frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2+\sigma_n^2}\right) \\ &> \log_2\left(1+\frac{P_2|h_{U_2,E}|^2}{P_1|h_{U_1,E}|^2+\sigma_n^2}\right). \end{aligned} \tag{4.6}$$

In (4.6), the left-hand side is the actual transmission rate of U_2 which is equal to the decode-able rate at its destination, D_2 . If condition (4.6) is satisfied, the eavesdropper has to decode U_1's signal by considering U_2's signal as interference. Interestingly, satisfying condition (4.2) just needs U_1 to adjust its transmission power and is independent from P_2. The condition on P_1 to satisfy (4.6) is derived as:

$$P_1 > \frac{A''}{B''} \quad \text{if} \quad A'' > 0, B'' > 0, \tag{4.7g}$$

$$P_1 > 0 \quad \text{if} \quad A'' < 0, B'' > 0, \tag{4.7h}$$

$$P_1 < \frac{A''}{B''} \quad \text{if} \quad A'' < 0, B'' < 0, \tag{4.7i}$$

$$P_1 < 0 \text{ (not feasible)} \quad \text{if} \quad A'' > 0, B'' < 0, \tag{4.7j}$$

where $A'' = \sigma_n^2\left(|h_{U_2,E}|^2 - |h_{U_2,D_2}|^2\right)$ and $B'' = |h_{U_2,D_2}|^2|h_{U_1,E}|^2 - |h_{U_1,D_2}|^2|h_{U_2,E}|^2$. As we can see, the channel conditions define whether U_1 can block the eavesdropper by adjusting its power. For the Cases 4.7g, 4.7h, and 4.7i, the instantaneous wiretap rate from U_1 toward E is obtained by $I_{U_1-E} = \log_2\left(1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}\right)$, and thus the

secrecy rate of U_1 in this case is as follows

$$C_{S_{U_1}} = I_{U_1-D_1} - I_{U_1-E} = \log_2\left(1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}\right) - \log_2\left(1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}\right). \tag{4.8}$$

For Case 4.7j, no power from U_1 is capable of preventing the eavesdropper from applying the SIC technique and deriving an interference-free version of U_1's signal and thus $I_{U_1-E} = \log_2\left(1+\frac{P_1|h_{U_1,E}|^2}{\sigma_n^2}\right)$. This results in the following secrecy rate

$$C_{S_{U_1}} = I_{U_1-D_1} - I_{U_1-E} = \log_2\left(1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}\right) - \log_2\left(1+\frac{P_1|h_{U_1,E}|^2}{\sigma_n^2}\right). \tag{4.9}$$

In the next two sections, we formulate and solve the underlying problems so as to find the optimal P_1 and P_2.

4.3 Problem Formulation: Altruistic Scenario

In this section, we maximize the secrecy rate of U_1 subject to the peak power limits of the users as well as the quality of service (QoS) at D_2. If one of the cases 4.7g, 4.7h, or 4.7i holds, using (4.8), the following secrecy rate optimization is solved:

$$\begin{aligned} &\max_{P_1,P_2} \ C_{S_{U_1}} \\ &\text{s.t.} \quad P_1 \le P_{\max_1},\ P_1 \underset{(4.7i)}{\overset{(4.7g)}{\gtrless}} \omega,\ P_2 \le P_{\max_2},\ I_{U_2-D_2} \ge \beta, \end{aligned} \tag{4.10}$$

where β is the minimum required data rate for U_2 and $\omega = \frac{A''}{B''}$. In Case 4.7h, any P_1 ensures that the eavesdropper cannot employ SIC. Therefore, no additional constraint over P_1 is necessary. For Case 4.7j, using (4.9), the following secrecy rate optimization problem should be solved

$$\begin{aligned} &\max_{P_1,P_2} \ C_{S_{U_2}} \\ &\text{s.t.} \quad P_1 \le P_{\max_1},\ P_2 \le P_{\max_2},\ I_{U_2-D_2} \ge \beta. \end{aligned} \tag{4.11}$$

We first solve (4.10) and then (4.11). By inserting (4.8) into (4.10), we obtain

$$\begin{aligned}
\max_{P_1,P_2} \quad & \log_2 \left(\frac{1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}}{1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}} \right) \\
\text{s.t.} \quad & P_1 \le P_{\max_1},\ P_1 \underset{(4.7i)}{\overset{(4.7g)}{\gtrless}} \omega,\ P_2 \le P_{\max_2}, \\
& \frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2+\sigma_n^2} \ge \gamma,
\end{aligned} \tag{4.12}$$

where γ is $2^\beta - 1$. Since log is a monotonic increasing function of its argument, we can just maximize the argument and thus we rewrite (4.12) as

$$\begin{aligned}
\max_{P_1,P_2} \quad & \frac{1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}}{1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}} \\
\text{s.t.} \quad & P_1 \le P_{\max_1},\ P_1 \underset{(4.7i)}{\overset{(4.7g)}{\gtrless}} \omega,\ P_2 \le P_{\max_2}, \\
& \frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2+\sigma_n^2} \ge \gamma.
\end{aligned} \tag{4.13}$$

Considering that the objective function is neither convex, nor concave, solving problem (4.13) is difficult. As a result, we shall adopt a two-step approach in order to solve (4.13). First, we consider P_2 to be fixed and derive the optimal value for P_1, and then we replace the obtained P_1 in (4.13) and solve the optimization problem for P_2.

4.3.1 Optimizing P_1 for a Given P_2

For this case, (4.13) is reduced to

$$\begin{aligned}
\max_{P_1} \quad & \frac{1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}}{1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}} \\
\text{s.t.} \quad & P_1 \le P_{\max_1},\ P_1 \underset{(4.7i)}{\overset{(4.7g)}{\gtrless}} \omega,\ P_1 \le \frac{P_2|h_{U_2,D_2}|^2-\gamma\sigma_n^2}{\gamma|h_{U_1,D_2}|^2}.
\end{aligned} \tag{4.14}$$

In order to solve (4.14), first, we find the range of P_2 for which the objective function in (4.14) is always positive, i.e., a positive secrecy rate can be achieved. In the following theorem, we outline the related bounds on P_2 where the positive secrecy rate is obtained.

Theorem 4.1. *Assume an interference network similar to the one mentioned in Fig. 4.1 along with the assumptions on power limits and the QoS. In order to achieve a positive secrecy rate, P_2 should satisfy the following bounds:*

$$P_2 > \frac{A}{B} \quad \text{if} \quad A > 0, B > 0, \tag{4.15k}$$

$$P_2 > 0 \quad \text{if} \quad A < 0, B > 0, \tag{4.15l}$$

$$P_2 < \frac{A}{B} \quad \text{if} \quad A < 0, B < 0, \tag{4.15m}$$

where $A = \sigma_n^2 \left(|h_{U_1,E}|^2 - |h_{U_1,D_1}|^2 \right)$ *and* $B = |h_{U_1,D_1}|^2 |h_{U_2,E}|^2 - |h_{U_2,D_1}|^2 |h_{U_1,E}|^2$. *Further, for* $A > 0, B < 0$, *irrespective of the value of* P_2, *no positive secrecy rate can be obtained for* U_1.

Proof. The proof is given in Appendix B. □

One immediate conclusion of Theorem 4.1 is given by the following corollary which can be considered as the most important result of this chapter.

Corollary 4.2. *In a wiretap interference channel as in Fig. 4.1, where the goal is to obtain a positive secrecy rate for U_1, the possibility of achieving a positive secrecy rate is independent from the value of P_1, and depends on the value of P_2 and the conditions of the channels.*

Now that we have defined the required conditions for P_2 to achieve a positive secrecy rate, we investigate the optimal value of P_1, denoted by $P_1^\star$ for a given P_2. If we take the derivative of the objective function in (4.14) with respect to P_1, we see that the conditions on P_2 to have a monotonically increasing, referred to as Case 1, or decreasing, referred to as Case 2, are the same as the conditions to have a positive or negative secrecy rate, respectively. These conditions are summarized as follows

$$\begin{aligned}
&P_{2_{(1)}} > \frac{A}{B},\ P_{2_{(2)}} < \frac{A}{B} && \text{if} \quad A > 0, B > 0,\\
&P_{2_{(1)}} = \emptyset,\ P_{2_{(2)}} > 0 && \text{if} \quad A > 0, B < 0,\\
&P_{2_{(1)}} > 0,\ P_{2_{(2)}} = \emptyset && \text{if} \quad A < 0, B > 0,\\
&P_{2_{(1)}} < \frac{A}{B},\ P_{2_{(2)}} > \frac{A}{B} && \text{if} \quad A < 0, B < 0,
\end{aligned} \tag{4.16}$$

where $P_{2_{(1)}}$ refers to the required power in Case 1, $P_{2_{(2)}}$ refers to the required power in Case 2 and $\emptyset$ denotes the empty set. According to Theorem 4.1, and the conditions in (4.16), the global optimal values for P_1 in Cases 1 and 2 are defined as

1. If the objective function in (4.10) is monotonically increasing, then

$$P_1^\star = \min\left\{\chi, \frac{P_2|h_{U_2,D_2}|^2 - \gamma\sigma_n^2}{\gamma|h_{U_1,D_2}|^2}\right\}. \tag{4.17}$$

   where $\chi = P_{\max_1}$ for Cases 4.7g and 4.7h, $\chi = \min\{P_{\max_1}, \omega\}$ for Case 4.7i.

2. If the objective function in (4.10) is monotonically decreasing, then $P_1^\star = 0$. This could also be concluded from the fact that when a positive secrecy rate cannot be granted, U_1 should be turned off.

4.3.2 Optimizing P_2 for a Given P_1

We insert the $P_1^\star$ obtained in Subsection 4.3.1 into (4.14), and try to obtain the optimal value for P_2. First, we decompose the optimal answer of P_1 in (4.17) into two different answers as follows

$$P_1^\star = \begin{cases} \chi & P_2 \geq \frac{\gamma\left(\chi|h_{U_1,D_2}|^2+\sigma_n^2\right)}{|h_{U_2,D_2}|^2}, \\ \frac{P_2|h_{U_2,D_2}|^2-\gamma\sigma_n^2}{\gamma|h_{U_1,D_2}|^2} & P_2 < \frac{\gamma\left(\chi|h_{U_1,D_2}|^2+\sigma_n^2\right)}{|h_{U_2,D_2}|^2}. \end{cases} \tag{4.18}$$

Using Theorem 4.1 and according to the two resulting cases in (5.24), we can break (4.13) into two problems in order to optimize P_2, respectively, as follows

$$\begin{aligned} \max_{P_2} \quad & \frac{1+\frac{P_{\max_1}|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}}{1+\frac{P_{\max_1}|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}} \\ \text{s.t.} \quad & P_2 \leq P_{\max_2},\ P_2 \geq \frac{\gamma\left(\chi|h_{U_1,D_2}|^2+\sigma_n^2\right)}{|h_{U_2,D_2}|^2} = \lambda_1, \\ & P_2 \underset{(4.15\text{m})}{\overset{(4.15\text{k})}{\gtrless}} \frac{\sigma_n^2\left(|h_{U_1,E}|^2-|h_{U_1,D_1}|^2\right)}{|h_{U_1,D_1}|^2|h_{U_2,E}|^2-|h_{U_2,D_1}|^2|h_{U_1,E}|^2} = \varphi_1, \end{aligned} \tag{4.19}$$

and

$$\max_{P_2} \quad \frac{1+\frac{\left(P_2\left|h_{U_2,D_2}\right|^2-\gamma\sigma_n^2\right)\left|h_{U_1,D_1}\right|^2}{\gamma\left|h_{U_1,D_2}\right|^2\left(P_2\left|h_{U_2,D_1}\right|^2+\sigma_n^2\right)}}{1+\frac{\left(P_2\left|h_{U_2,D_2}\right|^2-\gamma\sigma_n^2\right)\left|h_{U_1,E}\right|^2}{\gamma\left|h_{U_1,D_2}\right|^2\left(P_2\left|h_{U_2,E}\right|^2+\sigma_n^2\right)}}$$

$$\text{s.t.} \quad P_2 \le P_{\max_2},\ P_2 < \frac{\gamma\left(\chi\left|h_{U_1,D_2}\right|^2+\sigma_n^2\right)}{\left|h_{U_2,D_2}\right|^2} = \lambda_1,$$

$$P_2 \ge \frac{\gamma\sigma_n^2}{\left|h_{U_2,D_2}\right|^2} = \lambda_2,$$

$$P_2 \underset{(4.15m)}{\overset{(4.15k)}{\gtrless}} \frac{\sigma_n^2\left(\left|h_{U_1,E}\right|^2-\left|h_{U_1,D_1}\right|^2\right)}{\left|h_{U_1,D_1}\right|^2\left|h_{U_2,E}\right|^2-\left|h_{U_2,D_1}\right|^2\left|h_{U_1,E}\right|^2} = \varphi_1, \tag{4.20}$$

for $A \underset{(4.15m)}{\overset{(4.15k)}{\gtrless}} 0$ and $B \underset{(4.15m)}{\overset{(4.15k)}{\gtrless}} 0$. For the case $A < 0$ and $B > 0$ which is represented by (4.15l), the last constraint in (4.19) and (4.20) is removed from the problem since with any positive value for P_2, U_1 can have a positive secrecy rate. Also for $A > 0$ and $B < 0$, the secrecy rate is simply zero since $P_1 = 0$. Furthermore, the numerator and denumerator in (4.20) have the possibility to become less than unit and this leads to a negative rate. The constraint in (4.20) which is placed one to the last, ensures that the data and wiretap rates do not go below zero.

We discuss the feasibility conditions of (4.19) and (4.20) to derive the feasibility domain, p_2, in Proposition 4.3.

Proposition 4.3. *The feasibility domain for the problems* (4.19) *and* (4.20) *denoted by* p_2 *is defined as follows*

1. *Problem* (4.19)*: For case* (4.15k)*, we should have* $\max\{\lambda_1, \sup\varphi_1\} \le P_{\max_2}$ *which leads to* $p_2 = [\max\{\lambda_1, \sup\varphi_1\}, P_{\max_2}]$*. For case* (4.15m)*, we should have* $\min\{\inf\varphi_1, P_{\max_2}\} \ge \lambda_1$ *which leads to* $p_2 = [\lambda_1, \min\{\inf\varphi_1, P_{\max_2}\}]$.
2. *Problem* (4.20)*: For case* (4.15k)*, we should have* $\max\{\sup\varphi_1, \lambda_2\} \le \min\{\inf\lambda_1, P_{\max_2}\}$ *which leads to* $[\max\{\sup\varphi_1, \lambda_2\}, \min\{\inf\lambda_1, P_{\max_2}\}]$*. For case* (4.15m)*, we should have* $\min\{\inf\varphi_1, \inf\lambda_1, P_{\max_2}\} \ge \lambda_2$ *which leads to* $p_2 = [\min\{\inf\varphi_1, \inf\lambda_1, P_{\max_2}\}, \lambda_2]$.

Proof. The proof is straightforward, thus was omitted. □

If both (4.19) and (4.20) are feasible at the same time, we select the $P_2^\star$ and the corresponding secrecy rate from the problem which results in a higher secrecy rate. Here, we provide a generic closed-form solution depending on the channels' conditions in Theorems 4.4 and 4.5 for (4.19) and (4.20), respectively.

Theorem 4.4. *Assume* $a = P_{\max_1}|h_{U_1,D_1}|^2$, $b = |h_{U_2,D_1}|^2$, $c = P_{\max_1}|h_{U_1,E}|^2$, $d = |h_{U_2,E}|^2$, $C = b - d$, $D = b\left(c+\sigma_n^2\right) - d\left(a+\sigma_n^2\right)$, $E = -BP_{max_1} = bc - ad$, $F = cd\sigma_n^2 - a\left(b\left(c+\sigma_n^2\right) - cd\right)$, $G = \frac{AP_{max_1}}{\sigma_n^2} = c - a$, $\alpha = \min\left(\inf\varphi_1, P_{\max_2}\right)$, *and* $\beta = \max\left\{\lambda_1, \sup\varphi_1\right\}$. *Also, suppose that* (4.19) *is feasible. Then,* (4.19) *is solved as follows:*

1. *If* $CD < 0$

   (a) *If* $A < 0$ *and* $E > 0$

$$P_2^\star = \alpha \tag{4.21}$$

   (b) *If* $E < 0$

$$P_2^\star = \begin{cases} \beta & A > 0 \\ \lambda_1 & A < 0 \end{cases} \tag{4.22}$$

2. *If* $CD > 0$

   (a) *If* $A < 0$, $E > 0$ *and* $F < 0$

$$P_2^\star = \arg\max_{P_2 \in \{\lambda_1, \alpha\}} C_s \tag{4.23}$$

   (b) *If* $E < 0$ *and* $F > 0$

$$P_2^\star = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg\max_{P_2 \in \left\{\beta, P_{\max_2}\right\}} C_s & A > 0, P_{2C} \notin p_2 \\ \arg\max_{P_2 \in \left\{\lambda_1, P_{\max_2}\right\}} C_s & A < 0, P_{2C} \notin p_2 \end{cases} \tag{4.24}$$

   (c) *If* $E > 0$, $F > 0$ *and* $G < 0$

$$P_2^\star = \begin{cases} \arg\max_{P_2 \in \{P_{2C}, \lambda_1, \alpha\}} C_s & P_{2C} \in p_2 \\ \arg\max_{P_2 \in \{\lambda_1, \alpha\}} C_s & P_{2C} \notin p_2 \end{cases} \tag{4.25}$$

   (d) *If* $E < 0$, $F < 0$ *and* $G > 0$

$$P_2^\star = \begin{cases} \arg\max_{P_2 \in \left\{P_{2C}, \beta, P_{\max_2}\right\}} C_s & P_{2C} \in p_2 \\ \arg\max_{P_2 \in \left\{\beta, P_{\max_2}\right\}} C_s & P_{2C} \notin p_2 \end{cases} \tag{4.26}$$

(e) If $E < 0$, $F < 0$ and $G < 0$

$$P_2^\star = \lambda_1 \tag{4.27}$$

where C_s is the objective function in (4.19), $P_{2C} = \frac{-2bdG\sigma_n^2 - \sqrt{\Delta}}{2bdE}$, and $\Delta = 4abcdCD\sigma_n^2$.

Proof. The proof is given in Appendix C. □

Theorem 4.5. *Assume $e = |h_{U_1,D_1}|^2$, $f = |h_{U_2,D_2}|^2$, $g = |h_{U_1,D_2}|^2$, $h = |h_{U_2,D_1}|^2$, $i = |h_{U_1,E}|^2$, $j = |h_{U_2,E}|^2$, $H = h - j$, $\delta = \min(\inf \lambda_1, P_{\max_2})$, $\kappa = \min\{\inf \lambda_1, \inf \varphi_1, P_{\max_2}\}$, $\mu = \max\{\sup \varphi_1, \lambda_2\}$, $I = -fi + gh\gamma - (hi + gj)\gamma + e(f + j\gamma)$,*
$J = -gh^2 i\gamma(f + j\gamma) + e\left(f^2 i(-h + j) + fgj^2\gamma + ghj^2\gamma^2\right)$,
$K = -gi(f + j\gamma) + e(fg + gh\gamma - hi\gamma + ij\gamma)$,
$L = -ghi(f + j\gamma) + e(fhi + fgj - fij + ghj\gamma)$.
Also, suppose that (4.20) is feasible. Then, (4.20) can be solved as follows

1. *If $HI < 0$*

   (a) If $J > 0$

$$P_2^\star = \begin{cases} \delta & A > 0, B > 0 \\ \delta & A < 0, B > 0 \\ \kappa & A < 0, B < 0 \end{cases} \tag{4.28}$$

   (b) If $J < 0$

$$P_2^\star = \begin{cases} \mu & A > 0, B > 0 \\ \lambda_2 & A < 0, B > 0 \\ \lambda_2 & A < 0, B < 0 \end{cases} \tag{4.29}$$

2. *If $HI > 0$*

   (a) If $J > 0$ and $K < 0$

$$P_2^\star = \begin{cases} \arg\max\limits_{P_2} \max\limits_{P_2 \in \{\mu, \delta\}} C_s & A > 0, B > 0 \\ \arg\max\limits_{P_2} \max\limits_{P_2 \in \{\lambda_2, \delta\}} C_s & A < 0, B > 0 \\ \arg\max\limits_{P_2} \max\limits_{P_2 \in \{\lambda_2, \kappa\}} C_s & A < 0, B < 0 \end{cases} \tag{4.30}$$

(b) If $J < 0$ and $K > 0$

$$P_2^\star = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{\mu, \delta\}} C_s & A > 0, B > 0, P_{2C} \notin p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{\lambda_2, \delta\}} C_s & A < 0, B > 0, P_{2C} \notin p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{\lambda_2, \kappa\}} C_s & A < 0, B < 0, P_{2C} \notin p_2 \end{cases} \tag{4.31}$$

(c) If $J > 0$, $K > 0$ and $L < 0$ or $J < 0$, $K < 0$ and $L > 0$

$$P_2^\star = \begin{cases} \arg\limits_{P_2} \max\limits_{P_2 \in \{P_{2C}, \mu, \delta\}} C_s & A > 0, B > 0, P_{2C} \in p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{P_{2C}, \lambda_2, \delta\}} C_s & A < 0, B > 0, P_{2C} \in p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{P_{2C}, \lambda_2, \kappa\}} C_s & A < 0, B < 0, P_{2C} \in p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{\mu, \delta\}} C_s & A > 0, B > 0, P_{2C} \notin p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{\lambda_2, \delta\}} C_s & A < 0, B > 0, P_{2C} \notin p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{\lambda_2, \kappa\}} C_s & A < 0, B < 0, P_{2C} \notin p_2 \end{cases} \tag{4.32}$$

(d) If $J > 0$, $K > 0$ and $L > 0$

$$P_2^\star = \begin{cases} \delta & A > 0, B > 0 \\ \delta & A < 0, B > 0 \\ \kappa & A < 0, B < 0 \end{cases} \tag{4.33}$$

(e) If $J < 0$, $K < 0$ and $L < 0$

$$P_2^\star = \begin{cases} \mu & A > 0, B > 0 \\ \lambda_2 & A < 0, B > 0 \\ \lambda_2 & A < 0, B < 0 \end{cases} \tag{4.34}$$

where C_s is the objective function in (4.20) and $P_{2C} = \frac{-2\sigma_n^2 \gamma L - \sqrt{\Delta}}{2J}$, and $\Delta = 4egiHI\left(\sigma_n^2\right)^4 \gamma \left(f + h\gamma\right)\left(f + j\gamma\right)$.

Proof. The proof can be obtained in the similar way to that of Theorem 4.4. □

For problem (4.11), the optimal solution of P_1 is as (4.17) when $\chi = P_{\max_1}$. The closed-form solution for the P_2 is given in the following theorem.

Theorem 4.6. *Assume* $a = |h_{U_1,D_1}|^2$, $b = |h_{U_2,D_2}|^2$, $c = |h_{U_1,D_2}|^2$, $d = |h_{U_2,D_1}|^2$, $e = |h_{U_1,E}|^2$, $A = b(a-e)\sigma + d(-e\gamma\sigma + c\gamma\sigma)$, $B = 2bde(a\gamma\sigma - c\gamma\sigma)$, $C = -bce\gamma\sigma^2 + a(bc\gamma\sigma^2 + d\gamma\sigma(-e\gamma\sigma + c\gamma\sigma))$, $\psi = \frac{\sigma_n^2\left(|h_{U_1,D_1}|^2 - |h_{U_1,E}|^2\right)}{|h_{U_1,E}|^2 |h_{U_2,D_1}|^2}$, $\lambda_1 = \frac{\gamma\left(P_{\max_1}|h_{U_1,D_2}|^2 + \sigma_n^2\right)}{|h_{U_2,D_2}|^2}$, $\lambda_2 = \frac{\gamma\sigma_n^2}{|h_{U_2,D_2}|^2}$, *and* $\varsigma = \min\left(P_{\max_2}, \inf\psi, \inf\lambda_1\right)$. *Then, optimal* P_2 *is given as follows:*

1. *If* $A < 0$

$$P_2^\star = \lambda_2 \tag{4.35}$$

2. *If* $A > 0$

   (a) *If* $C > 0$ *or* $B > 0$ *and* $C < 0$

$$P_2^\star = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg\max\limits_{P_2} \max\limits_{P_2 \in \{\lambda_2, \psi\}} C_s & P_{2C} \notin p_2 \end{cases} \tag{4.36}$$

   (b) *If* $B < 0$ *and* $C < 0$

$$P_2^\star = \arg\max_{P_2} \max_{P_2 \in \{\lambda_2, \psi\}} C_s \tag{4.37}$$

where C_s *is the secrecy rate,* $P_{2C} = \frac{-B - \sqrt{\Delta}}{2D}$, $\Delta = 4Aabcde\gamma(d\gamma\sigma + b\sigma)$, $D = -bde(ab + cd\gamma)$, *and* p_2 *is the feasibility domain of the problem.*

Proof. The proof is similar to that of Theorem 4.4, thus was omitted. □

4.4 Problem Formulation: Egoistic Scenario

In this section, we develop closed-form solutions for the case when U_2 is selfish from the view point of U_1's secrecy rate, and adjusts its transmission power just to meet its QoS, i.e., SINR=γ. Later, we compare this case with respect to the altruistic scenario. If one of the Cases 4.7g, 4.7h, or 4.7i holds and U_2 is selfish, (4.14) can be written as

$$\begin{aligned} &\max_{P_1,P_2} \ \frac{1 + \frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2 + \sigma_n^2}}{1 + \frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2 + \sigma_n^2}} \\ &\text{s.t. } P_1 \le P_{\max_1},\ P_1 \underset{(4.7i)}{\overset{(4.7g)}{\gtrless}} \omega,\ P_2 \le P_{\max_2},\ \frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2 + \sigma_n^2} = \gamma. \end{aligned} \tag{4.38}$$

In Case 4.7h, any P_1 ensures that the eavesdropper cannot employ SIC, so no additional constraint over P_1 is necessary. For Case 4.7j, the problem is solved as follows

$$\max_{P_1,P_2} \frac{1+\frac{P_1\left|h_{U_1,D_1}\right|^2}{P_2\left|h_{U_2,D_1}\right|^2+\sigma_n^2}}{1+\frac{P_1\left|h_{U_1,E}\right|^2}{\sigma_n^2}}$$
$$\text{s.t. } P_1 \le P_{\max_1},\ P_2 \le P_{\max_2},\ \frac{P_2|h_{U_2,D_2}|^2}{P_1|h_{U_1,D_2}|^2+\sigma_n^2}=\gamma. \tag{4.39}$$

We first solve (4.38) and then (4.39). Using the last constraint in (4.38), we can directly derive the solution for P_2 as $P_2=\gamma\frac{\left(P_1\left|h_{U_1,D_2}\right|^2+\sigma_n^2\right)}{\left|h_{U_2,D_2}\right|^2}$ and replace it with the corresponding value. Consequently, we can rewrite (4.38) as

$$\max_{P_1} \frac{1+\frac{P_1\left|h_{U_1,D_1}\right|^2}{\gamma\frac{\left(P_1\left|h_{U_1,D_2}\right|^2+\sigma_n^2\right)}{\left|h_{U_2,D_2}\right|^2}\left|h_{U_2,D_1}\right|^2+\sigma_n^2}}{1+\frac{P_1\left|h_{U_1,E}\right|^2}{\gamma\frac{\left(P_1\left|h_{U_1,D_2}\right|^2+\sigma_n^2\right)}{\left|h_{U_2,D_2}\right|^2}\left|h_{U_2,E}\right|^2+\sigma_n^2}}$$
$$\text{s.t. } P_1 \le P_{\max_1},\ P_1 \underset{(4.7i)}{\overset{(4.7g)}{\gtrless}} \omega,\ P_1 \le \frac{P_{\max_2}|h_{U_2,D_2}|^2-\gamma\sigma_n^2}{\gamma|h_{U_1,D_2}|^2}. \tag{4.40}$$

Since the minimum value for the secrecy rate is zero, the objective function in (4.40) should be greater or equal to one. Proposition 4.7 gives the required condition on P_1 in order to have a positive secrecy rate. According to the channel conditions, these constraints should be added to (4.40).

Proposition 4.7. *In order for the objective function in (4.40) to result in a non-negative secrecy rate, P_1 should have the following bounds:*

$$P_1 > \frac{A'}{B'} \quad \text{if} \quad A'>0, B'>0, \tag{4.41n}$$
$$P_1 > 0 \quad \text{if} \quad A'<0, B'>0, \tag{4.41o}$$
$$P_1 < \frac{A'}{B'} \quad \text{if} \quad A'<0, B'<0, \tag{4.41p}$$

where $A'=((1+c)\,d-b\,(1+e))\,\sigma_n^2$, $B'=a\,(be-cd)$. Also, for the case $A'>0$ and $B'<0$, irrespective of the value for P_2, no positive secrecy rate is possible for U_1. The values for b, c, d and e are defined in Theorem 4.8.

Proof. The proof is similar to that of Theorem 4.1, thus was omitted. □

According to Proposition 4.7, we can rewrite (4.40) as

$$\begin{aligned}\max_{P_1}\ & \frac{1+\frac{P_1\left|h_{U_1,D_1}\right|^2}{\gamma\frac{\left(P_1\left|h_{U_1,D_2}\right|^2+\sigma_n^2\right)}{\left|h_{U_2,D_2}\right|^2}\left|h_{U_2,D_1}\right|^2+\sigma_n^2}}{1+\frac{P_1\left|h_{U_1,E}\right|^2}{\gamma\frac{\left(P_1\left|h_{U_1,D_2}\right|^2+\sigma_n^2\right)}{\left|h_{U_2,D_2}\right|^2}\left|h_{U_2,E}\right|^2+\sigma_n^2}}\\ \text{s.t.}\quad & P_1\le P_{\max_1},\ P_1\underset{(4.7i)}{\overset{(4.7g)}{\gtrless}}\omega,\ P_1\underset{(4.41p)}{\overset{(4.41n)}{\gtrless}}\frac{A'}{B'}=\varphi_3,\\ & P_1\le\frac{P_{\max_2}\left|h_{U_2,D_2}\right|^2-\gamma\sigma_n^2}{\gamma\left|h_{U_1,D_2}\right|^2}=\lambda_3.\end{aligned}\tag{4.42}$$

Assuming that (4.42) is feasible, we give a closed-form solution for (4.42) in Theorem 4.8.

Theorem 4.8. *Assuming* $a=\left|h_{U_1,D_2}\right|^2$, $b=\left|h_{U_1,D_1}\right|^2$, $c=\gamma\frac{\left|h_{U_2,D_1}\right|^2}{\left|h_{U_2,D_2}\right|^2}$, $d=\left|h_{U_1,E}\right|^2$, $e=\gamma\frac{\left|h_{U_2,E}\right|^2}{\left|h_{U_2,D_2}\right|^2}$, $Q=c-e$, $R=-(1+c)d+a(c-e)+b(1+e)$, $S=-ac^2d\,(1+e)+b\left(e\,(d+ae)+c\left(-d+ae^2\right)\right)$, $T=\frac{-A'}{\sigma_n^2}=-(1+c)d+b(1+e)$, $U=\frac{B'}{a}=be-cd$, $\eta=\min\{P_{\max_1},\lambda_3\}$, $\eta'=\min\{\eta,\omega\}$, $\theta=\min\{P_{\max_1},\lambda_3,\varphi_3\}$, *and* $\theta'=\min\{\theta,\omega\}$ (4.40) *can be solved as follows*

1. *If* $QR<0$

   (a) *If* $S>0$, $A''>0,B''>0$, *(or* $A''<0,B''>0$*)*

$$P_1^\star=\begin{cases}\eta & Q>0,R<0\\ \theta & B'<0,Q<0,R>0\\ \eta & B'>0,Q<0,R>0\end{cases}\tag{4.43}$$

   (b) *If* $S>0$, $A''<0,B''<0$

$$P_1^\star=\begin{cases}\eta' & Q>0,R<0\\ \theta' & B'<0,Q<0,R>0\\ \eta' & B'>0,Q<0,R>0\end{cases}\tag{4.44}$$

   (c) *If* $S<0$, $A''>0,B''>0$

$$P_1^\star=\begin{cases}\max\{\varphi_3,\omega\} & B'>0,Q>0,R<0\\ \omega & Q<0,R>0\end{cases}\tag{4.45}$$

(d) If $S<0$, $A''<0, B''<0$ *(or* $A''<0, B''>0$*)*

$$P_1^\star = \begin{cases} \varphi_3 & B'>0, Q>0, R<0 \\ 0 & Q<0, R>0 \end{cases} \tag{4.46}$$

2. If $QR>0$

(a) If $S>0$, $T<0$ *and* $B'>0$

$$P_1^\star = \begin{cases} \arg\max\limits_{P_1} \max\limits_{P_1\in\{\max\{\varphi_3,\omega\},\eta\}} C_s & A''>0, B''>0 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{\varphi_3,\eta'\}} C_s & A''<0, B''<0 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{\varphi_3,\eta\}} C_s & A''<0, B''>0 \end{cases} \tag{4.47}$$

(b) If $S<0$, $T>0$, $A''>0$, $B''>0$

$$P_1^\star = \begin{cases} P_{1C} & P_{1C}\in p_1 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{\omega,\eta\}} C_s & P_{1C}\notin p_1, B'>0 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{\omega,\theta\}} C_s & P_{1C}\notin p_1, B'<0 \end{cases} \tag{4.48}$$

(c) If $S<0$ *and* $T>0$, $A''<0$, $B''<0$

$$P_1^\star = \begin{cases} P_{1C} & P_{1C}\in p_1 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{0,\eta'\}} C_s & P_{1C}\notin p_1, B'>0 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{0,\theta'\}} C_s & P_{1C}\notin p_1, B'<0 \end{cases} \tag{4.49}$$

(d) If $S<0$ *and* $T>0$, $A''<0$, $B''>0$

$$P_1^\star = \begin{cases} P_{1C} & P_{1C}\in p_1 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{0,\eta\}} C_s & P_{1C}\notin p_1, B'>0 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{0,\theta\}} C_s & P_{1C}\notin p_1, B'<0 \end{cases} \tag{4.50}$$

(e) If $S>0$, $T>0$, $U<0$ *and* $A''>0$, $B''>0$

$$P_1^\star = \begin{cases} \arg\max\limits_{P_1} \max\limits_{P_1\in\{P_{1C},\omega,\theta\}} C_s & P_{1C}\in p_1 \\ \arg\max\limits_{P_1} \max\limits_{P_1\in\{\omega,\theta\}} C_s & P_{1C}\notin p_1 \end{cases} \tag{4.51}$$

(f) If $S>0$, $T>0$, $U<0$ and $A''<0$, $B''<0$

$$P_1^\star=\begin{cases}\arg\limits_{P_1}\max\limits_{P_1\in\{P_{1C},0,\theta'\}} C_s & P_{1C}\in p_1\\ \arg\limits_{P_1}\max\limits_{P_1\in\{0,\theta'\}} C_s & P_{1C}\notin p_1\end{cases} \tag{4.52}$$

(g) If $S>0$, $T>0$, $U<0$ and $A''<0$, $B''>0$

$$P_1^\star=\begin{cases}\arg\limits_{P_1}\max\limits_{P_1\in\{P_{1C},0,\theta\}} C_s & P_{1C}\in p_1\\ \arg\limits_{P_1}\max\limits_{P_1\in\{0,\theta\}} C_s & P_{1C}\notin p_1\end{cases} \tag{4.53}$$

(h) If $S<0$, $T<0$, $U>0$, $A''>0$, $B''>0$ (or $A''<0$, $B''>0$)

$$P_1^\star=\begin{cases}\arg\limits_{P_1}\max\limits_{P_1\in\{P_{1C},\max\{\varphi_3,\omega\},\eta\}} C_s & P_{1C}\in p_1\\ \arg\limits_{P_1}\max\limits_{P_1\in\{\max\{\varphi_3,\omega\},\eta\}} C_s & P_{1C}\notin p_1\end{cases} \tag{4.54}$$

(i) If $S<0$, $T<0$, $U>0$ and $A''<0$, $B''<0$

$$P_1^\star=\begin{cases}\arg\limits_{P_1}\max\limits_{P_1\in\{P_{1C},\varphi_3,\eta'\}} C_s & P_{1C}\in p_1\\ \arg\limits_{P_1}\max\limits_{P_1\in\{\varphi_3,\eta'\}} C_s & P_{1C}\notin p_1\end{cases} \tag{4.55}$$

(j) If $S>0$, $T>0$ and $U>0$

$$P_1^\star=\begin{cases}\eta & A''>0, B''>0\\ \eta & A''<0, B''>0\\ \eta' & A''<0, B''<0\end{cases} \tag{4.56}$$

where $P_{1C}=\frac{-2a(1+c)(1+e)U\sigma_n^2-\sqrt{\Delta}}{2aS}$ *and* $\Delta=4abdQR\left(\sigma_n^2\right)^4(1+c)(1+e)$.

Proof. The proof can be obtained in the similar way to that of Theorem 4.4. □

For problem (4.39), the closed-form solution for P_1 is given in the following theorem.

Theorem 4.9. *Assume $f=|h_{U_1,D_1}|^2$, $g=|h_{U_1,D_2}|^2$, $h=|h_{U_2,D_1}|^2$, $i=|h_{U_2,D_2}|^2$, $j=|h_{U_1,E}|^2$, $E=ad+bc\gamma-e(d+c\gamma)$, $F=ad-e(d+c\gamma)$, and $\tau=\min\left(P_{\max_2},\inf\rho\right)$. Then, optimal P_1 is as follows:*

1. *If* $E < 0$

$$P_2^\star = 0 \tag{4.57}$$

2. *If* $E > 0$

   (a) *If* $F > 0$

$$P_2^\star = \begin{cases} P_{2C} & P_{2C} \in p_2 \\ \arg\limits_{P_2} \max\limits_{P_2 \in \{0,\tau\}} C_s & P_{2C} \notin p_2 \end{cases} \tag{4.58}$$

   (b) *If* $F < 0$

$$P_2^\star = \arg\max_{P_2} \max_{P_2 \in \{0,\tau\}} C_s \tag{4.59}$$

where $P_{2C} = \frac{-G-\sqrt{\Delta}}{2H}$, $\Delta = 4Eabcde\gamma(d+c\gamma)\sigma^2$, $G = -2bce\gamma(d+c\gamma)\sigma$, $H = -bce\gamma(ad+bc\gamma)$, $\rho = \frac{\sigma_n^2\left(|h_{U_1,D_1}|^2-|h_{U_1,E}|^2\right)|h_{U_2,D_2}|^2}{\gamma|h_{U_1,E}|^2|h_{U_2,D_1}|^2|h_{U_1,D_2}|^2} - \frac{\sigma_n^2}{|h_{U_1,D_2}|^2}$, *and* p_2 *is the feasibility domain of the problem.*

Proof. The proof can be obtained in the similar way to that of Theorem 4.4. □

4.5 Secrecy Energy Efficiency

Before going to Section VI, we define a metric in order to investigate the energy efficiency of the considered scenario. We define the secrecy energy efficiency, η_{SEE}, as the maximum secrecy rate obtained from the objective of (9), namely Ψ, to the optimal consumed power of U_1, $P_1^\star$, ratio as $\eta_{SEE} = \frac{\max\limits_{P_1} \Psi}{P_1^\star}$.

Similarly, in the case we have only one transceiver pair and an eavesdropper with no interfering user, the secrecy energy efficiency metric, η_{SEE}, can be defined as $\eta_{SEE_{su}} = \frac{\log\left(\left(\sigma_n^2+P^\star|h_{U,D}|^2\right)/\left(\sigma_n^2+P^\star|h_{U,E}|^2\right)\right)}{P^\star}$, where P is the transmission power, and $P^\star$ is the optimal transmission power obtained from the optimization problem in the nominator. When the condition $|h_{U,D}|^2 > |h_{U,E}|^2$ holds, the optimum consumed power in the single-user case is P_{max}. In contrast, as we shall see in Section VI, the optimal power consumed by U_1 in the interference channel is considerably lower than P_{max}. Hence, as shall be shown in Section VI, in a wide range of powers, the interference network outperforms the single-user network in terms of secrecy energy efficiency.

4.6 Numerical Results

In this section, we present different scenarios as numerical examples to further clarify the derived results. As a benchmark, we consider a single-user scenario where only one user is present in the environment and there is no second user to produce interference [5]. Then, we compare this benchmark with our system model. Here, we refer to the altruistic and egoistic scenarios as interference channel modes. In all simulation scenarios, we assume that the noise power is equal to one, i.e., $\sigma_n^2 = 1$. All the channel coefficients are modeled as i.i.d. complex normal random variables with real and imaginary parts being as $\mathcal{N}(0,1)$. The channel coefficients are normalized to have a unit variance as $\mathcal{CN}(0,1)$.

For the first scenario, we consider the effect of the users' power limits, $P_{\max_1}$ and $P_{\max_2}$, on the average secrecy rate as shown in Fig. 4.3 for SINR $= 1$ at U_2's destination. By observing the results in Fig. 4.3, we can draw the following conclusions for both altruistic and egoistic scenarios:

1. Average secrecy rate of U_1 increases as $P_{\max_1}$ or $P_{\max_2}$ increases.
2. Increasing $P_{\max_1}$ is more effective on improving the average secrecy rate rather than increasing $P_{\max_2}$. The reason is that increasing U_2's power creates more interference to both U_1 and E.
3. The average secrecy rate of U_1 is lower in the egoistic scenario since U_2 does not change its transmitted power in favor of U_1, and only adjusts it according to the required QoS at D_2. Also, by comparing Fig. 4.4 and Fig. 4.5, it can be seen that U_2 consumes less power in the egoistic scenario. When the Cases (4.15k) and (4.15l) of Theorem 4.1 are true, U_2 can improve the secrecy rate by providing more power in the altruistic scenario.

The average optimal powers consumed by U_1 and U_2 are shown in Fig. 4.4 for the altruistic scenario. Following points are implied by Fig. 4.4 as:

1. In contrast to the single-user case where the maximum power consumption is optimum when the data link is stronger than the wiretap link, average optimal powers expended by users in the interference channel modes are considerably less than the available quantity. So, the optimum power control in the interference channel leads to enormous power saving.
2. As $P_{\max_1}$ increases, U_2 consumes more power. A higher power transmission from U_1 produces more interference on D_2. This makes U_2 to choose higher transmission power in order to maintain the QoS at D_2.

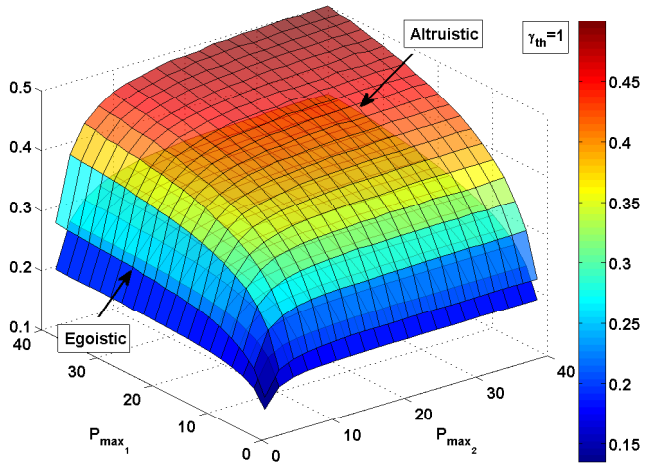


FIGURE 4.3: Average secrecy rate versus the users' maximum available powers in altruistic and egoistic scenarios.

3. As $P_{\max_2}$ increases, U_1 utilizes more power. A higher available power for U_2 enables it to compensate a higher interference from U_1, so U_1 transmits with a higher power to increase the secrecy rate.

4. Depending on the maximum available power to the users, the optimal consumed power by one user can be higher or lower than the power consumed by the other user.

Consumed powers by U_1 and U_2 for the egoistic scenario are illustrated in Fig. 4.5. As we can see, the power consumption pattern is similar to the altruistic scenario as in Fig. 4.4. By comparing Fig. 4.5 with Fig. 4.4, it is noticed that the power consumed by the users in the altruistic scenario is higher than the egoistic scenario.

Average excess SINR provided by U_2 at D_2 in the altruistic scenario is shown in Fig. 4.6 for different values of the required QoS, γ_{th}. Following messages are conveyed by Fig. 4.6 as:

1. By increasing $P_{\max_1}$ for a fixed $P_{\max_2}$, the excess SINR provided at D_2 drops due to increased interference from U_1's transmission.

2. Increasing $P_{\max_2}$ for a fixed $P_{\max_1}$ leads to a higher excess SINR at D_2.

The average secrecy rate comparison among the single-user benchmark and the interference channel modes is presented in Fig. 4.7 with respect to the maximum available power of U_1. Following conclusions can be made according to Fig. 4.7:

1. Increasing $P_{\max_2}$ also enhances the average secrecy rate but much less compared to increasing the $P_{\max_1}$, because U_2 induces interference on both D_1 and E.

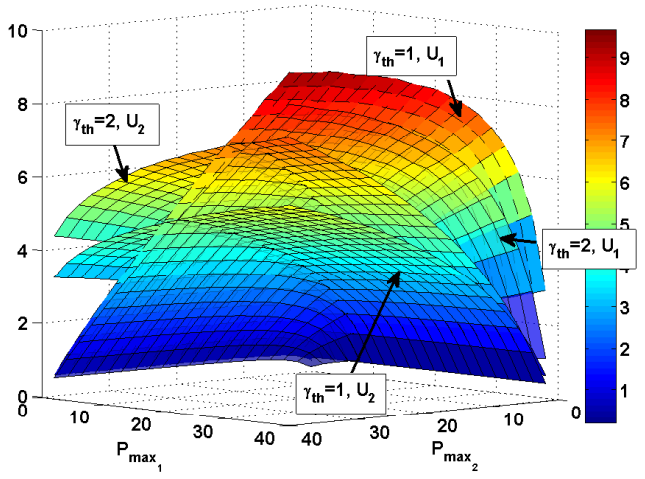


FIGURE 4.4: Average optimal power consumed by the users versus their maximum available powers in altruistic scenario.

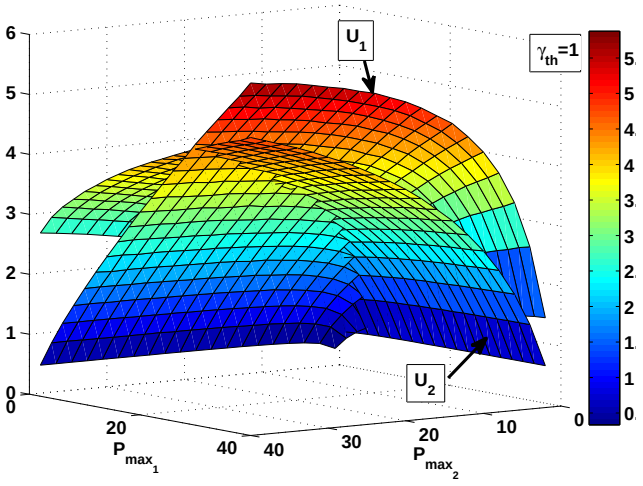


FIGURE 4.5: Average optimal power consumed by the users versus their maximum available powers in the egoistic scenario.

2. The secrecy rate in the egoistic scenario is always lower than the one in the altruistic scenario. In the egoistic scenario, U_2 consumes power to only fulfil the QoS at D_2. As a result, U_2 does not increase its transmission power to produce interference on E when the Cases (4.15k) and (4.15l) of Theorem 4.1 hold. However, in the altruistic scenario, U_2 can change its transmission power in favor of U_1 when it becomes necessary.

A similar comparison as in Fig. 4.7 is displayed in Fig. 4.8 with respect to the maximum available power of U_2. The Statements 1 and 2 of Fig. 4.7 also hold for Fig. 4.8. As we see in Fig. 4.8, increasing $P_{\max_2}$ also increases the average secrecy rate. By increasing $P_{\max_2}$, U_2 gets a higher ability to suppress the interference coming from U_1 as well as causing more interference on E when the Cases (4.15k) and (4.15l) of Theorem 4.1 hold. As a result, U_1 can transmit with a higher power and enhance the secrecy rate.

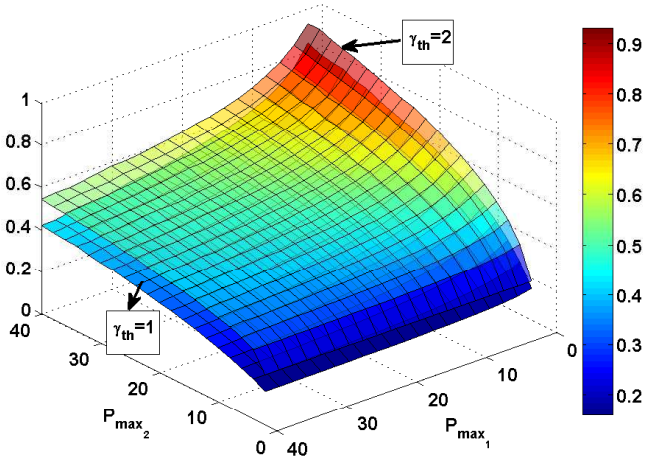


FIGURE 4.6: Average excess QoS provided at D_2 versus users' maximum available powers in the altruistic scenario.

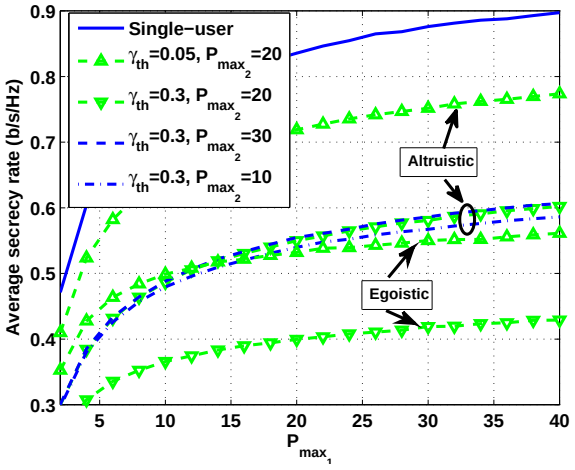


FIGURE 4.7: Average secrecy rate versus U_1's maximum available power.

As we can see from Fig. 4.7 and Fig. 4.8, the average secrecy rate in the interference channel modes is lower than its value in the single-user case. However, we should note that the power consumed in the interference channel modes is considerably lower than the single-user case. To make a fair comparison, we use the "secrecy energy efficiency" metric defined in Section 4.5 to compare the secrecy rates of the interference channel modes and the single-user benchmark. This metric is derived for different values of γ_{th} in Fig. 4.9. According to graphs in Fig. 4.9, we can make the following conclusions:

1. The secrecy energy efficiency is higher for the interference channel modes in a considerable range of γ_{th} and $P_{\max_1}$. If we consider a specific available power for U_1, the acquired secrecy rate in the interference channel modes becomes higher than the one achieved in the single-user case.

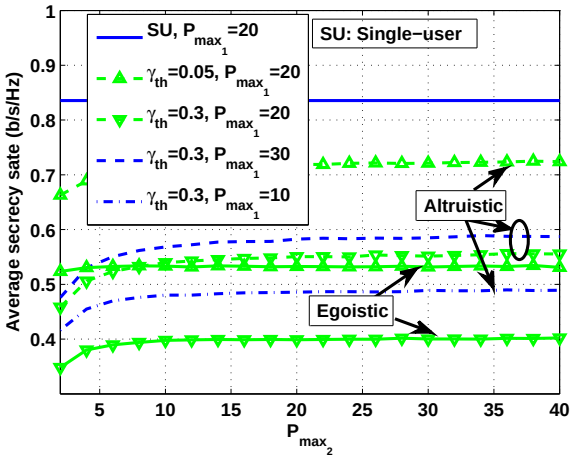


FIGURE 4.8: Average secrecy rate versus U_2's maximum available power.

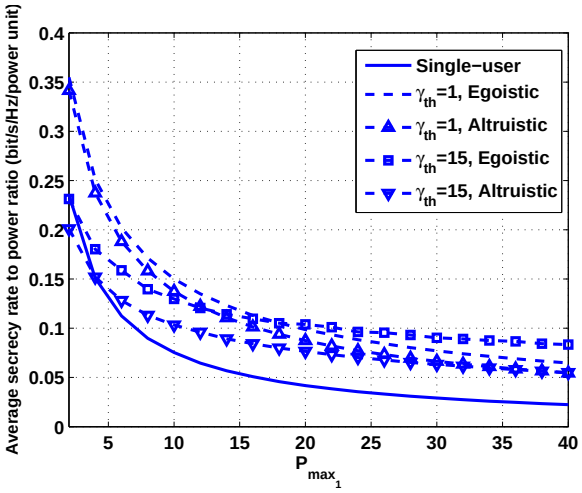


FIGURE 4.9: Average secrecy energy efficiency versus U_1's maximum available power.

2. As the maximum available power to U_1 increases, the secrecy energy efficiency falls faster for the cases with lower γ_{th}.

4.7 Conclusion

We considered a two-user interference wireless channel in this chapter where the first user, namely user 1, wants to sustain a positive secrecy rate while communicating with its destination. The second user of the network, namely user 2, requires to preserve a specific QoS at its destination. Both users create interference for their destinations and another unintended user of the network, i.e., the eavesdropper, which is interested in wiretapping user 2. We showed that by appropriate power control of user 1, the eavesdropper cannot perform SIC. We studied the effect of interference from user 2 on the secrecy rate of user 1. Specifically, depending on the channel conditions, we

derived the conditions on user 2's transmission power in which positive secrecy rate can be provided. In addition, we jointly derived closed-form expressions for optimal power transmission of user 1 and 2 to maximize the secrecy rate of user 1 and preserving the QoS at the destination of user 2. We solve the joint power control problem for both altruistic and egoistic scenarios. In the altruistic scenario, user 2 changes its power to over satisfy the QoS at its destination if it improves the secrecy rate. However, it preserves the minimum QoS at its destination in the egoistic scenario. The simulations showed that decreasing the QoS at the destination of user 2 improves the secrecy rate and the secrecy rate gets closer to the single-user case.

Moreover, the ratio of the secrecy rate over the optimal consumed power by user 1 was introduced as a new metric called "secrecy energy efficiency", in order to take into account both the secrecy rate and the consumed power. This was mainly done to have a fair comparison with the benchmark scheme which is the single-user channel. It was shown that in comparison with the single-user case, the secrecy energy efficiency is considerably higher in the interference channel for a wide range of QoS at user 2's destination.

Chapter 5

Secrecy Energy Efficiency in MISO and SISO Communication Networks

Energy-efficiency, high data rates and secure communications are essential requirements of the future wireless networks. In this chapter, optimizing the secrecy energy efficiency is considered. The optimal beamformer is designed for a MISO system with and without considering the minimum required secrecy rate. Further, the optimal power control in a SISO system is carried out using an efficient iterative method, and this is followed by analyzing the trade-off between the secrecy energy efficiency and the secrecy rate for both MISO and SISO systems. The contribution of this chapter is published in [25].

5.1 Introduction

Due to the presence of several wireless devices in a specific environment, the transmitted information may be exposed to unintended receivers. Using cryptography in higher layers, a secure transmission can be initiated. Nevertheless, it is probable that an unintended device, which maybe also be a part of the legitimate network, breaks the encryption [3]. Fortunately, physical layer security techniques can further improve the security by perfectly securing a transmission rate using the "*secrecy rate*" concept introduced in [5]. While security is a concern, power consumption is also another important issue in wireless communications since some wireless devices rely on limited battery power.

There are a wealth of research works in the literature which investigate the energy efficiency in wireless networks such as [230, 231] and the references therein. Recently, some research has been done to jointly optimize the secrecy rate and the power consumption. Sum secrecy rate and power are jointly optimized in [113] to attain a minimum quality of service (QoS). In [114], switched beamforming is used to maximize the secrecy outage probability over the consumed power ratio. Powers consumption for a fixed secrecy rate is minimized in [117] for an amplify-and-forward (AF) relay network. The secrecy outage probability over the consumed power is maximized subject to power limit for a large scale AF relay network in [118]. The optimal beamformer for a wiretap channel with multiple-antenna nodes is designed in [115] to maximize secrecy rate over power ratio.

Here, we consider a multiple-input single-output (MISO) and a single-input single-output (SISO) scenario while a single-antenna unintended receiver, which is part of the network, is listening. The secrecy rate over the power ratio, named "*secrecy energy efficiency*" and denoted by ζ, is maximized with and without considering the minimum required secrecy spectral efficiency, denoted by η_0, at the destination. For comparison, we derive the optimal beamformer when zero-forcing (ZF) technique is used to null the signal at the eavesdropper with considering the minimum required secrecy spectral efficiency. Note that the ZF can only be used for the MISO scenario. Furthermore, the trade-off between ζ and secrecy spectral efficiency, denoted by η, is studied.

The following issues distinct our work from the most related research. In [115], first-order Taylor series expansion and Hadamard inequality are used to approximate the optimal beamfromer for a MIMO system. However, the exact beamformer for the MISO system is derived in this chapter. Furthermore, the innermost layer of algorithm in [115] is based on the singular value decomposition, and is not applicable to SISO and MISO systems. In this chapter, apart from the MISO system exact beamformer design, exact optimal power allocation for the SISO system is also derived.

5.2 Signal and System Model

Consider a wireless communication network comprised of a transmitter denoted by T, a receiver denoted by R, and an unintended user denoted by E. Note that to obtain the secrecy rate, the legitimate user needs to be aware of the instantaneous channel to the eavesdropper. This knowledge for the most general case with a passive eavesdropper is not practical. In this work, the unintended user is assumed to be part of the network. Therefore, the transmitter T is able to receive the training sequence from E, in order to

estimate its channel. The signal model and the secrecy rates are derived in the following parts.

5.2.1 MISO System

Here, we assume that the transmitter employs multiple antennas. The received signals at R and E are then as follows

$$y_R = \mathbf{h}_{T,R}^T \mathbf{w} x + n_R, \tag{5.1}$$

$$y_E = \mathbf{h}_{T,E}^T \mathbf{w} x + n_E, \tag{5.2}$$

where x is the transmitted message, $\mathbf{w}$ is a vector containing beamforming gains, $\mathbf{h}_{T,R}$ and $\mathbf{h}_{T,E}$ are the transmitter's channel gains toward the receiver and eavesdropper, respectively. The additive white Gaussian noise at the receiver and eavesdropper are shown by n_R and n_E, respectively. The random variables x, n_R, and n_E are complex circularly symmetric (c.c.s.) and independent and identically Gaussian distributed (i.i.d.) with $x \sim \mathcal{CN}(0,1)$, $n_R \sim \mathcal{CN}(0,\sigma_{n_R}^2)$, and $n_E \sim \mathcal{CN}(0,\sigma_{n_E}^2)$, respectively, where $\mathcal{CN}$ denotes the complex normal random variable. The noise powers, $\sigma_{n_R}^2$ and $\sigma_{n_E}^2$, are equal to KT_iB where K is the boltzman constant, T_i is the temperature at the corresponding receiver with $i \in \{R,E\}$, and B is the transmission bandwidth. Using (5.1) and (5.2) and the result in [13], the secrecy spectral efficiency (or rate in bps/Hz) denoted by η is obtained by

$$\eta_{MISO} = \left[\log\left(\frac{1+a}{1+b}\right)\right]^+, \tag{5.3}$$

where $a = \frac{|\mathbf{h}_{T,R}^T \mathbf{w}|^2}{\sigma_{n_R}^2}$, $b = \frac{|\mathbf{h}_{T,E}^T \mathbf{w}|^2}{\sigma_{n_E}^2}$, and $[x]^+$ denotes $\max(x,0)$. In this chapter, all the logarithms are in base two. Further, the operator $[\cdot]^+$ is dropped throughout the chapter for the sake of simplicity.

5.2.2 SISO System

When one antenna is employed at the transmitter, using the result in [232], the secrecy spectral efficiency, η, is calculated as

$$\eta_{SISO} = \left[\log\left(\frac{1+a'}{1+b'}\right)\right]^+, \tag{5.4}$$

where $a' = \frac{P|h_{T,R}|^2}{\sigma^2_{n_R}}$, $b' = \frac{P|h_{T,E}|^2}{\sigma^2_{n_E}}$, P is the transmission power by T, and $h_{T,R}$ and $h_{T,E}$ are the channel gains to the receiver and eavesdropper, respectively. The statistical characteristics of the message signal and the noise are the same as those in Section 5.2.1.

5.3 Problem Formulation: MISO System

In this section, we maximize ζ in a MISO system by obtaining the optimal beamformer for the cases with and without QoS constraint at the receiver.

5.3.1 With QoS at the Receiver

The metric ζ is defined as η multiplied by bandwidth over the total consumed power ratio as

$$\zeta = \frac{B\eta}{\|\mathbf{w}\|^2 + P_c}, \tag{5.5}$$

where P_c is the circuit power consumption. We define our problem so as to maximize the secrecy energy efficiency subject to the peak power and QoS constraints as follows

$$\max_{\mathbf{w}} \ \zeta \qquad \text{s.t.} \qquad \|\mathbf{w}\|^2 \leq P_{\max}, \ \eta > \eta_0. \tag{5.6}$$

To design the optimal beamformer, we rewrite (5.6) as

$$\begin{aligned} \max_{\mathbf{w}} \ & B\frac{\log\left(\frac{\sigma^2_{n_E}}{\sigma^2_{n_R}}\frac{\sigma^2_{n_R}+\mathbf{w}^H\mathbf{h}^*_{T,R}\mathbf{h}^T_{T,R}\mathbf{w}}{\sigma^2_{n_E}+\mathbf{w}^H\mathbf{h}^*_{T,E}\mathbf{h}^T_{T,E}\mathbf{w}}\right)}{\|\mathbf{w}\|^2 + P_c} \\ \text{s.t.} \quad & \|\mathbf{w}\|^2 \leq P_{\max}, \ \mathbf{w}^H\mathbf{C}\mathbf{w} \geq 2^{\eta_0} - 1, \end{aligned} \tag{5.7}$$

where $\mathbf{C} = \frac{\mathbf{h}^*_{T,R}\mathbf{h}^T_{T,R}}{\sigma^2_{n_R}} - \frac{\mathbf{h}^*_{T,E}\mathbf{h}^T_{T,E}}{\sigma^2_{n_E}}2^{\eta_0}$. Using an auxiliary variable as $t = \|\mathbf{w}\|^2$, (5.7) is reformulated as follows

$$\begin{aligned} \max_{\mathbf{w}, 0<t\leq P_{\max}} \ & \mathrm{B}\frac{\log\left(\frac{\sigma^2_{n_E}}{\sigma^2_{n_R}}\frac{\mathbf{w}^H\mathbf{A}\mathbf{w}}{\mathbf{w}^H\mathbf{B}\mathbf{w}}\right)}{t + P_c} \\ \text{s.t.} \ & \|\mathbf{w}\|^2 = t, \ \mathbf{w}^H\mathbf{C}\mathbf{w} \geq 2^{\eta_0} - 1, \end{aligned} \tag{5.8}$$

where $\mathbf{A} = \frac{\sigma^2_{n_R}}{t}\mathbf{I} + \mathbf{h}^*_{\mathbf{T},\mathbf{R}}\mathbf{h}^{\mathbf{T}}_{\mathbf{T},\mathbf{R}}$ and $\mathbf{B} = \frac{\sigma^2_{n_E}}{t}\mathbf{I} + \mathbf{h}^*_{\mathbf{T},\mathbf{E}}\mathbf{h}^{\mathbf{T}}_{\mathbf{T},\mathbf{E}}$. The constraint $\|\mathbf{w}\|^2 \leq P_{\max}$ is omitted since the upper limit of the search on variable shall be $P_{\max}$, which satisfies this constraint. To make the last constraint convex, (5.8) is transformed to a semidefinite

programming (SDP) optimization problem.

$$\max_{\mathbf{W},0<t\leq P_{\max}} \mathrm{B}\frac{\log\left(\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\frac{\mathrm{tr}(\mathbf{WA})}{\mathrm{tr}(\mathbf{WB})}\right)}{t+P_c}$$
$$\text{s.t. } \mathrm{tr}\left(\mathbf{W}\right)=t,\ \mathrm{tr}\left(\mathbf{WC}\right)\geq 2^{\eta_0}-1,\ \mathbf{W}\succeq\mathbf{0}, \tag{5.9}$$

where $\mathrm{rank}(\mathbf{W})=\mathbf{1}$ constraint is dropped to have a set of convex constraints. Similar to [233], matrix $\mathbf{V}$ and scalar s are defined such that $\mathbf{V}=s\mathbf{W}$ and $\mathrm{tr}\left(s\mathbf{WB}\right)=1$. Accordingly, (5.9) is transformed into

$$\max_{\mathbf{V},0<t\leq P_{\max},s} \frac{\mathrm{B}}{t+P_c}\log\left(\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\mathrm{tr}\left(\mathbf{VA}\right)\right)$$
$$\text{s.t.}\quad \mathrm{tr}\left(\mathbf{V}\right)=st,\ \mathrm{tr}\left(\mathbf{VC}\right)\geq s\left(2^{\eta_0}-1\right),$$
$$\mathrm{tr}\left(\mathbf{VB}\right)=1,\mathbf{V}\succeq 0,s\geq 0. \tag{5.10}$$

Finally, by considering the auxiliary variable t to be fixed and dropping the log due to the monotonicity of logarithm function, (5.10) can be solved using SDP along with a one-dimensional search over the variable t where $t\in(0,P_{\max}]$. Since the matrices $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ in (5.10) are Hermitian positive semidefinite, Theorem 2.3 in [223] can used to derive an equivalent rank-one solution if the solution to (5.10) satisfies $\mathrm{rank}(\mathbf{W})\geq 3$.

In order to perform a comparison, we also design the optimal beamforming vector to maximize the secrecy energy efficiency when zero-forcing (ZF) strategy is used to null the received signal at the eavesdropper. Using (5.7), the ZF beamformer design problem can be defined as follows

$$\max_{\mathbf{w}} B\frac{\log\left(\frac{\sigma_{n_R}^2+\mathbf{w}^H\mathbf{h}_{T,R}^*\mathbf{h}_{T,R}^T\mathbf{w}}{\sigma_{n_R}^2}\right)}{\|\mathbf{w}\|^2+P_c}$$
$$\text{s.t. } \|\mathbf{w}\|^2\leq P_{\max},\ \mathbf{w}^H\mathbf{Cw}\geq 2^{\eta_0}-1,\ \mathbf{h}_{T,E}^T\mathbf{w}=0. \tag{5.11}$$

Using $t=\mathbf{w}^H\mathbf{w}$, we get

$$\max_{\mathbf{w}} \frac{B}{t+P_c}\left(\log\left(\mathbf{w}^H\mathbf{Aw}\right)-\log\sigma_{n_R}^2\right)$$
$$\text{s.t. } \|\mathbf{w}\|^2=t,\ \mathbf{w}^H\mathbf{Cw}\geq 2^{\eta_0}-1,\ \mathbf{h}_{T,E}^T\mathbf{w}=0, \tag{5.12}$$

which can be simplified into

$$\max_{\mathbf{w}} \mathbf{w}^H\mathbf{Aw}$$
$$\text{s.t. } \|\mathbf{w}\|^2=t,\ \mathbf{w}^H\mathbf{Cw}\geq 2^{\eta_0}-1,\ \mathbf{h}_{T,E}^T\mathbf{w}=0. \tag{5.13}$$

To make the third constraint convex, similar to (5.8), (5.13) can be transformed into a SDP optimization problem as

$$\begin{aligned} &\max_{\mathbf{W}} \quad \mathrm{tr}\left(\mathbf{WA}\right) \\ &\text{s.t. } \mathrm{tr}\left(\mathbf{W}\right) = t,\ \mathrm{tr}\left(\mathbf{WC}\right) \geq 2^{\eta_0} - 1, \\ &\quad \mathrm{tr}\left(\mathbf{WD}\right) = 0, \mathbf{W} \succeq 0, \end{aligned} \tag{5.14}$$

where $\mathbf{D} = \mathbf{h}_{T,E}^{*}\mathbf{h}_{T,E}^{T}$ and the rank-one constraint on $\mathbf{W}$ is dropped to make the problem convex. Since the matrices $\mathbf{A}$, $\mathbf{C}$, and $\mathbf{D}$ in (5.14) are Hermitian positive semidefinite, Theorem 2.3 in [223] can used to derive an equivalent rank-one solution if the solution to (5.14) satisfies rank$(\mathbf{W}) \geq 3$.

If the solution to (5.14) is not rank-one, Theorem 2.3 in [223] can be employed to derive an equivalent rank-one solution. Problem (5.14) can be solved using SDP along with a one-dimensional search over the variable t where $t \in (0, P_{\max}]$.

5.3.2 Without QoS at the Receiver

Using (5.8), the optimal beamformer design problem without considering the QoS is reduced to

$$\max_{\mathbf{w}, 0<t\leq P_{\max}} \mathrm{B}\frac{\log\left(\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\frac{\mathbf{w}^H\mathbf{A}\mathbf{w}}{\mathbf{w}^H\mathbf{B}\mathbf{w}}\right)}{t + P_c} \text{ s.t. } \|\mathbf{w}\|^2 = t. \tag{5.15}$$

For a fixed t, (5.15) can be written as

$$\max_{\mathbf{w}} \frac{\mathrm{B}}{t + P_c}\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\frac{\mathbf{w}^H\mathbf{A}\mathbf{w}}{\mathbf{w}^H\mathbf{B}\mathbf{w}}, \tag{5.16}$$

where $t \in (0, P_{\max}]$. Due to the homogeneity of (5.15), the constraints on the bamforming vector can be satisfied and thus dropped. The optimal value and the optimal beamforming vector in (5.16) are easily derived using Rayleigh-Ritz [234] when (5.16) is in its standardized form as

$$\max_{\mathbf{v}} \frac{\mathrm{B}}{t + P_c}\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\frac{\mathbf{v}^H\mathbf{D}\mathbf{v}}{\mathbf{v}^H\mathbf{v}}, \tag{5.17}$$

where $\mathbf{v} = \mathbf{C}^H\mathbf{w}$, $\mathbf{D} = \mathbf{C^{-1}AC^{-H}}$, and matrix $\mathbf{C}$ is the Cholesky decomposition of matrix $\mathbf{B}$ as $\mathbf{B} = \mathbf{C}\mathbf{C}^H$. The optimal beamforming vector is derived as $\mathbf{w}^\star = \mathbf{C}^{-H}\mathbf{v}^\star$ where $\mathbf{v}^\star$ is the eigenvector corresponding to $\lambda_{\max}\left(\mathbf{C^{-1}AC^{-H}}\right)$. Finally, the optimal ζ

is obtained in closed-form by

$$\zeta^{\star} = B\frac{\log\left(\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\lambda_{\max}\left(\mathbf{C}^{-1}\mathbf{A}\mathbf{C}^{-\mathbf{H}}\right)\right)}{t+P_c}. \tag{5.18}$$

Employing a one-dimensional search over $t \in (0, P_{\max}]$ and using (5.18), the optimal value of (5.17) is found.

5.4 Problem Formulation: SISO System

In the SISO case, the beamformer design is reduced to scalar power control. Similar to (5.6), the optimization problem for SISO system is defined as

$$\max_{P} \quad B\frac{\log\left(\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\frac{\sigma_{n_R}^2+P\left|h_{T,R}\right|^2}{\sigma_{n_E}^2+P\left|h_{T,E}\right|^2}\right)}{P_c+P} \text{ s.t. } P_{\min} \le P \le P_{\max}, \tag{5.19}$$

where $P_{\min} = \frac{2^{\eta_0}-1}{\alpha}$ is obtained from the minimum QoS constraint, and it is assumed that $\alpha = \frac{\left|h_{T,R}\right|^2}{\sigma_{n_R}^2} - \frac{\left|h_{T,E}\right|^2}{\sigma_{n_E}^2}2^{\eta_0} > 0$. The numerator in the objective of (5.19) is concave since the argument of the logarithm is concave for $P \ge 0$ and $\frac{\left|h_{T,R}\right|^2}{\sigma_{n_R}^2} > \frac{\left|h_{T,E}\right|^2}{\sigma_{n_E}^2}$, which are granted in our problem, and the denumerator is affine. Hence, (5.19) is categorized as a family member of fractional programming problems known as "*concave fractional program*" where a local optimum is a global one [235]. Here, we solve (5.19) using an iterative (parametric) algorithm named Dinkelbach [236]. For the sake of simplicity, we mention the values related to $|h_{T,R}|^2$ and $|h_{T,E}|^2$ by a and b, respectively. According to [236], after dropping the constant B, (5.19) is written as

$$F(q) = \max_{P\in S} \log\left(\frac{\sigma_{n_E}^2}{\sigma_{n_R}^2}\frac{\sigma_{n_R}^2+Pa}{\sigma_{n_E}^2+Pb}\right) - q\left(P_c+P\right), \tag{5.20}$$

$$q = \frac{f(P)}{g(P)}, \tag{5.21}$$

where $f(P)$ and $g(P)$ are the numerator and denumerator of (5.19), respectively. Also, S shows the feasible domain of P. To calculate the optimal P for (5.20), denoted by $P^{\star}$, the derivative of $F(q)$ with respect to P is calculated as follows

$$\begin{aligned}\frac{\partial F}{\partial P} =& -abq\beta P^2 + Pq\beta\left(-a\sigma_{n_E}^2 - b\sigma_{n_R}^2\right)\\ &+ a\sigma_{n_E}^2 - q\beta\sigma_{n_R}^2\sigma_{n_E}^2 - b\sigma_{n_R}^2,\end{aligned} \tag{5.22}$$

Algorithm 1 Iterative approach to solve (5.19)

1: Initialize $n = 0$;
2: Pick any $P_n \in S$;
3: Derive q_n using (5.21);
4: Derive $P_n^\star$ using (5.24) and calculate $F(q_n)$ using (5.20);
5: **if** $F(q_n) \geq \delta$ **then**
6: $\quad n = n + 1$;
7: $\quad$ **Go to** 3;
8: **end if**

which is a quadratic equation with a closed-form solution as

$$P_{1,2} = \frac{q\left(a\sigma_{n_E}^2 + b\sigma_{n_R}^2\right) \pm \sqrt{\Delta}}{-2abq}, \ \beta = \mathrm{Ln}2,$$
$$\Delta = q^2\left(a\sigma_{n_E}^2 + b\sigma_{n_R}^2\right)^2 + 4abq\left(a\sigma_{n_E}^2 - q\sigma_{n_R}^2\sigma_{n_E}^2 - b\sigma_{n_R}^2\right). \tag{5.23}$$

Since P_1 in (5.23) is always negative, $P^\star$ is derived as

$$P^\star = \begin{cases} P_2 & P_2 \in S, \\ \arg\max\limits_{P \in \{P_{\min}, P_{\max}\}} F(q) & P_2 \notin S, \end{cases} \tag{5.24}$$

where $P_2 = \frac{q\left(a\sigma_{n_E}^2 + b\sigma_{n_R}^2\right) - \sqrt{\Delta}}{-2abq}$. The procedure to solve (5.19) using Dinkelbach method is summarized in Algorithm 1. Using the closed-form solution of (5.20) given in (5.24), the following recursive relation is used to merge Steps 3 and 4 of Algorithm 1 as

$$P_{n+1} = \frac{\frac{f(P_n)}{g(P_n)}\left(a\sigma_{n_E}^2 + b\sigma_{n_R}^2\right) - \sqrt{\Delta_n}}{-2ab\frac{f(P_n)}{g(P_n)}}. \tag{5.25}$$

It is proven in [236] that Algorithm 1 converges. In addition, since a local optimum for a concave fractional program is the global optimum, and (5.19) falls into this category, the solution found using Algorithm 1 is a global optimum.

5.5 Trade-off between ζ and η

In this section, we study the trade-off between secrecy energy efficiency and secrecy spectral efficiency (i.e. ζ and η) for MISO and SISO systems.

5.5.1 MISO System

To find the trade-off between ζ and η, we solve the optimal beamforming design problem to maximize ζ and η separately for a specific power constraint, P. As a result, the pair (ζ, η) is available for different values of P. For ζ, the optimization problem is as follows

$$\max_{\mathbf{w}} B \frac{\log_2\left(\frac{\sigma^2_{n_E}}{\sigma^2_{n_R}} \frac{\sigma^2_{n_R}+\mathbf{w}^H\mathbf{h}^*_{T,R}\mathbf{h}^T_{T,R}\mathbf{w}}{\sigma^2_{n_E}+\mathbf{w}^H\mathbf{h}^*_{T,E}\mathbf{h}^T_{T,E}\mathbf{w}}\right)}{P+P_c} \text{ s.t. } \|\mathbf{w}\|^2 = P. \tag{5.26}$$

Using the constraint in (5.26), we conclude that $\frac{\mathbf{w}^H\mathbf{w}}{P} = 1$ which helps us homogenize (5.26) as

$$\max_{\mathbf{w}} \mathrm{B} \frac{\log_2\left(\frac{\sigma^2_{n_E}}{\sigma^2_{n_R}} \frac{\mathbf{w}^H\mathbf{A}\mathbf{w}}{\mathbf{w}^H\mathbf{B}\mathbf{w}}\right)}{P+P_c} \text{ s.t. } \|\mathbf{w}\|^2 = P, \tag{5.27}$$

where, $\mathbf{A} = \frac{\sigma^2_{n_R}}{P}\mathbf{I} + \mathbf{h}^*_{T,R}\mathbf{h}^T_{T,R}$ and $\mathbf{B} = \frac{\sigma^2_{n_E}}{P}\mathbf{I} + \mathbf{h}^*_{T,E}\mathbf{h}^T_{T,E}$. Similar to (5.15), the log and the power constraint can be dropped. Similar to the solution to (5.17), the optimal beamforming vector shall be $\mathbf{w}^\star = \mathbf{C}^{-H}\mathbf{v}^\star$ where $\mathbf{v}^\star$ is the eigenvector corresponding to $\lambda_{\max}\left(\mathbf{C}^{-1}\mathbf{A}\mathbf{C}^{-\mathbf{H}}\right)$. The final closed-form solution for $\zeta^\star$ is

$$\zeta^\star = B \frac{\log\left(\frac{\sigma^2_{n_E}}{\sigma^2_{n_R}} \lambda_{\max}\left(\mathbf{C}^{-1}\mathbf{A}\mathbf{C}^{-\mathbf{H}}\right)\right)}{P+P_c}. \tag{5.28}$$

The optimal beamforming vector for $\eta^\star$ shall be the same as for $\zeta^\star$ and the optimal value of η can be derived similar to the one for ζ. Hence, the pair $(\zeta^\star, \eta^\star)$ is available.

5.5.2 SISO System

By deriving P with respect to η using (5.4) as $P = \frac{\sigma^2_{n_R}\sigma^2_{n_E}(2^\eta-1)}{\sigma^2_{n_E}a - \sigma^2_{n_R}b2^\eta}$, the relation between ζ and η is calculated using (5.5) as follows

$$\zeta = \frac{B\eta\left(\sigma^2_{n_E}a - \sigma^2_{n_R}b2^\eta\right)}{\sigma^2_{n_R}\sigma^2_{n_E}\left(2^\eta-1\right) + P_c\left(\sigma^2_{n_E}a - \sigma^2_{n_R}b2^\eta\right)}. \tag{5.29}$$

By solving $\frac{d\zeta}{d\eta} = 0$ using numerical methods, η corresponding to the optimal ζ can be derived.

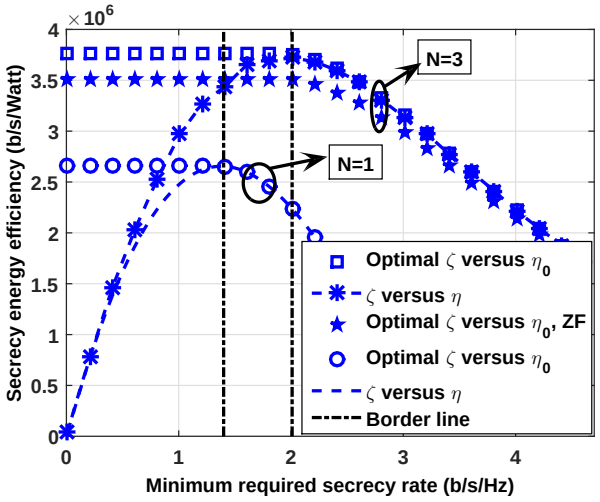


FIGURE 5.1: Optimal ζ versus η_0 and ζ versus η graphs.

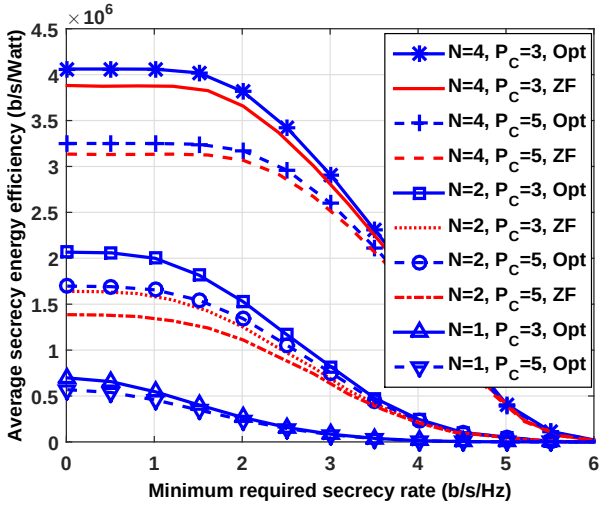


FIGURE 5.2: Average ζ versus η_0 for different N and P_c.

5.6 Simulation Results

In this section, we present numerical examples to investigate the secrecy energy efficiency and its trade-off with the secrecy spectral efficiency. The simulations' parameters are as follows. Distance from the transmitter to receiver and eavesdropper, d, is considered to be 2 km, Quasi-static block fading channel model as $\mathcal{CN}(0,1)$, path loss is $128.1 + 37.6 \log_{10} d$ dB [237], bandwidth is 20 MHz, $P_c = 5$, $P_{\max} = 50$, receiver noise temperature is 298 K, tolerance error for Dinkelbach algorithm is $\delta = 10^{-3}$, and N is the number of antennas. If the secrecy rate is negative, it is considered to be zero. For the figures presenting the average graphs, enough amount of channels are generated and the average of the resultant metrics are considered. In the first simulation scenario, the secrecy energy efficiency and secrecy spectral efficiency trade-off is studied. Optimal ζ versus the minimum required η graphs as well as the graphs related to the

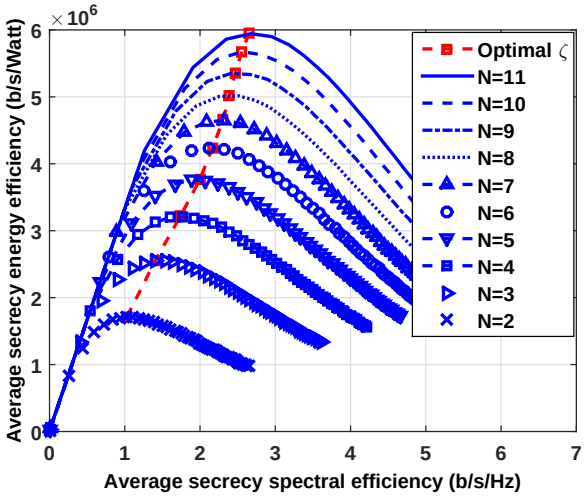


FIGURE 5.3: ζ and η relation for different antennas.

trade-off between ζ and η are presented in Fig. 5.1 using a single channel realization. Two different regions are defined in Fig. 5.1 using a border line. The border line defines the optimal operating point in terms of ζ. In the left-hand side region, increasing η also increases ζ. Hence, to get a higher ζ, the secrecy rate can be increased, which is desirable. However, the mechanism between ζ and η changes in the right-hand side of Fig. 5.1. After the optimal point of ζ, increasing η demands more power which is higher than the optimal power value for ζ. Therefore, as η increases, ζ falls below the optimal value which is opposite to the procedure in the left-hand side, and the trade-off is clear. Also, it is observed that ZF results in a lower secrecy energy efficiency. Nevertheless, as the minimum required secrecy rate increases, the performance of the ZF approaches the primary scheme, i.e., optimal beamformer design. For the second scenario, average ζ versus the minimum required η is investigated for different numbers of antennas, and circuit powers. The related graphs are depicted in Fig. 5.2. As it is shown, increasing the number of antennas results in increasing the optimal value of ζ and makes it stable for a longer range of η_0. Further, we can see that decreasing P_c leads to higher secrecy energy efficiency, and this is more significant for higher number of antennas. Similar to the result in Fig. 5.1, ZF scheme shows a sub-optimal performance. ZF's performance gets closer to the optimal scheme as the circuit power, P_c, increases. Interestingly, for fewer number of antennas, the gap between the performance of the ZF and the optimal scheme even gets larger. This is due to less degrees of freedom for the ZF beamformer design as the number of antennas decreases. To investigate the trade-off between ζ and η, the average (ζ, η) pair for different number of antennas is presented in Fig. 5.3. It is observed that the optimal ζ grows as number of antennas are increased.

5.7 Conclusion

In this chapter, we studied the secrecy energy efficiency and its trade-off with the secrecy spectral efficiency in MISO and SISO wiretap channels. We designed the optimal beamformer to maximize the secrecy energy efficiency with and without considering the minimum required secrecy spectral efficiency at the receiver side. In addition, we designed the beamformer to maximize the secrecy energy efficiency when the transmitter applies zero forcing to null out the information signal in the direction of the eavesdropper. The simulation results showed that the secrecy energy efficiency of the optimal beamformer and the ZF beamformer designs gets closer as the minimum required secrecy spectral efficiency increases. In addition, we observed that the difference between the secrecy energy efficiency of the optimal and ZF design decreases as the number of transmission antennas increases. This is due to the fact that the ZF design by nature limits the degrees of freedom in the beamformer design, while increasing the number of antennas gives more degrees of freedom to the ZF design. Particularly, the numerical results revealed that there is a specific point for the secrecy spectral efficiency where the secrecy energy efficiency gets to its maximum point. Above this point, the secrecy energy efficiency starts to fall below the optimal point. In addition, the simulations showed that increasing the transmitter antennas improves the secrecy energy efficiency considerably. Furthermore, increasing the transmitter antennas keeps the secrecy energy efficiency in its maximum level for a longer range of minimum required secrecy spectral efficiency.

Chapter 6

Secure Directional Modulation via Symbol-Level Precoding

Wireless transmission provides wide coverage, yet it exposes information. As an information-theoretic paradigm, secrecy rate derives bounds for secure transmission when the channel to the eavesdropper is known, however, it restricts us in practice and proper codings need to be developed to achieve these bounds. Here, we employ the concept of directional modulation and follow a signal processing approach to enhance the security of a multi-user MIMO communication system in the presence of a multi-antenna eavesdropper. Enhancing the security in this chapter means increasing the symbol error rate at the eavesdropper. Unlike the information-theoretic secrecy rate paradigm, we assume that the legitimate transmitter is not aware of its channel to the eavesdropper, which is a more realistic assumption. We show that when the eavesdropper has lower antennas than the users, regardless of the received signal SNR, it cannot recover any useful information, in addition, it has to go through extra noise enhancing processes to estimate the symbols when it has more antennas than the users. Using the channel knowledge and the intended symbols for the users, we design security enhancing symbol-level precoders for different transmitter and eavesdropper antenna configurations. We transform each design problem to a linearly constrained quadratic program and propose two algorithms, namely iterative algorithm and non-negative least squares, at each scenario for a computationally-efficient optimization design. Simulation results verify the analysis and show that the designed precoders outperform the benchmark scheme in terms of both power efficiency and security enhancement. The contribution of this chapter are published in [27, 28].

6.1 Introduction

6.1.1 Motivation

Wireless communications allows information flow through broadcasting; however, it may expose the information to unintended receivers, with eavesdroppers amongst them. To derive a bound for secure transmission, Wyner proposed the secrecy rate concept in his seminal paper [5] for discrete memoryless channels. The secrecy rate defines the bound for secure transmission and proper coding is being developed to achieve this bound [8]. However, the secrecy rate can restrict the communication system in some aspects. Primarily, the secrecy rate requires perfect or statistical knowledge of the eavesdropper's channel state information (CSI) [20–22, 179, 206], however, it may not be possible to acquire the perfect or statistical CSI of a passive eavesdropper in practice. In addition, in the secrecy rate approach, the transmission rate has to be lower than the achievable rate, which may conflict with the increasing rate demands in wireless communications. Furthermore, the transmit signal usually is required to follow a Gaussian distribution which is not the case in current digital communication systems.

Recently, there has been growing research interest on directional modulation technology and its security enhancing ability. As a pioneer, [17] implements a directional modulation transmitter using parasitic antenna. This system creates the desired amplitude and phase in a specific direction by varying the length of the reflector antennas for each symbol while scrambling the symbols in other directions. The authors of [18] suggest using a phased array at the transmitter and employ the genetic algorithm to derive the phase values of a phased array in order to create symbols in a specific direction. The directional modulation concept is later extended to directionally modulate symbols to more than one destination. In [158], the singular value decomposition (SVD) is used to directionally modulate symbols in a two user system. The authors of [159] derive the array weights to create two orthogonal far field patterns to directionally modulate two symbols to two different locations and [160] uses least-norm to derive the array weights and directionally modulate symbols towards multiple destinations in a multi-user multi-input multi-output (MIMO) system. The authors in [27] design the array weights of a directional modulation transmitter in a single-user MIMO system to minimize the power consumption while keeping the signal-to-noise ratio (SNR) of each received signal above a specific level. The directional modulation literature focuses on practical implementation and the security enhancing characteristics of this technology. On top of the works in the directional modulation literature where antennas excitation weight change on a symbol basis, the symbol-level precoding to create constructive interference between the transmitted symbols has been developed in [180–183] by focusing on the digital

processing of the signal before being fed to the antenna array. The main difference between directional modulation and the digital symbol-level precoding for constructive interference is that the former focuses on applying array weights in the analog domain such that the received signals on the receiving antennas have the desired amplitude and phase, whereas the latter uses symbol-level precoding for digital signal design at the transmitter to create constructive interference at the receiver. Furthermore, directional modulation was originally motivated by physical layer security, whereas symbol-level precoding by energy efficiency.

6.1.2 Contributions

In this chapter, we design the optimal precoder for a directional modulation transmitter to enhance the security in a quasi-static fading MIMO channel where a multi-antenna eavesdropper is present. Here, enhancing the security means increasing the SER at the eavesdropper. In directional modulation, users' channels and symbols meant for the users are used to design the precoder. The precoder is designed to induce the symbols on the receiver antennas rather than generating the symbols at the transmitter and sending them, which is the case in the conventional transmit precoding [23, 24]. In other words, in the directional modulation, the modulation happens in the radio frequency (RF) level while the arrays' emitted signals pass through the wireless channel. This way, we simultaneously communicate multiple interference-free symbols to multiple users. Also, the precoder is designed such that the receivers antennas can directly recover the symbols without CSI and equalization. Therefore, assuming the eavesdropper has a different channel compared to the users, it receives scrambled symbols. In fact, the channels between the transmitter and users act as secret keys [26] in the directional modulation. Furthermore, since the precoder depends on the symbols, the eavesdropper cannot calculate it. In contrast to the information theoretic secrecy rate paradigm, the directional modulation enhances the security by considering more practical assumptions. Particularly, directional modulation does not require the eavesdropper's CSI to enhance the security, furthermore, it does not reduce the transmission rate and signals are allowed to follow a non-Gaussian distribution. In light of the above, our contributions in this chapter can be summarized as follows:

1. The optimal symbol-level precoder is designed for a security enhancing directional modulation transmitter in a MIMO fading channel to communicate with arbitrary number of users and symbol streams. In addition, we derive the necessary condition for the existence of the precoder. The directional modulation literature mostly includes LoS analysis with one or limited number of users, and multi-user works do not perform security enhancing optimization.

2. It is shown that when the eavesdropper has less antennas than the transmitter, regardless of the SNR level, it cannot extract useful information from the received signal and when it has more antennas than the transmitter, it has to estimate the symbols by extra processes which enhance the noise. We minimize the transmission power for the former case and maximize the SER at the eavesdropper for the latter case to prevent successful decoding at the eavesdropper. This is done while keeping the SNR of users' received signals above a predefined threshold and thus the users' rate demands are satisfied. The directional modulation literature do not analyze the abilities of a multi-antenna eavesdropper and rely on the fact that it receives scrambled symbols

3. It is shown that in the conventional precoding, the eavesdropper needs to have more antennas than the receiver to estimate the symbols since the eavesdropper can calculate the precoder. In our design, the eavesdropper has to have more antennas than the transmitter since the precoder depends on both the channels and symbols. The transmitter, e.g., a base station, probably has more antennas than the receiver, hence, it is more likely to preserve the security in directional modulation, specially in a massive MIMO system.

4. The power and SNR minimization precoder design problems are simplified into a linearly-constrained quadratic programming problem. For faster design, we introduce new auxiliary variable to transform the constraint into equality and propose two different algorithms to solve the design problems. In the first algorithm, we use a penalty method to get an unconstrained problem and solve it by proposing using an iterative algorithm. Also, we prove that the algorithm converges to the optimal point. In the second one, we use the constraint to get a non-negative least squares design problem. For the latter, there are already fast techniques to solve the problem.

6.1.3 Additional Related Works to Directional Modulation

Array switching at the symbol rate is used in [161, 162] to induce the desired symbols. In connection with [17], [164] studies the far field area coverage of a parasitic antenna and shows that it is a convex region. The technique of [18] is implemented in [165] using a four element microstrip patch array where symbols are directionally modulated for Q-PSK modulation. The authors of [166] propose an iterative nonlinear optimization approach to design the array weights which minimizes the distance between the desired and the directly modulated symbols in a specific direction. The Fourier transform is used in [170, 171] to create the optimal constellation pattern for Q-PSK directional

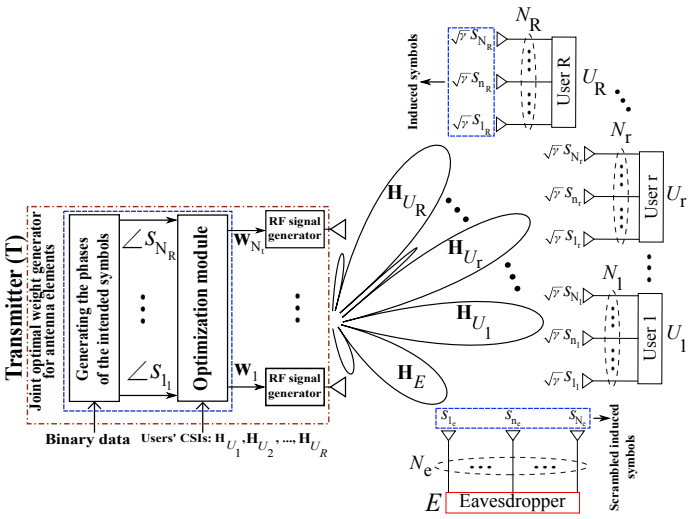


FIGURE 6.1: Generic architecture of a directional modulation transmitter, including the optimal security enhancing antenna weight generator using the proposed algorithms.

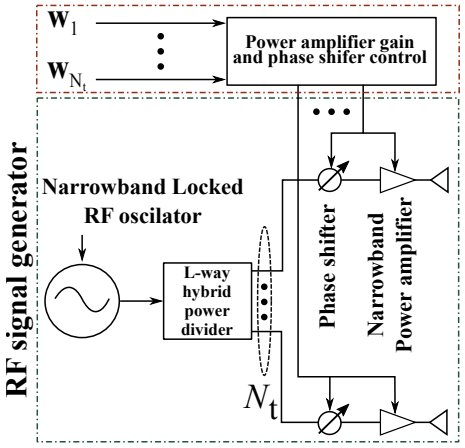


FIGURE 6.2: RF signal generation using actively driven elements, including high frequency power amplifiers and phase shifters.

modulation. In [158, 172–174] directional modulation is employed along with noise injection. The authors of [172, 173] utilize an orthogonal vector approach to derive the array weights in order to directly modulate the data and inject the artificial noise in the direction of the eavesdropper. The work of [172] is extended to retroactive arrays[1] in [174] for a multi-path environment. An algorithm including exhaustive search is used in [175] to adjust two-bit phase shifters for directly modulating information.

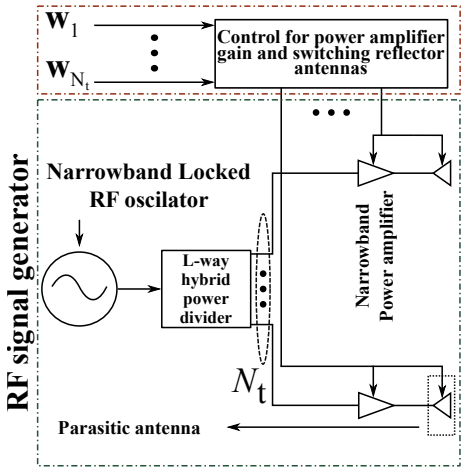


FIGURE 6.3: RF signal generation using power amplifiers and parasitic antennas.

6.2 Signal and System Model

We consider a communication network with a multi-antenna transmitter denoted by T, R multi-antenna users denoted by U_r for $r = 1, ..., R$ where the r-th user has N_r antennas, and a multi-antenna eavesdropper[2] denoted by E with N_e antennas, as shown in Fig. 6.1. In addition, all the communication channels are considered to be quasi-static block fading. We present two possible architectures for the RF signal generator block of Fig. 6.1 in Figures. 6.2 and 6.3. In Fig. 6.2, power amplifiers and phase shifters are used in each RF chain to adjust the gain and the phase of the transmitted signal from each antenna. In Fig. 6.3, we adapt the technique of [17] to adjust the phase using parasitic antennas in each RF chain. A parasitic antenna is comprised of a dipole antenna and multiple reflector antennas. Near field interactions between the dipole and reflector antennas creates the desired amplitude and phase in the far filed, which can be adjusted by switching the proper MOSFETs. When using parasitic, the channel from each parasitic antenna to the far field needs to be LoS, and we need to acquire the CSI of the fading channel from the far field of each parasitic antenna to the receiving antennas. For simplicity, we only consider the amplitude and phase of the received signals and drop $e^{j2\pi ft}$, which is the carrier frequency part.

After applying the optimal coefficients to array elements, the received signals by U_r and E are

$$\mathbf{y}_{U_r} = \mathbf{H}_{U_r}\mathbf{w} + \mathbf{n}_{U_r}, \ \forall r \tag{6.1}$$

$$\mathbf{y}_E = \mathbf{H}_E\mathbf{w} + \mathbf{n}_E, \ \forall r \tag{6.2}$$

[1] A retroactive antenna can retransmit a reference signal back along the path which it was incident despite the presence of spatial and/or temporal variations in the propagation path.

[2] The same system model and solution holds for multiple colluding single-antenna eavesdroppers.

where the random variables $\mathbf{n}_{U_r}$ and $\mathbf{n}_E$ denote the additive white Gaussian noise at U_r and E, respectively. The Gaussian random variables $\mathbf{n}_{U_r}$ and $\mathbf{n}_E$ are independent and identically distributed (i.i.d.) with $\mathbf{n}_{U_r} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{n_{U_r}} \mathbf{I}_{N_r \times N_r})$, and $\mathbf{n}_E \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{n_E} \mathbf{I}_{N_e \times N_e})$, respectively, where $\mathcal{CN}$ denotes a complex and circularly symmetric random variable. The signal $\mathbf{y}_{U_r}$ is an $N_r \times 1$ vector denoting the received signals by U_r, $\mathbf{y}_E$ is an $N_e \times 1$ vector denoting the received signals by E, $\mathbf{H}_{U_r} = [\mathbf{h}_{1_r}, ..., \mathbf{h}_{n_r}, ..., \mathbf{h}_{N_r}]^T$ is an $N_r \times N_t$ matrix denoting the channel from T to U_r, $\mathbf{h}_{n_r}$ is an $N_t \times 1$ vector containing the channel coefficients from the transmitter antennas to the n-th antenna of the r-th user, the channel for all users is $\mathbf{H}_U = [\mathbf{H}_{U_1}, ..., \mathbf{H}_{U_r}, ..., \mathbf{H}_{U_R}]^T$, $\mathbf{H}_E$ is an $N_e \times N_t$ matrix denoting the channel from T to E, and $\mathbf{w}$ is the transmit vector. In directional modulation, the elements of $\mathbf{H}_{U_r}\mathbf{w} = \left[\sqrt{\gamma}s_{1_r}, ..., \sqrt{\gamma}s_{n_r}, ..., \sqrt{\gamma}s_{N_r}\right]^T$ are the induced M-PSK symbols on the antennas of the r-th user where s_{n_r} is the induced M-PSK symbol on the n-th antenna of the r-th user with instantaneous unit energy, i.e., $|s_{n_r}|^2 = 1$ and γ is the SNR of the induced symbol. To detect the received symbols, U_r can apply conventional detectors on each antenna.

To consider the worst case, throughout the chapter, we assume that T knows only $\mathbf{H}_U$ while E knows both $\mathbf{H}_U$ and $\mathbf{H}_E$. In the following, we analyze the conditions under which we can enhance the system security.

6.3 Security analysis of directional modulation

In this section, we discuss the conditions under which the directional modulation can provide security benefits. We assume that E's channel is independent from those of the users, and to consider the worst case, we assume that $\mathbf{H}_E$ is full rank. Hence, the element numbers of $\mathbf{H}_E\mathbf{w}$, i.e., received signals on E's antennas, are different from those of $\mathbf{H}_{U_r}\mathbf{w}$, i.e., received signals on receiver antennas, for $r = 1, ..., R$. Since $\mathbf{w}$ depends on the symbols and E cannot calculate it, E has to remove $\mathbf{H}_E$ to estimate $\mathbf{w}$, and then multiply the estimated $\mathbf{w}$ by $\mathbf{H}_U$ to estimate the symbols. For $N_e < N_t$, E cannot estimate $\mathbf{H}_U\mathbf{w}$, however, when $N_e \geq N_t$, E can estimate $\mathbf{w}$ as follows

$$\widehat{\mathbf{w}} = \left(\mathbf{H}_E^H \mathbf{H}_E\right)^{-1} \mathbf{H}_E^H \mathbf{y}_E = \mathbf{w} + \left(\mathbf{H}_E^H \mathbf{H}_E\right)^{-1} \mathbf{H}_E^H \mathbf{n}_E, \tag{6.3}$$

where $\widehat{\mathbf{w}}$ is the estimated $\mathbf{w}$ at E. Next, E can multiply $\widehat{\mathbf{w}}$ by $\mathbf{H}_U$ to estimate the signals at receiver antennas, $\mathbf{H}_U\widehat{\mathbf{w}}$, as

$$\mathbf{H}_U\widehat{\mathbf{w}} = \mathbf{H}_U\mathbf{w} + \mathbf{H}_U\left(\mathbf{H}_E^H \mathbf{H}_E\right)^{-1} \mathbf{H}_E^H \mathbf{n}_E. \tag{6.4}$$

Through (6.3) to (6.4), E virtually puts itself in the location of the users, since we assume that E knows the users' channels $\mathbf{H}_U$, to estimate the received signal by them. This way, E gets access to the secret key, which is observing the signals from users' point of view, however, the required process increases the noise at E.

Remark 6.1. Using a large scale array transmitter, it is more probable to satisfy the condition $N_e < N_t$. Hence, the directional modulation technique seems to be a good candidate to enhance the security when the transmitter is equipped with a large scale array. ■

Remark 6.2. Assuming that the legitimate channel is reciprocal, the users can transmit pilots to T so it can estimate $\mathbf{H}_U$. This way, we avoid the additional downlink channel estimation and the users do not have to send feedback bits to T, hence, E cannot estimate $\mathbf{H}_U$. Assuming that E knows the channel from T to itself, i.e., $\mathbf{H}_E$, it can estimate $\mathbf{w}$ for $N_e \geq N_t$ as in (6.3), but it cannot perform (6.4) to estimate the received signals on the receiver antennas. ■

In the next section, optimal symbol-level precoders for the directional modulation are designed to enhance the security.

6.4 Optimal Precoder Design for Directional Modulation

In this section, we define the underlaying problems to design the security enhancing symbol-level precoder for the directional modulation when $N_e < N_t$ and $N_e \geq N_t$, respectively.

6.4.1 The Case of Strong Transmitter ($N_e < N_t$)

Since $N_e < N_t$, according to Section 6.3, E cannot estimate $\mathbf{w}$ and extract useful information from $\mathbf{y}_E$. In wireless transmission, adaptive coding and modulation (ACM) is used to enhance the link performance and the channel capacity. In ACM, the transmission power, coding rate, and the modulation order is set according to the channel signal to noise ratio (SNR) [238]. Based on this, we preserve the SNR of the induced symbol on the receiver antenna above or equal to a specific level to successfully decode it. Here, we only focus on the SNR of an uncoded signal since considering SNR of a coded transmission based on ACM is beyond the scope of this chapter.

To have a convex design problem and avoid an NP-hard problem [239], we separately consider amplitudes of the in-phase and quadrature-phase parts of the induced M-PSK

symbol, s_{n_r}, on the receiver antenna instead of the power of s_{n_r}. Since the real and imaginary valued parts of s_{n_r} may differ in amplitude, and the angle of s_{n_r} is fixed, we need to increase the real and imaginary valued parts of s_{n_r} in the same proportion, not the same amount. If we show the real and imaginary valued parts of s_{n_r} as $\mathrm{Re}\left(s_{k,r}\right)$ and $\mathrm{Im}\left(s_{k,r}\right)$, the required in-phase and quadrature-phase thresholds are defined as

$$\sqrt{\gamma}\mathrm{Re}\left(s_{n_r}\right),\ \sqrt{\gamma}\mathrm{Im}\left(s_{n_r}\right). \tag{6.5}$$

Since $|s_{n_r}|^2 = 1$, we can see that $\gamma = \gamma\mathrm{Re}^2\left(s_{n_r}\right) + \gamma\mathrm{Im}^2\left(s_{n_r}\right)$.

We design the directional modulation precoder to minimize the total transmit power such that 1) the signals received by the n-th antenna of the r-th user result in a phase equal to that of s_{n_r}, and 2) the signals received by the n-th antenna of the r-th user create in-phase and quadrature-phase signal levels satisfying the thresholds defined in (6.5). Accordingly, the precoder design problem is defined as

$$\begin{aligned}
\min_{\mathbf{w}}\ & \|\mathbf{w}\|^2 \\
\text{s.t.}\ & \arg\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) = \arg\left(s_{n_r}\right), && \text{(6.6a)}\\
& \mathrm{Re}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Re}\left(s_{n_r}\right), && \text{(6.6b)}\\
& \mathrm{Im}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Im}\left(s_{n_r}\right), && \text{(6.6c)}
\end{aligned}$$

for $r = 1, ..., R$ and $n = 1, ..., N$. Due to (6.6a), $\mathrm{Re}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right)$ and $\mathrm{Im}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right)$ have the same sign as $\mathrm{Re}\left(s_{n_r}\right)$ and $\mathrm{Im}\left(s_{n_r}\right)$, respectively. If both sides of (6.6b) or (6.6c) are negative, the signal level constraints may not be satisfied. Since (6.6a) holds at the optimal point, $\mathrm{Re}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right)$ and $\mathrm{Im}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right)$ have the same sign as $\mathrm{Re}\left(s_{n_r}\right)$ and $\mathrm{Im}\left(s_{n_r}\right)$, therefore, we can multiply both sides of the signal level constraints in (6.6b) and (6.6c) by $\mathrm{Re}(s_{n_r})$ and $\mathrm{Im}(s_{n_r})$, respectively, to get

$$\begin{aligned}
\min_{\mathbf{w}}\ & \|\mathbf{w}\|^2 \\
\text{s.t.}\ & \arg\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) = \arg\left(s_{n_r}\right), && \text{(6.7a)}\\
& \mathrm{Re}\left(s_{n_r}\right)\mathrm{Re}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Re}^2\left(s_{n_r}\right), && \text{(6.7b)}\\
& \mathrm{Im}\left(s_{n_r}\right)\mathrm{Im}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Im}^2\left(s_{n_r}\right). && \text{(6.7c)}
\end{aligned}$$

We can rewrite the phase constraint in (6.7a) as

$$\mathrm{Re}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right)\alpha_{n_r} - \mathrm{Im}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) = 0,\quad \forall\, n,\ \forall\, r, \tag{6.8}$$

where $\alpha_{n_r} = \tan\left(s_{n_r}\right)$. Since $\tan(\cdot)$ repeats after a π radian period, symbols with different phases can have the same tan value, e.g., $\tan\left(\frac{\pi}{4}\right) = \tan\left(\frac{3\pi}{4}\right)$. Therefore,

replacing (6.7a) with (6.8) creates ambiguity. To avoid this, we can add the constraints

$$\begin{aligned} &\mathrm{Re}\left(s_{n_r}\right)\mathrm{Re}\left(\mathbf{h}_{n_r}^{T}\mathbf{w}\right) \geq 0, \\ &\mathrm{Im}\left(s_{n_r}\right)\mathrm{Im}\left(\mathbf{h}_{n_r}^{T}\mathbf{w}\right) \geq 0, \end{aligned} \tag{6.9}$$

to the design problem (6.7) to avoid ambiguity. Interestingly, constraints (6.9) are already present in (6.7b) and (6.7c). Note that (6.8) and (6.9) together are equivalent to (6.6a), so the required condition to go from (6.6) to (6.7) still hold. Putting together the constraints (6.8), (6.7b), and (6.7c) for all the users, (6.7) is written into the following compact form

$$\begin{aligned} \min_{\mathbf{w}} \quad & \|\mathbf{w}\|^2 \\ \text{s.t.} \quad & \mathbf{A}\mathrm{Re}\left(\mathbf{H}_U\mathbf{w}\right) - \mathrm{Im}\left(\mathbf{H}_U\mathbf{w}\right) = \mathbf{0}, && \text{(6.10a)} \\ & \mathrm{Re}\left(\mathbf{S}\right)\mathrm{Re}\left(\mathbf{H}_U\mathbf{w}\right) \geq \sqrt{\gamma}\,\mathbf{s}_r, && \text{(6.10b)} \\ & \mathrm{Im}\left(\mathbf{S}\right)\mathrm{Im}\left(\mathbf{H}_U\mathbf{w}\right) \geq \sqrt{\gamma}\,\mathbf{s}_i, && \text{(6.10c)} \end{aligned}$$

where $\mathbf{S} = \mathrm{diag}\left(\mathbf{s}\right)$, $\mathbf{s}$ is an $N_U \times 1$ vector containing all the intended M-PSK symbols for the users with $N_U = \sum_{r=1}^{R} N_r$, $\mathbf{s}_r = \mathrm{Re}\left(\mathbf{s}\right) \circ \mathrm{Re}\left(\mathbf{s}\right)$, $\mathbf{s}_i = \mathrm{Im}\left(\mathbf{s}\right) \circ \mathrm{Im}\left(\mathbf{s}\right)$, $\mathbf{A} = \mathrm{diag}\left(\boldsymbol{\alpha}\right)$, $\boldsymbol{\alpha} = \left[\alpha_{1_1}, ..., \alpha_{n_r}, ..., \alpha_{N_R}\right]^T$.

To remove the real and imaginary valued parts from (6.10), we can use $\mathbf{H}_U = \mathrm{Re}\left(\mathbf{H}_U\right) + i\mathrm{Im}\left(\mathbf{H}_U\right)$ and $\mathbf{w} = \mathrm{Re}\left(\mathbf{w}\right) + i\mathrm{Im}\left(\mathbf{w}\right)$ presentations to separate the real and imaginary valued components of $\mathbf{H}_U\mathbf{w}$ as

$$\begin{aligned} \mathbf{H}_U\mathbf{w} =& \mathrm{Re}\left(\mathbf{H}_U\right)\mathrm{Re}\left(\mathbf{w}\right) - \mathrm{Im}\left(\mathbf{H}_U\right)\mathrm{Im}\left(\mathbf{w}\right) \\ &+ i\left[\mathrm{Re}\left(\mathbf{H}_U\right)\mathrm{Im}\left(\mathbf{w}\right) + \mathrm{Im}\left(\mathbf{H}_U\right)\mathrm{Re}\left(\mathbf{w}\right)\right], \end{aligned} \tag{6.11}$$

which leads into the following expressions

$$\mathrm{Re}\left(\mathbf{H}_U\mathbf{w}\right) = \mathbf{H}_{U_1}\widetilde{\mathbf{w}}, \;\; \mathrm{Im}\left(\mathbf{H}_U\mathbf{w}\right) = \mathbf{H}_{U_2}\widetilde{\mathbf{w}}, \tag{6.12}$$

where $\widetilde{\mathbf{w}} = \left[\mathrm{Re}\left(\mathbf{w}^T\right), \mathrm{Im}\left(\mathbf{w}^T\right)\right]^T$, $\mathbf{H}_{U_1} = \left[\mathrm{Re}\left(\mathbf{H}_U\right), -\mathrm{Im}\left(\mathbf{H}_{\mathrm{U}}\right)\right]$, and $\mathbf{H}_{U_2} = \left[\mathrm{Im}\left(\mathbf{H}_{\mathrm{U}}\right), \mathrm{Re}\left(\mathbf{H}_{\mathrm{U}}\right)\right]$. Also, it is easy to see that $\|\widetilde{\mathbf{w}}\|^2 = \|\mathbf{w}\|^2$.

Using the equivalents of $\mathrm{Re}\left(\mathbf{H}_U\mathbf{w}\right)$ and $\mathrm{Im}\left(\mathbf{H}_U\mathbf{w}\right)$ derived in (6.12), (6.10) transforms into

$$\begin{aligned}
\min_{\widetilde{\mathbf{w}}} \quad & \|\widetilde{\mathbf{w}}\|^2 \\
\text{s.t.} \quad & \left(\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}\right)\widetilde{\mathbf{w}} = \mathbf{0}, && \text{(6.13a)} \\
& \mathrm{Re}\left(\mathbf{S}\right)\mathbf{H}_{U_1}\widetilde{\mathbf{w}} \geq \sqrt{\gamma}\,\mathbf{s}_r, && \text{(6.13b)} \\
& \mathrm{Im}\left(\mathbf{S}\right)\mathbf{H}_{U_2}\widetilde{\mathbf{w}} \geq \sqrt{\gamma}\,\mathbf{s}_i. && \text{(6.13c)}
\end{aligned}$$

Proposition 6.3. *A necessary condition for the existence of the optimal precoder for the directional modulation is* $N_t > \frac{r^{'}}{2}$ *where* $r^{'}$ *is the rank of* $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$*. If* $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$ *is full rank, the necessary condition becomes* $N_t > \frac{N_U}{2}$*, which means that the number of transmit antennas needs to be more than half of the total number of receiver antennas.*

Proof. Constraint (6.13a), shows that $\widetilde{\mathbf{w}}$ should lie in the null space of the matrix $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$. If the SVD of $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$ is shown by $\mathbf{U}\Sigma\mathbf{V}^H$, the orthonormal basis for the null space of $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$ are the last $2N_t - r^{'}$ columns of the matrix $\mathbf{V}$ with $r^{'}$ being the rank of $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$ [240]. If $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$ is full rank, we have $r^{'} = N_U$. For (6.13) to be feasible, the mentioned null space should exist, meaning that $2N_t - r^{'} > 0$. □

Provided that the necessary condition of Proposition 6.3 is met, a sufficient condition can be proposed from a geometrical point of view; namely that the feasible set of (6.15) is not empty. This holds if and only if the intersection of the linear spaces in the constraint set constitutes a non-empty set.

According to Proposition 6.3, the null space of $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$ spans $\widetilde{\mathbf{w}}$ as $\widetilde{\mathbf{w}} = \mathbf{E}\boldsymbol{\lambda}$ where

$$\mathbf{E} = \left[\mathbf{v}_{r^{'}+1}, ..., \mathbf{v}_{2N_t}\right], \ \boldsymbol{\lambda} = \left[\lambda_1, ..., \lambda_{2N_t - r^{'}}\right]. \tag{6.14}$$

By replacing $\widetilde{\mathbf{w}}$ with $\mathbf{E}\boldsymbol{\lambda}$, (6.13) boils down into

$$\begin{aligned}
\min_{\boldsymbol{\lambda}} \quad & \|\boldsymbol{\lambda}\|^2 \\
\text{s.t.} \quad & \mathrm{Re}\left(\mathbf{S}\right)\mathbf{H}_{U_1}\mathbf{E}\boldsymbol{\lambda} \geq \sqrt{\gamma}\,\mathbf{s}_r, \\
& \mathrm{Im}\left(\mathbf{S}\right)\mathbf{H}_{U_2}\mathbf{E}\boldsymbol{\lambda} \geq \sqrt{\gamma}\,\mathbf{s}_i, && \text{(6.15)}
\end{aligned}$$

which can be written into the following compact form[3]

$$\begin{aligned} \min_{\boldsymbol{\lambda}} \quad & \|\boldsymbol{\lambda}\|^2 \\ \text{s.t.} \quad & \mathbf{B}\boldsymbol{\lambda} \geq \sqrt{\gamma}\mathbf{s}_T, \end{aligned} \tag{6.16}$$

where

$$\mathbf{B} = \begin{bmatrix} \mathrm{Re}\,(\mathbf{S})\,\mathbf{H}_{U_1}\mathbf{E} \\ \mathrm{Im}\,(\mathbf{S})\,\mathbf{H}_{U_2}\mathbf{E} \end{bmatrix}, \ \mathbf{s}_T = \left[\mathbf{s}_r^T, \mathbf{s}_i^T\right]^T. \tag{6.17}$$

Problem (6.16) is a convex linearly constrained quadratic programming problem and can be solved efficiently using standard convex optimization techniques. The design problem (6.18) needs to be solved once for each set of the symbol, $\mathbf{s}_T$. Using optimization packages such as CVX to solve (6.16) can be time consuming, hence, we propose two other approaches to solve (6.16).

6.4.1.1 Iterative solution

In this part, we propose an iterative approach to solve (6.16). To do so, first, we define an auxiliary real valued vector denoted by $\mathbf{u}$ to change the inequality constraint of (6.16) into equality as

$$\begin{aligned} \min_{\boldsymbol{\lambda},\mathbf{u}} \quad & \|\boldsymbol{\lambda}\|^2 \\ \text{s.t.} \quad & \mathbf{B}\boldsymbol{\lambda} = \sqrt{\gamma}\mathbf{s}_T + \mathbf{u}, \ \mathbf{u} \geq \mathbf{0}. \end{aligned} \tag{6.18}$$

Using the penalty method [224], we can write (6.16) as an unconstrained optimization problem

$$\min_{\boldsymbol{\lambda},\mathbf{u}\geq 0} \ \|\boldsymbol{\lambda}\|^2 + \eta\|\mathbf{B}\boldsymbol{\lambda} - (\sqrt{\gamma}\mathbf{s}_T + \mathbf{u})\|^2, \tag{6.19}$$

which is equivalent to (6.16) when $\eta \to \infty$. We can solve (6.19) using an iterative approach by first optimizing $\mathbf{u}$ and considering $\boldsymbol{\lambda}$ to be fixed, and then optimizing $\mathbf{u}$ and considering $\boldsymbol{\lambda}$ to be fixed. In the following, we mention these two optimization problems and their closed-form solutions.

When optimizing over $\mathbf{u}$ and keeping $\boldsymbol{\lambda}$ fixed, the optimization problem is

$$\min_{\mathbf{u}\geq 0} \ \|\mathbf{u} - (\mathbf{B}\boldsymbol{\lambda} - \sqrt{\gamma}\mathbf{s}_T)\|^2. \tag{6.20}$$

[3]The design problem (6.16) can be extended to M-QAM modulation [182] by changing the constraint into equality which is beyond the scope of this thesis.

The closed-form solution of (6.20) is given in Lemma 6.4.

Lemma 6.4. *The closed-form solution of* (6.20) *is* $\mathbf{u}^\star = \left(\mathbf{B}\boldsymbol{\lambda} - \sqrt{\gamma}\mathbf{s}_T\right)_+$.

Proof. To solve (6.20), we need to minimize the distance between the vectors $\mathbf{u}$ and $\left(\mathbf{B}\boldsymbol{\lambda} - \sqrt{\gamma}\mathbf{s}_T\right)$. Since $\boldsymbol{\lambda}$ is fixed, the elements of $\left(\mathbf{B}\boldsymbol{\lambda} - \sqrt{\gamma}\mathbf{s}_T\right)$ are known. If an element of $\mathbf{B}\boldsymbol{\lambda} - \sqrt{\gamma}\mathbf{s}_T$ is nonnegative, we pick up the same value for the corresponding element of $\mathbf{u}$. If an element of $\mathbf{B}\boldsymbol{\lambda} - \sqrt{\gamma}\mathbf{s}_T$ is negative, we pick up zero for the corresponding element of $\mathbf{u}$ since $\mathbf{u} \geq \mathbf{0}$. This is equivalent to picking up $\mathbf{u}$ as

$$\mathbf{u}^\star = \left(\mathbf{B}\boldsymbol{\lambda} - \sqrt{\gamma}\mathbf{s}_T\right)_+. \tag{6.21}$$

□

When optimizing over $\boldsymbol{\lambda}$ and keeping $\mathbf{u}$ fixed, the optimization problem is

$$\min_{\boldsymbol{\lambda}} \ \|\boldsymbol{\lambda}\|^2 + \eta\|\mathbf{B}\boldsymbol{\lambda} - (\sqrt{\gamma}\mathbf{s}_T + \mathbf{u})\|^2. \tag{6.22}$$

The closed-form solution of (6.22) is given in Lemma 6.5.

Lemma 6.5. *The closed-form solution of* (6.22) *is* $\boldsymbol{\lambda}^\star = \left(\frac{\mathbf{I}}{\eta} + \mathbf{B}^T\mathbf{B}\right)^{-1}\mathbf{B}^T(\mathbf{a} + \mathbf{u})$.

Proof. First, we expand (6.22) as

$$\begin{aligned} f(\boldsymbol{\lambda}) =& \|\boldsymbol{\lambda}\|^2 + \eta\|\mathbf{B}\boldsymbol{\lambda} - (\gamma\mathbf{s}_T + \mathbf{u})\|^2 \\ =& \boldsymbol{\lambda}^T\left(\mathbf{I} + \eta\mathbf{B}^T\mathbf{B}\right)\boldsymbol{\lambda} - 2\eta\boldsymbol{\lambda}^T\left(\mathbf{B}^T\gamma\mathbf{s}_T + \mathbf{B}^T\mathbf{u}\right) \\ &+ \eta(\sqrt{\gamma}\mathbf{s}_T + \mathbf{u})^T(\sqrt{\gamma}\mathbf{s}_T + \mathbf{u}). \end{aligned} \tag{6.23}$$

Taking the derivative of $f(\boldsymbol{\lambda})$ with respect to $\boldsymbol{\lambda}$ yields

$$\boldsymbol{\lambda}^\star = \left(\frac{\mathbf{I}}{\eta} + \mathbf{B}^T\mathbf{B}\right)^{-1}\mathbf{B}^T(\mathbf{a} + \mathbf{u}). \tag{6.24}$$

Since $\mathbf{B}^T\mathbf{B}$ is positive semidefinite, addition of $\frac{\mathbf{I}}{\eta}$ to $\mathbf{B}^T\mathbf{B}$ for $\eta \neq \infty$ leads into diagonal loading of $\mathbf{B}^T\mathbf{B}$, which makes $\frac{\mathbf{I}}{\eta} + \mathbf{B}^T\mathbf{B}$ invertible. □

Using the closed-form solutions mentioned in Lemmas 6.4 and 6.5, we propose Algorithm 2 to solve (6.19), where the matrix inversion in (6.24) needs to be calculated once per symbol transmission.

Lemma 6.6. *Algorithm 2 monotonically converges to the optimal point.*

Algorithm 2 Iterative approach to solve (6.19)

1: Pick up $\boldsymbol{\lambda}_n \in \mathbb{R}^{2N_t}$ and $\eta \in (0, \infty]$;
2: Substitute $\boldsymbol{\lambda}_n$ in (6.21) to get $\mathbf{u}_n$;
3: Substitute $\mathbf{u}_n$ in (6.24) to get $\boldsymbol{\lambda}_{n+1}$;
4: **if** $\|\boldsymbol{\lambda}_n - \boldsymbol{\lambda}_{n+1}\| \geq \epsilon$ **then**
5: $n = n + 1$;
6: **Go to** 1;
7: **end if**

Proof. Let's denote the objective function in (6.19) by $f(\boldsymbol{\lambda}, \mathbf{u})$. Assume $\boldsymbol{\lambda}_0$ and $\mathbf{u}_0$ are initial values of $f(\boldsymbol{\lambda}, \mathbf{u})$. Using $\boldsymbol{\lambda}_0$ in Algorithm 2 gives us $\mathbf{u}^\star$ and $\boldsymbol{\lambda}^\star$ from (6.21) and (6.24), respectively, which results in

$$f(\boldsymbol{\lambda}^\star, \mathbf{u}^\star) \leq f(\boldsymbol{\lambda}_0, \mathbf{u}^\star) \leq f(\boldsymbol{\lambda}_0, \mathbf{u}_0). \tag{6.25}$$

Since fixing $\boldsymbol{\lambda}$, (6.20), or $\mathbf{u}$, (6.22), leads into a convex function, each iteration in Algorithm 2 monotonically gets closer to the optimal point. This along with the fact that $f(\boldsymbol{\lambda}, \mathbf{u})$ is lower bounded at zero, guarantees the convergence of Algorithm 2 to the optimal point. □

6.4.1.2 Non-negative least squares

We can derive $\boldsymbol{\lambda}$ using the constraint of (6.18) as

$$\boldsymbol{\lambda} = \mathbf{B}^\dagger (\sqrt{\gamma}\mathbf{s}_T + \mathbf{u}). \tag{6.26}$$

Replacing the $\boldsymbol{\lambda}$ derived in (6.26) back into the objective of (6.18) yields

$$\begin{aligned} \min_{\mathbf{u}} \quad & \left\| \mathbf{B}^\dagger \mathbf{u} + \sqrt{\gamma}\mathbf{B}^\dagger \mathbf{s}_T \right\|^2 \\ \text{s.t.} \quad & \mathbf{u} \geq 0, \end{aligned} \tag{6.27}$$

which is a non-negative least squares optimization problem. Since $\mathbf{B}^\dagger$ and $\sqrt{\gamma}\mathbf{B}^\dagger \mathbf{s}_T$ are real valued, we can use the method of [241] or its fast version [242] to solve (6.27). Multiple loops exist in algorithm used to solve non-negative least squares problem which their iterations depend on the problem parameters, hence, the complexity of the algorithm may not be derived analytically [241]. However, we present numerical results in Section 6.5 to evaluate the computational time of this algorithm. Similar to Section 6.4.1.1, $\mathbf{B}^\dagger$ needs to be calculated once per symbol transmission.

6.4.2 The Case of Strong Eavesdropper ($N_e \geq N_t$)

In this case, as (6.4) shows, E can estimate the signals on receiver antennas, however, this process enhances the noise at E. This capability of E comes from the fact that it has more antennas than T and owns global CSI knowledge, which puts E in a superior position compared to T from hardware and CSI knowledge point of view. Nevertheless, there is still one possible way to enhance the security. Ignoring the noise, the estimated symbols by E are equal to those induced on receiver antennas, therefore, we can design the precoder such that the SNR of the induced s_{n_r} becomes equal to the required level for successful decoding, which is defined by ACM. However, due to enhanced noise at E, the SNR level at E is lower than that of the users, which may prevent successful decoding of the M-PSK symbol at E. Based on this, we can minimize the sum power of the received signals at the users, $\|\mathbf{H}_U\mathbf{w}\|^2$, which is the same as the sum power of the estimated signals at E. Since the power of the received signal on each receiving antenna is constrained, minimizing the sum power leads into minimizing the power of the signal on each receiving antenna. This results in a sort of *"security fairness"* among the users. Accordingly, the precoder design problem can be defined as

$$\begin{aligned}
\min_{\mathbf{w}} \quad & \|\mathbf{H}_U\mathbf{w}\|^2 \\
\text{s.t.} \quad & \arg\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) = \arg\left(s_{n_r}\right), && \text{(6.28a)} \\
& \mathrm{Re}\left(s_{n_r}\right)\mathrm{Re}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Re}^2\left(s_{n_r}\right), && \text{(6.28b)} \\
& \mathrm{Im}\left(s_{n_r}\right)\mathrm{Im}\left(\mathbf{h}_{n_r}^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Im}^2\left(s_{n_r}\right), && \text{(6.28c)}
\end{aligned}$$

for $r = 1, ..., R$ and $n = 1, ..., N$. Following a similar procedure as in Section 6.4.1, (6.28) can be transformed to

$$\begin{aligned}
\min_{\mathbf{w}} \quad & \|\mathbf{H}_U\mathbf{w}\|^2 \\
\text{s.t.} \quad & \mathbf{A}\mathrm{Re}\left(\mathbf{H}_U\mathbf{w}\right) - \mathrm{Im}\left(\mathbf{H}_U\mathbf{w}\right) = \mathbf{0}, \\
& \mathrm{Re}\left(\mathbf{S}\right)\mathrm{Re}\left(\mathbf{H}_U\mathbf{w}\right) \geq \sqrt{\gamma}\,\mathbf{s}_r, \\
& \mathrm{Im}\left(\mathbf{S}\right)\mathrm{Im}\left(\mathbf{H}_U\mathbf{w}\right) \geq \sqrt{\gamma}\,\mathbf{s}_i. && \text{(6.29)}
\end{aligned}$$

Using (6.11) to (6.12), we expand $\|\mathbf{H}_U\mathbf{w}\|^2$ as

$$\begin{aligned}
\|\mathbf{H}_U\mathbf{w}\|^2 &= \widetilde{\mathbf{w}}^T\mathbf{H}_{U_1}^T\mathbf{H}_{U_1}\widetilde{\mathbf{w}} + \widetilde{\mathbf{w}}^T\mathbf{H}_{U_2}^T\mathbf{H}_{U_2}\widetilde{\mathbf{w}} \\
&= \widetilde{\mathbf{w}}^T\left(\mathbf{H}_{U_1}^T\mathbf{H}_{U_1} + \mathbf{H}_{U_2}^T\mathbf{H}_{U_2}\right)\widetilde{\mathbf{w}}, && \text{(6.30)}
\end{aligned}$$

which along with (6.12) helps us to convert (6.29) into

$$\begin{aligned} \min_{\widetilde{\mathbf{w}}} \quad & \widetilde{\mathbf{w}}^T \left(\mathbf{H}_{U_1}^T \mathbf{H}_{U_1} + \mathbf{H}_{U_2}^T \mathbf{H}_{U_2} \right) \widetilde{\mathbf{w}} \\ \text{s.t.} \quad & \left(\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2} \right) \widetilde{\mathbf{w}} = \mathbf{0}, \\ & \mathrm{Re}\left(\mathbf{S} \right) \mathbf{H}_{U_1} \widetilde{\mathbf{w}} \geq \sqrt{\gamma}\, \mathbf{s}_r, \\ & \mathrm{Im}\left(\mathbf{S} \right) \mathbf{H}_{U_2} \widetilde{\mathbf{w}} \geq \sqrt{\gamma}\, \mathbf{s}_i. \end{aligned} \tag{6.31}$$

For (6.31) to be feasible, $\widetilde{\mathbf{w}}$ has to be in the null space of $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$. Hence, we can write $\widetilde{\mathbf{w}}$ as a linear combination of the null space basis of $\mathbf{A}\mathbf{H}_{U_1} - \mathbf{H}_{U_2}$ which yields $\widetilde{\mathbf{w}} = \mathbf{E}\boldsymbol{\lambda}$, where $\mathbf{E}$ and $\boldsymbol{\lambda}$ are as in (6.14). This way, (6.31) boils down to[4]

$$\begin{aligned} \min_{\boldsymbol{\lambda}} \quad & \boldsymbol{\lambda}^T \mathbf{E}^T \left(\mathbf{H}_{U_1}^T \mathbf{H}_{U_1} + \mathbf{H}_{U_2}^T \mathbf{H}_{U_2} \right) \mathbf{E}\boldsymbol{\lambda} \\ \text{s.t.} \quad & \mathbf{B}\boldsymbol{\lambda} \geq \sqrt{\gamma}\mathbf{s}_T, \end{aligned} \tag{6.32}$$

where $\mathbf{B}$ and $\mathbf{s}_T$ are as in (6.17). Similar as in Section 6.4.1, in the following, we propose and iterative algorithm and non-negative least squares formulation to solve (6.32).

6.4.2.1 Iterative solution

By introducing the new variable $\mathbf{u}$, we can rewrite (6.32) as

$$\begin{aligned} \min_{\boldsymbol{\lambda},\mathbf{u}} \quad & \boldsymbol{\lambda}^T \mathbf{E}^T \left(\mathbf{H}_{U_1}^T \mathbf{H}_{U_1} + \mathbf{H}_{U_2}^T \mathbf{H}_{U_2} \right) \mathbf{E}\boldsymbol{\lambda} \\ \text{s.t.} \quad & \mathbf{B}\boldsymbol{\lambda} = \sqrt{\gamma}\mathbf{s}_T + \mathbf{u}. \end{aligned} \tag{6.33}$$

We can adapt Algorithm 2 to solve (6.32) by replacing the solution to $\boldsymbol{\lambda}^\star$ as

$$\boldsymbol{\lambda}^\star = \left(\frac{\mathbf{E}^T \left(\mathbf{H}_{U_1}^T \mathbf{H}_{U_1} + \mathbf{H}_{U_2}^T \mathbf{H}_{U_2} \right) \mathbf{E}}{\eta} + \mathbf{B}^T\mathbf{B} \right)^{-1} \mathbf{B}^T \left(\mathbf{a} + \mathbf{u} \right), \tag{6.34}$$

which is derived using a similar procedure as in Section 6.4.1.1. Similar as in (6.24), the matrix inversion in (6.34) needs to be calculated only once per symbol transmission.

6.4.2.2 Non-negative least squares

Assuming that $\mathbf{H}_{U_1}$ and $\mathbf{H}_{U_2}$ are non-singular, the matrix $\mathbf{E}^T \left(\mathbf{H}_{U_1}^T \mathbf{H}_{U_1} + \mathbf{H}_{U_2}^T \mathbf{H}_{U_2} \right) \mathbf{E}$ is positive definite, hence, its Cholesky decomposition $\mathbf{E}^T \left(\mathbf{H}_{U_1}^T \mathbf{H}_{U_1} + \mathbf{H}_{U_2}^T \mathbf{H}_{U_2} \right) \mathbf{E} = \mathbf{L}\mathbf{L}^T$

[4]The design problem (6.32) can be extended to M-QAM modulation by changing the constraint into equality which is beyond the scope of this thesis.

exists and can be used in order to rewrite (6.33) as

$$\begin{aligned} &\min_{\boldsymbol{\lambda},\mathbf{u}} \ \left\|\mathbf{L}^T\boldsymbol{\lambda}\right\|^2 \\ &\text{s.t.} \quad \mathbf{B}\boldsymbol{\lambda} = \sqrt{\gamma}\mathbf{s}_T + \mathbf{u}. \end{aligned} \tag{6.35}$$

We can derive $\boldsymbol{\lambda}$ using the constraint of (6.35) as $\boldsymbol{\lambda} = \mathbf{B}^\dagger\left(\sqrt{\gamma}\mathbf{s}_T + \mathbf{u}\right)$ and replace it back into the objective of (6.35) to get

$$\begin{aligned} &\min_{\mathbf{u}} \ \left\|\mathbf{L}^T\mathbf{B}^\dagger\mathbf{u} + \mathbf{L}^T\mathbf{B}^\dagger\sqrt{\gamma}\mathbf{s}_T\right\|^2 \\ &\text{s.t.} \quad \mathbf{u} \geq \mathbf{0}, \end{aligned} \tag{6.36}$$

which is a non-negative least squares optimization problem. Since $\mathbf{L}^T\mathbf{B}^\dagger$ and $\mathbf{L}^T\mathbf{B}^\dagger\sqrt{\gamma}\mathbf{s}_T$ are real valued, we can use [241, 242] to solve (6.36) in an efficient way.

6.5 Simulation Results

In this part, we present different simulation scenarios to analyze the security and the performance of the directional modulation scheme for different precoding designs, and compare them with a benchmark scheme. In all simulations, channels are considered to be quasi static block Rayleigh which are generated using i.i.d. complex Gaussian random variables with distribution$\sim \mathcal{CN}(0,1)$ and remain fixed during the interval that the M-PSK symbols are being induced at the receiver. Also, the noise is generated using i.i.d. complex Gaussian random variables with distribution$\sim \mathcal{CN}(0,\sigma^2)$, and the modulation order used in all of the scenarios is uncoded 8-PSK modulation. Here, we simulate each precoder for both strong transmitter, $N_e < N_t$, and strong eavesdropper, $N_e \geq N_t$, cases. This way, we show the benefit of the power minimizer precoder in the strong transmitter case and the signal level minimizer precoder in the strong eavesdropper case. We use the acronym "min" instead of minimization in the legend of the figures. We consider the ZF at the transmitter [23] as the benchmark scheme since both our design and the benchmark scheme use CSI knowledge at the transmitter to design the precoder.

In the benchmark scheme, ZF precoder is applied at the transmitter to remove the interference among the symbol streams. The received signals at users and E in the benchmark scheme are

$$\mathbf{y}_U = \mathbf{H}_U\mathbf{W}\mathbf{s}\beta + \mathbf{n}_\mathbf{U}, \tag{6.37}$$

$$\mathbf{y}_E = \mathbf{H}_E\mathbf{W}\mathbf{s}\beta + \mathbf{n}_\mathbf{E}, \tag{6.38}$$

where $\mathbf{W} = \mathbf{H}_U^H\left(\mathbf{H}_U\mathbf{H}_U^H\right)^{-1}$ is the precoding vector, $\mathbf{s}$ contains the symbols, and β is the amplification factor for the symbols which acts similar as $\sqrt{\gamma}$ in the directional modulation scheme. For a fair comparison, we pick up the same values for $\sqrt{\gamma}$ and β in the simulations.

When using the benchmark, E has two ways to estimate the symbols. In the first way, given that $N_e \geq N_t$, E can follow a similar approach as in Section 6.3 to estimate $\mathbf{W}$ as follows

$$\begin{aligned}\widehat{\mathbf{W}} &= \left[\mathbf{H}_E^H\mathbf{H}_E\right]^{-1}\mathbf{H}_E^H\mathbf{y}_E \\ &= \mathbf{W} + \left[\mathbf{H}_E^H\mathbf{H}_E\right]^{-1}\mathbf{H}_E^H\mathbf{n}_E,\end{aligned} \tag{6.39}$$

then, it can estimate the symbols by calculating $\mathbf{H}_U\widehat{\mathbf{W}}$. In the second way, E can use the knowledge of $\mathbf{H}_U$ to calculate $\mathbf{W}$ and directly estimate $\mathbf{s}\beta$ as

$$\begin{aligned}\widehat{\mathbf{s}\beta} &= \left[(\mathbf{H}_E\mathbf{W})^H\mathbf{H}_E\mathbf{W}\right]^{-1}(\mathbf{H}_E\mathbf{W})^H\mathbf{y}_E \\ &= \mathbf{s}\beta + \left[(\mathbf{H}_E\mathbf{W})^H\mathbf{H}_E\mathbf{W}\right]^{-1}(\mathbf{H}_E\mathbf{W})^H\mathbf{n}_E\end{aligned} \tag{6.40}$$

where $\widehat{\mathbf{s}\beta}$ is the estimated $\mathbf{s}\beta$ at E. Since $\mathbf{H}_E\mathbf{W}$ is $N_e \times N_U$, $\left[(\mathbf{H}_E\mathbf{W})^H\mathbf{H}_E\mathbf{W}\right]^{-1}(\mathbf{H}_E\mathbf{W})^H\mathbf{H}_E\mathbf{W} = \mathbf{I}$ for $N_e \geq N_U$. Hence, in the benchmark scheme, E can derive the precoder and estimate the symbols when $N_e \geq N_U$. On the other hand, since our designed precoder depends on both the channels and symbols, E cannot derive the precoder and estimate the symbols when $N_e \geq N_U$. Broadly speaking, the base station has usually more antennas than the users, hence, satisfying the condition $N_e < N_t$ is more likely than $N_e < N_U$, specially with a large scale array. Therefore, it is more probable to preserve the security in our design compared to the benchmark scheme. Furthermore, by comparing (6.4) and (6.40), we see that E has to multiply $\widehat{\mathbf{W}}$ by $\mathbf{H}_U$ in our design whereas E does need to do this in the benchmark scheme.

In the first scenario, the effect of number of transmitter antennas, N_t, on transmitter's consumed power and the SER at users and E is investigated for power and signal level minimization precoders in (6.6) and (6.28), and the benchmark scheme. The average consumed power, $\|\mathbf{w}\|^2$, with respect to N_t is shown in Fig. 6.4 for $N_U = 8, 10$. As N_t increases, the power consumption of our design with power minimization precoder converges to that of other two schemes. The power consumed by power minimization precoder has the largest difference with other two schemes, almost 6 dB, for $N_t = N_U$. The signal level minimization precoder has almost the same power consumption as the benchmark scheme. When the difference between N_t and N_U increases, all three schemes consume considerably less power.

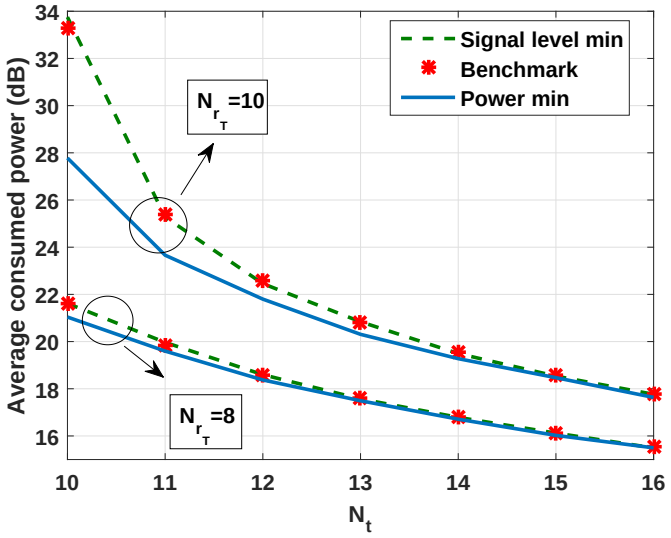


FIGURE 6.4: Average consumed power with respect to N_t for our designed precoders and the benchmark scheme when $\gamma = 15.56$ dB and $\beta^2 = 15.56$ dB.

The average total SER at users and the average SER at E with respect to N_t are presented in Fig. 6.5. Our designed precoders, power and signal level minimization, cause considerably more SER at E compared to the benchmark scheme for a long range of N_t. Furthermore, as N_e increases, there are cases, e.g., $N_t = 16$, that the error caused at E by the benchmark scheme decreases while the error caused by our designed precoders remains almost fixed. As Fig. 6.6 shows, our design with signal level minimization precoder and the benchmark scheme keep users' SER constant since they preserve a constant SNR for the received signals on receiver antennas. As mentioned earlier, when the SNR of the received signal is fixed, E may not successfully decode the symbols since it suffers from enhanced noise and in contrast to the users, its SNR is probably lower than the required level. Since the directional modulation with signal level minimization imposes more error on E and consumes the same power as the benchmark scheme, it is the preferable choice for secure communication when $N_e \geq N_t$. Comparing Figures. 6.4 and 6.5 shows when the difference between N_t and N_U goes above a specific amount, the power and signal level minimization precoders converge in both power consumption and the SER at E and users.

The instantaneous power of the induced symbols to average noise power in shown in Fig. 6.7 for power and signal level minimizer precoders when $N_e \geq N_t$. As we see, even with E being able to estimate the symbols, the SNR at E is lower than the users since E has to perform extra process to estimate the symbols which increases the noise. On the other hand, when using the power minimizer precoder, the SNR at E may go over the threshold value while for the signal level minimizer precoder, the SNR at E is always

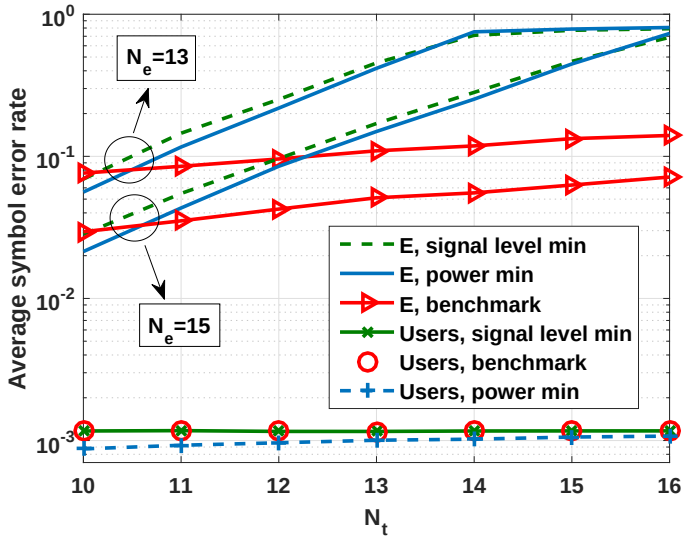


FIGURE 6.5: Average total SER at the users and average SER at E with respect to N_t for our designed precoders and the benchmark scheme when $N_U = 10$, $\gamma = 15.56$ dB, and $\beta^2 = 15.56$ dB.

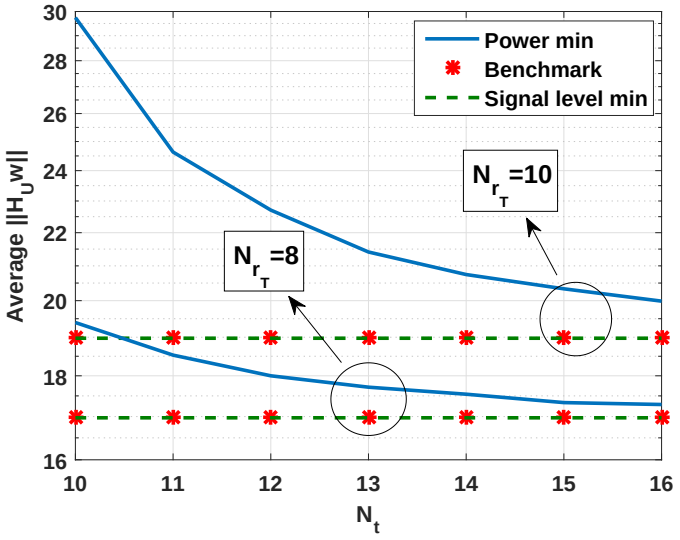


FIGURE 6.6: Average $\|\mathbf{H}_U\mathbf{w}\|$ for our designed precoders and the benchmark scheme when $\gamma = 15.56$ dB, and $\beta^2 = 15.56$ dB.

kept at a fixed level below the required threshold, which imposes the maximum SER at E.

In the second scenario, T's power consumption, total SER at the users, and SER at E are plotted with respect to total receiving antennas, N_U. Fig. 6.8 shows the average consumed power with respect to N_U. In contrast to Fig. 6.4, increasing N_U decreases the degrees of freedom and increases the power consumption. As N_U approaches N_t, the difference between the power consumed by the power minimization precoder and the other two schemes increases.

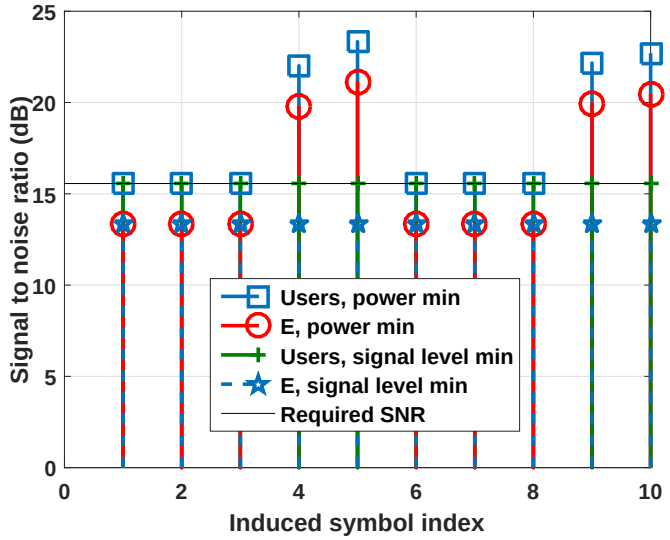


FIGURE 6.7: Instantaneous symbol power to average noise power for power and signal level minimization precoders when $N_t = 10$, $N_{r_t} = 10$, $N_e = 16$ and $\gamma = 15.56$ dB.

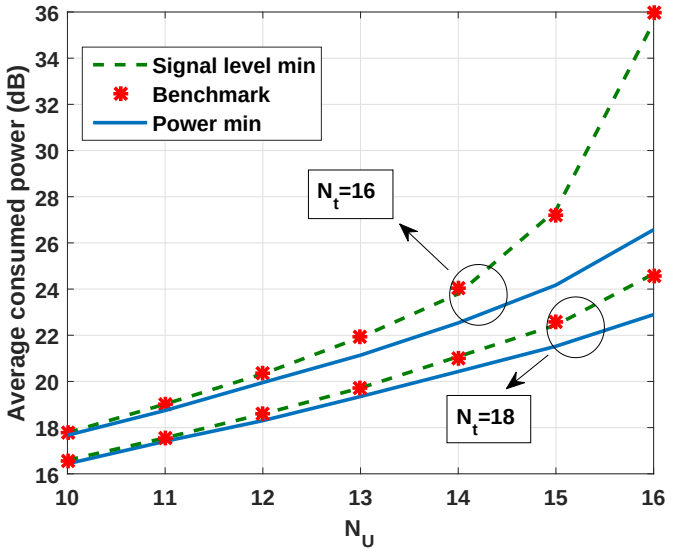


FIGURE 6.8: Average consumed power with respect to N_U for our designed precoders and the benchmark scheme when $\gamma = 15.56$ dB, and $\beta^2 = 15.56$ dB.

We investigate the effect of N_U on average total SER at the users and the average SER at E for all the schemes in Fig. 6.9. As N_U increases, the SNR provided by the power minimization precoder goes more above the threshold. This reduces the average SER at both users and E. On the other hand, regardless of difference between N_t and N_U, our design with signal level minimization precoder always preserves the SER at E in the maximum value. When $N_t > N_{r_K}$, our design imposes more SER at E compared to the benchmark scheme since $N_e \geq N_U$ is required for E to estimate the symbols in the benchmark scheme. As N_U approaches N_t, the SER imposed on E by the signal level minimization precoder and the benchmark scheme get closer.

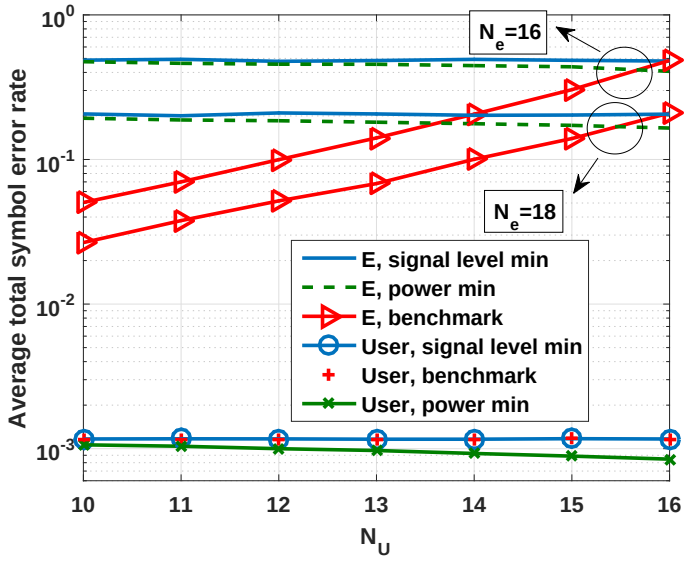


FIGURE 6.9: Average SER versus N_U for our designed precoders and the benchmark scheme when $N_t = 16$, $\gamma = 15.56$ dB, and $\beta^2 = 15.56$ dB.

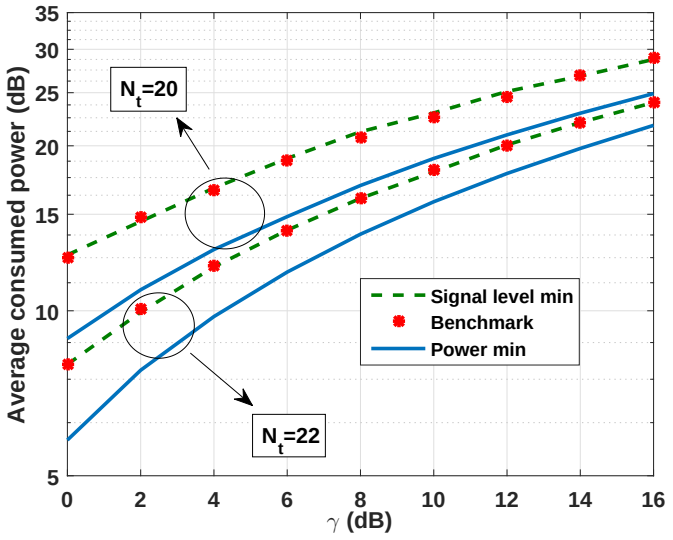


FIGURE 6.10: Average consumed power with respect to required SNR for our designed precoders and the benchmark scheme when $N_U = 19$.

The next scenario inspects the effect of the required SNR for the received signals, γ, on T's consumed power and the SER at users and E. The difference between the power consumed by the power minimizer precoder and the other two schemes in low SNRs is more than that of high SNRs. The average total SER at users and the average SER at E with respect to γ is shown in Fig. 6.11. As SNR increases, the difference between the SER imposed on E by our design and the benchmark scheme increases, where the difference is the most for $N_e = 20$. The difference between the average total SER at the users for power and signal level minimization precoders remains almost constant as γ increases. The effect of low-density parity-check (LDPC) codes on the average total

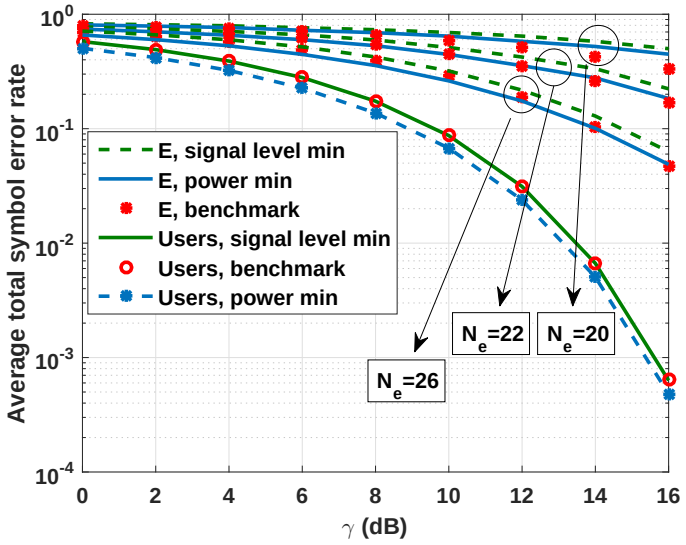


FIGURE 6.11: Average SER versus required SNR for our designed precoders and the benchmark scheme when $N_t = 20$ and $N_U = 19$.

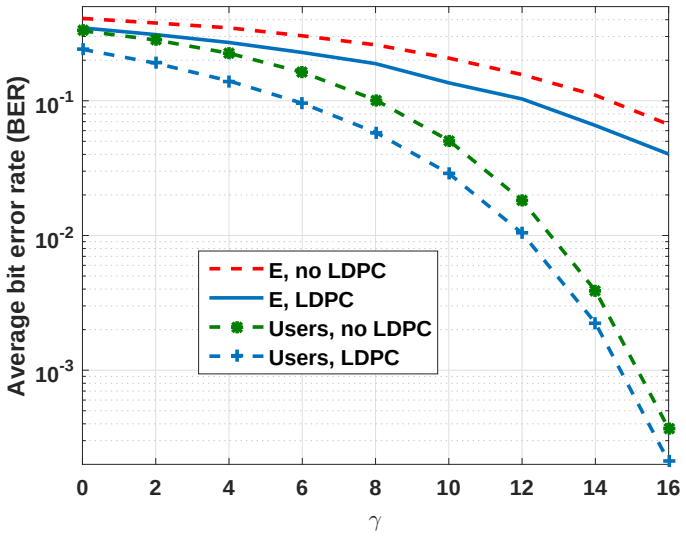


FIGURE 6.12: Average BER versus required SNR for our designed precoders and the benchmark scheme when $N_t = 6$, $N_U = 6$, and $N_e = 7$.

bit error rate (BER) at the users and the average BER at E is shown in Fig. 6.12. For a long range of SNRs, the usage of the LDPC at the users decreases the BER more than that of E.

In the last scenario, we investigate the computational time of the proposed solutions for the optimal directional modulation precoder design. Fig. 6.13 shows the average consumed time with respect to system dimensions when designing the optimal precoders using CVX package, iterative algorithm, and the non-negative least squares formulation of Section 6.4.1.2. Both iterative algorithm and non-negative least squares consume

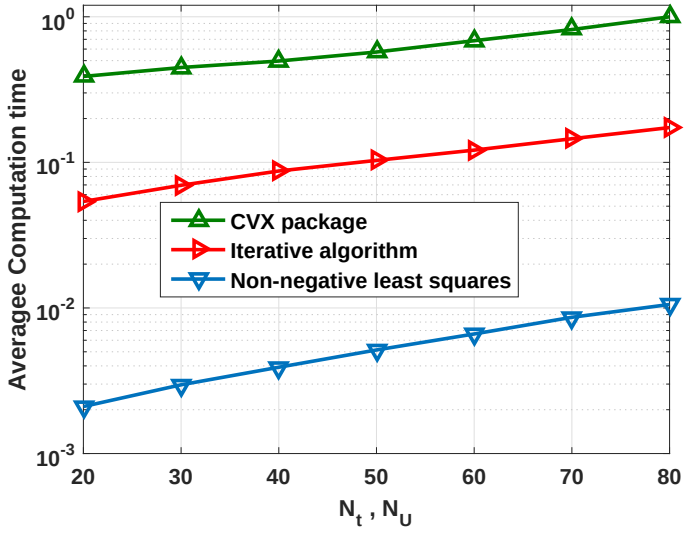


FIGURE 6.13: Average consumed time with respect to number of transmit and receive antennas to design the power minimization precoder using CVX package, iterative algorithm, and non-negative least squares formulation when $\gamma = 15.56$ dB and $\epsilon = 10^{-3}$.

considerably less time than CVX. Also, the average computation time of iterative algorithm and non-negative least squares problem get closer as we move toward larger system dimension.

6.6 Conclusions

We considered enhancing the security in a multi-user MIMO wireless network where a multiple-antenna eavesdropper can potentially intercept the wireless transmission. We used the directional modulation technique to follow a signal processing paradigm in order to improve the security. The security is enhanced by increasing the SER at the eavesdropper without using the eavesdropper's CSI for M-PSK modulation, which is a practical physical layer security scenario. In the directional modulation, the phase of the received signal at the destination depends on both the channel and symbols; hence, the receiver gets the phase of the intended M-PSK symbols while the eavesdropper gets different phases. Our analysis showed that when the eavesdropper has less antennas than the transmitter, the eavesdropper cannot get useful information from the received signal. On the other hand, when the eavesdropper has more antennas than the transmitter, it has to remove the effect of its own channel to estimate the precoding vector and then multiply the estimated precoder by the users' channel. This way, the eavesdropper can estimate the received signal by the users; however, these operations enhance the noise at the eavesdropper. This puts the users in a superior position compared to the eavesdropper since the users can directly detect the symbols without requiring extra

processes as in the eavesdropper. We proposed the power minimization for the case that the eavesdropper has less antennas than the transmitter and the SNR minimization precoder for the case than the eavesdropper has more antennas than the transmitter. More specifically, the SNR minimization precoder keeps the SNR at the eavesdropper below the required level for successful decoding. We developed an iterative algorithm and non-negative least squares formulation as fast ways to calculate the precoders. Further analysis on the security of the conventional precodes revealed that the eavesdropper can estimate the users' signals in this type of precoding when it has more antennas than the users. On the other hand, the eavesdropper has to have more antennas than the transmitter to estimate the symbols in the directional modulation precoding. Generally, the transmitter has more antennas than the users; as a result, it is more likely to enhance the security using the directional modulation precoding. This benefit comes from that fact that the precoder in the directional modulation depends on both the symbols and the channels, consequently, the eavesdropper cannot calculated it. On the other hand, the conventional precoder depends only on the channel CSI and can be calculated by the eavesdropper.

The simulation results showed when the eavesdropper has less antennas than the transmitter, the SNR minimization precoder causes more SER at the eavesdropper at the expense of more power consumption. As the difference between the antennas of the transmitter and users increases, the power and SNR minimization precoders consume almost the same power. Furthermore, the simulations verified that the SNR minimization precoder keeps the SNR level at the eavesdropper below the required threshold for successful decoding. The results showed that compared to the conventional precoder, the directional modulation precoders cause more SER at the eavesdropper and consume less power in most of the cases. This is due to the fact that our precoders depend on both the CSI knowledge and the symbols while the conventional precoder only depends on the CSI knowledge and the eavesdropper can calculate it.

Chapter 7

Conclusions and Future Work

7.1 Conclusion Summary

Physical layer security has shown to be a promising technique to strengthen the security of wireless networks and can complement the higher level network security approaches such as cryptography. The concept of keyless information-theoretic physical layer security proposed by Wyner [5] has undergone an enormous amount of research and has been extended to different types of direct link and cooperative wireless communication networks. In addition, the researchers have employed signal processing approaches to enhance the security. We reviewed the literature of both information-theoretic and signal processing paradigms in Chapter 2. This thesis has focused on both information-theoretic and signal processing approaches to improve the security of wireless communication networks.

We considered maximizing the sum secrecy rate in a satellite communications network in Chapter 3. The studied SATCOM network employs network coding to initiate the bidirectional data exchange. Network coding principle has been known to increase the throughput of bidirectional SATCOM. We studied the use of XOR network coding to improve the sum secrecy rate of bidirectional SATCOM. We showed through the analysis that if the RL has positive secrecy rate, the XOR network coding can help having a perfectly secure FL transmission for the corresponding message. The beamforming vector as well as the optimal time allocation between the RL and the FL were optimized to improve the secrecy rate in the considered SATCOM network. We compared the sum secrecy rate of the XOR network coding with the conventional scheme, which operates without network coding, using realistic system parameters. Our results demonstrated that the network coding based scheme outperforms the conventional scheme substantially, especially when the legitimate users and the eavesdroppers are not close.

Another focus of this thesis was studying the secrecy rate in wiretap interference channels in Chapter 4 and investing the effect of interference on the secrecy rate. In this direction, we studied the effect of interference on improving the secrecy rate in a two-user wireless interference network where signals had a Gaussian distribution. We developed channel dependent expressions for both altruistic and egoistic scenarios to define the proper range of transmission power for the interfering user, namely user 2, in order to sustain a positive secrecy rate for the other user, namely user 1. Closed-form solutions were obtained in order to perform joint optimal power control for both users in the altruistic and egoistic scenarios. It was shown that by decreasing the required QoS at user 2's destination, the secrecy rate in the interference channel improves and approaches to the single-user case. Moreover, to fairly compare our scheme with the benchmark, the ratio of the secrecy rate over the optimal consumed power by user 1 was introduced as a new metric called "secrecy energy efficiency", in order to take into account both the secrecy rate and the consumed power. It was shown that in comparison with the single-user case, the secrecy energy efficiency is considerably higher in the interference channel for a wide range of QoS at user 2's destination.

Since the energy efficiency is an important issue in wireless networks and is vital for battery operated devices, we performed a joint study on secrecy rate and energy efficiency in Chapter 5. In this chapter, we studied the secrecy energy efficiency and its trade-off with the secrecy spectral efficiency in MISO and SISO wiretap channels. An optimal beamformer was designed to maximize secrecy energy efficiency for the cases with and without considering the minimum required secrecy spectral efficiency at the receiver in a power limited system. We saw that as the minimum required secrecy spectral efficiency increases, the performance of the optimal beamformer and the ZF beamformer, the benchmark scheme, designs gets closer. Furthermore, as the number of antennas decreases, the performance gap between the optimal and the ZF design increases. It was observed that there is a specific amount of secrecy spectral efficiency below which increasing secrecy spectral efficiency leads to higher secrecy energy efficiency, and above which the opposite trend occurs. Depending on the power value corresponding to the optimal secrecy energy efficiency, increasing secrecy spectral efficiency can increase or decrease the secrecy energy efficiency. In addition, it was shown that adding more antennas to the transmitter side increases secrecy energy efficiency considerably and sustains the optimal secrecy energy efficiency for a longer range of minimum required secrecy spectral efficiency.

Implementing the information-theoretic secrecy rate in real work communication networks has several challenges. One major drawback is that in order to design the system parameters such as the optimal power or optimal beamformer, the perfect or partial CSI of the eavesdropper is required. However, it may be impossible to get the CSI of

an eavesdropper in practice, especially, when the eavesdropper is passive. In addition, implementing the secrecy rate requires transmitting lower than the achievable rate and the data need to follow a Gaussian distribution. To handle these challenges, we focused on using the signal processing paradigm to enhance the security in the second part of this thesis. In Chapter 6, we used the directional modulation technology and followed a signal processing approach to enhance the security over multiuser MIMO channels in the presence of a multi-antenna eavesdropper. When using directional modulation, we showed that the eavesdropper cannot estimate the symbols if it has fewer antennas than the transmitter. On the other hand, when it has more antennas than the transmitter, additional processing is required before estimating the symbols which enhances the noise, whereas the users can directly apply conventional detectors. In addition, we derived the necessary condition for the feasibility of the optimal precoder for the directional modulation. We proposed an iterative algorithm and non-negative least squares formulation to reduce the design time of the optimal precoders. The results showed that in most of the cases our designed directional modulation precoders impose a considerable amount of symbol errors on the eavesdropper compared to the conventional precoding. This is due to the fact that our precoders depend on both the CSI knowledge and the symbols while the conventional precoder only depends on the CSI knowledge and the eavesdropper can calculate it. The simulations showed that regardless of the number of antennas, the signal level minimization precoder keeps the SER at the eavesdropper on the maximum value, and it consumes the same power as the power minimization precoder when the difference between the number of transmit and receive antennas is above a specific value. Simulations showed that LDPC coding for the signal level minimization precoder improves the BER more at the users than the eavesdropper for a long range of SNRs. In addition, the numerical examples showed that both the power and signal level minimization precoders outperform the benchmark scheme in terms of the power consumption and/or the imposed error at the eavesdropper.

7.2 Future Work

In the directional of the information-theoretic secrecy rate, the contribution of Chapter 3 can be extended to the case where users and/or the eavesdroppers have multiple antennas. Furthermore, friendly external jammers can be considered to improve the secrecy rate when the satellite broadcasts the XORed content.

The research direction in enhancing the wireless security using signal processing paradigm seems to be a promising direction. In particular, the eavesdropper CSI is not required in this scheme. Furthermore, in contrast to the information-theoretic secrecy rate, the

signal processing paradigm improves the security without reducing the achievable rate and the data do not have to follow a Gaussian distribution. As an improvement, the artificial noise can be incorporated into the directional modulation scheme to improve the security when the transmitter has fewer number of antennas than the eavesdropper.

Appendix A

Proof of Theorem 3.3

Proof. In the objective function of problem (3.40), only the second argument of the "min" operators, FL secrecy rates, include the beamforming vector. Hence, we focus on these terms in our optimization. Using contradiction, we shall show that $\|\mathbf{w}_1^\star\|^2 = \beta P_S$ and $\|\mathbf{w}_2^\star\|^2 = (1-\beta) P_S$ must hold for the optimal solutions $\mathbf{w}_1^\star$ and $\mathbf{w}_2^\star$. Assume that $\mathbf{w}_1^\star$ and $\mathbf{w}_2^\star$ are the optimal solutions to (3.40) and satisfy $\|\mathbf{w}_1\|^2 < \beta P_S$ and $\|\mathbf{w}_2\|^2 < (1-\beta) P_S$, then there exist constants $\alpha_1 > 1$ and $\alpha_2 > 1$ that satisfy $\|\widehat{\mathbf{w}}_1^\star\|^2 = \beta P_S$ and $\|\widehat{\mathbf{w}}_2^\star\|^2 = (1-\beta) P_S$ where $\widehat{\mathbf{w}}_1^\star = \alpha_1 \mathbf{w}_1^\star$ and $\widehat{\mathbf{w}}_2^\star = \alpha_2 \mathbf{w}_2^\star$. Replacing $\mathbf{w}_1^\star$ by $\widehat{\mathbf{w}}_1^\star$ and $\mathbf{w}_2^\star$ by $\widehat{\mathbf{w}}_2^\star$ in the FL secrecy rates of the objective in (3.40), we get

$$
\begin{aligned}
f_1(\alpha_1) &= t_2 \log \left(\frac{\sigma_{E_2}^2}{\sigma_{U_2}^2} \frac{\sigma_{U_2}^2 + \alpha_1^2 |\mathbf{h}_{S,U_2}^T \mathbf{w}_1^\star|^2}{\sigma_{E_2}^2 + \alpha_1^2 |\mathbf{h}_{S,E_2}^T \mathbf{w}_1^\star|^2} \right), \\
f_2(\alpha_2) &= t_3 \log \left(\frac{\sigma_{E_1}^2}{\sigma_{U_1}^2} \frac{\sigma_{U_1}^2 + \alpha_2^2 |\mathbf{h}_{S,U_1}^T \mathbf{w}_2^\star|^2}{\sigma_{E_1}^2 + \alpha_2^2 |\mathbf{h}_{S,E_1}^T \mathbf{w}_2^\star|^2} \right).
\end{aligned} \tag{A.1}
$$

Also, we assume that in the RL and FL of each user the secrecy rate is nonzero which translates into

$$
\sigma_{E_2}^2 \left(\sigma_{U_2}^2 + |\mathbf{h}_{S,U_2}^T \mathbf{w}_1|^2 \right) > \sigma_{U_2}^2 \left(\sigma_{E_2}^2 + |\mathbf{h}_{S,E_2}^T \mathbf{w}_1|^2 \right), \exists \mathbf{w}_1, \tag{A.2}
$$

$$
\sigma_{E_1}^2 \left(\sigma_{U_1}^2 + |\mathbf{h}_{S,U_1}^T \mathbf{w}_2|^2 \right) > \sigma_{U_1}^2 \left(\sigma_{E_1}^2 + |\mathbf{h}_{S,E_1}^T \mathbf{w}_2|^2 \right), \exists \mathbf{w}_2. \tag{A.3}
$$

According to the conditions in (A.2) and (A.3), we can see that $f_1(\alpha)$ and $f_2(\alpha)$ are monotonically increasing functions in the parameters α_1 and α_2. This contradicts that $\mathbf{w}_1^\star$ and $\mathbf{w}_2^\star$ are the optimal solutions. Since adjusting the RL and FLs transmission time balances the RL and FL secrecy rates, the RL bottleneck does not limit the FL secrecy rate increment. Hence, the power constraint should be active. This completes the proof. □

Appendix B

Proof of Theorem 4.1

For the objective function in (4.12) to be positive, the following condition must hold

$$\begin{aligned}
&\log_2\left(1+\frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}\right)\\
&-\log_2\left(1+\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}\right)>0\\
&\Rightarrow \frac{P_1|h_{U_1,D_1}|^2}{P_2|h_{U_2,D_1}|^2+\sigma_n^2}>\frac{P_1|h_{U_1,E}|^2}{P_2|h_{U_2,E}|^2+\sigma_n^2}\\
&\Rightarrow \begin{cases} P_2>\frac{\sigma_n^2\left(|h_{U_1,E}|^2-|h_{U_1,D_1}|^2\right)}{B} & B>0\\ P_2<\frac{\sigma_n^2\left(|h_{U_1,E}|^2-|h_{U_1,D_1}|^2\right)}{B} & B<0 \end{cases}
\end{aligned} \tag{B.1}$$

where $B=|h_{U_1,D_1}|^2|h_{U_2,E}|^2-|h_{U_2,D_1}|^2|h_{U_1,E}|^2$.

Appendix C

Proof of Theorem 4.4

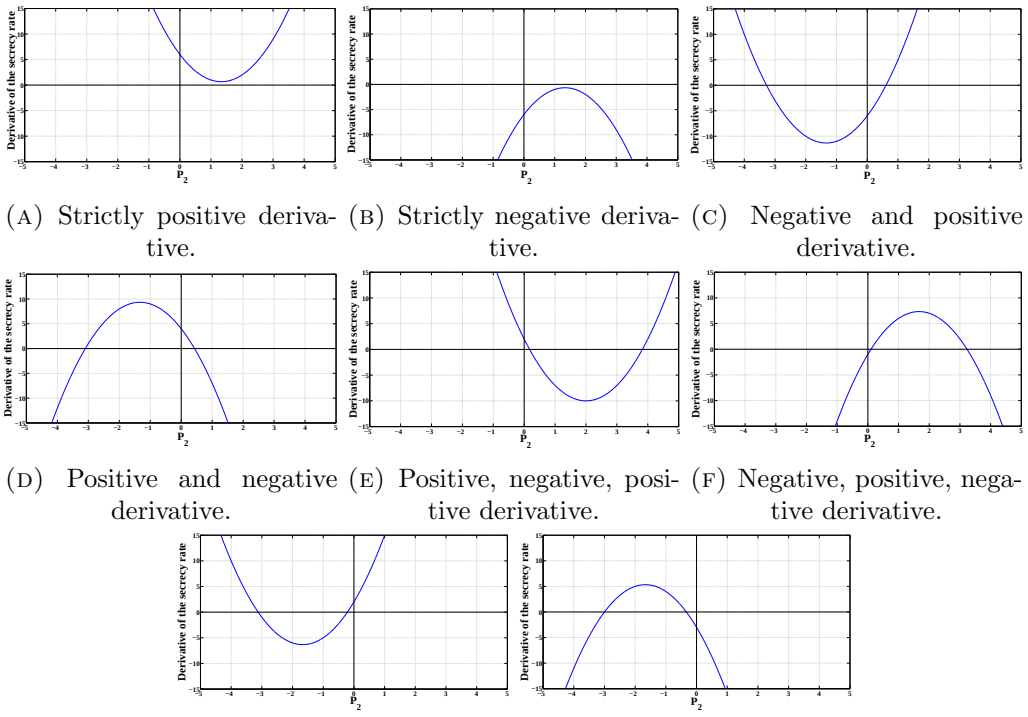
In order to find the optimal P_2 for (4.19), we analyze the derivative of the objective function in (4.19). The derivative is defined at the top of next page in (C.61) where $a = P_{\max_1}|h_{U_1,D_1}|^2$, $b = |h_{U_2,D_1}|^2$, $c = P_{\max_1}|h_{U_1,E}|^2$, and $d = |h_{U_2,E}|^2$. According to the sign of the derivative, the optimal P_2 can be found. The denumerator in (C.61) is already positive, so the sign of (C.61) directly depends on the sign of the numerator. The numerator is a quadratic equation. According to the sign of the discriminant of the quadratic equation [243, Section 5.1], denoted by $\Delta = 4abcd\sigma_n^2\left(b-d\right)\left[-d\left(a+\sigma_n^2\right)+b\left(c+\sigma_n^2\right)\right]$, the status of the roots can be defined. The sign of the discriminant can be defined as

1. If $\left(b-d\right)\left[-d\left(a+\sigma_n^2\right)+b\left(c+\sigma_n^2\right)\right] < 0$, $\Delta < 0$.
2. If $\left(b-d\right)\left[-d\left(a+\sigma_n^2\right)+b\left(c+\sigma_n^2\right)\right] > 0$, $\Delta > 0$.

Using the sign of Δ as well as the sign of the P_2's coefficients in the quadratic equation which we denote them from highest order to constant as a', b' and c' in (C.61), the sign of the derivative can be defined and consequently the optimal value for P_2, $P_2^\star$, can be found as follows:

1. If $\Delta < 0$, no root exists for the numerator in (C.61) leading to the following cases:

$$\frac{\partial OF}{\partial P_2} = \frac{bd\left(bc-ad\right)P_2^2 + 2b\left(-a+c\right)d\sigma_n^2 P_2 + \sigma_n^2\left(cd\sigma_n^2 - a\left(-cd+b\left(c+\sigma_n^2\right)\right)\right)}{\left(\sigma_n^2+bP_2\right)^2\left(c+\sigma_n^2+dP_2\right)^2} \tag{C.61}$$



(A) Strictly positive derivative. (B) Strictly negative derivative. (C) Negative and positive derivative.

(D) Positive and negative derivative. (E) Positive, negative, positive derivative. (F) Negative, positive, negative derivative.

(G) Negative, positive, negative derivative. (H) Negative, positive, negative derivative.

FIGURE C.1: Different cases for the sign of the derivative in (C.61).

(a) $a' > 0$, then the derivative is strictly positive, as shown in Fig. C.1a, and is monotonically increasing, so the highest value in the feasible set is the $P_2^\star$.

(b) $a' < 0$, then the derivative is strictly negative, as shown in Fig. C.1b, and is monotonically decreasing, so the lowest possible value in the feasible set is the $P_2^\star$.

2. If $\Delta > 0$, there exist two roots (two critical points for the objective function in (4.19)) for the derivative leading to the following cases:

   (a) Only one of the roots is positive. This happens when the product of the roots [243, Section 5.1], $\frac{c'}{a'}$, is negative in the following cases:

      i. $a' > 0$ and $c' < 0$, as shown in Fig. C.1c. In this case, the critical point is a minimum, so one of the vertices of the feasible domain is the $P_2^\star$.

      ii. $a' < 0$ and $c' > 0$, as shown in Fig. C.1d. For this case, the critical point is a maximum and if falls into the feasibility domain of P_2, it is the $P_2^\star$. Otherwise, one of the vertices of the feasible domain is the $P_2^\star$.

   (b) Both of the roots are positive. This happens when both the product, $\frac{c'}{a'}$, and the sum [243, Section 5.1], $-\frac{b'}{a'}$, of the roots are positive in two following conditions:

i. $a' > 0$, $c' > 0$ and $b' < 0$, as shown in Fig. C.1e. For the first case, the derivative is first positive, then negative and then positive, respectively, meaning that the first root results in a maximum and the second root results in a minimum. If the smaller root falls in the feasibility domain of P_2, then by comparing it with the vertices of the feasibility domain, $P_2^\star$ is found. If the smaller root is not in the feasibility domain of P_2, the optimal value of P_2 is at one of the vertices of the feasibility domain.

ii. $a' < 0$, $c' < 0$ and $b' > 0$, as shown in Fig. C.1f. In this case, we find out that the larger root is a maximum. If the larger root falls in the feasibility domain of P_2, then by comparing it to the vertices of the feasibility domain of P_2, we can find the $P_2^\star$. If the larger root is not in the feasibility domain of P_2, we should find the optimal value of P_2 in the vertices of the feasibility domain.

(c) Both of the roots are negative. This happens when the product of the roots, $\frac{c'}{a'}$, is positive and the sum of the roots, $-\frac{b'}{a'}$, is negative in two following conditions:

i. $a' > 0$, $c' > 0$ and $b' > 0$, as shown in Fig. C.1g. Since the transmission power is always positive, the critical points cannot be the answer to $P_2^\star$. For the first case, the derivative is first positive, then negative and then positive, respectively. As a result, the secrecy rate will be increasing after $P_2 > 0$. So, $P_2^\star$ is the maximum possible value of P_2 inside the feasibility set.

ii. $a' < 0$, $c' < 0$ and $b' < 0$, as shown in Fig. C.1h. As in Case 2(c)i, the critical points cannot be the answer to $P_2^\star$. For the first case, the derivative is first negative, then positive and then negative, respectively. So, the secrecy rate is decreasing after $P_2 > 0$. Hence, $P_2^\star$ is the minimum possible value of P_2 inside the feasibility set.

In deriving the above closed-form optimal solutions, we have considered all the possible cases of discriminant sign, Δ, and the coefficients of the quadratic equation, a', b', and c'. In each case, we have calculated all the critical points and if applicable, these critical points are compared with the vertices of the domain to make sure that the derived power value is globally optimum. Hence, the optimal solutions presented in Appendix **??** are global optimum.

Bibliography

[1] A. Roy-Chowdhury, J. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Commun. Mag.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.

[2] H. Cruickshank, M. Howarth, S. Iyengar, Z. Sun, and L. Claverotte, "Securing multicast in DVB-RCS satellite systems," *IEEE Wireless Commun. Mag.*, vol. 12, no. 5, pp. 38–45, Oct. 2005.

[3] N. Sklavos and X. Zhang, Wireless Security and Cryptography: Specifications and Implementations. Taylor & Francis, 2007.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technical Journal*, vol. 28, pp. 656–715, July 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[6] Physical layer wireless security. Seventh framework programme (FP7). [Online]. Available: http://www.phylaws-ict.org

[7] M. Bloch and J. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[8] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1765–1779, Nov. 2014.

[9] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[11] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[12] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, Mar. 2007, pp. 905–910.

[13] F. Oggier and B. Hassibi, "The MIMO wiretap channel," in *Int. Symp. on Commun., Control and Signal Proces. (ISCCSP)*, St. Julians, Malta, Mar. 2008, pp. 213–218.

[14] B. Evans, M. Werner, E. Lutz, M. Bousquet, G. Corazza, and G. Maral, "Integration of satellite and terrestrial systems in future multimedia communications," *IEEE Wireless Commun.*, vol. 12, no. 5, pp. 72–80, Oct. 2005.

[15] M. A. Olson, M. M. Bykowsky, and W. W. Sharkey, "Modeling the efficiency of spectrum designated to licensed service and unlicensed operations," *FCC OSP Working Paper Series*, Feb. 2008.

[16] C. Chiasserini and R. Rao, "Coexistence mechanisms for interference mitigation in the 2.4-GHz ISM band," *IEEE Trans. Wireless Commun.*, vol. 2, no. 5, pp. 964–975, Sep. 2003.

[17] A. Babakhani, D. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.

[18] M. Daly and J. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[19] M. Salehi and J. Proakis, *Digital Communications*, ser. McGraw-Hill higher education. McGraw-Hill Education, 2007.

[20] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[21] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810–3823, Jul. 2015.

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

[23] L.-U. Choi and R. Murch, "A transmit preprocessing technique for multiuser MIMO systems using a decomposition approach," *IEEE Trans. Wireless Commun.*, vol. 3, no. 1, pp. 20–24, Jan. 2004.

[24] Q. Spencer, A. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, Feb. 2004.

[25] A. Kalantari, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secrecy energy efficiency optimization for MISO and SISO communication networks," in *IEEE Int. Workshop on Signal Proces. Advances in Wireless Commun. (SPAWC)*, Jun. 2015, pp. 21–25.

[26] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[27] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secure M-PSK communication via directional modulation," in *IEEE Int. Conf. on Acoustics, Speech and Signal Proces. (ICASSP)*. Shanghai, China: to appear, Mar. 2016.

[28] ——, "Security enhancing directional modulation via symbol-level precoding," *IEEE Journal of Selected Topics in Signal Processing*, (submitted).

[29] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEECommun. Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[30] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[31] C. Mitrpant, A. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[32] L. Kong, H. Tran, and G. Kaddoum, "Performance analysis of physical layer security over α-μ fading channel," *Electronics Letters*, vol. 52, no. 1, pp. 45–47, Jan. 2016.

[33] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 5:1–5:12, Mar. 2009. [Online]. Available: http://dx.doi.org/10.1155/2009/142374

[34] S. Maleki, A. Kalantari, S. Chatzinotas, and B. Ottersten, "Power allocation for energy-constrained cognitive radios in the presence of an eavesdropper," in *IEEE Int. Conf. on Acoustics, Speech and Signal Proces. (ICASSP)*, Florence, Italy, May 2014, pp. 5695–5699.

[35] A. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[36] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Sep. 2005, pp. 2152–2155.

[37] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Jun. 2007, pp. 2466–2470.

[38] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[39] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[40] ——, "Secure transmission with multiple antennas–part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[41] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[42] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[43] H. Lei, C. Gao, I. Ansari, Y. Guo, G. Pan, and K. Qaraqe, "On physical layer security over SIMO generalized-k fading channels," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2015.

[44] F. Wu, R. Zhang, L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[45] S. Rezaei Aghdam and T. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2016.

[46] K. Peppas, N. Sagias, and A. Maras, "Physical layer security for multiple-antenna systems: A unified approach," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 314–328, Jan. 2016.

[47] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141–144, Feb. 2013.

[48] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.

[49] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[50] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816–3825, Dec. 2012.

[51] A. Chorti, "Helping interferer physical layer security strategies for M-QAM and M-PSK systems," in *Annual Conf. on Inf. Sciences and Syst. (CISS)*, Princeton, NJ, Mar. 2012.

[52] H. Alves, R. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[53] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and I. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[54] Y. Huang, F. Al-Qahtani, T. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[55] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, Jan. 2016.

[56] S. Fakoorian and A. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[57] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[58] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

[59] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[60] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[61] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

[62] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *Wireless Communications, IEEE Transactions on*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[63] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, April 2012.

[64] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[65] H. Reboredo, J. Xavier, and M. Rodrigues, "Filter design with secrecy constraints: The MIMO Gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[66] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage constrained robust secure transmission for MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558–5570, Oct. 2014.

[67] H.-M. Wang, C. Wang, and D. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[68] T. Zheng, H. Wang, J. Yuan, D. Towsley, and M. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[69] H. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov 2010.

[70] Y. Liang and H. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[71] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Toronto, Canada, Jul. 2008, pp. 379–383.

[72] J. Xie and S. Ulukus, "Secrecy games on the one-sided interference channel," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, St. Petersburg, Russia, Jul. 2011, pp. 1245–1249.

[73] R. Liu, I. Maric, P. Spasojević, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[74] R. Liu and H. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.

[75] R. Liu, T. Liu, H. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Jun. 2010, pp. 2578–2582.

[76] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 885–887, Oct. 2010.

[77] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *Annual Conf. on Inf. Sciences and Syst. (CISS)*, Baltimore, MD, Mar. 2009, pp. 318–323.

[78] S. Fakoorian and A. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans.Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sept. 2011.

[79] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[80] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[81] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2730–2745, May 2011.

[82] S. Fakoorian and A. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[83] S. A. A. Fakoorian and A. L. Swindlehurst, "Competing for secrecy in the MISO interference channel," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 170–181, Jan. 2013.

[84] S. Fakoorian and A. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May 2013.

[85] J. Ni, K.-K. Wong, Z. Fei, C. Xing, H. Chen, K.-F. Tong, and J. Kuang, "Secrecy-rate balancing for two-user MISO interference channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 6–9, Feb. 2014.

[86] Z. Fei, J. Ni, N. Wang, C. Xing, and J. Kuang, "A robust and distributed design for coordinated downlink beamforming for secure MISO interference channels," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 10, pp. 1020–1027, Apr. 2014.

[87] Z. Mheich, F. Alberge, and P. Duhamel, "Achievable secrecy rates for the broadcast channel with confidential message and finite constellation inputs," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 195–205, Jan. 2015.

[88] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Asilomar Conf. on Signals, Syst. and Computers (ASILOMAR)*, Oct. 2005, pp. 1747–1751.

[89] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[90] R. Liu, Y. Liang, and H. Poor, "Fading cognitive multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4992–5005, Aug. 2011.

[91] Z. Gao, Y.-H. Yang, and K. Liu, "Anti-eavesdropping space-time network coding for cooperative communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3898–3908, November 2011.

[92] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[93] A. Sonee and G. Hodtani, "On the secrecy rate region of multiple-access wiretap channel with noncausal side information," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1151–1166, Jun. 2015.

[94] S. Agrawal and S. Vishwanath, "On the secrecy rate of interference networks using structured codes," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Seoul, Korea, Jun. 2009, pp. 2091–2095.

[95] O. Koyluoglu, H. El Gamal, L. Lai, and H. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[96] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[97] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Feasibility of positive secrecy rate in wiretap interference channels," in *IEEE Global Conf. on Signal and Inf. Proces. (GlobalSIP)*, Atlanta, GA, Dec. 2014, pp. 1190–1194.

[98] O. Koyluoglu, H. El-Gamal, L. Lai, and H. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Toronto, Canada, Jul. 2008, pp. 384–388.

[99] P. Mohapatra and C. Murthy, "Secrecy in the 2-user symmetric deterministic interference channel with transmitter cooperation," in *IEEE Workshop on Signal Proces. Advances in Wireless Commun. (SPAWC)*, Darmstadt, Germany, Jun. 2013, pp. 270–274.

[100] A. Rabbachin, A. Conti, and M. Win, "The role of aggregate interference on intrinsic network secrecy," in *IEEE Int. Conf. on Commun. (ICC)*, Ottawa, Canada, Jun. 2012, pp. 3548–3553.

[101] P. Xu, Z. Ding, X. Dai, and K. Leung, "A general framework of wiretap channel with helping interference and state information," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 182–195, Feb. 2014.

[102] M. El-Halabi and C. Georghiades, "On secure communication with known interference," in *Int. Symp. on Inf. Theory and its Applications (ISITA)*, Honolulu, HI, Oct. 2012.

[103] A. Rabbachin, A. Conti, and M. Win, "Intentional network interference for denial of wireless eavesdropping," in *IEEE Global Commun. Conf. (GLOBECOM)*, Houston, TX, Dec. 2011.

[104] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[105] L. Li, C. Huang, and Z. Chen, "Cooperative secrecy beamforming in wiretap interference channels," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2435–2439, Dec. 2015.

[106] Z. Shu, Y. Yang, Y. Qian, and R. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *IEEE Global Commun. Conf. (GLOBECOM)*, Houston, TX, Dec. 2011.

[107] Y. Liang, A. Somekh-Baruch, H. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[108] Y. Pei, Y.-C. Liang, L. Zhang, K. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[109] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[110] S. Jeong, K. Lee, J. Kang, Y. Baek, and B. Koo, "Transmit beamforming with imperfect CSIT in spectrum leasing for physical-layer security," in *IEEE Consumer Commun. and Networking Conf. (CCNC)*, Las Vegas, NV, Jan. 2012, pp. 874–878.

[111] T. Kwon, V. Wong, and R. Schober, "Secure MISO cognitive radio system with perfect and imperfect CSI," in *IEEE Global Commun. Conf. (GLOBECOM)*, Anaheim, CA, Dec. 2012, pp. 1236–1241.

[112] K. Lee, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4672–4678, Nov. 2013.

[113] D. Ng, E. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA syststems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.

[114] X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Commun. Lett.*, vol. 17, no. 4, pp. 637–640, Apr. 2013.

[115] H. Zhang, Y. Huang, S. Li, and L. Yang, "Energy-efficient precoder design for MIMO wiretap channels," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1559–1562, Sep. 2014.

[116] D. Wang, B. Bai, W. Chen, and Z. Han, "Energy efficient secure communication over decode-and-forward relay channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 892–905, Mar. 2015.

[117] H.-M. Wang, Q. Yin, W. Wang, and X.-G. Xia, "Joint null-space beamforming and jamming to secure AF relay systems with individual power constraint," in *IEEE Int. Conf. on Acoustics, Speech and Signal Proces. (ICASSP)*, May 2013, pp. 2911–2914.

[118] J. Chen, X. Chen, T. Liu, and L. Lei, "Energy-efficient power allocation for secure communications in large-scale MIMO relaying systems," in *IEEE/CIC Int. Conf. on Commun. in China (ICCC)*, Shanghai, China, Oct. 2014, pp. 385–390.

[119] Z. Han and Y. Sun, "Securing cooperative transmission in wireless communications," in *Int. Conf. on Mobile and Ubiquitous Systems: Networking Services*, NJ, Piscataway, Aug. 2007.

[120] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[121] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[122] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[123] J. Huang, A. Mukherjee, and A. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[124] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[125] A. Mukherjee, "Imbalanced beamforming by a multi-antenna source for secure utilization of an untrusted relay," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1309–1312, Jul. 2013.

[126] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2015.

[127] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[128] D. Ng, E. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[129] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[130] S. Lee and A. Khisti, "Degraded Gaussian diamond–wiretap channel," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5027–5038, Dec. 2015.

[131] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[132] X. Chen, J. Chen, and T. Liu, "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2015.

[133] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[134] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[135] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in af multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[136] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[137] R. Bassily and S. Ulukus, "Deaf cooperation for secrecy with multiple antennas at the helper," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1855–1864, Dec. 2012.

[138] ——, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[139] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[140] J. Huang and A. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[141] Y. Liu, J. Li, and A. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[142] G. Chen, Y. Gong, P. Xiao, and J. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[143] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Journal of Commun. Netw.*, vol. 14, no. 4, pp. 364–373, Aug. 2012.

[144] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[145] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[146] F. Al-Qahtani, C. Zhong, and H. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.

[147] T. Hoang, T. Duong, H. Suraweera, C. Tellambura, and H. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5051, Dec. 2015.

[148] S.-I. Kim, I.-M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724–3737, Jul. 2015.

[149] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[150] J. Lee, "Optimal power allocation for physical layer security in multi-hop DF relay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 28–38, Jan. 2016.

[151] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2015.

[152] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Veh. Technology Conf. (VTC)*, vol. 3, Stockholm, Sweden, Sep. 2005, pp. 1906–1910.

[153] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[154] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.

[155] J. Zhu, R. Schober, and V. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *Wireless Communications, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[156] O. Bakr and R. Mudumbai, "A new jamming technique for secrecy in multi-antenna wireless networks," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Austin, TX, Jun. 2010, pp. 2513–2517.

[157] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Commun.*, vol. 2, no. 3, pp. 24–32, May 2007.

[158] Y. Ding and V. Fusco, "MIMO inspired synthesis of directional modulation systems," *IEEE Antennas Wireless Propag. Lett.*, vol. PP, no. 99, 2015.

[159] ——, "Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters," *IEEE Antennas Wireless Propag. Lett.*, vol. 14, pp. 1330–1333, Jun. 2015.

[160] M. Hafez and H. Arslan, "On directional modulation: An analysis of transmission scheme with multiple directions," in *IEEE International Conference on Communication Workshop (ICCW)*, London, UK, Jun. 2015, pp. 459–463.

[161] E. J. Baghdady, "Directional signal modulation by means of switched spaced antennas," *IEEE Trans. Commun.*, vol. 38, no. 4, pp. 399–403, Apr. 1990.

[162] M. Daly and J. Bernhard, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, no. 7, pp. 2259–2265, Jul. 2010.

[163] A. Chang, A. Babakhani, and A. Hajimiri, "Near-field direct antenna modulation (NFDAM) transmitter at 2.4GHz," in *IEEE Antennas and Propagation Society International Symposium (APSURSI)*, North Charleston, SC, Jun. 2009.

[164] J. Lavaei, A. Babakhani, A. Hajimiri, and J. Doyle, "A study of near-field direct antenna modulation systems using convex optimization," in *American Control Conference (ACC)*, Baltimore, MD, Jun. 2010, pp. 1065–1072.

[165] M. Daly, E. Daly, and J. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[166] M. Daly and J. Bernhard, "Directional modulation and coding in arrays," in *IEEE International Symposium on Antennas and Propagation (APSURSI)*, Spokane, WA, Jul. 2011, pp. 1984–1987.

[167] T. Hong, M.-Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 1417–1420, Dec. 2011.

[168] N. Valliappan, A. Lozano, and R. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[169] Y. Ding and V. Fusco, "BER-driven synthesis for directional modulation secured wireless communication," *International Journal of Microwave and Wireless Technologies*, vol. 6, no. 2, pp. 139–149, Apr. 2014.

[170] ——, "Directional modulation transmitter radiation pattern considerations," *IET Microwaves, Antennas & Propagation*, vol. 7, no. 15, pp. 1201–1206, Dec. 2013.

[171] ——, "Constraining directional modulation transmitter radiation patterns," *IET Microwaves, Antennas & Propagation*, vol. 8, no. 15, pp. 1408–1415, Jul. 2014.

[172] ——, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361–370, Jan. 2014.

[173] ——, "Directional modulation far-field pattern separation synthesis approach," *IET Microwaves, Antennas & Propagation*, vol. 9, no. 1, pp. 41–48, Aug. 2014.

[174] ——, "Directional modulation-enhanced retrodirective array," *Electronics Lett.*, vol. 51, no. 1, pp. 118–120, Jan. 2015.

[175] H. Shi and A. Tennant, "Simultaneous, multichannel, spatially directive data transmission using direct antenna modulation," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 403–10, Jan. 2014.

[176] N. Alotaibi and K. Hamdi, "Switched phased-array transmission architecture for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. PP, no. 99, pp. 1–1, 2016.

[177] S. Bross, Y. Steinberg, and S. Tinguely, "The discrete memoryless interference channel with one-sided generalized feedback," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4171–4191, Jul. 2013.

[178] M. Dohler and Y. Li, *Cooperative Communications: Hardware, Channel and PHY*. Wiley, 2010. [Online]. Available: https://books.google.lu/books?id=YWj0PrnD78AC

[179] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[180] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive multiuser interference in symbol level precoding for the MISO downlink channel," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2239–2252, May 2015.

[181] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3628–3640, Jul. 2015.

[182] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive interference through symbol level precoding for multi-level modulation," in *IEEE Global Commun. Conf. (GLOBECOM)*, CA, San Diego, Dec. 2015.

[183] ——, "Symbol-level multiuser MISO precoding for multi-level adaptive modulation: A multicast view," 2016. [Online]. Available: http://arxiv.org/abs/1601.02788

[184] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[185] R. Bassoli, H. Marques, J. Rodriguez, K. Shum, and R. Tafazolli, "Network coding theory: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1–29, Fourth quarter 2013.

[186] I. Hammerstrom, M. Kuhn, C. Esli, J. Zhao, A. Wittneben, and G. Bauch, "MIMO two-way relaying with transmit CSI at the relay," in *IEEE Workshop on Signal Proces. Advances in Wireless Commun. (SPAWC)*, Helsinki, Finland, Jun. 2007.

[187] A. Amah and A. Klein, "Regenerative multi-group multi-way relaying," *IEEE Trans. Veh. Technol.*, vol. 60, no. 7, pp. 3017–3029, Sep. 2011.

[188] F. Rossetto, "A comparison of different physical layer network coding techniques for the satellite environment," in *Advanced Satellite Multimedia Syst. Conf. (ASMA) and the 11th Signal Proces. for Space Commun. Workshop (SPSC)*, Cagliari, Italy, Sep. 2010, pp. 25–30.

[189] S. Sorour, S. Valaee, and N. Alagha, "Joint control of delay and packet drop rate in satellite systems using network coding," in *Advanced Satellite Multimedia Syst. Conf. (ASMA) and the 11th Signal Proces. for Space Commun. Workshop (SPSC)*, Cagliari, Italy., Sep. 2010, pp. 46–53.

[190] F. Rossetto and D. Lucani, "Systematic design of network coding-aware buffering strategies," in *Military Commun. Conf. (MILCOM)*, Baltimore, MD, Nov. 2011, pp. 316–322.

[191] F. Vieira, D. Lucani, and N. Alagha, "Codes and balances: Multibeam satellite load balancing with coded packets," in *IEEE Int. Conf. on Commun. (ICC)*, Ottawa, Canada, Jun. 2012, pp. 3316–3321.

[192] ——, "Load-aware soft-handovers for multibeam satellites: A network coding perspective," in *Advanced Satellite Multimedia Syst. Conf. (ASMA) and the 11th Signal Proces. for Space Commun. Workshop (SPSC)*, Baiona, Spain, Sep. 2012, pp. 189–196.

[193] H. Bischl, H. Brandt, and F. Rossetto, "An experimental demonstration of network coding for satellite networks," *CEAS Space Journal*, vol. 2, no. 1-4, pp. 75–83, Jun. 2011.

[194] J. Chen, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure decode-and-forward two-way relay commun." in *IEEE Global Commun. Conf. (GLOBECOM)*, Houston, TX, Dec. 2011.

[195] A. Mukherjee and A. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *IEEE Int. Workshop*

on Signal Proces. Advances in Wireless Commun. (SPAWC), Marrakech, Morocco, Jun. 2010.

[196] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, June 2011.

[197] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[198] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, July 2012.

[199] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans.Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[200] L. Jiang, Z. Han, M. Vazquez-Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraintss," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sept. 2011.

[201] G. Zheng, P. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[202] D. Sunderland, G. Duncan, B. Rasmussen, H. Nichols, D. Kain, L. Lee, B. Clebowicz, I. Hollis, R.W., L. Wissel, and T. Wilder, "Megagate ASICs for the thuraya satellite digital signal processor," in *Int. Symp. on Quality Electronic Design*, San Jose, CA, Mar. 2002, pp. 479–486.

[203] B. Devillers, A. Perez-Neira, and C. Mosquera, "Joint linear precoding and beamforming for the forward link of multi-beam broadband satellite systems," in *IEEE Global Commun. Conf. (GLOBECOM)*, Houston, Texas, USA, Dec. 2011.

[204] A. Khan, M. Imran, and B. Evans, "Semi-adaptive beamforming for OFDM based hybrid terrestrial-satellite mobile system," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3424–3433, Oct. 2012.

[205] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

[206] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 229–238, Jan. 2013.

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

[208] Q. Li, H. Song, and K. Huang, "Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892–895, May 2013.

[209] W. Harrison and S. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *IEEE Int. Conf. on Commun. (ICC)*, Dresden, Germany, Jun. 2009.

[210] J. Li and A. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.

[211] ——, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[212] Z. Rezki, A. Khisti, and M.-S. Alouini, "Ergodic secret message capacity of the wiretap channel with finite-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3364–3379, Jun. 2014.

[213] M. Girnyk, M. Vehkapera, J. Yuan, and L. Rasmussen, "On the ergodic secrecy capacity of MIMO wiretap channels with statistical CSI," in *Int. Symp. on Inf. Theory and its Applications (ISITA)*, Melbourne, Australia, Oct. 2014, pp. 398–402.

[214] B.-G. Kim, C.-S. Kim, and D.-S. Ahn, "Performance evaluation for a closed loop power control using an efficient channel estimation in SAT-CDMA," in *IEEE Veh. Technology Conf. (VTC)*, vol. 6, Melbourne, Australia, May 2006, pp. 2625–2629.

[215] L. Cottatellucci, M. Debbah, G. Gallinaro, R. Mueller, M. Neri, and R. Rinaldo, "Interference mitigation techniques for broadband satellite systems," in *AIAA Int. Commun. Satellite Syst. Conf. (ICSSC)*, San Diego, CA, Jun. 2006.

[216] D. Christopoulos, S. Chatzinotas, G. Zheng, J. Grotz, and B. Ottersten, "Linear and nonlinear techniques for multibeam joint processing in satellite communications," *EURASIP Journal on Wireless Commun. and Networking*, vol. 2012, pp. 1–13, May 2012.

[217] J. Arnau, B. Devillers, C. Mosquera, and A. Pérez-Neira, "Performance study of multiuser interference mitigation schemes for hybrid broadband multibeam satellite architectures," *EURASIP Journal on Wireless Commun. and Networking*, vol. 2012, pp. 1–19, Apr. 2012.

[218] V. Joroughi, B. Devillers, M. Vazquez, and A. Perez-Neira, "Design of an on-board beam generation process for the forward link of a multi-beam broadband satellite system," in *IEEE Global Commun. Conf. (GLOBECOM)*, Atlanta, GA, Dec. 2013, pp. 2921–2926.

[219] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 497–510, Jun. 2008.

[220] X. Zhang, A. Ghrayeb, and M. Hasna, "On hierarchical network coding versus opportunistic user selection for two-way relay channels with asymmetric data rates," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2900–2910, Jul. 2013.

[221] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication.* New York, NY: Cambridge University Press, 2005.

[222] Z. Awan, A. Zaidi, and L. Vandendorpe, "Secure communication over parallel relay channel," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 359–371, Apr. 2012.

[223] W. Ai, Y. Huang, and S. Zhang, "New results on hermitian matrix rank-one decomposition," *Mathematical Programming*, vol. 128, no. 1-2, pp. 253–283, Jun. 2011.

[224] S. Boyd and L. Vandenberghe, *Convex Optimization.* New York, NY: Cambridge University Press, 2004.

[225] B. Vucetic and J. Du, "Channel modeling and simulation in satellite mobile communication systems," *IEEE J. Sel. Areas Commun.*, vol. 10, no. 8, pp. 1209–1218, Oct. 1992.

[226] Radio Sector, *Propagation data and prediction methods required for the design of Earth-space telecommunication systems*, Int. Telecommunication Union (ITU) Std., Oct. 2009.

[227] C. Fossa, R. Raines, G. Gunsch, and M. A. Temple, "An overview of the iridium low earth orbit (LEO) satellite system," in *IEEE National Aerospace and Electronics Conf.*, Dayton, OH, Jul. 1998, pp. 152–159.

[228] T. Chiueh and P. Tsai, *OFDM Baseband Receiver Design for Wireless Communications*. Wiley, 2008.

[229] D. Tse and S. Hanly, "Multiaccess fading channels. I. polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, Nov. 1998.

[230] S. Cui, A. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1089–1098, Aug. 2004.

[231] E.-V. Belmega and S. Lasaulce, "Energy-efficient precoding for multiple-antenna terminals," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 329–340, Jan. 2011.

[232] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Seattle, WA, Jul. 2006, pp. 356–360.

[233] A. De Maio, Y. Huang, D. Palomar, S. Zhang, and A. Farina, "Fractional QCQP with applications in ML steering direction estimation for radar detection," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 172–185, Jan. 2011.

[234] R. Horn and C. Johnson, *Matrix Analysis*. Cambridge University Press, 1990.

[235] S. Schaible and T. Ibaraki, "Fractional programming," *European Journal of Operational Research*, vol. 12, no. 4, pp. 325–338, Apr. 1983.

[236] W. Dinkelbach, "On nonlinear fractional programming," *Management Science*, vol. 13, no. 7, pp. 492–498, Mar. 1967.

[237] 3GPP, "3rd generation partnership project, technical specification group radio access network, coordinated multi-point operation for lte physical layer aspects," Technical report 36.819, 2011-2012. [Online]. Available: http://www.3gpp.org

[238] A. Goldsmith and S.-G. Chua, "Adaptive coded modulation for fading channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 595–602, May 1998.

[239] N. Sidiropoulos, T. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.

[240] G. Strang, *Introduction to Linear Algebra*, 4th ed. Wellesley-Cambridge Press and SIAM, 2009.

[241] C. L. Lawson and R. J. Hanson, *Solving least squares problems*, ser. Classics in applied mathematics. Philadelphia (Pa.): Society for Industrial and Applied Mathematics (SIAM), 1995.

[242] R. Bro and S. De Jong, "A fast non-negativity-constrained least squares algorithm," *Journal of Chemometrics*, vol. 11, no. 5, pp. 393–401, Sep. 1997.

[243] M. Spiegel, S. Lipschutz, and J. Liu, *Schaum's Outline of Mathematical Handbook of Formulas and Tables*, 3rd ed., ser. McGraw Hill professional. Mcgraw-hill, 2008.