

MIMO-BASED FRIENDLY JAMMING AND INTERFERENCE  
MANAGEMENT TECHNIQUES FOR SECURE WIRELESS  
COMMUNICATIONS

by  
Peyman Siyari

---

Copyright © Peyman Siyari 2019

A Dissertation Submitted to the Faculty of the  
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

In Partial Fulfillment of the Requirements  
For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

2019

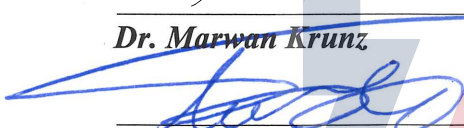
THE UNIVERSITY OF ARIZONA  
GRADUATE COLLEGE

As members of the Dissertation Committee, we certify that we have read the dissertation prepared by *Peyman Siyari*, titled *MIMO-based Friendly Jamming and Interference Management Techniques for Secure Wireless Communications* and recommend that it be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.



**Dr. Marwan Krunz**

Date: 04/10/2019



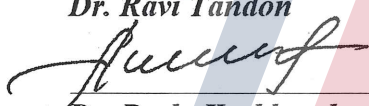
**Dr. Loukas Lazos**

Date: 04/10/2019



**Dr. Ravi Tandon**

Date: 04/10/2019



**Dr. Pavlo Krokhmal**

Date: 04/10/2019

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to the Graduate College.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it be accepted as fulfilling the dissertation requirement.



**Dr. Marwan Krunz**

Date: 04/25/2019

**Professor**

**Department of Electrical and Computer Engineering**

## ACKNOWLEDGEMENTS

I would like to thank my PhD advisor, Professor Marwan Krunz, for all the help and advice he gave me during my PhD. Through his support I was able to overcome the many obstacles of scientific research work. I will be forever grateful of the fruitful research journey I had with him.

During my PhD, I collaborated with Dr. Diep N. Nguyen, University of Technology Sydney, Australia in the projects related to distributed and secure design of wiretap interference networks (Chapters 3,4, and 5). I would like to thank Dr. Nguyen for all his support and help.

I would like to thank Professor Loukas Lazos, Professor Ravi Tandon, and Professor Pavlo Krokhamal for accepting the invitation to serve in the defense committee and for all the valuable discussions we had.

I would like to thank all my colleagues for their help and support, including Dr. Hanif Rahbari, Dr. Wessam Afifi, Berk Akgun, Irmak Aykin, Mohammed Hirzallah, Zheng-guang Zhang, Wenhan Zhang, AmirHossein Yazdani Abiyaneh, Alexander Armen Berian, Dr. Mingjie Feng, Dr. Mohammad Hassan, and Dr. Yong Xiao.

I would also thank Tami Whelan for handling all the paperwork and giving various forms of support during my graduate study.

Parts of my PhD work were sponsored by National Science Foundation (NSF) and The Qatar National Research Fund (QNRF). I would like to acknowledge both NSF and QNRF for their support.

I would like to express my deepest gratitude to my family, especially my mother Parvin and my father Davood. The long distance never separated us because of your love and

encouragement; I am blessed to be your son. My brothers Masood and Mohsen have always been there for me; I will be forever indebted to all sacrifices they have made for me. Last but not least, I would like to thank my twin brother Payam and my sister Negar who both got to live close to me in the US during my PhD. Their company was a true blessing for me in the last few years; I am thankful for having them as my siblings.

## TABLE OF CONTENTS

LIST OF FIGURES . . . . .	9
LIST OF TABLES . . . . .	11
ABSTRACT . . . . .	12
CHAPTER 1 Introduction . . . . .	15
1.1 Motivation . . . . .	15
1.2 A Primer on Information-Theoretic PHY-Layer Security . . . . .	17
1.2.1 Friendly Jamming for a Single Link . . . . .	21
1.2.2 Friendly Jamming in Multi-Link Scenarios . . . . .	23
1.2.3 Review of Existing FJ Schemes in Multi-link Scenarios . . . . .	25
1.2.4 Applications of FJ in Machine-Type Communications . . . . .	27
1.3 Main Contributions . . . . .	31
1.3.1 Game-Theoretic Precoder Design for FJ-Aided Transmissions . . . . .	32
1.3.2 Achieving PHY-Layer Secrecy via Power Control and Practical Precoder Design . . . . .	34
1.3.3 Friendly Jamming with Full-Duplex Radios in a MIMO Wiretap Channel . . . . .	35
1.3.4 PHY-Layer Security and Linear Precoding in Overloaded MU- MIMO Networks . . . . .	36
1.4 Organization . . . . .	38
CHAPTER 2 Background . . . . .	40
2.1 Mathematical Formulation of MIMO-Based Friendly Jamming . . . . .	40
2.1.1 Single-Link Scenario . . . . .	40
2.1.2 MU-MIMO Networks . . . . .	43
2.2 A Review of Game Theory for Wireless Communication Networks . . . . .	46
2.2.1 Strategic-Form Games . . . . .	48
2.2.2 Strategic Games in Interference Channels . . . . .	49
2.2.3 Power Control Game with Continuous Powers . . . . .	51
2.2.4 On Efficiency of NE . . . . .	52
CHAPTER 3 Game-Theoretic Techniques for Precoding in MIMO Wiretap Inter- ference Networks . . . . .	54
3.1 Overview . . . . .	54
3.2 System Model . . . . .	57
3.3 Problem Formulation . . . . .	59
3.4 Game-Theoretic Analysis . . . . .	65

TABLE OF CONTENTS – *Continued*

3.4.1	Variational Inequality in Complex Domain . . . . .	66
3.4.2	Quasi-Nash Equilibrium . . . . .	67
3.4.3	Analysis of QNE . . . . .	71
3.4.4	Existence and Uniqueness of the QNE . . . . .	72
3.5	Analysis of Proposed Game in the Presence of Multiple QNEs . . . . .	75
3.5.1	Convergence of Proposed Algorithm . . . . .	75
3.5.2	The Gradient-Response Algorithm . . . . .	75
3.5.3	Tikhonov Regularization . . . . .	79
3.5.4	QNE Selection Using Tikhonov Regularization . . . . .	79
3.5.5	Guaranteeing Monotonicity of $F^{\text{TR}}$ in Tikhonov Regularization . . . . .	81
3.5.6	Distributed Tikhonov Regularization . . . . .	83
3.6	QNE Selection Algorithm . . . . .	85
3.6.1	Algorithm Description . . . . .	85
3.6.2	Criterion for QNE Selection . . . . .	87
3.6.3	Signaling Overhead and Running Time . . . . .	89
3.6.4	Effect of Initial Conditions . . . . .	98
3.7	Centralized Precoder Design . . . . .	99
3.8	Simulation Results and Discussion . . . . .	104
3.9	Summary . . . . .	109
 CHAPTER 4 Pareto-Optimal Power Control with Rate Demands in MIMO Wiretap		
	Interference Networks . . . . .	111
4.1	Overview . . . . .	111
4.2	System Model . . . . .	112
4.3	Problem Formulation . . . . .	117
4.4	Game Formulation . . . . .	122
4.4.1	Greedy FJ Control . . . . .	122
4.4.2	Price-Based FJ Control . . . . .	124
4.4.3	Optimality of Greedy FJ Control . . . . .	125
4.5	Price-Based FJ Under E-CSI Uncertainties . . . . .	127
4.5.1	Mixed-Strategy Game Formulation . . . . .	128
4.5.2	Robust Solutions . . . . .	132
4.6	Comparison of Signaling Overhead . . . . .	136
4.7	Numerical Results . . . . .	140
4.8	Software-Defined Radio Implementation of Tx FJ for a Single-User Scenario . . . . .	147
4.9	Summary . . . . .	154

## TABLE OF CONTENTS – *Continued*

CHAPTER 5	Distributed Asynchronous Power Control for TxFJ and RxFJ . . . .	155
5.1	Overview . . . . .	155
5.2	System Model . . . . .	158
5.3	Problem Formulation . . . . .	164
5.3.1	Computation of RxFJ Power . . . . .	164
5.3.2	Power Allocation for TxFJ and Information Signals . . . . .	167
5.4	Game Formulation . . . . .	172
5.4.1	Existence and Uniqueness of Nash Equilibrium . . . . .	174
5.4.2	Algorithm Design . . . . .	176
5.4.3	Sufficient Conditions for NE Uniqueness . . . . .	178
5.5	Robust Power Allocation Game . . . . .	180
5.5.1	Best Response Under E-CSI Uncertainties . . . . .	180
5.5.2	Distributed Power Control Under E-CSI Uncertainties . . . . .	185
5.6	Numerical Results . . . . .	187
5.7	Summary . . . . .	196
CHAPTER 6	Linear Precoding in Overloaded Wiretap MU-MIMO Networks . .	198
6.1	Overview . . . . .	198
6.2	Conventional Precoder Design . . . . .	202
6.3	Proposed Signaling Scheme . . . . .	205
6.3.1	Security Analysis of Proposed Method . . . . .	207
6.3.2	Comparison Between Conventional ZF Method and Proposed Method . . . . .	209
6.3.3	Antenna Selection for Zero-Forcing Precoding . . . . .	210
6.4	Proposed Precoding Method . . . . .	211
6.5	Numerical Results . . . . .	216
6.6	Summary . . . . .	218
CHAPTER 7	Conclusions and Future Work . . . . .	219
7.1	Conclusions . . . . .	219
7.2	Future Work . . . . .	222
APPENDIX A	Proofs of Chapter 3 . . . . .	225
A.1	Proof of Proposition 1 . . . . .	225
A.2	Proof of Theorem 4 . . . . .	226
A.3	Proof of Theorem 5 . . . . .	227
APPENDIX B	Proofs of Chapter 4 . . . . .	233
B.1	Proof of Theorem 7 . . . . .	233
B.2	Proof of Proposition 3 . . . . .	234

TABLE OF CONTENTS – *Continued*

B.3	Proof of Proposition 4 . . . . .	239
B.4	Proof of Proposition 5 . . . . .	242
B.5	Proof of Proposition 6 . . . . .	245
APPENDIX C	Proofs of Chapter 5 . . . . .	247
C.1	Proof of Theorem 7 . . . . .	247
C.2	Proof of Theorem 9 . . . . .	250
C.3	Proof of Theorem 10 . . . . .	252
C.4	Comparison of Complexity and Signaling Overhead Between MRC and MMSE Receivers . . . . .	253
C.4.1	Computing the Optimal RxFJ Power . . . . .	255
C.4.2	Computing the Optimal Power Allocation between Information and TxFJ Signals . . . . .	255
C.5	Detailed Analysis of the Robust Scheme . . . . .	257
C.5.1	Detailed Formulation of the Robust Scheme . . . . .	257
REFERENCES	. . . . .	260



## LIST OF FIGURES

1.1	Eavesdropping in a single-link wireless communication scenario. . . . .	18
1.2	Generation of TxFJ in a single-link scenario. . . . .	22
1.3	Generation of RxFJ in a single-link scenario. . . . .	24
1.4	General model of P2P and broadcast networks. . . . .	25
1.5	General architecture of HetNet in the presence of eavesdropper(s). . . . .	29
1.6	General architecture of D2D network in the presence of eavesdropper(s). . . . .	30
1.7	System model of our work in Chapter 3 [64, 65]. . . . .	33
1.8	System model of our work in Chapter 5 [68, 69]. . . . .	37
3.1	A (clustered) MANET where two clusters (indicated by green circle) of ad-hoc nodes are near each other. . . . .	91
3.2	Comparison of the actual running time of the proposed algorithms vs. number of links and number of Eves. . . . .	98
3.3	Comparison of convergence trend of the proposed QNE selection methods. . . . .	99
3.4	Convergence of secrecy sum-rate when QNE is unique, and when multiple QNEs exist. . . . .	105
3.5	Comparison of secrecy sum-rate, sum-rate, and sum of Eves' received rates vs. number of links. . . . .	107
3.6	Comparison of total power, power allocated to information signal, and power allocated to TxFJ vs. number of links. . . . .	108
3.7	Comparison of secrecy sum-rate vs. number of Eves. . . . .	109
4.1	System model. . . . .	113
4.2	Rate pairs for the two eavesdropping channels shown as a two-user multiple access channel. . . . .	119
4.3	Probability of monotonicity of $\sigma_q^*$ w.r.t. $\sigma_r$ , $(r, q) = 1, 2, r \neq q$ . . . . .	130
4.4	Probability of convergence and secrecy sum-rate of price-based FJ control for different interference levels and different Eve locations. . . . .	141
4.5	Convergence of price-based FJ control and rate demands under Jacobi and Gauss-Seidel Methods. . . . .	142
4.6	Optimality of the greedy FJ control under different scenarios. . . . .	144
4.7	Effect of SIC on individual secrecy rates. . . . .	145
4.8	Effect of Eve's location and number of transmissions on the secrecy sum-rate for two links. . . . .	147
4.9	Experimental setup for TxFJ in a single-link scenario. . . . .	149

LIST OF FIGURES – *Continued*

4.10	Received QPSK constellation on Bob and Eve with half of total power allocated to TxFJ. . . . .	152
4.11	Placements of Eve for experiment. . . . .	153
5.1	System model. . . . .	161
5.2	Probability of having both positive secrecy and the assignment in (5.15) being the optimal solution for a single-link scenario. . . . .	188
5.3	Number of links that use fixed-power RxFJ under full (no) knowledge of E-CSI vs. transmit and RxFJ powers. . . . .	189
5.4	Probability of convergence vs. Eve's location for the full E-CSI case. . . .	191
5.5	Comparison of secrecy sum-rate between the one-dimensional search method and the heuristic method for setting $\delta$ in (5.27). . . . .	191
5.6	Probability of convergence vs. $r_{\text{circ}}$ . . . . .	192
5.7	Comparison of secrecy sum-rate, and information/leaked rates. . . . .	193
5.8	Convergence of asynchronous algorithm for different update schemes. . .	195
6.1	Comparison of SER, achieved SINR, achievable rate, and Eve's SER in underloaded and overloaded scenarios. . . . .	215

## LIST OF TABLES

4.1	Strategy table for the two-link finite jamming game with pricing. . . . .	131
4.2	Comparison of message exchange requirements for the proposed approaches. . . . .	137
4.3	SER of the main channel for different Eve placements. . . . .	153
4.4	SER of the eavesdropping channel for different Eve placements. . . . .	153

## ABSTRACT

The ever-increasing growth of wireless systems has made them an essential part of our daily life. People rely heavily on wireless networks for communications and to conduct critical transactions from their mobile devices, including financial transactions, access to health records, etc. The proliferation of wireless communication devices opens the door for many security breaches, ranging from eavesdropping to jamming attacks. Such a disadvantage stems from the broadcast nature of wireless transmissions, which creates an exposed environment.

In this dissertation, we focus on eavesdropping attacks. While cryptographic techniques can be used to thwart eavesdropping attacks and enable secure wireless communications, they are not sufficient to protect the lower-layer headers of a packet (i.e., PHY and MAC headers). Hence, even though the secret message is encrypted, these unencrypted headers can be exploited by an adversary to extract invaluable information and initiate malicious attacks (e.g., traffic classification). Physical-layer (PHY-layer) security has been introduced as a promising candidate to prevent attacks that exploit unencrypted lower layer headers.

PHY-layer security techniques typically rely on injecting an intentional interference into the medium so as to confuse nearby eavesdroppers (Eve). Specifically, a legitimate transmit-receive (Alice-Bob) pair generates a bogus signal, namely friendly jamming (FJ), along with the information signal, to increase interference at Eve(s) but without affecting the legitimate receiver (Bob). Depending on which end of a legitimate link is responsible

for generating the FJ signal, two types of FJ techniques exist: transmitter-based (TxFJ) and receiver-based (RxFJ).

In this dissertation, we propose to advance the state-of-art in PHY-layer security by considering multi-link scenarios, including multi-user multiple-input multiple-output (MU-MIMO) and peer-to-peer (P2P) networks. Specifically, we consider a scenario where one or more external Eve(s) attempt to snoop on communications of various links. In such networks, transmission of one link may be interfered with neighboring links' transmissions. Thus, special care must be dedicated to handling interference.

In our first contribution in this dissertation, we consider a P2P network tapped by external Eve(s) in which each Alice-Bob pair conceals its communications using TxFJ. TxFJ is realized at Alice side using MIMO precoding. The goal is to design the precoders for both information and TxFJ signals at all Alices so as to maximize a given utility (e.g., sum of communication rates) while preventing eavesdropping elsewhere. Because legitimate links do not cooperate with each other and there is no centralized authority to perform optimization, every link selfishly aims at maximizing its secrecy rate. Using non-cooperative game theory, we design a distributed method for maximizing the sum of secrecy rates. Under the exact knowledge of eavesdropping channels, we show that our distributed method has a comparable secrecy sum-rate to a centralized approach.

In our next contribution, we focus on employing practical precoders in our design for a P2P network. Specifically, we employed a zero-forcing-based (ZF-based) precoder for the TxFJ of each Alice-Bob pair in a P2P network. We also assume that each link has a certain rate demand to be satisfied. In such a scenario, even though the non-cooperative game designed for this P2P network is shown to be convergent to its unique Nash Equilibrium (NE), there is still no guarantee that the resulting NE is Pareto-optimal. Hence, we propose a modified price-based game, in which each link is penalized for generating

interference on other legitimate links. We show that the price-based game converges to the Pareto-optimal point of secrecy rate region. We then leverage mixed-strategy games to provide solutions that are robust to uncertainties in knowledge of eavesdropping channels. The proposed ZF-based design of precoders is also implemented on software-defined radios to assess its performance on a single link in real-world scenarios.

In another contribution of this dissertation, we consider to further enhance the secrecy of each link in a P2P network by equipping each receiver with RxFJ. Hence, in addition to the power allocation between TxFJ and information signals, we optimize RxFJ power as well. We show that by using RxFJ at each Bob, we could leverage the well-established concept of concave games, which compared to non-convex games enjoy more simplified game-theoretic analysis. We derive sufficient conditions under which the game admits a unique NE. We also propose another version of our power control algorithm that can be implemented asynchronously, making it robust to transmission delays in the network.

In our last contribution, we consider the downlink of a MU-MIMO network in the presence of an external Eve. No knowledge of Eve's location is assumed at the access point. The network is studied in underloaded and overloaded conditions. In an underloaded (overloaded) network, the number of antennas at the access point is larger (smaller) than the total number of downlink users' antennas. In the overloaded setting, traditional methods of creating TxFJ, such as ZF-based methods, are infeasible. We propose a linear precoding scheme that relaxes such infeasibility in overloaded MU-MIMO networks. In the worst-case scenario where Eve has knowledge of the channels between access point and downlink users, we show that our method imposes the most stringent condition on the number of antennas required at Eve to cancel out TxFJ signals. We also show that choosing the number of independent streams to be sent to downlink users has an important role in achieving a tradeoff between security, reliability, and the achievable rate.

## CHAPTER 1

# Introduction

### 1.1 Motivation

The traffic generated by users who access the Internet via Wi-Fi and mobile devices will soon account for 71 percent of traffic volume over the Internet [1]. This trend has been largely fueled by recent advances in wireless communications and the integration of wireless transceivers into many applications, such as smart home appliances, health monitoring and implantable devices, smart infrastructure and utility management grids (power, water, sewage), etc. Stemming from such proliferation of wireless systems, we are constantly challenged with serious threats related to privacy and data confidentiality. Many of these threats come from the broadcast nature of the wireless medium which makes communications vulnerable to passive and active attacks.

Adversaries with moderate hardware can easily eavesdrop on wireless signals and analyze them to extract information about a user, including his online activities (e.g., browsing habits [2]), his location and movement [3], or his health status (eavesdropping on wireless medical telemetry devices [4]). Other than eavesdropping, an attack may be designed to jam specific wireless communication protocols. Identifying devices that operate under a certain protocol can be a fairly easy task, as the attacker only needs to search the wireless channel for protocol-specific transmission fingerprints that are communicated in open air. Recent examples of such threats include attacks on cellular and wireless local area networks [5, 6] and implantable cardiac defibrillators [4].

Of the various malicious activities that threaten a wireless network, the main focus of this dissertation is on eavesdropping attacks. While cryptographic techniques have been exploited to thwart eavesdropping attacks on upper layers of communication protocols, they are not sufficient to safeguard lower-layer headers and control packets (e.g., preamble, and modulation scheme fields). Such packets –which are also referred to as *side-channel information (SCI)*– must be transmitted in the clear for correct protocol operation. Therefore, even when the payload is encrypted, an eavesdropper can exploit SCI to perform several malicious attacks, such as traffic analysis and selective jamming [7].

One example for exploiting SCI could target the medium access control (MAC) layer of 802.11 networks. Specifically, in the virtual carrier sensing phase of such networks, a transmitting node sends a “duration” field in the MAC header, so that other devices in the vicinity of the transmitting node update their *network allocation vectors (NAVs)* [7]. The duration field is unencrypted, which makes it possible for an eavesdropper to easily find out about the packet duration of the transmitting node. Encrypting this field is also not a good solution because the overhearing devices may have never communicated with the transmitting node but need to have established a key with the transmitting node to decrypt the duration field.

Another example of exploiting SCI was shown in [8], where an eavesdropper could target the unsecured paging protocol of 4G and 5G networks to identify the globally-unique International Mobile Subscriber Identity (IMSI) of a cellular phone. IMSI can then be exploited to extract location information of the victim. In this attack, eavesdropper only needs to know the phone number of the victim. By calling the victim a few times, the subsequent activity in the paging channel can be associated to the outgoing call and then the IMSI of the victim. Specifically, the base station notifies the cellphone user of the incoming call by sending beacons in certain occasions which are also known as *paging*



*occasions*. The paging occasions for each cellphone user is directly related to the IMSI of that user. Hence, at the time of calling the victim, eavesdropper observes the increased activity in certain paging occasions, which lead her to inferring the IMSI of the victim. Randomizing the paging occasions (via cryptography or other methods) requires base station to have established long-term sessions with the mobile user, which can increase the overhead in protocol. In fact, the mobile user may leave the cell area and thus not be served by that base station anymore.

Many other examples of SCI-based attacks (see e.g., [7]) suggest that cryptography may not be the answer to all security issues in modern wireless networks, signifying that newer directions should be explored in scenarios where cryptography falls short. Recently, researchers have started to recognize the significance of *physical-layer (PHY-layer) security* techniques that exploit the properties wireless channels/environments for encryption, authentication and device fingerprinting [9]. The interest in PHY-layer security is mainly due to its potential for enabling keyless confidential communications and its ability to obfuscate lower-layer headers. Such attributes of PHY-layer security can enable designers to complement cryptography-based schemes and add security features to the PHY-layer via novel transmission strategies. In this dissertation, we focus on *information-theoretic* PHY-layer security whose main emphasis is on preventing eavesdropping attacks.

## 1.2 A Primer on Information-Theoretic PHY-Layer Security

PHY-layer security in its information theoretic sense was introduced by Shannon in [10]. The secrecy problem that Shannon considered states that a message from a sending device (Alice) to a receiving one (Bob) is not to be captured by an eavesdropping node

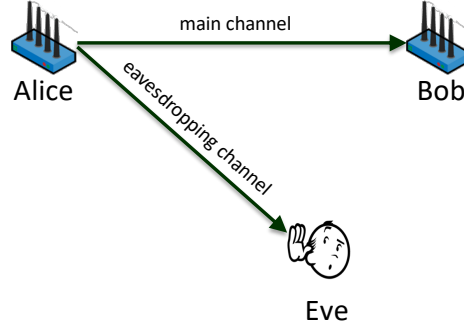


Figure 1.1: Eavesdropping in a single-link wireless communication scenario.

(Eve). Shannon assumed that both the main channel (i.e., Alice-Bob channel) and the eavesdropping channel (i.e., Alice-Eve channel) are noiseless and that Alice and Bob share a secret key. Shannon considered the communication to be *perfectly secure* if and only if the entropy of the secret message given Eve's observation is the same as the entropy of the secret message itself, i.e., Eve's observation does not contain any information about the secret message. Moreover, Shannon proved that perfectly secure communication is possible if the entropy of the secret key is at least equal to that of the secret message.

Following Shannon's theory, Wyner in [11] formulated the secrecy problem with the assumption that both Bob and Eve receive noisy versions of the secret message and that the sequence of Alice's message, Bob's received message, and Eve's wiretapped message, construct a Markov chain. Wyner also had a different (relaxing) definition of secrecy which was later termed as *weak secrecy* [12]. He claimed that for large block lengths perfect secrecy is achievable if information leakage to the eavesdropper normalized by block length goes to zero. Such definition of secrecy is not as strict as Shannon's. In fact, Shannon considered the communication to be completely untraceable at Eve, while Wyner states the leakage over a large block length is negligible. The result of Wyner's work is now referenced as the fundamental definition of *secrecy rate*. Secrecy rate is the difference of mutual information between Alice-Bob and Alice-Eve channels. Wyner's result

shows that a secure rate is achievable even if there is no key shared between legitimate nodes.

After Wyner's work, Csizar and Korner in [13] extended the wiretap model to the case that is closer to the settings in wireless communication environments. Specifically, in this model, Alice broadcasts the same secret message to both Bob and Eve. In other words, Wyner's assumption of having a Markov chain between Bob's received message and Eve's wiretapped message was removed. Moreover, Bob and Eve's received messages are corrupted by additive white Gaussian noise (AWGN). The secrecy rate was again shown to be computable by subtracting the leaked rate at Eve from the main channel's achievable rate. Intuitively, this subtraction indicates that the information rate that is not decodable by Eve(s) is the rate that can be securely communicated. Since then, most of the research in PHY-layer security has been based on this study.

The definition of secrecy rate was later extended to channels where Alice, Bob and/or Eve are equipped with multiple antennas (see [14–17]). For instance, the authors in [14] characterized the secrecy rate when the legitimate link is a multiple-input-single-output (MISO) channel and Eve has a single antenna. This result was then extended to a  $2 \times 2$  multiple-input-multiple-output (MIMO) channel with a single-antenna Eve [15]. Later on, in [16] the secrecy rate was characterized for a MISO channel with multiple antennas at Eve (MISOME channel); the same authors derived the secrecy rate of the MIMOME channel [17], and showed that Gaussian codebook achieves this secure rate.

Secrecy rate is the most common measure for PHY-layer secrecy. However, a complete characterization of secrecy rate may be prohibitive in some scenarios. For example, in the case of block-fading channels, some works have considered *secrecy outage probability* as their main metric (see [9, 12] and references therein). This measure of secrecy is weaker than secrecy rate, as security cannot be guaranteed for the entire transmission duration.

The works mentioned so far mostly rely on Gaussian codebooks and infinite block length coding. Both of these assumptions are far from being practical. To relax these assumptions and achieve practicality, there have been active research on PHY-layer security with finite block length coding and finite alphabet codebooks [12, 18, 19]. The notion of secrecy rate derived in Wyner's work assumes that probability of error can be arbitrarily decreased by increasing the block length of the underlying coding scheme. However, in finite block length regime, a certain probability of error must be considered. In addition, the notion of secrecy in Wyner's work can no longer be used, as the leakage is non-zero for finite block length regime.

Despite these differences, the secrecy definition in Wyner's work can still be used to obtain an upper bound on the secrecy rate of a channel. For example the bit-error-rate (BER) performance of M-QAM modulation scheme is directly related to the value of  $M$ . Such a relation has shown to be closely related to the information rate that is achieved using a Gaussian codebook when there is no finite-block-length assumption [20]. Specifically, the achievable  $M$  for a given BER is a function of signal-to-noise ratio (SNR); this function can be approximated as the information rate of a transmission using the Gaussian codebook with the addition of certain term known as *capacity gap*. This capacity gap determines the BER that the resulting M-QAM modulation attains at a given SNR. Therefore, both the main channel and eavesdropping channel can be studied under such approximation, so that while the assumption of finite block length coding can be relaxed, the analysis for Gaussian codebooks can be leveraged for finite-alphabet codebooks as well. Obviously, under such an approximation, the leakage will not be zero, and parts of the (encoded) bitstream can still be received at Eve. However, by creating dependencies in the bitstream (using e.g., convolutional coding of moderate length), decoding the secret

message becomes more difficult for Eve.

### 1.2.1 Friendly Jamming for a Single Link

A widely used method to provide PHY-layer secrecy is to utilize interference as a means to degrade Eve's reception. Specifically, the transmission of a secret message can be accompanied by an artificial noise (AN) that is designed to degrade the SNR at Eve but not affect Bob's reception [21]. Such a PHY-layer security technique is often referred to as *friendly jamming (FJ)*. A wide variety of methods for generating FJ signals have been proposed in the literature. Many of them focus on generating the FJ signal at Alice (the information sender), thus the name *transmit-based FJ (TxFJ)* (see [21]).

When used with single-antenna devices, TxFJ techniques cannot guarantee positive secrecy rate for all types of channels, thus not guaranteeing PHY-layer security. In such situations, it has been suggested to use dedicated FJ nodes [22]. Such a method is usually referred to as *cooperative jamming (CJ)*. Despite guaranteeing positive secrecy rate, CJ approaches face several implementation challenges related to mobility and trustworthiness. Specifically, if a legitimate receiver is mobile it may be out of the reach of a stationary CJ, or if the CJ node is a malicious node itself, it does not prevent its jamming signal to be nullified at Bob, thus compromising the legitimate transmission.

Another class of FJ schemes use multiple antennas to generate a FJ signal, which by design is nullified at Bob's location [22]. Specifically, multiple antennas prevent FJ from decreasing the SNR at Bob, as FJ can be designed to fall in the null space of the Alice-Bob channel. It has been shown that by generating FJ using multiple antennas and by having sufficient transmit power, a legitimate link can achieve positive secrecy rate even when Eve has much better conditions than Bob [22–24]. Figure 1.2 shows an example of creating TxFJ using multiple antennas.

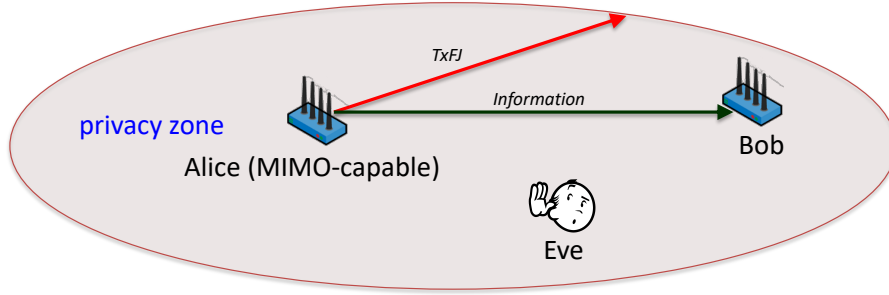


Figure 1.2: Generation of TxFJ in a single-link scenario.

The interest in applying TxFJ to a single legitimate link is driven by pragmatic considerations, and not necessarily due to its optimality. In fact, it was shown in [17] that in the case of a single eavesdropper, the optimal approach for securing a link, given knowledge of Eve's location, is not to use TxFJ. Specifically, designing MIMO precoders towards minimum leakage at Eve was shown to be the optimal approach. A practical advantage in MIMO-based FJ is that it can be used in scenarios where no knowledge on Eve's location is available [12]. Complementing the classical TxFJ approach in [22], which relies on transmitting the FJ signal in the null-space of the legitimate channel, it was shown in [25] that adding TxFJ to both the legitimate channel and its null-space can further improve the secrecy rate of a link. In the case of multiple eavesdroppers, it was shown in [26] that the use of TxFJ can significantly improve the secrecy rate compared to the case when TxFJ is not used.

Another group of FJ-based techniques exploit in-band full-duplex (FD) devices to generate FJ at the receiver (Bob) side of a legitimate link. These techniques are referred to as *receiver-based FJ (RxFJ)* methods. The main interest in using RxFJ is due to some practicality issues of TxFJ. Specifically, in a real-world wireless channel, a *vulnerability*

*region* exists which encompasses several wavelengths around Bob. The channels between Alice and any point inside this vulnerability region are highly correlated to each other. Hence, the TxFJ that was set to be nullified only at Bob will be nullified in the whole vulnerability region. If Eve exists in the vulnerability region, she will receive the secret message interference-free, thus making TxFJ ineffective [7].

To address the issue of vulnerability region, Bob can be equipped with in-band FD capability to generate RxFJ [27,28]. FD is one of the recent advances in wireless communication devices [29] that allows a device to simultaneously transmit and receive over the same frequency channel. Many implementations have been proposed over the last decade to enable in-band FD [29–33]. Each of these schemes demonstrated that the transmitted signal of a device (i.e., the device’s *self-interference*) can be sufficiently suppressed at its receive chain. Depending on the underlying suppression scheme, different self-interference suppression gains have been achieved.

In RxFJ techniques Bob generates the FJ signal while receiving the information signal from Alice. Bob’s FD capabilities allow it to prevent its transmitted FJ interfering with its reception of Alice’s information signal. By using RxFJ, it is ensured that the vulnerability region is eliminated. Figure 1.3 shows a basic setting where RxFJ can help a legitimate pair to cover the vulnerability region. Other works also considered PHY-layer security when FD capability is adopted at both Alice and Bob for bidirectional communications, i.e., Bob transmits information signals to Alice rather than generating RxFJ (see [34] and its references).

### 1.2.2 Friendly Jamming in Multi-Link Scenarios

Secrecy analysis for multi-link settings introduces new challenges not present in the single-link scenario. The multi-link scenarios that we consider in this dissertation are

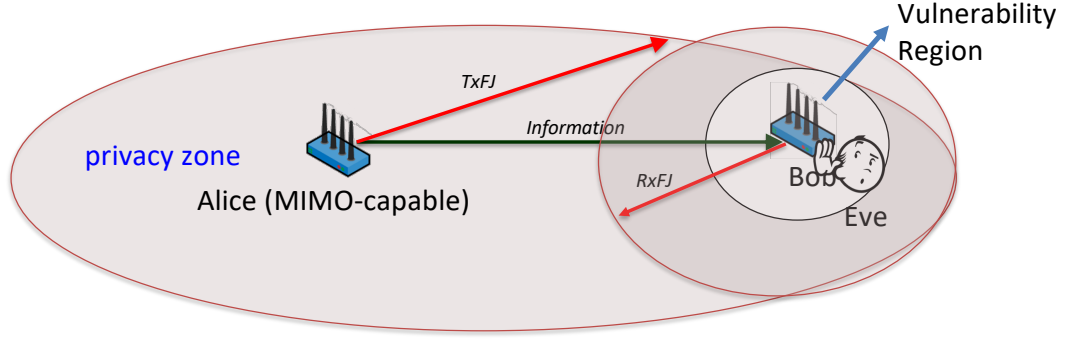


Figure 1.3: Generation of Rx FJ in a single-link scenario.

as follows: 1) peer-to-peer (P2P) network which is a network model used to study multiple transmit-receive pairs coexisting in each other's vicinity, and 2) a broadcast network where a transmitter and multiple receivers exist in an area and the transmitter sends each receiver a separate signal. Illustrations of these networks are shown in Figure 1.4.

The definition of secrecy in these multi-link settings depends on the eavesdropping behavior that causes security threat. For instance, devices in the same network may be curious about the transmissions of their neighboring devices. Thus, the design must ensure that a given link's transmission is secured from other links. Such a network is referred to as *multi-link channel with confidential messages (MCCM)*. Another possibility is when external Eves exist in the network and the transmissions of legitimate links must be kept secure from these Eves. Such a network is referred to as *multi-link wiretap channel (MWC)*. In this dissertation, we study PHY-layer security in MWCs.

For the case of P2P networks, several senders (Alices) convey their messages simultaneously to their respective Bobs. Hence, the FJ signal of each Alice must not interfere with other unintended Bobs. A key challenge here is to ensure that the null space of any Tx FJ signal is "rich enough" to include the locations of all Bobs, and yet not too large to



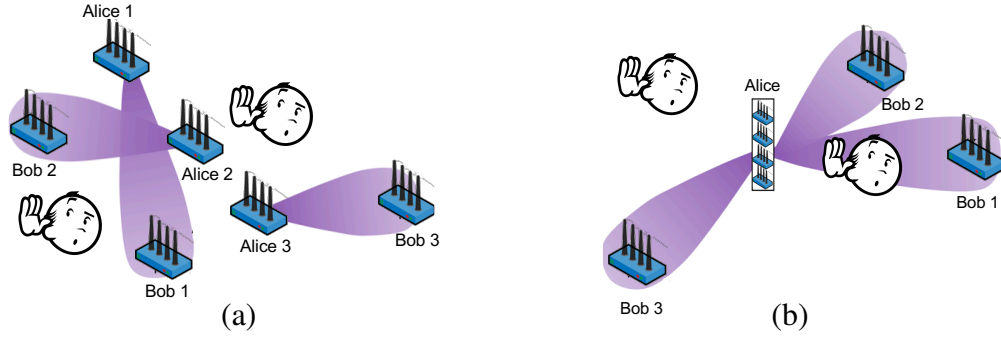


Figure 1.4: General model of a (a) P2P (b) broadcast network.

include potential eavesdropping locations. This can be quite difficult to achieve when only limited or no coordination is possible between links. Therefore, the need for interference management is crucial to guarantee a secure yet interference-limited communications.

Interference management roots back to power control problems in wireless networks, which have been extensively investigated (see for example [35–39]). The main challenge there is to manage the interference at all receivers so as to maximize a certain network utility function (e.g., sum of individual rates). In an analogous manner, in a multi-link wiretap channel, the unwanted interference from one Alice degrades the received signal at unintended Bobs, reducing the throughput in the network. However, the possibility of also degrading Eve’s reception makes the unwanted interference potentially useful in terms of improving the security of communications. In the following, we briefly mention a few of recently-proposed networking frameworks in which interference exploitation can be conducted to provide PHY-layer security.

### 1.2.3 Review of Existing FJ Schemes in Multi-link Scenarios

One of the first observations about the usefulness of interference for secret communications was made in [40], where it was shown that interference caused by information signals can be exploited to confuse nearby Eves. A similar result was observed in a sce-

nario where the secrecy of a number of links was enhanced by other active links in the network [41]. In [42] the authors considered a two-link SISO WIC with one eavesdropper. By jointly optimizing the transmission powers of the two links, the authors attempted to maximize the secrecy rate for one link while maintaining a given throughput for the second link. Other instances of exploiting interference for secure communications can be found in [43–46].

To provide secrecy for all links in the network, the authors in [47] studied two Alice-Bob-Eve triplets (i.e., each link is being eavesdropped on by a separate Eve) and proposed a cooperative beamforming approach to achieve the maximum secure degree of freedom for both links. Generalizations of interference alignment for PHY-layer secrecy were accomplished in [48]. An MWC model was considered in [49] where dedicated cooperative jammers assist legitimate links by generating FJ signals. Then, a distributed power control scheme was proposed to maximize the sum of secrecy rates (i.e., secrecy sum-rate) subject to a power budget for cooperative jammers.

For an MCCM model with MIMO links, game theory was used in [50] to study the trade-off between the network performance and fairness. Furthermore, the work in [51] considered the secrecy-rate region of the interference channel when users transmit FJ along with their information signals. They showed that by using FJ, the secrecy-rate region will be larger than when FJ is not employed. Regarding FD capability, there have been several efforts to analyze PHY-layer security when FD capability is used at both Alice and Bob for bi-directional communications, i.e., Bob is not used for generating RxFJ because he also communicates information with Alice [52–55]. The authors of [56] exploited full-duplex capability at the base station of a broadcast/multiple-access wiretap channel to secure multiple half-duplex downlink and uplink users by generating RxFJ/TxFJ for uplink/downlink communications. They proposed a multi-objective opti-

mization framework to find the best tradeoff in minimizing downlink and uplink powers, subject to certain constraints on information and secrecy rates of downlink and uplink users.

#### 1.2.4 Applications of FJ in Machine-Type Communications

Many future wireless devices will be used for machine-type communications (MTC). Examples include health monitoring and implantable devices, smart home appliances, etc. MTC devices are characterized by machine-to-machine data generation/exchange with no or little human intervention. The massive deployment of MTC devices will impose an unprecedented challenge to wireless networks. New network architectures have been designed to cope with MTC. For example, *cellular MTC (cMTC)* and *multi-tier heterogeneous networks (HetNets)* directly focus on improving current structures to enable massive connectivity [57,58]; other methods propose innovative solutions to lighten up the traffic, such as *device-to-device (D2D) communications* [59,60]. Since their introduction, each of the aforementioned network architectures have put significant effort in handling interference. Before diving into the applications of PHY-layer security in such networks, we give a brief description of them.

##### **cMTC**

As its name suggests, cMTC enables coverage for a (large) group of MTC devices using cellular networks. This network architecture mainly focuses on extending current broadcast networks such as cellular networks to achieve massive interconnections. Because of their prevalent deployment and support for mobility, cellular networks have been envisioned to carry a large portion of MTC-related applications with reduced installation cost [57]. However, to accommodate massive amounts of MTC devices, access points

(AP) require to employ scalable scheduling, multiple access and signal processing techniques.

### **HetNets**

In HetNets, small cells are added to conventional macro-cell-based networks to increase frequency reuse for more connectivity and better quality of service [58]. There have been two well-known spectrum sharing mechanisms in the literature of HetNets: 1) overlay and 2) underlay. In overlay spectrum sharing (OSS) the macro-cell users (MUs) and small-cell users (SUs) with their respective APs –i.e., macro-AP (MAP) and small-AP (SAP)– access the shared spectrum sequentially. On the other hand, in underlay spectrum sharing (USS), both tiers can simultaneously have their communications on the condition that interference is well-handled. In OSS, both tiers are in fact independent of each other. Hence, an MAP/SAP together with its associated users form a broadcast network. A distinctive assumption in HetNets is that all APs are connected together via the backhaul of the network. Thus, coordination between APs to jointly optimize transmission attributes (e.g., power allocation, transmit beamformers, etc.) is possible.

### **D2D**

D2D allows devices to communicate directly without any communication infrastructure, thus basically creating an infrastructure-less P2P network instead of having uplink and downlink communications with AP. Doing so, a portion of traffic from the infrastructure network is offloaded to a P2P network. The D2D links form a D2D cluster. D2D communication can be carried out in the same band as the uplink/downlink communications; alternatively, the links of a D2D cluster can switch to a different channel. In any case, the links within a D2D cluster share the same band, thus interfering with one

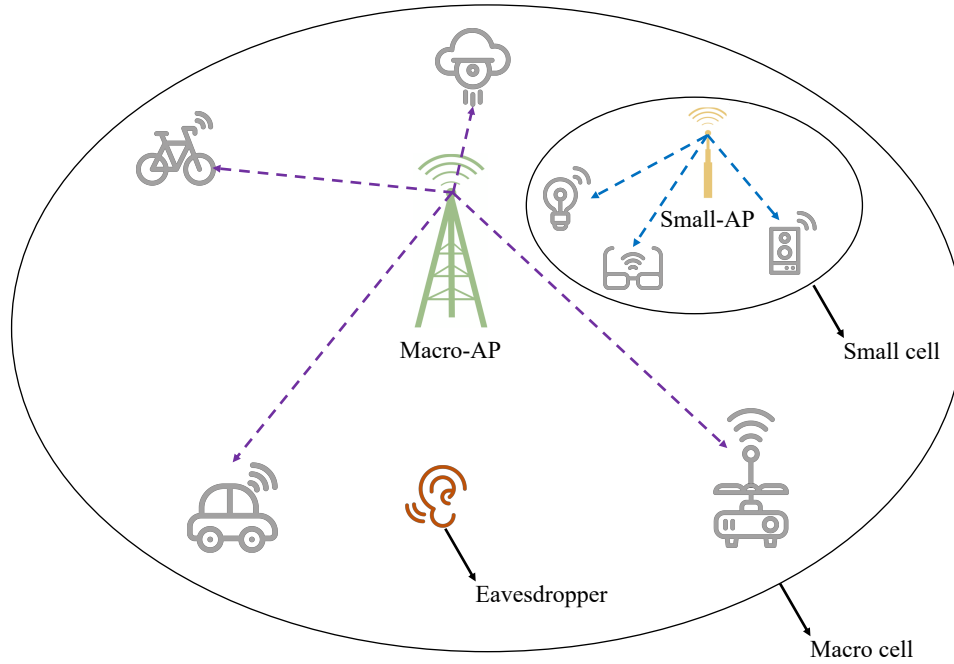


Figure 1.5: General architecture of HetNet in the presence of eavesdropper(s).

another. Such a network formed throughout the D2D cluster can be studied using the well-known P2P networks. The P2P links are not aware of each other's presence. Thus, in contrast to HetNets where coordination between APs is possible (due to the presence of backhaul), in D2D coordination among the pairs is minimal.

In the case of HetNets, interference may be generated through dense deployment of small cells. In the case of cMTC, limited feedback resources that an AP provides to MTC devices may cause erroneous acquisition of channel state information at the transmit side (CSIT), thus leading to inter-user interference. The existence of interference in D2D mainly stems from either the lack of coordination between the nodes or the absence of a central entity to perform interference attenuation/cancellation. With such an inherent existence of interference in these networks, it is possible to optimize transmission attributes of links in a way to drive away interference from legitimate links to Eves. In other words, while commonly been noted as an undesirable phenomenon, interference can be exploited

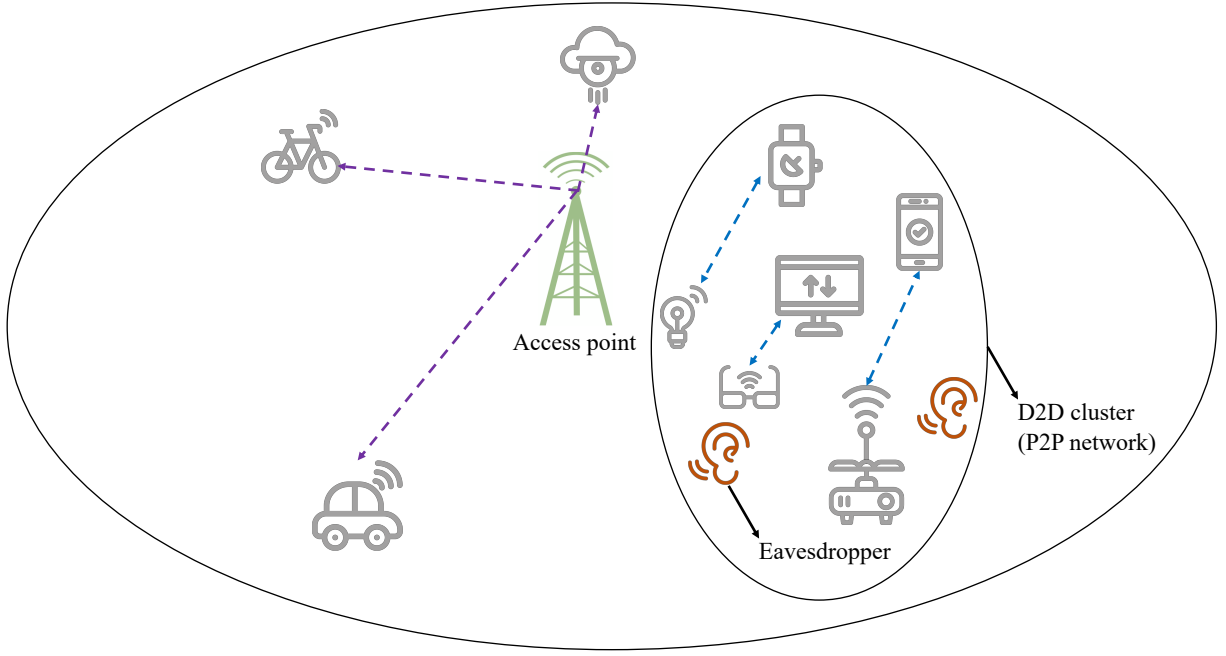


Figure 1.6: General architecture of D2D network in the presence of eavesdropper(s).

to jam potential eavesdroppers at the PHY layer and thus provide secrecy throughout these networks.

The work in [61], is one of the earliest studies in the PHY-layer security for the down-link of multi-antenna HetNets. In this work, the authors assume that APs coordinate with each other to design their transmit beamformer to maximize the secrecy rate of one MU that is being eavesdropped, subject to some rate constraints for the rest of MUs/SUs. An interesting result of this work is that the use of FJ can be redundant, as interference generated from APs already acts as FJ. The work in [62] considers the same HetNet system model with multi-antenna nodes where there is one Eve that is interested in the communications of one MU. Due to the coordination between APs, the author proposes to design an FJ-like signal at MAP to be transmitted along with the secret message, such that the interference coming from SAP is cancelled at the MU. This technique is shown to effectively decrease Eve's SINR. The Eve's CSI (E-CSI) is assumed to be partially

available as well. The author then analyzes the secrecy outage probability of the proposed scheme and shows that exploiting and mitigating the interference that is coming from SAP is more beneficial than managing it via power control. Regarding the existing work in D2D networks, because of close similarities between the structure of a P2P network and a D2D cluster, the results of secrecy analysis in P2P networks that were mentioned earlier (e.g., [42, 43, 55]) can be leveraged for D2D as well.

The authors in [63] studied a cMTC network for when the limited capacity of feedback channel –that is shared among many MTC devices– results in erroneous CSIT feedback at AP, which makes interference-free transmission more difficult. In such a situation, other than inter-user interference, the FJ signal(s) designed by AP –that were supposed to be nullified on legitimate users and confuse nearby Eves– interfere with secret messages as well. Given such settings, the authors formulate an optimization problem in which the sum of secrecy rates of several users is maximized with respect to the number of feedback bits, power allocation between the secret message and FJ, and the number of transmit antennas. This optimization is constrained by total number of feedback bits and maximum secrecy outage for each user. It is shown that as the total number of feedback bits decreases, the number of antennas required to achieve the given secrecy constraints increase to establish sufficiently good beamformers for FJ and secret messages. This result suggests that designing APs with massive number of antennas can be beneficial for cMTC networks.

### 1.3 Main Contributions

This dissertation focuses on designing and evaluating FJ-based secure communication methods in some multi-user networks. Novel PHY-layer obfuscation techniques that care-

fully control intentional interference from Alices and/or Bobs are designed. We will focus on a single collision domain, e.g., a wireless LAN or an ad hoc network where multiple authorized but potentially interfering flows are transported wirelessly (one hop) in the presence of several Eves (i.e., MWC model). Different degrees of uncertainty regarding the locations or CSI of Eves will be considered, ranging from no information to complete information. Our study will be conducted under various eavesdropping capabilities, e.g., size of antenna array at Eve, Eve's receive-based beamforming capabilities (if any), the possibility of collusion among multiple Eves, etc. From a system architecture standpoint, two networking scenarios will be considered in this dissertation: Multi-user MIMO (MU-MIMO) and P2P. In what follows, we detail our contributions in each of these networks.

### 1.3.1 Game-Theoretic Precoder Design for FJ-Aided Transmissions

In Chapter 3 of this dissertation, we consider a P2P network tapped by external Eve(s) in which each Alice-Bob pair conceals its communications using TxFJ. TxFJ is realized at Alice side using MIMO precoding. Figure 1.7 shows the general model of this network where  $Q$  Alice-Bob pairs exist in the neighborhood of  $K$  Eves. The goal is to design the precoders for both information and TxFJ signals at all  $Q$  Alices so as to maximize a given utility (e.g., sum-rate of information signals) while preventing eavesdropping elsewhere [64, 65].

Because legitimate links do not cooperate with each other and there is no centralized authority to perform optimization, every link selfishly aims at maximizing its secrecy rate. Hence, we leverage non-cooperative game theory to study the behavior of the network. In this game, the players are legitimate links, each player's strategy is the set of all TxFJ and information signal covariance matrices that satisfy a certain power constraint. Finally, the utility of each player is its secrecy rate.



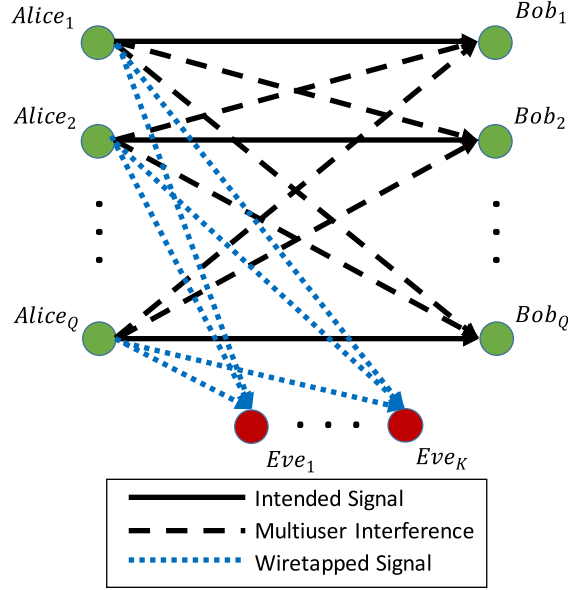


Figure 1.7: System model of our work in Chapter 3 [64, 65].

Despite coming up with a suitable game-theoretic model, the non-convexity of each link's optimization problem (i.e., best response) makes conventional convex (non-cooperative) games inapplicable to study such a network, even to find whether a Nash Equilibrium (NE) exists. To tackle this issue, we analyze the proposed game using a relaxed equilibrium concept, called *quasi-Nash equilibrium (QNE)*. We show that under a constraint qualification condition for each player's problem, the set of QNEs includes the NE of the proposed game. We also derive the conditions for the existence and uniqueness of the resulting QNE.

It turns out that the uniqueness conditions derived for the QNE of the proposed game are too restrictive, and do not always hold in typical network scenarios. Thus, the proposed game often has multiple QNEs, and the convergence to a QNE is not always guaranteed. To overcome these issues, we modify the utility functions of players by adding several specific terms to each utility function. The modified game is shown to converge

to a QNE even when multiple QNEs exist. Furthermore, we show that such modifications enable players to select a desired QNE that optimizes a given social objective (e.g., sum-rate or secrecy sum-rate). To be more specific, we propose three different QNE selection methods. Each of these methods require different signaling overheads and provide different levels of improvement on the efficiency of the proposed non-convex game.

In our first QNE selection, we suggest to select the QNE that maximize the sum of secrecy rates. The second QNE selection advises to select the QNE that maximizes the sum-rate of the network. In the last QNE selection method, we propose to select the QNE that minimizes the total leaked rate to Eves. Using simulations, we show that not only we are able to guarantee the convergence to a QNE, but also due to the QNE selection mechanism, we can achieve a significant improvement in terms of secrecy sum-rate and power efficiency, especially in dense networks. However, a not-so-suitable QNE selection method can force the links to exhaust all their resources and yet have a dismal performance.

### 1.3.2 Achieving PHY-Layer Secrecy via Power Control and Practical Precoder Design

The design of precoders in Chapter 3 is based on covariance matrix optimization. On one hand the non-convexity of secrecy rate maximization in Chapter 3 forces us to settle with a sub-optimal solution. On the other hand, the resulting covariance matrices from these sub-optimal methods are not guaranteed to be rank-1, which makes it difficult to extract practical precoders from these solutions. Therefore, in Chapter 4, we focus on exploiting practical precoders in our design. Specifically, we design a zero-forcing-based (ZF-based) precoder so that  $\mathbf{TxFJ}$  falls in the null space of the channel between Alice and her corresponding Bob, thus not affecting her corresponding Bob's reception. Such a design relaxes the complexities that resulted from optimization of covariance matrices

and makes our game-theoretic framework more practical. After designing the precoders of TxFJ and information signals, the strategy profile of each link would be to control the amount of TxFJ it generates subject to a given information-rate constraint and a power budget [66,67]. The proposed ZF-based precoder design is also implemented on software-defined radios (SDRs) to assess its performance on a single link in real-world scenarios.

Even-though the QNE selection techniques that we design in Chapter 3 can improve the performance of purely non-cooperative games, there is still no guarantee that the resulting convergence points are (Pareto-)optimal. Hence, in the remainder of Chapter 4 we propose a modified price-based game, in which each link is penalized for generating interference on other legitimate links. Under the exact knowledge of E-CSI, we show that the price-based game converges to the Pareto-optimal point of secrecy rate region and has a comparable secrecy sum-rate to a centralized approach. We then relax the assumption of knowledge of E-CSI and leverage mixed-strategy games to provide alternative solutions to the distributed secrecy sum-rate maximization problem that are robust to uncertainties in E-CSI knowledge.

### 1.3.3 Friendly Jamming with Full-Duplex Radios in a MIMO Wiretap Channel

In Chapter 5 of this dissertation, we consider to further enhance the secrecy of each link in interference networks by equipping each Bob with RxFJ [68,69]. An illustration of the system model under study in Chapter 5 is given in Figure 1.8 for a two-link network. It can be seen that the interference components at each Bob include his self-interference signal as well as information, TxFJ, and RxFJ signals of the other link. Eve also receives all information, TxFJ, and RxFJ signals. We assume that the TxFJ of each Alice falls in the null space of the channel between herself and her corresponding Bob, thus not affecting her corresponding Bob's reception. In other words, same as Chapter 4, we aim at using

practical precoders (i.e., ZF-based precoders) to create TxFJ at each link.

We show that by using RxFJ at each Bob, we can model a non-cooperative game which can leverage the well-established concept of concave (non-cooperative) games. Hence, compared to non-convex games in Chapter 3, this new game offers a much simpler analysis, enabling us to derive sufficient conditions under which the game admits a unique NE (instead of a QNE in Chapter 3) with guaranteed convergence conditions. We also design a framework in which a careful power assignment between the information signal and TxFJ at the Alice side of each link is done such that the corresponding Bob is able to decide on using RxFJ independent of any multi-user interference (MUI) factors. This ability sets Bobs free from having to measure MUI at eavesdropper(s), thus making our design robust to uncertainties in E-CSI knowledge. Our results indicate that the framework that is robust to uncertainties in E-CSI knowledge performs close to when E-CSI is fully known to legitimate links. Moreover, empirically it is shown that the secrecy sum-rate scales with the power budget of transmitters.

#### 1.3.4 PHY-Layer Security and Linear Precoding in Overloaded MU-MIMO Networks

In Chapter 6 we study precoding in the downlink of MU-MIMO wiretap networks [70]. In general, when secrecy is desired, the precoders designed for MU-MIMO networks aim to cancel out two sources of interference on Bobs. First, the MUI which occurs when signals intended for different Bobs interfere with each other<sup>1</sup>. The second source of interference that secure MU-MIMO designs have to minimize/mitigate is the one coming from FJ signals. Eve must also combat with these two sources of interference to wiretap ongoing communications.

We are primarily interested in linear precoding design approaches, as non-linear de-

---

<sup>1</sup>Mitigating MUI is a design goal that also exists in MU-MIMO networks with no secrecy considerations.

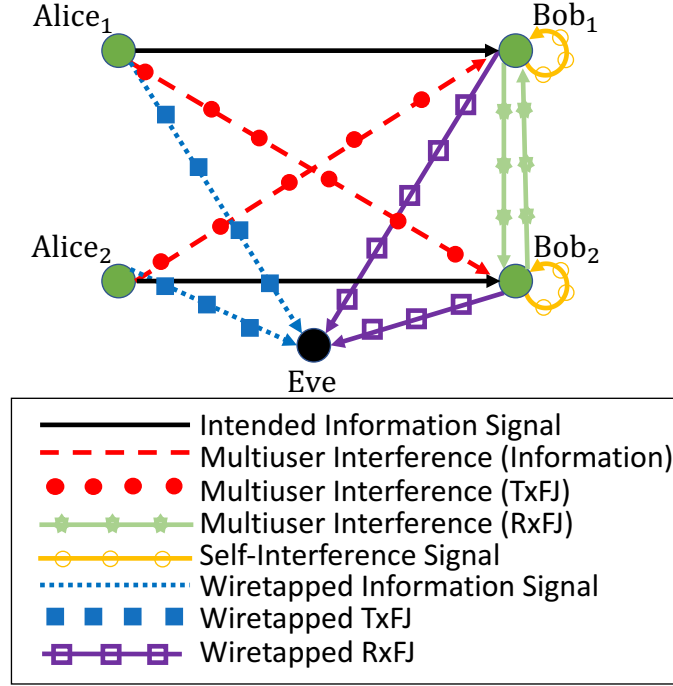


Figure 1.8: System model of our work in Chapter 5 [68, 69].

signals are not suitable for practical implementation. A fundamental condition on the capacity of MU-MIMO networks in downlink/uplink that utilize linear precoders suggests that in order to cancel out the MUI on all Bobs, the number of antennas at Alice must be greater than or equal to the total number of antennas at Bobs, i.e., the network must be *underloaded*. In *overloaded* scenarios where this condition does not hold, zero-forcing MUI and FJ signals is infeasible.

Motivated by such a challenge, we propose a new linear precoding scheme for the downlink of MU-MIMO networks which still uses FJ for preserving the secrecy but aims to extend the functionality of FJ to overloaded scenarios. In particular, we aim to minimize interference leakage of the downlink signals, which consequently minimizes the MUI. Next, we design for each Bob an exclusive FJ signal to protect the information signal that is intended for that Bob. The interference coming from this FJ signal is also minimized

as a consequence of minimization of MUI. Specifically, the FJ signal created for a Bob is similar to the information signal intended for that Bob, except that the FJ signal employs an extra precoder such that it does not affect its associated Bob's reception.

In the worst-case scenario where Eve has knowledge of the channels between Alice and Bobs, we show that our method imposes the most stringent condition on the number of antennas required at Eve to cancel out FJ signals. We verify our analyses with simulations, and it turns out that choosing the number of independent streams to be sent to Bobs has an important role in achieving a trade-off between security, reliability and the achievable rate of the Bobs.

## 1.4 Organization

The rest of this dissertation is organized as follows. In Chapter 2, we go over mathematical formulation of FJ in single-link and MU-MIMO settings. We then review game theory concepts with an emphasis on its application in wireless networks, as it is one of the key tools in most of our analyses throughout this dissertation. In Chapter 3 we focus on secure precoding design for MIMO wiretap interference networks, and introduce equilibrium selection to improve PHY-layer security of the network [64, 65]. Chapter 4 discusses power control with practical precoders for FJ and information signal. We also introduce pricing methods to approach Pareto-optimal solutions of the secrecy rate region of MIMO wiretap interference networks [66, 67]. We also discuss our SDR implementation for our proposed practical precoder design. In Chapter 5, we extend power control in MIMO wiretap interference network to the case where receivers use FD capability to transmit RxFJ. Handling the harmful interference [resulting from RxFJ] in distributed fashion and with partial knowledge of E-CSI is the main focus of this chapter [68, 69]. In

Chapter 6 we propose novel precoding design for MU-MIMO wiretap networks to extend the functionality of FJ techniques to overloaded networks [70]. Lastly, in Chapter 7, the main contributions of this dissertation are summarized and future directions for further research are discussed.

## CHAPTER 2

# Background

In this chapter we go over the design fundamentals of TxFJ techniques. The details of design in single-link and MU-MIMO scenarios are given. We then give a primer on the concepts of game theory and its applications in wireless networks.

### Notation

Boldface uppercase/lowercase letters denote matrices/vectors.  $\mathbf{a} \geq \mathbf{b}$  denotes element-wise inequality between vectors  $\mathbf{a}$  and  $\mathbf{b}$ .  $\mathbf{A}^{(:,a:b)}$  denotes a matrix that is comprised of columns  $a$  to  $b$  of  $\mathbf{A}$ .  $\mathbf{A}^{(a:b,:)}$  denotes a matrix that is comprised of rows  $a$  to  $b$  of  $\mathbf{A}$ .  $\mathbf{I}$  and  $\mathbf{0}$  denote the identity matrix and the zero matrix (i.e., matrix with zero entries) of appropriate sizes.  $E[\bullet]$ ,  $\bullet^\dagger$ ,  $\text{Tr}(\bullet)$  and  $\det(\bullet)$  are, respectively, the expected value, conjugate transpose, trace, and determinant operators. The sets of real and complex numbers are indicated by  $\mathbb{R}$  and  $\mathbb{C}$ , respectively.

## 2.1 Mathematical Formulation of MIMO-Based Friendly Jamming

### 2.1.1 Single-Link Scenario

In this scenario, two nodes, Alice and Bob communicate with each other in the presence of an eavesdropping node Eve. Alice has  $N$  transmit antennas, and Bob has  $M$  antennas. Eve is a passive node with  $L$  antennas that exists in the range of communications between



Alice and Bob. The received signal at Bob is:

$$\mathbf{y} = \tilde{\mathbf{H}}\mathbf{u} + \mathbf{n} \quad (2.1)$$

where  $\tilde{\mathbf{H}} \in \mathbb{C}^{M \times N}$ , is the  $M$ -by- $N$  complex channel matrix between Alice and Bob,  $\mathbf{u} \in \mathbb{C}^N$  is the transmitted signal from Alice, and  $\mathbf{n} \in \mathbb{C}^M$  is the complex additive white Gaussian noise (AWGN) whose covariance matrix is  $E[\mathbf{n}\mathbf{n}^\dagger] = N_0\mathbf{I}$  with  $N_0 \in \mathbb{R}^+$ . We assume  $\tilde{\mathbf{H}} = \bar{\mathbf{H}}d^{-\eta/2}$ , where  $\bar{\mathbf{H}} \in \mathbb{C}^{M \times N}$  represents the small-scale fading,  $d$  is the distance between Alice and Bob in meters, and  $\eta$  is the path-loss exponent.

The received signal at Eve is

$$\mathbf{z} = \tilde{\mathbf{G}}\mathbf{u} + \mathbf{e} \quad (2.2)$$

where  $\tilde{\mathbf{G}} \in \mathbb{C}^{L \times N}$ , denotes, the complex channel matrix between Alice and Eve. Let  $\tilde{\mathbf{G}} = \bar{\mathbf{G}}d_e^{-\eta/2}$ , where  $\bar{\mathbf{G}} \in \mathbb{C}^{L \times N}$  and  $d_e$  is the distance between Alice and Eve. Finally,  $\mathbf{e}$  has the same statistical characteristics as  $\mathbf{n}$ . The transmitted signal from Alice  $\mathbf{u} = \mathbf{s} + \mathbf{w}$  consists of the information signal  $\mathbf{s}$  and TxFJ  $\mathbf{w}$ . We set  $\mathbf{s} \triangleq \mathbf{T}\mathbf{x}$ , where  $\mathbf{T} \in \mathbb{C}^{N \times K}$  is the precoder and  $\mathbf{x} \in \mathbb{C}^K$  is the  $K$ -stream information signal.

Assume that a Gaussian codebook is used for  $\mathbf{x}$ , i.e., the elements of  $\mathbf{x}$  are distributed as a zero-mean circularly symmetric complex Gaussian random variables (ZMCSCG-RVs) with  $E[\mathbf{x}\mathbf{x}^\dagger] = \frac{\phi P}{K}\mathbf{I}$ , where  $P$  is the total transmit power of Alice and  $0 \leq \phi \leq 1$  is the fraction of transmit power allocated to the information signal. For the TxFJ, we write  $\mathbf{w} \triangleq \mathbf{Z}\mathbf{v}$ , where  $\mathbf{Z} \in \mathbb{C}^{N \times (N-K)}$  is the precoder for the TxFJ signal and  $\mathbf{v} \in \mathbb{C}^{(N-K)}$  is the TxFJ signal with i.i.d. ZMCSCG entries and  $E[\mathbf{v}\mathbf{v}^\dagger] = \sigma\mathbf{I}$ . The scalar value  $\sigma = \frac{(1-\phi)P}{N-K}$  denotes the TxFJ power<sup>1</sup>. Let  $\tilde{\mathbf{H}} = \mathbf{U}\Sigma\mathbf{V}^\dagger$  denote the singular value decomposition (SVD)

---

<sup>1</sup>Notice that the TxFJ power is distributed uniformly between various dimensions of  $\mathbf{v}$ . In the case of full knowledge of E-CSI, such power division is not optimal. However, when no knowledge of E-CSI is available, it can be shown that uniform distribution of TxFJ power among different dimensions of  $\mathbf{v}$  is

of  $\tilde{\mathbf{H}}$  where  $\Sigma$  is the diagonal matrix of singular values in descending order, and  $\mathbf{U}$  and  $\mathbf{V}$  are left and right matrices of singular vectors, respectively. We set  $\mathbf{Z} = \mathbf{V}^{(2)}$  where  $\mathbf{V}^{(2)}$  denotes the matrix of  $N - K$  rightmost columns of  $\mathbf{V}$  corresponding to the smallest singular values [22]. We assume that Alice knows  $\tilde{\mathbf{H}}^2$ . The information signal precoder  $\mathbf{T}$  is set to  $\mathbf{T} = \mathbf{V}^{(1)}$ , where  $\mathbf{V}_q^{(1)}$  is the first  $K$  columns of  $\mathbf{V}$  corresponding the largest singular values. Let  $\mathbf{H} \triangleq \tilde{\mathbf{H}}\mathbf{V}^{(1)}$ ,  $\mathbf{H}_j \triangleq \tilde{\mathbf{H}}\mathbf{V}^{(2)}$ ,  $\mathbf{G} \triangleq \tilde{\mathbf{G}}\mathbf{V}^{(1)}$ , and  $\mathbf{G}_j \triangleq \tilde{\mathbf{G}}\mathbf{V}^{(2)}$ . The terms  $\mathbf{G}$  and  $\mathbf{G}_j$ ,  $\forall q \in \mathcal{Q}$ , denote the E-CSI components. Hence, (2.1) and (2.2) can be written as

$$\begin{aligned}\mathbf{y} &= \mathbf{H}\mathbf{x} + \mathbf{H}_j\mathbf{v} + \mathbf{n} \\ \mathbf{z} &= \mathbf{G}\mathbf{x} + \mathbf{G}_j\mathbf{v} + \mathbf{e}.\end{aligned}\tag{2.3a}$$

After receiving  $\mathbf{y}$  at Bob, a linear receiver/combiner  $\mathbf{D} \in \mathbb{C}^{M \times K}$  is applied. Assuming that  $\mathbf{D}^\dagger \mathbf{H}_j \mathbf{v} = 0$ , an estimate of  $\mathbf{x}$  is given by:

$$\hat{\mathbf{x}} = \mathbf{D}^\dagger (\mathbf{H}\mathbf{x} + \mathbf{n}).\tag{2.4}$$

Eve also applies a linear combiner  $\mathbf{R} \in \mathbb{C}^{L \times K}$  while eavesdropping on Alice's signal to obtain the following estimate of  $\mathbf{x}$

$$\hat{\mathbf{z}} = \mathbf{R}^\dagger (\mathbf{G}\mathbf{x} + \mathbf{G}_j\mathbf{v} + \mathbf{e}).\tag{2.5}$$

We set  $\mathbf{D} = \mathbf{U}^{(1)}$ , where  $\mathbf{U}^{(1)}$  is the first column of  $\mathbf{U}$  (recall that  $\tilde{\mathbf{H}} = \mathbf{U}\Sigma\mathbf{V}^\dagger$ ). Using

---

optimal (see [22, 71]).

<sup>2</sup>Acquiring channel state information (CSI) between Alice and Bob is assumed to be done securely. For example, a two-phase channel estimation can be performed, where in the first/second time-slot, Alice/Bob sends the pilot signals to Bob/Alice. This way, we avoid having to send explicit CSI feedback from one communication end to another, thus lowering the probability of eavesdropping on channel estimates.

this linear combiner, the TxFJ signal of Alice will be nullified at Bob. In other words,  $\mathbf{D}^\dagger \mathbf{H}_j \mathbf{v} = 0$ . However, such a nullification does not occur on Eve's side. Hence, the TxFJ appears to Eve as interference.

### 2.1.2 MU-MIMO Networks

Consider a network where Alice with  $M$  antennas communicates with  $Q$  Bobs,  $Q \geq 2$ . Let  $\mathcal{Q} = \{1, 2, \dots, Q\}$ . Bob $_q$  has  $N_q < M$  antennas,  $q \in \mathcal{Q}$ . Without loss of generality, assume that all Bobs have the same number of antennas, i.e.,  $N_q = N < M$ ,  $\forall q \in \mathcal{Q}$ . An external Eve with  $L$  antennas also exists in the range of communications<sup>3</sup>. The setting where  $M = NQ$  is referred to as the *fully-loaded* scenario. When  $M < NQ$  the network is *overloaded*, and when  $M > NQ$  the network is *underloaded*.

Bob $_q$ ,  $q \in \mathcal{Q}$ , receives  $K_q$  independent streams from Alice where  $K_q \leq N$ . Without loss of generality, assume that  $K_q = K$ ,  $\forall q \in \mathcal{Q}$ . The number of streams determines how the antennas at Alice and Bobs are exploited. For example,  $K = N$  indicates that the signals intended for Bobs have the maximum number of streams, thus the antennas are used to exploit *spatial multiplexing* feature of the MU-MIMO network. In contrast,  $K = 1$  signifies that the combining features of Bobs are used to increase the *diversity* (thus reliability) of transmissions.

We now focus on the long-established ZF method to design the required precoding matrices. The received signal at Bob $_q$ ,  $q \in \mathcal{Q}$ , can be expressed as

$$\mathbf{y}_q = \mathbf{H}_q(\mathbf{u} + \mathbf{f}) + \mathbf{n} \quad (2.6)$$

where  $\mathbf{y}_q \in \mathbb{C}^N$ ,  $\mathbf{H}_q \in \mathbb{C}^{N \times M}$  is the complex channel between Alice and Bob $_q$ ,  $\mathbf{u} \in \mathbb{C}^M$

---

<sup>3</sup>Note that a single Eve with  $L$  antennas can also represent multiple multi-antenna colluding Eves. However, for the sake of simplicity, we consider Eve as a single entity.

is the signal containing information from Alice,  $\mathbf{f} \in \mathbb{C}^M$  is the TxFJ signal, and  $\mathbf{n} \in \mathbb{C}^N$  is the AWGN whose power  $N_0/N$  in each dimension, i.e.,  $E[\mathbf{n}\mathbf{n}^\dagger] = N_0/N\mathbf{I}$ . The signal  $\mathbf{u}$  is expressed as

$$\mathbf{u} \triangleq \sum_{q=1}^Q \mathbf{u}_q \triangleq \sum_{q=1}^Q \mathbf{T}_q \mathbf{s}_q \quad (2.7)$$

where  $\mathbf{u}_q \in \mathbb{C}^M$  is the signal intended for Bob<sub>q</sub>.  $\mathbf{T}_q$  is the precoder that is responsible for cancelling the MUI generated from  $\mathbf{u}_q$ .  $\mathbf{s}_q \in \mathbb{C}^K$  is the information signal intended for Bob<sub>q</sub>.

Assume that a Gaussian codebook is used for  $\mathbf{s}_q$ , i.e.,  $\mathbf{s}_q$  has i.i.d. entries that are ZMCSCG-RVs with  $E[\mathbf{s}_q \mathbf{s}_q^\dagger] = \phi P_q / K \mathbf{I}$  where  $P_q$  is the power of Alice allocated to Bob<sub>q</sub>'s signal, and  $\phi$  is the portion of Alice's total power allocated to all information signals. Let  $P \triangleq \sum_{q=1}^Q P_q$  where  $P$  is the total power of Alice. Alice allocates  $\phi P$  of her total power to all information signals. The rest of the power (i.e.,  $(1 - \phi)P$ ) goes to the TxFJ signal.

We assume that Alice knows all  $\mathbf{H}_i$ ,  $\forall i \in \mathcal{Q}$ , and Bob<sub>q</sub> only knows  $\mathbf{H}_q$ . In the channel estimation phase, Alice sends pilot signals to Bobs, so that Bob<sub>q</sub> can estimate  $\mathbf{H}_q$  and feed it back to Alice. Applying (2.7) in (2.6), the effective channel that Bob<sub>q</sub> sees from Alice would be  $\mathbf{H}_q \mathbf{T}_q$ . After cancelling MUI via  $\mathbf{T}_q$  (to be explained later), Alice can apply another precoder for each Bob to optimize her transmissions. Specifically, Alice can assign an extra precoder  $\mathbf{W}_q \in \mathbb{C}^{K \times K}$ , so that  $\mathbf{y}_q$  can be written as

$$\mathbf{y}_q = \mathbf{H}_q \left( \sum_{q=1}^Q \mathbf{T}_q \mathbf{W}_q \mathbf{s}_q + \mathbf{f} \right) + \mathbf{n}. \quad (2.8)$$

Bob<sub>q</sub> also applies a linear combiner to estimate the transmitted information signal. In

particular, Bob<sub>q</sub> applies  $\mathbf{D}_q \in \mathbb{C}^{K \times N}$  to have the following estimate from  $\mathbf{s}_q$ :

$$\hat{\mathbf{s}}_q \triangleq \mathbf{D}_q \mathbf{y}_q = \mathbf{D}_q \left( \mathbf{H}_q \left( \sum_{q=1}^Q \mathbf{T}_q \mathbf{W}_q \mathbf{s}_q + \mathbf{f} \right) + \mathbf{n} \right). \quad (2.9)$$

Let  $\mathbf{H}_q \mathbf{T}_q = \mathbf{U}_q \Sigma_q \mathbf{V}_q^\dagger$  be the singular-value decomposition (SVD) of  $\mathbf{H}_q \mathbf{T}_q$  where  $\mathbf{U}_q$  and  $\mathbf{V}_q$  are the unitary matrices of left and right singular vectors, and  $\Sigma_q$  is the matrix of singular values. Therefore, if Alice sets  $\mathbf{W}_q = \mathbf{V}_q^{(:,1:K)}$  and Bob<sub>q</sub> sets  $\mathbf{D}_q = \mathbf{U}_q^{(:,1:K)\dagger}$  the optimal precoder/combiner duo to receive  $K$  streams of information signals at Bob<sub>q</sub> can be established [72, Chapter 3].

Overall, the ZF method is based on nullifying both the TxFJ signal and MUI on Bobs, i.e., the design of  $\mathbf{T}_q$  and  $\mathbf{f}$  must satisfy the following:

$$\mathbf{H}_r \mathbf{T}_q = \mathbf{0}, \quad r \neq q, \quad \forall r, q \in \mathcal{Q} \quad (2.10a)$$

$$\mathbf{H}_q \mathbf{f} = \mathbf{0}, \quad \forall q \in \mathcal{Q} \quad (2.10b)$$

Therefore, the precoder  $\mathbf{T}_q$  can be determined as follows. Define  $\tilde{\mathbf{H}}_q \triangleq [\mathbf{H}_1^\dagger, \dots, \mathbf{H}_{q-1}^\dagger, \mathbf{H}_{q+1}^\dagger, \dots, \mathbf{H}_Q^\dagger]^\dagger \in \mathbb{C}^{N(Q-1) \times M}$ , and let  $\tilde{\mathbf{H}}_q = \mathbf{L}_q \mathbf{J}_q \mathbf{R}_q$  be the SVD of  $\tilde{\mathbf{H}}_q$  where  $\mathbf{L}_q$  and  $\mathbf{R}_q$  denote the matrices of left and right singular vectors, and  $\mathbf{J}_q$  denotes the matrix of singular values. Provided that  $M > N(Q-1)$ ,  $\tilde{\mathbf{H}}_q$  has a non-trivial null-space which can be exploited to meet condition (2.10a). Specifically, if  $M > N(Q-1)$  Alice sets  $\mathbf{T}_q = \mathbf{R}_q^{(:,N(Q-1)+1:M)} \in \mathbb{C}^{M \times M-N(Q-1)}$  to satisfy (2.10a) for all  $q \in \mathcal{Q}$ . The condition

$$M > N(Q-1) \quad (2.11)$$

constitutes the *information rate rank constraint (IRRC)* in the downlink of the ZF method.

The TxFJ signal mentioned in (2.6) has the following structure in the ZF method.

Define  $\tilde{\mathbf{H}} \triangleq [\mathbf{H}_1^\dagger, \dots, \mathbf{H}_Q^\dagger]^\dagger \in \mathbb{C}^{NQ \times M}$ . Let  $\tilde{\mathbf{H}} = \mathbf{L}\mathbf{J}\mathbf{R}$  be the SVD of  $\tilde{\mathbf{H}}$  where  $\mathbf{L}$  and  $\mathbf{R}$  denote the matrices of left and right singular vectors and  $\mathbf{J}$  denotes the matrix of singular values. To satisfy (2.10b),  $\tilde{\mathbf{H}}$  must have a non-trivial null-space, which requires  $M > NQ$ . Hence, the inequality

$$M > NQ \quad (2.12)$$

is the *secrecy rank constraint (SRC)* in the ZF method which satisfies the condition in (2.10b). Hence, the FJ signal can be expressed as

$$\mathbf{f} = \mathbf{Z}\mathbf{v} \quad (2.13)$$

where  $\mathbf{Z} = \mathbf{R}(:, NQ+1:M)$ .  $\mathbf{v} \in \mathbb{C}^B$  with  $B = M - NQ$  is the vector of artificial noise that has the same characteristics of AWGN except that  $E[\mathbf{v}\mathbf{v}^\dagger] = (1 - \phi)P/B\mathbf{I}$ .

## 2.2 A Review of Game Theory for Wireless Communication Networks

In this section, we introduce the fundamentals of game theory which has become visible in the last 20 years as a valuable framework for solving different problems in communication networks and signal processing. Many ongoing engineering problems in communication networks stem from a set of nodes that compete for a shared resource (e.g, spectrum). With game theory, the nodes can be modeled as players of a game, and thus the many game-theoretic studies that have been accomplished over decades can be applied to these engineering problems as well. This would be a head start for network engineers to better understand their problems.

Of all the different applications of game theory in networks (see [73] and references therein), we focus on using game theory to analyze some problems that appear in wireless

communication networks. Specifically, in a wireless network where many nodes share a specific resource (e.g., computation power, storage, spectrum), the benefit achieved by a node depends not only on its own decisions but also on those taken by other nodes. For example, wireless devices that share the same spectrum and do not know of the each other's presence in their proximity, are bound to inflict unwanted interference on each other. Thus, the transmission strategy of a node must be according to not only its own capabilities but also the amount of interference it receives from other nodes. Many research efforts have been conducted in the literature to address interference management in wireless networks using game theory, such as controlling the power of transmitted signals [36], beamforming for multi-antenna systems [39], and spectrum sensing [74].

There are three dominant mathematical representations of a game: 1) the strategic form, 2) the extensive form 3) the coalition form [73]. In the following, we mainly focus on strategic form-games, as this type of games is mainly what we exploit later on to model several problems in wireless networks and propose solutions for them. We first introduce the basic notions related to strategic-form games. Next, we give an example of application of strategic-form games in wireless networks. Lastly, we introduce special cases of strategic-form games that had a crucial rule in modeling our problems in this dissertation.

To model a problem as a game, we need to identify three components:

- players of the game, whose interests conflict each other's
- the strategy set of each player to determine what are the possible actions of each player
- a utility function for each player to determine the amount of benefit that each player can achieve by choosing a particular action.

### 2.2.1 Strategic-Form Games

A strategic-form game that has  $K$  players attributes a utility function to each player. Denote these utility function as  $u_1, \dots, u_K$ . Let  $\mathcal{K} = \{1, \dots, K\}$ . The utility function  $u_k$ ,  $k \in \mathcal{K}$ , is a function of the following form:

$$\begin{aligned} u_k : \mathcal{S} = \mathcal{S}_1 \times \dots \times \mathcal{S}_K &\rightarrow \mathbb{R} \\ \mathbf{s} = (s_1, \dots, s_K) &\rightarrow u_k(\mathbf{s}) \end{aligned} \quad (2.14)$$

where  $\mathcal{S}_k$  is the strategy set of player  $k$ ,  $s_k$  is the strategy of player  $k$ , and  $\mathbf{s}$  is the strategy profile. For player  $k$ ,  $k \in \mathcal{K}$ , the strategy profile can be equivalently shown as  $\mathbf{s} = (s_k, \mathbf{s}_{-k})$  where  $\mathbf{s}_{-k} \triangleq (s_1, \dots, s_{k-1}, s_{k+1}, \dots, s_K)$  denotes the strategies of all players except player  $k$ . Hence,  $u_k(\mathbf{s}) = u_k(s_k, \mathbf{s}_{-k})$ . We use this alternative notation for  $\mathbf{s}$  to emphasize that each player  $k$ ,  $k \in \mathcal{K}$  can only control its own strategy  $s_k \in \mathcal{S}_k$ . We define the triplet  $\mathcal{G} = (\mathcal{K}, (\mathcal{S}_k)_{k \in \mathcal{K}}, (u_k)_{k \in \mathcal{K}})$  to refer to the aforementioned strategic-form game. In some terminologies, this assumption is what makes a strategic-form game to be called a *non-cooperative game*. Such an assumption is closely related to the framework of distributed optimization in which the decision-making process is performed by independent agents who have different objective functions (i.e., utilities).

In general, the notion of optimality of a strategy profile is unclear in this type of games, as the strategies and utilities cannot be jointly controlled. The *Nash equilibrium* (NE) is a fundamental solution concept for strategic-form games, based on which the strategies of players can be found/designed. An NE of the game  $\mathcal{G}$  is a strategy profile  $\mathbf{s}^* = (s_1^*, \dots, s_K^*)$  such that

$$\forall k \in \mathcal{K}, \forall s_k \in \mathcal{S}_k, u_k(s_k^*, \mathbf{s}_{-k}^*) \geq u_k(s_k, \mathbf{s}_{-k}^*). \quad (2.15)$$



In other words, the NE is a strategy profile where no player is willing to unilaterally deviate from its strategy given the other players' strategies because any deviation degrades its utility.

In what follows, we give an example of using strategic-form games to model a problem in wireless communication networks.

### 2.2.2 Strategic Games in Interference Channels

A common wireless communication scenario is *the interference channel*, where several wireless links are placed in the vicinity of each other, and thus their transmissions may interfere with one another. A simple example for interference channel involves two transmitters and receivers. The two transmitters interfere with each other as a result of attempting to reach their respective receivers. Many wireless networks are in fact instances of an interference channel, such as

- multi-cell networks where the two (or more) transmitters belong to different cells
- a heterogeneous network where the transmitters belong to different network tiers (e.g., small cells and macro-cells)
- a cognitive radio network where the two transmitters are primary users and secondary users, respectively.

Assume that the transmitters can either transmit at a power level  $P$  or backoff from transmission. Obviously, the interference generated from a transmitter's signal degrades the signal quality of the other transmitter. Such a situation can be modeled as a game in which a transmitter-receiver pair can be considered as a player, the strategy set of player  $k$ ,  $k \in \mathcal{K} = \{1, 2\}$ , can be written as  $s_k \in \{0, P\}$ . Depending on the finiteness of strategy sets, we can judge on the existence of the NE based on the following theorem:

**Theorem 1.** *In a strategic-form game, if the number of players and the strategy set of each player are finite, then there exists at least one possible NE either in pure or mixed form [75]<sup>4</sup>.*

In the physical-layer analysis of wireless networks, most common utilities for a link are functions of end-to-end signal-to-interference-plus-noise ratio (SINR) of its comprising transmitter and receiver. Normally, SINR covers all requirements that the utility of a player must have. Specifically, the quality of the signal that is captured at the receiver side indicates the amount of satisfaction that a player gains from its action. Moreover, the interference that is also reflected in the value of SINR signifies the effect of the other player's action on the overall utility of a player. Assuming that the communication channel between a transmitter-receive pair is a *flat-fading* with AWGN noise, the SINR of player  $k$  in the interference channel can be described as

$$\gamma_k(\mathbf{s}) = \frac{h_{kk}s_k}{\sigma_k^2 + h_{rk}s_r}, \quad r \neq k, \quad r \in \{1, 2\}. \quad (2.16)$$

where  $h_{kk}$  is the channel gain from the transmitter of link  $k$  to its corresponding receiver,  $h_{rk}$  is the channel gain from the transmitter of the  $r$ th link to the receiver of the  $k$ th link, and  $\sigma_k^2$  is the power of noise at the receiver of the  $k$ th link.

Because the strategy set of each player is finite (i.e.,  $s_k \in \{0, P\}$ ), we can establish the table of strategies for both players and use Theorem 1 to find the NE. Apart from the theorems of existence of NE, the NE uniqueness can also be studied [76, Ch.3]. When the NE uniqueness is not guaranteed, there have been many studies on designing a mechanism for NE selection, such that the best NE (according to a certain criterion) is chosen (see

---

<sup>4</sup>The *mixed-strategic games* and the concept of mixed NEs are used to analyze a type of games that have the same structure of strategic-form games except that the action of a player is chosen in a probabilistic way and the satisfaction level of each player is determined by taking the expectation of its utility w.r.t its actions.

e.g., [77]).

### 2.2.3 Power Control Game with Continuous Powers

The power control game defined in the last section can be extended to the case where the strategy set  $S_k$ ,  $k \in \mathcal{K}$ , is a continuous interval. In other words, assume  $S_k = \{s_k \in \mathbb{R} : 0 \leq s_k \leq P\}$ . The existence of NE in such a setting can be analyzed based on the following theorem:

**Theorem 2.** *In a strategic-form game, if the strategy set of each player is compact and continuous, then the game has at least one NE either in pure or mixed form [78].*

Depending on the utility functions and the (compact) strategy sets, the NE of a strategic-form game with continuous strategy sets can be found from several ways (see [73] and references therein). In this section, we focus on one framework which is the foundation of most of our research efforts.

It has been shown that the NE of a non-cooperative game can often coincide with the convergence point of an interaction between several independent agents that implement an iterative or learning algorithm. Therefore, the concepts of non-cooperative games are closely related to those of multi-agent learning methods. To continue further with the idea of connecting non-cooperative games to iterative/learning algorithms, we need to define the notion of best response:

**Definition 1.** *The best response of player  $k$ ,  $k \in \mathcal{K}$  given the vector  $s_{-k}$  is a set-valued map defined as*

$$BR_k(s_{-k}) = \arg \max_{s_k \in S_k} u_k(s_k, s_{-k}). \quad (2.17)$$

Moreover, the composite best response of a game is defined as

$$\begin{aligned} BR &= \mathcal{S} \rightarrow \mathcal{S} \\ s &\rightarrow BR_1(s_{-1}) \times \dots \times BR_K(s_{-K}) \end{aligned} \quad (2.18)$$

Therefore, an alternative interpretation of NE can be given as follows:

**Corollary 1.** *Let  $\mathcal{G} = (\mathcal{K}, (\mathcal{S}_k)_{k \in \mathcal{K}}, (u_k)_{k \in \mathcal{K}})$  be a strategic-form game. A strategy profile  $s^*$  is the NE iff  $s^* \in BR(s^*)$*

Using the interconnection between NE and best response of the players, the concept of best-response dynamics can be established. Best-response dynamics is a simple interaction between players in which a player is always given the best response of other players. Such dynamics may lead to the NE of the underlying strategic-form game with continuous strategy sets. Normally, best-response dynamics involves an iterative application of each player's best response whose convergence point coincides with the NE. In some problems of communication networks, such as the one studied in [38], the best-response dynamics of a game can be simplified to a fixed-point problem, thus many analyses of convergence for fixed-point problems can be used to comment on the uniqueness of NE and designing (distributed) algorithms to achieve it.

#### 2.2.4 On Efficiency of NE

A natural question that one may ask about the NE of a game relates to the efficiency of the NE. To answer this question, we first need to define our measure of efficiency, as the notion of efficiency can be relative in games. A convenient way to examine the efficiency of NE is to evaluate it in terms of *Pareto-optimality*. A profile  $\bar{s}$  is Pareto-optimal if there

exists no  $\mathbf{s}$  such that: 1)  $u_k(\mathbf{s}) \geq u_k(\bar{\mathbf{s}})$ ,  $\forall k \in \mathcal{K}$ . Of course a Pareto-optimal profile is not dominated by the profiles for which  $u_k(\mathbf{s}) = u_k(\bar{\mathbf{s}})$ ,  $\forall k \in \mathcal{K}$ , thus all of such points are considered Pareto-optimal. The NE points of strategic-form games are not generally guaranteed to be Pareto-optimal. Hence, many studies have been done to improve the efficiency of NE to achieve Pareto-optimality. Examples of improving the performance of NE include:

- modifying the utility functions of players [37]
- letting players interact more than once (i.e., repeated games) [79]
- letting players cooperate [80]
- determining conditions where a non-cooperative game yields Pareto-optimal solutions [81].

Another appropriate measure of efficiency (i.e., social welfare) in a game would be the sum of utilities of all players. Hence, the *price of anarchy (PoA)* of a game can be defined as the ratio between the maximum sum-utility value and the minimum sum-utility value that NEs yield. The closer the PoA is to 1, the higher the efficiency of the NE. An important feature of PoA is that it can be upper-bounded in some special cases (e.g., [82]). Such a property can give us a convenient measure on the efficiency of NE, as finding the maximum sum-utility can lead to a non-convex optimization problem. With this introduction on game theory, we are now ready to apply these concepts to our problems in PHY-layer security of wireless networks. More game-theoretic concepts are introduced in next chapters which mainly stem from the fundamental concepts we described so far.

## CHAPTER 3

# Game-Theoretic Techniques for Precoding in MIMO Wiretap Interference Networks

## 3.1 Overview

In this chapter, we consider a peer-to-peer multi-link interference network where the transmission of each link (i.e., transmit-receive or Alice-Bob pair) is wiretapped by a group of eavesdroppers (Eves). Each node in the network is equipped with multiple antennas and each Alice accompanies her transmissions with TxFJ to blind nearby Eves. Our goal is to design a framework through which the co-channel interference at each Bob is minimized while the aggregate interference at Eves remains high. Because nodes cannot cooperate with each other in our settings, each link independently aims to maximize its secrecy rate by designing the covariance matrices (essentially, the precoders) of its information and TxFJ signals. This independent secrecy optimization can be modeled under a game-theoretic framework in which the utility of each player (i.e., link) is his secrecy rate, and the player's strategy is to optimize the covariance matrices of information and TxFJ signals. It turns out that finding the best response of each link requires solving a non-convex optimization problem. Thus, the existence of a Nash Equilibrium (NE) cannot be proved using traditional concepts of convex (concave) games (See Theorem 2 of Section 2).

To study this non-convex game, we utilize a relaxed equilibrium concept called quasi-Nash equilibrium (QNE) [83]. QNE is the solution of a variational inequality [84] ob-

tained under the Karush-Kuhn-Tucker (K.K.T) optimality conditions of the players' problems. We show that under a constraint qualification (CQ) condition for each player's problem, the set of QNEs also includes the NE. Sufficient conditions for the existence and uniqueness of the resulting QNE are provided. Then, an iterative algorithm is proposed to achieve the unique QNE. We also derive the conditions for the existence and uniqueness of the resulting QNE.

Due to no coordination among links, QNEs of a purely non-cooperative game often suffer from social-welfare loss. Furthermore, it turns out that the uniqueness conditions are too restrictive, and do not always hold in typical network scenarios. Thus, the proposed game often has multiple QNEs, and convergence to a QNE is not always guaranteed. To overcome these issues, we modify the utility functions of the players by adding several specific terms to each utility function. The modified game converges to a QNE even when multiple QNEs exist. Furthermore, players have the ability to select a desired QNE that optimizes a given social objective (e.g., sum rate or secrecy sum-rate). Depending on the chosen objective, the amount of signaling overhead as well as the performance of resulting QNE can be controlled. We propose three possibilities for QNE selection, each providing different benefits and requiring a different amounts of communication overhead. The proposed QNE selection algorithm can improve the performance of the formerly proposed non-cooperative game while keeping the communication overhead reasonably low.

While the works in [42, 43, 85] proposed interesting ideas for precoding/power control in wiretap interference networks, they all considered two-user scenarios and global availability of CSI, which limits their applicability. Specifically, in [42] one of the users generates only interference to provide PHY-layer security for the other user, so providing the PHY-layer secrecy of the former user is overlooked. Moreover, although [85] and [43] considered providing secrecy for both users, they assume full coordination between the

two users. In this chapter however, we aim to provide PHY-layer security for all users while limiting the amount of coordination as much as possible.

The concept of QNE has been recently used in [86] in sum-rate maximization in cognitive radio users. However, no effort has been made to improve the performance of achieved QNEs. The work in [87] also considers the use of QNEs to jointly optimize the sensing and power allocation of cognitive radio users in the presence of primary users. Although in this work some improvements have been made on the performance of the resulting QNEs, they are specific to cognitive radios and thus not extendable to other networks. The framework we propose can be generalized to any similarly structured game. Overall, our major contributions in this chapter are as follows:

- We propose a non-cooperative game to model the PHY- layer secrecy optimization in a multi-link MIMO wiretap interference network. Due to the non-convexity of each player's optimization problem, the analysis of equilibria is done through the concept of QNE. We show that the set of QNEs includes NE as well.
- Because many network scenarios may involve multiple QNEs, purely non-cooperative games do not always guarantee the convergence to a unique QNE. Hence, we introduce the additional terms in the utility function of the players to guarantee the convergence to a QNE.
- We design mechanisms that allow us to select a QNE of a specific interest from multiple QNEs. QNE selection makes it possible to improve the resulting secrecy sum-rate of the modified game compared to a purely non-cooperative game.
- We find out that managing the network interference (through both information signal and TxFJ) is more effective than aiming to increase the interference at eavesdroppers, in terms of improving the network secrecy sum-rate.



### 3.2 System Model

Consider an interference network where  $Q$  Alices,  $Q > 1$ , communicate with  $Q$  corresponding Bobs. The  $q$ th Alice is equipped with  $N_{T_q}$  antennas,  $q = 1, \dots, Q$ . The  $q$ th Bob has  $N_{R_q}$  antennas,  $q = 1, \dots, Q$ . The link between each Alice-Bob pair may experience interference from the other  $Q - 1$  links. There are  $K$  non-colluding Eves overhearing the communications. The  $k$ th Eve,  $k = 1, \dots, K$ , has  $N_{e,k}$  receive antennas<sup>1</sup>. The received signal at the  $q$ th Bob,  $\mathbf{y}_q$ , is

$$\mathbf{y}_q = \mathbf{H}_{qq}\mathbf{u}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{rq}\mathbf{u}_r + \mathbf{n}_q, \quad q \in \mathbb{Q} \quad (3.1)$$

where  $\mathbf{H}_{rq}$  ( $\mathbf{H}_{qq}$ ) denotes the  $N_{R_q} \times N_{T_r}$  ( $N_{R_q} \times N_{T_q}$ ) channel matrix between the  $r$ th ( $q$ th) Alice and  $q$ th Bob,  $\mathbf{u}_q$  is the  $N_{T_q} \times 1$  vector of transmitted signal from the  $q$ th Alice,  $\mathbf{n}_q$  is the  $N_{R_q} \times 1$  vector of additive noise whose elements are identically-independently-distributed (i.i.d) zero-mean circularly symmetric complex Gaussian (ZMCSCG) with unit variance, and  $\mathbb{Q} \triangleq \{1, \dots, Q\}$ . The term  $\sum_{\substack{r=1 \\ r \neq q}}^Q \tilde{\mathbf{H}}_{rq}\mathbf{u}_r$  is the multi-user interference (MUI). The received signal at the  $k$ th Eve,  $\mathbf{z}_k$ , is expressed as

$$\mathbf{z}_k = \sum_{q=1}^Q \mathbf{G}_{qk}\mathbf{u}_q + \mathbf{n}_{e,k}, \quad k \in \mathbb{K} \quad (3.2)$$

where  $\mathbf{G}_{qk}$  is the  $N_{e,k} \times N_{T_q}$  channel matrix between the  $q$ th Alice and the  $k$ th Eve,  $\mathbf{n}_{e,k}$  is the  $N_{e,k} \times 1$  vector of additive noise at the  $k$ th Eve, and  $\mathbb{K} \triangleq \{1, \dots, K\}$ . The transmitted

---

<sup>1</sup>The treatment can be easily extended to colluding eavesdroppers by combining the  $K$  Eves into one with  $\sum_{k=1}^K N_{e,k}$  antennas.

signal  $\mathbf{u}_q$  has the following form:

$$\mathbf{u}_q \triangleq \mathbf{s}_q + \mathbf{w}_q \quad (3.3)$$

where  $\mathbf{s}_q$  is the information signal and  $\mathbf{w}_q$  is the TxFJ. We use the Gaussian codebook for the information signal and the Gaussian noise for the TxFJ<sup>2</sup>. The matrices  $\Sigma_q$  and  $\mathbf{W}_q$  indicate the covariance matrices of  $\mathbf{s}_q$  and  $\mathbf{w}_q$ , respectively.

The  $q$ th link,  $q \in \mathbb{Q}$ , together with  $K$  Eves form a compound wiretap channel for which the achievable secrecy rate of the  $q$ th link is written as [88]:

$$R_q^{sec}(\Sigma_q, \mathbf{W}_q) \triangleq C_q(\Sigma_q, \mathbf{W}_q) - \max_{k \in \mathbb{K}} C_{e,q,k}(\Sigma_q, \mathbf{W}_q), \quad q \in \mathbb{Q} \quad (3.4)$$

where  $C_q(\Sigma_q, \mathbf{W}_q)$  is the information rate and  $C_{e,q,k}(\Sigma_q, \mathbf{W}_q)$  is the received rate at the  $k$ th eavesdropper,  $k \in \mathbb{K}$ , while eavesdropping on the  $q$ th link,  $q \in \mathbb{Q}$ . Specifically,

$$C_q(\Sigma_q, \mathbf{W}_q) \triangleq \ln |\mathbf{I} + \mathbf{M}_q^{-1} \mathbf{H}_{qq} \Sigma_q \mathbf{H}_{qq}^H| = \ln |\mathbf{M}_q + \mathbf{H}_{qq} \Sigma_q \mathbf{H}_{qq}^H| + \ln |\mathbf{M}_q^{-1}| \quad (3.5)$$

where  $\mathbf{M}_q \triangleq \mathbf{I} + \mathbf{H}_{qq} \mathbf{W}_q \mathbf{H}_{qq}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{rq} (\Sigma_r + \mathbf{W}_r) \mathbf{H}_{rq}^H$  and

$$C_{e,q,k}(\Sigma_q, \mathbf{W}_q) \triangleq \ln |\mathbf{I} + \mathbf{M}_{e,q,k}^{-1} \mathbf{G}_{qk} \Sigma_q \mathbf{G}_{qk}^H| = \ln |\mathbf{M}_{e,q,k} + \mathbf{G}_{qk} \Sigma_q \mathbf{G}_{qk}^H| + \ln |\mathbf{M}_{e,q,k}^{-1}| \quad (3.6)$$

where  $\mathbf{M}_{e,q,k} \triangleq \mathbf{I} + \mathbf{G}_{qk} \mathbf{W}_q \mathbf{G}_{qk}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{G}_{rk} (\Sigma_r + \mathbf{W}_r) \mathbf{G}_{rk}^H$ . The term  $\mathbf{M}_q$  is the covariance matrix of received interference at the  $q$ th Bob and  $\mathbf{M}_{e,q,k}$  is the covariance matrix of

---

<sup>2</sup>Other practical codebooks for the information signal (e.g., QAM) can be approximated to a Gaussian codebook with a capacity gap (see [20]).

interference received at the  $k$ th Eve while eavesdropping on the  $q$ th link<sup>3</sup>. Notice that both  $\mathbf{M}_q$  and  $\mathbf{M}_{e,q,k}$  include the information signal and TxFJ of other  $Q - 1$  links. Furthermore, we require  $\text{Tr}(\mathbf{\Sigma}_q + \mathbf{W}_q) \leq P_q$  for all  $q \in \mathbb{Q}$ , where  $\text{Tr}(\cdot)$  is the trace operator and  $P_q$  is a positive value that represents the amount of power available (for both information and TxFJ signals) at the  $q$ th Alice.

### 3.3 Problem Formulation

We assume that the  $q$ th link,  $q \in \mathbb{Q}$ , optimizes its information and TxFJ signals (through their covariance matrices  $\mathbf{\Sigma}_q$  and  $\mathbf{W}_q$ ) to maximize its own secrecy rate. The dynamics of such interaction between  $Q$  links can be modeled as a non-cooperative game where each player (i.e., link) uses his best strategy to maximize his own utility (i.e., secrecy rate) given the strategies of other players. The best response of each player can be found by solving the following optimization problem

$$\begin{aligned} & \underset{\mathbf{\Sigma}_q, \mathbf{W}_q}{\text{maximize}} \quad R_q^{\text{sec}}(\mathbf{\Sigma}_q, \mathbf{W}_q) \\ & \text{s.t.} \quad (\mathbf{\Sigma}_q, \mathbf{W}_q) \in \mathcal{F}_q, \quad q \in \mathbb{Q} \end{aligned} \tag{3.7}$$

where  $\mathcal{F}_q \triangleq \{(\mathbf{\Sigma}_q, \mathbf{W}_q) | \text{Tr}(\mathbf{\Sigma}_q + \mathbf{W}_q) \leq P_q, \mathbf{\Sigma}_q \succeq 0, \mathbf{W}_q \succeq 0\}$  is the set of all Hermitian matrices  $(\mathbf{\Sigma}_q, \mathbf{W}_q)$  that are positive semi-definite (i.e.,  $\mathbf{\Sigma}_q \succeq 0, \mathbf{W}_q \succeq 0$ ) and meet the link's power constraint.

Unfortunately, (3.7) is a non-convex optimization problem. In the remainder of this section, we aim to find a tractable solution for this problem. To that end, we first mention

---

<sup>3</sup>Specifically, while eavesdropping on a user, an eavesdropper is treating interference as additive (colored) noise.

the following identity for a positive definite matrix  $\mathbf{M}_q$  of size  $N_{R_q}$  [89, Example 3.23]:

$$\ln |\mathbf{M}_q^{-1}| = f(\mathbf{S}^*) = \max_{\mathbf{S} \in \mathbb{C}^{N_{R_q} \times N_{R_q}}, \mathbf{S} \succeq 0} f(\mathbf{S}) \quad (3.8)$$

where  $f(\mathbf{S}) \triangleq -\text{Tr}(\mathbf{S}\mathbf{M}_q) + \ln |\mathbf{S}| + N_{R_q}$  and  $\mathbf{S}^* \triangleq \mathbf{M}_q^{-1}$  is the solution to the most right-hand-side (RHS) of (3.8). Applying the reformulation in (3.8) to the term  $\ln |\mathbf{M}_q^{-1}|$  in (3.5) and  $\ln |\mathbf{M}_{e,q,k} + \mathbf{G}_{qk}\Sigma_q\mathbf{G}_{qk}^H|$  in (3.6), (3.7) can be rewritten as

$$\begin{aligned} & \underset{\Sigma_q, \mathbf{W}_q, \mathbf{S}_q}{\text{maximize}} \quad f_q(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K), \\ & \text{s.t.} \quad (\Sigma_q, \mathbf{W}_q) \in \mathcal{F}_q, \mathbf{S}_{q,k} \succeq 0, q \in \mathbb{Q}, k \in \{0\} \cup K \end{aligned} \quad (3.9)$$

where  $\{\mathbf{S}_{q,k}\}_{k=0}^K = [\mathbf{S}_{q,0}^T, \dots, \mathbf{S}_{q,K}^T]^T$ , and

$$f_q(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K) \triangleq \varphi_q(\Sigma_q, \mathbf{W}_q, \mathbf{S}_{q,0}) - \max_{k \in \mathbb{K}} \varphi_{e,q,k}(\Sigma_q, \mathbf{W}_q, \mathbf{S}_{q,k}) \quad (3.10a)$$

$$\varphi_q(\Sigma_q, \mathbf{W}_q, \mathbf{S}_{q,0}) \triangleq -\text{tr}(\mathbf{S}_{q,0}\mathbf{M}_q) + \ln |\mathbf{S}_{q,0}| + N_{R_q} + \ln |\mathbf{M}_q + \mathbf{H}_{qq}\Sigma_q\mathbf{H}_{qq}^H| \quad (3.10b)$$

$$\varphi_{e,q,k}(\Sigma_q, \mathbf{W}_q, \mathbf{S}_{q,k}) \triangleq \text{tr}(\mathbf{S}_{q,k}(\mathbf{M}_{e,q,k} + \mathbf{G}_{qk}\Sigma_q\mathbf{G}_{qk}^H)) - \ln |\mathbf{S}_{q,k}| - N_{e,k} - \ln |\mathbf{M}_{e,q,k}|. \quad (3.10c)$$

Problem (3.9) is still non-convex with respect to (w.r.t)  $(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K)$ . However, it is easy to verify that problem (3.9) is convex w.r.t either  $(\Sigma_q, \mathbf{W}_q)$  or  $\{\mathbf{S}_{q,k}\}_{k=0}^K$  (by checking its Hessian). A stationary point to problem (3.7) that satisfies its K.K.T optimality conditions then can be found by solving (3.9) sequentially w.r.t  $(\Sigma_q, \mathbf{W}_q)$  and  $\{\mathbf{S}_{q,k}\}_{k=0}^K$  [26, Section IV-B]. Specifically, in one iteration, problem (3.9) is solved w.r.t only  $\{\mathbf{S}_{q,k}\}_{k=0}^K$  to find an optimal solution  $\{\mathbf{S}_{q,k}^*\}_{k=0}^K$ . Next, with  $\{\mathbf{S}_{q,k}^*\}_{k=0}^K$  plugged in (3.10a), the problem in (3.9) is optimized w.r.t  $(\Sigma_q, \mathbf{W}_q)$  to find an optimal solution  $(\Sigma_q^*, \mathbf{W}_q^*)$ . This Alternating Optimization (AO) cycle continues until reaching a conver-

gence point. The  $n$ th iteration of AO, i.e.,  $(\mathbf{\Sigma}_q^n, \mathbf{W}_q^n, \{\mathbf{S}_{q,k}^n\}_{k=0}^K)$ , is as follows:

$$(\mathbf{\Sigma}_q^n, \mathbf{W}_q^n) = \arg \max_{(\mathbf{\Sigma}_q, \mathbf{W}_q) \in \mathcal{F}_q} f_q(\mathbf{\Sigma}_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}^{n-1}\}_{k=0}^K) \quad (3.11a)$$

$$\begin{aligned} \mathbf{S}_{q,0}^n &\triangleq \arg \max_{\mathbf{S}_{q,0} \succeq 0} \varphi_q(\mathbf{\Sigma}_q^n, \mathbf{W}_q^n, \mathbf{S}_{q,0}) = (\mathbf{M}_q^n)^{-1} \\ &= \left( \mathbf{I} + \mathbf{H}_{qq} \mathbf{W}_q^n \mathbf{H}_{qq}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{rq} (\mathbf{\Sigma}_r^0 + \mathbf{W}_r^0) \mathbf{H}_{rq}^H \right)^{-1} \end{aligned} \quad (3.11b)$$

$$\begin{aligned} \mathbf{S}_{q,k}^n &\triangleq \arg \max_{\mathbf{S}_{q,k} \succeq 0} \varphi_{e,q,k}(\mathbf{\Sigma}_q^n, \mathbf{W}_q^n, \mathbf{S}_{q,k}) = \left( \mathbf{M}_{e,q,k}^n + \mathbf{G}_{qk} \mathbf{\Sigma}_q^n \mathbf{G}_{qk}^H \right)^{-1} \\ &= \left( \mathbf{I} + \mathbf{G}_{qk} (\mathbf{\Sigma}_q^n + \mathbf{W}_q^n) \mathbf{G}_{qk}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{G}_{rk} (\mathbf{\Sigma}_r^0 + \mathbf{W}_r^0) \mathbf{G}_{rk}^H \right)^{-1}, \quad k \neq 0 \end{aligned} \quad (3.11c)$$

where  $\mathbf{\Sigma}_r^0$  and  $\mathbf{W}_r^0$  (for  $r \neq q$ ) denote the received interference components at the  $q$ th Bob prior to solving (3.9). Incorporating (3.11b) and (3.11c) in (3.11a), the solution to the convex problem (3.11a) can be found using a convex optimization solver. Notice that in (3.11b) and (3.11c), the users do not coordinate with each other in the middle of finding a stationary point for (3.9), for all  $q \in \mathbb{Q}$ . Hence, the terms  $\mathbf{\Sigma}_r^0$  and  $\mathbf{W}_r^0$ ,  $r \neq q$  remain constant during the AO iterations. To solve problem (3.9) faster, the authors in [26] solved the smooth approximation of (3.7) based on the log-sum-exp inequality [89, chapter 3.1.5], which states that

$$\max\{a_1, \dots, a_K\} \leq \frac{1}{\beta} \ln \left( \sum_{k=1}^K e^{\beta a_k} \right) \leq \max\{a_1, \dots, a_K\} + \frac{1}{\beta} \ln K. \quad (3.12)$$

where  $a_k \in \mathbb{R}$  and  $\beta > 0$ . Applying (3.12) to (3.4), we can write problem (3.7) as

$$\begin{aligned} & \underset{\Sigma_q, \mathbf{W}_q}{\text{maximize}} \quad \bar{R}_{s,q}(\Sigma_q, \mathbf{W}_q) \\ & \text{s.t.} \quad (\Sigma_q, \mathbf{W}_q) \in \mathcal{F}_q, \quad q \in \mathbb{Q} \end{aligned} \quad (3.13)$$

where

$$\bar{R}_{s,q}(\Sigma_q, \mathbf{W}_q) \triangleq C_q(\Sigma_q, \mathbf{W}_q) - \frac{1}{\beta} \ln \left( \sum_{k=1}^K \exp \{ \beta C_{e,q,k}(\Sigma_q, \mathbf{W}_q) \} \right), \quad q \in \mathbb{Q}. \quad (3.14)$$

Hence, we can do the same reformulation procedure for (3.9) to end up with the following smooth reformulation [26]:

$$\begin{aligned} & \underset{\Sigma_q, \mathbf{W}_q, \mathbf{S}_q}{\text{maximize}} \quad \bar{f}_q(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K), \\ & \text{s.t.} \quad (\Sigma_q, \mathbf{W}_q) \in \mathcal{F}_q, \quad \mathbf{S}_k \succeq 0, \quad q \in \mathbb{Q}, k \in \mathbb{K} \end{aligned} \quad (3.15)$$

where

$$\bar{f}_q(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K) \triangleq \varphi_q(\Sigma_q, \mathbf{W}_q, \mathbf{S}_{q,0}) - \frac{1}{\beta} \ln \left( \sum_{k=1}^K e^{\beta \varphi_{e,q,k}(\Sigma_q, \mathbf{W}_q, \mathbf{S}_{q,k})} \right). \quad (3.16)$$

with  $\varphi_q$  and  $\varphi_{e,q,k}$  defined in (3.10b) and (3.10c), respectively. Hence, the AO iteration in (3.11a) changes to

$$(\Sigma_q^n, \mathbf{W}_q^n) = \arg \max_{(\Sigma_q, \mathbf{W}_q) \in \mathcal{F}_q} \bar{f}_q(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}^{n-1}\}_{k=0}^K), \quad (3.17)$$

while  $\{\mathbf{S}_{q,k}^{n-1}\}_{k=0}^K$  remain the same as (3.11b) and (3.11c)<sup>4</sup>. After plugging (3.11b) and

---

<sup>4</sup>As far as optimality is concerned, it is shown in [26] that in the single-user scenario, the limit point

(3.11c) into (3.17), the solution to (3.17) at the  $n$ th iteration is computed using the Projected Gradient (PG) algorithm. The  $l$ th iteration of PG algorithm while solving (3.17) is as follows.

$$\begin{pmatrix} \hat{\Sigma}_q^{n,l+1} \\ \hat{\mathbf{W}}_q^{n,l+1} \end{pmatrix} = \text{Proj}_{\mathcal{F}_q} \begin{pmatrix} \Sigma_q^{n,l} + \alpha_l \nabla_{\Sigma_q} \bar{f}_q^{n,l} \\ \mathbf{W}_q^{n,l} + \alpha_l \nabla_{\mathbf{W}_q} \bar{f}_q^{n,l} \end{pmatrix}, \quad (3.18)$$

$$\begin{pmatrix} \Sigma_q^{n,l+1} \\ \mathbf{W}_q^{n,l+1} \end{pmatrix} = \begin{pmatrix} \Sigma_q^{n,l} \\ \mathbf{W}_q^{n,l} \end{pmatrix} + \varepsilon_l \begin{pmatrix} \hat{\Sigma}_q^{n,l+1} - \Sigma_q^{n,l} \\ \hat{\mathbf{W}}_q^{n,l+1} - \mathbf{W}_q^{n,l} \end{pmatrix}, \quad (3.19)$$

where  $\alpha_l$  and  $\varepsilon_l$  are step sizes that can be determined using Wolfe conditions for PG method [90];  $\text{Proj}_{\mathcal{F}_q}$  is the projection operator to the set  $\mathcal{F}_q$ , which can be written as

$$\text{Proj}_{\mathcal{F}_q} \begin{pmatrix} \tilde{\Sigma} \\ \tilde{\mathbf{W}} \end{pmatrix} = \min_{\mathbf{W}, \Sigma \in \mathcal{F}_q} \|\mathbf{W} - \tilde{\mathbf{W}}\|_F^2 + \|\Sigma - \tilde{\Sigma}\|_F^2; \quad (3.20)$$

$$\text{and } (\nabla_{\Sigma_q} \bar{f}_q^{n,l}, \nabla_{\mathbf{W}_q} \bar{f}_q^{n,l}) = \left( \nabla_{\Sigma_q} \bar{f}_q(\Sigma_q^{n,l}, \mathbf{W}_q^{n,l}, \{\mathbf{S}_{q,k}^{n-1}\}_{k=0}^K) \right),$$

---

of AO iterations done using (3.17), (3.11b), and (3.11c) are very close to the solutions found from AO iterations done using (3.11a), (3.11b), and (3.11c).

$\nabla_{\mathbf{W}_q} \bar{f}_q(\boldsymbol{\Sigma}_q^{n,l}, \mathbf{W}_q^{n,l}, \{\mathbf{S}_{q,k}^{n-1}\}_{k=0}^K)$  where

$$\nabla_{\boldsymbol{\Sigma}_q} \bar{f}_q(\boldsymbol{\Sigma}_q^{n,l}, \mathbf{W}_q^{n,l}, \{\mathbf{S}_{q,k}^{n-1}\}_{k=0}^K) = \mathbf{H}_{qq}^H (\mathbf{M}_q^{n,l} + \mathbf{H}_{qq} \boldsymbol{\Sigma}_q^{n,l} \mathbf{H}_{qq}^H)^{-1} \mathbf{H}_{qq} - \sum_{k=1}^K \rho_{q,k}^{n,l} \mathbf{G}_{q,k}^H \mathbf{S}_{q,k}^{n-1} \mathbf{G}_{q,k}, \quad (3.21a)$$

$$\mathbf{M}_q^{n,l} = \mathbf{I} + \mathbf{H}_{qq} \mathbf{W}_q^{n,l} \mathbf{H}_{qq}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{rq} (\boldsymbol{\Sigma}_r^0 + \mathbf{W}_r^0) \mathbf{H}_{rq}^H, \quad (3.21b)$$

$$\rho_{q,k}^{n,l} = \frac{e^{\beta \varphi_{e,q,k}(\boldsymbol{\Sigma}_q^{n,l}, \mathbf{W}_q^{n,l}, \mathbf{S}_{q,k}^{n-1})}}{\sum_{j=1}^K e^{\beta \varphi_{e,q,j}(\boldsymbol{\Sigma}_q^{n,l}, \mathbf{W}_q^{n,l}, \mathbf{S}_{q,j}^{n-1})}}, \quad (3.21c)$$

$$\nabla_{\mathbf{W}_q} \bar{f}_q(\boldsymbol{\Sigma}_q^{n,l}, \mathbf{W}_q^{n,l}, \{\mathbf{S}_{q,k}^{n-1}\}_{k=0}^K) = \mathbf{H}_{qq}^H \left( (\mathbf{M}_q^{n,l} + \mathbf{H}_{qq} \boldsymbol{\Sigma}_q^{n,l} \mathbf{H}_{qq}^H)^{-1} - \mathbf{S}_{q,0}^{n-1} \right) \mathbf{H}_{qq} + \sum_{k=1}^K \rho_{q,k}^{n,l} \mathbf{G}_{qk}^H \left( (\mathbf{M}_{e,q,k}^{n,l})^{-1} - \mathbf{S}_{q,k}^{n-1} \right) \mathbf{G}_{qk}, \quad (3.21d)$$

$$\mathbf{M}_{e,q,k}^{n,l} = \mathbf{I} + \mathbf{G}_{qk} \mathbf{W}_q^{n,l} \mathbf{G}_{qk}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{G}_{rk} (\boldsymbol{\Sigma}_r^0 + \mathbf{W}_r^0) \mathbf{G}_{rk}^H. \quad (3.21e)$$

The projection in (3.20) can be efficiently computed according to [26, Fact 1]. We refer to the game where the actions of the players are defined by (3.15) as the *proposed smooth game*. Now that we have the response of each user, we can analyze the dynamics of the proposed smooth game.

A pseudo-code of the proposed smooth game mentioned so far is shown in Algorithm 1. As mentioned earlier, finding a stationary point for (3.15) for each user consists of two nested loops. The inner loop involves the gradient projection which is shown in (3.18) and (3.19) (i.e., the loop in Line 6 of Algorithm 1). Once the optimal solution to inner loop is found, one AO iteration is done by recalculating  $\{\mathbf{S}_{q,k}\}_{k=0}^K$  according to (3.11b) and (3.11c) in the outer loop (i.e., Line 4). After the AO iterations converge to a stationary point, the users begin their transmissions using the computed precoders of information



signal and TxFJ<sup>5</sup>. Therefore, one round of this competitive secrecy rate maximization is done. Notice that according to Line 2, players will be notified of actions of each other (i.e., recalculate the received interference) only after the AO iterations has converged<sup>6</sup>. The last round of the game will be the one where the convergence is reached.

---

**Algorithm 1** Proposed Smooth Game

---

**Initialize:**  $\Sigma_q^{1,1}, \mathbf{W}_q^{1,1}, \text{Tr}(\Sigma_q^{1,1} + \mathbf{W}_q^{1,1}) < P_q, \forall q \in \mathbb{Q}$

- 1: **repeat**
- 2: Each link  $q$  computes  $\mathbf{M}_q, \mathbf{M}_{e,q,k}, \forall k \in \mathbb{K}$  locally
- 3:   **for**  $q=1, \dots, Q$  **do**
- 4:     **for**  $n = 1, \dots$  **do**
- 5:       Compute  $\mathbf{S}_{q,k}^{n-1}, k = 0, \dots, K$
- 6:       **for**  $l = 1, \dots$  **do**
- 7:          Compute  $\varphi_{e,q,k}(\Sigma_q^{n,l}, \mathbf{W}_q^{n,l}, \mathbf{S}_{q,k}^{n-1}), \mathbf{M}_q^{n,l}, \mathbf{M}_{e,q,k}^{n,l}, \forall (q, k)$
- 8:          Compute  $(\Sigma_q^{n,l+1}, \mathbf{W}_q^{n,l+1})$  using (3.18)-(3.21)   % Use Wolfe conditions
- 9:       **end for**
- 10:     **end for**
- 11:   **end for**
- 12: **until** Convergence to QNE

---

### 3.4 Game-Theoretic Analysis

Before we begin to analyze the existence and uniqueness of the QNE, we review fundamentals of *variational inequality (VI) theory* as the basis of our analyses.

#### Variational Inequality Theory

Let  $F : \mathcal{Q} \rightarrow \mathbb{R}^N$  be a vector-valued continuous real function, where  $N > 1$  and  $\mathcal{Q} \subseteq \mathbb{R}^N$  is a non-empty, closed, and convex set. The variational inequality  $\text{VI}(F, \mathcal{Q})$  is the problem

---

<sup>5</sup>Although the optimization of covariance matrices of information signal and TxFJ has been taken into account so far, the precoders can be found using eigenvalue decomposition.

<sup>6</sup>Such procedure in Line 2 of Algorithm 1 also explains the reason why  $\mathbf{W}_r^0$  and  $\Sigma_r^0$  in (3.11) and (3.21) remain constant during AO iterations.

of finding a vector  $x^*$  such that

$$(x - x^*)^T F(x^*) \geq 0, \quad \forall x \in \mathcal{Q}. \quad (3.22)$$

The relation between VI and game theory is summarized in the following theorem:

**Theorem 3.** [84, Chapter 2] *Consider  $Q$  players in a non-cooperative game with utility function  $f_q(x)$  for the  $q$ th player (not to be confused with the  $f_q$  defined in (3.9)), where  $x \in \mathcal{Q}$  and  $x = [x_1, x_2, \dots, x_Q]^T$ ,  $x_q$  is the  $q$ th player's strategy, and  $f_q(x)$  is concave w.r.t  $x_q$  for all  $q$ . The set  $\mathcal{Q}$  is comprised of all strategy sets (i.e.,  $\mathcal{Q} = \prod_{q=1}^Q \mathcal{Q}_q$ , where  $\mathcal{Q}_q$  is the  $q$ th player's strategy set). Assuming the differentiability of  $f_q(x)$  w.r.t  $x_q$  and that  $\mathcal{Q}_q$  is a closed and convex set for all  $q$ , the vector  $x^*$  is the NE of the game if for  $F(x) = [-\nabla_{x_1} f_1(x), -\nabla_{x_2} f_2(x), \dots, -\nabla_{x_Q} f_Q(x)]^T$  we have:*

$$(x - x^*)^T F(x^*) \geq 0, \quad \forall x \in \mathcal{Q}.$$

□

### 3.4.1 Variational Inequality in Complex Domain

The theory of VI mentioned in (3.22) assumes that  $\mathcal{Q} \subseteq \mathbb{R}^n$ . However, this assumption might not be of our interest because the strategies of the players in our proposed game are two complex matrices (i.e.,  $\Sigma_q$  and  $\mathbf{W}_q$ ). Therefore, an alternative definition for VI in complex domain is needed. We use the definitions derived by the authors in [91] to define VI in complex domain.

### Minimum Principle in Complex Domain

Consider the following optimization

$$\begin{aligned} & \underset{\mathbf{Z}}{\text{minimize}} \quad f(\mathbf{Z}) \\ & \text{s.t.} \quad \mathbf{Z} \in \mathcal{K} \end{aligned} \tag{3.23}$$

where  $f : \mathcal{K} \rightarrow \mathbb{R}$  is convex and continuously differentiable on  $\mathcal{K}$  where  $\mathcal{K} \subseteq \mathbb{C}^{N' \times N}$ ,  $N' > 1$ , and  $N > 1$ .  $X \in \mathcal{K}$  is an optimal solution to (3.23) if and only if we have [91, Lemma 23]

$$\langle \mathbf{Z} - \mathbf{X}, \nabla_{\mathbf{Z}} f(\mathbf{X}) \rangle \geq 0, \quad \forall \mathbf{Z} \in \mathcal{K}. \tag{3.24}$$

where  $\langle \mathbf{A}, \mathbf{B} \rangle = \text{Re}(\text{Tr}(\mathbf{A}^H \mathbf{B}))$ .

Using the definition of minimum principle in complex domain, we can now define the VI problem in the domain of complex matrices. For a complex-valued matrix  $F^{\mathbb{C}}(\mathbf{Z}) : \mathcal{K} \rightarrow \mathbb{C}^{N' \times N}$  where  $\mathcal{K} \subseteq \mathbb{C}^{N' \times N}$ , the VI in the complex domain is the problem of finding a complex matrix  $\mathbf{Y}$  such that the following is satisfied [91, Definition 25]

$$\langle \mathbf{Z} - \mathbf{Y}, F^{\mathbb{C}}(\mathbf{Y}) \rangle \geq 0, \quad \forall \mathbf{Z} \in \mathcal{K}. \tag{3.25}$$

#### 3.4.2 Quasi-Nash Equilibrium

It should be emphasized that the optimization problem of each player mentioned in (3.13) is non-convex. Hence, the solution found for each link by solving (3.15) at Line 10 of Algorithm 1 is only a stationary point of problem (3.13). As a consequence, traditional concepts of concave games used in proving the existence of a NE are not applicable here. Specifically, according to [78], the quasi-concavity of each player's utility w.r.t his strat-

egy is required in proving the existence of a NE— an assumption that is not true in our game. Instead, we analyze the proposed (non-convex) smooth game based on the relaxed equilibrium concept of QNE [83]. In the following, a formal definition of QNE is given [83].

Consider a non-cooperative game with  $Q$  player each of whose strategies are restricted by some private constraints denoted as

$$\mathcal{X}_q = \{x_q \in X_q | h_q(x_q) \leq 0\}. \quad (3.26)$$

The set  $X_q$  is a convex set, and  $h_q : \xi_q \rightarrow \mathbb{R}^{l_q}$  is a continuously differentiable mapping on the open convex set  $\xi_q$  containing  $X_q$ . No convexity assumption is made on  $h_q$ . Hence, although  $X_q$  is a convex set,  $\mathcal{X}_q$  is not necessarily so. Player  $q$  has an objective function  $g_q : \xi \rightarrow \mathbb{R}$ , assumed to be continuously differentiable where  $\xi = \prod_{q=1}^Q \xi_q$ . The action of each player is formulated as follows:

$$\begin{aligned} & \underset{x_q \in \mathcal{X}_q}{\text{minimize}} \quad g_q(x_q, x_{-q}) \\ & \text{s.t.} \quad x_q \in \mathcal{X}_q. \end{aligned} \quad (3.27)$$

Obviously, the equivalent formulation can be written for when the action of each player is maximizing an objective (e.g., utility). Given the actions of other players, i.e.,  $x_{-q}^*$ , and provided that a CQ condition holds at a point  $x_q^*$ , a necessary condition for  $x_q^*$  to be an optimal point of player  $q$ 's optimization problem (i.e., action) is the existence of a

non-negative constant vector  $\mu_q^* \in \mathbb{R}_+^{l_q}$  such that

$$\nabla_{x_q} L_q(x_q^*, x_{-q}^*, \mu_q^*) = \nabla_{x_q} g_q(x_q^*, x_{-q}^*) + \mu_q^{*T} \nabla_{x_q} h_q(x_q^*) = 0, \quad (3.28a)$$

$$\mu_q^{*T} h_q(x_q^*) = 0, \quad (3.28b)$$

$$h_q(x_q^*) \leq 0, \quad x_q \in X_q. \quad (3.28c)$$

If any CQ is satisfied at  $x_q^*$ , the optimality conditions in (3.28) can be written as a VI over the set  $X_q$ . That is, the necessary condition for  $x_q^*$  to be an optimal solution to player  $q$ 's optimization problem is if  $x_q^*$  solves  $\text{VI}(\nabla_{x_q} L_q(\bullet, x_{-q}^*, \mu_q^*), X_q)$  [84, Proposition 1.3.4]. Furthermore, the existence of a non-negative vector  $\mu_q^*$  together with the complementarity of  $\mu_q^*$  and  $h_q(x_q^*)$  can be interpreted as  $\mu_q^*$  being such that

$$-(\mu_q - \mu_q^*)^T h_q(x_q^*) \geq 0, \quad \forall \mu_q \in \mathbb{R}_+^{l_q}. \quad (3.29)$$

Clearly, if  $h_q(x_q^*)$  is not binding, i.e.,  $h_q(x_q^*) < 0$ , then  $\mu_q^* = 0$  satisfies (3.29). Furthermore, when  $h_q(x_q^*)$  is binding, i.e.,  $h_q(x_q^*) = 0$ , inequality (3.29) is trivially satisfied for all  $\mu_q \in \mathbb{R}_+^{l_q}$ . Hence, using (3.29) and the fact that  $x_q^*$  solves  $\text{VI}(\nabla_{x_q} L_q(\bullet, x_{-q}^*, \mu_q^*), X_q)$ , the pair  $(x_q^*, \mu_q^*)$  solves the following VI:

$$\left( \begin{array}{c} x_q - x_q^* \\ \mu_q - \mu_q^* \end{array} \right)^T \Gamma_q(x, \mu_q) \geq 0, \quad \forall (x_q, \mu_q) \in \mathcal{R}_q = X_q \times \mathbb{R}_+^{l_q} \quad (3.30)$$

where

$$\Gamma_q(x, \mu_q) = \left( \begin{array}{c} \nabla_{x_q} L_q(\bullet, x_{-q}^*, \mu_q^*) \\ -h_q(x_q^*) \end{array} \right). \quad (3.31)$$

Notice that although it might seem that  $\text{VI}(\nabla_{x_q} L_q(\bullet, x_{-q}^*, \mu_q^*), X_q)$  and (3.29) cannot be

combined to build (3.30), using the fact that VI is a generalized definition of a set-valued mapping<sup>7</sup>, we are able to justify (3.30). it can be proved that for the set-valued mappings  $N_{X_q}(x_q)$  and  $N_{\mathbb{R}_+^{l_q}}(\mu_q)$ , we have  $N_{X_q \times \mathbb{R}_+^{l_q}}(x_q, \mu_q) = N_{X_q}(x_q) \times N_{\mathbb{R}_+^{l_q}}(\mu_q)$  [92]. The same conclusion holds for VI problems. Hence, inequality (3.30) can be deduced.

Concatenating the inequality in (3.30) over the set of players, the QNE can be defined as follows:

**Definition 2.** *The QNE is the pair  $(x_q^*, \mu_q^*)$ ,  $q = 1 \dots, Q$ , that satisfies the following inequality:*

$$\left( \left( \begin{array}{c} x_q - x_q^* \\ \mu_q - \mu_q^* \end{array} \right)_{q=1}^Q \right)^T (\Gamma_q(x, \mu_q))_{q=1}^Q \geq 0, \quad \forall (x_q, \mu_q)_{q=1}^Q \in \prod_{q=1}^Q \mathcal{R}_q = \prod_{q=1}^Q (X_q \times \mathbb{R}_+^{l_q}) \quad (3.32)$$

where  $(\bullet)_{q=1}^Q$  denotes a column vector.

Notice that the set  $\prod_{q=1}^Q \mathcal{R}_q$  is a convex set, and if the actions of each player is a convex program, the QNE reduces to NE. In our scenario, since the private constraints for each player is a convex set, we embedded the private constraints into the set  $\mathcal{R}_q$  defined in (3.32). We need to emphasize the fact that the constant vectors  $\mu_q^*$  for all  $q$  can only be defined if the optimization problem of each player satisfies some CQ conditions. For players with convex problems, these constant vectors are trivially satisfied since the K.K.T conditions are necessary and sufficient conditions of optimality in convex programs.

One intuition that can be given on the concept of QNE is as follows. QNE is point where no player has an incentive to unilaterally change his strategy because any change

---

<sup>7</sup>A point-to-set map, also called a multi-function or a set-valued map, is a map  $N$  from  $\mathbb{R}^n$  into the power set of  $\mathbb{R}^n$ , i.e., for every  $x \in \mathbb{R}^n$ ,  $N_{\mathbb{R}^n}(x)$  is a (possibly empty) subset of  $\mathbb{R}^n$  [84, Chapter 2.1.3].

makes a player not satisfy the K.K.T conditions of his problem. This is in contrast with the definition of NE in which the lack of incentives at NE is because of losing optimality. Again, optimality and satisfying the K.K.T conditions are equivalent when players solve convex programs.

### 3.4.3 Analysis of QNE

According to the aforementioned definition, the QNEs are tuples that satisfy the K.K.T conditions of all players' optimization problems. Under a constraint qualification, stationary points of each player's optimization problem satisfy its K.K.T conditions. To begin the analysis of the QNE, we first show that the stationary point found using AO mentioned previously (i.e., Line 4-10 of Algorithm 1) satisfies the K.K.T conditions of (3.13).

**Proposition 1.** *For the  $q$ th link,  $q \in \mathbb{Q}$ , the stationary point found using AO (i.e., Line 4-10 of Algorithm 1) satisfies the K.K.T conditions of (3.13).*

*Proof.* See Appendix A. □

Now that the K.K.T optimality of the stationary point found by AO iterations is proved, we rewrite the K.K.T conditions of all players to a proper VI problem [83]. The solution(s) to the obtained VI is the QNE(s) of the proposed smooth game. For the proposed smooth game defined using (3.15), we can establish the following VI to characterize the QNE points. Let the QNE point be as follows

$$\mathbf{Y} = \{\mathbf{Y}_q\}_{q=1}^Q \triangleq [\boldsymbol{\Sigma}^T, \mathbf{W}^T]^T = \{[\boldsymbol{\Sigma}_q^T, \mathbf{W}_q^T]^T\}_{q=1}^Q \quad (3.33)$$

where  $\{[\boldsymbol{\Sigma}_q^T, \mathbf{W}_q^T]^T\}_{q=1}^Q = [\boldsymbol{\Sigma}_1^T, \mathbf{W}_1^T, \boldsymbol{\Sigma}_2^T, \mathbf{W}_2^T, \dots, \boldsymbol{\Sigma}_Q^T, \mathbf{W}_Q^T]^T$ . The function  $F^C(Z)$  is writ-

ten as

$$F^{\mathbb{C}} = F^{\mathbb{C}}(\mathbf{\Sigma}, \mathbf{W}, \mathbf{S}) = \left\{ F_q^{\mathbb{C}}(\mathbf{\Sigma}_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K) \right\}_{q=1}^Q \triangleq \left\{ \left[ -(\nabla_{\mathbf{\Sigma}_q} \bar{f}_q)^T, -(\nabla_{\mathbf{W}_q} \bar{f}_q)^T \right]^T \right\}_{q=1}^Q \quad (3.34)$$

where the terms  $\nabla_{\mathbf{\Sigma}_q} \bar{f}_q$  and  $\nabla_{\mathbf{W}_q} \bar{f}_q$  are given in (3.21). Therefore, the system of inequalities indicated as  $VI(F^{\mathbb{C}}, \mathcal{K})$  can be established according to (3.25), where  $\mathcal{K} = \prod_{q=1}^Q \mathcal{F}_q$ . Furthermore, for a given response  $\mathbf{\Sigma}_q$  and  $\mathbf{W}_q$ , the solutions of  $\{\mathbf{S}_{q,k}\}_{k=0}^K$  are uniquely determined by (3.11b) and (3.11c) for all  $q$ . Hence, from now on, we assume that the values of  $\{\mathbf{S}_{q,k}\}_{k=0}^K$  are already plugged into  $F_q^{\mathbb{C}}(\mathbf{\Sigma}_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K)$ , so we drop the term  $\{\mathbf{S}_{q,k}\}_{k=0}^K$  in the subsequent equations for notational convenience.

In order to show that K.K.T conditions are valid necessary conditions for a stationary solution of (3.13), an appropriate CQ must hold [93]. We use the Slater's CQ [93] as the strategy set of each player is a convex set. Moreover, at NE (if it exists) all of the players use their best responses, i.e., each player has found the optimal solution to his optimization problem and will not deviate from that. Since the optimal solution for each player also satisfies the K.K.T conditions, then NE must be a QNE [83]. In fact, the set of QNEs includes the NE.

#### 3.4.4 Existence and Uniqueness of the QNE

To begin our analysis in this part, we consider the VI described by (3.25), (3.33), and (3.34) again. In the case of the domain of  $\mathbf{Z}$  being square complex matrices, the definition of VI in complex domain can be further simplified to achieve the same form of VI in the real case (i.e., (3.22)). More specifically, let  $F^{\mathbb{C}}$  be a  $2N \times N$  matrix and let  $\text{vec}(F^{\mathbb{C}}) \triangleq [(F_1)^T, \dots, (F_N)^T]^T$  denote a  $2N^2 \times 1$  vector where  $F_i \triangleq [F^{\mathbb{C}}(\mathbf{Z})]_{:,i}$ ,  $i = 1, \dots, N$ ,



denotes the vector corresponding to the  $i$ th column of  $F^{\mathbb{C}}(\mathbf{Z})$ . Furthermore, let  $\text{vec}(\mathbf{Z}) = [[\mathbf{Z}]_{:,1}^T, \dots, [\mathbf{Z}]_{:,N}^T]^T$  be the vector version of the complex matrix  $\mathbf{Z}$ . Hence, the vector version of the VI in complex domain can be expressed as

$$(\text{vec}(\mathbf{Z}) - \text{vec}(\mathbf{Y}))^H \text{vec}(F^{\mathbb{C}}(\mathbf{Y})) \geq 0, \forall \mathbf{Z} \in \mathcal{K}. \quad (3.35)$$

In order to further simplify the VI in complex domain to be completely identical to the real case, we define  $F^{\mathbb{R}} \triangleq [\text{Re}\{\text{vec}(F^{\mathbb{C}})\}^T, \text{Im}\{\text{vec}(F^{\mathbb{C}})\}^T]^T$  and  $\mathbf{Z}^{\mathbb{R}} \triangleq [\text{Re}\{\text{vec}(\mathbf{Z})\}^T, \text{Im}\{\text{vec}(\mathbf{Z})\}^T]^T$  where  $\text{Re}\{\dots\}$  and  $\text{Im}\{\dots\}$  are the real and imaginary parts, respectively. Therefore, the real-vectorized representation of (3.25) can be written as

$$(\mathbf{Z}^{\mathbb{R}} - \mathbf{Y}^{\mathbb{R}})^T (F^{\mathbb{R}}(\mathbf{Y}^{\mathbb{R}})) \geq 0, \forall \mathbf{Z}^{\mathbb{R}} \in \mathcal{K}^{\mathbb{R}}, \text{ where } \mathcal{K}^{\mathbb{R}} \subseteq \mathbb{R}^{2N^2}. \quad (3.36)$$

The vector form of (3.33) and (3.34) are as follows:

$$\text{vec}(\mathbf{Z}) = [\text{vec}(\bar{\mathbf{\Sigma}})^T, \text{vec}(\bar{\mathbf{W}})^T]^T = \{[\text{vec}(\bar{\mathbf{\Sigma}}_q)^T, \text{vec}(\bar{\mathbf{W}}_q)^T]^T\}_{q=1}^Q \quad (3.37)$$

$$\text{vec}(F^{\mathbb{C}}(\mathbf{Z})) = \left\{ [\text{vec}(-\nabla_{\mathbf{\Sigma}_q} \bar{f}_q)^T, \text{vec}(-\nabla_{\mathbf{W}_q} \bar{f}_q)^T]^T \right\}_{q=1}^Q. \quad (3.38)$$

Hence, the vector form of the complex VI problem  $VI(F^{\mathbb{C}}, \mathcal{K})$  can be written as

$$([\text{vec}(\mathbf{\Sigma})^T, \text{vec}(\mathbf{W})^T]^T - [\text{vec}(\bar{\mathbf{\Sigma}})^T, \text{vec}(\bar{\mathbf{W}})^T]^T)^H \text{vec}(F^{\mathbb{C}}(\bar{\mathbf{\Sigma}}, \bar{\mathbf{W}})) \geq 0. \quad (3.39)$$

$$\left( [\mathbf{\Sigma}^{\mathbb{R}T}, \mathbf{W}^{\mathbb{R}T}] - [\bar{\mathbf{\Sigma}}^{\mathbb{R}T}, \bar{\mathbf{W}}^{\mathbb{R}T}] \right) F^{\mathbb{R}} \geq 0, \forall (\mathbf{\Sigma}^{\mathbb{R}}, \mathbf{W}^{\mathbb{R}}) \in \mathcal{K}^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}} \subseteq \mathbb{R}^m, \quad (3.40)$$

and the equivalent real-vectorized representation of the VI in (3.25) that complies with the definition in (3.22) can be determined as (3.40) where  $m \triangleq \sum_{q=1}^Q 2N_{T_q}^2$ . Note that the set of matrices  $(\Sigma_1, \dots, \Sigma_Q, \mathbf{W}_1, \dots, \mathbf{W}_Q)$  that are in  $\mathcal{K} = \prod_{q=1}^Q \mathcal{F}_q$  are the ones whose real-vectorized versions will be inside  $\mathcal{K}^{\mathbb{R}}$ . Now that the proposed smooth game is modeled as a real-vectorized VI, we can use the following theorem to prove the existence of the QNE.

**Theorem 4.** *The proposed smooth game, where the actions of each player is given by (3.15) admits at least one QNE.*

*Proof.* See Appendix A □

The uniqueness of the QNE is discussed in the following theorem:

**Theorem 5.** *The proposed smooth game characterized by (3.15) has a unique QNE if*

$$\lambda_{q,\min} > \sum_{\substack{q=1 \\ q \neq l}}^Q |||D_{Z_l} F_q^{\mathbb{C}}(Z_q)|||_2, \quad q \in \mathbb{Q} \quad (3.41)$$

where  $\lambda_{q,\min}$  is the smallest eigenvalue of  $D_{Z_q} F_q^{\mathbb{C}}(Z_q)$ , and  $D_{Z_l} F_q^{\mathbb{C}}(Z_q) \triangleq \frac{\partial \text{vec}(F_q^{\mathbb{C}}(Z_q))}{\partial \text{vec}(Z_l)^T}$ , for all  $q, l \in \mathbb{Q}^2$ , is defined as

$$D_{Z_l} F_q^{\mathbb{C}}(Z_q) \triangleq \begin{bmatrix} D_{\Sigma_l}(-\nabla_{\Sigma_q} \bar{f}_q) & D_{\mathbf{W}_l}(-\nabla_{\Sigma_q} \bar{f}_q) \\ D_{\Sigma_l}(-\nabla_{\mathbf{W}_q} \bar{f}_q) & D_{\mathbf{W}_l}(-\nabla_{\mathbf{W}_q} \bar{f}_q) \end{bmatrix}. \quad (3.42)$$

*Proof.* See Appendix A. □

### 3.5 Analysis of Proposed Game in the Presence of Multiple QNEs

#### 3.5.1 Convergence of Proposed Algorithm

The conditions for the uniqueness of QNE do not guarantee the convergence of Algorithm 1 to a (unique) QNE. Since the optimization of each player is non-convex, only stationary points of players' utilities could be achieved. Hence, solving each player's optimization problem using AO does not necessarily lead to the best response of each player. This hinders us from proving the convergence of Algorithm 1. However, we verified the convergence via simulations. In this section, we present a slightly modified algorithm, namely the gradient-response algorithm with proof of convergence. Furthermore, the gradient-response algorithm paves the way for further performance improvements introduced later in this chapter.

#### 3.5.2 The Gradient-Response Algorithm

A solution to the VI in (3.40) can be characterized by the following iteration [84, Chapter 12]:

$$x^{(i+1)} = \Pi_{\mathcal{K}^{\mathbb{R}}} \left( x^{(i)} - \gamma F^{\mathbb{R}}(x^{(i)}, \{S_{q,k}^{(i)}\}_{k=0}^K) \right) \quad (3.43)$$

where  $\Pi_{\mathcal{K}^{\mathbb{R}}}$  is the projection to set  $\mathcal{K}^{\mathbb{R}}$ ,  $x = [\Sigma^{\mathbb{R}^T}, \mathbf{W}^{\mathbb{R}^T}]^T$ , the superscript  $(i)$  is the number of iterations, and  $\gamma = \text{diag}([\gamma_1, \dots, \gamma_m]^T)$  is a diagonal matrix which indicates the step size that each player takes in the improving direction of his utility function. The

solutions to  $\{\mathbf{S}_{q,k}^{(i)}\}_{k=0}^K$  are as follows:

$$\mathbf{S}_{q,0}^{(i)} \triangleq (\mathbf{M}_q^{(i)})^{-1} = \left( \mathbf{I} + \mathbf{H}_{qq} \mathbf{W}_q^{(i)} \mathbf{H}_{qq}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{rq} \left( \boldsymbol{\Sigma}_r^{(i-1)} + \mathbf{W}_r^{(i-1)} \right) \mathbf{H}_{rq}^H \right)^{-1}, \quad (3.44a)$$

$$\mathbf{S}_{q,k \neq 0}^{(i)} \triangleq \left( \mathbf{M}_{e,q,k}^{(i)} + \mathbf{G}_{qk} \boldsymbol{\Sigma}_q^{(i)} \mathbf{G}_{qk}^H \right)^{-1} = \left( \mathbf{I} + \mathbf{G}_{qk} (\boldsymbol{\Sigma}_q^{(i)} + \mathbf{W}_q^{(i)}) \mathbf{G}_{qk}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{G}_{rk} \left( \boldsymbol{\Sigma}_r^{(i-1)} + \mathbf{W}_r^{(i-1)} \right) \mathbf{G}_{rk}^H \right)^{-1} \quad (3.44b)$$

where (3.44b) holds for  $k \neq 0$ . It is easy to confirm that the iteration in (3.43) is a simplified version of the projection done by each user in (3.18) and (3.19). Notice that the only difference of the gradient-response algorithm, characterized by iteration in (3.43), from Algorithm 1 is that at each round of the gradient-response algorithm, a player only does one iteration of the PG method (i.e., (3.18)) and one iteration according to (3.44). The real-vectorized version of the gradient-response algorithm is shown in (3.43). Since the values of  $\{\mathbf{S}_{q,k}^{(i)}\}_{k=0}^K$  are uniquely determined for a given  $x^{(i)}$ , we drop the term  $\{\mathbf{S}_{q,k}^{(i)}\}_{k=0}^K$  from the argument of  $F^{\mathbb{R}}$  for notational convenience.

Assuming that  $F^{\mathbb{R}}$  is *strongly monotone* (with modulus  $c_s/2$ )<sup>8</sup> and *Lipschitz continuous* (with constant  $L$ )<sup>9</sup> w.r.t  $(\boldsymbol{\Sigma}_q, \mathbf{W}_q)$ , the convergence to a unique solution follows if  $\gamma_{i'} = d < \frac{c_s}{L^2}$ ,  $\forall i' = 1, \dots, m$ , where  $d$  is constant. Hence, the mapping  $x \rightarrow \Pi_{\mathcal{K}^{\mathbb{R}}} (x - \gamma F^{\mathbb{R}}(x))$  becomes a contraction mapping and the fixed points of this map are solutions of the VI in (3.40) [84, Chapter 12]. It turns out that sufficient conditions for strong monotonicity of  $VI(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  are in fact the same as the conditions derived in (3.41) for the uniqueness of the QNE<sup>10</sup>. Therefore, based on (3.43), a pseudo-code of the gradient-response algorithm is given in Algorithm 2. Note that the operation in Line 6 of

<sup>8</sup>The notion of strong monotonicity is a basic definition in the topic of VI (see [91, Appendix A]).

<sup>9</sup>It can be seen from (3.18) and (3.19) that the power constraint of each user makes the variations of  $\nabla_{\boldsymbol{\Sigma}_q} \bar{f}_q$  and  $\nabla_{\mathbf{W}_q} \bar{f}_q$  bounded for all  $q \in \mathbb{Q}$ . Hence,  $F^{\mathbb{R}}$  is Lipschitz continuous on  $\mathcal{K}^{\mathbb{R}}$ .

<sup>10</sup>More explanation can be found in Appendix A.

Algorithm 2 is the same as the iteration in (3.43). In fact, since the set  $\mathcal{K}^{\mathbb{R}}$  is a Cartesian product of players' strategies, the iteration in (3.43) can be easily converted back to its matrix form to have the the following iteration for each link:

$$\begin{pmatrix} \Sigma_q^{(i+1)} \\ \mathbf{W}_q^{(i+1)} \end{pmatrix} = \text{Proj}_{\mathcal{F}_q} \begin{pmatrix} \Sigma_q^{(i)} + \gamma'_q \nabla_{\Sigma_q} \bar{f}_q(\Sigma_q^{(i)}, \mathbf{W}_q^{(i)}, \{\mathbf{S}_{q,k}^{(i)}\}_{k=0}^K) \\ \mathbf{W}_q^{(i)} + \gamma'_q \nabla_{\mathbf{W}_q} \bar{f}_q(\Sigma_q^{(i)}, \mathbf{W}_q^{(i)}, \{\mathbf{S}_{q,k}^{(i)}\}_{k=0}^K) \end{pmatrix}, \forall q \in \mathbb{Q}. \quad (3.45)$$

Notice that  $\gamma'_q$  is a diagonal matrix that can be obtained by dividing the matrix  $\gamma$  into  $Q$  block-diagonal matrices. That is, with a slight abuse of notations,  $\gamma = \text{diag}([\gamma_1, \dots, \gamma_m]^T) = \gamma' = \text{diag}(\gamma'_1, \dots, \gamma'_Q)$ ,  $Q < m$ . Therefore, the gradient response in (3.43) can be shown as an iteration that is done in each link, independent of other links. This is essentially a distributed implementation. The gradient-response algorithm is given in Algorithm 2.

---

**Algorithm 2** The Gradient-Response Algorithm

---

**Initialize:**  $\Sigma_q^{(1)}, \mathbf{W}_q^{(1)}, \text{Tr}(\Sigma_q^{(1)} + \mathbf{W}_q^{(1)}) < P_q, \forall q$

- 1: **repeat**    % superscript  $(i)$  indicates the iterations starting from here
  - 2:    Compute  $\mathbf{M}_q, \mathbf{M}_{e,q,k}, \forall (q, k) \in \mathbb{Q} \times \mathbb{K}$
  - 3:    Compute  $\mathbf{S}_{q,k}^{(i)}, \forall (q, k) \in \mathbb{Q} \times \mathbb{K}$
  - 4:    Compute  $\varphi_{e,q,k}(\Sigma_q^{(i)}, \mathbf{W}_q^{(i)}, \mathbf{S}_{q,k}^{(i)}), \forall (q, k) \in \mathbb{Q} \times \mathbb{K}$
  - 5:    **for**  $q=1, \dots, Q$  **do**
  - 6:        Compute  $(\Sigma_q^{(i+1)}, \mathbf{W}_q^{(i+1)})$  using (3.45)
  - 7:    **end for**
  - 8: **until** Convergence to QNE
- 

The convergence point of Algorithm 2 is a QNE of the game where players' actions are defined by (3.15). Specifically, assume that for  $i \rightarrow \infty$ , the convergence point is

denoted as  $(\bar{\Sigma}, \bar{\mathbf{W}})$ . Hence, we have for all  $q \in \mathbb{Q}$

$$\bar{\mathbf{S}}_{q,0} = \arg \max_{\mathbf{S}_{q,0} \succeq 0} \varphi_q(\bar{\Sigma}_q, \bar{\mathbf{W}}_q, \mathbf{S}_{q,0}) \quad (3.46a)$$

$$\bar{\mathbf{S}}_{q,k} = \arg \max_{\mathbf{S}_{q,k} \succeq 0} \varphi_{e,q,k}(\bar{\Sigma}_q, \bar{\mathbf{W}}_q, \mathbf{S}_{q,k}), \quad k \neq 0. \quad (3.46b)$$

The solution of (3.46a) and (3.46b) is the same as (3.44a) and (3.44b) for  $i \rightarrow \infty$ . By plugging the solutions of (3.46a) and (3.46b) in  $\nabla_{\Sigma_q} \bar{f}_q(\bar{\Sigma}_q, \bar{\mathbf{W}}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K)$  and  $\nabla_{\mathbf{W}_q} \bar{f}_q(\bar{\Sigma}_q, \bar{\mathbf{W}}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K)$ , the convergence point of Algorithm 2 is a QNE of the proposed game. Overall, by using the gradient-response algorithm, the uniqueness of the QNE and  $\gamma_{i'} = d < \frac{c_s}{L^2}$ ,  $\forall i' = 1, \dots, m$  directly suggest the convergence of the iteration in (3.43). Hence, a separate proof for the convergence of Algorithm 2 is not needed.

The iteration proposed in (3.43) has two major issues. First, the Lipschitz constant of  $F^{\mathbb{R}}(x)$  has to be known. Apart from being difficult to derive, the knowledge of Lipschitz constant requires a centralized computation. Second, the strong monotonicity of  $F^{\mathbb{R}}$  cannot be always guaranteed. In fact, the conditions derived in (3.41) are very dependent on the channel gains and network topology. Hence, in most typical network scenarios, the inequality in (3.41) cannot be satisfied. This means that in some situations, the game might have more than one QNE. Consequently, the convergence of Algorithm 2 is in jeopardy. However, on the condition that  $F^{\mathbb{R}}$  is *monotone*<sup>11</sup>, which is a weaker condition than strong monotonicity, the ability to choose between multiple QNEs is possible. This means that the users are able to select the QNE that satisfies a certain design criterion, thus guaranteeing convergence in the case of multiple QNEs. Moreover, depending on the design criterion, the performance of the resulting QNE in terms of the achieved secrecy sum-rate can be improved. To do this, we first review the regularization methods proposed for VIs.

---

<sup>11</sup>See [94] to recall the difference between monotonicity and strong monotonicity.

### 3.5.3 Tikhonov Regularization

The general idea of regularization techniques is to modify the players' utility functions such that the VI becomes strongly monotone (and hence easily solvable by using Algorithm 2), and the limit point of a sequence of solutions for the modified VI converges to some solution of the original VI. In Tikhonov regularization, the process of regularizing  $\text{VI}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  involves solving a sequence of VIs, where the following iteration is characterized for a given  $\epsilon$  [84, chapter 12]:

$$x^{(i+1)} = \Pi_{\mathcal{K}^{\mathbb{R}}} \left( x^{(i)} - \gamma^T (F^{\mathbb{R}}(x^{(i)}) + \epsilon x^{(i)}) \right). \quad (3.47)$$

The solution to (3.47) when  $i \rightarrow \infty$  is denoted as  $x(\epsilon)$ . Given that  $F^{\mathbb{R}}$  is monotone, solving a sequence of (strongly monotone)  $\text{VI}(F^{\mathbb{R}}(x) + \epsilon x, \mathcal{K}^{\mathbb{R}})$ 's while  $\epsilon \rightarrow 0$  has a limit point, (i.e.,  $\lim_{\epsilon \rightarrow 0} x(\epsilon)$  exists) and that limit point is equal to least-norm solution of the  $\text{VI}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  [84, Theorem 12.2.3].

### 3.5.4 QNE Selection Using Tikhonov Regularization

Generalizing the applicability of Tikhonov regularization, we are more interested in converging to the QNE that is more beneficial to the links. In our approach to QNE selection, we define benefit as when the selected QNE satisfies a particular design criterion. Let the set of solutions of  $\text{VI}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  be denoted as  $\text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$ . We want to select the NE that minimizes a strongly convex<sup>12</sup> function  $\Phi(x) : \mathcal{K}^{\mathbb{R}} \rightarrow \mathbb{R}$ . In fact, the QNE selection

---

<sup>12</sup>A strongly convex function is a function whose derivative is strongly monotone. We use the definitions of [94] to distinguish between different types of convexity.

satisfies the following design criterion<sup>13</sup>

$$\begin{aligned} & \text{minimize} \quad \Phi(x) \\ & \text{s.t.} \quad x \in \text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}}). \end{aligned} \tag{3.48}$$

The optimization in (3.48) is convex because the monotonicity of  $F^{\mathbb{R}}$  suggests that  $\text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  is a convex set [84, Chapter 2]. The unique point that solves problem (3.48), is the solution to  $\text{VI}(\nabla\Phi(x), \text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}}))$ . However, as there is no prior knowledge on  $\text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  (i.e., QNEs are not known), this optimization cannot be solved easily. To overcome this issue, we modify the function  $F^{\mathbb{R}}$  in  $\text{VI}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  to

$$F_{\epsilon}^{\mathbb{R}} \triangleq F^{\mathbb{R}} + \epsilon \nabla\Phi(x). \tag{3.49}$$

As the function  $\Phi(x)$  is a strongly convex function, its derivative w.r.t  $x$  is strongly monotone. Assuming that  $F^{\mathbb{R}}$  is monotone, then the function  $F_{\epsilon}^{\mathbb{R}}$  is strongly monotone and the solution to  $\text{VI}(F_{\epsilon}^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$ , namely  $x(\epsilon)$ , is unique for all values of  $\epsilon > 0$  (i.e., convergence to a QNE can be guaranteed). Note that the iteration used for QNE selection is the same as (3.47) with the difference that the multiplier of  $\epsilon$  in (3.47) is replaced by  $\nabla\Phi(x)$ . The following theorem shows the potential of using (3.49) in (3.43) for QNE selection:

**Theorem 6.** [84, pp. 1128 and Theorem 12.2.5] *Consider  $\text{VI}(F_{\epsilon}^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  with  $x(\epsilon)$  as its solution. Assume that  $\mathcal{K}^{\mathbb{R}}$  is closed and convex, and  $\text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  is non-empty. The following claims hold:*

- *The assumption that  $\mathcal{K}^{\mathbb{R}}$  is closed and convex together with the non-emptiness of  $\text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}})$  (i.e., the existence of the QNE, proved in Theorem 4) are necessary*

---

<sup>13</sup>The discussion on how we determine the function  $\Phi(x)$  will be tackled in Section 3.6.2.



and sufficient for  $x_\infty = \lim_{\epsilon \rightarrow 0} x(\epsilon)$  to exist.

- Assuming that  $F^\mathbb{R}$  is monotone<sup>14</sup>,  $x_\infty$  is the solution of  $VI(\nabla\Phi(x), SOL(F^\mathbb{R}, \mathcal{K}^\mathbb{R}))$ .

This means that a QNE among several QNEs can be selected.  $\square$

### 3.5.5 Guaranteeing Monotonicity of $F^\mathbb{R}$ in Tikhonov Regularization

Theorem 6 requires  $F^\mathbb{R}$  to be monotone to be applicable. However, the monotonicity of  $F^\mathbb{R}$ , as highlighted by Theorem 5, depends on many factors such as channels between different nodes in the network, meaning that it is not possible to always guarantee the monotonicity of  $F^\mathbb{R}$ . In order to guarantee the monotonicity, we add a strongly concave term to the utility of each player. Let this term be  $-\frac{\tau_q}{2} (\|\Sigma_q - Y_{\Sigma_q}\|_F^2 + \|\mathbf{W}_q - Y_{\mathbf{W}_q}\|_F^2)$  where  $\|\cdot\|_F$  indicates the Frobenius norm. Hence, the utility of each player defined in (3.15) will change to

$$\begin{aligned} & \underset{\Sigma_q, \mathbf{W}_q, \mathbf{S}_q}{\text{maximize}} \quad \bar{f}_q(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K) - \frac{\tau_q}{2} (\|\Sigma_q - Y_{\Sigma_q}\|_F^2 + \|\mathbf{W}_q - Y_{\mathbf{W}_q}\|_F^2), \\ & \text{s.t.} \quad (\Sigma_q, \mathbf{W}_q) \in \mathcal{F}_q, \mathbf{S}_k \succeq 0, q \in \mathbb{Q}, k \in \mathbb{K} \end{aligned} \quad (3.50)$$

where  $Y_{\Sigma_q}$  and  $Y_{\mathbf{W}_q}$  are complex constants and will be characterized later. With this modification on the utility of each player, a new VI problem,  $VI(F_\tau^\mathbb{R}, \mathcal{K}^\mathbb{R})$  is established where:

$$F_\tau^\mathbb{R}(x) = F^\mathbb{R}(x) + \tau(x - y) \quad (3.51)$$

where  $y$  is the vector that contains the vectorized versions of  $Y_{\Sigma_q}$  and  $Y_{\mathbf{W}_q}$ , and  $\tau = \text{diag}(\tau_1, \tau_2, \dots, \tau_m)$  is an  $m \times m$  diagonal matrix. This perturbation is also known as *proximal-point regularization method* [84, Chapter 12.3.2]. Recalling Definition 4 in

---

<sup>14</sup>Later on, we elaborate on the monotonicity assumption for  $F^\mathbb{R}$  (see Section 3.6.3).

Appendix A, the augmented Jacobian matrix of  $F_\tau^\mathbb{R}(x)$ , namely  $\mathcal{J}_\tau$ , is as follows

$$\mathcal{J}_\tau \triangleq \mathcal{J} + \tau I \quad (3.52)$$

where  $\mathcal{J}$  is the augmented Jacobian matrix of  $F^\mathbb{R}$  and  $I$  is the identity matrix. Considering the matrix  $\tau$  as a free parameter, we can choose a suitable value for each diagonal element of  $\tau$ , such that the matrix  $\mathcal{J}_\tau$  becomes a diagonally dominant matrix. In the following we exploit the diagonal dominance of  $\mathcal{J}_\tau$  to establish the monotonicity property of  $F_\tau^\mathbb{R}$ <sup>15</sup>.

Let  $D(d_i, [\mathcal{J}_\tau]_{ii})$ ,  $i = 1, \dots, m$  be the closed disc centered at  $[\mathcal{J}_\tau]_{ii}$  with radius  $d_i = \sum_{j \neq i} |[\mathcal{J}_\tau]_{ij}|$ , where  $[\cdot]_{ii}$  denotes the diagonal element and  $[\mathcal{J}_\tau]_{ii} = [\mathcal{J}]_{ii} + \tau_i$ . Using the Gerschgorin circle theorem [95], for all  $i = 1, \dots, m$ , every eigenvalue of  $\mathcal{J}_\tau$  is within at least one of the discs. We also know that for the function  $F_\tau^\mathbb{R}$ , in order to be monotone, the matrix  $\mathcal{J}_\tau$  has to be APSD (see Appendix A). Hence, provided that a suitable value for  $\tau_i$  is chosen for all  $i = 1, \dots, m$ , all the radii of the Gershgorin circles must be less than their respective diagonal elements, ensuring that  $\mathcal{J}_\tau$  remains APSD. Using this fact, the value for  $\tau_i$  that guarantees  $\mathcal{J}_\tau$  to be APSD is

$$\tau_i \geq d_i - \mathcal{J}_{ii}, \quad \forall i. \quad (3.53)$$

Therefore, using the condition (3.53) with equality, the matrix  $\mathcal{J}_\tau$  becomes an APSD matrix, and consequently,  $F_\tau^\mathbb{R}$  becomes monotone. Therefore, the Tikhonov regularization changes to solving the problem  $VI(F_{\tau,\epsilon}^\mathbb{R}, \mathcal{K}^\mathbb{R})$  where

$$F_{\tau,\epsilon}^\mathbb{R} \triangleq F^\mathbb{R}(x) + \tau(x - y) + \epsilon^{(j)} \nabla \Phi(x) \quad (3.54)$$

---

<sup>15</sup>Later as we proceed, we present the equivalent regularization for the complex version of  $F^\mathbb{R}$ , i.e.,  $F^\mathbb{C}$  as well.

Building upon the perturbation in (3.51), we can now use  $F_\tau^\mathbb{R}$  instead of  $F^\mathbb{R}$  in the original VI in (3.40) which makes us able to use Tikhonov regularization and perform equilibrium selection. One might argue that using  $F_\tau^\mathbb{R}$  instead of  $F^\mathbb{R}$  is actually creating a new game with different solutions. In the following we give a property that makes the use of  $F_\tau^\mathbb{R}$  reasonable. It can be easily seen that the perturbation  $F_\tau^\mathbb{R}$  does not change the fact that the NE in  $VI(F_\tau^\mathbb{R}, \mathcal{K}^\mathbb{R})$  still exists, i.e., the set  $\text{SOL}(F_\tau^\mathbb{R}, \mathcal{K}^\mathbb{R})$  is non-empty (see Theorem 11). Furthermore, the addition of a monotone term (i.e.,  $\tau(x - y)$ ) does not change the convexity of utilities to their actions. We set the vector  $y$  to be  $y = x(\epsilon^{(j-1)})$ , which means that while computing the  $j$ -th member of solutions of  $VI(F_{\tau,\epsilon}^\mathbb{R}, \mathcal{K}^\mathbb{R})$ , namely  $x(\epsilon^{(j)})$ , the vector  $y$  is the same as the solution found for  $VI(F_{\tau,\epsilon}^\mathbb{R}, \mathcal{K}^\mathbb{R})$  when  $\epsilon = \epsilon^{(j-1)}$ . Therefore, in the limit point where  $x_\infty \in \text{SOL}(F_\tau^\mathbb{R}, \mathcal{K}^\mathbb{R})$ , we have

$$\begin{aligned}
x_\infty \in \text{SOL}(F_\tau^\mathbb{R}, \mathcal{K}^\mathbb{R}) &\Rightarrow (x - x_\infty)F_\tau^\mathbb{R}(x_\infty) > 0 \\
&\Rightarrow (x - x_\infty) \left( F^\mathbb{R}(x_\infty) + \tau(x_\infty - x_\infty) \right) > 0 \\
&\Rightarrow x_\infty \in \text{SOL}(F^\mathbb{R}, \mathcal{K}^\mathbb{R}).
\end{aligned} \tag{3.55}$$

Hence, the term  $\tau(x_\infty - x_\infty)$  vanishes since the limit point is guaranteed to be reached.

### 3.5.6 Distributed Tikhonov Regularization

Tikhonov regularization (QNE selection) is done in two nested loops. In the inner loop, for a given  $\epsilon^{(j)}$ , the solution to  $VI(F_\epsilon^\mathbb{R}, \mathcal{K}^\mathbb{R})$  will be found from the iteration in (3.47) (where the multiplier of  $\epsilon$  is replaced with  $\nabla\Phi(x)$ ). In the outer loop, the next value of  $\epsilon^{(j)}$  will be chosen (according to a predefined sequence such that  $\lim_{j \rightarrow \infty} \epsilon^{(j)} = 0$ ) until the solution to  $VI(\nabla\Phi(x), \text{SOL}(F^\mathbb{R}, \mathcal{K}^\mathbb{R}))$  is reached (see Theorem 6).

Despite having the ability to select a specific QNE among multiple QNEs, QNE se-

lection requires heavy signaling and centralized computation because still the Lipschitz Continuity constant  $L$  and strong monotonicity modulus of  $F_\epsilon^\mathbb{R}(x)$  (or  $F_{\tau,\epsilon}^\mathbb{R}(x)$ ) must be known (see Section 3.5.2). In order to address these issues, we introduce another regularization method. In this regularization, a term  $\theta^{(i)}(x^{(i)} - x^{(i-1)})$  is added to the function  $F_{\tau,\epsilon}^\mathbb{R}(x)$  to build a function  $F_{\tau,\epsilon,\theta}^\mathbb{R}(x) \triangleq F_{\tau,\epsilon}^\mathbb{R}(x) + \theta^{(i)}(x^{(i)} - x^{(i-1)})$  where  $\theta^{(i)}$  is a diagonal matrix. Considering this modification, the following property can be used:

**Proposition 2.** *Let  $F_{\tau,\epsilon}^\mathbb{R}(x)$  be a strictly monotone and Lipschitz continuous mapping<sup>16</sup>;  $\max_{z \in \mathcal{K}^\mathbb{R}} \|x\| \leq C$ , and  $\max_{z \in \mathcal{K}^\mathbb{R}} \|F_{\tau,\epsilon}^\mathbb{R}\| \leq B$  where  $C$  and  $B$  are positive constants. Furthermore, suppose that for a given  $\epsilon^{(j)}$ , the solution to  $VI(F_{\tau,\epsilon}^\mathbb{R}, \mathcal{K}^\mathbb{R})$  is denoted as  $x(\epsilon^{(j)})$ . Let  $x^{(i)}$  denote the set of iterates defined by*

$$x^{(i+1)} = \Pi_{\mathcal{K}^\mathbb{R}} \left( x^{(i)} - \gamma^{(i)} \left( F^\mathbb{R}(x^{(i)}) + \tau(x^{(i)} - x(\epsilon^{(j-1)})) + \epsilon^{(j)} \nabla \Phi(x^{(i)}) + \theta^{(i)}(x^{(i)} - x^{(i-1)}) \right) \right) \quad (3.56)$$

where the step size matrix  $\gamma^{(i)}$  is changing with the iterations. Lastly, set  $\gamma^{(i)}\theta^{(i)} = c = \text{diag}([c_1, \dots, c_m])$  where  $c_{i'} \in (0, 1), \forall i' = 1, \dots, m$  is a constant, and let the following hold:

$$\sum_{i=1}^{\infty} \gamma^{(i)} = \infty, \quad \sum_{i=1}^{\infty} \left( \gamma^{(i)} \right)^2 < \infty, \quad \text{and} \quad \sum_{i=1}^{\infty} (\gamma_{\max}^{(i)} - \gamma_{\min}^{(i)}) < \infty. \quad (3.57)$$

where  $\gamma_{\max}^{(i)}$  and  $\gamma_{\min}^{(i)}$  are respectively the maximum and minimum diagonal elements of the matrix  $\gamma^{(i)}$ . Therefore, we have  $\lim_{i \rightarrow \infty} x^{(i)} = x(\epsilon^{(j)})$ .  $\square$

The proof of Proposition 2 can be found in [96, Proposition 3.4]. However, note that the assumption of strict monotonicity of  $F_{\tau,\epsilon}^\mathbb{R}(x)$  is immediately satisfied as  $F_{\tau,\epsilon}^\mathbb{R}(x)$  is already strongly monotone. The conditions  $\max_{z \in \mathcal{K}^\mathbb{R}} \|x\| \leq C$  and  $\max_{z \in \mathcal{K}^\mathbb{R}} \|F_{\tau,\epsilon}^\mathbb{R}\| \leq B$  can also be satisfied due to having power constraints on each link. According to [96, Proposition 3.4], the step size  $\gamma^{(i)}$  can be chosen as  $\gamma_{i'}^{(i)} = (i + \alpha_{i'})^{-\omega}$  where  $\alpha_{i'}$  is a positive integer for  $i' = 1, \dots, N$  and  $0 < \omega < 1$ . Hence, we can write

<sup>16</sup>Note that Lipschitz continuity of  $F_{\tau,\epsilon}^\mathbb{R}(x)$  requires both  $F^\mathbb{R}(x)$  and  $\nabla \Phi(x)$  to be Lipschitz continuous. Hence, the proposed choices for  $\Phi(x)$  in the next section are all Lipschitz continuous.

$$\gamma_{max}^{(i)} = (i + \alpha_{max})^{-\omega}, \quad \gamma_{min}^{(i)} = (i + \alpha_{min})^{-\omega}. \quad (3.58)$$

Note that in Proposition 2,  $\theta^{(i)}$  is already set to  $\theta^{(i)} = \frac{c}{\gamma^{(i)}}$ . Using Proposition 2, we can design a distributed transmit optimization algorithm without the knowledge of Lipschitz constant and strong monotonicity modulus of  $F_{\tau, \epsilon}^{\mathbb{R}}$ . The next section discusses the implementation of QNE selection using (3.56)<sup>17</sup>.

### 3.6 QNE Selection Algorithm

In this section we propose the QNE selection algorithm together with three possible choices for the design criterion (i.e.,  $\Phi(x)$ ). Each of these choices imposes a certain amount of signaling overhead as well as a certain amount of improvement on the performance of Algorithm 1 and Algorithm 2.

#### 3.6.1 Algorithm Description

The pseudo-code for the QNE selection algorithm is shown in Algorithm 3. As mentioned previously, it can be seen that the QNE selection algorithm is comprised of two nested loops: outer loop (i.e., line 1), and inner loop (i.e., line 3). In the outer loop the  $j$ th member of  $\epsilon^{(j)}$ 's is selected. In the inner loop, the game  $s$  played among the players, and the players update their strategies according to (3.56). The sequence  $\epsilon^{(j)}$  must be a decreasing sequence such that  $\lim_{j \rightarrow \infty} \epsilon^{(j)} = 0$ . The operation in line 10 of Algorithm 3

---

<sup>17</sup>Note that in all of the proposed algorithms throughout this chapter, it was assumed that at each round of the game, all of the players are maximizing the utilities. This update fashion is also known as Jacobi implementation. The feasibility of implementing the algorithms using other update fashions (e.g., Gauss-Seidel or Asynchronous) can be a subject of future research.

can be written as

$$\begin{pmatrix} \Sigma_q^{(i+1)} \\ \mathbf{W}_q^{(i+1)} \end{pmatrix} = \text{Proj}_{\mathcal{F}_q} \begin{pmatrix} \Sigma_q^{(i)} + \gamma'_q \left( \nabla_{\Sigma_q} \bar{f}_q + \tau_q \left( \Sigma_q^{(i)} - \Sigma_q(\epsilon^{(j-1)}) \right) + \epsilon^{(j)} \nabla_{\Sigma_q} \Phi(x^{(i)}) - \theta_q^{(i)} (\Sigma_q^{(i)} - \Sigma_q^{(i-1)}) \right) \\ \mathbf{W}_q^{(i)} + \gamma'_q \left( \nabla_{\mathbf{W}_q} \bar{f}_q + \tau_q \left( \mathbf{W}_q^{(i)} - \mathbf{W}_q(\epsilon^{(j-1)}) \right) + \epsilon^{(j)} \nabla_{\mathbf{W}_q} \Phi(x^{(i)}) - \theta_q^{(i)} (\mathbf{W}_q^{(i)} - \mathbf{W}_q^{(i-1)}) \right) \end{pmatrix}. \quad (3.59)$$

Notice that  $\theta_q^{(i)}$  is a diagonal matrix that can be obtained via dividing the matrix  $\theta^{(i)}$  into  $Q$  block-diagonal matrices. That is, (with a slight abuse of notations)  $\theta^{(i)} = \text{diag}(\theta_1^{(i)}, \dots, \theta_Q^{(i)})$ . In the next subsection, we specifically explain the terms  $\nabla_{\Sigma_q} \Phi(x)$  and  $\nabla_{\mathbf{W}_q} \Phi(x)$  in line 10, so that Algorithm 3 will be completely defined. Lastly, notice that all of our analysis on VI problems were under the assumption that every player is solving a minimization problem as his strategy. Hence, if maximization is the strategy of each player, the proximal terms in (3.59) appear as a negative values. Furthermore, the addition of  $\nabla_{\Sigma_q} \Phi(x)$  and  $\nabla_{\mathbf{W}_q} \Phi(x)$  means that  $\Phi(x)$  must be a strongly concave function of  $x$ .

---

**Algorithm 3** The QNE Selection Algorithm

---

**Initialize:**  $\Sigma_q^{(1)}, \mathbf{W}_q^{(1)}, \text{Tr}(\Sigma_q^{(1)} + \mathbf{W}_q^{(1)}) < P_q, \forall q$ , and  $j = 1$

- 1: **repeat**    % Outer loop: superscript  $(j)$  indicates the iterations starting from here
  - 2: Choose the  $j$ th member of the sequence  $\epsilon^{(j)}$
  - 3:    **repeat**    % Inner loop: superscript  $(i)$  indicates the iterations starting from here
  - 4:    Compute  $\mathbf{M}_q, \mathbf{M}_{e,q,k}, \forall (q, k) \in \mathbb{Q} \times \mathbb{K}$
  - 5:    Compute  $\mathbf{S}_{q,k}^{(i)}, \forall (q, k) \in \mathbb{Q} \times \mathbb{K}$
  - 6:    Compute  $\varphi_{e,q,k}(\Sigma_q^{(i)}, \mathbf{W}_q^{(i)}, \mathbf{S}_{q,k}^{(i)}), \forall (q, k) \in \mathbb{Q} \times \mathbb{K}$
  - 7:       **for**  $q = 1, \dots, Q$  **do**
  - 8:    Update the values of  $\tau_q$  for all  $q = 1, \dots, Q$  such that the inequality in (3.41) is satisfied
  - 9:       Replace  $\nabla_{\Sigma_q} \bar{f}_q$  with  $\nabla_{\Sigma_q} \bar{f}_q - \tau_q \left( \Sigma_q^{(i)} - \Sigma_q(\epsilon^{(j-1)}) \right) + \epsilon^{(j)} \nabla_{\Sigma_q} \Phi(x^{(i)}) - \theta_q^{(i)} \left( \Sigma_q^{(i)} - \Sigma_q^{(i-1)} \right)$
  - 10:       Replace  $\nabla_{\mathbf{W}_q} \bar{f}_q$  with  $\nabla_{\mathbf{W}_q} \bar{f}_q - \tau_q \left( \mathbf{W}_q^{(i)} - \mathbf{W}_q(\epsilon^{(j-1)}) \right) + \epsilon^{(j)} \nabla_{\mathbf{W}_q} \Phi(x^{(i)}) - \theta_q^{(i)} \left( \mathbf{W}_q^{(i)} - \mathbf{W}_q^{(i-1)} \right)$
  - 11:       Compute  $(\Sigma_q^{(i+1)}, \mathbf{W}_q^{(i+1)})$  using (3.59)
  - 12:       **end for**
  - 13:    **until** Convergence to QNE    %  $x(\epsilon^j)$  is found
  - 14:  $j = j+1$
  - 15: **until** Convergence to limit point of  $x(\epsilon^j)$ 's
- 

### 3.6.2 Criterion for QNE Selection

Assume that the derivatives of  $\Phi(x)$  are described as follows:

$$\nabla \Phi(x) \triangleq [\nabla_{\Sigma_1, \mathbf{W}_1}^{\mathbb{R}} \Phi(x)^T, \dots, \nabla_{\Sigma_Q, \mathbf{W}_Q}^{\mathbb{R}} \Phi(x)^T]^T, \quad (3.60a)$$

$$\nabla_{\Sigma_q, \mathbf{W}_q}^{\mathbb{R}} \Phi(x) \triangleq [\nabla_{\Sigma_q}^{\mathbb{R}} \Phi(x)^T, \nabla_{\mathbf{W}_q}^{\mathbb{R}} \Phi(x)^T]^T, \quad q \in \mathbb{Q}, \quad (3.60b)$$

$$\nabla_{\Sigma_q}^{\mathbb{R}} \Phi(x) \triangleq [\text{Re}\{\text{vec}(\nabla_{\Sigma_q} \Phi(x))\}^T, \text{Im}\{\text{vec}(\nabla_{\Sigma_q} \Phi(x))\}^T]^T, \quad (3.60c)$$

$$\nabla_{\mathbf{W}_q}^{\mathbb{R}} \Phi(x) \triangleq [\text{Re}\{\text{vec}(\nabla_{\mathbf{W}_q} \Phi(x))\}^T, \text{Im}\{\text{vec}(\nabla_{\mathbf{W}_q} \Phi(x))\}^T]^T. \quad (3.60d)$$

We are now ready to present the possible choices of the criterion function  $\Phi(x)$ :

### Maximizing the sum of information rates

We aim to select the QNE that maximizes the sum-rate of all links. Recalling the reformulated information rate (i.e.,  $\varphi_q(\Sigma_q, \mathbf{W}_q, \mathbf{S}_{q,k})$ ) in (3.10b),  $\Phi(x)$  can be described as (with  $q \in \mathbb{Q}$ ):

$$\nabla_{\Sigma_q} \Phi(x) = \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{qr}^H ((\mathbf{M}_r + \mathbf{H}_{rr} \Sigma_r \mathbf{H}_{rr}^H)^{-1} - \mathbf{S}_{r,0}) \mathbf{H}_{qr}, \quad (3.61a)$$

$$\nabla_{\mathbf{W}_q} \Phi(x) = \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{qr}^H ((\mathbf{M}_r + \mathbf{H}_{rr} \Sigma_r \mathbf{H}_{rr}^H)^{-1} - \mathbf{S}_{r,0}) \mathbf{H}_{qr}. \quad (3.61b)$$

Notice that although we wrote  $\Phi$  as a function of  $x$ , one can easily relate the vector  $x$  to the covariance matrices  $\{(\Sigma_q, \mathbf{W}_q)\}_{q=1}^Q$  using (3.60) and (3.43). Hence, the derivatives of  $\Phi(x)$  at the end of Algorithm 3 would be:

$$\nabla_{\Sigma_q} \Phi(x) = \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{qr}^H ((\mathbf{M}_r^* + \mathbf{H}_{rr} \Sigma_r^* \mathbf{H}_{rr})^{-1} - \mathbf{S}_{r,0}^*) \mathbf{H}_{qr} \quad (3.62a)$$

$$\nabla_{\mathbf{W}_q} \Phi(x) = \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{qr}^H ((\mathbf{M}_r^* + \mathbf{H}_{rr} \Sigma_r^* \mathbf{H}_{rr})^{-1} - \mathbf{S}_{r,0}^*) \mathbf{H}_{qr} \quad (3.62b)$$

where  $\mathbf{M}_r^* = \mathbf{I} + \mathbf{H}_{rr}(\mathbf{W}_r^*)\mathbf{H}_{rr}^H + \mathbf{H}_{qr}(\mathbf{W}_q^* + \Sigma_q^*)\mathbf{H}_{qr}^H + \sum_{\substack{l=1 \\ l \neq q, r}}^Q \mathbf{H}_{lr}(\Sigma_l^* + \mathbf{W}_l^*)\mathbf{H}_{lr}^H$ , with  $\Sigma_q^*$  and  $\mathbf{W}_q^*$  being the limit points of  $\Sigma_q$  and  $\mathbf{W}_q$ . Integrating (3.62a) w.r.t.  $\Sigma_q^*$  and integrating (3.62b) w.r.t.  $\mathbf{W}_q^*$ , we end up with  $\Phi(x) = \sum_{q=1}^Q \sum_{\substack{r=1 \\ r \neq q}}^Q \varphi_r(\Sigma_r, \mathbf{W}_r, \mathbf{S}_{r,0})$ . Hence, at the end of Algorithm 3, the QNE that is a stationary point of sum-rate of all links is selected, i.e., the point that is the unique solution of  $\text{VI}(\nabla \Phi(x), \text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}}))$ .

### Minimizing the received rates at Eves

We can describe  $\Phi(x)$  by (with  $q \in \mathbb{Q}$ )



$$\nabla_{\Sigma_q} \Phi(x) = \sum_{\substack{r=1 \\ r \neq q}}^Q \sum_{k=1}^K \rho_{r,k} \mathbf{G}_{rk}^H ((\mathbf{M}_{e,r,k})^{-1} - \mathbf{S}_{r,k}) \mathbf{G}_{rk} \quad (3.63a)$$

$$\nabla_{\mathbf{W}_q} \Phi(x) = \sum_{\substack{r=1 \\ r \neq q}}^Q \sum_{k=1}^K \rho_{r,k} \mathbf{G}_{rk}^H ((\mathbf{M}_{e,r,k})^{-1} - \mathbf{S}_{r,k}) \mathbf{G}_{rk} \quad (3.63b)$$

$$\mathbf{M}_{e,r,k} \triangleq \mathbf{I} + \mathbf{G}_{rk} \mathbf{W}_r \mathbf{G}_{rk}^H + \mathbf{G}_{qk} (\Sigma_q + \mathbf{W}_q) \mathbf{G}_{qk}^H + \sum_{\substack{l=1 \\ l \neq q,r}}^Q \mathbf{G}_{lk} (\Sigma_l + \mathbf{W}_l) \mathbf{G}_{lk}^H \quad (3.63c)$$

where the term  $\rho_{r,k}$  is defined in (3.72). Following the same reasoning used in the previous QNE selection, at the limit point of  $x(\epsilon^{(j)})$ , we end up with  $\Phi(x) = \sum_{q=1}^Q \sum_{\substack{r=1 \\ r \neq q}}^Q -\frac{1}{\beta} \ln(\sum_{k=1}^K \exp\{\beta \varphi_{e,r,k}(\Sigma_r, \mathbf{W}_r, \mathbf{S}_{r,k})\})$ , where  $\varphi_{e,r,k}(\Sigma_r, \mathbf{W}_r, \mathbf{S}_{r,k})$  is defined in (3.10c). Hence, the selected QNE guides the game to the stationary point of minimizing Eves' received rates, i.e., the point that is the unique solution of  $\text{VI}(\nabla \Phi(x), \text{SOL}(F^{\mathbb{R}}, \mathcal{K}^{\mathbb{R}}))$ .

### Maximizing the sum of secrecy rates

In this criterion, a simple addition of previous design criteria gives us another QNE selection method, in which the QNE that is a stationary point of secrecy sum-rate is selected.

#### 3.6.3 Signaling Overhead and Running Time

While the distributed implementation of our proposed algorithms is now complete (see (3.45) and (3.59)), we still need to make sure that the amount of coordination that each link has to do (to make each QNE selection method possible) is reasonably low. That is, we need to check how much (if any) information a link needs to know about other links' corresponding channels and transmission attributes (i.e., covariance matrices of information signal and TxFJ) in order to execute one iteration of each algorithm.

Algorithm 1 only requires each link to measure the interference at its receiver to perform the optimization in (3.15). By examining the iteration in (3.45) for each link, where  $\nabla_{\mathbf{\Sigma}_q} \bar{f}_q$  and  $\nabla_{\mathbf{W}_q} \bar{f}_q$  are given in (3.21), we can deduce that Algorithm 2 requires the same amount of coordination as Algorithm 1. The amount of coordination for Algorithm 3, however, depends on the choice of the function  $\Phi(x)$ . Here, we compare all of the flavors of Algorithm 3 in terms of how much signaling overhead they impose on the network.

If maximizing sum-rate is the criterion, from (3.61) it can be seen that during the computation of  $x(\epsilon^{(j)})$ , at each iteration, the  $q$ th link,  $q \in \mathbb{Q}$ , needs the values of received signal, noise-plus-interference, and  $\mathbf{S}_{r,0}$  ( $r \in \mathbb{Q}, r \neq q$ ) of other links. Furthermore, the cross-channel gains of the  $q$ th link with other (unintended) legitimate receivers (i.e.,  $\mathbf{H}_{qr}, \forall r \in \mathbb{Q}, r \neq q$ ) should also be available. Note that the cross-channel gains need not to be acquired multiple times at each iteration, as they are fixed throughout the coherence time of the channels<sup>18</sup>. If the  $r$ th receiver sends training signals to its corresponding transmitter, for (implicit) channel estimation,  $r \in \mathbb{Q}, r \neq q$ , the channel gains  $\mathbf{H}_{qr}$  can be estimated by the  $q$ th transmitter using channel reciprocity. Moreover, it should be noted that while the  $q$ th link,  $q = 1, \dots, Q$ , is using this criterion, it does not need to know any information about the channel gains between other links and Eves. This feature makes this design criterion more practical than other criteria, which require obtaining E-CSI (i.e.,  $\mathbf{G}_{rk}$  and  $\mathbf{S}_{r,k}, \forall r \neq q, \forall k$ ) of all other links.

For the case of passive Eves, it does not seem difficult to derive the responses (or gradients) while assuming the knowledge of only statistics of E-CSI. This can be done if in (3.16) we replace the term  $\varphi_{e,q,k}$  with  $E[\varphi_{e,q,k}]$  where the expectation is w.r.t  $G_{qk}, \forall q, k \in \mathbb{Q} \times \mathbb{K}$ . Note that including the expectation operator in the utilities, does not compromise the generality of any of the analyses done in previous sections. Despite general difficulties

---

<sup>18</sup>Note that all aforementioned algorithms must run during the coherence time of the channels.

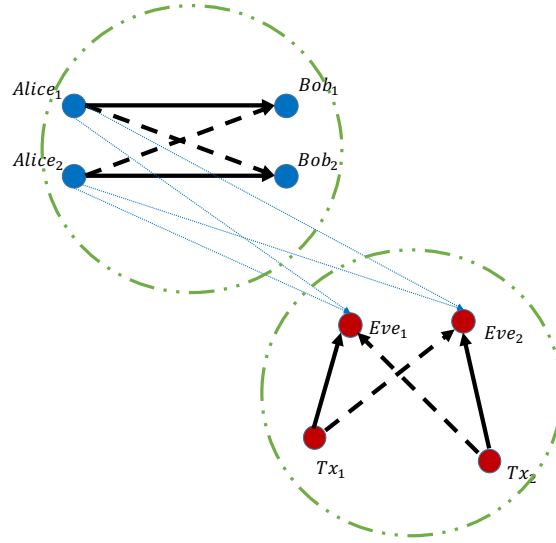


Figure 3.1: A (clustered) MANET where two clusters (indicated by green circle) of ad-hoc nodes are near each other.

in acquiring E-CSI, some applications can be considered as practical examples where the knowledge of E-CSI can be easily captured. One such example is mobile ad-hoc networks (MANETs) where the ad-hoc links of one cluster are interfering with one another, and can be considered as the legitimate links of our setup (See Figure 3.1). On the other hand, the receivers of another cluster may try to overhear the communications of the legitimate links in the nearby clusters. These receivers can be considered as the external eavesdroppers of our setup. The clustering may have been done to ease the routing process in the network. It is possible that the clustering algorithm requires the links to exchange their location, power, and (possibly) channel state information (CSI). Hence, provided that the coherence time of the channels are long enough, each link can maintain the CSI between itself and the links from another cluster. Hence, the E-CSI can be known to the links.

Another instance of our setup involves the downlink scenario of current cellular networks. Specifically, assume that the communication of the BS of a cell is interfering with other nearby cells. Each BS-user pair can be assumed as a legitimate link in our scenario.

We assume that no MU-MIMO technique is done in this scenario, so a BS is only communicating with one receiver (i.e., UE) at a given time. There might be other idle users in such network that are interested in overhearing the current communications. We can consider these idle users as the external eavesdroppers. It is possible that during the cell association phase, the idle users –which are now the external eavesdroppers– exchange their location information (using known packets) with all the nearby BSs to eventually select a cell for their respective communications. Hence, the BSs can extract the CSI between themselves and the external eavesdroppers and maintain it (till the end of one coherence time) for use in PHY-layer security optimizations.

The issue of knowledge of E-CSI has also been investigated in the recent literature. One example is when Eve is acting as a reactive jammer. That is, after some eavesdropping on the current transmissions, Eve injects her jamming signal to disrupt the ongoing communications. In such a case when jamming happens, assuming that the jamming signal of Eves are previously known, the E-CSI can be extracted by the legitimate links using channel reciprocity. Moreover, in [97], it was shown that in a massive MIMO scenario, a passive Eve cannot be very dangerous and must therefore be active and attack the training phase. This active attack can make Eve exposed, and hence the legitimate links can acquire some knowledge about E-CSI. Recently, the authors in [98] proposed a method with which the legitimate nodes can detect the passive eavesdropper from the local oscillator power leaked from its RF front end. Hence, an approximation on the location of Eve can be acquired. Lastly, in some scenarios where the legitimate nodes can detect the transmissions from Eves (e.g., active eavesdropping attacks), blind channel estimation techniques can be exploited to capture E-CSI [99, 100].

An interesting research question regarding the justification of signaling overhead is as follows: If a given algorithm requires each link to acquire its interfering channel gains,

then why not use a ZF-based solution to nullify the interference of a link on unintended (but legitimate) nodes? To answer this question, we first need to mention that the type of interference network that we consider in this chapter inherently assumes that an Alice-Bob pair consists of (most probably) nodes of the same specifications; that includes for example the number of antennas at each node, number of RF chains, etc. Hence, if an Alice wants to nullify her interference on unintended Bobs she must have more antennas than the total number of antennas of unintended Bobs, which may not be according to our aforementioned (implicit) assumption.

The possibility of using ZF-based solution would make sense in a multi-cell network where the cell-edge users are interfered by the transmissions of base stations of neighboring cells<sup>19</sup>. Such a scenario complies with an interference network model in which each Alice-Bob pair is a base station and its intended cell-edge (downlink) user. Now, it is possible to assume that each Alice has large number of antennas, so a ZF-based solution may be a good strategy. Studying this scenario can be a good subject of future research<sup>20</sup>.

Regarding the computation of the proximal term  $\tau_q$  as described by (3.53), through numerous simulations we found that regardless of the topology of the network and the channel gains, the value found for  $\tau_q$  is always a vary small value (i.e.,  $\tau_q < 10^{-4}$ ). This does not compromise the validity of inequality (3.53). However, in practice it seems that the transmit optimization game is always a monotone VI problem. The derivation of inequality (3.53) was done because of the fact that it is not that obvious to see the monotonicity of  $VI(F^{\mathbb{C}}, \mathcal{K})$ .

It is also interesting to understand how the choice of design criterion changes the running time of our proposed algorithm. To do this, we start from analyzing the computa-

---

<sup>19</sup>We focus on downlink scenario of multi-cell networks. The discussion for uplink communications can be easily drawn form that for downlink communications.

<sup>20</sup>More details on this potential future work are given in Chapter 7.

tional complexity of Algorithm 1 and extend it to the analysis of our proposed algorithms.

### Algorithm 1

In Line 2 of Algorithm 1, there is no need to compute every term of  $\mathbf{M}_q$  and  $\mathbf{M}_{e,q,k}$ ; that is, in measuring the interference, only the aggregate value is needed. Hence, the complexity of Line 2 is equivalent to the complexity of calculating the covariance matrix of the received interference. More specifically, at the receivers of legitimate links, the covariance matrix calculation of the  $N_{R_q} \times 1$  received interference vector (i.e.,  $\mathbf{M}_q$ ) yields a complexity of  $\mathcal{O}(N_{R_q}^2)$ . Similar computation is needed to obtain  $\mathbf{M}_{e,q,k}$ , which has the complexity of  $\mathcal{O}(\sum_{k=1}^K N_{e,k}^2)$ . Line 5 of Algorithm 1 involves a matrix inversion for  $\mathbf{S}_{q,0}$  and a matrix multiplication together with a matrix inversion for  $\{\mathbf{S}_{q,k}\}_{k=1}^K$ . The total complexity of this line is  $\mathcal{O}(\sum_{k=1}^K (N_{T_q} N_{e,k}^2 + N_{e,k} N_{T_q}^2 + N_{e,k}^3) + N_{R_q}^3)$ . Computation of the gradients in Line 8 requires the computation of  $\varphi_{e,q,k}$  for all  $k \in \mathbb{K}$  and  $(\mathbf{M}_q^{n,l} + \mathbf{H}_{qq} \Sigma_q \mathbf{H}_{qq}^H)^{-1}$ . Computation of  $\varphi_{e,q,k}$  for all  $k \in \mathbb{K}$  has the complexity of  $\mathcal{O}(\sum_{k=1}^K N_{T_q} N_{e,k}^2 + N_{e,k} N_{T_q}^2 + N_{e,k}^3)$  due to matrix multiplications and determinant calculations (see (3.10c)). The inverse of  $(\mathbf{M}_q^{n,l} + \mathbf{H}_{qq} \Sigma_q \mathbf{H}_{qq}^H)$  yields an additional complexity of  $\mathcal{O}(N_{R_q}^3 + N_{R_q}^2 N_{T_q} + N_{R_q} N_{T_q}^2)$ . Notice that in calculating  $\mathbf{M}_q^{n,l}$  and  $\mathbf{M}_{e,q,k}^{n,l}$  for all  $k \in \mathbb{K}$ , an additional computation for calculating  $\mathbf{H}_{qq} \mathbf{W}_q^{n,l} \mathbf{H}_{qq}^H$  and  $\mathbf{G}_{qk} \mathbf{W}_q^{n,l} \mathbf{G}_{qk}^H$  must be carried at each iteration of the PG method (i.e., Line 6 of Algorithm 1), which respectively have complexities of  $\mathcal{O}(N_{R_q}^2 N_{T_q} + N_{R_q} N_{T_q}^2)$  and  $\mathcal{O}(\sum_{k=1}^K N_{T_q} N_{e,k}^2 + N_{e,k} N_{T_q}^2)$ . The other computations that were not mentioned in gradient derivation are redundant and do not affect the general complexity. Apart from the gradient derivations, the Euclidean projection also has its own complexity. The projection in (3.20) requires eigenvalue decomposition, and thus has  $\mathcal{O}(N_{T_q}^3)$  complexity. Adding all of the aforementioned computations, the complexity of Algorithm 1 for each user  $q$  is  $\mathcal{O}\left(N_{R_q}^3 + N_{T_q}^3 + N_{R_q}^2 N_{T_q} + N_{R_q} N_{T_q}^2 + K(N_{T_q} N_{e,k}^2 + N_{e,k} N_{T_q}^2 + N_{e,k}^3)\right)$

or simply  $\mathcal{O}\left(N_{R_q}^3 + N_{T_q}^3 + KN_{e,k}^3\right)$ . Note that one might also multiply this complexity by the amount of iterations in the PG method and the AO process. Let the constants  $N_{PG}$  and  $N_{AO}$  denote the iterations taken in the PG method and AO process, respectively. Hence, the total complexity for each player  $q$  is<sup>21</sup>  $\mathcal{O}\left(N_{PG}N_{AO}\left(N_{R_q}^3 + N_{T_q}^3 + KN_{e,k}^3\right)\right)$ .

### Algorithm 2

This algorithm can also be handled with the same complexity as Algorithm 1 with the difference that the number of iterations in Algorithm 2 (i.e., repeating the loop at Line 1 of Algorithm 2) is more than Algorithm 1, and hence a slower algorithm compared to Algorithm 1. Let the convergence time of the loop in Line 1 of Algorithm 2 be  $N_{GR}$ . Thus, the total complexity of Algorithm 2 for each player  $q$  is  $\mathcal{O}\left(N_{GR}\left(N_{R_q}^3 + N_{T_q}^3 + KN_{e,k}^3\right)\right)$ .

### Algorithm 3

In this algorithm, some additional calculations are generally required. For the criterion of sum-rate maximization, the derivation of the gradients of  $\Phi(x)$  are shown in (3.61), which has the additional complexity of  $\mathcal{O}\left(\sum_{r=1}^Q N_{R_r}^3 + N_{R_r}^2 N_{T_r} + N_{R_r} N_{T_r}^2\right)$ . In the case of minimizing Eves' rates as the QNE selection method, according to (3.63), computing  $\Phi(x)$  would have the complexity of  $\mathcal{O}\left(\sum_{r=1}^Q \sum_{k=1}^K N_{T_r} N_{e,k}^2 + N_{e,k} N_{T_r}^2 + N_{e,k}^3\right)$ . The convergence time of Algorithm 3 is generally different from that of Algorithm 2 due to the presence of criterion function in Algorithm 3. Setting  $N_{QNE}$  as the convergence time of the loop in Line 1 of Algorithm 3, the total complexity of Algorithm 3 is obtained as follows:

- Under sum-rate maximization as the QNE selection method, for every player  $q$ , the

---

<sup>21</sup>Notice that this result only makes sense when the QNE is unique. Otherwise if QNE is not unique, Algorithm 2 might not even converge, taking the running time to infinity.

computational complexity is

$$\mathcal{O} \left( N_{QNE} N_{GR} \left( N_{T_q}^3 + Q(N_{R_q}^3 + N_{R_q}^2 N_{T_q} + N_{R_q} N_{T_q}^2) + K(N_{T_q} N_{e,k}^2 + N_{e,k} N_{T_q}^2 + N_{e,k}^3) \right) \right),$$

or simply

$$\mathcal{O} \left( N_{QNE} N_{GR} \left( N_{T_q}^3 + Q N_{R_q}^3 + K N_{e,k}^3 \right) \right). \quad (3.64)$$

- Under the minimization of Eves' rates as the QNE selection method, for every player  $q$ , the complexity is

$$\mathcal{O} \left( N_{QNE} N_{GR} \left( N_{T_q}^3 + N_{R_q}^3 + N_{R_q}^2 N_{T_q} + N_{R_q} N_{T_q}^2 + QK(N_{T_q} N_{e,k}^2 + N_{e,k} N_{T_q}^2 + N_{e,k}^3) \right) \right),$$

or simply

$$\mathcal{O} \left( N_{QNE} N_{GR} \left( N_{T_q}^3 + N_{R_q}^3 + QK N_{e,k}^3 \right) \right) \quad (3.65)$$

- Under the maximization of the secrecy sum-rate as the QNE selection method, for every player  $q$ , the complexity is

$$\mathcal{O} \left( N_{QNE} N_{GR} Q \left( N_{R_q}^3 + N_{T_q}^3 + N_{R_q}^2 N_{T_q} + N_{R_q} N_{T_q}^2 + K(N_{T_q} N_{e,k}^2 + N_{e,k} N_{T_q}^2 + N_{e,k}^3) \right) \right),$$

or simply

$$\mathcal{O} \left( N_{QNE} N_{GR} Q \left( N_{R_q}^3 + N_{T_q}^3 + K N_{e,k}^3 \right) \right) \quad (3.66)$$

We also computed the actual running time of our algorithm using MATLAB on a commercial PC with the following specifications:



- CPU: 2.4 GHz Intel Core i5.
- RAM: 8 GB 1333 MHz DDR3.
- OS: Mac OS X El Capitan v. 10.11.6.

We show the results in Figure 3.2 for one iteration of Algorithm 3 while using different criteria. Hence, in comparing these results with the theoretical derivations, one should skip the term  $N_{GR}$  and  $N_{QNE}$ . Each point in the presented curves is averaged over the number of iterations and also over 100 channel realizations of a given (random) network topology. The results in Figure 3.2 show that the running time of the QNE selection when secrecy sum-rate is the criterion (i.e., Alg. 3 (Secrecy sum-rate)) is relatively higher than the other two QNE selection methods. It can be seen in Figure 3.2 (a) that as the number of links grows, the difference in the computational complexity of Alg. 3 (Eves' rates) (i.e., QNE selection when minimizing Eves' rates is the criterion) and Alg. 3 (Secrecy sum-rate) appears to be in the slope of the curves, which complies with theoretical derivations in (3.65) and (3.66). However, this difference becomes clear when the number of links/antennas are high enough<sup>22</sup>. It can be seen from Figure 3.2 (b) that both Alg. 3 (Secrecy sum-rate) and Alg. 3 (Eves' rates) have the same slope. This can be seen in the theoretical derivation for the complexity of both QNE selection methods in (3.65) and (3.66), where for both criteria, the complexity w.r.t  $K$  is a multiple  $QN_{e,k}^3$ . For the case of Alg. 3 (Sum-rate) the complexity w.r.t  $K$  is only a multiple of  $N_{e,k}^3$ . The gap between the Alg. 3 (Secrecy sum-rate) and Alg. 3 (Eves' rates) in Figure 3.2 (b) is because of the additional complexity of Alg. 3 (Secrecy sum-rate), which is independent of the number Eves (i.e.,  $K$ ).

---

<sup>22</sup>Note that the theoretical derivations are derived for the worst case.

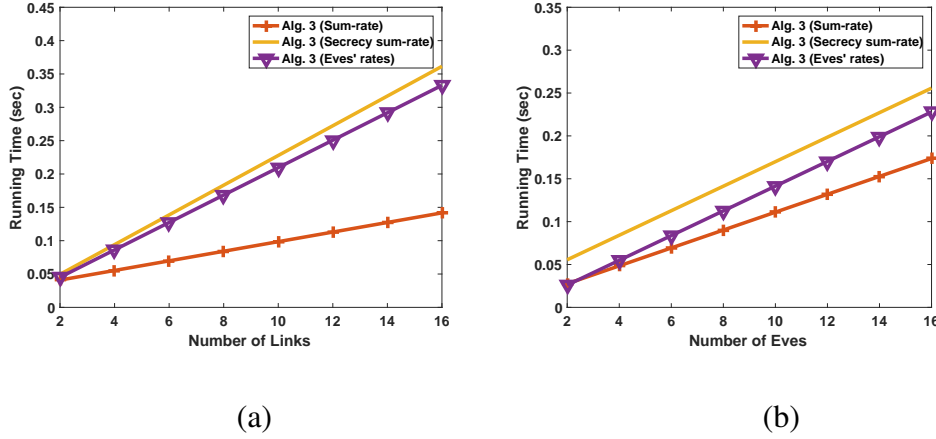


Figure 3.2: Comparison of the actual running time of the proposed algorithms vs. (a) number of links, (b) number of Eves ( $r_{circ} = 30$  m,  $K = 5$ ,  $N_{T_q} = 5$ ,  $N_{r_q} = 5 \forall q$ ,  $N_{e,k} = 5 \forall k$ ,  $d_{link} = 10$  m,  $P_q = 40$  dBm).

### 3.6.4 Effect of Initial Conditions

In general, the initial values for the covariance matrices of information and TxFJ signals can affect the results. Given the non-convexity of links' optimization problems, and the fact that at a QNE links operate at their stationary points, which are not necessarily unilaterally optimal, it is theoretically expected that different initial values can make the algorithm converge to different stationary points, thus affecting the final results. However, in our simulations, we did not see any significant variations in the secrecy sum-rate when the initial values of information and TxFJ covariance matrices are changed. For example, by changing the initial values, for networks with 10 to 16 links, a maximum difference of 3 nats/sec/Hz and maximum of 150 iterations until convergence were observed. The results can be seen in Figure 3.3, where the simulated convergence behavior of all three QNE selection methods is depicted for one channel realization. A point at the  $n$ th iteration of a curve represents the resulting secrecy sum-rate of that particular QNE selection method at the  $n$ th iteration, averaged over 100 random initial points. The corresponding

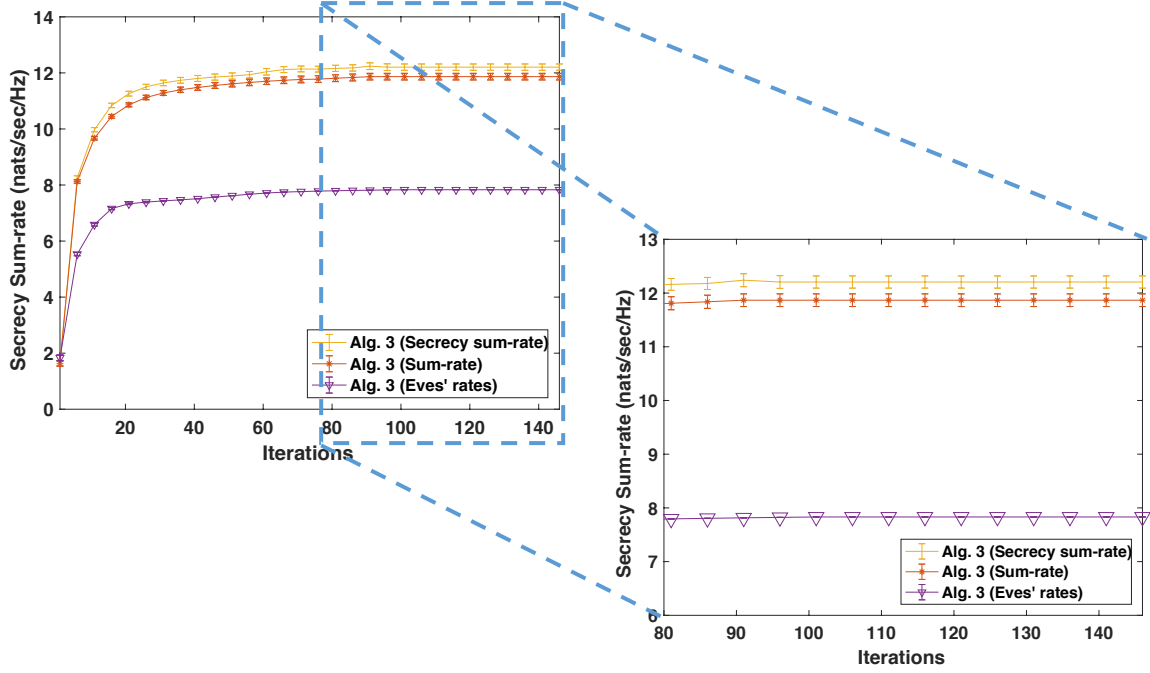


Figure 3.3: Comparison of convergence trend of the proposed QNE selection methods: (8 links ( $Q = 8$ ) and 7 Eves ( $K = 7$ ),  $r_{circ} = 30$  m,  $N_{T_q} = 5$ ,  $N_{r_q} = 2 \forall q$ ,  $N_{e,k} = 2 \forall k$ ,  $d_{link} = 10$  m,  $P_q = 40$  dBm).

95% confidence intervals are also shown. The tightness of the confidence intervals indicate that while the performance varies when the initial points change, this variation is negligible. Note that in all of our simulations, we considered random initializations for each channel realization of a given (random) network topology.

### 3.7 Centralized Precoder Design

So far, our efforts were in the direction that facilitated distributed implementation with minimum amount of signaling overhead. However, no discussion on the efficiency of the resulting QNEs has been given yet. In this section we discuss this issue and design a centralized algorithm that can be considered as a measure of efficiency in our game.

An appropriate measure of efficiency (i.e., social welfare) in our game would be the sum of utilities of all players or the secrecy sum-rate. Hence, the price of anarchy (PoA) can be defined as the ratio between the performance of the optimal centralized solution for the secrecy sum-rate maximization problem and the *worst* NE. However, such definition of PoA requires us to solve the secrecy sum-rate maximization problem, which is a non-convex problem. Moreover, as explained earlier, all of the proposed algorithms converge to the QNEs of the proposed game, which are not necessarily NEs. Hence, direct PoA analysis is not feasible.

To evaluate the goodness of QNEs, we propose a centralized algorithm that provides locally optimal solutions for the secrecy sum-rate maximization problem. We refer to this algorithm as Centralized Secrecy Sum-rate Maximization method (CSSM). We used the objective value of the solutions found via the CSSM as the social welfare or measure of efficiency in our game. In the following, a summary of the CSSM method is given.

In CSSM, the objective is to find a stationary solution for the following optimization problem:

$$\underset{(\mathbf{\Sigma}_q, \mathbf{W}_q) \in \mathcal{F}_q, \forall q}{\text{maximize}} \sum_{q=1}^Q \bar{R}_{s,q}(\mathbf{\Sigma}_q, \mathbf{W}_q). \quad (3.67)$$

Using the reformulation techniques given in Section 3, the secrecy sum-rate maximization problem in (3.67) can be rewritten as

$$\begin{aligned} & \underset{\substack{(\mathbf{\Sigma}_q, \mathbf{W}_q, \mathbf{S}_{q,k}) \\ \forall q,k}}{\text{maximize}} \sum_{q=1}^Q \bar{f}_q(\mathbf{\Sigma}_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}\}_{k=0}^K) \\ & \text{s.t. } (\mathbf{\Sigma}_q, \mathbf{W}_q) \in \mathcal{F}_q, \forall q \in \mathbb{Q}, \\ & \mathbf{S}_{q,k} \succeq 0, \forall (q,k) \in \mathbb{Q} \times \{0\} \cup \mathbb{K}. \end{aligned} \quad (3.68)$$

The problem in (3.68) can be shown to be convex w.r.t either  $[\mathbf{\Sigma}, \mathbf{W}] = \{\mathbf{\Sigma}_q, \mathbf{W}_q\}_{q=1}^Q = [[\mathbf{\Sigma}_1, \mathbf{W}_1]^T, \dots, [\mathbf{\Sigma}_Q, \mathbf{W}_Q]^T]$  or  $\mathbf{S} = \{\mathbf{S}_{q,k}\}_{\forall q,k} = [\mathbf{S}_{1,0}, \dots, \mathbf{S}_{1,K}, \mathbf{S}_{2,0}, \dots, \mathbf{S}_{2,K}, \dots, \mathbf{S}_{Q,K}]^T$ . Hence, a stationary point that satisfies the K.K.T optimality conditions of (3.67) can be found by solving (3.68) sequentially w.r.t.  $[\mathbf{\Sigma}, \mathbf{W}]$  and  $\mathbf{S}$ . That is, in one iteration, problem (3.68) is solved w.r.t. only  $\mathbf{S}$  to find an optimal solution  $\mathbf{S}^*$ . Next, with  $\mathbf{S}^*$  plugged in the objective of (3.68), problem (3.68) can be optimized w.r.t.  $[\mathbf{\Sigma}, \mathbf{W}]$  to find an optimal solution  $[\mathbf{\Sigma}^*, \mathbf{W}^*] = \{\mathbf{\Sigma}_q^*, \mathbf{W}_q^*\}_{q=1}^Q$ . This Alternating Optimization (AO) cycle continues until reaching a convergence point. It can be seen that problem (3.68) is separable w.r.t. every element of  $\mathbf{S}$ . Hence, the elements of  $\mathbf{S}^*$  can be written as

$$\mathbf{S}_{q,0}^* \triangleq \arg \max_{\mathbf{S}_{q,0} \succeq 0} \sum_{q=1}^Q \bar{f}_q(\mathbf{\Sigma}_q, \mathbf{W}_q, \mathbf{S}_{q,k}) = (\mathbf{M}_q)^{-1} \quad (3.69a)$$

$$= \left( \mathbf{I} + \mathbf{H}_{qq} \mathbf{W}_q \mathbf{H}_{qq}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_{rq} (\mathbf{\Sigma}_r + \mathbf{W}_r) \mathbf{H}_{rq}^H \right)^{-1} \quad (3.69b)$$

$$\mathbf{S}_{q,k}^* \triangleq \arg \max_{\mathbf{S}_{q,k} \succeq 0} \sum_{q=1}^Q \bar{f}_q(\mathbf{\Sigma}_q, \mathbf{W}_q, \mathbf{S}_{q,k}) = (\mathbf{M}_{e,q,k}^n + \mathbf{G}_{qk} \mathbf{\Sigma}_q \mathbf{G}_{qk}^H)^{-1} \quad (3.69c)$$

$$= \left( \mathbf{I} + \mathbf{G}_{qk} (\mathbf{\Sigma}_q + \mathbf{W}_q) \mathbf{G}_{qk}^H + \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{G}_{rk} (\mathbf{\Sigma}_r + \mathbf{W}_r) \mathbf{G}_{rk}^H \right)^{-1}, \quad k \neq 0. \quad (3.69d)$$

Now, while  $\mathbf{S}^*$  is plugged in the objective of (3.68), we can solve (3.68) w.r.t  $[\mathbf{\Sigma}, \mathbf{W}]$ . We use the augmented Lagrangian multiplier method [101] to derive a centralized solution for  $[\mathbf{\Sigma}^*, \mathbf{W}^*]$ . Let  $\mathbf{c}_q = \text{Tr}(\mathbf{\Sigma}_q + \mathbf{W}_q) - P_q < 0$ . The augmented Lagrangian of (3.68) can

be written as [101]<sup>23</sup>

$$L(\mathbf{\Sigma}, \mathbf{W}, \mathbf{a}, \mathbf{p}, \mathbf{S}^*) = - \sum_{q=1}^Q \bar{f}_q(\mathbf{\Sigma}_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}^*\}_{k=0}^K) + \frac{1}{2\mathbf{p}} \sum_{q=1}^Q \{(\max\{\mathbf{a}_q + \mathbf{p}\mathbf{c}_q, 0\})^2 + \mathbf{a}_q^2\} \quad (3.70)$$

where  $\mathbf{p}$  is a positive penalty (to prevent violating the constraints) and  $\mathbf{a}_q$ ,  $q = 1, \dots, Q$ , are the non-negative Lagrange multipliers. At a stationary point, the following equalities hold for all  $q \in \mathbb{Q}$ :

$$\begin{aligned} \frac{\partial}{\partial \mathbf{\Sigma}_q} L(\mathbf{\Sigma}, \mathbf{W}, \mathbf{a}, \mathbf{p}, \mathbf{S}^*) = \\ - \sum_{r=1}^Q \frac{\partial}{\partial \mathbf{\Sigma}_q} \bar{f}_r(\mathbf{\Sigma}_r, \mathbf{W}_r, \{\mathbf{S}_{r,k}^*\}_{k=0}^K) + \frac{1}{2\mathbf{p}} \sum_{r=1}^Q \frac{\partial}{\partial \mathbf{\Sigma}_q} (\max\{\mathbf{a}_r + \mathbf{p}\mathbf{c}_r, 0\})^2 = 0 \end{aligned} \quad (3.71a)$$

$$\begin{aligned} \frac{\partial}{\partial \mathbf{W}_q} L(\mathbf{\Sigma}, \mathbf{W}, \mathbf{a}, \mathbf{p}, \mathbf{S}^*) = \\ - \sum_{r=1}^Q \frac{\partial}{\partial \mathbf{W}_q} \bar{f}_r(\mathbf{\Sigma}_r, \mathbf{W}_r, \{\mathbf{S}_{r,k}^*\}_{k=0}^K) + \frac{1}{2\mathbf{p}} \sum_{r=1}^Q \frac{\partial}{\partial \mathbf{W}_q} (\max\{\mathbf{a}_r + \mathbf{p}\mathbf{c}_r, 0\})^2 = 0 \end{aligned} \quad (3.71b)$$

where

$$\frac{\partial}{\partial \mathbf{\Sigma}_q} \bar{f}_r(\mathbf{\Sigma}_r, \mathbf{W}_r, \{\mathbf{S}_{r,k}^*\}_{k=0}^K) = \begin{cases} \mathbf{H}_{qq}^H (\mathbf{M}_q + \mathbf{H}_{qq} \mathbf{\Sigma}_q \mathbf{H}_{qq}^H)^{-1} \mathbf{H}_{qq} - \sum_{k=1}^K \rho_{q,k} \mathbf{G}_{q,k}^H \mathbf{S}_{q,k}^* \mathbf{G}_{q,k}, & r = q, \\ \mathbf{H}_{qr}^H ((\mathbf{M}_r + \mathbf{H}_{rr} \mathbf{\Sigma}_r \mathbf{H}_{rr}^H)^{-1} - \mathbf{S}_{r,0}^*) \mathbf{H}_{qr} + \\ \sum_{k=1}^K \rho_{r,k} \mathbf{G}_{rk}^H ((\mathbf{M}_{e,r,k})^{-1} - \mathbf{S}_{r,k}^*) \mathbf{G}_{rk}, & r \neq q \end{cases}$$

with

$$\rho_{q,k} = \frac{e^{\beta \varphi_{e,q,k}(\mathbf{\Sigma}_q, \mathbf{W}_q, \mathbf{S}_{q,k}^*)}}{\sum_{j=1}^K e^{\beta \varphi_{e,q,j}(\mathbf{\Sigma}_q, \mathbf{W}_q, \mathbf{S}_{q,j}^*)}}. \quad (3.72)$$

---

<sup>23</sup>We converted the problem in (3.68) to a minimization problem by considering the negative of the objective function.

Note that the second term in the RHS of (3.71a) is a continuously differentiable function w.r.t  $\Sigma_q$  when  $r = q$  [101, pp. 397]. Thus,

$$\frac{\partial}{\partial \Sigma_q} (\max\{\mathbf{a}_r + \mathbf{p}\mathbf{c}_r, 0\})^2 = \begin{cases} 2\mathbf{p}(\mathbf{a}_q + \mathbf{p}\mathbf{c}_q)\Sigma_q & , \quad r = q \text{ \& } \mathbf{a}_q + \mathbf{p}\mathbf{c}_q > 0 \\ 0 & , \quad \text{otherwise.} \end{cases} \quad (3.73)$$

Furthermore, the terms in (3.71b) are described as follows:

$$\frac{\partial}{\partial \mathbf{W}_q} \bar{f}_r(\Sigma_r, \mathbf{W}_r, \{\mathbf{S}_{r,k}^*\}_{k=0}^K) = \begin{cases} \mathbf{H}_{qq}^H ((\mathbf{M}_q + \mathbf{H}_{qq}\Sigma_q\mathbf{H}_{qq})^{-1} - \mathbf{S}_{q,0}^*) \mathbf{H}_{qq} + \\ \sum_{k=1}^K \rho_{q,k} \mathbf{G}_{qk}^H ((\mathbf{M}_{e,q,k})^{-1} - \mathbf{S}_{q,k}^*) \mathbf{G}_{qk}, \quad r = q, \\ \mathbf{H}_{qr}^H ((\mathbf{M}_r + \mathbf{H}_{rr}\Sigma_r\mathbf{H}_{rr})^{-1} - \mathbf{S}_{r,0}^*) \mathbf{H}_{qr} + \\ \sum_{k=1}^K \rho_{r,k} \mathbf{G}_{rk}^H ((\mathbf{M}_{e,r,k})^{-1} - \mathbf{S}_{r,k}^*) \mathbf{G}_{rk}, \quad r \neq q, \end{cases} \quad (3.74)$$

and

$$\frac{\partial}{\partial \mathbf{W}_q} (\max\{\mathbf{a}_r + \mathbf{p}\mathbf{c}_r, 0\})^2 = \begin{cases} 2\mathbf{p}(\mathbf{a}_q + \mathbf{p}\mathbf{c}_q)\mathbf{W}_q & , \quad r = q \text{ \& } \mathbf{a}_q + \mathbf{p}\mathbf{c}_q > 0 \\ 0 & , \quad \text{otherwise.} \end{cases} \quad (3.75)$$

To satisfy the conditions in (3.71), we used gradient descent with a line search satisfying Armijo rule. The details of the centralized algorithm is presented in Algorithm 4. The centralized nature of Algorithm 4 can be seen in Line 12, where the equalities in (3.71) are checked for all  $q \in \mathbb{Q}$  and Line 11, where the Armijo rule is applied. The convergence of this algorithm can be proved by extending the proof of [102, Corollary 2], which is skipped here for the sake of brevity. Note that Algorithm CSSM is sensitive to the initial values of  $[\Sigma, \mathbf{W}]$ . Thus, we simulated this algorithm with random initializations and averaged its performance over the total number of initializations.

---

**Algorithm 4** The Centralized Secrecy Sum-rate Maximization Algorithm
 

---

**Initialize:**  $\Sigma_q^{(1)}, \mathbf{W}_q^{(1)}, \text{Tr}(\Sigma_q^{(1)} + \mathbf{W}_q^{(1)}) < P_q, \forall q, i = 0$

- 1: **repeat**  $i = i + 1$     % superscript ( $i$ ) indicates the iterations starting from here
- 2: Compute  $\mathbf{S}_{q,k}^{(i)}, \forall (q, k) \in \mathbb{Q} \times \mathbb{K}, \mathbf{p} = 1, \mathbf{a}_q = 0, \forall q$ , and  $s_t$  (Armijo step size)
- 3:    **repeat**    Set  $m = 1$
- 4:        **repeat**    Set  $n = 1$     % superscript ( $m$ ) indicates the iterations starting from here
- 5:        Set  $[d_{\Sigma_q}, d_{\mathbf{W}_q}]^T = -[\frac{\partial}{\partial \Sigma_q} L^{(m)T}, \frac{\partial}{\partial \mathbf{W}_q} L^{(m)T}]^T, \forall q \Rightarrow d = \{d_{\Sigma_q}, d_{\mathbf{W}_q}\}_{q=1}^Q$
- 6:        Set  $[\hat{\Sigma}, \hat{\mathbf{W}}] = [\Sigma^{(m)}, \mathbf{W}^{(m)}] + \mathbf{d}$
- 7:        Set  $[\Sigma^{(m+1)}, \mathbf{W}^{(m+1)}] = [\Sigma^{(m)}, \mathbf{W}^{(m)}] + \mathbf{s}_t^n([\hat{\Sigma}, \hat{\mathbf{W}}] - [\Sigma^{(m)}, \mathbf{W}^{(m)}])$
- 8:        **repeat**    % superscript ( $n$ ) indicates the iterations starting from here
- 9:         $s_t^{n+1} = s_t(s_t^n)$
- 10:        Set  $[\Sigma^{(m+1)}, \mathbf{W}^{(m+1)}] = [\Sigma^{(m)}, \mathbf{W}^{(m)}] + \mathbf{s}_t^{n+1}([\hat{\Sigma}, \hat{\mathbf{W}}] - [\Sigma^{(m)}, \mathbf{W}^{(m)}])$
- 11:        **until**     $L(\Sigma^{(m+1)}, \mathbf{W}^{(m+1)}, \mathbf{a}^{(m+1)}, \mathbf{p}, \mathbf{S}^{(i)}) < L(\Sigma^{(m)}, \mathbf{W}^{(m)}, \mathbf{a}^{(m)}, \mathbf{p}, \mathbf{S}^{(i)}) + s_t^n d^T \{\frac{\partial}{\partial \Sigma_q} L^{(m)}, \frac{\partial}{\partial \mathbf{W}_q} L^{(m)}\}_{q=1}^Q$
- 12:        **until**     $\frac{\partial}{\partial \Sigma_q} L = \frac{\partial}{\partial \mathbf{W}_q} L = 0, \forall q$
- 13:         $\mathbf{a}_q = \max\{\mathbf{a}_q + p\mathbf{c}_q, 0\}$
- 14:         $\mathbf{p} = \mathbf{p} \times u$     %  $u \geq 1$  increase the penalty.
- 15:        **until**     $\max\{\mathbf{c}_1, \dots, \mathbf{c}_q\} \leq 0$
- 16: **until** Convergence of  $L(\Sigma, \mathbf{W}, \mathbf{a}, \mathbf{p}, \mathbf{S})$

---

### 3.8 Simulation Results and Discussion

In this section, we simulate and compare all the algorithms presented so far. In these simulations, we set the noise power to 0 dBm.  $Q$  links as well as  $K$  Eves are randomly placed in a circle, namely the simulation region, with radius  $r_{\text{circ}}$ . The distance between the transmitter and the receiver of each link is set to be a constant  $d_{\text{link}} = 10$  m. The path-loss exponent is set to 2.5. For all simulated algorithms,  $\beta = 5$  (see (3.12)) and the termination criterion is set to when the normalized relative difference in each link's secrecy rate for two consecutive iterations is less than  $10^{-3}$ . For the QNE selection algorithms, we set their parameters as follows: The step size matrix (i.e.,  $\gamma'$ ) is set such that  $\gamma_j'^{(i)} = \gamma_0 i^{(-0.6)}, j = 1, \dots, m$ , where  $\gamma_0$  is a positive constant<sup>24</sup>,  $c = 0.08I_{m \times m}$ , and

---

<sup>24</sup>We found out that setting the maximum value of  $\gamma_0 = 20000$  brings the best performance for our algorithms.



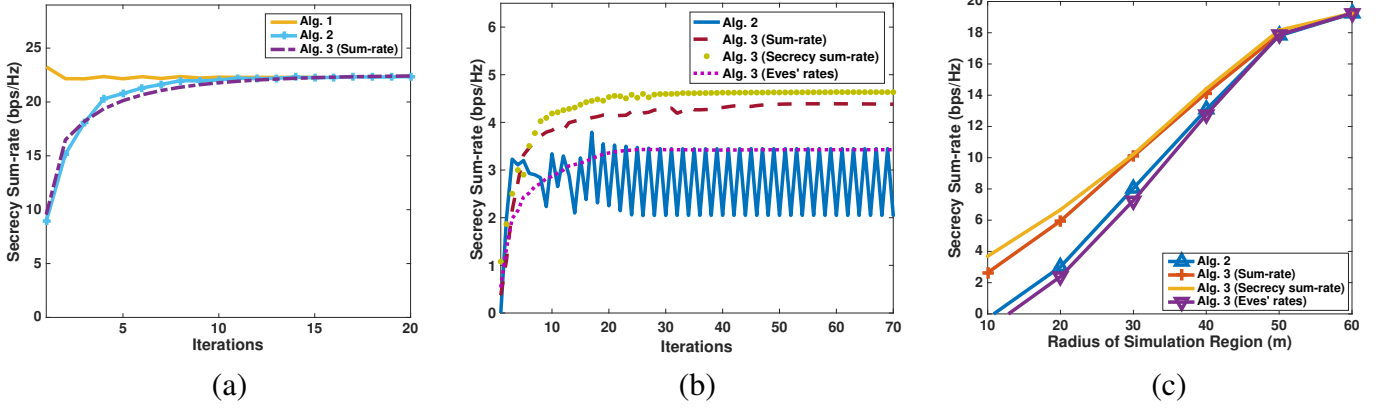


Figure 3.4: (a) Convergence of secrecy sum-rate when QNE is unique; (b) convergence of secrecy sum-rate when multiple QNEs exist; (c) secrecy sum-rate vs.  $r_{circ}$  :  $Q = 8, K = 5, N_{T_q} = 5, N_{r_q} = 2 \forall q, N_{e,k} = 2 \forall k, r_{circ} =$  (a) 100 m, (b) 20 m,  $P_q =$  (a) 20 dBm, (b) 30 dBm, (c) 40 dBm.

$$\epsilon^{(j)} = \frac{1}{j}.$$

Figure 3.4 (a) compares the three proposed algorithms in a channel realization for the case when the QNE is unique. According to the uniqueness condition in Theorem 5, it is generally expected that if links are far enough from each other, then the resulting QNE is likely to be unique. We simulate this scenario by increasing  $r_{circ}$  significantly. We consider the secrecy sum-rate as the measure of comparison between the algorithms. It can be seen that all of the algorithms converge to almost the same point. This result indicates the equivalence between the QNEs found by both Algorithms 1 and 2. Furthermore, it can be concluded that the QNE selection algorithm with sum-rate as its design criterion (indicated by Alg. 3 (Sum-rate)) does not outperform Algorithm 2 when the QNE is unique (i.e., the condition in Theorem 5 is satisfied). That is, if the QNE is unique the QNE selection algorithms only have one QNE to choose from. It should be noted that Algorithm 1 converges faster than other algorithms. This might be because Algorithms 2 and 3 use smaller steps towards the QNE at each iteration.

Figure 3.4 (b) compares the achieved secrecy sum-rate in a channel realization be-

tween Algorithm 2 and different versions of Algorithm 3, indicated by “Alg. 3 (Secrecy sum-rate)” when secrecy sum-rate is the design criterion, “Alg. 3 (Eves’ rates)” when reducing Eves’ rates is the design criterion, and “Alg. 3 (Sum-rate)” when sum-rate is the design criterion. Furthermore, due to the existence of multiple QNEs, Algorithm 2 is oscillating between QNEs and never converges even after 70 iterations<sup>25</sup>. We increased the number of iterations to 1000, but did not see the convergence of Algorithm 2. However, all of the versions of Algorithm 3 converge to a QNE<sup>26</sup>.

Figure 3.4 (c) shows the secrecy sum-rate resulting from different algorithms vs.  $r_{circ}$ . For Algorithm 2, we limit the iterations to 100. For Algorithm 3, we limit the iterations of the inner loop (i.e., line 3 in Algorithm 3) and the outer loop (i.e., line 1 in Algorithm 3) to 50 and 3, respectively. Each point in the figure is the result of averaging over 50 random network topologies, where in each topology, 200 channel realizations are simulated and averaged. It can be seen that when  $r_{circ}$  is small (i.e., high interference), Alg. 3 (Sum-rate) and Alg. 3 (Secrecy sum-rate) have higher secrecy sum-rate than Algorithm 2. This is due to the fact that the myopic maximization of secrecy rates in Algorithm 2 is not guaranteed to converge to a QNE. Moreover, it can be seen that in Alg. 3 (Eves’ rates), we cannot increase the secrecy rate as much as other versions of Algorithm 3. This is due to the fact that in minimizing the received rate at Eves, too much TxFJ power creates unwanted interference on legitimate receivers, preventing any improvement on the secrecy sum-rate.

Figure 3.5 (a) compares the secrecy sum-rate of Algorithms 2 and 3 for different number of links. Alg. 3 (Secrecy sum-rate) and Alg. 3 (Sum-rate) consistently outperform

<sup>25</sup>Recall that convergence of Algorithm 2 is tied to the uniqueness of the QNE. Furthermore, due to the similarity in the behavior of Algorithms 1 and 2, we only showed Algorithm 2 in subsequent simulations.

<sup>26</sup>The result in Figure 3.4 (b) should not be confused with the previous simulation in Figure 3.4 (a). In fact, equal secrecy sum-rate for all of the algorithms happen only when QNE is unique (i.e., the condition in Theorem 5 is satisfied). However, Figure 3.4 (b) is showing results when the condition in Theorem 5 is not likely to be satisfied.

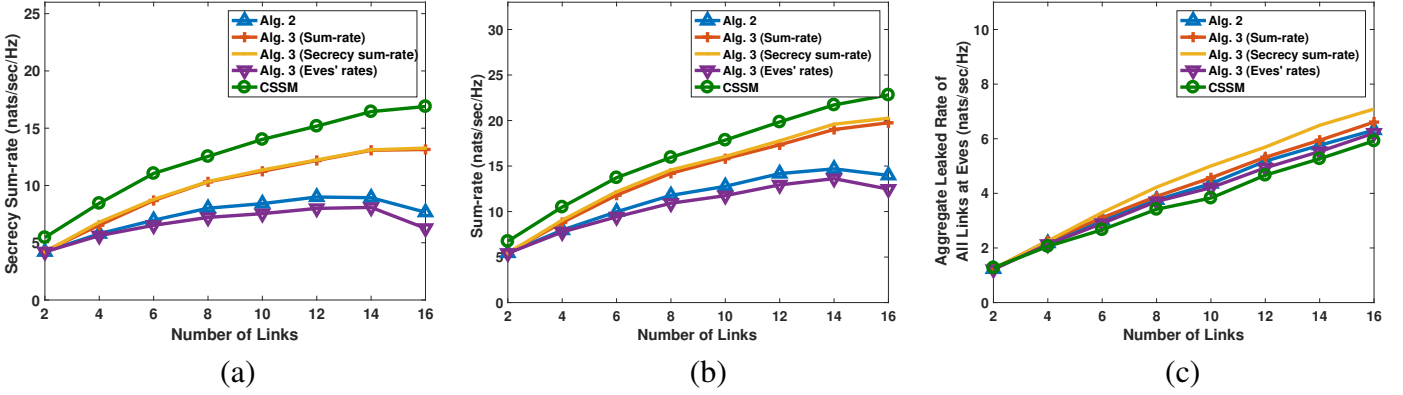


Figure 3.5: Comparison of (a) secrecy sum-rate, (b) sum-rate, (c) sum of Eves' received rates vs. number of links:

$$r_{\text{circ}} = 30 \text{ m}, K = 5, N_{T_q} = 5, N_{r_q} = 2 \forall q, N_{e,k} = 2 \forall k, d_{\text{link}} = 10 \text{ m}, P_q = 40 \text{ dBm}.$$

Algorithm 2 in terms of secrecy sum-rate (Figure 3.5 (a)) and sum-rate (Figure 3.5 (b)), and Alg. 3 (Eves' rates) does not result in a secrecy sum-rate as high as the other two flavors of Algorithm 3. As shown in Figure 3.5 (c), using Alg. 3 (Eves' rates) slightly reduces sum of Eves' received rates by increasing interference at Eves, but this directly affects legitimate transmissions as well. Furthermore, Alg. 3 (Secrecy sum-rate) does not have a significant advantage over Alg. 3 (Sum-rate). Another interesting point is that Alg. 3 (Secrecy sum-rate) has slightly higher sum-rate and higher leaked rate compared to Alg. 3 (Sum-rate). Hence, the performance of Alg. 3 (Secrecy sum-rate) is not necessarily a combination of Alg. 3 (Sum-rate) and Alg. 3 (Eves' rates), but rather a good tradeoff point. Lastly, it can be seen that the proposed algorithms have lower secrecy sum-rates compared to CSSM. We conjecture that this might be due to the fact that CSSM has a larger solution space compared to our methods. Note that the solution space of CSSM may contain some points that are not necessarily the QNEs of the game, whereas both Algorithms 2 and 3 can only converge to QNEs of the game. The difference between Algorithms 2 and 3 is that Algorithm 3 selects the best QNE (according to a criterion), but Algorithm 2 does not. As can be seen in Figure 3.5 (a), for the case of 16 links, the

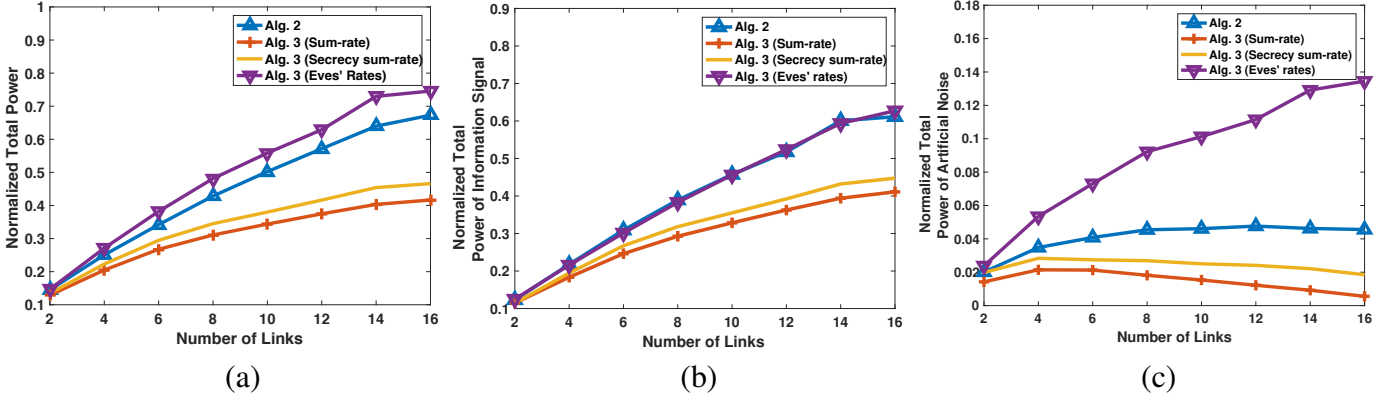


Figure 3.6: Comparison of (a) total power (b) power allocated to information signal (c) power allocated to artificial noise (TxFJ) vs. number of links:  $r_{circ} = 30$  m,  $K = 5$ ,  $N_{T_q} = 5$ ,  $N_{r_q} = 2 \forall q$ ,  $N_{e,k} = 2 \forall k$ ,  $d_{link} = 10$  m,  $P_q = 40$  dBm.

loss of Algorithm 3 compared to CSSM is less than 25% when either secrecy sum-rate or sum-rate is the criterion for the QNE selection phase of Algorithm 3. Despite this loss, using Algorithm 3 facilitates not only a distributed implementation, but also the flexibility in the amount of coordination. The latter gives us freedom to keep the coordination as low as possible. Neither of these features are available in CSSM.

In Figure 3.6 (a)–(c) the power consumption of different algorithms are compared. The total power in Figure 3.6 (a)–(c) is normalized w.r.t the total power budget  $\sum_q P_q$ . Generally, Alg. 3 (Sum-rate) is the most energy efficient algorithm. Both Alg. 2 and Alg. 3 (Eves' rates) perform poorly in energy efficiency as the increase in the power of TxFJ creates interference at other legitimate receivers. This makes the links to spend even more power on the information signal which eventually leads to neither a high sum-rate nor a high secrecy sum-rate. Moreover, the increase in the power of TxFJ seems to be more significant in Alg. 3 (Eves' rates), as the design criterion forces the users to carelessly increase the interference at Eves. Lastly, Alg. 3 (Secrecy sum-rate) and Alg. 3 (Sum-rate) decrease the power of TxFJ as the number of links increases because as the links abound,

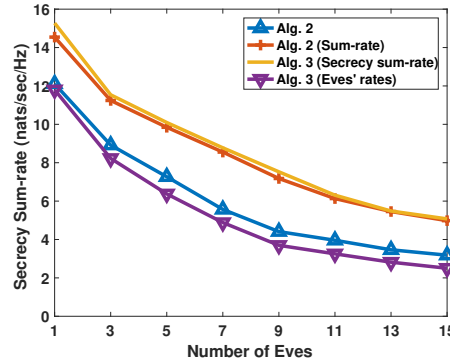


Figure 3.7: Comparison of secrecy sum-rate vs. number of Eves:  $r_{circ} = 30$  m,  $Q = 8$ ,  $N_{T_q} = 5$ ,  $N_{r_q} = N_{e,k} = 2$ ,  $P_q = 40$  dBm

they automatically create additional interference at Eves. Hence, the links do not spend more power on TxFJ.

Figure 3.7 shows that as the number of Eves in the network increases, Alg. 3 (Sum-rate) and Alg. 3 (Secrecy sum-rate) still outperform Algorithm 2 in terms of secrecy sum-rate, and Alg. 3 (Eves' rates) still achieves a low secrecy sum-rate. Overall, in these simulations, maximizing sum-rate as a design criterion seems to be the best choice to increase the secrecy sum-rate because other proposed criteria cannot add significant improvements despite requiring more extensive signaling between the links (e.g., knowledge of E-CSI). Lastly, minimizing Eves' rates as the design criterion although brings poor performance to the QNE selection, it gives us valuable insights on the importance of interference management such that if it is overlooked, the secrecy sum-rate in the network can be severely decreased.

### 3.9 Summary

In this chapter, we designed a game-theoretic secure transmit optimization for a MIMO interference network with several MIMO-enabled Eves. We proposed three algo-

rithms to increase secrecy sum-rate. In the first algorithm, the links myopically optimize their transmission until a quasi-Nash equilibrium (QNE) is reached. Because of the inferior performance of first algorithm in case of multiple QNEs, we designed the second algorithm based on the concept of variational inequality. The second algorithm enables us to analytically derive convergence conditions, but achieves the same secrecy sum-rate as the first algorithm. To increase the secrecy sum-rate, we proposed the third algorithm in which links can select the best QNE according to a certain design criterion. Simulations showed that not every criterion is good for the performance improvement. Specifically, reducing co-channel interference is a better criterion compared to increasing interference at Eves to improve secrecy sum-rate.

## CHAPTER 4

## Pareto-Optimal Power Control with Rate Demands in MIMO Wiretap Interference Networks

### 4.1 Overview

In this chapter, we focus on secure power control in MIMO wiretap interference networks. Contrary to the contributions made in the previous chapter, here we use more practical precoders which are based on zero-forcing TxFJ on intended Bob. In addition to being more practical, such choice of precoders give us more freedom in approaching Pareto-optimal points of the secrecy rate region. Moreover, we show that analysis of the network with partial knowledge of E-CSI is also possible. Each contending link acts selfishly, motivating us to leverage non-cooperative game theory for distributed power control. The non-cooperative game designed to model our power control scheme assumes that each player (i.e., Alice-Bob pair) seeks to maximize its secrecy rate subject to a given information-rate constraint and a power budget. The strategy profile of each player is to control the amount of TxFJ it generates. Achieving (Pareto-)optimal points of the secrecy rate region is done by proposing a price-based game, in which each link is penalized for generating interference on other legitimate links. Under the exact knowledge of E-CSI, we show that the price-based game has a comparable secrecy sum-rate to a centralized approach. Lastly, study of the network under partial knowledge of E-CSI is possible by leveraging mixed-strategy games.

One of the main differences between this chapter and previous chapter is that here we assume that each link performs MIMO *beamforming*, i.e., the covariance matrix of the information signal of a given Alice is rank one. Such an approach has been shown to be optimal for rate maximization under several channel models (see [103]). Although in our case beamforming is a suboptimal approach in terms of rate maximization, it helps us achieve more resilience [to cope with Eve's capabilities] and gain valuable insight into solving the underlying optimization problems. We further assume that legitimate nodes cannot implement multi-user (secure) encoding. Hence, the problem reduces to controlling the power distribution between the information and TxFJ signals at each link.

## 4.2 System Model

While the network under our study in this chapter is mostly similar to the one considered in the previous chapter, due to the different problem considered here, we briefly go over the system model that we introduced in Chapter 3 again and then evolve on it to introduce the problem that is the focus of this chapter. Consider  $Q$  transmitters, Alice<sub>1</sub>, ..., Alice<sub>Q</sub>, ( $Q \geq 2$ ) that communicate with their respective receivers, Bob<sub>1</sub>, ..., Bob<sub>Q</sub>. Let  $\mathcal{Q} = \{1, \dots, Q\}$ . Alice<sub>q</sub> and Bob<sub>q</sub>,  $q \in \mathcal{Q}$ , have  $N_q$  and  $M_q$  antennas, respectively. A passive Eve with  $L$  antennas is also present in the network<sup>1</sup>. The received signal at Bob<sub>q</sub> is

$$\mathbf{y}_q = \tilde{\mathbf{H}}_{qq} \mathbf{u}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q \tilde{\mathbf{H}}_{rq} \mathbf{u}_r + \mathbf{n}_q \quad (4.1)$$

where  $\tilde{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$ ,  $r \in \mathcal{Q}$ , is the  $M_q \times N_r$  complex channel matrix between Alice<sub>r</sub>

---

<sup>1</sup>Though we assume a single eavesdropper,  $L$  can capture the case of multiple (multi-antenna) colluding eavesdroppers.



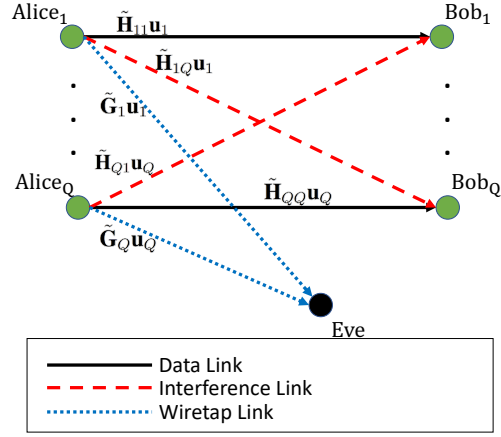


Figure 4.1: System model.

and Bob<sub>q</sub>,  $\mathbf{u}_q \in \mathbb{C}^{N_q}$  is the transmitted signal from Alice<sub>q</sub>. The term  $\mathbf{n}_q \in \mathbb{C}^{M_q}$  is the complex AWGN at Bob<sub>q</sub>; its power is  $N_0$  and its covariance matrix is  $E[\mathbf{n}_q \mathbf{n}_q^\dagger] = \frac{N_0}{M_q} \mathbf{I}$ . The received signal at Eve is

$$\mathbf{z} = \tilde{\mathbf{G}}_q \mathbf{u}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q \tilde{\mathbf{G}}_r \mathbf{u}_r + \mathbf{e} \quad (4.2)$$

where  $\tilde{\mathbf{G}}_q \in \mathbb{C}^{L \times N_q}$ ,  $q \in \mathcal{Q}$  denotes the channel matrix between Alice<sub>q</sub> and Eve, and  $\mathbf{e}$  is the noise term. Figure 4.1 depicts a visual representation of our system model defined by (4.1) and (4.2). The signal  $\mathbf{u}_q = \mathbf{s}_q + \mathbf{w}_q$  consists of the information-bearing signal  $\mathbf{s}_q$  and TxFJ signal  $\mathbf{w}_q$ .  $\mathbf{s}_q$  can be written as  $\mathbf{s}_q = \mathbf{T}_q x_q$ , where  $\mathbf{T}_q$  is the precoding matrix (precoder) and  $x_q$  is the information signal. Assume that a Gaussian codebook is used for  $x_q$ , i.e.,  $x_q$  is a zero mean circularly symmetric complex Gaussian (ZMCSCG) random variable with  $E[x_q x_q^\dagger] = \phi_q P_q \triangleq \gamma_q$ , where  $P_q$  is the total transmit power of Alice<sub>q</sub> and  $0 \leq \phi_q \leq 1$  is the portion of that power allocated to the information signal. For the TxFJ signal, we write  $\mathbf{w}_q \triangleq \mathbf{Z}_q \mathbf{v}_q$ , where  $\mathbf{Z}_q \in \mathbb{C}^{N_q \times (N_q - 1)}$  is the precoder of the TxFJ signal,  $\mathbf{v}_q \in \mathbb{C}^{N_q - 1}$  is a vector of i.i.d. ZMCSCG random variables, and  $E[\mathbf{v}_q \mathbf{v}_q^\dagger] = \sigma_q^2 \mathbf{I}$ .

<sup>2</sup> It was shown in [104] that *structured signaling* can have a better secrecy compared to Gaussian signaling when channel gains are real numbers. However, to the best of our knowledge, proving the usefulness

The scalar term  $\sigma_q = \frac{(1-\phi_q)P_q}{N_q-1}$  denotes the power allocated to each dimension of  $\mathbf{v}_q$ . Let  $\tilde{\mathbf{H}}_{qq} = \mathbf{U}_q \Sigma_q \mathbf{V}_q^\dagger$  denote the singular value decomposition (SVD) of  $\tilde{\mathbf{H}}_{qq}$ , where  $\Sigma_q$  is the diagonal matrix of singular values, and  $\mathbf{U}_q$  and  $\mathbf{V}_q$  are left and right matrices of singular vectors, respectively. We set  $\mathbf{Z}_q = \mathbf{V}_q^{(2)}$ , where  $\mathbf{V}_q^{(2)}$  is the matrix of  $N_q - 1$  rightmost columns of  $\mathbf{V}_q$ . We assume that Alice<sub>q</sub> knows the channel state information (CSI)<sup>3</sup>. The precoder  $\mathbf{T}_q$  is set to  $\mathbf{T}_q = \mathbf{V}_q^{(1)}$ , where  $\mathbf{V}_q^{(1)}$  is the first column of  $\mathbf{V}_q$ . Let  $\mathbf{H}_{qq} \triangleq \tilde{\mathbf{H}}_{qq} \mathbf{V}_q^{(1)}$ ,  $\mathbf{H}'_{qq} \triangleq \tilde{\mathbf{H}}_{qq} \mathbf{V}_q^{(2)}$ ,  $\mathbf{H}_{qr} \triangleq \tilde{\mathbf{H}}_{qr} \mathbf{V}_q^{(1)}$ ,  $\mathbf{H}'_{qr} \triangleq \tilde{\mathbf{H}}_{qr} \mathbf{V}_q^{(2)}$ ,  $\mathbf{G}_q \triangleq \tilde{\mathbf{G}}_q \mathbf{V}_q^{(1)}$ , and  $\mathbf{G}'_q \triangleq \tilde{\mathbf{G}}_q \mathbf{V}_q^{(2)}$ . The terms  $\mathbf{G}_q$  and  $\mathbf{G}'_q$  indicate the E-CSI components. Hence,

$$\begin{aligned} \mathbf{y}_q &= \mathbf{H}_{qq}x_q + \mathbf{H}'_{qq}\mathbf{v}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{H}_{rq}x_r + \mathbf{H}'_{rq}\mathbf{v}_r) + \mathbf{n}_q \\ \mathbf{z} &= \mathbf{G}_q x_q + \mathbf{G}'_q \mathbf{v}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{G}_r x_r + \mathbf{G}'_r \mathbf{v}_r) + \mathbf{e}. \end{aligned}$$

The choice of precoders (i.e., beamformers) for TxFJ signals in this chapter is mainly driven by the fact that acquiring E-CSI knowledge may not be always possible. For a single-link scenario, it was shown in [26] that optimizing the precoders of information and TxFJ signals requires knowledge of E-CSI. However, in this chapter, the beamforming vector of TxFJ signal for each link depends only on the channel between the two nodes comprising that link.

After receiving  $\mathbf{y}_q$  at Bob<sub>q</sub>, a linear receiver  $\mathbf{d}_q \in \mathbb{C}^{M_q}$  is applied to estimate  $x_q$ .  $\mathbf{d}_q$ ,  $q \in \mathcal{Q}$ , is assumed to be chosen according to the maximum ratio combining (MRC) method. Hence,  $\mathbf{d}_q = \mathbf{U}_q^{(1)}$ , where  $\mathbf{U}_q^{(1)}$  is the first column of  $\mathbf{U}_q$ . Hence, the estimate  $\hat{x}_q$

---

of structured codes for the case of complex channels and interference networks is still an open problem.

<sup>3</sup>Acquiring CSI between Alice and her corresponding Bob is assumed to be done securely. For example, implicit channel estimation (i.e., Bob sending pilot signals to Alice) can be used to avoid having to send explicit CSI feedback.

can be described as

$$\hat{x}_q \triangleq \mathbf{d}_q^\dagger (\mathbf{H}_{qq} x_q + \mathbf{H}'_{qq} \mathbf{v}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{H}_{rq} x_r + \mathbf{H}'_{rq} \mathbf{v}_r) + \mathbf{n}_q). \quad (4.3)$$

The terms  $\mathbf{d}_q^\dagger \mathbf{U}_q \Sigma_q$  and  $\mathbf{V}_q^\dagger \mathbf{V}_q^{(2)}$  are orthogonal to each other. Hence,  $\mathbf{d}_q^\dagger \mathbf{H}'_{qq} \mathbf{v}_q = \mathbf{d}_q^\dagger \mathbf{U}_q \Sigma_q \mathbf{V}_q^\dagger \mathbf{V}_q^{(2)} \mathbf{v}_q = 0$ . The information rate for the  $q$ th link can be written as

$$C_q = \log\left(1 + \frac{\gamma_q}{a_q}\right) \quad (4.4)$$

where

$$a_q \triangleq \frac{\sum_{\substack{r=1 \\ r \neq q}}^Q \left( |\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r \right) + N_0}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \quad (4.5)$$

is the normalized interference received at Bob <sub>$q$</sub> . Assuming a worst-case scenario in which Eve knows the channel between herself and each Alice (obtained by possibly spoofing on the pilot sequences), Eve applies the linear receiver  $\mathbf{r}_q \in \mathbb{C}^L$  while eavesdropping on the  $q$ th link's communications so as to obtain the following estimate of  $x_q$

$$\hat{z}_q = \mathbf{r}_q^\dagger (\mathbf{G}_q x_q + \mathbf{G}'_q \mathbf{v}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{G}_r x_r + \mathbf{G}'_r \mathbf{v}_r) + \mathbf{e}). \quad (4.6)$$

Let  $\tilde{\mathbf{G}}_q = \mathbf{L}_q \mathbf{D}_q \mathbf{R}_q$  be the SVD of  $\tilde{\mathbf{G}}_q$ , where  $\mathbf{L}_q$  and  $\mathbf{R}_q$  are matrices of left and right singular vectors, and  $\mathbf{D}_q$  is the diagonal matrix of singular values. Eve chooses  $\mathbf{r}_q = \mathbf{L}_q^{(1)}$ , where  $\mathbf{L}_q^{(1)}$  is the first column of  $\mathbf{L}_q$ , to perform MRC.

We need to point out that our choice of beamforming vector of information signal for each link comes from the fact that the number of antennas at eavesdropper(s) may not be

known in some cases. As pointed out in [22], the main limitation of the TxFJ method is that if the eavesdropper has more antennas than the legitimate Tx, then the eavesdropper may be able to nullify the effect of TxFJ on itself by a specific choice of decoder (i.e., linear receiver) at its receive antennas.

In general, the TxFJ signal from the  $q$ th Tx received at the eavesdropper can be written as  $\mathbf{r}_q \tilde{\mathbf{G}}_q \mathbf{V}'_q \mathbf{v}_q$  where  $\mathbf{V}'_q$  is the  $N$  rightmost columns of  $\mathbf{V}_q$ . Let  $\tilde{\mathbf{G}}_q \mathbf{V}'_q = \mathbf{G}'_q = \mathbf{L}'_q \mathbf{D}'_q \mathbf{R}'_q$  be the SVD of the  $L \times N$  matrix  $\mathbf{G}'_q$ , where  $\mathbf{L}'_q$  and  $\mathbf{R}'_q$  are matrices of left and right singular vectors, respectively, and  $\mathbf{D}'_q$  is the diagonal matrix of singular values.

Considering  $\mathbf{G}'_q$ , if we have  $L > N$ , indicating that the channel  $\mathbf{G}'_q$  is a tall matrix, then eavesdropper has more antennas than the total dimensions considered for the TxFJ signal at the  $q$ th Tx. Hence, if eavesdropper knows  $\mathbf{G}'_q$  it can choose  $\mathbf{r}_q$  to be the rightmost  $L - N$  columns of the matrix  $\mathbf{L}'_q$ . This way, eavesdropper can nullify the TxFJ signal, i.e.,  $\mathbf{r}_q \tilde{\mathbf{G}}_q \mathbf{V}'_q = 0$ . Therefore, an eavesdropper with sufficiently high number of antennas can nullify the effect of TxFJ on itself. To prevent this, we need to make sure that  $L - N \leq 0$ , so  $N \geq L$ . To ensure that  $N \geq L$  the  $q$ th Tx uses as many dimensions for the TxFJ signal as possible. Hence, we set  $N$  to its maximum value, i.e.,  $N = N_q - 1$ . This way, at least we know that the  $q$ th Tx cannot do any better to prevent nullification of TxFJ on the eavesdropper. Obviously, by choosing  $N = 1$  (i.e., allocating one dimension to the TxFJ precoder), even an eavesdropper with  $L = 2$  antennas can nullify the effect of TxFJ on itself.

Hence, the precoder of TxFJ signal  $\mathbf{Z}_q$  must include the  $N_q - 1$  rightmost columns of  $\mathbf{V}_q$ . Accordingly, the information signal  $\mathbf{s}_q$  can be written as  $\mathbf{s}_q = \mathbf{T}_q x_q$ , where  $\mathbf{T}_q$  is the precoding matrix (precoder) and  $x_q$  is the information signal. With the aforementioned choice of TxFJ beamformer, the beamformer that can maximize the information rate of the  $q$ th Tx would be  $\mathbf{T}_q = \mathbf{V}_q^{(1)}$ , where  $\mathbf{V}_q^{(1)}$  is the  $N_q - N = N_q - (N_q - 1) = 1$  leftmost

column of  $\mathbf{V}_q$ , i.e., the first column of  $\mathbf{V}_q$ . Such choices of precoders forces  $x_q$  to be a scalar value, signifying that only single-stream signals are allowed to be transmitted.

Overall, with these choices of precoders, we first make sure that our precoders do not require knowledge of E-CSI, then we make sure that our TxFJ signal will not be nullified at an eavesdropper with relatively low number of antennas. Such an approach in assigning precoders was also used in [23,24]. Notice that in the case of having knowledge of number of antennas at eavesdropper, one can easily choose exact amount of dimensions for the TxFJ beamformer to ensure that eavesdropper is not able to nullify the TxFJ at itself. However, in case of collusion between multiple eavesdroppers, they can form a MIMO receiver with higher number of receive antennas.

Such an approach in assigning precoders was also used in [23,24]. Notice that in the case of having knowledge of number of antennas at eavesdropper, one can easily choose exact amount of dimensions for the TxFJ beamformer to ensure that eavesdropper is not able to nullify the TxFJ at itself. However, here we assumed that the eavesdropper has close specifications to the legitimate nodes. This forces us to allocate as many dimensions as possible to the TxFJ beamformer, i.e., increase the rank of TxFJ beamformer as much as possible (to prevent nullification of TxFJ at Eve) and use the remaining dimensions for the precoder of information signal.

### 4.3 Problem Formulation

The multi-user channel between the  $Q$  Alices and Eve can be modeled as a multiple-access channel. If Eve is capable of using successive interference cancellation (SIC), she may be able to simultaneously decode all signals. To illustrate the impact of SIC, consider the example of  $Q = 2$ . The rate region of Eve's multi-access channel is shown in Figure 4.2, where  $C_{eq}$  denotes the rate at Eve while decoding Alice <sub>$q$</sub> 's signal ( $q = 1, 2$ ).

The points  $\beta_q$  and  $\psi_q$  are defined later on in (4.7) and (4.10), respectively. Figure 4.2 suggests that to prevent Eve from using SIC, we must have  $C_q > \beta_q$  for  $q = 1, 2$  [42], where

$$\beta_q \triangleq \log\left(1 + \frac{\gamma_q}{c_q}\right) \quad (4.7)$$

$$c_q = \frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q| \sigma_q + \left(|\mathbf{r}_q^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2 \sigma_r\right) + N_0}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \quad (4.8)$$

where  $r \neq q$  ( $c_q$  is not to be confused with  $C_q$  defined in (4.4)). In this case, the secrecy rate for Alice <sub>$q$</sub> ,  $q = 1, 2$ , would be  $C_q^{sec} = \max\{C_q - \beta_q, 0\}$  [42]. Because  $C_q > \beta_q$ , it can be guaranteed that Eve does not have complete knowledge of the  $q$ th information signal. Thus, the rate at Eve while eavesdropping on Alice <sub>$r$</sub> 's signal,  $r \neq q$ , is  $C_{er} = \beta_r$ , and the secrecy rate of the  $r$ th link is

$$C_r^{sec} \triangleq \max\{C_r - \beta_r, 0\} = \max\left\{\log\left(1 + \frac{\gamma_r}{a_r}\right) - \log\left(1 + \frac{\gamma_r}{c_r}\right), 0\right\}. \quad (4.9)$$

This operating point is shown as the tuple  $(\beta_1, \beta_2)$  in Figure 4.2. If  $C_q \leq \beta_q$ , Eve has complete knowledge of Alice <sub>$q$</sub> 's signal,  $q = 1, 2$ . Hence, Eve can consider Alice <sub>$r$</sub> 's signal,  $r \neq q$ , as interference and decode Alice <sub>$q$</sub> 's signal. Knowledge of Alice <sub>$q$</sub> 's signal allows Eve to remove it from the total received signal and obtain Alice <sub>$r$</sub> 's signal without

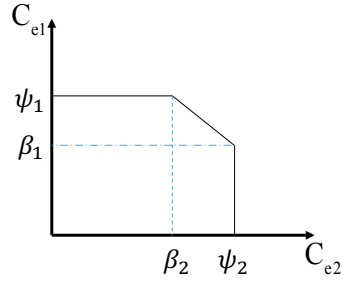


Figure 4.2: Rate pairs for the two eavesdropping channels shown as a two-user multiple access channel.

interference. Hence,  $C_{er} = \psi_r$  and  $C_r^{sec} = \max\{C_r - \psi_r, 0\}$  where

$$\psi_r \triangleq \log\left(1 + \frac{\gamma_r}{d_r}\right) \quad (4.10)$$

$$d_r = \frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r| \sigma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2 \sigma_q + N_0}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2}. \quad (4.11)$$

This operating point can be shown as the tuple  $(\psi_1, \beta_2)$  or  $(\beta_1, \psi_2)$  in Figure 4.2, depending on which Alice is targeted first by Eve. Overall, in order to achieve the maximum secrecy, both transmitters have to choose a transmission rate higher than Eve's decodable rate. For  $Q > 2$ , in order to prevent Eve from using SIC, we must have  $C_q > \zeta_q \forall q$ , where

$$\zeta_q \triangleq \log\left(1 + \frac{\gamma_q}{f_q}\right) \quad (4.12a)$$

$$f_q = \frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q| \sigma_q + \sum_{\substack{r=1 \\ r \neq q}}^Q \left( |\mathbf{r}_q^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2 \sigma_r \right) + N_0}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}. \quad (4.12b)$$

Hence,

$$C_q^{sec} = \max\{C_q - \zeta_q, 0\}. \quad (4.13)$$

We define  $C^{sec} \triangleq \sum_{q=1}^Q C_q^{sec}$  as the *secrecy sum-rate*, where  $C_q^{sec}$  is defined in (4.13) and  $\zeta_q$  is defined in (4.12a). We aim to maximize  $C^{sec}$  while ensuring a minimum information rate for all links. This problem can be formally written as:

$$\begin{aligned} & \underset{\gamma, \sigma}{\text{maximize}} \quad C^{sec} \\ & \text{s.t.} \quad \begin{cases} \gamma_q + \sigma_q(N_q - 1) \leq P_q, \quad \forall q \\ C_q \geq R_q \end{cases} \end{aligned} \quad (4.16)$$

where  $\gamma \triangleq [\gamma_q]_{q=1}^Q = [\gamma_1, \dots, \gamma_Q]$  and  $\sigma \triangleq [\sigma_q]_{q=1}^Q$ . The first constraint imposes a power constraint on each legitimate Tx; and the second constraint ensures a minimum information rate  $R_q$  for each link  $q$ . The optimization in (4.16) is non-convex. We relax this problem by assuming that the second constraint in (4.16) is satisfied with equality for some amount of power for the information signal, i.e.,  $C_q = R_q$  for some  $\gamma_q^*$ , for all  $q$ <sup>4</sup>. The second constraint can now be embedded into the objective function and the first constraint. Hence, (4.16) is simplified into<sup>5</sup>

$$\begin{aligned} & \underset{\sigma}{\text{maximize}} \quad C^{sec} \\ & \text{s.t.} \quad \sigma_q \leq \frac{P_q - \gamma_q^*}{N_q - 1}, \quad \forall q. \end{aligned} \quad (4.17)$$

Recalling how we prevent Eve from applying SIC in (4.12a),  $\sigma_q$  is chosen such that  $C_q > \zeta_q$  is satisfied for all  $q$ , i.e.,

$$\sigma_q > \frac{A_q}{B_q} \quad (4.18)$$

---

<sup>4</sup>Later on, when we propose our FJ control algorithm, we devise a procedure for finding  $\gamma_q^*$ .

<sup>5</sup>Later, as we present our TxFJ control algorithm, we provide more explanation of this simplification.



where

$$A_q \triangleq |\mathbf{r}_q^\dagger \mathbf{G}_q|^2 \left( \sum_{\substack{r=1 \\ r \neq q}}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r) + N_0 \right) - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \left( \sum_{\substack{r=1 \\ r \neq q}}^Q (|\mathbf{r}_q^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2 \sigma_r) + N_0 \right) \quad (4.19a)$$

$$B_q \triangleq |\mathbf{r}_q^\dagger \mathbf{G}'_q| |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2. \quad (4.19b)$$

Simplifying (4.18), the following constraints can be established:

$$\sigma_q = \frac{P_q - \gamma_q^*}{N_q - 1} \quad \text{if} \quad \frac{A_q}{B_q} \geq \frac{P_q - \gamma_q^*}{N_q - 1} \quad (4.20a)$$

$$\sigma_q > \frac{A_q}{B_q} \quad \text{if} \quad A_q > 0 \ \& \ \frac{A_q}{B_q} < \frac{P_q - \gamma_q^*}{N_q - 1} \quad (4.20b)$$

$$\sigma_q > 0 \quad \text{if} \quad A_q = 0. \quad (4.20c)$$

$$\sigma_q = 0 \quad \text{if} \quad A_q < 0. \quad (4.20d)$$

For the case in (4.20a), no amount of TxFJ power can prevent Eve from using SIC. Because the inequalities in (4.20b) and (4.20c) are strict, we define  $\delta_q > 0$  to denote an arbitrarily small positive value, so that we can have

$$\sigma_q = \frac{P_q - \gamma_q^*}{N_q - 1} \quad \text{if} \quad \frac{A_q}{B_q} \geq \frac{P_q - \gamma_q^*}{N_q - 1} \quad (4.21a)$$

$$\sigma_q \geq \frac{A_q}{B_q} + \delta_q \quad \text{if} \quad A_q > 0 \ \& \ \frac{A_q}{B_q} < \frac{P_q - \gamma_q^*}{N_q - 1} \quad (4.21b)$$

$$\sigma_q \geq \delta_q \quad \text{if} \quad A_q = 0. \quad (4.21c)$$

$$\sigma_q = 0 \quad \text{if} \quad A_q < 0. \quad (4.21d)$$

Considering that any of (4.20b), (4.20c), or (4.20d) holds, the optimization in (4.17) becomes

$$\begin{aligned} & \underset{\boldsymbol{\sigma}}{\text{maximize}} \quad C^{sec} \\ & \text{s.t.} \quad \sigma_q \in \mathcal{D}_q \triangleq \left[ \chi_q, \frac{P_q - \gamma_q^*}{N_q - 1} \right], \quad \forall q \end{aligned} \quad (4.22)$$

where  $\chi_q \triangleq \min \left\{ \max \left( \delta_q \frac{A_q}{|A_q|}, \frac{A_q}{B_q} + \delta_q \frac{A_q}{|A_q|}, 0 \right), \frac{P_q - \gamma_q^*}{N_q - 1} \right\}$  and  $[a, b]$  denotes a continuous interval between  $a$  and  $b$ . The optimization in (4.22) aims to find the best tradeoff (i.e., Pareto-optimal solutions) of secrecy sum-rate<sup>6</sup>. Unfortunately, the optimization in (4.22) is still non-convex. Furthermore, it requires the knowledge of E-CSI (i.e.,  $\mathbf{G}_q$  and  $\mathbf{G}'_q$ ).

#### 4.4 Game Formulation

##### 4.4.1 Greedy FJ Control

One method to reduce the complexity of (4.22), and at the same time enable distributed implementation with low signaling overhead, is to let each Alice maximize the secrecy of her transmission to the corresponding Bob and ignore the effect of her TxFJ on unintended Bobs. This locally optimized TxFJ control leads to a game-theoretic interpretation of this network. That is, a non-cooperative game can be formulated in which the best strategy of each link  $q$  is

$$\begin{aligned} & \underset{\sigma_q}{\text{maximize}} \quad C_q^{sec} \\ & \text{s.t.} \quad \sigma_q \in \mathcal{D}_q. \end{aligned} \quad (4.23)$$

---

<sup>6</sup>To be more specific, the solutions of (4.22) only correspond to one Pareto-optimal solution on the convex portion of the secrecy rate region. We skip the details of the relationship between the Pareto-optimal points and (weighted) sum utility optimization for the sake of brevity (see [38, Section 6], Appendix B, and [105]).

In this game, the utility function of each player (link) is his secrecy rate and his strategy is to choose the best TxFJ power to maximize his utility subject to a power constraint (i.e., strategy set). Although one may argue that the game formulation in (4.23) is essentially different from the formulation in (4.22), we use (4.23) to build foundations on how we find suitable solutions for (4.22).

The existence of a NE for game (4.23) can be proved by showing that the strategy set of each player is a non-empty, compact, and convex subset of  $\mathbb{R}$ , and the utility function of each player is a continuous and quasi-concave function of the TxFJ power [106]. Verifying these properties in our game is straightforward, and is thus skipped for brevity. Since the objective function in (4.23) is strictly concave in  $\sigma_q$ , the best strategy that maximizes the secrecy rate of the  $q$ th player is to select the maximum available TxFJ power, i.e.,  $\sigma_q = P_q^{jam} \triangleq \frac{P_q - \gamma_q^*}{N_q - 1}$ ,  $q = 1, 2$ . When  $\sigma_q = P_q^{jam} \forall q$ , no player will be willing to unilaterally change his own strategy because any other strategy can degrade the secrecy rate of that player. Therefore, the point  $\sigma_q = P_q^{jam}, \forall q$  is the NE.

This NE point, however, may not always be efficient, because selfish maximization of the secrecy rate by each player is not always guaranteed to be Pareto-optimal. Hence, we seek a modification that prevents legitimate links from using all their TxFJ powers, so as to reduce interference in the network.

#### 4.4.2 Price-Based FJ Control

The efficiency of the NE in the greedy FJ approach can be improved by using pricing policies. Specifically, for all  $q$ , the utility of player  $q$  in (4.23) would be modified into:

$$\begin{aligned} & \underset{\sigma_q}{\text{maximize}} \quad C_q^{sec} - \lambda_q \sigma_q \\ & \text{s.t.} \quad \sigma_q \in \mathcal{D}_q \end{aligned} \quad (4.24)$$

where  $\lambda_q$  is a pricing factor for the  $q$ th link, defined as

$$\lambda_q \triangleq \sum_{\substack{r=1 \\ r \neq q}}^Q -\frac{\partial C_r^{sec}}{\partial \sigma_q}. \quad (4.25)$$

The optimal TxFJ power can be found by writing the K.K.T. conditions for (4.24). A close-form representation of the optimal TxFJ power for the  $q$ th link can be written as

$$\sigma_q^* = \frac{1}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2} \left( \sqrt{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2 \frac{\gamma_q^*}{\lambda_q} + |\mathbf{r}_q^\dagger \mathbf{G}_q|^4 \frac{\gamma_q^{*2}}{4}} - |\mathbf{r}_q^\dagger \mathbf{G}_q|^2 \frac{\gamma_q^*}{2} - \sum_{\substack{r=1 \\ r \neq q}}^Q (|\mathbf{r}_q^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2 \sigma_r + N_0) \right) \Bigg]_{\chi_q}^{\frac{P_q - \gamma_q^*}{N_q - 1}} \quad (4.26)$$

where  $\bullet_a^b$  denotes  $\min\{\max\{\bullet, a\}, b\}$ ,  $a \leq b$ . It is easy to verify that in (4.4.2), by setting  $\lambda_q = 0$ , we end up with the greedy TxFJ approach. By iteratively using (4.4.2) to set the TxFJ power for all players, the game converges to a NE from which neither player is willing to deviate. Later on, we further explain the feasibility of converging to a NE. The following theorem clarifies the reason for setting the pricing factor as in (4.25).

**Theorem 7.** *The NE of the game (4.24) where players apply (4.25) as the pricing factor equals to that of a locally optimal solution to (4.22).*

*Proof.* See Appendix B. □

Next, we introduce an important property of the price-based FJ control.

**Proposition 3.** *The price-based FJ control admits a unique NE that is the global optimum of the secrecy sum-rate maximization problem in (4.22) if the following conditions are satisfied:*

- *All links have feasible strategies, i.e., they satisfy the bound in (4.18), i.e.,  $\sigma_q > \frac{A_q}{B_q}, \forall q$ .*
- *Low interference at each Bob, i.e.,  $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \gg \sum_{r=1, r \neq q}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r) + N_0, \forall q$ .*

*Furthermore, assuming only feasible strategies for all links, using (4.4.2) to update Tx FJ powers in a sequential manner (i.e., the Gauss-Seidel method in the sense of [107, Chapter 3]) for all  $q \in \mathcal{Q}$  converges to a (unique) NE.*

*Proof.* See Appendix B. □

**Remark:** While we were not able to show the convergence under synchronous updates (i.e., the Jacobi method in the sense of [107, Chapter 3]), where all links update their actions simultaneously at each iteration, we verified it in our simulations.

#### 4.4.3 Optimality of Greedy FJ Control

As a first attempt, we now analyze the situation where the use of greedy FJ control results in a unique Pareto-optimal point for the secrecy sum-rate maximization in (4.17). This analysis allows us to find the conditions under which there is no need for an iterative price-based FJ control optimization (and subsequently, no need for knowledge of E-CSI) because each Alice sets her Tx FJ power to the maximum available.

**Proposition 4.** *The greedy FJ approach results in the unique Pareto-optimal operating point for problem (4.17) if the matrix  $\nabla C^{sec}$ , whose  $(i, j)$  element is given by  $\frac{\partial C_i^{sec}}{\partial \sigma_j}$ ,  $i, j \in \mathcal{Q}$ , has non-negative elements and non-zero rows.*

*Proof.* See Appendix B. □

**Remark:** In the following, we give a simple side result of Proposition 4, which serves as an intuitive example to understand Proposition 4.

**Corollary 1.** *For a network of two legitimate links, the greedy FJ control results in a unique Pareto-optimal point if  $\lambda_q \leq 0$ ,  $q = 1, 2$ .*

*Proof.* Given that  $\lambda_q = -\frac{\partial C_r^{sec}}{\partial \sigma_q}$ ,  $q, r = 1, 2$  (see (4.25)), for  $\lambda_q > 0$ , then  $\frac{\partial C_r^{sec}}{\partial \sigma_q} < 0$ . Hence, a positive price is effective as long as the increase in one player's TxPJ power reduces the secrecy rate for the other link. Now, considering  $\lambda_q \leq 0$ , the increase in one player's TxPJ power results in either no change (i.e.,  $\lambda_q = 0$ ) or an increase (i.e.,  $\lambda_q < 0$ ) in the other player's secrecy rate. Therefore, whenever  $\lambda_q \leq 0$  the right decision would be to use the maximum TxPJ power (i.e., setting  $\lambda_q = 0$ ). □

**Remark:** We would like to clarify that in general, the efficiency of the Greedy FJ control is not superior to that of the pricing-based approach. However, under some special conditions, detailed in Proposition 4, the price-based FJ control reduces to greedy FJ control (i.e.,  $\lambda_q = 0$ ,  $\forall q \in \mathcal{Q}$ ).

For the general case of  $Q > 2$ , we now aim at making sense out of the conditions in Proposition 4, i.e., what would be the physical interpretation of these conditions.

**Proposition 5.** *The Pareto-optimality of the greedy FJ method occurs when  $\frac{\gamma_q}{\sigma_q} \gg 1$ ,  $\forall q$ .*

*Proof.* See Appendix B. □

**Remark:** The result of Proposition 5 is rather intuitive because preserving positive secrecy requires a link to spend a portion of its power for TxFJ. Therefore, whatever scenario that leaves low power to the TxFJ of all Alices (e.g., low transmit power, high rate demands or a dense network) can be the scenario where  $\frac{\gamma_q}{\sigma_q} \gg 1, \forall q$ .

#### 4.5 Price-Based FJ Under E-CSI Uncertainties

When the E-CSI is unknown, it is difficult to compute  $\sigma_q^*$  and  $\lambda_q$ . Besides, the use of greedy FJ cannot be always guaranteed to be a Pareto-optimal point. In the following, we propose a method to overcome the issue of not having complete knowledge of E-CSI. We first need to introduce some new definitions for our game.

Let  $U_q(s_q, s_{-q})$  be the utility of the  $q$ th player, where  $s_q$  and  $s_{-q}$  denote the strategy taken by player  $q$  and by other players except  $q$ , respectively. Without loss of generality, assume that the lower bound on  $\sigma_q$  for guaranteeing positive secrecy (as in (4.20)) has not been taken into account yet. Hence, the strategy space for each player  $q$  is a continuous interval, which can be written as  $\sigma_q \in [0, P_q^{jam}]$ . The strategy set of each player has infinitely many real numbers. In order to proceed further with our analysis, we need to make the strategy sets countable and finite. Hence, we discretize the TxFJ power. Assuming that we have  $n$  bits to convey  $M = 2^n$  power levels, the power level increment is  $\Delta\sigma_q = \frac{P_q^{jam}}{2^n}$ . The strategy set of the  $q$ th player now becomes  $\mathcal{S}_q = \{0, \Delta\sigma_q, 2\Delta\sigma_q, \dots, (M-1)\Delta\sigma_q, P_q^{jam}\}$ . Discretizing the players' strategies allows us to leverage a property of games with finite strategy sets for the players (i.e., *finite*

games): Every finite game has a mixed-strategic NE [108].

#### 4.5.1 Mixed-Strategy Game Formulation

**Definition 3.** A mixed-strategy vector for the  $q$ th player  $\mathcal{A}_q = \{[\alpha_{i,q}]_{i=1}^M \mid 0 \leq \alpha_{i,q} \leq 1, \sum_i \alpha_{i,q} = 1, \forall q\}$  is a probability distribution of the  $q$ th player's strategies. In other words, the  $q$ th player chooses power level  $i\Delta\sigma_q$  with probability  $\alpha_{i,q}$ .

In the mixed-strategy jamming game, players choose their TxFJ powers based on probability distributions. Hence, the best response of each player is to maximize the expected value of his own utility. We note that some games can be limited to only pure strategies. In particular, if the utility function of a player is concave w.r.t. his strategy, then using Jensen's inequality, we deduce that  $\forall (s_q, s_{-q}) \in \mathcal{S}_q \times \mathcal{S}_{-q}$ , where  $\mathcal{S}_{-q} \triangleq \mathcal{S}_1 \times \cdots \times \mathcal{S}_{q-1} \times \mathcal{S}_{q+1} \times \cdots \times \mathcal{S}_Q$ , we must have

$$E_{s_q} [E_{s_{-q}} [U_q(s_q, s_{-q})]] \leq E_{s_{-q}} [U_q(E_{s_q}[s_q], s_{-q})]. \quad (4.27)$$

Equation (4.27) is satisfied with equality if and only if  $s_q$  reduces to pure strategies. Hence, using pure strategies is more efficient than using mixed strategies. However, sufficiency of pure strategies cannot be guaranteed if the utility function of a player is not concave w.r.t. his action. Hence, mixed strategies should also be investigated for non-concave utilities. Unfortunately, to the best of our knowledge, even though the existence of a mixed NE in games with finite strategy spaces is guaranteed regardless of concavity of utility functions [109], finding the mixed NE in games with non-concave utilities is in general difficult. In our case, we limit our study to  $Q = 2$ , for which the mixed-strategy games are well-understood.

Before exploring the application of mixed-strategy games in our FJ control problem,



we present an important observation related to the behavior of price-based FJ control when  $Q = 2$ . Assume now that the constraints imposed on  $\sigma_q$  in (4.20) are taken into account.

**Conjecture 1.** *When  $Q = 2$ , the optimal update of one player in (4.4.2) is a monotonic function of the TxFJ power of the other player's action, i.e.,  $\sigma_q^*$  is a monotonic function of  $\sigma_r^*$  for  $q = 1, 2$  and  $r \neq q$ .*

Although we were not able to analytically prove the above relationship between the two TxFJ powers, we verified it via the following simulation. We replaced the term  $\lambda_q$  in (4.4.2) with the right hand side (RHS) of (4.25) and examined whether the optimal update on TxFJ of one link is a monotonic function of TxFJ of another link. We randomly placed both links as well as the eavesdropper in a circle with radius  $r_{circ} = 25$  m. The distance between the transmitter and the receiver of each link is set to be a constant  $d_{link} = 15$  m. Due to the importance of this conjecture, we have a high number of runs for this simulation. we ran this simulation for a total of 100 random link placements. For each link placement, we created 1000 channel realizations. Then, the probability of monotonicity of TxFJ powers w.r.t each other can be calculated by counting the number of times that  $\sigma_q^*$  is a monotonic function of  $\sigma_r$ ,  $r, q \in \mathcal{Q}$  and dividing this number by  $100 * 1000$ . This simulation is done for different transmit powers at both Alices. We assumed that both Alices use the same amount of transmit power for each run. It can be seen in Figure 4.3 that the monotonicity of TxFJ powers w.r.t. each other occurs almost every time we run this simulation. We ended up with the same results for different values of  $r_{circ}$  and  $d_{link}$  as well. Such verification of Conjecture 1 allows us to conclude the following:

**Proposition 6.** *If  $Q = 2$  and  $\lambda_q > 0$ , the NE tuple of TxFJ powers  $(\sigma_1, \sigma_2)$  will take one*

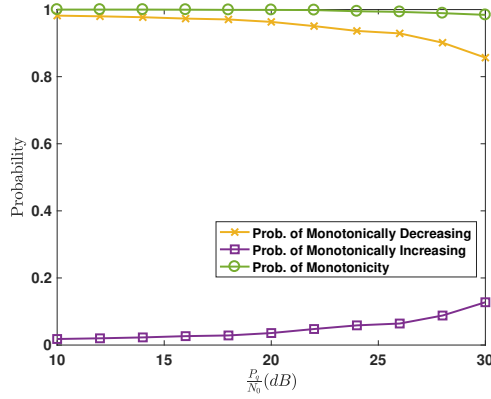


Figure 4.3: Probability of monotonicity of  $\sigma_q^*$  w.r.t.  $\sigma_r$ ,  $(r, q) = 1, 2$ ,  $r \neq q$ . of the following forms:

$$\begin{aligned}
 (\sigma_1, \sigma_2) &= (\sigma_{int}, \chi_2) \text{ or } (\sigma_{int}, P_2^{jam}) \text{ or } (\chi_1, \sigma_{int}) \text{ or} \\
 & (P_1^{jam}, \sigma_{int}) \text{ or } (\chi_1, \chi_2) \text{ or } (P_1^{jam}, P_2^{jam})
 \end{aligned} \tag{4.28}$$

where  $\chi_q < \sigma_{int} < P_q^{jam}$ .

*Proof.* See Appendix B. □

For  $Q = 2$ , we can establish the strategy table shown in Table 4.1. A utility matrix  $\mathbf{U}_q$ ,  $q = 1, 2$ , can be obtained such that the  $(i, j)$ th entry is  $[\mathbf{U}_q]_{ij} = \{U_q(i\Delta\sigma_1, j\Delta\sigma_2) | (i, j) \in \{0, \dots, M\}^2, r \neq q\}$  where  $U_q$  is the utility function of the  $q$ th player and will be characterized shortly. Because problem (4.22) is non-convex w.r.t the TxFJ powers, the Pareto-optimal points can be found via exhaustive search in Table 4.1. Considering a finite jamming game, the complexity of this optimization is in the order of  $\mathcal{O}(n^2)$ , where  $n$  is the number of strategies for each player. Proposition 6 reduces the complexity to  $\mathcal{O}(4n - 4)$  signifying that only a small set of TxFJ power tuples comprises the NE points of price-based FJ game

In price-based FJ, the utility function of each player changes at every iteration due to

$s_1 \backslash s_2$	0	$\Delta\sigma_2$	...	$P_2^{jam}$
0	$U_1(0,0), U_2(0,0)$	$U_1(0, \Delta\sigma_2), U_2(0, \Delta\sigma_2)$	...	$U_1(0, P_2^{jam}), U_2(0, P_2^{jam})$
$\Delta\sigma_1$	$U_1(\Delta\sigma_1, 0), U_2(\Delta\sigma_1, 0)$	$U_1(\Delta\sigma_1, \Delta\sigma_2), U_2(\Delta\sigma_1, \Delta\sigma_2)$	...	$U_1(\Delta\sigma_1, P_2^{jam}), U_2(\Delta\sigma_1, P_2^{jam})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$P_1^{jam}$	$U_1(P_1^{jam}, 0), U_2(P_1^{jam}, 0)$	$U_1(P_1^{jam}, \Delta\sigma_2), U_2(P_1^{jam}, \Delta\sigma_2)$	...	$U_1(P_1^{jam}, P_2^{jam}), U_2(P_1^{jam}, P_2^{jam})$

Table 4.1: Strategy table for the two-link finite jamming game with pricing.

the price updates. However, such update cannot be shown in a strategy table, i.e., the terms  $U_1(i\Delta\sigma_1, j\Delta\sigma_2)$  and  $U_2(i\Delta\sigma_1, j\Delta\sigma_2)$ ,  $(i, j) \in \{0, \dots, M\}$ , in Table 4.1 can only show the utilities of the two players (at  $s_1 = i\Delta\sigma_1$  and  $s_2 = j\Delta\sigma_2$ ) for one iteration. Hence, it is not possible to designate the objective function in (4.24) as a utility function in the strategy table. In order to establish the strategy table, we inspect (4.22) again. Theorem 1 suggests that the K.K.T. conditions of secrecy sum-rate maximization in (4.22) are met at the NE point of the price-based game. Hence, we consider the utility of each player at the NE point to be  $U_q(s_1, s_2) = C^{sec}(\sigma_q)$ ,  $q \in \{1, 2\}$ , which is in general a non-concave function w.r.t.  $\sigma_q$ . Because the two players have the same utility, it is reasonable for the  $q$ th player,  $q = 1, 2$  to assume that the  $r$ th player ( $r \neq q, r = 1, 2$ ) chooses a strategy that is towards maximizing the utility of the  $q$ th player. Considering this fact and Proposition 6, the objective of player 1 (and equivalently for player 2) in the mixed-strategy FJ control game can be written as:

$$\begin{aligned}
& \underset{\{\alpha_{i,1}\}_{i=1}^M}{\text{maximize}} && \max_{s_2} \sum_{i=1}^M \alpha_{i,1} U_1(i\Delta\sigma_1, s_2) \\
& \text{s.t.} && \sum_{i=1}^M \alpha_{i,1} = 1 \\
& && 0 < \alpha_{i,1} < 1, \forall i
\end{aligned} \tag{4.29}$$

where  $\{\alpha_{i,1}\}_{i=1}^M$  is a probability set and  $s_2 \in \{\lceil \frac{\chi_2}{M} \rceil \Delta\sigma_2, P_2^{jam}\}$  with  $\lceil \bullet \rceil$  denoting the ceiling function. In other words, the  $q$ th player mixes his strategies to maximize the

maximum utility that is seen from  $r$ th player's action.

#### 4.5.2 Robust Solutions

So far, our derivations are based on complete knowledge of E-CSI. However, if Eve is a passive device, this assumption is unrealistic. For the  $q$ th player, the computation of the secrecy rate defined in (4.9) depends on  $C_q$  and  $C_{eq}$ . Because we assumed that Bob can measure his received interference level and Alice is aware of the channel between herself and her corresponding Bob, the computation of  $C_q$  can be done locally. Each component of (unknown) E-CSI can be equivalently shown as the product of some large-scale and small-scale fading parts, so  $|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 = |\bar{\mathbf{G}}_q|^2 d_{qe}^{-\eta}$  and  $|\mathbf{r}^\dagger \mathbf{G}'_q|^2 = |\bar{\mathbf{G}}'_q|^2 d_{qe}^{-\eta}$ , where  $\bar{\mathbf{G}}_q$  and  $\bar{\mathbf{G}}'_q$  represent the small-scale fading parts, and are, respectively, scalar and  $1 \times (N_q - 1)$  matrix with i.i.d. standard complex Gaussian entries<sup>7</sup>;  $d_{qe}$  is the distance between Alice <sub>$q$</sub>  and Eve in meters, and  $\eta$  is the path-loss exponent. The secrecy rate is now given by

$$C_q^{sec} = C_q - E_{[d_{qe}, \bar{\mathbf{G}}_q, d_{re}, \bar{\mathbf{G}}_r, \bar{\mathbf{G}}'_q, \bar{\mathbf{G}}'_r]} [C_{eq}] = C_q - E \left[ \log \left( 1 + \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 \gamma_q}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2 \sigma_q + |\mathbf{r}_q^\dagger \mathbf{G}_r|^2 \gamma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2 \sigma_r + N_0} \right) \right] \quad (4.30)$$

where  $E_{[d_{qe}, \dots, \bar{\mathbf{G}}'_r]} [\bullet] \triangleq E_{d_{qe}} \left[ E_{\bar{\mathbf{G}}_q} \left[ \dots \left[ E_{\bar{\mathbf{G}}'_r} [\bullet] \right] \right] \right]$ . We rewrite (4.30) as

$$E_{[d_{qe}, \dots, \bar{\mathbf{G}}'_r]} [C_{eq}] = E_{[d_{qe}, \mathbf{w}_q, d_{re}, \mathbf{Y}_q]} \left[ \log \left| \frac{\mathbf{W}_q \Gamma_{1q} \mathbf{W}_q^H}{\mathbf{Y}_q \Gamma_{2q} \mathbf{Y}_q^H} \right| \right] \quad (4.31)$$

<sup>7</sup>Note that the transmit precoders  $\mathbf{T}_q$  and  $\mathbf{Z}_q$ ,  $\forall q \in \mathcal{Q}$  are unitary matrices that do not change the characteristics of the original channel matrices  $\tilde{\mathbf{H}}_{rq}$ ,  $\tilde{\mathbf{G}}_q$ , and  $\tilde{\mathbf{G}}'_q$  (see (4.2) and Section 4).

where  $\mathbf{W}_q \triangleq [\bar{\mathbf{G}}_q, \bar{\mathbf{G}}_q', \bar{\mathbf{G}}_r, \bar{\mathbf{G}}_r', 1]$ ,  $\mathbf{Y}_q \triangleq [\bar{\mathbf{G}}_q', \bar{\mathbf{G}}_r, \bar{\mathbf{G}}_r', 1]$ , and

$$\Gamma_{1q} = \text{diag} \left\{ \left[ \gamma_q, \sigma_q \underbrace{[1, \dots, 1]}_{N_q-1}, \left( \frac{d_{re}}{d_{qe}} \right)^{-\eta} \gamma_r, \sigma_r \underbrace{[1, \dots, 1]}_{N_r-1} \left( \frac{d_{re}}{d_{qe}} \right)^{-\eta}, d_{qe}^{\eta/2} \sqrt{N_0} \right]^T \right\} \quad (4.32)$$

$$\Gamma_{2q} = \text{diag} \left\{ \left[ \sigma_q \underbrace{[1, \dots, 1]}_{N_q-1} \left( \frac{d_{qe}}{d_{re}} \right)^{-\eta}, \gamma_r, \sigma_r \underbrace{[1, \dots, 1]}_{N_r-1}, d_{re}^{\eta} \sqrt{N_0} \right]^T \right\} \quad (4.33)$$

with  $\text{diag}\{\mathbf{f}^T\}$  representing an  $m \times m$  diagonal matrix whose diagonal entries are the entries of  $\mathbf{f}$  with size  $m$ . The expectation in (4.31) w.r.t.  $\mathbf{W}_q$  and  $\mathbf{Y}_q$  can be efficiently computed using the random matrix result in [110, Appendix A, Lemma 2]. However, according to (4.31)  $C_{eq}$  is still a random variable over the distances  $d_{qe}$  and  $d_{re}$ . Since we were not able to analytically formulate this distribution, we numerically approximate the expectation of  $C_{eq}$  w.r.t. distances. To do this approximation, in simulations, we assume that Eve is uniformly distributed within a circle of a given radius. The center of this circle is determined depending on our simulation scenario (see Section 4.5.2 for more details). A similar idea can be found in [111]. Another example is [112] where the authors assumed that the location of Eve follows a Poisson point process.

Following the same technique used to manipulate (4.31), we take the expectation of (4.18) and end up with:

$$\sigma_q > \frac{(|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r + N_0)}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} E_{[\bar{\mathbf{G}}_q, \bar{\mathbf{G}}_q']} \left[ \frac{|\bar{\mathbf{G}}_q|^2}{|\bar{\mathbf{G}}_q'|^2} \right] - E_{[\bar{\mathbf{G}}_r, d_q, d_r, \bar{\mathbf{G}}_r', \bar{\mathbf{G}}_q']} \left[ \left( \frac{d_{re}}{d_{qe}} \right)^{-\eta} \frac{(|\bar{\mathbf{G}}_r|^2 \gamma_r + |\bar{\mathbf{G}}_r'|^2 \sigma_r + N_0)}{|\bar{\mathbf{G}}_q'|^2} \right]. \quad (4.34)$$

The numerator and the denominator inside the first expectation term in (4.34) correspond

to a central Wishart matrix [113]. The numerator inside the second expectation term corresponds to the quadratic form of a Wishart matrix, which preserves the Wishartness property [114]. Hence, both expectation terms correspond to the ratio of two Wishart matrices. Since we assumed a MIMO single-stream system, all Wishart matrices are in fact scalars. Hence, the expectations in (4.34) can be computed using the result in [115, Section 1]. Computing the expectation w.r.t.  $d_{qe}$ ,  $\forall q$  can be tackled numerically as explained above.

Since (4.30) and (4.34) are computable, we can set  $U_q(s_1, s_2) = E[C^{sec}(\sigma_q)]$ ,  $q \in \{1, 2\}$ , where the expectation is w.r.t. E-CSI components. Hence, the objective function of (4.29) can be defined without knowledge of E-CSI. Hence, we can establish Table 4.1 to solve (4.29). A summary of the procedure to solve (4.29) is given in Algorithm 5 (Line 3 to 14). The solution found after Line 14 for each player is the probability set  $\{\alpha_{i,q}\}_{i=1}^M$ ,  $q = 1, \dots, Q$ . Creating a probabilistic TxPJ power assignment is done by converting the uniform distribution to a probability mass function corresponding to  $\{\alpha_{i,q}\}_{i=1}^M$  for  $q = 1, 2$ , which is as follows [116]: 1) Generate a uniform random variable  $U(0, 1)$ ; 2) Determine the index  $I$  such that  $\sum_{i=1}^{I-1} \alpha_{i,q} \leq U < \sum_{i=1}^I \alpha_{i,q}$ ; 3) Use the TxPJ power  $I\Delta\sigma_q$ . Such a probabilistic TxPJ power assignment must be done several times to approximate the probability mass  $\{\alpha_{i,q}\}_{i=1}^M$ . The expected value of secrecy sum-rate can be calculated by averaging achieved secrecy rates using the probabilistic TxPJ power assignment<sup>8</sup>.

---

<sup>8</sup>Such a procedure for practical implementation of mixed solutions may not be of interest because all probabilistic transmissions have to be done in one channel realization. However, in practical scenarios, the coherence time is not long enough to accommodate more than a few transmissions. We examine this deficiency in the simulation section.

---

**Algorithm 5** Robust Friendly Jamming Control
 

---

**Initialize:**  $0 < \gamma_q < P_q$ ,  $\Delta\sigma_q = \frac{P_q^{jam}}{M} \quad \forall q$

```

1: repeat
2:   for  $q = 1$  to  $2$  do
3:     for  $i = 1$  to  $M$  do
4:       Set  $\sigma_q = i\Delta\sigma_q$ .
5:       Compute  $\sigma_r = \chi_r$ ,  $r \neq q$ .
6:       Compute  $\chi_q$ .
7:       if  $\sigma_q < \chi_q$  then Set  $\alpha_{i,q} = 0$ .
8:       else Compute and store  $U_q(\sigma_q, \sigma_r)$ .
9:       end if
10:    end for    % do the same loop again but change
11:                % line 5 to “Set  $\sigma_r = P_r^{jam}$ ”.
12:     $U_q(\sigma_q) = \max_{\sigma_r} U_q(\sigma_q, \sigma_r)$ .
13:    Find  $\{\alpha_{i,q}\}_{i=1}^M$  by solving (4.29) (with  $U_q(\sigma_q)$  as the summands in the objective function).
14:    end for    % Choose the probability set that maximizes the
15:                % secrecy sum-rate.
16:    for  $q = 1$  to  $2$  do    % Rate adjustment procedure:
17:      if  $C_q < R_q - \epsilon$  then Set  $\gamma_q = \gamma_q + \delta$ .
18:      if  $\gamma_q > P_q$  then Set  $\gamma_q = P_q$ .
19:      end if
20:    else
21:      if  $C_q > R_q + \epsilon$  then Set  $\gamma_q = \gamma_q - \delta$ .
22:      end if
23:    end if
24:    end for    %  $\gamma_q^*$  is found.
25: until  $R_q - \epsilon < C_q < R_q + \epsilon \quad \forall q$ .
  
```

---

Lines 15 to 24 of Algorithm 5 aim at satisfying the rate constraints for both links, i.e., finding  $\gamma_q^*$  mentioned in (4.17). For some choice of  $\delta$  and  $\epsilon$ , as long as the rate requirements are feasible, the linear adjustment used in lines 16 and 20 converges without the need for central control (similar procedure can be found in [117, Algorithm 1]). Hence, this linear adjustment ensures that each link achieves its minimum target rate. If the tar-

get rates are not achievable, then line 17 limits the links to their maximum total transmit powers, i.e., no power will be allocated to TxFJ. The linear adjustments used in line 16 and 20 can be easily added to the price-based game for multiple links in (4.24) as well. Specifically, the loop between lines 3 and 14 can be replaced with the game (4.24). Then, at the convergence point of the game (4.24) or after reaching the maximum iteration number, the rate adjustments in lines 15 and 24 (to satisfy the information rate constraints) can be done for price-based game as well.

#### 4.6 Comparison of Signaling Overhead

In this section, we compare the signaling overhead requirement of our proposed distributed schemes.

In the case of price-based FJ control where the links' actions are defined by (4.24), notice that compared to (4.17), problem (4.24) only sets  $\sigma_q$  as the decision variable. This means that the  $q$ th link is responsible to only find a solution for its own TxFJ power. Each link needs to solve (4.24) and start transmission with the obtained solutions. This makes up one iteration of price-based FJ control. At the next iteration, each link  $q$  needs to recalculate the pricing factor  $\lambda_q$  and update the parameters of its objective function. This update procedure taken before solving individual problems is the *message exchange* phase of our distributed algorithm. Simplifying  $\lambda_q$  in (4.25) we have

$$\lambda_q = \sum_{\substack{r=1 \\ r \neq q}}^Q |\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2 \frac{(1 + \frac{\gamma_r}{a_r}) - 1}{b_r(1 + \frac{\gamma_r}{a_r})} + |\mathbf{r}_r^\dagger \mathbf{G}'_q|^2 \frac{(1 + \frac{\gamma_r}{f_r}) - 1}{g_r(1 + \frac{\gamma_r}{f_r})} \quad (4.35)$$



Method	Utility Functions, $\forall q \in \mathcal{Q}$	# of Players ( $Q$ )	Type of NE (How achieved)	Local optimality of the solution	Amount of Message Exchange $\forall q$
Greedy FJ Control	$C_q^{sec}$	$Q \geq 2$	Pure NE (one-shot)	Not guaranteed	None
Price-based FJ Control (Full E-CSI)	$C_q^{sec} - \lambda_q \sigma_q$	$Q \geq 2$	Pure NE (iterative)	Guaranteed	$b_r, \frac{a_r}{b_r}, d_r, \frac{c_r}{d_r},  \mathbf{d}_r^\dagger \mathbf{H}'_{qr} ^2,  \mathbf{r}_r^\dagger \mathbf{G}'_q ^2 \forall r \neq q, r \in \mathcal{Q}$
Price-based FJ Control (Unknown E-CSI) [49]	$E[C_1^{sec} + C_2^{sec}]$	$Q = 2$	Mixed NE (one-shot)	Guaranteed	$\frac{a_r}{b_r}, E[\log(1 + \frac{c_r}{d_r})], \forall r \neq q, r \in \mathcal{Q}$
	$C_q^{sec}$	$Q \geq 2$	Pure NE (Iterative)	Guaranteed	Same as Price-based FJ control under Full E-CSI + Calculation of Lagrange multipliers to satisfy cooperative jammers' power budgets
[55]	$C_q^{sec}$	$Q \geq 2$	Pure NE (iterative)	Not guaranteed	$b_r, \frac{a_r}{b_r}, d_r, \frac{c_r}{d_r}, \forall r \neq q, r \in \mathcal{Q}$

Table 4.2: Comparison of message exchange requirements for the proposed approaches.

where

$$b_r = \frac{\sum_{t=1, t \neq r}^Q (|\mathbf{d}_r^\dagger \mathbf{H}_{tr}|^2 \gamma_t + |\mathbf{d}_r^\dagger \mathbf{H}'_{tr}|^2 \sigma_t) + N_0}{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2} \quad (4.36)$$

$$g_r = \frac{\sum_{t=1, t \neq r}^Q (|\mathbf{r}_r^\dagger \mathbf{G}_t|^2 \gamma_t + |\mathbf{r}_r^\dagger \mathbf{G}'_t|^2 \sigma_t) + |\mathbf{r}_r^\dagger \mathbf{G}'_r|^2 \sigma_r + N_0}{|\mathbf{r}_r^\dagger \mathbf{G}'_q|^2} \quad (4.37)$$

are interference (plus noise) levels at the  $r$ th link and Eve, respectively. Furthermore, the terms  $\frac{\gamma_r}{a_r}$  and  $\frac{\gamma_r}{f_r}$  are SINR levels at the  $r$ th link and Eve, respectively. From (4.35), one can deduce that to calculate the price in (4.25) and the optimal Tx FJ power in (4.4.2), the  $q$ th link,  $q \in \mathcal{Q}$ , needs to acquire the following: 1) interference and SINR levels at both the  $r$ th link and eavesdropper(s) while eavesdropping on the  $r$ th link,  $r \neq q$ ,  $r \in \mathcal{Q}$ , and 2) the equivalent channel gains (after beamforming) caused from the information and Tx FJ signals of the  $q$ th link on the  $r$ th link and eavesdropper's receptions, i.e.,  $|\mathbf{r}_q^\dagger \mathbf{G}_q|^2$ ,  $|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2$  and  $|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2$ ,  $|\mathbf{r}_r^\dagger \mathbf{G}'_q|^2$ ,  $\forall r \neq q \in \mathcal{Q}$ <sup>9</sup>. On the contrary, a centralized approach aims to solve (4.17) in one shot. This necessitates knowledge of all channel gains between legitimate nodes and eavesdropper(s). By distributing the problem between links in the

<sup>9</sup>Clearly, recalculation of pricing factor and the objective function requires a link to know the eavesdropper's CSI (E-CSI), which is not practical when eavesdroppers are passive nodes. The explanation regarding how to relax such knowledge is discussed in detail in Section 4.4.3.

price-based approach, the problem can be solved iteratively and the message exchange reduces to interference and SINR levels plus a portion of channel gains, which are relatively easier to obtain.

In the greedy FJ control, the price  $\lambda_q = 0, \forall q \in \mathcal{Q}$ . Therefore, there is no need to update the objective function of the  $q$ th link,  $q \in \mathcal{Q}$ , after each iteration because we showed that the maximum available TxFJ power maximizes the secrecy rate of the  $q$ th link in the greedy approach. This greatly reduces the amount of message exchange at the cost of losing the performance.

In Section 4.4.3, we established another framework that relaxes knowledge of E-CSI at legitimate links. Notice that according to Algorithm 5, each link's utility function is set to  $E[C^{sec}]$ , where  $E[\bullet]$  is the expectation over E-CSI. As for the amount of message exchange, this approach requires SINR levels of both links (which is the same as that of price-based scheme) plus the expectation of leaked rate at Eve where the expectation is w.r.t. E-CSI components.

In what follows, we have provided a detailed analysis of the messaging overhead of the techniques in [49, 55, 118] and compare them to ours<sup>10</sup>. One important note about the works in [49, 55] is that both of these works assume full knowledge of E-CSI in their analyses. Hence, we compare these schemes with our price-based FJ method for which full knowledge of E-CSI must be available. We first give a summary of each of these works and then characterize the amount of messaging overhead they impose on the network.

The authors in [49] investigated the secrecy sum-rate maximization problem in an interference network with cooperative jammers. The decision variables for their optimiza-

---

<sup>10</sup>It is difficult to compare our approach to those in [42, 43, 47, 61], as such works differ in the system model and/or optimization variables.

tion problem are the powers of legitimate links and the powers of cooperative jammers. The work in [49] also imposes a constraint on the total power budget of the cooperative jammers. This is a shared constraint between the legitimate links, and cannot be decomposed to enable distributed implementation.

The work in [118] studied power control for a dense network of small cells that coexist with some macrocells. They focused on the uplink communication of small-cell networks and proposed a distributed power optimization to maximize the sum of uplink rates subject to constraints on transmission powers as well as a tolerable interference level at macrocell users. The solution method in [118] closely follows the work in [49]. The constraint on interference level at macrocell users is a shared constraint and cannot be decomposed to enable distributed implementation. Thus, the amount of overhead in [118] is comparable to [49].

The work in [55] considers the Physical-layer security for a multi-channel interference network with full-duplex-enabled nodes. The authors did not assume that Alices are capable of generating TxFJ and only focused on the power allocation of information signals to study the problem of greedy secrecy-rate maximization. They proposed a water-filling-like power allocation to different channels of a given link. While the system model in [55] is quite different from ours in terms of adopting multi-channel and full-duplex communications, due to the greedy nature of this algorithm, we can compare this method to our proposed greedy method. In other words, no pricing model (i.e., any attempt on secrecy sum-rate maximization) was considered in [55]. We found out that the method in [55] requires each link to know the interference and SINR at the receiver as well as the interference and SINR at Eve. In contrast, in our work, due to the adoption of TxFJ, no messaging is needed to implement the greedy algorithm.

Table 4.2 shows a more unified comparison between our methods (greedy FJ control,

price-based FJ control with perfect E-CSI and imperfect E-CSI) and those in [49] and [55] in terms of messaging overhead.

#### 4.7 Numerical Results

We consider a four-link network with one eavesdropper. To assess different aspects of our method, we manipulate the placement of these links as well as the eavesdropper from one simulation to another.

Figure 4.4 (a) shows the probability of convergence of the price-based game in (4.24) under different interference levels. The total power of each Alice is  $P_q = 13$  dBm  $\forall q \in \mathcal{Q}$ . We also set the rate demands such that  $\gamma_q = 10$  dBm  $\forall q \in \mathcal{Q}$ . All interfering distances  $d_{rq}$ ,  $(r, q) \in \mathcal{Q}, r \neq q$  are equal to each other. Also, the direct distance between Alice <sub>$q$</sub>  and Bob <sub>$q$</sub>  is set to  $d_{qq} = 10$  m,  $\forall q \in \mathcal{Q}$ . The path-loss exponent is set to  $\eta = 2.5$ , and  $N_0 = 0$  dBm. We ran the game (4.24) iteratively between all links using the Jacobi iterative method. For each point on a curve in Figure 4.4 (a), we calculate the probability of convergence by counting the number of times that solving (4.24) iteratively for all links converges to a point, and divide this number by a total of 1000 times running the iterative optimization. Each run creates a different realization of small scale-fading components of all channels. The maximum number of iterations was set to 50. We plotted the the probability of convergence of our algorithm vs. the ratio  $\frac{d_{rq}}{d_{qq}}$  for four different locations of Eve. Same as interfering distances, the distance between all Alices and Eve,  $d_{qe}$   $\forall q \in \mathcal{Q}$  are equal to each other.

It can be seen that when Eve is close to Alices, the probability of convergence is very low, such that for  $\frac{d_{rq}}{d_{qq}} = 10$ ,  $\forall (r, q) \in \mathcal{Q}$  only a convergence probability of 0.2 can be expected. The reason is that when Eve is close to Alices, large amounts of Tx FJ is needed to guarantee positive secrecy. In some realizations where the required Tx FJ power exceeds

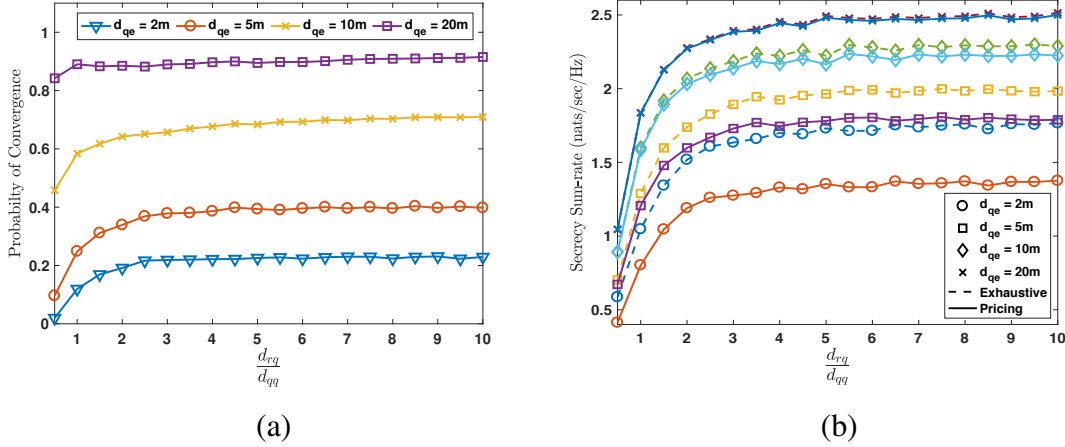


Figure 4.4: (a) Probability of convergence (b) Secrecy sum-rate of price-based FJ control for different interference levels and different Eve locations, ( $Q = 4$ ,  $\frac{P_q}{N_0} = 30$  dB,  $N_q = 5$ ,  $M_q = 4$ ,  $L = 4$ ).

the maximum available power at Alice, achieving positive secrecy for some or all Alices becomes infeasible, which also violates the first condition of Proposition 3. Thus, the NE uniqueness and consequently the convergence of iterations cannot be guaranteed. However, it can be seen that as Eve becomes farther from Alices, the convergence probability increases. Lastly, it can be seen that the second condition in Proposition 3 is not very strict, as for  $\frac{d_{qq}}{d_{rq}} > 3$ , no noticeable improvement in convergence can be seen.

Figure 4.4 (b) shows the resulting secrecy sum-rate of the four curves plotted in Figure 4.4 (a). We compared the performance of our price-based FJ control with that of an exhaustive search method which solves (4.17). All solid/dashed curves show the resulting secrecy sum-rate of the price-based/exhaustive approach<sup>11</sup>. A pair of curves with the same markings show the performance of the two methods for a certain value of  $d_{qe}$ . It can be seen that for a relatively far Eve, which satisfies the first condition of Proposition 3, there is not much difference between the price-based approach and the exhaustive search approach. This indicates that the local optimum point(s) of the secrecy-sum-rate becomes

<sup>11</sup>To do exhaustive search, we discretize Tx/FJ powers of all links to very small increments and find the combination that results in the highest secrecy sum-rate.

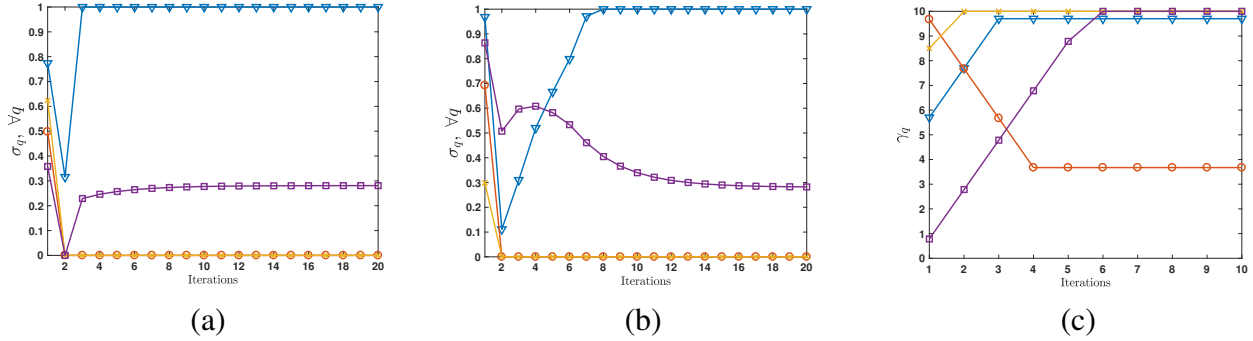


Figure 4.5: Convergence of (a) price-based FJ control (Jacobi Method) (b) price-based FJ control (Gauss-Seidel) (c) rate demands, ( $Q = 4$ ,  $\frac{P_q}{N_0} = 30$  dB,  $N_q = 5$ ,  $M_q = 4$ ,  $L = 4$ )

the global optimum when the conditions of Proposition 3 are satisfied. It should be noted that for both Figure 4.4 (a) and (b), similar results can be obtained if instead of changing the proximity of Eve to Alices, all links adopt high information rate demands.

Figure 4.5 (a) and (b) show the convergence of the TxFJ power of each link for price-based FJ control under Jacobi and Gauss-Seidel methods, respectively. Both figures are plotted in the same channel realization with the same placement of links. The initial TxFJ power is set randomly for each link. Each curve shows the value of TxFJ of a link normalized by the maximum available TxFJ of that link over 20 iterations. Although the Jacobi method was not proved to be convergent in our analyses, we did not find any case where Jacobi method does not follow the same convergence behavior as the Gauss-Seidel method. Furthermore, the Jacobi method was found to be a bit faster in rate of convergence, as all links simultaneously update their TxFJ powers compared to the Gauss-Seidel method in which at each iteration only one link updates its TxFJ power.

Figure 4.5 (c) shows the convergence of the rate adjustment for one channel realization. We randomly initialize  $\gamma_q, \forall q$ , and then the rate adjustments are done the same way as it is shown in lines 15 to 24 of Algorithm 5. The maximum value of  $\gamma_q$  in this simulation is 10 dBm. Each iteration of Figure 4.5 (c) consists of running the game (4.24) until the convergence. Then, the  $q$ th  $q \in \mathcal{Q}$ , link adjusts  $\gamma_q$  by increasing or decreasing

it. During our simulation, we found out that setting  $\delta$  (as the increment of  $\gamma_q$ ) to  $0.2\gamma_q$  gives us a fast and reliable convergence for all links. We terminate these iterations once the information rate of a link is within a tight neighborhood of its rate demand (e.g.,  $0.95R_q < \log(1 + \frac{\gamma_q}{a_q}) < 1.05R_q$ ). It can be seen that the convergence of rate adjustments is fairly quick once a suitable increment for the power of information signal and a suitable neighborhood around rate demands is considered.

Figure 4.6 (a) and (b) show the secrecy sum-rate of the greedy FJ control compared to the price-based FJ control and exhaustive search method for different power constraints of Alices. We assumed that all Alices use the same amount of power constraint. For both figures of Figure 4.6, all  $Q$  links as well as the eavesdropper are randomly placed in a circle, namely, the simulation region with radius  $r_{circ} = 25$  m. The distance between the transmitter and the receiver of each link is set to be a constant  $d_{link} = 5$  m. The required rate demand for each link is set to  $R_q = 2$  nats/sec/Hz,  $\forall q \in Q$ . The maximum number of iteration for both the pricing part and rate adjustment is set to 50. We ran each method for a total of 30 link placements. For each placement, we tested 100 channel realizations. It can be seen that for low transmit powers, the greedy FJ has a comparable secrecy sum-rate to the exhaustive approach, verifying Proposition 5. As the transmit power increases, the secrecy sum-rate of the greedy method becomes more inferior to the exhaustive and pricing approaches, as high interference decreases the information rate of legitimate links, thus lowering the total secrecy in the network.

We see that for the simulation in Figure 4.6 (a) which is a more realistic scenario compared to the settings of Figure 4.4 (b), the price-based FJ control has a comparable performance to the exhaustive search for low transmit powers, indicating that convergence is a less concerning issue in more realistic scenarios. Figure 4.6 (b) shows the same comparison with the difference that now the four links' placements is done in a circle with

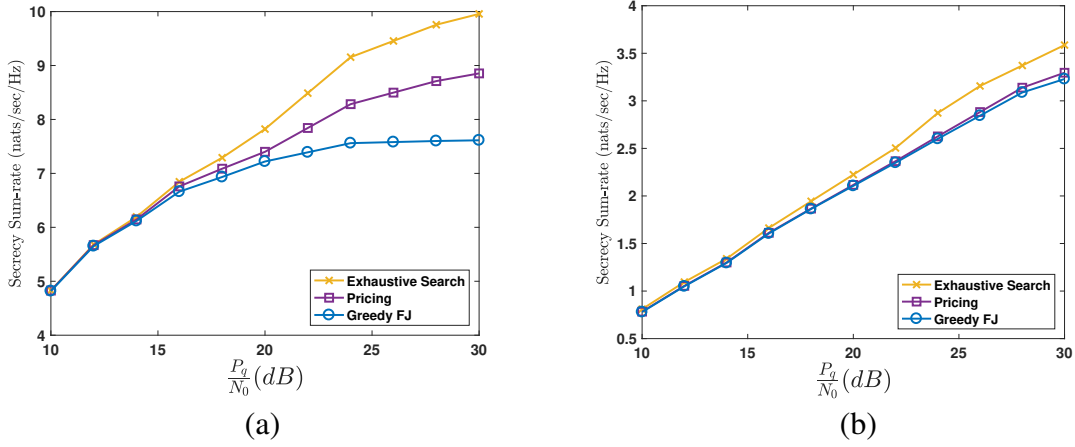


Figure 4.6: Optimality of the greedy FJ control under different scenarios, ( $Q = 4, N_q = 5, M_q = 4, L = 4$ )

$r_{\text{circ}} = 20$  m and  $d_{\text{link}} = 15$  m. It can be seen that the secrecy sum-rate of greedy FJ control is very close to that of the exhaustive search. The reason is that this simulation is done in a denser network in which each link experiences more interference on links and each Bob receives a weaker information signal. Thus, each link has to spend a lot of its power on the information signal to meet its rate demand ( $R_q = 2$  nats/sec/Hz,  $\forall q \in \mathcal{Q}$ ). The rest of the power left for TxFJ is small, forcing each user to spend all the remaining power on TxFJ to preserve positive secrecy. Such network conditions satisfy the conditions of Proposition 4, allowing the greedy FJ control to have a performance close to that of the exhaustive search method.

We now consider a two-link scenario to assess the performance of the price-based game with partial knowledge of E-CSI. In all simulations of this part, the noise floor at both Bobs and at Eve is set to  $N_0 = -50$  dBm. The information rate constraints are chosen such that Alices allocate no more than  $1/3$  of their total transmit powers for the information signal. In all figures, the horizontal axis is the horizontal coordinate for the center of the circle within which Eve is uniformly distributed. Each point on every plot is the result of averaging over 10 random locations for Eve (in order to approximate (4.30))



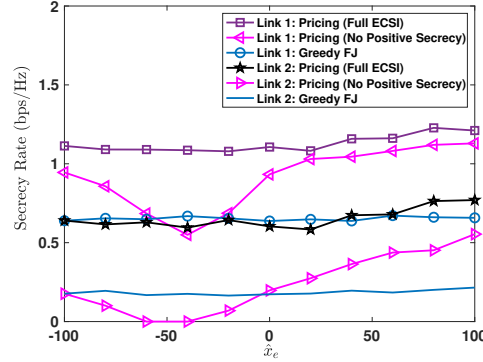


Figure 4.7: Effect of SIC on individual secrecy rates:

( $\text{Alice}_1 = (-50, 10)$ ,  $\text{Bob}_1 = (5, 10)$ ,  $\text{Alice}_2 = (-50, -10)$ ,  $\text{Bob}_2 = (50, 10)$ ,  $\hat{y}_e = 0$ ,  $\hat{r}_e = 10$ ,  $P_q = 0$  dBm,  $N_q = 3$ ,  $M_q = L = 1$ ).

w.r.t. distances). At each random location, 500 channel realizations are simulated and then averaged. We compare the performance of the proposed price-based FJ control under complete/partial knowledge of E-CSI (indicated by “Pricing (Full E-CSI)”/“Robust”) with other methods including when every link allocates all its power to information signal (indicated by “No Jamming”), exhaustive search (indicated by “Exhaustive Search”), and the greedy FJ control (indicated by “Greedy FJ”).

In Figure 4.7, we depict, individual secrecy rates for when constraint (4.18) is taken into account in the price-based FJ control (indicated as “Pricing (Full E-CSI)” and for when it is not (indicated as “Pricing (No Positive Secrecy)”). It can be seen that applying constraint (4.18) in the price-based FJ control significantly affects the secrecy sum-rate such that if it is overlooked, the performance of the price-based FJ control can be even lower than the greedy approach with zero secrecy rate for one or both links at some locations of Eve.

In Figure 4.8 (a), we compare the performance of Algorithm 5 (indicated as “Robust”) with other approaches. The spatial distribution for Eve is the same as in previous

simulation, but with  $P_q = 10$  dBm. For the pricing method with full CSI, transmitters sequentially apply (4.4.2) to optimize their TxFJ powers (i.e., the Gauss-Seidel method is used [107, Chapter 3]). Note that because the performance of the pricing method generally depends on the starting point for the iterative procedure (except for when the conditions of Proposition 3 hold), for each channel realization, the performance of the pricing method is the result of averaging the convergence point of Gauss-Seidel method over 30 different starting points. For the robust TxFJ control algorithm, we use 8 bits to quantize power levels. After finding the probability set  $\{\alpha_{i,q} : i = 1, \dots, M\}$  that maximizes the expected utility in (4.29), probabilistic assignment of the TxFJ powers in robust jamming control is done as follows. The  $q$ th player generates a sample from the probability set  $\{\alpha_{i,q} : i = 1, \dots, M\}$ . Depending on the value of this sample, player  $q$  selects TxFJ power, say  $i\Delta\sigma_q$ , and starts transmitting. This procedure is repeated 50 times per channel realization and the expected utility in (4.29) is approximated by averaging over these repeats. It can be seen that the robust approach is 25% better than the greedy approach. When E-CSI is known, the advantage of price-based FJ becomes more significant.

The expected value in (4.29) must be computed after averaging over several samples of data transmissions for one channel realization. However, in practical scenarios, the coherence time is not long enough to accommodate more than a few transmissions. In order to test this limitation, we compare the performance of robust optimization between 50 data transmissions and 1 data transmission per each channel realization so as to approximate the expected utility in (4.29). To reduce the effect of other parameters on this comparison, we simulated 50 channel realizations at each location of Eve. It can be seen in Figure 4.8 (b) that averaging over 1 data transmission (indicated as “Robust(1)”) does not affect the secrecy sum-rate very much, compared to averaging over 50 data transmissions (indicated as “Robust(50)”). Therefore, the robust jamming control can also be

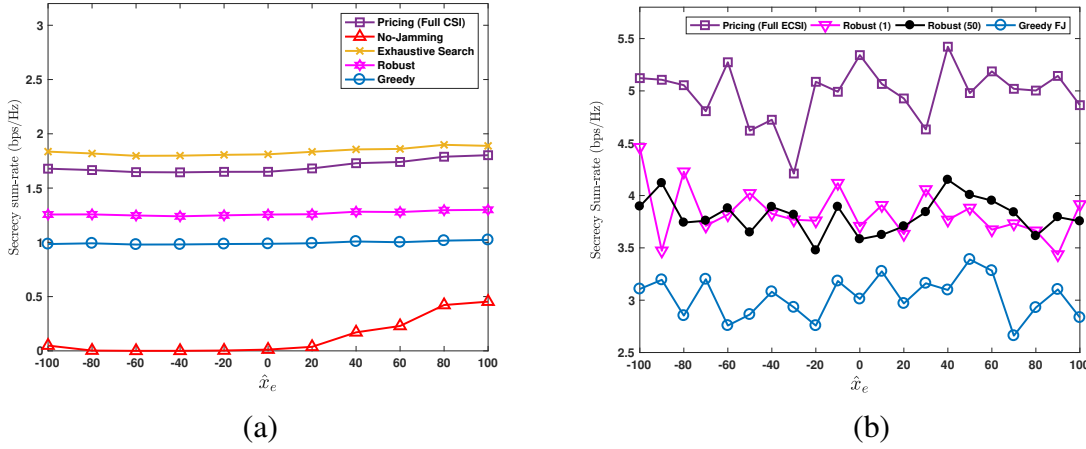


Figure 4.8: Effect of (a) Eve's location (b) number of transmissions on the secrecy sum-rate for two links:

(a) : Alice<sub>1</sub> = (−40, 20), Bob<sub>1</sub> = (40, 20), Alice<sub>2</sub> = (−40, −20), Bob<sub>2</sub> = (40, −20),  $\hat{y}_e = 25$ ,  $\hat{r}_e = 20$ ,  $P_q = 10$  dBm.

(b) : Alice<sub>1</sub> = (−20, 20), Bob<sub>1</sub> = (20, 20), Alice<sub>2</sub> = (−20, −20), Bob<sub>2</sub> = (20, −20),  $\hat{y}_e = 10$ ,  $\hat{r}_e = 20$ ,  $P_q = 10$  dBm.

implemented in channels with low coherence times.

#### 4.8 Software-Defined Radio Implementation of TxFJ for a Single-User Scenario

We implemented a MIMO-capable Alice-Bob link that is tapped by an external multi-antenna Eve. All three nodes are based on National Instruments USRP-2922 software-defined radios. The USRP-2922 is a tunable RF transceiver for streaming baseband signals to a host PC over Ethernet port using any carrier frequency from 400 MHz to 4.4 GHz and the maximum bandwidth of 20 MHz. It can be used for experimentation in a plethora of applications such as WiFi, WiMax, and 2.4GHz industrial, scientific and medical (ISM) band transceivers. Each USRP-2922 device has one receiving chain and one transmitting chain. Thus, for MIMO transmission/reception, several USRP-2922 devices should be connected together via a proprietary MIMO cable. There is also limited ability to simultaneously transmit and receive over the two chains. However, more

self-interference suppression is required to enable in-band full-duplex capability in these devices.

In our experiment, each of Alice, Bob and Eve has two antennas. For simplicity, single-carrier transmission was implemented between Alice and its corresponding Bob. We used carrier frequency of 2.4 GHz and instantaneous bandwidth of 1MHz for signal transmission. The LabView program written for this experiment covers the essential PHY-layer tasks required to enable an end-to-end MIMO communication, such as frame synchronization (finding the beginning of a frame), channel estimation, pulse-shaping, precoding and decoding. To simplify the process of phase/frequency offset estimation, we used one of the Ettus' centralized clock generators, namely Ettus OctoClock, to provide synchronous and coherent carrier frequencies for Alice, Bob and Eve. Note that providing a coherent and synchronous carrier for Eve is one aspect of realizing the worst-case scenario where Eve has the same PHY-layer abilities as the legitimate nodes. In our initial experiments reported here, Bob and Eve are both located 3'5" away from Alice, respectively. Both Bob and Eve have a line of sight (LoS) to Alice. Figure 4.9 shows our experimental setup.

To keep her transmission secret from Eve, Alice creates a bogus signal, known as TxFJ, along with her secret message to confuse Eve. This TxFJ signal is created in a way that does not affect Bob's reception. To do that, same as what is explained in Section 4 Alice uses precoding such that the TxFJ signal falls in the null space of the channel between herself and Bob. To enable precoding and subsequently creating the TxFJ signal, Alice must acquire the channel estimate between herself and Bob. Bob also needs the channel estimate to perform equalization. As another aspect of the worst-case scenario, we assume Eve is also able to perform equalization, to recover the secret message of Alice. Hence, Eve has the ability to acquire the estimate of the channel between herself

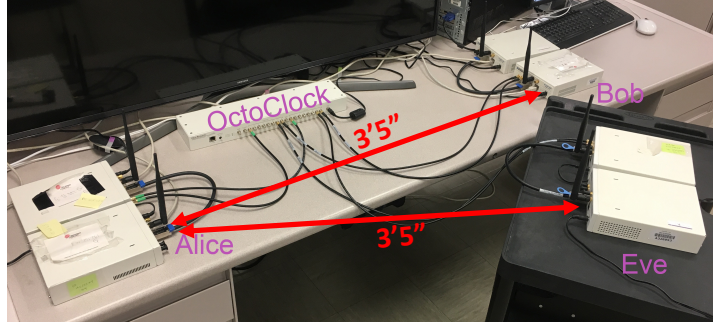


Figure 4.9: Experimental setup for TxFJ in a single-link scenario.

and Alice.

To estimate the CSI between Alice and Bob, pilot sequences were sent at the beginning of each packet. CSI estimates obtained at Bob are fed back to Alice for precoding and design of TxFJ signal. Each pilot sequence consists of 8 known BPSK symbols. The pilot sequences assigned to each of the two antennas are orthogonal to each other. To ensure accurate channel estimation, 20 repetitions of the same assigned pilot sequence are concatenated and used to produce a “training packet”. One training packet is prepended to each data packet, as described later on. CSI estimation is performed for each pilot repetition and the final channel estimate for the given Tx-Rx pair is taken as the average over all 20 repetitions. Our chosen method of estimation is the minimum mean-square estimation (MMSE). The MMSE method is an unbiased estimation technique that mainly focuses on minimizing the variance of the estimation error. The MMSE method is more robust to signal strength variations when compared to the least-squares estimation method because it takes into account the noise perturbations in its design procedure.

No encryption was done for pilot symbols, so Eve is also able to estimate the channel between herself and Alice. This way, Eve can choose from a variety of powerful detection

and estimation techniques that rely on acquired Alice-Eve CSI to eavesdrop on legitimate communications. Although representing a worst-case scenario, facilitating channel estimation for Eve allows us to identify any limitations in our design. In fact, considering a strong eavesdropping scenario such as ours not only enables us to obtain a lower bound on the performance of our techniques, but also helps us correct our design to cope with less stringent environments. The secret information message transmitted from Alice to Bob is a 512-by-512 (in pixels) image, with each pixel represented by 8 bits. The image is transmitted as QPSK symbols at a symbol rate of 1 M symbols/sec.

Each training packet is prepended to a data packet to construct one data-link frame. The size of a data packet can vary depending on the coherence time of the propagation environment. In our case, to ensure an up-to-date channel estimate in most environments, we let the data packet consist of 1000 QPSK symbols. For simplicity, data packets are always transmitted using QPSK. The training packets are also exploited for frame synchronization. In fact, because the pilot sequences are globally known, then Bob (Eve) can cross-correlate a sample training packet with the frames he (she) receives. Over a period of a data frame, the time when the result of the cross-correlation has the maximum value marks the beginning of a frame.

Each antenna transmits at Tx power of 20 dBm (100 mW). Due to the non-linearity of the power amplifier of the USRPs, we kept the total transmit power fixed at this value. However, we varied the power assignment between the TxFJ and information signals. In some of our experiments, we kept the power assignment of information signal fixed at half of the total transmit power and varied the power allocated to TxFJ from zero to the half of the transmit power. This way, we can keep the power of information rate fixed at a given value and vary the power of TxFJ signal. The TxFJ signal is designed in a way to not interfere with the information signal. Specifically, we used MIMO precoding, so

that the TxFJ signal falls in the null space of the channel between Alice and Bob, thus not affecting Bob's reception. Each stream of the information and TxFJ signals occupies one degree of freedom (DoF) to be transmitted from Alice. Because in our experiment Alice has two antennas (thus two DoFs), we can only send a single-stream information signal and a single-stream TxFJ signal to fully exploit Alice's DoFs for both data transmission and secrecy. To enable spatial multiplexing (i.e., sending multi-stream information signals to achieve multiples of the single-stream information rate), more than two antennas are needed. Our experimental testbed can be easily extended to cover multi-stream cases as well.

We observed that given a fixed power for information signal, the secret message was transmitted error-free regardless of the amount of power allocated to the TxFJ signal. This means that the FJ signal was nullified at Bob perfectly. However, Eve could not in general nullify the effect of FJ on itself. At low power for FJ (below 20% of the transmit total power), Eve was still able to decode the secret message despite receiving a less clean signal compared to Bob. However, for a sufficiently high FJ power (e.g., above 30% of the total transmit power), Eve was not able to decode any of Alice's transmitted packets, despite its closer distance to Alice than Bob. Exemplary received constellations at both Bob and Eve are shown in Figure 4.10.

We then observed the effect of channel estimation on the nullification of FJ at Bob by using different types of pilot signals. It turned out for some pilot signals, the FJ is not nullified completely thus increasing the BER at Bob. We also observed that in an office room, the wireless channel always exhibits rich-scattering behavior. The absence of rich-scattering environment creates the so-called "vulnerability zone" around Bob. This zone can span several wavelengths around the Bob, and if Eve is placed anywhere in this zone, Alice-Bob and Alice-Eve channels would become similar to each other. The immediate

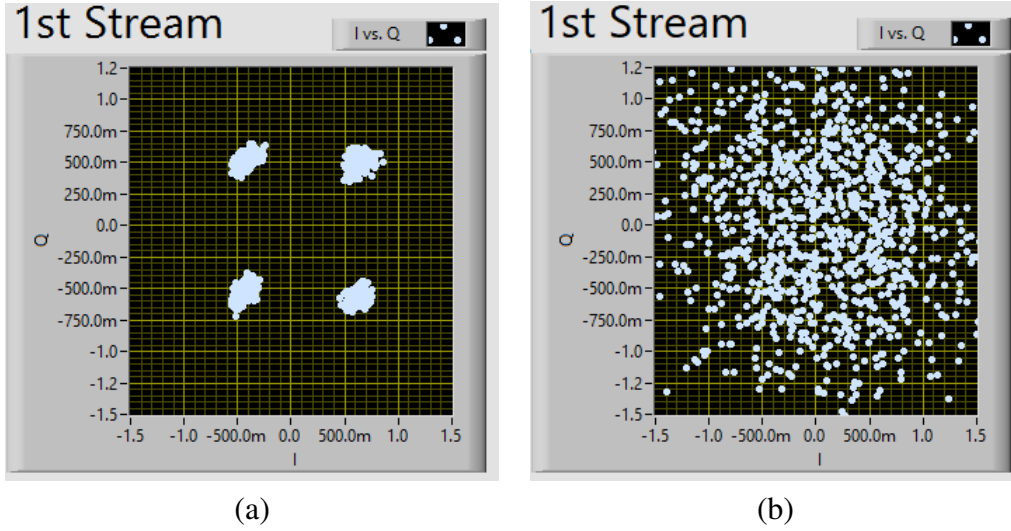


Figure 4.10: Received QPSK constellation on (a) Bob (b) Eve, with half of total power allocated to TxFJ.

result of such similarity is that the null spaces of Alice-Bob and Alice-Eve channels becomes similar to each other. Hence, the FJ signal created at Alice would be nullified at both Eve and Bob, causing Eve to receive a clean signal without any disturbance from FJ.

In previous studies in literature, it has been reported that the area of the vulnerability zone at ISM frequency bands can span up to 10 wavelengths around Bob. However, we found out that the real-world wireless channel of an office room precludes the presence of the vulnerability zone, such that even if Eve is placed extremely close to Alice the FJ still affects Eve's receptions. Tables 4.3 and 4.4 show the symbol-error-rate (SER) results that are achieved by placing Eve in different locations. As mentioned earlier, Bob and Eve are both located 3'5" away from Alice. For each experiment, Eve is placed according to one of the settings shown in Figure 4.11. For SNR variation, we added an AWGN signal to the digital transmit signal at Alice side. The reason for doing so is that changing the transmit power of USRP may not be possible due nonlinearities in power amplifier. Hence, we vary the SNR by keeping the transmit power constant and changing the amount of AWGN



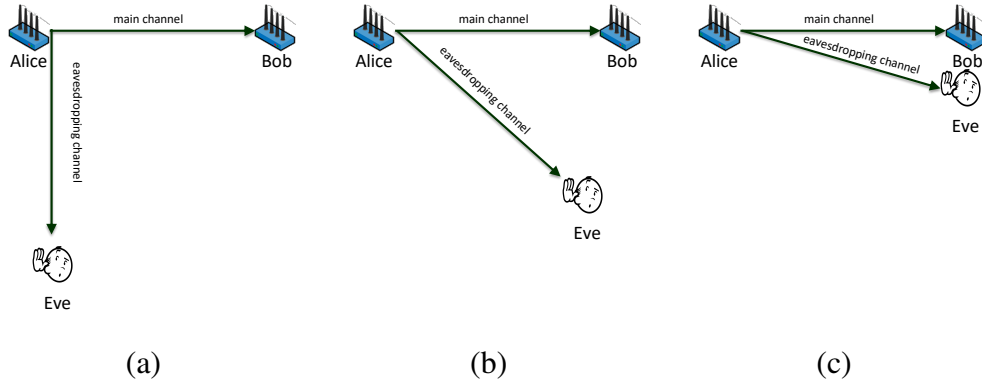


Figure 4.11: Placements of Eve for experiment: (a)  $90^\circ$ , (b)  $45^\circ$ , (c)  $10^\circ$ .

SNR	SER for $90^\circ$	SER for $45^\circ$	SER for $10^\circ$
6	0.479282	0.556779	0.617551
8	0.271464	0.365629	0.345778
10	0.036926	0.068769	0.068504
12	0.013100	0.010599	0.015118
14	0.001448	0.002469	0.004381

Table 4.3: SER of the main channel for different Eve placements.

SNR	SER for $90^\circ$	SER for $45^\circ$	SER for $10^\circ$
6	0.817053	0.790755	0.814479
8	0.720394	0.926080	0.907803
10	0.771758	0.704939	0.792374
12	0.770608	0.811839	0.843291
14	0.720957	0.735692	0.745816

Table 4.4: SER of the eavesdropping channel for different Eve placements.

noise from Alice side. Because of the close distance between USRPs, the additive noise at the receive (i.e., Bob or Eve) is negligible, so the AWGN noise at Alice side controls the SNR value. It can be seen from both tables that first the SER at Eve remains high despite the increase in SNR. Second, such SERs at Eve seem to not depend on Eve's placement, even when Eve is resided very close to Bob (see results for " $10^\circ$ ").

Another important observation that was made in our simulations was the effect of LoS on our results. Specifically, in simulations we noticed that under Rayleigh fading (i.e., no

LoS), even in the absence of FJ, Eve still requires complete knowledge of the channel between Alice and Bob (i.e., legitimate channel) to successfully decode the secret message. Without such knowledge, Eve still has a high BER. This is related to the beamforming of the information signal at Alice, which increases the directionality of Alice's transmission to Bob. Hence, Eve must know where Alice beam is pointed to in order to perform better equalization. However, in a Rician fading environment, where LoS exists between Alice and Eve, Eve only has to know the channel between herself and Alice. The reason for such phenomenon is that the LoS component makes the legitimate channel and Alice-Eve channel comparable to each other (provided that Eve is reasonably close to Bob).

#### **4.9 Summary**

In this chapter, we studied distributed design of FJ control in a MIMO wiretap interference network. We showed that greedy FJ is not an optimal approach in terms of total network secrecy rate. Accordingly, we designed a price-based TxFJ control that guarantees a local optimum point in maximizing the secrecy sum-rate. Through simulations, we observed a noticeable improvement in the secrecy sum-rate when pricing is leveraged for FJ control. We then introduced uncertainty in E-CSI and designed a robust method. We showed via simulations that the robust method achieves a higher secrecy sum-rate than the greedy FJ approach.

## CHAPTER 5

## **Distributed Asynchronous Power Control for TxFJ and RxFJ**

### **5.1 Overview**

In this chapter, we study PHY-layer security in a wiretap interference network where both TxFJ and RxFJ are utilized by each link. Our design parameters are the RxFJ power, and the power assignment (PA) between the information and TxFJ signals. The joint optimization of these parameters is a non-convex, computationally intractable problem. To address it, instead we seek sub-optimal solutions but distributed solutions that can be implemented by individual links.

Our work is motivated by the following simple observation: For a given link, when no secrecy is required, the higher the power budget at Alice, the higher is the information rate at the intended receiver (Rx). However, when secrecy is also a requirement, although information rate still increases monotonically with Alice's power, secrecy rate may not necessarily behave as such because more power transmitted from Alice also increases the leakage rate at Eve. Using this observation, we find a lower bound on TxFJ power above which positive secrecy is achievable for a given link. Once positive secrecy is achieved, secrecy rate becomes a monotonically increasing function of Alice's power, thus having the same trend as information rate. Therefore, the rest of Alice's power can be allocated to information signal.

Although guaranteeing positive secrecy does not offer any sort of optimality in terms of individual or network-wide secrecy, it ensures that no link experiences zero secrecy. In contrast, when the aim is to maximize the sum of secrecy rates, we cannot ensure that every link achieves a non-zero secrecy rate [65]. A zero secrecy scenario can be exploited by Eve, who can perform sophisticated multiuser detection techniques (e.g., successive interference cancellation or SIC) to decode ongoing communications. Such an issue was reported in [42], and it was shown in [66] that an SIC-capable Eve can significantly decrease the network secrecy if some links experience zero secrecy rates. By ensuring that every link achieves a non-zero secrecy rate, Eve cannot apply SIC<sup>1</sup>.

We assume that when legitimate nodes set their transmission parameters, there is no centralized authority responsible for computations and optimization. Hence, links have to make distributed decisions. Such a design inevitably produces interference at several links. However, because Eve also receives interference from all links, a careful design ensures that interference at legitimate links is properly managed while interference at Eve is kept high as much as possible. We model these interactions between legitimate links using the theory of non-cooperative games.

The works in [43, 46, 119] studied secure precoding in wiretap interference networks. Moreover, the authors in [55] studied power control in a multi-channel interference network without considering TxFJ and RxFJ. All of these works assumed that Alice has full knowledge of the eavesdropper's channel state information (E-CSI), which may not be a practical assumption. Regarding the power assignment between the information and TxFJ signals, the works in [71] and [120] focused only on a single-link scenario, and their approaches are not extendable to the case of multiple links. The authors of [56] exploited

---

<sup>1</sup>A full description of the effect of a zero secrecy rate on the secrecy of an interference network was given in Section 4, where we showed that Eve can cancel the interference coming from links with zero secrecy rates, thus increasing her received SINR.

full-duplex capability at the base station of a broadcast/multiple-access wiretap channel to secure multiple half-duplex downlink and uplink users by generating RxFJ/TxFJ for uplink/downlink communications. They proposed a multi-objective optimization framework to find the best tradeoff in minimizing downlink and uplink powers, subject to certain constraints on information and secrecy rates of downlink and uplink users. Furthermore, in [121] the case of imperfect knowledge of Alice-Eve channel was modeled using elliptic uncertainty, which assumes there is a bounded error in the knowledge of E-CSI. While this assumption helps to gain tractable results, it is not always practical to make because knowledge of the error bound might be difficult to acquire. In contrast, we assume that only the distribution of the E-CSI is known to Alices.

Overall, our contributions can be summarized as follows:

- Using TxFJ and RxFJ, we define a lower bound on the power allocated to the TxFJ that guarantees positive secrecy for each given link.
- We propose a non-cooperative game to model a power control problem. Assuming first that Alice-/Bob-Eve channels are fully known, we derive sufficient conditions under which the proposed non-cooperative game admits a unique NE.
- We propose alternative sufficient conditions for the uniqueness of the NE. Such conditions allow for predicting the existence of a unique NE in a distributed fashion.
- We show that our distributed design can be implemented using an asynchronous update algorithm. This algorithm is robust to transmission delays over various links.
- Lastly, we relax the assumption of full knowledge of E-CSI at each Alice and propose a version of our algorithm that is robust to uncertainties in knowledge of E-CSI.

Same as previous chapter, we first propose the distributed design under full knowledge of E-CSI to build foundations for our distributed algorithm and establish important performance metrics. After conducting such analysis, we then relax knowledge of E-CSI and propose a version of our algorithm that is robust to uncertainties in E-CSI knowledge.

## 5.2 System Model

We first describe a model for the network under consideration and introduce the main performance metrics. Due to the use of RxFJ in this chapter, we require to re-introduce the basic notations for a better flow of this chapter. Consider  $Q$  transmitters ( $Q \geq 2$ ), Alice<sub>1</sub>, ..., Alice<sub>Q</sub>, that communicate with their respective receivers, Bob<sub>1</sub>, ..., Bob<sub>Q</sub>. Let  $\mathcal{Q} \triangleq \{1, 2, \dots, Q\}$ . Alice<sub>q</sub>,  $q \in \mathcal{Q}$ , has  $N_q$  transmit antennas, and Bob<sub>q</sub> has  $M_q$  antennas. A passive Eve with  $L$  antennas is also present in the communication range<sup>2</sup>. The received signal at Bob<sub>q</sub> is

$$\mathbf{y}_q = \tilde{\mathbf{H}}_{qq} \mathbf{u}_q + \sqrt{\tau_q} \mathbf{H}'_{qq} \mathbf{m}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\tilde{\mathbf{H}}_{rq} \mathbf{u}_r + \mathbf{H}'_{rq} \mathbf{m}_r) + \mathbf{n}_q \quad (5.1)$$

where  $\tilde{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$ ,  $r \in \mathcal{Q}$ , is the  $M_q$ -by- $N_r$  complex channel matrix between Alice<sub>r</sub> and Bob<sub>q</sub>,  $\mathbf{u}_q \in \mathbb{C}^{N_q}$  is the transmitted signal from Alice<sub>q</sub>,  $\tau_q \in \mathbb{R}^+$  and  $\mathbf{H}'_{qq} \in \mathbb{C}^{M_q \times M_q}$  are, respectively, the positive-real-valued self-interference-suppression (SIS) factor and the self-interference channel at Bob<sub>q</sub> due to imperfect SIS<sup>3</sup>. This self-interference model was adopted in several works (see [56, 122]), and practical implementations of it ex-

<sup>2</sup> $L$  can be assumed to be large enough to represent multiple multi-antenna colluding eavesdroppers [22]. However, for ease of presentation, we consider the  $L$ -antenna Eve as a single entity.

<sup>3</sup>In-band full-duplex communications requires suppression of the transmitted signal of the FD-enabled device at its receive chain to allow for simultaneous transmission and reception. However, such suppression may not be perfect, leading to residual self-interference at the receive chain [29].

ist in the literature (see e.g., [31])<sup>4</sup>.  $\mathbf{m}_r \in \mathbb{C}^{M_r}$ ,  $r \in \mathcal{Q}$  is the RxFJ signal created by Bob<sub>*r*</sub>, which is a zero mean circularly symmetric complex Gaussian random variable (ZMCSCG-RV) with covariance matrix of  $E[\mathbf{m}_r \mathbf{m}_r^\dagger] = p'_r \mathbf{I}$  where  $p'_r$  is RxFJ power.  $\text{Tr}(\mathbf{m}_q \mathbf{m}_q^\dagger) = M_q p'_q \leq P'_q$  where  $P'_q$  denotes the power limit at Bob<sub>*q*</sub> for RxFJ.  $\mathbf{H}'_{rq} \in \mathbb{C}^{M_q \times M_r}$ ,  $r \neq q$ , is the channel from Bob<sub>*r*</sub> to Bob<sub>*q*</sub> because the RxFJ created by other Bobs interfere with Bob<sub>*q*</sub>'s reception.  $\mathbf{n}_q \in \mathbb{C}^{M_q}$  is the complex additive white Gaussian noise (AWGN) whose covariance matrix is  $E[\mathbf{n}_q \mathbf{n}_q^\dagger] = N_0 \mathbf{I}$  with  $N_0 \in \mathbb{R}^+$ . We assume  $\tilde{\mathbf{H}}_{rq} = \bar{\mathbf{H}}_{rq} d_{rq}^{-\eta/2}$ , where  $\bar{\mathbf{H}}_{rq} \in \mathbb{C}^{M_q \times N_r}$  represents the small-scale fading,  $d_{rq}$  is the distance between Alice<sub>*r*</sub> and Bob<sub>*q*</sub> in meters, and  $\eta$  is the path-loss exponent. The same equivalent assumption holds for  $\mathbf{H}'_{rq}$ ,  $r \neq q$ , i.e.,  $\mathbf{H}'_{rq} = \bar{\mathbf{H}}'_{rq} d'_{rq}{}^{-\eta/2}$  where  $\bar{\mathbf{H}}'_{rq} \in \mathbb{C}^{M_q \times M_r}$  and  $d'_{rq}$  is the distance from Bob<sub>*r*</sub> to Bob<sub>*q*</sub>.

The received signal at Eve is

$$\mathbf{z} = \tilde{\mathbf{G}}_q \mathbf{u}_q + \mathbf{G}'_q \mathbf{m}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\tilde{\mathbf{G}}_r \mathbf{u}_r + \mathbf{G}'_r \mathbf{m}_r) + \mathbf{e} \quad (5.2)$$

where  $\tilde{\mathbf{G}}_q \in \mathbb{C}^{L \times N_q}$ ,  $q \in \mathcal{Q}$  denotes, the complex channel matrix between Alice<sub>*q*</sub> and Eve. Let  $\tilde{\mathbf{G}}_q = \bar{\mathbf{G}}_q d_{qe}^{-\eta/2}$ , where  $\bar{\mathbf{G}}_q \in \mathbb{C}^{L \times N_q}$  and  $d_{qe}$  is the distance between Alice<sub>*q*</sub> and Eve.  $\mathbf{G}'_q \in \mathbb{C}^{L \times M_q}$  is the channel between Bob<sub>*q*</sub> and Eve, and  $\mathbf{G}'_q = \bar{\mathbf{G}}'_q d'_{qe}{}^{-\eta/2}$  where  $\bar{\mathbf{G}}'_q \in \mathbb{C}^{L \times M_q}$  and  $d'_{qe}$  is the distance from Bob<sub>*q*</sub> to Eve. Finally,  $\mathbf{e}$  has the same statistical characteristics as  $\mathbf{n}_q$ . For Alice<sub>*q*</sub>,  $q \in \mathcal{Q}$ , its transmitted signal  $\mathbf{u}_q = \mathbf{s}_q + \mathbf{w}_q$  consists of the information signal  $\mathbf{s}_q$  and TxFJ  $\mathbf{w}_q$ . We only consider the case of single-stream data transmission using multiple antennas. That is, we set  $\mathbf{s}_q \triangleq \mathbf{T}_q x_q$ , where  $\mathbf{T}_q \in \mathbb{C}^{N_q}$  is the precoder and  $x_q \in \mathbb{C}$  is the information signal. In other words, we use multiple

---

<sup>4</sup>We assume that FD receivers are not experiencing dynamic range issues (as pointed out in [123]), that cause the additive noise at the receive chain to be dependent on the transmit power of the FD device. Relaxing this assumption is a subject for future research.

transmit and receive antennas at each link to achieve MIMO-diversity gain, and spatial-multiplexing gain, i.e., multiple antennas are used for *beamforming*<sup>5</sup>.

Assume that a Gaussian codebook is used for  $x_q$ , i.e.,  $x_q$  is distributed as a ZMCSCG-RV with  $E[x_q x_q^\dagger] = \phi_q P_q$ , where  $P_q$  is the total transmit power of Alice <sub>$q$</sub>  and  $0 \leq \phi_q \leq 1$  is the fraction of transmit power allocated to the information signal. For the TxFJ, we write  $\mathbf{w}_q \triangleq \mathbf{Z}_q \mathbf{v}_q$ , where  $\mathbf{Z}_q \in \mathbb{C}^{N_q \times (N_q - 1)}$  is the precoder for the TxFJ signal and  $\mathbf{v}_q \in \mathbb{C}^{(N_q - 1)}$  is the TxFJ signal with i.i.d. ZMCSCG entries and  $E[\mathbf{v}_q \mathbf{v}_q^\dagger] = \sigma_q \mathbf{I}$ . The scalar value  $\sigma_q = \frac{(1 - \phi_q) P_q}{N_q - 1}$  denotes the TxFJ power<sup>6</sup>. Let  $\tilde{\mathbf{H}}_{qq} = \mathbf{U}_q \Sigma_q \mathbf{V}_q^\dagger$  denote the singular value decomposition (SVD) of  $\tilde{\mathbf{H}}_{qq}$  where  $\Sigma_q$  is the diagonal matrix of singular values in descending order, and  $\mathbf{U}_q$  and  $\mathbf{V}_q$  are left and right matrices of singular vectors, respectively. We set  $\mathbf{Z}_q = \mathbf{V}_q^{(2)}$  where  $\mathbf{V}_q^{(2)}$  denotes the matrix of  $N_q - 1$  rightmost columns of  $\mathbf{V}_q$  corresponding to the smallest singular values [22]. We assume that Alice <sub>$q$</sub>  knows  $\tilde{\mathbf{H}}_{qq}$ <sup>7</sup>. The information signal precoder  $\mathbf{T}_q$  is set to  $\mathbf{T}_q = \mathbf{V}_q^{(1)}$ , where  $\mathbf{V}_q^{(1)}$  is the first column of  $\mathbf{V}_q$  corresponding the largest singular value, achieving the maximum transmit-diversity gain [72]. Let  $\mathbf{H}_{qq} \triangleq \tilde{\mathbf{H}}_{qq} \mathbf{V}_q^{(1)}$ ,  $\mathbf{H}_{jq} \triangleq \tilde{\mathbf{H}}_{jq} \mathbf{V}_q^{(2)}$ ,  $\mathbf{H}_{qr} \triangleq \tilde{\mathbf{H}}_{qr} \mathbf{V}_q^{(1)}$ ,  $\mathbf{H}_{jqr} \triangleq \tilde{\mathbf{H}}_{jqr} \mathbf{V}_q^{(2)}$ ,  $\mathbf{G}_q \triangleq \tilde{\mathbf{G}}_q \mathbf{V}_q^{(1)}$ , and  $\mathbf{G}_{jq} \triangleq \tilde{\mathbf{G}}_q \mathbf{V}_q^{(2)}$ . The terms  $\mathbf{G}_q$  and  $\mathbf{G}_{jq}$ ,  $\forall q \in \mathcal{Q}$ , denote the E-CSI

<sup>5</sup>Later on, we explain the rationale behind this choice.

<sup>6</sup>Notice that the TxFJ power is distributed uniformly between various dimensions of  $\mathbf{v}_q$ . In the case of full knowledge of E-CSI, such power division is not optimal. However, when no knowledge of E-CSI is available (which we assume later in this chapter), it was shown that uniform distribution of TxFJ power among different dimensions of  $\mathbf{v}_q$  is optimal (see [22, 71]).

<sup>7</sup>Acquiring channel state information (CSI) between Alice <sub>$q$</sub>  and its corresponding Bob <sub>$q$</sub>  is assumed to be done securely. For example, a two-phase channel estimation can be performed, where in the first/second time-slot, Alice <sub>$q$</sub> /Bob <sub>$q$</sub>  sends the pilot signals to Bob <sub>$q$</sub> /Alice <sub>$q$</sub> . This way, we avoid having to send explicit CSI feedback from one communication end to another, thus lowering the probability of eavesdropping on channel estimates.



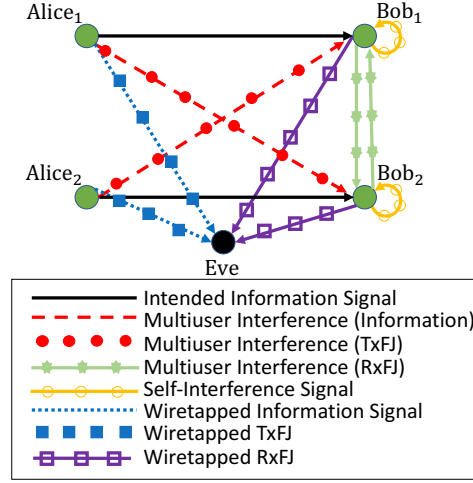


Figure 5.1: System model.

components. Hence, (5.1) and (5.2) can be written as

$$\mathbf{y}_q = \mathbf{H}_{qq}x_q + \mathbf{H}_{jq}\mathbf{v}_q + \sqrt{\tau_q}\mathbf{H}'_{qq}\mathbf{m}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{H}_{rq}x_r + \mathbf{H}_{jr}\mathbf{v}_r + \mathbf{H}'_{rq}\mathbf{m}_r) + \mathbf{n}_q \quad (5.3a)$$

$$\mathbf{z} = \mathbf{G}_q x_q + \mathbf{G}_{jq} \mathbf{v}_q + \mathbf{G}'_q \mathbf{m}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{G}_r x_r + \mathbf{G}_{jr} \mathbf{v}_r + \mathbf{G}'_r \mathbf{m}_r) + \mathbf{e}. \quad (5.3b)$$

An illustration of the system model under study is given in Figure 5.1 for a two-link network. It can be seen that the interference components at each Bob include his self-interference signal as well as information, TxFJ, and RxFJ signals of the other link. Eve also receives all information, TxFJ, and RxFJ signals.

After receiving  $\mathbf{y}_q$  at Bob<sub>*q*</sub>, a linear receiver  $\mathbf{d}_q \in \mathbb{C}^{M_q}$  is applied. Assuming that  $\mathbf{d}_q^\dagger \mathbf{H}_{jq} \mathbf{v}_q = 0$ <sup>8</sup>, an estimate of  $x_q$  is given by:

$$\hat{x}_q = \mathbf{d}_q^\dagger \left( \mathbf{H}_{qq}x_q + \sqrt{\tau_q}\mathbf{H}'_{qq}\mathbf{m}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{H}_{rq}x_r + \mathbf{H}_{jr}\mathbf{v}_r + \mathbf{H}'_{rq}\mathbf{m}_r) + \mathbf{n}_q \right). \quad (5.4)$$

<sup>8</sup>Note that the choice of the linear receiver (to be discussed near the end of this section) affects this assumption. In this chapter, we choose the linear receiver so that this assumption holds.

Hence, the information rate for the  $q$ th link is expressed as:

$$C_q \triangleq \log\left(1 + \frac{\phi_q P_q}{a_q + b_q p'_q}\right) \quad (5.5)$$

where

$$a_q \triangleq \frac{\sum_{\substack{r=1 \\ r \neq q}}^Q \left( |\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \phi_r P_r + |\mathbf{d}_q^\dagger \mathbf{H}_{jr q}|^2 \sigma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 p'_r \right) + N_0}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \quad (5.6a)$$

$$b_q \triangleq \tau_q \frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}. \quad (5.6b)$$

Eve also applies a linear receiver  $\mathbf{r}_q \in \mathbb{C}^L$  while eavesdropping on  $q$ th link's signal to obtain the following estimate of  $x_q$

$$\hat{z}_q = \mathbf{r}_q^\dagger \left( \mathbf{G}_q x_q + \mathbf{G}_{jq} \mathbf{v}_q + \mathbf{G}'_q \mathbf{m}_q + \sum_{\substack{r=1 \\ r \neq q}}^Q (\mathbf{G}_r x_r + \mathbf{G}_{jr} \mathbf{v}_r + \mathbf{G}'_r \mathbf{m}_r) + \mathbf{e} \right). \quad (5.7)$$

Thus, the rate at Eve while eavesdropping on Alice <sub>$q$</sub>  (i.e., leaked rate of Alice <sub>$q$</sub>  at Eve) is

$$C_{eq} \triangleq \log\left(1 + \frac{\phi_q P_q}{c_q + d_q p'_q}\right) \quad (5.8)$$

where

$$c_q \triangleq \frac{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}| \sigma_q}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} + \frac{\sum_{\substack{r=1 \\ r \neq q}}^Q \left( |\mathbf{r}_q^\dagger \mathbf{G}_r|^2 \phi_r P_r + |\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2 \sigma_r + |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2 p'_r \right) + N_0}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \quad (5.9a)$$

$$d_q \triangleq \frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}. \quad (5.9b)$$

Finally, the secrecy rate of Alice<sub>q</sub> can be written as<sup>9</sup>

$$C_q^{sec} \triangleq \max\{C_q - C_{eq}, 0\}. \quad (5.10)$$

The linear receivers  $\mathbf{d}_q$  and  $\mathbf{r}_q$ ,  $q \in \mathcal{Q}$ , are chosen according to the maximal ratio combining (MRC) [72] method so as to maximize the reception of the signal at Bob<sub>q</sub> and Eve, respectively. Hence,  $\mathbf{d}_q = \mathbf{U}_q^{(1)}$ , where  $\mathbf{U}_q^{(1)}$  is the first column of  $\mathbf{U}_q$  (recall that  $\tilde{\mathbf{H}}_{qq} = \mathbf{U}_q \Sigma_q \mathbf{V}_q^\dagger$ ). Using this linear receiver, the TxFJ signal of Alice<sub>q</sub> will be nullified at Bob<sub>q</sub>. In other words,  $\mathbf{d}_q^\dagger \mathbf{H}_{jq} \mathbf{v}_q = 0$ . Let  $\tilde{\mathbf{G}}_q = \mathbf{L}_q \mathbf{D}_q \mathbf{R}_q$  be the SVD of  $\tilde{\mathbf{G}}_q$  where  $\mathbf{L}_q$  and  $\mathbf{R}_q$  are matrices of left and right singular vectors, respectively, and  $\mathbf{D}_q$  is the diagonal matrix of singular values in descending order. Thus, while eavesdropping on the  $q$ th link, Eve sets its linear receiver  $\mathbf{r}_q = \mathbf{L}_q^{(1)}$ , where  $\mathbf{L}_q^{(1)}$  is the first column of matrix  $\mathbf{L}_q$ <sup>10</sup>.

We need to emphasize that the choice of precoder (i.e., beamformers) for TxFJ signal in this chapter is mainly driven by the fact that acquiring E-CSI knowledge may not be possible in cases where Eve is a passive node. For a single-link scenario, it was shown in [26] that optimizing the precoders of information and TxFJ signals requires complete knowledge of E-CSI. However, in this chapter, the beamforming vector for the TxFJ signal for each link depends only on the channel between the two nodes comprising that link, which is relatively more practical to obtain.

Our choice of the beamforming vector  $\mathbf{T}_q$  comes from the fact that the number of antennas at Eve may not be known. As pointed out in [22], the main limitation of the TxFJ method is that if Eve has more antennas than Alice, then Eve may be able to nullify

---

<sup>9</sup>Because none of the links knows whose transmission Eve is interested in, each link tries to protect its own transmission from Eve. Thus, the secrecy rate of each link can be determined by (5.10) (see [61]).

<sup>10</sup>Other decoders (such as MMSE [72]) can also be employed by Eve. This issue will be discussed later in the simulation section.

the effect of TxFJ on itself.

### 5.3 Problem Formulation

In this section, we present conditions to achieve positive secrecy and establish the foundation for our game-theoretic formulation. We form the following optimization problem for link  $q$ ,  $q \in \mathcal{Q}$ :

$$\begin{aligned}
 & \underset{\phi_q, p'_q}{\text{maximize}} \quad C_q^{sec} \\
 & \text{s.t.} \quad 0 \leq \phi_q \leq 1 \\
 & \quad \quad 0 \leq p'_q \leq P'_q.
 \end{aligned} \tag{5.11}$$

Due to the non-concavity of the objective function in (5.11) w.r.t. the decision variables<sup>11</sup>, the optimization in (5.11) is non-convex. To find a tractable (and yet suboptimal) solution, we decompose the analysis of RxFJ and power assignment (PA) between information and TxFJ signals into two sub-problems. We first propose a tractable solution for  $p'_q$ . Then, we propose a method to find a suboptimal PA between information and TxFJ signals.

#### 5.3.1 Computation of RxFJ Power

Removing the  $\max\{\bullet\}$  and  $\log(\bullet)$  operators from  $C_q^{sec}$  in (5.10), the secrecy maximization w.r.t.  $p'_q$  can be written as

$$\begin{aligned}
 & \underset{p'_q}{\text{maximize}} \quad \frac{1 + \frac{\phi_q P_q}{a_q + b_q p'_q}}{1 + \frac{\phi_q P_q}{c_q + d_q p'_q}} \\
 & \text{s.t.} \quad 0 \leq p'_q \leq P'_q.
 \end{aligned} \tag{5.12}$$

---

<sup>11</sup>The non-concavity of objective function can be easily seen by examining the Hessian matrix of the objective function.

One can do a simple one-dimensional search to find the optimal value of  $p'_q$ . However, such an approach demands knowledge of multiuser interference (MUI) at Eve (i.e.,  $c_q$ ), which may not be available to Bob<sub>q</sub>. In the remainder of this section, we propose a different method for setting the RxFJ power. While at first it may seem that our method requires knowledge of MUI at Eve, we later show that this method can be relaxed to handle the case when knowledge of Eve's MUI is not available.

We first obtain conditions that result in positive secrecy at link  $q$ . Positive secrecy in (5.10) is achievable if and only if the objective value in (5.12) is larger than one. It can be easily shown that this is true if and only if the optimal objective value of the following optimization is larger than one<sup>12</sup>:

$$\begin{aligned} \underset{p'_q}{\text{maximize}} \quad & g(p'_q) \triangleq \frac{\frac{\phi_q P_q}{a_q + b_q p'_q}}{\frac{\phi_q P_q}{c_q + d_q p'_q}} = \frac{c_q + d_q p'_q}{a_q + b_q p'_q} \\ \text{s.t.} \quad & 0 \leq p'_q \leq P'_q. \end{aligned} \quad (5.13)$$

Note that the relationship between the solutions of (5.12) and (5.13) (that result in their corresponding objective values being larger than one) is of necessary-and-sufficient type. Hence, if we are seeking a set of conditions/solutions that result in positive secrecy, we can examine these solutions by checking the objective value they yield for (5.13) instead of (5.12). The first and second derivatives of  $g(p'_q)$  are as follows:

$$\frac{\partial g(p'_q)}{\partial p'_q} = -\frac{b_q c_q - a_q d_q}{(a_q + b_q p'_q)^2} \quad (5.14a)$$

$$\frac{\partial^2 g(p'_q)}{\partial p_q'^2} = 2b_q \frac{b_q c_q - a_q d_q}{(a_q + b_q p'_q)^3}. \quad (5.14b)$$

---

<sup>12</sup> One can simply set the objective of (5.12) to be larger than one and end up with  $g(p'_q) > 1$  (and vice versa), where  $g(p'_q)$  is defined in (5.13).

Hence, the optimal value of  $p'_q$  (i.e.,  $p'^*_q$ ) that solves (5.13) is given by:

$$p'^*_q = \begin{cases} P'_q & \text{if } b_q < \frac{a_q d_q}{c_q} \\ 0 & \text{if } b_q > \frac{a_q d_q}{c_q}. \end{cases} \quad (5.15)$$

Simplifying the first condition of (5.15), a threshold for SIS factor can be established<sup>13</sup>

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2} \frac{a_q d_q}{c_q}. \quad (5.16)$$

Later on, we show in simulations that whenever positive secrecy is achievable (i.e., the objective in (5.12) is larger than one), (5.15) often yields the optimal RxFJ power, signifying that the solution to (5.13) is very likely the optimal solution to (5.12) as well.

Considering (5.16), we can conclude the following: Given  $c_q$  and  $d_q$ , if the (normalized) MUI at Bob<sub>q</sub> ( $a_q$ ) is not as strong as the (normalized) self-interference channel ( $\frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}$ ), i.e., if  $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 a_q}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$  is small, the power of RxFJ should be very weak to maintain positive secrecy, leading to  $p'^*_q = 0$ . However, if  $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 a_q}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$  is large, the effect of RxFJ on Bob<sub>q</sub> is not as significant as MUI, so less suppression of self-interference can be allowed and still maintain positive secrecy, i.e.,  $p'^*_q = P'_q$  becomes the favorable solution. An equivalent intuition holds for  $d_q/c_q$  when  $\frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$  and  $a_q$  are given. Specifically, a large  $d_q/c_q$  indicates that RxFJ degrades Eve's reception more than the MUI received at Eve ( $c_q$ ). Hence, smaller SIS suppression (i.e., larger  $\tau_q$ ) is allowed, indicating that  $p'^*_q = P'_q$  becomes the favorable solution.

It can be seen in (5.15) that the optimal RxFJ power that solves (5.13) depends on two factors: MUI at Bob<sub>q</sub> (i.e.,  $a_q$ ) and MUI at Eve while eavesdropping on the  $q$ th link

<sup>13</sup>Although when  $p'_q = 0$  the benefits of RxFJ are lost, one can set a minimum RxFJ power to prevent RxFJ from going to zero.

(i.e.,  $c_q$ ). It may not be practical for a legitimate node to know the MUI at Eve. Later on, we show that using a specific technique in setting TxFJ can help us to mitigate the dependence on Eve's MUI.

A full treatment of the optimal value of RxFJ in a single-link scenario is given in [28]. However, extending the approach in [28] would require knowledge of interference at both Bob<sub>*q*</sub> and Eve,  $q \in \mathcal{Q}$ . Such a requirement is not practical in our scenario, as there is no cooperation allowed between legitimate links. Nevertheless, we show that our proposed on-off solution in (5.15) helps us to mitigate the dependency of RxFJ on MUI at both Bob<sub>*q*</sub>,  $q \in \mathcal{Q}$  and Eve, thus facilitating our distributed design.

### 5.3.2 Power Allocation for TxFJ and Information Signals

After finding a set of conditions/solutions for RxFJ power (i.e., the rule in (5.15)), we now focus on finding the optimal PA between TxFJ and information signals of Alice<sub>*q*</sub> (i.e.,  $\phi_q$ ). This is done through the following formulation:

$$\begin{aligned} & \underset{\phi_q}{\text{maximize}} \quad C_q^{sec} \\ & \text{s.t.} \quad 0 \leq \phi_q \leq 1. \end{aligned} \tag{5.17}$$

Although the optimal  $\phi_q$  can be found via a simple one-dimensional search, we would like to eventually solve (5.17) without requiring knowledge of Eve's MUI. In the remainder of this section, we propose a solution to (5.17) in the perfect E-CSI scenario. Later on, we show that our approach is extendable to the case of unknown E-CSI.

Similar to the approach taken in the previous section, we approach problem (5.17) by first finding a bound on  $\phi_q$  that guarantees positive secrecy of link  $q$ . Thus, the objective

in (5.17) is assumed to be positive, which reduces to

$$\frac{\phi_q P_q}{a_q + b_q p'_q} > \frac{\phi_q P_q}{c_q + d_q p'_q}. \quad (5.18)$$

Simplifying this inequality, we end up with the following:

$$c_q > a_q + (b_q - d_q)p'_q. \quad (5.19)$$

The inequality in (5.19) is a bound on the TxFJ power of Alice<sub>q</sub> (i.e.,  $\sigma_q$ ) because according to (5.9a),  $c_q$  is a function of  $\sigma_q$ . Reducing (5.19) gives us a bound on the portion of power allocated to the information signal (i.e.,  $\phi_q$ ), i.e.,

$$\phi_q \leq \max \left\{ \min \left\{ 1 - \frac{1}{P_q} \sum_{\substack{r=1 \\ r \neq q}}^Q \left\{ (A_{q,r} - B_{q,r}) \phi_r P_r + C_{q,r} P_r + D_{q,r} p'_r \right\} - \frac{p'_q}{P_q} E_q - \frac{F_q}{P_q} \delta, 1 \right\}, 0 \right\} \quad (5.20)$$

For ease of presentation, we do not introduce the new notations in (5.3.2) yet; we do so in in the next section. We refer to (5.19) as *the lower-bound on TxFJ power of link q to guarantee positive secrecy*. To make use of this lower bound, we first introduce the following result.

**Lemma 1.** *If (5.19) is satisfied, the secrecy rate  $C_q^{sec}$  is a monotonically increasing function of  $P_q$  and  $\phi_q$ .*

*Proof.* The inequality in (5.19) can be written as

$$c_q = a_q + (b_q - d_q)p'_q + \delta \quad (5.21)$$



where  $\delta > 0$  is a positive real value. Replacing the term  $c_q$  in (5.9a) with the RHS of (5.21), and taking the derivative of (5.10) (without the  $\max\{\bullet\}$  operator) w.r.t.  $P_q$  and  $\phi_q$ , we have

$$\frac{\partial C_q^{sec}}{\partial P_q} = \frac{\phi_q \delta}{(a_q + \phi_q P_q + b_q p'_q)(a_q + \phi_q P_q + b_q p'_q + \delta)} \quad (5.22a)$$

$$\frac{\partial C_q^{sec}}{\partial \phi_q} = \frac{P_q \delta}{(a_q + \phi_q P_q + b_q p'_q)(a_q + \phi_q P_q + b_q p'_q + \delta)} \quad (5.22b)$$

which are both positive, and hence the lemma is proved.  $\square$

Recall that in setting the RxFJ power in (5.15), we observed that its optimal value  $p_q'^*$  depends on Eve's and Bob<sub>q</sub> MUI. In order to mitigate knowledge of MUI at Bob<sub>q</sub> and Eve in (5.15) (i.e.,  $a_q$  and  $c_q$ ), we examine the following alternative conditions for RxFJ:

$$p_q'^* = \begin{cases} P'_q, & \text{if } b_q < d_q \\ 0, & \text{if } b_q > d_q. \end{cases} \quad (5.23)$$

Using the bound in (5.19), the following property shows the sufficiency of (5.23) to conclude (5.15).

**Proposition 7.** *Provided that the following conditions hold, the conditions on the optimal RxFJ power in (5.23) imply those of (5.15):*

- $c_q$  satisfies (5.19) and  $a_q + (b_q - d_q)p'_q + \delta > 0$ .
- $(b_q - d_q)P'_q + \delta < 0$  when  $b_q < d_q$

*Proof.* Assume that (5.23) is used to obtain the RxFJ power of link  $q$ . Hence, we set  $p_q'^* = P'_q$  when  $b_q < d_q$ . If  $c_q > 0$  and  $c_q$  satisfies (5.19) (first condition of Proposition 7), then  $c_q = a_q + (b_q - d_q)P'_q + \delta > 0$  when  $b_q < d_q$ . Assuming that  $(b_q - d_q)P'_q + \delta <$

0 (second condition of Proposition 7), one can conclude that  $a_q > c_q$ , or equivalently  $a_q > a_q + (b_q - d_q)P'_q + \delta$ . Hence,  $b_q < d_q$  is readily sufficient to deduce  $b_q < \frac{a_q d_q}{c_q}$  that appears in (5.15). Similarly,  $b_q > d_q$  can be proved to be sufficient to satisfy  $b_q > \frac{a_q d_q}{c_q}$ . Specifically, we set  $p'_q = 0$  according to (5.23). Given (5.19) and  $p'_q = 0$ ,  $c_q$  must satisfy  $c_q = a_q + \delta$ , and since  $\delta > 0$ ,  $a_q < c_q$ . Therefore,  $b_q > d_q$  is sufficient to deduce  $b_q > \frac{a_q d_q}{c_q}$  that appears in (5.15).  $\square$

**Remark 1:** If  $b_q < d_q$  and  $c_q = a_q + (b_q - d_q)P'_q > 0$ , then  $b_q < d_q$  is sufficient to satisfy  $b_q < \frac{a_q d_q}{c_q}$ , so both RxFJ schemes in (5.15) and (5.23) result in  $p_q^* = P'_q$ . However, when  $b_q < d_q$  (suggesting  $p_q^* = P'_q$  in (5.23)) but  $c_q = a_q + (b_q - d_q)P'_q < 0$ , we have  $b_q > \frac{a_q d_q}{c_q}$  (suggesting  $p_q^* = 0$  in (5.15)). Hence, we have conflicting decisions made by (5.15) and (5.23). Condition  $(b_q - d_q)P'_q + \delta < 0$  sets an upper bound on  $\delta$ , i.e.,  $0 < \delta < (d_q - b_q)P'_q$  if  $b_q < d_q$ . According to (5.6) and (5.9), the terms  $b_q$  and  $d_q$  are in fact functions of self-interference, Alice-Bob, Bob-Eve, and Alice-Eve channels. Hence, if Proposition 7 holds, Bob<sub>q</sub> only has to check whether or not

$$\tau_q < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \quad (5.24)$$

to decide whether RxFJ is needed or not. In other words, (5.23) is sufficient to set the RxFJ power of Bob<sub>q</sub><sup>14</sup>. The intuitive interpretation of (5.24) is that the SIS factor needs to be small if the self-interference channel (i.e.,  $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|$ ) has a large value, but if the Bob-Eve channel (i.e.,  $|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2$ ) is large enough, it can cancel out the effect of self-interference channel. In other words, Bob<sub>q</sub> must not use RxFJ if the self interference is not removed well enough. However, if Eve suffers more from the generated RxFJ, then Bob<sub>q</sub> can use it. Compared to (5.15), the RxFJ power assignment in (5.23) is more desirable, as it does

<sup>14</sup>The sufficiency of (5.23) is examined in Section 5.5.2.

not require real-time tracking of Eve's MUI at Bob<sub>q</sub>. Combining (5.19) and (5.23), we have

$$\begin{cases} c_q > a_q + (b_q - d_q)P'_q, & \text{if } b_q < d_q \\ c_q > a_q, & \text{if } b_q > d_q \end{cases}. \quad (5.25)$$

Since the inequalities in (5.25) are strict, we write the following:

$$\begin{cases} c_q = a_q + (b_q - d_q)P'_q + \delta, & \text{if } b_q < d_q \\ c_q = a_q + \delta, & \text{if } b_q > d_q \end{cases}. \quad (5.26)$$

Using mathematical manipulations of Equations (5.18)–(5.26), we can convert problem (5.17) to the following problem:

$$\begin{aligned} & \underset{\phi_q, \delta}{\text{maximize}} \quad C_q^{sec} \\ & \text{s.t.} \quad c_q = a_q + (b_q - d_q)p_q'^* + \delta \\ & \quad c_q > 0 \\ & \quad 0 < \delta < (d_q - b_q)P'_q + J(1 - t_q) \\ & \quad 0 \leq \phi_q \leq 1 \end{aligned} \quad (5.27)$$

where  $p_q'^*$  in the first constraint is set according to (5.23),  $J$  is a sufficiently large positive number, and

$$t_q = \begin{cases} 1 & \text{if } b_q < d_q \\ 0 & \text{if } b_q > d_q \end{cases}. \quad (5.28)$$

The first constraint in (5.27) is a constraint on  $\phi_q$ , which is needed so that the optimal

solution yields positive secrecy<sup>15</sup>. In other words, this constraint replaces the more general constraint in (5.17), so that we can ignore the  $\max\{\bullet\}$  operator in  $C_q^{sec} = \max\{C_q - C_{eq}\}$ . This constraint together with the second and third constraints in (5.27) ensure that setting  $p_q'^*$  according to (5.23) is sufficient to satisfy the more general conditions in (5.15). Note that  $t_q$  is not a decision variable of (5.27), and can be easily computed by knowing  $b_q$  and  $d_q$ .

Because  $c_q$  is a function of  $\phi_q$ , one can simplify the first constraint in (5.27) to find the value of  $\phi_q$  that yields positive secrecy for the objective of (5.27). However, we still need to determine the value of  $\delta$  to ensure that such value found for  $\phi_q$  is the optimal one for problem (5.27). A simple one-dimensional search in the interval defined by the third constraint in (5.27) can provide us with the best value of  $\delta$  and subsequently the optimal value of  $\phi_q$ . To avoid additional computation imposed by the one-dimensional search process, we propose the following heuristic technique to obtain  $\delta$ . On the one hand, we do not wish to choose  $\delta$  near its upper bound due to the fact that a higher  $\delta$  increases the lower bound on TxFJ, which subsequently decreases the amount of power allocated to the information signal. On the other hand, selecting  $\delta$  close to zero is also not desirable, as in (5.22b) the growth rate of secrecy rate would be decreased. Hence, we choose  $\delta = \frac{1}{2} |d_q - b_q| P_q'$ . We show later that this heuristic choice of  $\delta$  yields a performance close to that of the optimal solution found by a one-dimensional search.

## 5.4 Game Formulation

In this section, using the ideas in Section 5, we propose a power control scheme based on non-cooperative games. The first constraint in (5.27) can be written in a general form,

---

<sup>15</sup>Note that the term  $c_q$  is a function of  $\phi_q$  (see (5.9)). An equivalent expanded version of this constraint is given in equation (5.3.2). In (5.27), however, for the sake of simplicity, we present this constraint in a more compact form.

as follows

$$\begin{cases} c_q \geq a_q + (b_q - d_q)P'_q + \delta, & \text{if } b_q < d_q \\ c_q \geq a_q + \delta, & \text{if } b_q > d_q. \end{cases} \quad (5.29)$$

Simplifying (5.29) and taking into account the other constraints of (5.27), an upper bound on  $\phi_q$  can be written as in (5.3.2), with  $\delta = \frac{1}{2}|d_q - b_q|P'_q$  and the newly introduced notations in (5.3.2) are given in (5.30):

$$A_{q,r} \triangleq \frac{N_q - 1}{N_r - 1} \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2} \left( (N_r - 1) |\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{jr q}|^2 \right) \quad (5.30a)$$

$$B_{q,r} \triangleq \frac{N_q - 1}{N_r - 1} \frac{(N_r - 1) |\mathbf{r}_q^\dagger \mathbf{G}_r|^2 - |\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2} \quad (5.30b)$$

$$C_{q,r} \triangleq \frac{N_q - 1}{N_r - 1} \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{jr q}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \quad (5.30c)$$

$$D_{q,r} \triangleq (N_q - 1) \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \quad (5.30d)$$

$$E_q \triangleq (N_q - 1) \frac{\tau_q |\mathbf{r}_q^\dagger \mathbf{G}_q|^2 |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2 |\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \quad (5.30e)$$

$$F_q \triangleq (N_q - 1) \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2}. \quad (5.30f)$$

Hence, link  $q$ 's optimization problem in (5.27), where  $q \in \mathcal{Q}$ , can be written as

$$\begin{aligned} & \underset{\phi_q}{\text{maximize}} \quad C_q^{sec} \\ & \text{s.t.} \quad (5.3.2). \end{aligned} \quad (5.31)$$

With every legitimate link following such a strategy, the resulting interaction between them can be modeled as a non-cooperative game, where players are links, the strategy set of the  $q$ th player is the set of constraints in (5.31), and the utility of each player is

his secrecy rate. According to Lemma 1, upon achieving positive secrecy for link  $q$  (i.e., satisfying the constraint in (5.31)), the secrecy rate becomes a monotonically increasing function of  $\phi_q$ . Hence, the best-response of the  $q$ th link,  $q \in \mathcal{Q}$ , is when  $\phi_q$  meets its upper bound in (5.3.2) with equality. The Nash equilibrium is a point at which no player is willing to unilaterally change his strategy given the strategies of other players.

#### 5.4.1 Existence and Uniqueness of Nash Equilibrium

The first game-theoretic analysis that we perform is to examine whether the game characterized by (5.31) admits a NE. An NE exists if the strategy set of each player is non-empty, compact, and convex; and the utility function of each player is a continuous and (quasi-)concave function of its action, i.e.,  $C_q^{sec}$  is concave w.r.t.  $\phi_q$  [106]. Convexity of each player's strategy set is easy to prove, and thus omitted for brevity. Replacing  $c_q$  with  $a_q + (b_q - d_q)P'_q + \delta$  in (5.10) (as the first constraint in (5.27) suggests) and taking the second derivative of (5.10) w.r.t.  $\phi_q$ , we have:

$$\frac{\partial^2 C_q^{sec}}{\partial \phi_q^2} = P_q^2 \left( \frac{1}{a_q + \delta + \phi_q P_q + b p'_q} - \frac{1}{a_q + \phi_q P_q + b p'_q} \right) \quad (5.32)$$

which is always negative, indicating that  $C_q^{sec}$  is concave w.r.t.  $\phi_q$ . A necessary and sufficient condition for the uniqueness of NE is proved in the following theorem.

**Theorem 8.** *The game in (5.31), for which the best response of each player is when (5.3.2) holds with equality, has a unique NE iff:*

$$\rho(\mathbf{A} + \mathbf{B}) < 1 \quad (5.33)$$

where  $\rho(\bullet)$  indicates the spectral radius of a matrix (i.e., largest absolute value of eigen-

values of a matrix),  $\mathbf{A}$  is a matrix whose  $(q, r)$  element,  $\forall (q, r) \in \mathcal{Q}^2$ , is given by

$$[\mathbf{A}]_{q,r} \triangleq \begin{cases} -\frac{P_r}{P_q} A_{q,r} , & r \neq q \\ 0 , & r = q \end{cases}, \forall (r, q) \in \mathcal{Q} \quad (5.34)$$

and  $[\mathbf{B}]_{q,r}$ ,  $\forall (q, r) \in \mathcal{Q}^2$  is defined as:

$$[\mathbf{B}]_{q,r} \triangleq \begin{cases} \frac{P_r}{P_q} B_{q,r} , & r \neq q \\ 0 , & r = q \end{cases}. \quad (5.35)$$

with  $A_{q,r}$  and  $B_{q,r}$  defined in (5.30).

*Proof.* The uniqueness of NE can be proved by leveraging the fixed-point theorem. In fact, if the iterative computation of each player's best-response (i.e.,  $\phi_q$  meeting its upper bound in (5.3.2) with equality for all  $q$ ) has a fixed point, the convergence point is the NE of the game [107]. We first analyze the existence of a fixed point for the argument inside  $\max\{\min\{\bullet, 1\}, 0\}$  in (5.3.2). Then, we extend the analysis to include  $\max\{\min\{\bullet, 1\}, 0\}$ . Concatenating the best responses of all links, the following fixed-point problem in its  $n$ -th iteration can be established:

$$\Phi^{(n+1)} = \mathcal{T}(\Phi^{(n)}) = \mathbb{1} + (\mathbf{A} + \mathbf{B})\Phi^{(n)} + \mathbf{f} \quad (5.36)$$

where  $\Phi = [\phi_1, \dots, \phi_Q]^T$ ,  $\mathbb{1}$  is a vector of appropriate size whose entries are all 1, and  $\mathbf{f}$  is a vector constructed by concatenating other terms in (5.3.2) for all  $q$ . The rest of the proof is presented in Appendix C.  $\square$

**Remark 2:** Using the condition in (5.33), the convergence of the Jacobi iterative algo-

rithm in the sense of [107, Ch. 2, Proposition 6.8] is guaranteed. In fact, at every iteration, all players simultaneously update their actions. Later on, we prove the convergence of our secure power control game under totally asynchronous updates (in the sense of [107, Ch. 6]).

#### 5.4.2 Algorithm Design

We now design an algorithm to implement the proposed power control game. Let  $\mathbb{T}_q, \forall q \in \mathcal{Q}$ , be the set of iteration numbers when the  $q$ th link updates its action. For example,  $\mathbb{T}_q = \{1, 3, 5\}$  indicates that the  $q$ th link performs the update in (5.31) in first, third and fifth iterations. Furthermore, Let  $\Theta_q^{(n)} = \{\theta_{1,q}^{(n)}, \dots, \theta_{Q,q}^{(n)}\}$  denote the set of most recent times that the interference coming from each link is measured at Bob <sub>$q$</sub>  in the  $n$ th iteration. Hence,  $\theta_{r,q}^{(n)}$  is the most recent iteration in which the interference from the  $r$ th link,  $r \neq q$  is captured/updated, and  $\theta_{r,q}^{(n)} \leq n - 1$ . Therefore, in the  $n$ th iteration, the  $q$ th link,  $q \in \mathcal{Q}$ , performs the update in (5.31) based on  $\Theta_q^{(n)}$  if  $n \in \mathbb{T}_q$ . Using these definitions, we can now present an asynchronous algorithm that implements our proposed game, which is shown in Algorithm 6. Other termination criteria can be used instead of the maximum iteration number.

---

**Algorithm 6** Asynchronous Iterative Secure Power Allocation (full E-CSI version)

---

- 1: Set  $p'_q$  and  $\delta$  according to (5.23) and Proposition 7 (see Section III).
  - 2: **for**  $n=1$  to maximum iteration **do**
  - 3:   Set  $\phi_q^{(n)} = \begin{cases} \text{Equal to RHS of (5.3.2),} & \text{if } n \in \mathbb{T}_q \\ \phi_q^{(n-1)} & \text{otherwise} \end{cases}, \forall (q) \in \mathcal{Q}.$
  - 4: **end for**
- 

Special cases of the asynchronous scheme include Jacobi (or simultaneous) and Gauss-Seidel (or sequential) schemes [107]. The Jacobi scheme can be described as fol-



lows ( $q \in \mathcal{Q}$ ):

$$\begin{aligned}\mathbb{T}_q &= \{1, 2, \dots, it_{max}\} \\ \Theta_q^{(n)} &= \{n-1, \dots, n-1\}\end{aligned}$$

where  $it_{max}$  is the maximum iteration number. In other words, in the Jacobi scheme, all links simultaneously update their actions at each iteration. The Gauss-Seidel scheme can be described as follows:

$$\begin{aligned}\mathbb{T}_q &= \{q, q+Q, q+2Q, \dots, q + \left(\frac{it_{max}}{Q} - 1\right)Q\} \\ \Theta_j^{(n)} &= \begin{cases} \{n - (q-1), \dots, n-1\} & \text{if } j = 1, \dots, q-1 \\ \{n, n - (Q-1), \dots, n-q\} & \text{if } j = q, \dots, Q \end{cases}\end{aligned}$$

which means that in each iteration, only one link updates its action, while all other links use their previously chosen actions. The following theorem guarantees the feasibility of asynchronous implementation of our proposed game:

**Theorem 9.** *Algorithm 6 converges asynchronously to the unique NE of the proposed game if Theorem 8 holds.*

*Proof.* See Appendix C. □

Note that (5.3.2) was derived only to proceed with the game-theoretic analysis of the problem. A detailed procedure to find the optimal value of  $\phi_q$  in a node is as follows. At a given iteration of our algorithm, say the  $n$ th iteration, after setting the optimal value of RxFJ, in order to determine the optimal PA, Bob <sub>$q$</sub>  needs to first measure the interference at his receive chain, i.e.,  $a_q^{(n-1)} + b_q^{(n-1)}p_q'^*$  must be measured, where  $a_q^{(n-1)}$  and  $b_q^{(n-1)}$

indicate the values of  $a_q$  and  $b_q$  at the previous iteration. Assuming that full knowledge of E-CSI is available, Bob<sub>q</sub> also knows the MUI at Eve in the previous iteration, i.e.,  $c_q^{(n-1)} + d_q^{(n-1)} p_q'^*$  is known<sup>16</sup>. Hence, Bob<sub>q</sub> does the following: **1)** He subtracts the term  $\frac{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}| \sigma_q^{(n-1)}}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}$  from  $c_q^{(n-1)}$ ; **2)** He adds the result of subtraction to  $d_q^{(n-1)} p_q'^*$ . Denote the result of this addition as  $g_q$ ; **3)** He finds the optimal PA in the  $n$ th iteration, which can be described as:

$$\phi_q^* = \max \left\{ \min \left\{ 1 - \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}| P_q} (a_q^{(n-1)} + b_q^{(n-1)} p_q' - g_q), 1 \right\}, 0 \right\}. \quad (5.37)$$

It can be seen that setting the optimal PA involves simple addition, subtraction and division of scalar values. Moreover, there is no need to know all interference terms at Bob<sub>q</sub> and Eve because only the aggregate of these terms (i.e.,  $a_q$  and  $c_q$ ) need to be known.

#### 5.4.3 Sufficient Conditions for NE Uniqueness

Although (5.33) is a tight condition, evaluating it requires knowledge of the whole matrix  $\mathbf{A} + \mathbf{B}$ , which is not desirable for distributed implementation. We introduce a sufficient condition which can be evaluated in distributed fashion. It is shown in [107, Proposition A.20] that for any induced matrix norm<sup>17</sup>  $\|\bullet\|$  and any square matrix  $\mathbf{M}$  we have  $\rho(\mathbf{M}) \leq \|\mathbf{M}\|$ . Using this property, we consider the induced norm  $\|\bullet\|$  to be  $\|\bullet\|_\infty$ , which is the infinity norm. Hence, assuming that  $\mathbf{M}$  is a  $Q$ -by- $Q$  matrix, a sufficient condition for  $\rho(\mathbf{M}) < 1$  is whether  $\|\mathbf{M}\|_\infty < 1$ . Using this property in our game, a sufficient condition

<sup>16</sup>Notice that throughout the iterations of our algorithm,  $b_q^{(n-1)} = b_q^{(n)}$  and  $d_q^{(n-1)} = d_q^{(n)}$ . However, the values of  $a_q$  and  $c_q$  can vary across iterations.

<sup>17</sup>The induced norm of matrix  $\mathbf{M}$  is defined as  $\|\mathbf{M}\| \triangleq \max_{\|\mathbf{x}\|=1} \|\mathbf{M}\mathbf{x}\|$  where  $\mathbf{x}$  is a vector and both norms in the RHS are vector norms.

for our game to have a unique NE is whether

$$\|\mathbf{A} + \mathbf{B}\|_\infty = \max_q \sum_{r=1}^Q \frac{P_r}{P_q} |A_{q,r} - B_{q,r}| < 1. \quad (5.38)$$

The physical intuition drawn from the condition in (5.38) is not straightforward. One way to interpret this condition is to decompose this condition as follows: The term  $A_{q,r}$  in (5.38) is mostly related to the MUI at each Bob which should be low enough, i.e.,  $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|$ ,  $\forall q \in \mathcal{Q}$  in  $A_{q,r}$  should be large enough to guarantee the uniqueness of NE (see (5.30)). A sufficient separation between the links can satisfy this condition. The term  $B_{q,r}$  in (5.38) is related to E-CSI components (see (5.30)). At first, it may seem that this condition requires each link to be the dominant interferer at Eve w.r.t. other links (i.e.,  $|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|$ ,  $\forall q \in \mathcal{Q}$  in  $B_{q,r}$  should be large enough). However, this is physically not possible.

It can be seen that the uniqueness condition depends on the location of Eve as well because both  $A_{q,r}$  and  $B_{q,r}$  depend on Eve's channels. Other studies such as [46, 55, 65] have also confirmed the dependency of the unique NE (of non-cooperative secure power control games) on Eve's channels. Such a coupling is neither practical (because E-CSI must be known) nor favorable (because Eve plays a role in the stability of the game). In what follows, we aim to mitigate knowledge of E-CSI and set the NE uniqueness (derived in Theorem 8) free of Eve's role. None of the approaches in [43, 46, 55] were shown to be extendable to the case of unknown E-CSI. However, we show that our approach can be simply extended to cover the case of unknown E-CSI.

## 5.5 Robust Power Allocation Game

In this section, we incorporate the assumption of unknown E-CSI in our game.

### 5.5.1 Best Response Under E-CSI Uncertainties

As knowledge of E-CSI becomes unknown, each legitimate link needs to ensure that positive secrecy is still preserved. Recalling the inequalities in (5.29) and (5.3.2), positive secrecy happens when  $c_q > a_q + (b_q - d_q)p'_q$  or equivalently

$$(1 - \phi_q)P_q > \psi_q + \tau_q p'_q E_q \quad (5.39)$$

where

$$\psi_q \triangleq \sum_{\substack{r=1 \\ r \neq q}}^Q \{(A_{q,r} - B_{q,r}) \phi_r P_r + C_{q,r} P_r + D_{q,r} p'_r\}.$$

Under unknown E-CSI, for a given *probability of positive secrecy*, denoted by  $\varepsilon$ , the  $q$ th link needs to satisfy the following:

$$\Pr\{(1 - \phi_q)P_q > \psi_q + \tau_q p'_q E_q\} \geq \varepsilon. \quad (5.40)$$

Using (5.23) and the Bayes law of total probability, we have

$$\begin{aligned} & \Pr\{(1 - \phi_q)P_q > \psi_q + \tau_q p'_q E_q\} = \\ & \Pr\{b_q < d_q\}(1 - \Pr\{(1 - \phi_q)P_q \leq \psi_q + \\ & \tau_q p'_q E_q\}) + \Pr\{b_q > d_q\}(1 - \Pr\{(1 - \phi_q)P_q \leq \psi_q\}). \end{aligned} \quad (5.41)$$

We assume that  $\psi_q + \tau_q p'_q E_q$  is a non-negative number for both values of  $p'_q$ , i.e.,  $\Pr\{\psi_q + \tau_q p'_q E_q > 0\} = 1$ , otherwise (5.40) is always satisfied when  $\psi_q + \tau_q p'_q E_q < 0$ , and Alice<sub>q</sub> can spend all of the transmit power on information signal<sup>18</sup>. Using Markov inequality in (5.41), the following holds

$$\begin{aligned} & \Pr\{b_q < d_q\}(1 - \Pr\{(1 - \phi_q)P_q < \psi_q + \tau_q P'_q E_q\}) + \\ & \Pr\{b_q > d_q\}(1 - \Pr\{(1 - \phi_q)P_q < \psi_q\}) > \\ & \Pr\{b_q < d_q\}(1 - \frac{\mathbb{E}[\psi_q + \tau_q P'_q E_q]}{(1 - \phi_q)P_q}) + \Pr\{b_q > d_q\}(1 - \frac{\mathbb{E}[\psi_q]}{(1 - \phi_q)P_q}). \end{aligned} \quad (5.42)$$

Hence, (5.40) remains true as long as we have

$$\Pr\{b_q < d_q\}(1 - \frac{\mathbb{E}[\psi_q + \tau_q P'_q E_q]}{(1 - \phi_q)P_q}) + \Pr\{b_q > d_q\}(1 - \frac{\mathbb{E}[\psi_q]}{(1 - \phi_q)P_q}) \geq \varepsilon. \quad (5.43)$$

Simplifying this inequality, we end up with

$$\phi_q \leq \max \left\{ \min \left\{ 1 - \Pr\{b_q < d_q\} \frac{\mathbb{E}[\psi_q + \tau_q P'_q E_q]}{(1 - \varepsilon)P_q} - \Pr\{b_q > d_q\} \frac{\mathbb{E}[\psi_q]}{(1 - \varepsilon)P_q}, 1 \right\}, 0 \right\}. \quad (5.44)$$

For the rest of this section, we explain how different terms in (5.5.1) can be computed.

We first focus on computing  $\Pr\{b_q < d_q\}$ . Using (5.6) and (5.9), we simplify  $b_q < d_q$ , which is as follows

$$b_q < d_q \Rightarrow |\mathbf{r}_q^\dagger \mathbf{G}_q|^2 < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2} |\mathbf{r}_q^\dagger \mathbf{G}'_q|^2. \quad (5.45)$$

---

<sup>18</sup>Intuitively, if Eve is not close-by no power needs to be allocated to TxFJ, hence suggesting that  $\psi_q + \tau_q p'_q E_q < 0$ .

The probability  $\Pr\{b_q < d_q\}$  can be written as

$$\Pr\left\{\frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2} < \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}\right\}. \quad (5.46)$$

The small-scale fading components of  $\mathbf{r}_q^\dagger \mathbf{G}'_q$  and  $\mathbf{r}_q^\dagger \mathbf{G}_q$  are ZMCSCG-RVs with unit variances. Hence  $|\mathbf{r}_q^\dagger \mathbf{G}_q|^2$  and  $|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2$  both have chi-square distributions with 2 and  $2N_q$  degrees of freedom, respectively. The division of a (central) chi-square random variable by another independent (central) chi-square random variable has *F-distribution*. To tackle the issue of unknown large-scale fading components of  $\mathbf{r}_q^\dagger \mathbf{G}'_q$  and  $\mathbf{r}_q^\dagger \mathbf{G}_q$  we use *stochastic geometry* [124]. One can model nodes' positions according to a spatial distribution, e.g., a Poisson point process (PPP). For instance, stochastic geometry has been used in modeling eavesdroppers' positions in several recent works [125]. We model the location(s) of Eve(s) according to an independent homogenous PPP, namely  $\Omega$ , with density  $\lambda$ . Such a representation can be used to model single or multiple Eves depending on the choice of  $\lambda$ <sup>19</sup>. In summary, let  $\Gamma\gamma \triangleq \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}$  where  $\Gamma$  and  $\gamma$  are RVs that represent large-scale and small-scale fading components of  $\frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}$ , respectively. Furthermore, let  $\nu \triangleq \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}$ . Using stochastic geometry and F-distribution, we have the following theorem<sup>20</sup>:

**Theorem 10.** *An analytical solution for (5.46) that is used in (5.5.1) is as follows:*

$$\Pr\{\Gamma\gamma < \nu\} = \exp\left(-\lambda \int_0^{d_0} \int_0^{2\pi} \Pr\{\xi_q \gamma > \nu\} \beta d\beta d\varphi\right) \quad (5.47)$$

where  $\xi_q \triangleq \left(\frac{\beta}{\sqrt{d_{qq}^2 + \beta^2 - 2d_{qq}\beta \cos\varphi}}\right)^\eta$  and  $\Pr\{\xi_q \gamma > \nu\} = (1 + \frac{\nu}{\xi_q})^{-N_q}$ .

<sup>19</sup>For example, if Eve is known to be distributed inside a certain region, we can find a suitable  $\lambda$  (that represents the density as  $\lambda$  Eves per unit of the surface area) such that the PPP matches our settings.

*Proof.* See Appendix C.  $\square$

We now turn our attention to  $E[\psi_q + \tau_q P'_q E_q]$  and  $E[\psi_q]$  in (5.5.1). We propagate the expectation in  $E[\psi_q + \tau_q P'_q E_q]$  to each term inside  $\psi_q$  using (5.30). Because the expectation terms in  $E[\psi_q + \tau_q P'_q E_q]$  contain non-negative RVs we can use the following identity:

$$E \left[ \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2} \right] = \int_0^\infty \Pr\{\Gamma\gamma > \nu\} d\nu \quad (5.48)$$

where  $\Pr\{\Gamma\gamma > \nu\}$  can be derived from Theorem 10. Hence, the terms involving expectation in  $E[\psi_q + \tau_q P'_q E_q]$  are computable and can be treated the same as  $E \left[ \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2} \right]$ .

While in the simulation section, we focus on the case where no knowledge on E-CSI components is available to links (i.e., both large-scale and small-scale fading parts of E-CSI components are not known), we can extract more insights from the derivations for unknown E-CSI by considering the case where large-scale fading part of E-CSI is available. Hence, we can give a close-form representation to (5.5.1). Knowledge of large-scale fading of Alice-Eve and Bob-Eve channel is not new and has been assumed to be known for various scenarios. One example is when Eve is acting as a reactive jammer. That is to say after some eavesdropping on the current transmissions, Eve injects her jamming signal to disrupt the ongoing communications. In such a case when jamming happens, assuming that the jamming power of Eve and the statistical features of the jamming signal are previously known (e.g., PDF, mean), the legitimate links can measure the jamming signal strength when it interferes with their transmissions. Hence, the approximate location of Eve can be estimated. Moreover, in [97], it was shown that in a massive MIMO scenario, a passive Eve might not be very dangerous and must therefore be active and attack the training phase. This active attack can make Eve exposed, and hence the legitimate links can acquire some knowledge about her location. Recently, the authors in [98]

proposed a method with which the legitimate nodes can detect the passive eavesdropper from the local oscillator power leaked from its RF front end. Hence, an approximation on the location of Eve can be acquired. Furthermore, the knowledge of large-scale fading was recently analyzed in [126] where the directional properties (i.e., small-scale fading) of Eve(s) are unknown to Alice.

Regarding the calculation of  $\Pr\{b_q < d_q\}$  in (5.5.1), the small-scale part of  $X \triangleq \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}$  in (5.46) is equivalent to the SINR of a one-branch diversity combiner with  $N_q$  interferers [127, eq. (19)]. Thus,

$$F_X(\xi) = 1 - \frac{1}{1 + \xi}. \quad (5.49)$$

Using (5.49) in (5.46), we end up with <sup>21</sup>

$$\Pr\{b_q < d_q\} = 1 - \left( 1 + \left( \frac{d_{qe}}{d'_{qe}} \right)^\eta \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2} \right)^{-N_q}. \quad (5.50)$$

To compute  $\mathbb{E}[\psi_q + \tau_q P'_q E_q]$  and  $\mathbb{E}[\psi_q]$  in (5.5.1), we know that the small-scale fading part of random variables  $|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|^2$ ,  $|\mathbf{r}_q^\dagger \mathbf{G}_{jr}|^2$ ,  $|\mathbf{r}_q^\dagger \mathbf{G}_r|^2$ , and  $|\mathbf{r}_q^\dagger \mathbf{G}'_r|^2$  have chi-square distributions with  $2(N_q - 1)$ ,  $2(N_r - 1)$ , 2, and  $N_r$  degrees of freedom, respectively [120, Lemma 2]. Note that all of the aforementioned RVs are independent from each other because the precoding matrices  $\mathbf{V}_q^{(1)}$  and  $\mathbf{V}_q^{(2)}$ ,  $\forall q$  are unitary and orthogonal to each other (see Section II). The division of a (central) chi-square random variable by another independent

---

<sup>21</sup>Note that it is assumed that the knowledge of Alice-Bob channel, self-interference, and multi-user interference still hold.



(central) chi-square random variable has *F-distribution* [128]. Hence,

$$E[A_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{(N_r - 1)|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 - |\mathbf{d}_q^\dagger \mathbf{H}_{jq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} \quad (5.51a)$$

$$E[B_{q,r}] = 0 \quad (5.51b)$$

$$E[C_{q,r}] = \frac{N_q - 1}{(N_r - 1)(N_q - 3)} \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{jq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \frac{N_q - 1}{N_q - 3} \left(\frac{d_{re}}{d_{qe}}\right)^{(-\eta)} \quad (5.51c)$$

$$E[D_{q,r}] = \frac{N_q - 1}{N_q - 3} \left( \frac{|\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \left(\frac{d'_{re}}{d_{qe}}\right)^{(-\eta)} \right) \quad (5.51d)$$

$$E[E_q] = \frac{N_q - 1}{N_q - 3} \left( \frac{\tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2} - \left(\frac{d'_{qe}}{d_{qe}}\right)^{(-\eta)} \right). \quad (5.51e)$$

$$E[F_q] = \frac{N_q - 1}{N_q - 3}. \quad (5.51f)$$

The last issue is related to the on-off scheme proposed earlier for the RxFJ. As it was shown in Section 5, whether the RxFJ is used or not depends on  $b_q < d_q$  or  $b_q > d_q$  (See (5.23)). When  $b_q < d_q$  becomes a random variable in the case of unknown E-CSI, we choose to use RxFJ whenever  $\Pr\{b_q < d_q\} > 0.5$ .

Interestingly, in the scenario where knowledge of E-CSI is not available, it can be shown that our robust scheme introduced in this section is in fact aimed at maximizing the *ergodic secrecy rate*. The details of describing our robust scheme as an ergodic secrecy rate maximization method can be found in Appendix C.4.2.

### 5.5.2 Distributed Power Control Under E-CSI Uncertainties

Using (5.5.1)-(5.48), we construct a game with the same structure as in Section 5 where each link's best response is computed from (5.5.1). Same as what we did in the proof of Theorem 1, we concatenate the solution in (5.5.1) for all  $q$  to establish the following fixed

point problem in its  $n$ -th iteration

$$\Phi^{(n+1)} = \mathbb{1} + \frac{1}{1-\varepsilon} \left( E[\mathbf{A} + \mathbf{B}] \Phi^{(n)} + E[\mathbf{f}] \right) \quad (5.52)$$

It can be seen that (5.52) is similar to (36) with the only difference that in (5.52) we applied expectation w.r.t E-CSI to all terms. To analyze the uniqueness of NE, the fixed point problem in (5.52) must be in closed form, i.e., the expectation terms in (5.52) must be computable. The close-form representation of these terms was given in (45)–(48). Hence, all the analysis that we did for the NE in the full-ECSI scenario is applicable in the robust scheme as well.

Using the same logic behind Theorem 8, the following must hold to ensure a unique NE for the robust game:

$$\rho \left( \frac{E[\mathbf{A} + \mathbf{B}]}{1 - \varepsilon} \right) < 1 \quad (5.53)$$

where the expected value is element-wise. Note that  $E[B_{q,r}] = 0$  (See (5.51b)), so one can see that the analysis of  $E[\mathbf{A} + \mathbf{B}]$  is simplified to  $E[\mathbf{A}]$ . Therefore, the E-CSI is no longer present in NE uniqueness conditions. Moreover, for the  $q$ th link,  $q \in \mathcal{Q}$  to perform the PA scheme in (5.5.1), it requires the PA's set by other links (i.e.,  $\phi_r, \forall r \in \mathcal{Q}, r \neq q$ ), as well as the interfering channels between other legitimate links and Bob $_q$  (i.e.,  $\mathbf{H}_{rq}$  and  $\mathbf{H}_{jrq}, H'_{rq}, \forall r, q \in \mathcal{Q}, r \neq q$ ). Hence, no knowledge of MUI at Eve or E-CSI components is needed. Same as the previous section, an alternative condition to (5.53) is to replace the spectral radius with the infinity norm (see also (5.38)). Interestingly, the alternative condition for the robust game has a nice interpretation. Specifically, (5.53) is deduced if

$$\left\| \frac{E[\mathbf{A}]}{1 - \varepsilon} \right\|_{\infty} = \max_q \sum_{r=1}^Q \frac{1}{1 - \varepsilon} |E[A_{q,r}]| < 1. \quad (5.54)$$

Intuitively, if the interfering channels are small enough, a unique NE exists. Thus, the uniqueness conditions in the robust schemes are not dependent on E-CSI. Algorithm 7 implements the robust version of our game:

---

**Algorithm 7** Asynchronous Iterative Secure Power Allocation (robust version)

---

- 1: Given  $\varepsilon$ , calculate (5.46) and set  $p'_q = P'_q$  if  $\Pr\{b_q < c_q\} \geq 0.5$ , or  $p'_q = 0$  if  $\Pr\{b_q < c_q\} < 0.5$ .
  - 2: **for**  $n=1$  to maximum iteration **do**
  - 3:     Set  $\phi_q^{(n)} = \begin{cases} \text{Equal to RHS of (5.5.1),} & \text{if } n \in \mathbb{T}_q, \forall (q) \in \mathcal{Q}. \\ \phi_q^{(n-1)} & \text{otherwise} \end{cases}$
  - 4: **end for**
- 

## 5.6 Numerical Results

In this section, we verify our theoretical analyses. We show our results for a four-link network<sup>22</sup>. Eve is located at  $(X_e, Y_e)$  on a 2-D coordinate system. Alices are randomly placed on the boundary of a circle, known as simulation region, with radius  $r_{\text{circ}}$  whose center is at the origin of the coordinate system. Each Alice has a fixed distance (communication range) with her corresponding Bob denoted as  $d_{\text{link}}$ <sup>23</sup>. Each Bob is placed randomly around his corresponding Alice on the boundary of a circle whose center is the location of Bob's corresponding Alice with radius  $d_{\text{link}}$ . The noise level is set to 0 dBm. Unless stated otherwise, the power constraint for each legitimate link is set to  $P_q = 20$  dBm,  $\forall q$ , the maximum RxFJ power at each Bob is  $P'_q = 15$  dBm,  $\eta = 2.5$ ,  $\tau_q = -100$  dB<sup>24</sup>,  $d_{\text{link}} = 10$  m, and finally Jacobi algorithm is used in all simulations. Regarding

---

<sup>22</sup>The results for this case can be generalized to larger number of links.

<sup>23</sup>Using a common communication range is a generic assumption in wireless ad hoc networks [125].

<sup>24</sup>Such SIS factors that reduce self-interference below the noise level were reported in recent practical implementation of full-duplex radios [29].

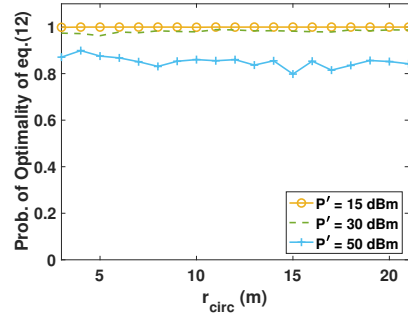


Figure 5.2: Probability of having both positive secrecy and the assignment in (5.15) being the optimal solution for a single-link scenario ( $X_e = Y_e = 0$ ,  $N_q = 8$ ,  $M_q = L = 5$ ,  $P_q = 25 \text{ dBm}$ ,  $\forall q$ ,  $Q = 4$ )

the unknown location for Eve,  $\text{Bob}_q$  assumes that Eve is distributed in a circle around him with radius  $r_0 = 5 \text{ m}$  according to a PPP with  $\lambda = \frac{1}{25\pi} \text{ Eve/m}^2$ ,  $q \in \mathcal{Q}$ .

For the first numerical result, we set up our system model in the presence of an eavesdropper where the PA between TxFJ and information signal for all links is set to  $\phi = 0.5$ . We aim to find out if the RxFJ PA scheme in (5.15) is sufficiently close to an optimal scheme to solve (5.12). To do so, we perform the optimal assignment of RxFJ power for (5.12) with a simple one-dimensional search method for several channel realizations and count the times when the solution found from one-dimensional search reduces to the solution in (5.15). In Figure 5.2, we plot the probability of having both positive secrecy and the optimal value of RxFJ power for problem (5.12) (found from a one-dimensional search) being either the maximum or zero according to the scheme in (5.15) for all links. Such probability shows how frequent the scheme in (5.15) gives us the optimal value of RxFJ power. It can be seen in Figure 5.2 that this probability is very high even for when the power budget for RxFJ is high. Also, the size of simulation region has a negligible effect.

Figure 5.3 (a)-(c) show the number of links that use RxFJ in the network for the two RxFJ PA schemes derived in (5.15) and (5.23) where in (5.15),  $c_q$  is set according to

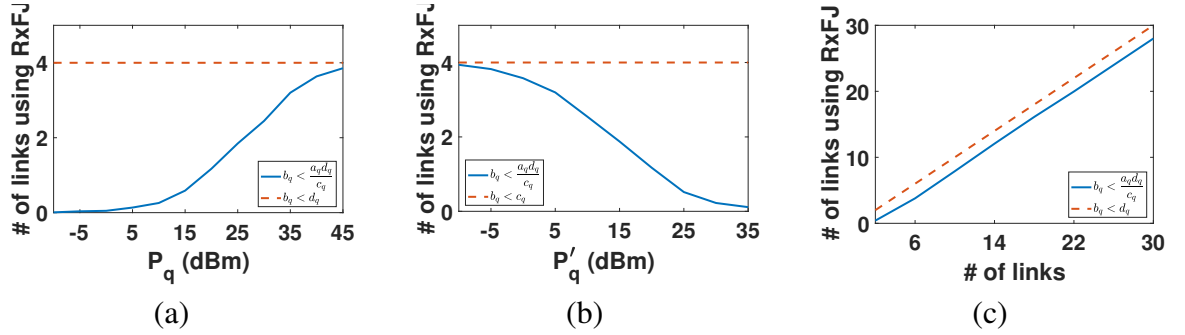


Figure 5.3: Number of links that use fixed-power RxFJ under full knowledge of E-CSI (i.e., rule (5.15)) and no knowledge of E-CSI (i.e., rule (5.23)) vs. (a) transmit powers ( $P'_q = 15$  dBm) (b) RxFJ powers ( $P_q = 25$  dBm) (c) number of links given that per-link secrecy is guaranteed ( $X_e = Y_e = 0$ ,  $r_{\text{circ}} = 20$  m,  $N_q = 8$ ,  $M_q = L = 5$ ,  $\forall q, Q = 4$ ).

(5.26). We assumed that all links use  $\phi_q = 0.5$  as the PA for information and TxFJ signals.

It can be seen from these figures that using the RxFJ PA in (5.23) has a close performance to (5.15) whenever Alices' power budgets are high enough (see Figure 5.3(a)) or when Bobs' RxFJ power budgets are low enough (see Figure 5.3(b)). Examining  $c_q$  in (5.26), one can easily see that low transmit powers would decrease  $a_q$  and high RxFJ powers would increase  $(b_q - d_q)P'_q$ . Both of these situations are detrimental to the scheme in (5.23), as they violate the condition  $c_q > 0$  which is a requirement for sufficiency of the scheme in (5.23) (See Proposition 7 and Remark 1). Using high enough power budgets at Alices (i.e.,  $P_q, \forall q \in \mathcal{Q}$ ) and low enough RxFJ powers at Bobs ( $P'_q, \forall q \in \mathcal{Q}$ ) for all links can ensure that  $c_q$  will remain positive. As it can be seen in Figure 5.3 (c), for a suitable choice of transmit power and RxFJ power, both conditions stay close to each other regardless of number of links in the network. Overall, under high enough transmit power budget and low enough RxFJ power budget, the sufficient condition (5.23) yield a performance equivalent to (5.15) and sets Alice<sub>q</sub> free of having to track the MUI at Bob<sub>q</sub> and Eve.

Next, we compare the performance of our proposed methods for PA between TxFJ and information signals. Specifically, in one method, we use one-dimensional search to find

the best value of  $\delta$  in (5.27). In the other method, we use our proposed heuristic method for finding  $\delta$ , i.e.,  $\delta = \frac{1}{2}|d_q - b_q|P'_q$ . We compare the resulting secrecy sum-rate of these two methods in Figure 5.5<sup>25</sup>. It can be seen that the proposed heuristic method has a very close performance to that of the one-dimensional search, suggesting that we can use the heuristic method for assigning  $\delta$  without imposing the relatively larger computational complexity of the one-dimensional search method.

Figure 5.4 shows the probability of satisfying the uniqueness conditions derived in (5.33) and (5.38) for a two-link scenario with full knowledge of E-CSI. The vertical axis at the left of each subfigure indicates the probability of satisfying (5.33), i.e.,  $\rho(\mathbf{A} + \mathbf{B}) < 1$ . Specifically, each point on the curve related to (5.33) (indicated by  $n_1$ ) is the result of averaging the number of times (5.33) holds over 100 network topologies where in each topology 500 channel realizations are simulated and averaged. Thus, the probability of convergence for (5.33) is  $n_1/(100*500)$  where  $n_1$  denotes the number of times that (5.33) is satisfied over all network topologies and channel realizations. Let  $n_2$  denote the number of times that condition (5.38) is satisfied given that (5.33) is already satisfied. Hence, the vertical axis at the right of each subfigure indicates the ratio  $n_2/n_1$  for which we have  $n_2/n_1 < 1$ , since  $n_2$  counts the times (5.38) is true among the times (5.33) holds.

The horizontal axis in Figure 5.4 indicates the value of  $X_e$ . While the value of  $Y_e$  is fixed for a subfigure, it is different from one subfigure to another. For the two-link case, condition (5.33) is highly probable in all scenarios. The practical condition in (5.38), however, is only good when Eve is relatively far from the network, but as Eve becomes closer to the network this condition is less efficient. Interestingly, as Eve approaches the origin, for  $Y_e = 0$  in Figure 5.4 (a), the probability of satisfying (5.38) increases. The reason for such a result is because of the simulation model, which verifies the physical interpretation

<sup>25</sup>Note that the one-dimensional search is in fact the optimal approach in solving (5.27).

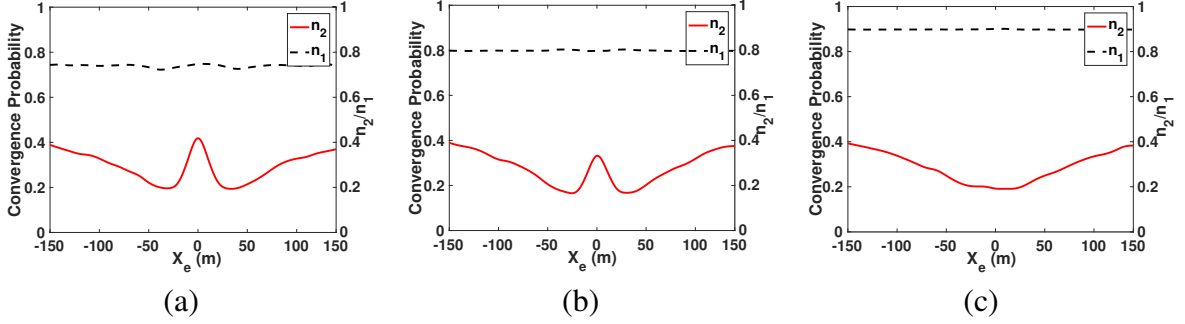


Figure 5.4: Probability of convergence vs. eavesdropper's location for the full E-CSI case: (a)  $Y_e=0$ , (b)  $Y_e=10\text{m}$ , (c)  $Y_e=40\text{ m}$ , ( $r_{\text{circ}}=30\text{m}$ ,  $N_q = 8$ ,  $M_q = L = 1$ ,  $\forall q$ ,  $Q = 2$ ).

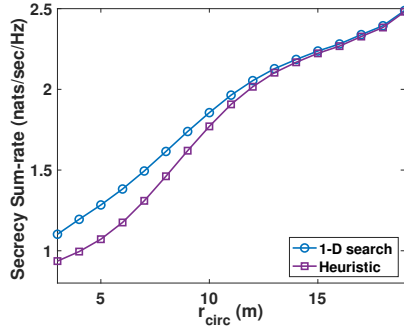


Figure 5.5: Comparison of secrecy sum-rate between the one-dimensional search method and the heuristic method for setting  $\delta$  in (5.27) ( $X_e = Y_e = 0$ ,  $N_q = 8$ ,  $M_q = L = 5$ ,  $P_q = 25\text{ dBm}$ ,  $P'_q = 15\text{ dBm}$ ,  $\forall q$ ,  $Q = 4$ )

given for (5.38). In fact, the origin is where the distance of all links to Eve is the same because the simulation model puts all of Alices in the boundary of the simulation region which is a circle. One can see that when the y-coordinate of Eve changes in Figure 5.4 (b) and Figure 5.4 (c), the location  $X_e = 0$  becomes more similar to other points inside the simulation region. We did not however, see this phenomenon for higher number of links, which is attributed to the fact that the second summation in (5.38) becomes too large with high number of links, even though it is a constant for when  $(X_e, Y_e) = (0, 0)$ .

Figure 5.6 shows the variation of convergence (i.e., NE uniqueness) probabilities in robust and full E-CSI methods w.r.t  $r_{\text{circ}}$  for the four-link case. The convergence probability is calculated as number of times the conditions in (5.33) and (5.38) (indicated by

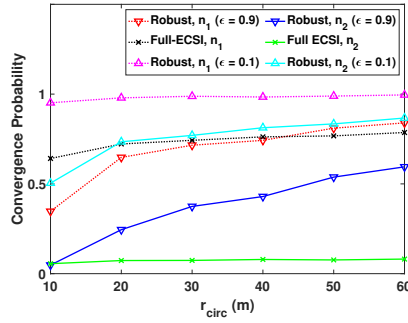


Figure 5.6: Probability of convergence vs.  $r_{\text{circ}}$  ( $X_e = Y_e = 5$ ,  $N_q = 8$ ,  $M_q = L = 5$ ,  $\forall q$ ,  $Q = 4$ ).

“full E-CSI,  $n_1$ ” and “full E-CSI,  $n_2$ ”, respectively), and their equivalents for the robust game (i.e., (5.53) indicated by “Robust,  $n_1$ ” and (5.54) indicated by “Robust,  $n_2$ ”) hold true divided by the number of channel realizations. It can be seen that for the case of full E-CSI, probability of uniqueness of NE using (5.38) is very low. However, in the case of unknown E-CSI, since the nodes are indifferent w.r.t. E-CSI, far less restrictive conditions than that of full E-CSI scenario can be achieved. In fact, although the distances between links and Eve become larger as  $r_{\text{circ}}$  grows, the uniqueness of NE in the full E-CSI case still remains unpredictable. On the contrary, in the robust method, by increasing the radius of simulation region, interference at each Bob becomes weaker. So, as the physical interpretation mentioned for (5.54) suggested, the NE uniqueness becomes more often. Moreover, in robust version, as  $\varepsilon$  becomes larger, the uniqueness conditions become more restrictive, which is in line with the derivation in (5.53).

Figure 5.7(a)-(c) show the achieved secrecy sum-rate of our proposed power control (under known/unknown E-CSI) vs. the radius of our simulation region. We also plotted the secrecy sum-rate of globally optimal solutions of the secrecy sum-rate maximization. We used Algorithm 1 when the E-CSI is fully known to the legitimate links (indicated by “Full E-CSI” in Figure 5.7(c)), and used Algorithm 2 when E-CSI is unknown (indicated



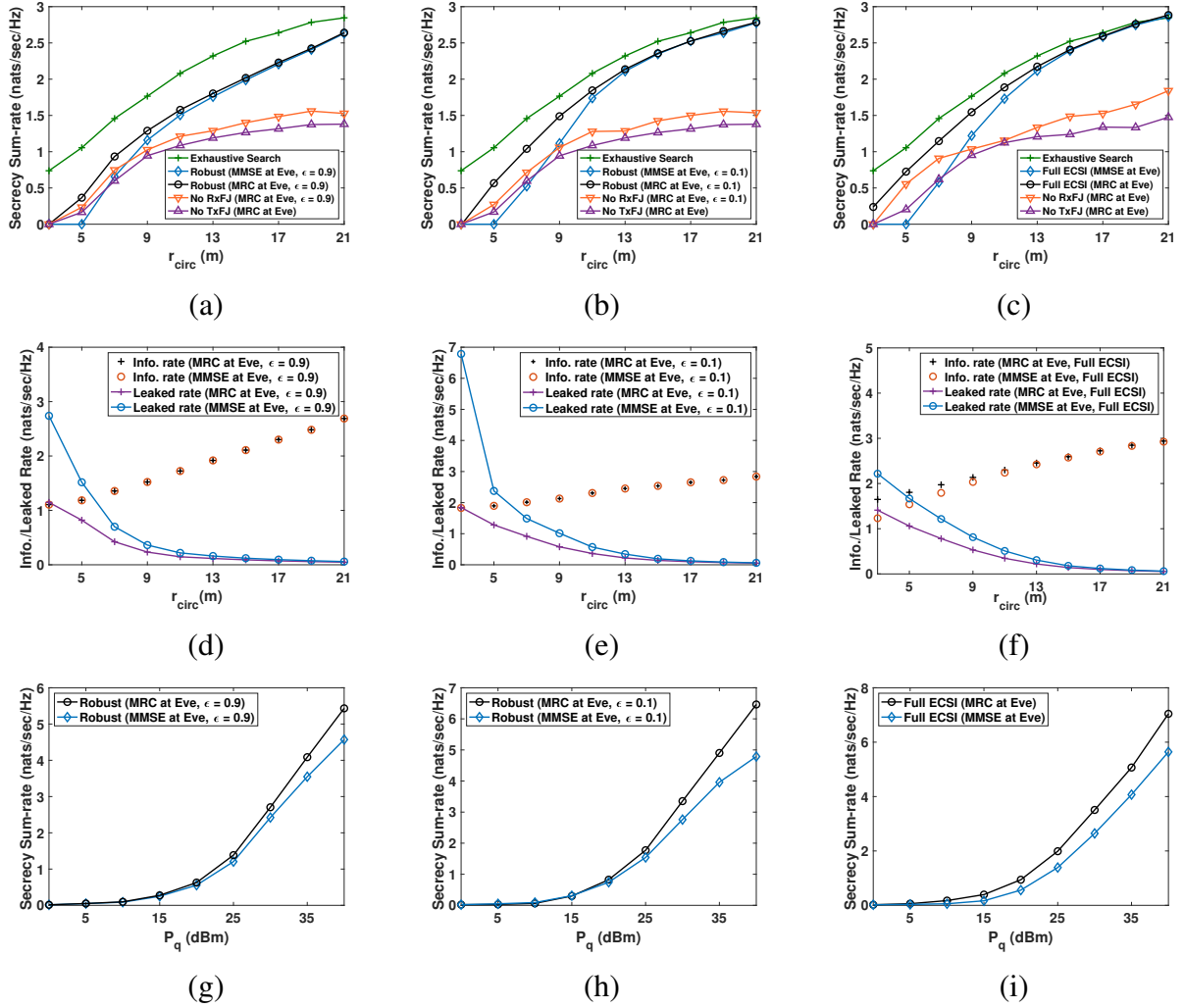


Figure 5.7: (a)-(c): Comparison of secrecy sum-rate, (d)-(e): Comparison of information/leaked rate ( $X_e = Y_e = 5$ ,  $N_q = 8$ ,  $M_q = L = 5$ ,  $\forall q$ ,  $Q = 4$ ), (g)-(i) Secrecy sum-rate vs. transmit power ( $X_e = Y_e = 0$ ,  $r_{\text{circ}} = 10$  m,  $N_q = 8$ ,  $M_q = L = 5$ ,  $\forall q$ ,  $Q = 4$ )

by “Robust” in Figure 5.7(a)-(b)). Furthermore, Figure 5.7 (d)-(f) show the resulting sum of information and leaked rates of our methods vs. the radius of our simulation region. Figure 5.7(a) and (d) correspond to our robust approach where the probability of positive secrecy is  $\varepsilon = 0.9$ , while Figure 5.7(b) and (e) correspond to  $\varepsilon = 0.1$ , and Figure 5.7(c) and (f) correspond to the case of full E-CSI. We also have two baseline schemes in Figure 5.7(a)-(c): the scheme where no RxFJ is used at Bob, and the scheme where no TxFJ is used at Alices. The maximum amount of iterations for Algorithm 1 and 2 is 50. Each approach is examined under two scenarios: 1) when Eve uses MRC decoder, and 2) when Eve uses MMSE decoder.

Although our analysis was limited to the case of using MRC decoder at Eve (see Section II), we still observed the convergence of our algorithm for the case of MMSE decoder. One reason that we did not analyze the case of MMSE receivers at legitimate links or Eve is that MMSE receivers add to the complexity of links’ best responses. In fact, in addition to the TxFJ and RxFJ powers being updated at each iteration of the game, the MMSE receiver needs to be updated at each iteration of the game as well, thus increasing the complexity of a link’s actions. In contrast, using the MRC decoder employed at Eve/Bobs allows us to only focus on TxFJ and RxFJ PA<sup>26</sup>.

From Figure 5.7(a)-(c), it can be seen that our approaches have less secrecy compared to globally optimal solutions because the NEs of our proposed game are not necessarily guaranteed to be globally optimum for the secrecy sum-rate. Both cases of the robust method have less secrecy sum-rates than that of the full E-CSI method, although the gap is not large. Furthermore, it can be seen that both no RxFJ and no TxFJ schemes have significantly less secrecy sum-rates compared to our approaches, which signifies

---

<sup>26</sup>Further discussion of the difference in computational complexity between MRC and MMSE receivers is provided in Appendix C.

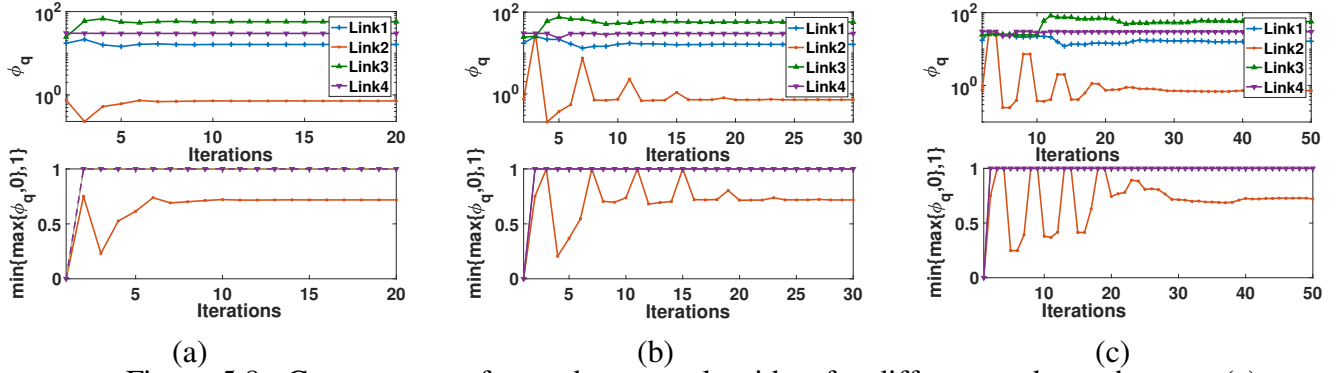


Figure 5.8: Convergence of asynchronous algorithm for different update schemes: (a) Jacobi, (b) Gauss-Seidel, (c) Random updates.

the importance of FJ. Lastly, in our particular simulation scenario, it seems that using no TxFJ affects the secrecy sum-rate more than using no RxFJ. Both of these schemes exhibit worse performance when Eve employs MMSE receiver, which is not shown here due to space limitations.

According to Figure 5.7 (d)-(e), for a given  $\varepsilon$  in the robust method, regardless of the decoder at Eve, the sum of information rates remains the same, which indicates that the interference management between legitimate links in the robust method is completely decoupled from Eve characteristics. In other words, in the robust method, the nodes are indifferent to E-CSI. Moreover, for when  $\varepsilon = 0.9$ , the leaked rate is significantly reduced compared to when  $\varepsilon = 0.1$  because the probability of achieving positive secrecy is set to be higher for when  $\varepsilon = 0.9$ . However, the penalty for achieving positive secrecy with high probability (in the robust method) is that the nodes have less power remaining for their information signals and thus cannot manage interference between themselves as efficiently as in the full E-CSI case or the case where  $\varepsilon = 0.1$ . We can see that when  $r_{\text{circ}}$  is large (i.e., low SINR at Eve) the performance of MRC and MMSE are very close to each other. This is in fact expected, as the MMSE receiver at Eve theoretically reduces to the MRC receiver for low SINR [129]. For smaller  $r_{\text{circ}}$  however, there is a gap between

the performance of MMSE and MRC receivers used at Eve.

Figure 5.7(g)-(i) show that in all approaches secrecy sum-rate grows as  $P_q$  increases. Hence, by using RxFJ and TxFJ, positive secrecy and arbitrary secrecy levels (by changing the links' transmit powers) are achievable, thus extending the same property that existed in the single-user scenario [22]. We also verified such a scaling at the per-link level. Same as what was discussed in previous figures, the secrecy sum-rate achieved for the full E-CSI method (Figure 5.7(i)) is larger than that of the robust methods (Figure 5.7(g)-(h)). Also, comparing Figure 5.7(g) and Figure 5.7(h), we conclude that when  $\varepsilon$  is chosen to be too large, the nodes are not able to do an efficient interference management, thus lower secrecy sum-rate is achieved compared to when  $\varepsilon$  is small.

Figure 5.8 shows the convergence of Algorithm 2 under different update schemes for a settings where the NE is unique. All schemes converge to the same point, indicating the uniqueness of NE. The Jacobi method converges faster due to simultaneous updates for all users at each iteration. For the random updates in Figure 5.8(c), each link generates a random integer between 2 and 6 that specifies the number of iterations when its action is updated after the current one. As expected, asynchronous actions degrade the convergence speed.

## 5.7 Summary

In this chapter, we proposed a framework for a wiretap interference network under which every link can utilize both RxFJ and TxFJ to achieve a positive secrecy rate. Next, we modeled the interaction between the players as a game and derived sufficient conditions for the uniqueness of the resulting NE. We also proposed an asynchronous algorithm that can implement the proposed game. Next, we proposed another version of our game that is robust to when the eavesdropping channels are unknown. We showed in simu-

lation that our proposed approach for achieving positive secrecy using TxFJ and RxFJ are efficient enough to be considered as best responses for legitimate links. Moreover, the performance of robust schemes are close to the one that assumes knowledge of E-CSI. Lastly, the secrecy sum-rate scales with the power budget at legitimate transmitters, regardless of the knowledge of E-CSI.

## CHAPTER 6

# Linear Precoding in Overloaded Wiretap MU-MIMO Networks

## 6.1 Overview

In this chapter, we focus on the application of TxFJ techniques in the downlink of a broadcast network<sup>1</sup>. Alice and Bobs, all have multiple antennas, resulting in a *multiuser MIMO (MU-MIMO) network*. MU-MIMO networks have been the subject of numerous studies, and several standards such as 802.11ac and LTE have been pushed to support this network architecture at least for downlink communications. The use of multiple antennas in MU-MIMO networks grants the best use of spectral resources by simultaneously servicing Bobs in downlink/uplink communications. Precoding approaches proposed over the last two decades have come a long way to approach the capacity of MU-MIMO networks. The theoretical precoding method of *dirty-paper coding* guarantees to achieve the capacity of these networks [130]. However, complicated and non-linear design procedure of this method declines the feasibility of implementing it in real-world systems. Instead, linear precoding schemes, such as the ones based on *zero forcing (ZF)* and *minimum mean square error (MMSE)* [131] criteria, have been extensively used in practical realizations of MU-MIMO networks. The PHY-layer secrecy of MU-MIMO networks has also been studied in the literature, and several precoders have been designed to create TxFJ in such

---

<sup>1</sup>A *broadcast network* refers to a network of one Alice and many Bobs, where each Bob receives his own separate message from Alice.

networks [9, 132]. We narrow down our focus to an MU-MIMO network where Bobs are not malicious nodes, i.e., Bobs are not interested in transmissions of their neighbors. Instead, an external Eve exists in the network. The lower and upper bounds on the secrecy capacity of such networks were derived in [133]. The authors in [132] introduced TxFJ techniques for MU-MIMO networks. The study of MU-MIMO networks when massive number of antennas exist in Alice side was done in [134]. Other interesting problems related to the secrecy performance of FJ, such as the case where spatial correlation exists between Alice's antennas and power allocation between FJ and information signals were considered in [121, 135], respectively.

We are primarily interested in linear precoding design approaches, as non-linear designs are not suitable for practical implementation. In conventional ZF-based methods for MU-MIMO networks, the number of antennas at Alice must be greater than or equal to the total number of antennas at Bobs so as to generate interference-free signals on all Bobs [72]. We refer to this condition as *information rate rank constraint (IRRC)*. The case where IRRC is met is referred to as the *underloaded* scenario. If IRRC is violated, the network is *overloaded*, and hence the ZF-based and MMSE-based precoder designs are infeasible. To satisfy IRRC in overloaded networks, scheduling algorithms have been used to select a subset of Bobs, thus creating an underloaded network. When no information on Eve's location is known (hence FJ techniques are typically used), the ZF method requires the MU-MIMO network to be underloaded to allow for creation of FJ signals [132]. We refer to this condition as the *secrecy rank constraint (SRC)*.

Antenna selection and scheduling are two different approaches to satisfy either IRRC or SRC in MU-MIMO networks. In fact, antenna selection decreases the number of data streams that Bobs can receive by selecting a subset of their antennas, while scheduling aims to reduce the total number of serviced Bobs without removing any of their anten-

nas/streams. In an extensive recent study done by Björnson et.al [136], it was shown that in MU-MIMO networks where several multi-antenna Bobs exist, it is more beneficial (in terms of lowering the bit-error-rate) to decrease the number of streams for each Bob and service many Bobs than to decrease the number of Bobs (by scheduling). Henceforth, we focus on schemes where the number of streams are kept low to serve more Bobs.

While antenna selection can force the network to satisfy IRRC and SRC, selecting a subset of antennas is a difficult integer programming problem [72]. Antenna selection also requires RF switchers. These components can impose delay on receivers' operations if the wireless channels are sufficiently far from being slowly fading channels [137]. RF switchers also increases the cost of production [138]. Lastly, antenna selection may reduce the combining capabilities of Bobs. Specifically, when Bobs switch on a few number of antennas (or RF chains), they cannot increase the diversity as much as when all their antennas are functioning.

Motivated by these challenges, we propose a new linear precoding scheme for the downlink of a MU-MIMO network which uses FJ for achieving secrecy but relies on using a few streams per Bob to function in overloaded settings. To do this, we relax IRRC conditions, allowing for multi-user interference (MUI) between downlink users. However, we aim to minimize MUI at each downlink user via a specific precoder design. Our scheme offers the same complexity as the combination of a ZF-based (or MMSE-based) precoding with a suboptimal antenna selection algorithm. However, the sum-rate of our algorithm is the same as that of ZF-based precoding schemes merged with the optimal antenna selection algorithm.

It turns out that allowing MUI between downlink users not only enables our scheme to operate in overloaded settings, but also imposes the most stringent condition on the number of antennas that Eve requires to cancel out the FJ signals. Overall, the contributions



of this chapter are as follows:

- We propose a linear precoding scheme for the downlink of MU-MIMO networks that relies on minimizing the interference leakage caused from downlink signals. Our precoders are different from ZF-based precoders, as we relax the zero interference leakage condition to improve on the feasibility conditions of traditional precoders in over/fully loaded MU-MIMO networks.
- We also create FJ signals using the linear precoders that we designed for minimizing MUI. Compared to traditional methods of FJ, our approach demands the same complexity but imposes the most stringent condition on the number of antennas that Eve requires to cancel out FJ signals. Using simulations, we show that the freedom in choosing rank of our precoding matrices enables us to establish a trade-off between secrecy, reliability and sum rate of the network.

## Notation

Boldface uppercase/lowercase letters denote matrices/vectors.  $\mathbf{A}^{(:,a:b)}$  and  $\mathbf{A}^{(a:b,:)}$ , respectively denote matrices comprised of columns  $a$  to  $b$  of  $\mathbf{A}$  and rows  $a$  to  $b$  of  $\mathbf{A}$ .  $\mathbf{I}$  and  $\mathbf{0}$  denote the identity matrix and the zero matrix (i.e., matrix with zero entries) of appropriate sizes.  $\mathbb{E}[\bullet]$ ,  $\bullet^\dagger$ ,  $\text{Tr}(\bullet)$  are respectively, the expected value, conjugate transpose, and trace operators. Lastly,  $\mathbb{C}$  is the set of complex numbers.

## General System Model

Consider a network where Alice has  $M$  antennas and communicates with  $Q$  Bobs,  $Q \geq 2$ . Let  $\mathcal{Q} = \{1, 2, \dots, Q\}$ . Bob $_q$  has  $N_q < M$  antennas,  $q \in \mathcal{Q}$ . Without loss of generality, assume that all Bobs have the same number of antennas, i.e.,  $N_q = N < M$ ,  $\forall q \in \mathcal{Q}$ .

An external Eve with  $L$  antennas also exists in the range of communications<sup>2</sup>. The setting where  $M = NQ$  is referred to as the fully-loaded scenario. When  $M < NQ$ , the network is overloaded, and when  $M > NQ$  the network is underloaded. Bob $_q$ ,  $q \in \mathcal{Q}$ , receives  $K_q$  independent streams from Alice, where  $K_q \leq N$ . Without loss of generality, assume that  $K_q = K$ ,  $\forall q \in \mathcal{Q}$ . The number of streams determines how the antennas at Alice and Bobs are exploited. For example,  $K = N$  indicates that the signals intended for Bobs have the maximum number of streams, thus the antennas are used to provide spatial multiplexing. In contrast,  $K = 1$  signifies that the combining features of Bobs are used to increase the diversity (thus reliability) of transmissions.

## 6.2 Conventional Precoder Design

To better understand our method, we first explain the ZF method used in designing the precoding matrices. The received signal at Bob $_q$ ,  $q \in \mathcal{Q}$ , can be expressed as

$$\mathbf{y}_q = \mathbf{H}_q(\mathbf{u} + \mathbf{f}) + \mathbf{n} \quad (6.1)$$

where  $\mathbf{y}_q \in \mathbb{C}^N$ ,  $\mathbf{H}_q \in \mathbb{C}^{N \times M}$  is the complex channel between Alice and Bob $_q$ ,  $\mathbf{u} \in \mathbb{C}^M$  is the signal containing information from Alice,  $\mathbf{f} \in \mathbb{C}^M$  is the FJ signal, and  $\mathbf{n} \in \mathbb{C}^N$  is the AWGN which has i.i.d. zero-mean-circularly-symmetric-complex Gaussian- (ZMCSCG-) distributed entries with  $E[\mathbf{nn}^\dagger] = N_0/N\mathbf{I}$ . The signal  $\mathbf{u}$  is expressed as

$$\mathbf{u} \triangleq \sum_{q=1}^Q \mathbf{u}_q \triangleq \sum_{q=1}^Q \mathbf{T}_q \mathbf{s}_q \quad (6.2)$$

---

<sup>2</sup>A single Eve with  $L$  antennas can also represent several multi-antenna colluding Eves.

where  $\mathbf{u}_q \in \mathbb{C}^M$  is the signal intended for Bob<sub>*q*</sub>.  $\mathbf{T}_q$  is the precoder that is responsible for cancelling the MUI generated from  $\mathbf{u}_q$ .  $\mathbf{s}_q \in \mathbb{C}^K$  is the  $K$ -dimensional information signal ( $K$  streams of data) intended for Bob<sub>*q*</sub>.

Assume that  $\mathbb{E}[\mathbf{s}_q \mathbf{s}_q^\dagger] = \phi P_q / K \mathbf{I}$ , where  $P_q$  is the power of Alice allocated to Bob<sub>*q*</sub>'s signal and  $\phi$  is the portion of Alice's total power allocated to all information signals. Let  $P \triangleq \sum_{q=1}^Q P_q$ , where  $P$  is the Alice's total power. Alice allocates  $\phi P$  of her total power to all information signals. The rest of the power (i.e.,  $(1 - \phi)P$ ) goes to the FJ signal.

We assume that Alice knows all  $\mathbf{H}_i$ ,  $\forall i \in \mathcal{Q}$ , and Bob<sub>*q*</sub> only knows  $\mathbf{H}_q$ . In the channel estimation phase, Alice sends pilot signals to Bobs, so that Bob<sub>*q*</sub> can estimate  $\mathbf{H}_q$  and feed it back to Alice. Substituting (6.2) in (6.1), the effective channel that Bob<sub>*q*</sub> sees from Alice would be  $\mathbf{H}_q \mathbf{T}_q$ . Hence, Alice can apply another precoder for each Bob to optimize her transmissions. Specifically, assume that  $\mathbf{T}_q \in \mathbb{C}^{M \times \tau}$ ,  $K < \tau \leq N$ . Then, Alice can assign an extra precoder  $\mathbf{W}_q \in \mathbb{C}^{\tau \times K}$ , so that  $\mathbf{y}_q$  can be written as

$$\mathbf{y}_q = \mathbf{H}_q \left( \sum_{q=1}^Q \mathbf{T}_q \mathbf{W}_q \mathbf{s}_q + \mathbf{f} \right) + \mathbf{n}. \quad (6.3)$$

Bob<sub>*q*</sub> also applies a linear combiner to estimate the transmitted information signal. In particular, Bob<sub>*q*</sub> applies  $\mathbf{D}_q \in \mathbb{C}^{K \times N}$  to have the following estimate of  $\mathbf{s}_q$ :

$$\hat{\mathbf{s}}_q \triangleq \mathbf{D}_q \mathbf{y}_q = \mathbf{D}_q \left( \mathbf{H}_q \left( \sum_{q=1}^Q \mathbf{T}_q \mathbf{W}_q \mathbf{s}_q + \mathbf{f} \right) + \mathbf{n} \right). \quad (6.4)$$

Let  $\mathbf{H}_q \mathbf{T}_q = \mathbf{U}_q \mathbf{\Sigma}_q \mathbf{V}_q^\dagger$  be the singular-value decomposition (SVD) of  $\mathbf{H}_q \mathbf{T}_q$ , where  $\mathbf{U}_q$  and  $\mathbf{V}_q$  are the unitary matrices of left and right singular vectors, and  $\mathbf{\Sigma}_q$  is the matrix of singular values. Therefore, if Alice sets  $\mathbf{W}_q = \mathbf{V}_q^{(:,1:K)}$  and Bob<sub>*q*</sub> sets  $\mathbf{D}_q = \mathbf{U}_q^{(:,1:K)\dagger}$ , the optimal precoder/combiner duo to estimate  $\mathbf{s}_q$  at Bob<sub>*q*</sub> can be established [132].

We now focus on the design of  $\mathbf{T}_q$  and  $\mathbf{f}$ . The ZF method is based on nullifying both the FJ signal and MUI on unintended Bobs. Formally, the following conditions must be satisfied:

$$\mathbf{H}_r \mathbf{T}_q = \mathbf{0}, \quad r \neq q, \quad \forall r, q \in \mathcal{Q} \quad (6.5a)$$

$$\mathbf{H}_q \mathbf{f} = \mathbf{0}, \quad \forall q \in \mathcal{Q} \quad (6.5b)$$

The precoder  $\mathbf{T}_q$  can be determined as follows. Define  $\bar{\mathbf{H}}_q \triangleq [\mathbf{H}_1^\dagger, \dots, \mathbf{H}_{q-1}^\dagger, \mathbf{H}_{q+1}^\dagger, \dots, \mathbf{H}_Q^\dagger]^\dagger \in \mathbb{C}^{N(Q-1) \times M}$ , and let  $\bar{\mathbf{H}}_q = \mathbf{L}_q \mathbf{J}_q \mathbf{R}_q$  be the SVD of  $\bar{\mathbf{H}}_q$ , where  $\mathbf{L}_q$  and  $\mathbf{R}_q$  denote the matrices of left and right singular vectors, and  $\mathbf{J}_q$  denotes the matrix of singular values. Provided that  $M > N(Q-1)$ ,  $\bar{\mathbf{H}}_q$  has a non-trivial null-space, which can be exploited to meet condition (6.5a). Specifically, if  $M > N(Q-1)$ , Alice sets  $\mathbf{T}_q = \mathbf{R}_q^{(:, B:B+\tau)} \in \mathbb{C}^{M \times \tau}$ , where  $B = N(Q-1) + 1$ , to satisfy (6.5a) for all  $q \in \mathcal{Q}$ . The condition

$$M \geq N(Q-1) + \tau \quad (6.6)$$

constitutes the IRRC in the downlink of the ZF method. The FJ signal mentioned in (6.1) has the following structure in the ZF method. Define  $\tilde{\mathbf{H}} \triangleq [\mathbf{H}_1^\dagger, \dots, \mathbf{H}_Q^\dagger]^\dagger \in \mathbb{C}^{NQ \times M}$ . Let  $\tilde{\mathbf{H}} = \mathbf{L} \mathbf{J} \mathbf{R}$  be the SVD of  $\tilde{\mathbf{H}}$ , where  $\mathbf{L}$  and  $\mathbf{R}$  denote the matrices of left and right singular vectors, and  $\mathbf{J}$  denotes the matrix of singular values. To satisfy (6.5b),  $\tilde{\mathbf{H}}$  must have a non-trivial null-space, which requires  $M > NQ$ . Hence, the inequality  $M > NQ$  is the SRC for the ZF method. We choose  $\tau = N$ , as IRRC in (6.6) is dominated by SRC. The FJ signal is expressed as  $\mathbf{f} = \mathbf{Z} \mathbf{v}$ , where  $\mathbf{Z}$  is the associated precoder for FJ, which spans the null space of  $\tilde{\mathbf{H}}$ , and  $\mathbf{v}$  is the vector of artificial noise that has the same characteristics

of AWGN except that  $\text{Tr}[\mathbf{v}\mathbf{v}^\dagger] = (1 - \phi)P$ . If SRC is violated, the creation of FJ signal becomes infeasible.

### 6.3 Proposed Signaling Scheme

In this section, we introduce our proposed signaling scheme. Although the precoding design in this section is not much different from previous section, the signaling scheme that we propose here will play an important role in the design of our precoders in the next section. We first modify the signal model at Bobs and Eve in (6.3) and (6.12). Specifically, the received signal at Bob<sub>*q*</sub>,  $q \in \mathcal{Q}$  can be expressed as

$$\mathbf{y}_q = \mathbf{H}_q \mathbf{u}' + \mathbf{n} \quad (6.7)$$

where  $\mathbf{u}'$  is Alice's signal in our proposed signaling scheme:

$$\mathbf{u}' = \sum_{q=1}^Q (\mathbf{u}'_q + \mathbf{f}'_q) \quad (6.8)$$

where  $\mathbf{u}'_q$  is the signal intended for Bob<sub>*q*</sub>,  $q \in \mathcal{Q}$ , and  $\mathbf{f}'_q$  is the FJ signal designed to protect Alice's transmissions that are intended for Bob<sub>*q*</sub>. In fact, compared to (6.1), the main change in the signal model is the decomposition of the FJ signal (i.e., convert  $\mathbf{f}$  to  $\mathbf{f}'_q$ ,  $q \in \mathcal{Q}$ ) in a way that each FJ signal exclusively protects the transmissions intended for one Bob.

A more detailed representation of  $\mathbf{u}'$  can be given as

$$\mathbf{u}' = \sum_{q=1}^Q \mathbf{T}'_q (\mathbf{W}'_q \mathbf{s}_q + \mathbf{Z}'_q \mathbf{v}'_q) \quad (6.9)$$

with  $\mathbf{u}'_q = \mathbf{T}'_q \mathbf{W}'_q \mathbf{s}_q$  and  $\mathbf{f}'_q = \mathbf{T}'_q \mathbf{Z}'_q \mathbf{v}'_q$ . The precoder  $\mathbf{T}'_q$  is responsible for cancelling MUI and FJ on unintended Bobs,  $\mathbf{W}'_q$  is the precoder to boost signal strength on Bob<sub>*q*</sub> (same as  $\mathbf{W}_q$  in previous section),  $\mathbf{Z}'_q$  is the precoder for the FJ signal that protects Bob<sub>*q*</sub>, and  $\mathbf{v}'_q$  is the vector of artificial noise. As before,  $\mathbf{s}_q$  is the  $K$ -stream information signal intended for Bob<sub>*q*</sub>. Because precoder  $\mathbf{T}'_q$  is applied to both information and FJ signals (compare (6.9) and (6.2)), we are ensured that FJ will have no effect on unintended Bobs. As in (6.4), a linear receiver  $\mathbf{D}'_q$  is applied at Bob<sub>*q*</sub> to recover  $\mathbf{s}_q$ . Using (6.7) and (6.9), Bob<sub>*q*</sub> has the following estimate of  $\mathbf{s}_q$

$$\hat{\mathbf{s}}_q \triangleq \mathbf{D}'_q \mathbf{y}_q = \mathbf{D}'_q \left( \mathbf{H}_q \left( \sum_{q=1}^Q \mathbf{T}'_q (\mathbf{W}'_q \mathbf{s}_q + \mathbf{Z}'_q \mathbf{v}'_q) \right) + \mathbf{n} \right). \quad (6.10)$$

The conditions for completely nullifying the MUI and FJ signals for the signal model in this section are as follows:

$$\mathbf{H}_r \mathbf{T}'_q = \mathbf{0}, \quad r \neq q, \quad \forall r, q \in \mathcal{Q} \quad (6.11a)$$

$$\mathbf{D}'_q \mathbf{H}_q \mathbf{T}'_q \mathbf{Z}'_q \mathbf{v}'_q = \mathbf{0}, \quad \forall q \in \mathcal{Q} \quad (6.11b)$$

The design of  $\mathbf{T}'_q$ ,  $\mathbf{W}'_q$ , and  $\mathbf{D}'_q$  would be the same as those of  $\mathbf{T}_q$ ,  $\mathbf{W}_q$  and  $\mathbf{D}_q$  in the previous section. Therefore, the IRRC of our method is the same as that of conventional ZF. All FJ signals are removed by a combination of (6.11a) and (6.11b). Notice that (6.11b) is different from (6.5b) in that  $\mathbf{Z}'_q$  in (6.11b) is designed so that only  $\mathbf{v}'_q$  is nullified at Bob<sub>*q*</sub> with the help of  $\mathbf{D}'_q$ . The rest of FJ signals (i.e.,  $\mathbf{v}'_r$ ,  $r \neq q$ ) are removed by  $\mathbf{T}'_q$  that satisfies (6.11a). Therefore, the SRC of our method is determined by the condition that is the most dominant in (6.9). Due to keeping the same design of the conventional ZF method for  $\mathbf{T}'_q$ , the SRC is the same as IRRC in our method, i.e.,  $M \geq NQ$  given that  $\tau = N$  (see (6.6)).

Because we use a different procedure to nullify the FJ signal, the design of  $\mathbf{Z}'_q$  is different from  $\mathbf{Z}$  of the previous section in that  $\mathbf{Z}'_q$  is designed for each Bob $_q$ . Let  $\mathbf{H}_q \mathbf{T}'_q = \mathbf{U}'_q \mathbf{\Sigma}'_q \mathbf{V}'_q{}^\dagger$  be the SVD of  $\mathbf{H}_q \mathbf{T}'_q$ , where  $\mathbf{U}'_q$  and  $\mathbf{V}'_q$  are the unitary matrices of left and right singular vectors, and  $\mathbf{\Sigma}'_q$  is the matrix of singular values. Therefore, if Alice sets  $\mathbf{W}'_q = \mathbf{V}'_q(:, 1:K)$ ,  $\mathbf{D}'_q = \mathbf{U}'_q(:, 1:K)^\dagger$  (same as previous section), and  $\mathbf{Z}'_q = \mathbf{V}'_q(:, K+1:\tau)$ , then (6.11b) is also satisfied (compare with the design of  $\mathbf{Z}$ ).

### 6.3.1 Security Analysis of Proposed Method

The received signal at Eve can be expressed as

$$\mathbf{z} = \mathbf{G}\mathbf{u}' + \mathbf{e} = \mathbf{G} \left( \sum_{q=1}^Q (\mathbf{u}'_q + \mathbf{f}'_q) \right) + \mathbf{e} \quad (6.12)$$

where  $\mathbf{G} \in \mathbb{C}^{L \times M}$  is the channel between Alice and Eve, and  $\mathbf{e}$  has the same characteristics as  $\mathbf{n}$  in (6.1). Eve has to first combat the MUI to be able to wiretap ongoing communications. Eve does so by applying a linear combiner. For example, to eavesdrop on signals intended for Bob $_q$ , Eve first applies  $\mathbf{A}'_q$  on the signal she receives. Define  $\mathbf{z}_q \triangleq \mathbf{A}'_q \mathbf{z}$ . Upon cancelling MUI with  $\mathbf{A}'_q$ , Eve applies  $\mathbf{B}'_q$  on  $\mathbf{z}_q$  to estimate  $\mathbf{s}_q$ . In other words, Eve's estimation from  $\mathbf{s}_q$  is  $\tilde{\mathbf{s}}_q = \mathbf{B}'_q \mathbf{z}_q$ . We assume the worst-case scenario where Eve knows  $\mathbf{G}$ . For instance, Eve can use the pilot signals sent from Alice in the channel estimation phase to estimate  $\mathbf{G}$ . Moreover, because Bobs have to explicitly feed back the channel estimates to Alice, Eve can snoop on the channel estimation feedback from Bobs to gain knowledge of all  $\mathbf{H}_q$ ,  $\forall q \in \mathcal{Q}$ . Note, however, that neither Alice nor Bobs have any knowledge of  $\mathbf{G}$ , i.e., Eve is a passive eavesdropper.

We now describe how Eve chooses her combiners to decode Alice's transmissions. We also show how many antennas Eve requires to decode all messages. Using (6.12),

$\mathbf{z}_q = \mathbf{A}'_q \mathbf{z}$ , and the linear estimate  $\tilde{\mathbf{s}}_q = \mathbf{B}'_q \mathbf{z}_q$ , we have the following

$$\tilde{\mathbf{s}}_q = \mathbf{B}'_q \mathbf{A}'_q \left( \mathbf{G} \left( \sum_{q=1}^Q (\mathbf{u}'_q + \mathbf{f}'_q) \right) + \mathbf{e} \right). \quad (6.13)$$

Eve cancels MUI by designing a combiner  $\mathbf{A}'_q$  such that

$$\mathbf{A}'_q \mathbf{G} (\mathbf{u}'_r + \mathbf{f}'_r) = 0, \quad r \neq q, \quad \forall r, q \in \mathcal{Q} \quad (6.14a)$$

$$\mathbf{A}'_q \mathbf{G} \mathbf{f}'_q = 0, \quad \forall q \in \mathcal{Q} \quad (6.14b)$$

Using (6.8), (6.9) and (6.13), Eve first constructs the following blocked matrix

$$\mathbf{G}'_q = [\Omega'_1, \dots, \Omega'_{q-1}, \Omega'_{q+1}, \dots, \Omega'_Q, \Gamma'_q] \quad (6.15)$$

where  $\Omega'_q = \mathbf{G} \mathbf{T}'_q \in \mathbb{C}^{L \times \tau}$  and  $\Gamma'_q = \mathbf{G} \mathbf{T}'_q \mathbf{Z}'_q \in \mathbb{C}^{L \times \tau - K}$ . Eve sets  $\mathbf{A}'_q$  to be the last  $K$  columns of the matrix of left singular values of  $\mathbf{G}'_q$ . For such a choice of  $\mathbf{A}'_q$  that allows Eve to cancel MUI and FJ, the minimum value of  $L$  is derived by counting the column of  $\mathbf{G}'_q$ , i.e.,

$$\Psi' = \tau(Q - 1) + (\tau - K) + K = \tau Q \quad (6.16)$$

Setting  $\tau = N$ , we have  $\Psi' = NQ$ . The first term in the right hand side (RHS) of (6.16) is the number of antennas that  $\Omega_r$ ,  $r \neq q$ ,  $r \in \mathcal{Q}$  occupies in establishing  $\mathbf{G}'_q$  in (6.15). The second term in (6.16) is the number of antennas that  $\Gamma'_q$  occupies in (6.15). Finally, the third term is the number of antennas that are required to recover  $\mathbf{s}_q$  after nullifying MUI and FJ. The same security analysis can be done for the ZF method, and it can be shown that if Alice uses the conventional ZF method, Eve requires at least  $\Psi = M - (N - K)Q$



antennas.

### 6.3.2 Comparison Between Conventional ZF Method and Proposed Method

We now compare required the number of Eve's antennas for both the ZF and the proposed method to decode all messages in an underloaded scenario, i.e., we compare  $\Psi$  and  $\Psi'$  when  $M > NQ$ . Consider the conditions when  $\Psi > \Psi'$ , i.e.,  $M - (N - K)Q > NQ$ . In other words, we examine when the ZF method is better than our approach. Clearly such a comparison depends on  $K$ , which is analyzed as follows:

- For  $K = N$ , we end up with  $M > NQ$ , which is always true in the underloaded scenario, so in the case of using all streams (i.e., spatial multiplexing), the ZF method imposes a more stringent condition than our method.
- For  $K < N$ , the simplified inequality is  $2N - K < \frac{M}{Q}$ . By lowering the number of streams ( $K$ ), it can be deduced that the ZF method imposes more antennas on Eve than our method only when the network is *sufficiently* underloaded. To clarify, take the extreme example of  $K = 1$ ; In this case,  $M - (N - K)Q > NQ$  is reduced to  $M > (2N - 1)Q$  which is more demanding than an underloaded network (i.e.,  $M > NQ$ ) with  $N > 1$ .

Overall, when a few streams are selected for each Bob, the ZF method does not impose more antennas on Eve than our proposed method unless the network is sufficiently underloaded. Normally, a sufficiently underloaded is not preferred, as the MU-MIMO network would not be fully utilized.

### 6.3.3 Antenna Selection for Zero-Forcing Precoding

To compensate for the absence of FJ in over/fully loaded scenarios, antenna selection algorithms can be used to decrease the number of functioning receive antennas at Bobs from  $N$  to  $N'$ , so that SRC can be satisfied, i.e.,  $M > N'Q$ . We mainly focus on *capacity-based* antenna selection algorithms, but our analysis can be simply extended to other types of antenna selection algorithms. We introduce antenna selection for when the network is over/fully loaded, i.e., the number of Bobs is large enough that  $M \leq NQ$ .

The capacity of the channel between Alice and Bob <sub>$q$</sub> ,  $q \in \mathcal{Q}$  can be expressed as<sup>3</sup>

$$C_q = \log \det(\mathbf{I} + \phi P_q \mathbf{H}_q \mathbf{H}_q^\dagger) \quad (6.17)$$

Using antenna selection, we are interested in switching on only  $K \leq N' < N$  antennas of Bob <sub>$q$</sub>  such that  $M > N'Q$ . Denote  $\bar{\mathbf{H}}_q$  as a matrix comprised of  $N'$  columns of  $\mathbf{H}_q$ . Denote  $\mathcal{S}(\mathbf{H}_q)$  as the set of matrices that are formed using  $N'$  rows of  $\mathbf{H}_q$ . Therefore, the problem of antenna selection can be formulated as

$$\bar{\mathbf{H}}_q^* = \arg \max_{\mathcal{S}(\mathbf{H}_q)} \left( \log \det(\mathbf{I} + \phi P_q \bar{\mathbf{H}}_q \bar{\mathbf{H}}_q^\dagger) \right) \quad (6.18)$$

where  $\bar{\mathbf{H}}_q^* \in \mathbb{C}^{N' \times M}$ . The optimal antenna selection is a difficult integer programming problem, thus suboptimal algorithms such as [139] can be used which are based on maximizing the upper bounds of the capacity. After performing the antenna selection at each Bob, the SRC is expected to be met (i.e.,  $M > N'Q$ ), which allows for creation of FJ. Hence, by replacing  $N$  with  $N'$ , we can deduce that the number of antennas required

---

<sup>3</sup>Note that such a capacity can be achieved with dirty-paper coding scheme, which is a non-linear precoding method [130].

at Eve to cancel out FJ and MUI in the ZF method with antenna selection would be  $M - (N' - K)^4$ .

#### 6.4 Proposed Precoding Method

The current precoder design for  $\mathbf{T}'_q$  in our proposed signaling scheme has two issues. First, the IRRC condition is still the same as that of the conventional ZF method, which prohibits our signaling scheme from operating in overloaded scenarios. Second, after implementation of these precoders, although for  $K < N$  our signaling scheme can impose more antennas on Eve to decode the ongoing messages –by adding more columns to matrix  $\mathbf{G}'_q$  in (6.13), see Section 6.3.2–, it turns out that the rank of  $\mathbf{G}'_q$  does not increase with the added columns. Therefore, Eve can still decode the signals with fewer antennas than what our proposed signaling scheme claims. In this section, we modify the design of  $\mathbf{T}'_q$  to resolve these issues.

To do so, we relax condition (6.11a) in a way that MUI created from  $\mathbf{s}_q$  inflicts the least amount of damage on the reception of other Bobs. Formally, we design the precoder  $\mathbf{T}'_q$ ,  $q \in \mathcal{Q}$  using an optimization problem that is detailed later on. Before presenting this optimization problem, we formulate the ZF method as a variant of a family of optimization problems. Consider the following optimization problem

$$\begin{aligned} \underset{\mathbf{T}'_q}{\text{maximize}} \quad & \frac{\|\mathbf{H}_q \mathbf{T}'_q\|_F}{\sum_{\substack{r=1 \\ r \neq q}}^Q \|\mathbf{H}_r \mathbf{T}'_q\|_F + \frac{N_0}{\phi P_q}} \\ \text{s.t.} \quad & \mathbf{T}'_q{}^\dagger \mathbf{T}'_q = \mathbf{I} \end{aligned} \tag{6.19}$$

where  $\|\bullet\|_F$  is the Frobenius norm. In problem (6.19) the precoder for Bob<sub>*q*</sub> must be de-

---

<sup>4</sup>Clearly, antenna selection can also be performed in situations where IRRC is also violated. However, for the sake of brevity, we only apply antenna selection to satisfy SRC.

signed in a way that the interference generated from  $\mathbf{s}_q$  (i.e., denominator of the objective in (6.19)) is minimized while the strength of  $\mathbf{s}_q$  at Bob<sub>*q*</sub> (i.e., the numerator of the objective) is maximized. The constraint on  $\mathbf{T}'_q$  causes the product  $\mathbf{H}_q \mathbf{T}'_q$  to have the same statistical properties of  $\mathbf{H}_q$ . Problem (6.19) is identified as a Rayleigh quotient problem [140]. It is easy to see that when  $N_0 \ll \phi P_q$  (i.e., high SNR scenario), the solution to (6.19) reduces to the ZF method from the previous section because the maximum objective value would be achieved if the denominator goes to zero, which is in line with condition (6.5a) or (6.11a). In moderate SNRs, the solution to (6.19) reduces to MMSE-based precoding methods [141]. Also notice that problem (6.19) does not impose any rank constraint on its solution. We now examine (6.11a) again. This condition imposes the result of  $\mathbf{H}_q \mathbf{T}'_q$  to have entries with the minimum possible value. We decompose (6.11a) as follows:

$$\mathbf{H}_r \mathbf{T}'_q(:,n) = \mathbf{0}, \quad r \neq q, \quad \forall r, q \in \mathcal{Q} \ \& \ \forall n \quad (6.20)$$

where  $\mathbf{T}'_q(:,n)$  is the  $n$ th column of  $\mathbf{T}'_q$ . In fact (6.20) suggests the same condition in (6.11a) but is represented on a column-by-column basis. Also notice that since we have not explicitly designed  $\mathbf{T}'_q$  yet, we do not impose any constraints on its rank, thus no information is yet available on the values that  $n$  in (6.20) can take. For now, assume that  $n \in \{1, \dots, \tau\}$  where  $K \leq \tau \leq N$ . Instead of (6.19), we propose our precoding method by formulating the following optimization problem

$$\begin{aligned} & \underset{\mathbf{T}'_q}{\text{maximize}} \quad \frac{\|\mathbf{H}_q \mathbf{T}'_q(:,n)\|_F}{\sum_{\substack{r=1 \\ r \neq q}}^Q \|\mathbf{H}_r \mathbf{T}'_q(:,n)\|_F + \frac{N_0}{\phi P_q N}} \\ & \text{s.t.} \quad \mathbf{T}'_q(:,n) \mathbf{T}'_q(:,n)^\dagger = \frac{1}{\tau}, \quad n \in \{1, \dots, \tau\}. \end{aligned} \quad (6.21)$$

Problem (6.21) is still a Rayleigh quotient problem, but the difference with (6.19) is that

in (6.21) we find the solution on a column-by-column basis. The constraint in (6.21) ensures that the resulting precoder does not violate the power constraint. In fact, because we assumed that  $E[\mathbf{s}_q \mathbf{s}_q^\dagger] = \phi P_q / K \mathbf{I}$ , we must also ensure that ideally,  $E[\mathbf{T}'_q \mathbf{s}_q \mathbf{s}_q^\dagger \mathbf{T}'_q{}^\dagger] = \phi P_q / K \mathbf{I}$  (see (6.2) and description of  $\mathbf{s}_q$  below it). The solution to (6.21) is given by [142]

$$\mathbf{T}'_q{}^{*(:,n)} = \frac{1}{\sqrt{\tau}} \frac{\Delta^{(:,n)}}{\|\Delta^{(:,n)}\|_F} \quad (6.22)$$

where  $\Delta$  is the matrix of generalized eigenvectors corresponding to  $\tau$  non-zero generalized eigenvalues of numerator and denominator of the objective in (6.21), i.e.,

$$\Delta \triangleq \text{eig}_{\max, \tau} \left( \mathbf{H}_q^\dagger \mathbf{H}_q, \sum_{\substack{r=1 \\ r \neq q}}^Q \mathbf{H}_r^\dagger \mathbf{H}_r + \frac{N_0}{\phi P_q N} \right) \quad (6.23)$$

where  $\text{eig}_{\max, \tau}$  is the operator for extracting  $\tau$  generalized eigenvector that correspond to  $\tau$  non-zero generalized eigenvalues. From the properties of generalized eigenvalue problems, it can be deduced that there are  $N$  eigenvectors that correspond to non-zero generalized eigenvalues in (6.23) [142]. Hence,  $\Delta \in \mathbb{C}^{M \times \tau}$ .

Solving problem (6.21) allows us to relax the condition in (6.11a). Interestingly, there is no guarantee on the solution of (6.21) to satisfy the constraint of (6.19), which makes (6.19) and (6.21) to be essentially not equivalent to each other. Even in high SNR scenario, there is no guarantee on the equivalence of the solutions of (6.19) and (6.21). In fact, that the resulting precoders of (6.21) are do not necessarily have diagonal covariance matrices to satisfy the constraint in (6.19). However, the constraint in (6.21) ensures that  $\mathbf{T}'_q{}^*$  does not violate the power constraint at Alice. Specifically, in  $\mathbf{T}'_q{}^{*\dagger} \mathbf{T}'_q{}^*$ , we have the following

$$\mathbf{T}'_q{}^{*(:,r)\dagger} \mathbf{T}'_q{}^{*(:,n)} = \frac{1}{\tau} \frac{\Delta^{(:,r)\dagger} \Delta^{(:,n)}}{\|\Delta^{(:,r)}\|_F \|\Delta^{(:,n)}\|_F} \leq \frac{1}{\tau}. \quad (6.24)$$

Therefore,  $\|\mathbf{T}_q'^{*(:,n)\dagger}\mathbf{T}_q'^*\|_F \leq 1$  is guaranteed, ensuring that our proposed precoding in (6.21) does not violate the power constraint, i.e.,  $E[\mathbf{T}_q'^*\mathbf{s}_q\mathbf{s}_q^\dagger\mathbf{T}_q'^*] \leq \phi P_q/K\mathbf{I}$ <sup>5</sup>. In summary, our proposed method in (6.21) relaxes the general shape of the ZF-based and MMSE-based precoders that are known from problem (6.19), such that the MUI is still minimized as much as possible.

In case of an underloaded network (i.e.,  $M > NQ$ ), we set  $\tau = N$  (i.e., same as Section 6 and 6). In case of over/fully loaded networks (i.e.,  $M \leq NQ$ ), we set  $\tau = \lceil \frac{M}{Q} \rceil$ , where  $\lceil \bullet \rceil$  is the ceiling function to handle the case of non-integer values of  $\tau$ . Notice that in an overloaded scenario, we do not decrease  $Q$  via scheduling. Instead, we have the freedom in choosing  $\tau$  and still keeping all users in the network. Using the fact that  $K < \tau \leq N$ , we can also determine the value of  $K$ . After designing  $\mathbf{T}_q'$  and determining  $K$ , the remaining matrices in our proposed method (i.e.,  $\mathbf{W}_q'$ ,  $\mathbf{D}_q'$  and  $\mathbf{Z}_q'$ ) can be designed as in Section 6. Hence, all terms in (6.9) and (6.10) are defined, and our proposed precoding method is complete.

The security analysis of our method in underloaded scenarios was already done in Section 6.3.2, where we showed Eve requires  $\Psi' = \tau Q$  antennas to decode all messages. In the case of overloaded network as mentioned before, we choose  $\tau = \lceil \frac{M}{Q} \rceil$ . Hence,  $\Psi' = \max\{\tau Q, M\}$  which is the most stringent condition on Eve's number of antennas. The conventional ZF method is not able to generate the FJ signal in an overloaded network because condition (6.5b) cannot be satisfied. Hence, it can be shown that Eve only requires  $\Psi = KQ$  antennas to decode all messages in ZF method. As  $KQ < \max\{\tau Q, M\}$ , then our method always performs better than the conventional ZF scheme in overloaded networks.

---

<sup>5</sup>In the ZF method, it can be easily seen that the resulting ZF precoder satisfies  $\|\mathbf{T}_q'^{(:,n)\dagger}\mathbf{T}_q'\|_F = 1$ . Thus,  $E[\mathbf{T}_q'\mathbf{s}_q\mathbf{s}_q^\dagger\mathbf{T}_q'] = \phi P_q/K\mathbf{I}$ .

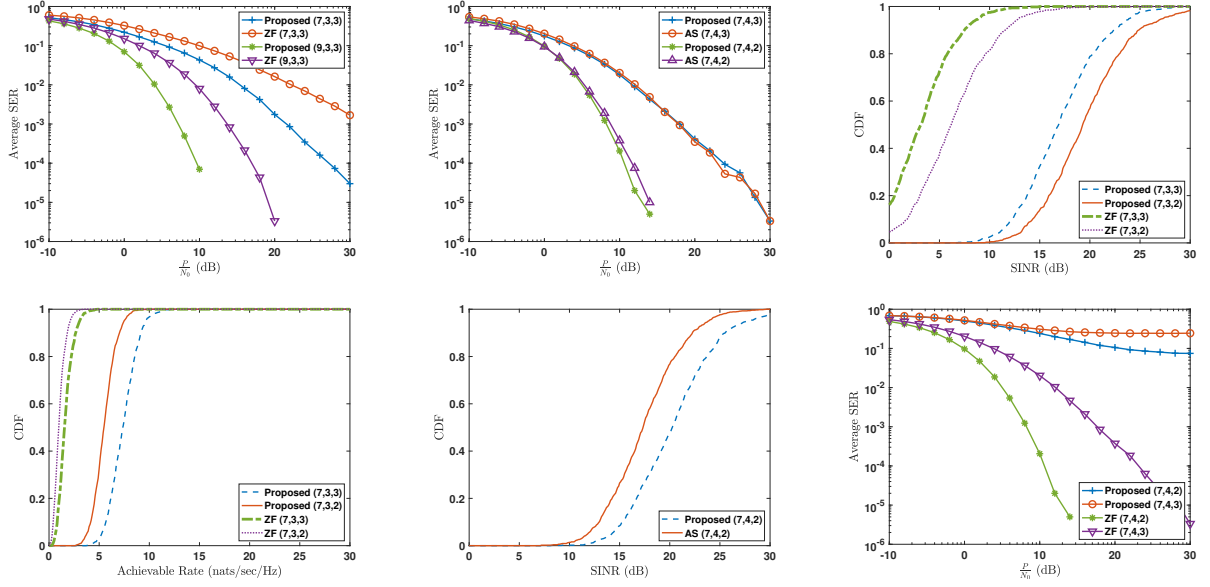


Figure 6.1: Comparison of (a) SER (Underloaded) (b) SER (Overloaded) (c) achieved SINR (Underloaded) (d) achievable rate (Underloaded) (e) achieved SINR (Overloaded) (f) Eve's SER (Overloaded)

Notice that our proposed precoder design for  $\mathbf{T}'_q$  in this section can also be used in the conventional ZF method to design  $\mathbf{T}_q$  for overloaded scenarios and relax condition (6.5a). However, there will be no increase in the number of Eve's antennas required to decode Alice's messages because the design of FJ in the conventional ZF method is decoupled from the design of  $\mathbf{T}_q$ .

Overall, the combination of our signaling scheme in Section 6 and the precoder design in Section 6.3.3 not only handles the overloaded scenarios (without scheduling), but also increases the rank of  $\mathbf{G}'_q$  in (6.13), which leads to increase in the number of antennas that Eve requires to decode all messages.

Although our method and the optimal antenna selection perform equally, we already mentioned that antenna selection methods are prone to many issues which are mainly to do with requiring RF switchers. However, our approach does not require these con-

siderations. In terms of computational complexity of our method and antenna selection, our method is dominated by the computation of generalized eigenvalues and several SVD calculations. The complexity of antenna selection methods are also dominated by the calculation of SVD and solving the optimization in (6.18). Our derivations –which are skipped here for the sake of brevity– show that both methods demand the same amount of computational complexity.

## 6.5 Numerical Results

We verify our theoretical analyses via simulations. All simulations are done for a network of  $Q = 2$  Bobs. Similar conclusions can be drawn for networks with more Bobs and more antennas at Alice. Our *proposed method* in these simulations is the combination of the methods in Section 6 and Section 6.3.3, while the simulated ZF method is the scheme that we discussed in Section 6. In our proposed method, the power allocated to Bob’s message is divided equally between its associated information and FJ signals. Same is done for the ZF method. We use uncoded QPSK modulation for all simulations. For simulation that show SINR and achievable rate, we use Gaussian codebooks. The triplet  $(M, N, K)$  in all simulations denote number of Alice/Bob antennas and number of data streams.

Figure 6.1 (a) shows the symbol error rate (SER) of the Alice-Bob channels, averaged across all Bobs for an underloaded scenario. It can be seen that our proposed method outperforms the ZF method for both settings because our precoders are more flexible. In fact, although the precoders designed by the ZF method completely suppress MUI, they also do not contribute to the strength of the signal to the intended user.

Figure 6.1 (b) shows the SER for an overloaded scenario. It can be seen that our method’s performance is close to that of antenna selection (AS) schemes. However, as



mentioned earlier, our method does not have the problems of AS schemes (see Section 6 for our thorough explanation about AS schemes).

Figure 6.1 (c) shows the CDF of the achieved SINR in an underloaded scenario. Our method achieves higher SINR compared to the ZF method. This in fact decreases the SER of our scheme as shown in Figure 6.1 (a).

Figure 6.1 (d) shows the CDF of achievable information rate. As can be seen, our method also achieves a higher rate. Therefore, our method achieves a better tradeoff between diversity (i.e., SINR in Figure 6.1 (b) and multiplexing (i.e., achievable rate in Figure 6.1 (c)). Moreover, in both Figs 2 and 3, it can be seen that using a higher number of streams results in a lower SINR but higher achievable rate, and vice versa, signifying that a lower number of streams exploits the diversity of multiple antennas.

Figure 6.1 (e) shows the SINR of our method in an overloaded scenario. It can be seen that our method performs better than AS schemes because in AS, by switching off  $\lceil \frac{M}{Q} \rceil$  antennas, the combining capabilities of Bobs decreases, but our method does not require to turn off RF chains at Bobs. However, this achieved SINR does not result in a better BER as seen in Figure 6.1 (b). Similar results can be established for the achievable rate of our method and AS in overloaded networks.

Figure 6.1 (f) shows the SER of Eve in an overloaded scenario when  $L = 6$ . Both  $(7, 4, 3)$  and  $(7, 4, 2)$  settings represent overloaded scenarios. In both settings, we set  $\tau = 4$ . Clearly, no FJ can be created in these settings using the ZF method. It can be seen that our method performs significantly better than the ZF scheme in both overloaded settings because our method forces Eve to have at least  $\Psi' = \max\{\tau Q, M\}$  antennas to decode all messages. However, the ZF method only imposes  $\Psi = KQ$  antennas in overloaded scenarios. In both of these settings,  $L = 6$  antennas would be enough to decode all messages in the ZF design. It can be seen that the setting  $(7, 4, 3)$  experiences

more SER because more data streams are used per user, which decrease the diversity gain.

## **6.6 Summary**

In this chapter, we proposed a novel precoding scheme that not only manages the interference in MU-MIMO networks better than the zero-forcing method, but also enables the nodes to operate in overloaded settings. Compared to the ZF method, our scheme is able to impose more stringent conditions on Eve's number of antennas in overloaded scenarios. Our method also did not require the hardware modifications that some other methods, such as antenna selection schemes, demand in overloaded networks. Analysis of this scheme in massive MIMO networks, or with limited feedback from downlink users, or with in-band full-duplex capability in nodes are the subject of future research.

## CHAPTER 7

## Conclusions and Future Work

### 7.1 Conclusions

In this dissertation, we proposed to advance the state-of-art in PHY-layer wireless security in multi-user, multi-link scenarios, including MU-MIMO and P2P networks. We considered that external eavesdropper(s) snoop on ongoing communications in such networks. Our security techniques were all based on creation of an intentional artificial interference known as friendly jamming (FJ) at each legitimate node to accompany its secret message, such that eavesdroppers' reception quality are degraded but the intended legitimate receiver's signal quality is intact. In designing such techniques, a significant challenge was how to prevent friendly jamming signals from interfering with multiple unintended but legitimate ongoing receptions. Overall, we showed that careful management of multi-user interference between legitimate links can improve secrecy in the network, as interference can be used to jam potential eavesdroppers once it is avoided from being captured on legitimate nodes.

First, we designed a game theoretic secure precoder optimization for a MIMO interference network with several MIMO-enabled eavesdroppers. We proposed three algorithms to increase secrecy sum-rate. In the first algorithm, the links myopically optimize their transmission until a quasi-Nash equilibrium (QNE) is reached. Because of the inferior performance of first algorithm in case of multiple QNEs, we designed the second algorithm based on the concept of variational inequality. The second algorithm enables us to analytically

ically derive convergence conditions, but achieves the same secrecy sum-rate as the first algorithm. To increase the secrecy sum-rate, we proposed the third algorithm in which the links can select the best QNE according to a certain design criterion. Simulations showed that not every criterion is good for the performance improvement. Specifically, reducing co-channel interference is a better criterion compared to explicitly increasing interference at the eavesdroppers to improve secrecy sum-rate.

Second, we studied distributed design of FJ control in a MIMO wiretap interference network using practical precoders. Our study was conducted under various eavesdropping capabilities, e.g., size of antenna array at Eve, as well as her receive-based beamforming capabilities. Compared to the precoder optimization in our first contribution, our methods in the second contribution enjoyed a variety of improvements, such as more robustness to Eve's capabilities (i.e., disabling powerful decoders at Eve), low control signaling overhead, etc. We then showed that greedy FJ is not an optimal approach in terms of total network secrecy rate. Accordingly, we designed a price-based FJ control that guarantees a local optimum point in maximizing the secrecy sum-rate. Through simulations, we observed a noticeable improvement in the secrecy sum-rate when pricing is leveraged for FJ control. We then introduced uncertainty in the eavesdropping channel and designed a robust method. We showed via simulations that the robust method achieves a higher secrecy sum-rate than the greedy FJ approach. Some of the proposed designs were also implemented on software-defined radios to assess their performances in real-world scenarios.

Third, we proposed a game-theoretic approach for power control in an interference network tapped by an external eavesdropper. In addition to transmit-based FJ (TxFJ), in this design every link can utilize receiver-based FJ (RxFJ) as well. We then modeled the interaction between the players as a game and derived sufficient conditions for the unique-

ness of the resulting Nash equilibrium (NE). Compared to previous designs, our design allowed us to implement an asynchronous algorithm, hence making our design robust to transmission delays in the network. Next, we proposed another version of our game that is robust to when the eavesdropping channels are unknown. Compared to the second contribution, in here we were able to conduct the analysis for more than two links. We also analytically derived each link's optimal strategy using only knowledge of distribution of eavesdropping channel components, while in the previous contribution, we only showed the performance of our method using simulations. Lastly, the secrecy sum-rate scales with the power budget at legitimate transmitters, regardless of the knowledge of eavesdropping channels, thus extending the same property from single-link scenarios.

Fourth, we considered the downlink of a MU-MIMO network in the presence of an external eavesdropper. No knowledge of eavesdropper's location was assumed at the access point. The information signals for downlink users were accompanied by TxFJ. The network was studied in underloaded and overloaded conditions. We proposed a novel precoding scheme for the downlink of MU-MIMO networks that not only manages the interference in MU-MIMO networks better than conventional precoding methods (e.g., zero-forcing), but also enables the nodes to operate in overloaded settings. Apart from better utilization of resources, in terms of PHY-layer secrecy Compared to the zero-forcing (ZF) method, our scheme was shown to be able to impose more stringent conditions on eavesdropper's number of antennas in overloaded scenarios. All of these improvements were made possible by allowing interference in the system. In fact, conditioned on the fact that interference for legitimate downlink users are minimized, the secrecy of the system was shown to be increased when facing an eavesdropper with high number of antennas. In contrast, the ZF method explicitly removes interference on legitimate links. Such a constraint leads to precoders that cannot neither operate in overloaded settings nor deal

with an eavesdropper with large number of antenna arrays.

## 7.2 Future Work

There exist multiple directions for future research. In the following, we list several of them.

- **Analysis under finite block length coding and/or finite alphabet inputs:**

Throughout this dissertation, we used secrecy rate equations that are achievable via Gaussian codebooks. Such a choice enabled us to have tractable mathematical optimization problems for complete analysis of interference networks. Hence, we were able to take the first steps in developing methods for interference exploitation. However, the next step would be to extend these analyses to both finite block length coding schemes and finite alphabet inputs. The analysis under finite block length regime can be beneficial for links with bursty transmissions. In such cases, even the M-QAM approximation of Gaussian codebook's rate (see Chapter 1) may not be justifiable.

Regarding the analysis under finite alphabet input, most works so far considered codebooks with fixed rates (see [12] and references therein). In such a situation, the analysis of secrecy must be conducted over many codebooks to ensure a good tradeoff point between leakage and information rate. Even if this issue can be handled, the achievable secrecy rates do not have close-form expressions, which can complicate the analysis under multi-link scenarios. Therefore, more research is needed on developing methods for tackling such secrecy rates and integrating them into the schemes developed in this dissertation.

- **Achieving asynchronous and distributed precoder design:** In our first contri-

bution for precoder optimization, it was assumed that at each round of the game, “all” of the players are maximizing the utilities. The feasibility of implementing the algorithms using asynchronous update fashions can be a subject of future research.

- **Assessment of vulnerability zone:** A critical hypothesis in this dissertation was the dependence between the Alice-Bob CSI and Alice-Eve CSI when Eve is in the proximity of Bob. Such dependence gives rise to a vulnerability zone, within which the nullified FJ at Bob will also extend to Eve. As shown in our preliminary experiments, such dependence was not observed in a Rayleigh fading environment but observed over a Rician channel (with line-of-sight component). This is yet to be verified experimentally.
- **RxFJ and dynamic range issues:** We assumed that FD receivers are not experiencing dynamic range issues that cause the additive noise at the receive chain to be dependent on the transmit power of the FD device. Relaxing this assumption is a subject for future research to show the trade off in terms of achieved secrecy with RxFJ while approaching dynamic range limits of the receiving device.
- **Implement a highly capable eavesdropping attack:** Theoretically, it is known that such a capable Eve can combat FJ by nullifying its effect. It would be interesting experimentally implement such scenario to verify the extent of this theoretical result.
- **MU-MIMO with large number of antennas and FD-capable downlink users:** Analysis of the secure linear precoding in MU-MIMO settings can be extended to massive MIMO networks as well. In addition, considering limited feedback from downlink users, or in-band full-duplex capability in nodes are also interesting sub-

ject of future research.

- **PHY-layer security in multi-cell networks:** An interesting extension to the current designs in this dissertation would be to design precoders or perform power control for cell-edge users that are being eavesdropped in a multi-cell network. In a sense, such a scenario includes both MU-MIMO and interference networks discussed in this dissertation. Hence, it would be interesting to see how the design evolves from such basic networks.



## APPENDIX A

## Proofs of Chapter 3

## A.1 Proof of Proposition 1

Let  $(\Sigma_q^*, \mathbf{W}_q^*, \{\mathbf{S}_{q,k}^*\}_{k=0}^K)$  denote the limit point of AO iterations found in Line 10 of Algorithm 1 for the  $q$ th link,  $q \in \mathbf{Q}$ . As mentioned earlier, problem (3.15) is convex w.r.t either  $(\Sigma_q, \mathbf{W}_q)$  or  $\{\mathbf{S}_q\}_{k=0}^K$ . Then, recalling the minimum principle in (3.24), we have the following<sup>1</sup>:

$$X_q = [\Sigma_q^{*T}, \mathbf{W}_q^{*T}]^T, Z_q = [\Sigma_q^T, \mathbf{W}_q^T]^T, \quad (\text{A.1a})$$

$$\nabla_{Z_q} \bar{f}_q(\Sigma_q^*, \mathbf{W}_q^*, \{\mathbf{S}_{q,k}^*\}_{k=0}^K) = [-(\nabla_{\Sigma_q} \bar{f}_q)^T, -(\nabla_{\mathbf{W}_q} \bar{f}_q)^T]^T, \quad (\text{A.1b})$$

$$\langle Z_q - X_q, \nabla_{Z_q} \bar{f}_q(\Sigma_q^*, \mathbf{W}_q^*, \{\mathbf{S}_{q,k}^*\}_{k=0}^K) \rangle \geq 0, \forall (\Sigma_q, \mathbf{W}_q) \in \mathcal{F}_q, \quad (\text{A.1c})$$

$$\langle \mathbf{S}_{q,k} - \mathbf{S}_{q,k}^*, \nabla_{\mathbf{S}_{q,k}} \bar{f}_q(\Sigma_q^*, \mathbf{W}_q^*, \{\mathbf{S}_{q,k}^*\}_{k=0}^K) \rangle \geq 0, \forall \mathbf{S}_{q,k} \succeq 0, \forall k \in \mathbf{K}. \quad (\text{A.1d})$$

It should be noted that for a given  $(\Sigma_q^*, \mathbf{W}_q^*)$ , the value of  $\{\mathbf{S}_{q,k}^*\}_{k=0}^K$  are uniquely determined (cf. (3.11b) and (3.11c)). Hence, using Danskin's theorem [101], the function  $\bar{f}_q(\Sigma_q, \mathbf{W}_q, \{\mathbf{S}_{q,k}^*\}_{k=0}^K)$  is differentiable w.r.t  $(\Sigma_q, \mathbf{W}_q)$ , and inequality (A.1c) holds<sup>2</sup>. Moreover, it can be verified that

$$\nabla_{\Sigma_q} \bar{f}_q(\Sigma_q^*, \mathbf{W}_q^*, \{\mathbf{S}_{q,k}^*\}_{k=0}^K) = \nabla_{\Sigma_q} \bar{R}_{s,q}(\Sigma_q^*, \mathbf{W}_q^*), \quad (\text{A.2})$$

$$\nabla_{\mathbf{W}_q} \bar{f}_q(\Sigma_q^*, \mathbf{W}_q^*, \{\mathbf{S}_{q,k}^*\}_{k=0}^K) = \nabla_{\mathbf{W}_q} \bar{R}_{s,q}(\Sigma_q^*, \mathbf{W}_q^*) \quad (\text{A.3})$$

<sup>1</sup>AO iterations converge to a stationary point of (3.15) [26, Section IV-B], [102, Corollary 2].

<sup>2</sup>Similar reasoning for  $\bar{f}_q(\Sigma_q^*, \mathbf{W}_q^*, \mathbf{S}_{q,k})$  can be used to justify the inequality in (A.1d).

where  $\bar{R}_{s,q}$  is the smooth approximation of secrecy rate mentioned in (3.13). Then, according to (A.2),

$$\langle Z_q - X_q, \nabla_Z \bar{R}_{s,q}(\mathbf{\Sigma}_q^*, \mathbf{W}_q^*) \rangle \leq 0, \forall (\mathbf{\Sigma}_q, \mathbf{W}_q) \in \mathcal{F}_q \quad (\text{A.4})$$

where  $\nabla_Z \bar{R}_{s,q}(\mathbf{\Sigma}_q^*, \mathbf{W}_q^*) = [(\nabla_{\mathbf{\Sigma}_q} \bar{R}_{s,q})^T, (\nabla_{\mathbf{W}_q} \bar{R}_{s,q})^T]^T$ . Hence,  $(\mathbf{\Sigma}_q^*, \mathbf{W}_q^*)$  is the optimal solution to

$$\begin{aligned} & \underset{Z_q}{\text{maximize}} \quad \langle Z_q - X_q, \nabla_Z \bar{R}_{s,q}(\mathbf{\Sigma}_q^*, \mathbf{W}_q^*) \rangle \\ & \text{s.t.} \quad Z_q \in \mathcal{F}_q. \end{aligned} \quad (\text{A.5})$$

Hence,  $(\mathbf{\Sigma}_q^*, \mathbf{W}_q^*)$  must satisfy the K.K.T conditions of (A.5), which can be written as

$$\nabla_{\mathbf{\Sigma}_q} \bar{R}_{s,q}(\mathbf{\Sigma}_q^*, \mathbf{W}_q^*) - \zeta_q I + \Xi_{q,1} = 0 \quad (\text{A.6a})$$

$$\nabla_{\mathbf{W}_q} \bar{R}_{s,q}(\mathbf{\Sigma}_q^*, \mathbf{W}_q^*) - \zeta_q I + \Xi_{q,2} = 0 \quad (\text{A.6b})$$

$$\zeta_q (\text{Tr}(\mathbf{\Sigma}_q^* + \mathbf{W}_q^*) - P_q) = 0, \mathbf{\Sigma}_q^* \Xi_{q,1} = 0, \mathbf{W}_q^* \Xi_{q,2} = 0 \quad (\text{A.6c})$$

$$\zeta_q \geq 0, \Xi_{q,1} \succeq 0, \Xi_{q,2} \succeq 0. \quad (\text{A.6d})$$

where  $\zeta_q$ ,  $\Xi_{q,1}$ , and  $\Xi_{q,2}$  are Lagrange multipliers. Therefore, the stationary point of AO iterations satisfies the K.K.T conditions of (3.13).

## A.2 Proof of Theorem 4

To prove the existence of the QNE, we use the following theorem:

**Theorem 11.** [84, Corollary 2.2.5] *For a mapping  $F : \mathcal{Q} \rightarrow \mathcal{R}^N$  that is continuous on the compact and convex set  $\mathcal{Q} \subseteq \mathcal{R}^N$ , the solution set for  $VI(F, \mathcal{Q})$  is non-empty and compact.*  $\square$

The objective in (3.15) is continuously differentiable on its domain, making  $F^{\mathbb{R}}$  continuous. Furthermore, the set  $\mathcal{K}$  is a compact convex set because it is the Cartesian product of compact convex sets (i.e., players' strategy sets). Hence,  $\mathcal{K}^{\mathbb{R}}$ , the real-vector version of  $\mathcal{K}$ , is a convex set. Due to the presence of power constraints, the strategy set of each player is compact, then the set  $\mathcal{K}^{\mathbb{R}}$  is also compact. Thus, according to Theorem 11, the solution set to the VI in (3.40) is non-empty, meaning that the QNE in the proposed smooth game exists.

### A.3 Proof of Theorem 5

We first introduce following definition:

**Definition 4.** [91, Definition 26] *Considering the complex VI in (3.25), with  $F^{\mathbb{C}}(Z) : \mathcal{K} \rightarrow \mathbb{C}^{N' \times N}$ ,  $\mathcal{K} \subseteq \mathbb{C}^{N' \times N}$  being a continuously  $\mathbb{R}$ -differentiable function and  $\mathcal{K}$  being a convex set that has a non-empty interior. The augmented Jacobian matrix for  $F^{\mathbb{C}}(Z)$ , namely,  $JF^{\mathbb{C}}(Z)$ , is defined as follows<sup>3</sup>:*

$$JF^{\mathbb{C}}(Z) \triangleq \frac{1}{2} \begin{bmatrix} D_Z F^{\mathbb{C}}(Z) & D_{Z^*} F^{\mathbb{C}}(Z) \\ D_Z (F^{\mathbb{C}}(Z)^*) & D_{Z^*} (F^{\mathbb{C}}(Z)^*) \end{bmatrix} \quad (\text{A.7})$$

where  $D_Z(F^{\mathbb{C}}(Z)) \triangleq \frac{\partial \text{vec}(F^{\mathbb{C}}(Z))}{\partial \text{vec}(Z)^T}$  is a  $N'N \times N'N$  derivative matrix,  $D_{Z^*} F^{\mathbb{C}}(Z)^* = D_Z(F^{\mathbb{C}}(Z)^*)$ , and  $D_Z(F^{\mathbb{C}}(Z)^*) = D_{Z^*} F^{\mathbb{C}}(Z)$ .

Using this definition, the following proposition holds for  $VI(F^{\mathbb{C}}, \mathcal{K})$ .

**Proposition 8.** [91, Proposition 27] *For the  $VI(F^{\mathbb{C}}, \mathcal{K})$  defined in Definition 1, it holds that:*

---

<sup>3</sup>For the case of  $\mathcal{K}$  having a possibly empty interior, the equivalent condition in [91, Proposition 28] can be used.

- $F^{\mathbb{C}}$  is monotone on  $\mathcal{K}$  if and only if  $JF^{\mathbb{C}}(Z)$  is Augmented Positive Semi-Definite (APSD) on  $\mathcal{K}$ . That is, for all  $Y \in \mathbb{C}^{N' \times N}$  and  $Z \in \mathcal{K}$ ,

$$[\text{vec}(Y^*)^T, \text{vec}(Y)^T] JF^{\mathbb{C}}(Z) [\text{vec}(Y)^T, \text{vec}(Y^*)^T]^T \geq 0 \quad (\text{A.8})$$

Therefore,  $VI(F^{\mathbb{C}}, \mathcal{K})$  is called a monotone VI and has a (possibly empty) convex solution set.

- If  $JF^{\mathbb{C}}(Z)$  is Augmented Positive Definite (APD) on  $\mathcal{K}$ , then  $F^{\mathbb{C}}$  is strictly monotone on  $\mathcal{K}$ .  $JF^{\mathbb{C}}(Z)$  is APD if the inequality in (A.8) is strict. Hence,  $VI(F, \mathcal{Q})$  is a strictly monotone VI and has at most one solution (if there exists any).
- $F^{\mathbb{C}}$  is strongly monotone on  $\mathcal{K}$  with constant  $c_s > 0$  if and only if  $JF^{\mathbb{C}}(Z)$  is uniformly APD on  $\mathcal{K}$  with constant  $c_s/2$ . That is, for all  $Y \in \mathbb{C}^{N' \times N}$  and  $Z \in \mathcal{K}$ , there exists a constant  $c_s$  such that

$$[\text{vec}(Y^*)^T, \text{vec}(Y)^T] JF^{\mathbb{C}}(Z) [\text{vec}(Y)^T, \text{vec}(Y^*)^T]^T \geq c_s \|Y\|_F^2 \quad (\text{A.9})$$

where  $\|\cdot\|_F$  is the Frobenius norm. Hence,  $VI(F, \mathcal{Q})$  is a strongly monotone VI and has a unique solution.

We write the augmented Jacobian matrix for  $F^{\mathbb{C}}(\Sigma, \mathbf{W})$  according to (A.7). Let  $D_Z F^{\mathbb{C}}(Z)$  be defined as

$$D_Z F^{\mathbb{C}}(Z) \triangleq \begin{bmatrix} D_{Z_1} F_1^{\mathbb{C}}(Z_1) & \dots & D_{Z_Q} F_1^{\mathbb{C}}(Z_1) \\ \vdots & \ddots & \vdots \\ D_{Z_1} F_Q^{\mathbb{C}}(Z_Q) & \dots & D_{Z_Q} F_Q^{\mathbb{C}}(Z_Q) \end{bmatrix} \quad (\text{A.10})$$

where  $D_{Z_l} F_q^{\mathbb{C}}(Z_q)$  for all  $q, l \in 1, \dots, Q^2$  is defined as

$$D_{Z_l} F_q^{\mathbb{C}}(Z_q) \triangleq \begin{bmatrix} D_{\Sigma_l}(-\nabla_{\Sigma_q} \bar{f}_q) & D_{\mathbf{W}_l}(-\nabla_{\Sigma_q} \bar{f}_q) \\ D_{\Sigma_l}(-\nabla_{\mathbf{W}_q} \bar{f}_q) & D_{\mathbf{W}_l}(-\nabla_{\mathbf{W}_q} \bar{f}_q) \end{bmatrix}, \quad (\text{A.11})$$

and  $D_{Z^*} F^{\mathbb{C}}(Z) = D_Z(F^{\mathbb{C}}(Z))^* = 0$  (cf. (3.34)). Thus the matrix  $JF^{\mathbb{C}}$  becomes a block diagonal matrix. For a QNE to be unique, the matrix  $JF^{\mathbb{C}}$  has to satisfy inequality (A.8) with strict inequality. Since the game is proved to have at least one QNE (using Theorem 2), and since a strictly monotone VI has at most one solution (if there exists any), then the strict monotonicity of the resulting VI from the game is sufficient to prove the uniqueness of QNE. The strict monotonicity property requires  $JF^{\mathbb{C}}$  to be APD. In order to satisfy this condition, we only need  $D_Z F^{\mathbb{C}}(Z)$  to be Positive Definite (PD). Given  $F^{\mathbb{C}}$  in (3.34), the entries of  $D_{Z_l} F_q^{\mathbb{C}}(Z_q)$  are:

$$D_{\Sigma_l}(-\nabla_{\Sigma_q} \bar{f}_q) \triangleq \sum_{k=1}^K (\Lambda_{q,l,k} \otimes \mathbf{G}_{qk}^H \mathbf{S}_{q,k} \mathbf{G}_{qk}) - \Psi_{ql}^* \otimes \Psi_{ql}. \quad (\text{A.12})$$

where:

$$\Psi_{ql} \triangleq -\mathbf{H}_{qq}^H (\mathbf{M}_q + \mathbf{H}_{qq} \Sigma_q \mathbf{H}_{qq}^H)^{-1} \mathbf{H}_{ql}, \quad (\text{A.13})$$

$$\Lambda_{q,l,k} \triangleq \begin{cases} \frac{\beta e^{\beta \varphi_{e,q,k}}}{\left(\sum_{k'=1}^K e^{\beta \varphi_{e,q,k'}}\right)^2} \mathbf{G}_{lk}^H \left(\mathbf{S}_{q,k} - \mathbf{M}_{e,q,k}^{-1}\right) \mathbf{G}_{lk} - \\ \frac{\beta e^{\beta \varphi_{e,q,k}}}{\left(\sum_{k'=1}^K e^{\beta \varphi_{e,q,k'}}\right)^2} \sum_{k'=1}^K \left(e^{\beta \varphi_{e,q,k'}} \mathbf{G}_{lk}^H \left(\mathbf{S}_{q,k} - \mathbf{M}_{e,q,k}^{-1}\right) \mathbf{G}_{lk'}\right), \quad l \neq q, \\ \frac{\beta e^{\beta \varphi_{e,q,k}}}{\left(\sum_{k'=1}^K e^{\beta \varphi_{e,q,k'}}\right)^2} \mathbf{G}_{qk}^H \mathbf{S}_{q,k} \mathbf{G}_{qk} - \\ \frac{\beta e^{\beta \varphi_{e,q,k}}}{\left(\sum_{k'=1}^K e^{\beta \varphi_{e,q,k'}}\right)^2} \sum_{k'=1}^K \left(e^{\beta \varphi_{e,q,k'}} \mathbf{G}_{qk'}^H \mathbf{S}_{q,k'} \mathbf{G}_{qk'}\right), \quad l = q, \end{cases}$$

and the operator  $\otimes$  represents the Kronecker product. Furthermore,

$$D_{\mathbf{W}_l}(-\nabla_{\Sigma_q} \bar{f}_q) \triangleq D_{\Sigma_l}(-\nabla_{\mathbf{W}_q} \bar{f}_q) = \sum_{k=1}^K (\Omega_{q,l,k} \otimes \mathbf{G}_{qk}^H \mathbf{S}_{q,k} \mathbf{G}_{qk}) - \Psi_{ql}^* \otimes \Psi_{ql} \quad (\text{A.14})$$

where  $\forall (l, q) \in \{1, \dots, Q\}^2$ ,

$$\begin{aligned} \Omega_{q,l,k} \triangleq & \frac{\beta e^{\beta \varphi_{e,q,k}}}{\left(\sum_{k'=1}^K e^{\beta \varphi_{e,q,k'}}\right)^2} \mathbf{G}_{lk}^H \left(\mathbf{S}_{q,k} - \mathbf{M}_{e,q,k}^{-1}\right) \mathbf{G}_{lk} - \\ & \frac{\beta e^{\beta \varphi_{e,q,k}}}{\left(\sum_{k'=1}^K e^{\beta \varphi_{e,q,k'}}\right)^2} \sum_{k'=1}^K \left(e^{\beta \varphi_{e,q,k'}} \mathbf{G}_{lk'}^H \left(\mathbf{S}_{q,k'} - \mathbf{M}_{e,q,k'}^{-1}\right) \mathbf{G}_{lk'}\right), \end{aligned} \quad (\text{A.15})$$

and the first inequality in (A.14) holds because both of the derivatives  $D_{\mathbf{W}_l}(-\nabla_{\Sigma_q} \bar{f}_q)$  and  $D_{\Sigma_l}(-\nabla_{\mathbf{W}_q} \bar{f}_q)$  are continuous which implies the symmetry of the Hessian matrix (i.e., equality of mixed derivatives). Lastly,

$$\begin{aligned} D_{\mathbf{W}_l}(-\nabla_{\mathbf{W}_q} \bar{f}_q) \triangleq & \sum_{k=1}^K \left( \Omega_{q,l,k} \otimes \mathbf{G}_{qk}^H \mathbf{S}_{q,k} \mathbf{G}_{qk} - \Omega_{q,l,k} \otimes \mathbf{G}_{qk}^H \mathbf{M}_{e,q,k}^{-1} \mathbf{G}_{qk} + \pi_{q,l,k} \otimes \pi_{q,l,k} \right) \\ & - \Psi_{ql}^* \otimes \Psi_{ql} \text{ where} \\ \pi_{q,l,k} \triangleq & \mathbf{G}_{qk}^H \mathbf{M}_{e,q,k}^{-1} \mathbf{G}_{lk}. \end{aligned} \quad (\text{A.16})$$

Recalling equations (A.10) and (A.11) again, to prove  $D_Z F^{\mathbb{C}}(Z)$  is PD, we rely on the generalized Gerschgorin circle theorem [95]. Specifically, for a block matrix  $\mathbf{A}$  in which the blocks  $A_{ij}$ ,  $(i, j) = 1, \dots, M$  are  $N \times N$  matrices with complex entries, define the matrix norm  $||| \bullet |||$  in  $\mathbb{C}^{N \times N}$  as follows:

$$|||A_{ij}||| \triangleq \sup_{x \in \mathbb{C}^N} \frac{||A_{ij}x||}{||x||}. \quad (\text{A.17})$$

where  $|| \bullet ||$  is a vector norm on  $\mathbb{C}^N$ . Using the Gerschgorin circle theorem, every eigen-

value  $\lambda$  of  $\mathbf{A}$  satisfies

$$|||(A_{ii} - \lambda I)^{-1}|||^{-1} \leq \sum_{\substack{k=1 \\ k \neq i}}^M |||A_{i,k}||| \quad (\text{A.18})$$

for at least one  $1 \leq i \leq M$ , where  $|||A^{-1}|||^{-1} \triangleq \inf_{x \in \mathbb{C}^N} \frac{\|Ax\|}{\|x\|}$ , and  $I$  is the identity matrix.

**Proposition 9.** [95] *If the diagonal block  $A_{ii}$ ,  $i = 1, \dots, M$  of the block matrix  $\mathbf{A}$  are non-singular and if*

$$|||A_{i,i}^{-1}|||^{-1} \geq \sum_{\substack{k=1 \\ k \neq i}}^M |||A_{i,k}|||, \quad i = 1, \dots, M \quad (\text{A.19})$$

*for norm  $||| \bullet |||$  in  $\mathbb{C}^{N \times N}$  (where  $|||A_{i,i}^{-1}|||^{-1} = \inf_{x \in \mathbb{C}^N} \frac{\|A_{i,i}x\|}{\|x\|}$ ), then  $\mathbf{A}$  is a diagonally dominant matrix. Also if the diagonal blocks are PSD, the condition in (A.19) is sufficient for the matrix  $\mathbf{A}$  to be PSD.*

We can use the aforementioned Gerschgorin circle theorem, Proposition 8, and Proposition 9 on  $D_Z F^{\mathbb{C}}(Z)$  defined in (A.10) to obtain the set of conditions with which the augmented Jacobian matrix  $JF^{\mathbb{C}}$  is APSD. We also set the norm  $||| \bullet |||$  to be the spectral norm. (i.e.,  $|||A|||_2 = \sqrt{\lambda_{\max}(A^H A)}$  where  $\lambda_{\max}(\bullet)$  denotes the spectral radius of a matrix). Therefore, for  $JF^{\mathbb{C}}$  to satisfy the condition in (A.19), we must have [95, Chapter 6.1]

$$|\lambda_{q,\min}| \geq \sum_{\substack{q=1 \\ q \neq l}}^Q |||D_{Z_l} F_q^{\mathbb{C}}(Z_q)|||_2, \quad q = 1, \dots, Q \quad (\text{A.20})$$

where  $\lambda_{q,\min}$  is the smallest eigenvalue of  $D_{Z_q} F_q^{\mathbb{C}}(Z_q)$ . Using the strict inequality to (A.20) –as required by the strict monotonicity– and since the diagonal blocks of  $D_Z F^{\mathbb{C}}(Z)$  are already PSD (i.e.,  $\lambda_{q,\min} \geq 0$  due to concavity of  $q$ th player's utility to  $(\Sigma_q, \mathbf{W}_q)$ ), then

the condition in (A.20) changes to

$$\lambda_{q,\min} > \sum_{\substack{q=1 \\ q \neq l}}^Q |||D_{Z_l} F_q^{\mathbb{C}}(Z_q)|||_2, \quad q = 1, \dots, Q \quad (\text{A.21})$$



## APPENDIX B

**Proofs of Chapter 4****B.1 Proof of Theorem 7**

Let the Lagrangian of (4.22) w.r.t  $\sigma$  be denoted as  $\mathcal{L}(\sigma)$ . Also, let the Lagrangian of (4.24) w.r.t  $\sigma_q$  be denoted as  $\mathcal{L}_q(\sigma_q)$ ,  $\forall q$ . For  $\sigma^* = [\sigma_q^*]_{q=1}^Q$ , with  $\sigma_q^*$  defined in (4.4.2), to be a locally optimal solution of (4.22), the K.K.T. conditions of both (4.22) and (4.24) must be equivalent. That is,

$$\frac{\partial \mathcal{L}(\sigma^*)}{\partial \sigma} = \begin{bmatrix} \frac{\partial \mathcal{L}(\sigma^*)}{\partial \sigma_1} \\ \vdots \\ \frac{\partial \mathcal{L}(\sigma^*)}{\partial \sigma_Q} \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathcal{L}_1(\sigma^*)}{\partial \sigma_1} \\ \vdots \\ \frac{\partial \mathcal{L}_Q(\sigma^*)}{\partial \sigma_Q} \end{bmatrix} = 0. \quad (\text{B.1})$$

Simplifying (B.1), we have  $\lambda_q = -\sum_{\substack{r=1 \\ r \neq q}}^Q \frac{\partial C_r^{sec}}{\partial \sigma_q}$  which is the same as (4.25). Thus, assuming that iterative application of (4.4.2) converges to a NE, that NE is a locally optimal solution to (4.22)

The local optimality of the NE requires proving that (4.4.2) converges to the NE. Convergence to NE can be proved following the same approach used in [143, Appendix A]. Basically, once positive secrecy of link  $q$  is achieved for all  $q$ , then the secrecy rate of the  $q$ th link becomes a convex function of  $\sigma_r$ ,  $r \neq q$ ,  $r \in \mathcal{Q}$ . Then, the convergence can be proved using monotonic convergence theorem, i.e., the secrecy sum-rate becomes an upper-bounded and non-decreasing function of the Tx/FJ powers at each iteration.

## B.2 Proof of Proposition 3

Before proving this property, we present a useful lemma. We then leverage the result of this lemma to the game in (4.24) and prove the uniqueness of its NE<sup>1</sup>. The following lemma sets the conditions that allow us to approximate the secrecy sum-rate as a concave function:

**Lemma 2.** *For all links that satisfy the bound in (4.18), in the case of low interference, the secrecy sum-rate  $C^{sec}$  becomes a concave function of the vector  $\ln \boldsymbol{\sigma} = [\ln \sigma_q]_{q=1}^Q$ .*

*Proof.* Note that satisfying the bound in (4.18), or  $\sigma_q \in \mathcal{D}_q$ ,  $\forall q$ , with  $\mathcal{D}_q$  defined in (4.22), is directly interpreted as either having an eavesdropper that is far enough from the links or having not too demanding rate constraints at the  $q$ th link which leaves enough power for Tx/FJ to satisfy the positive secrecy constraint in (4.18) (i.e., not ending up to the case in (4.20a)). Hence, considering  $\sigma_q \in \mathcal{D}_q$ ,  $\forall q$ , one can set  $\sigma_q$  as  $\sigma_q = \frac{A_q}{B_q} + \delta_q$  where  $\delta_q > 0$  is upper-bounded until  $\sigma_q$  meets its maximum value defined in (4.22)<sup>2</sup>. Note that contrary to (4.21) where  $\delta_q$  is a small positive value, here,  $\delta_q$  can take any positive value as long as  $\sigma_q \in \mathcal{D}_q$ . For example in the case of  $A_q < 0$ , we can set  $\delta_q = -\frac{A_q}{B_q}$ , so that  $\sigma_q = 0$  as in (4.21d). Replacing  $\sigma_q = \frac{A_q}{B_q} + \delta_q$  in the secrecy rate given in (4.13), wherein  $\mathcal{G}_q$  is as in (4.12a), we can have a simplified equation for secrecy rate given in (B.2)<sup>3</sup>. It can be easily seen in (B.2) that with  $\sigma_q = \frac{A_q}{B_q} + \delta_q$  (or equivalently  $\sigma_q \in \mathcal{D}_q$ ), positive secrecy is achievable because the second term in (B.2) is always less than the first term as long as

<sup>1</sup>Note that the existence of NE is already known, as the strategy set of each player is a closed and convex set, and the utility of each player is a concave function of his action [106].

<sup>2</sup>Note that we do not simply subtract  $\frac{A_q}{B_q}$  from  $P^{jam} = \frac{P_q - \gamma_q}{N_q - 1}$  to find an upper bound for  $\delta_q$ , as it is possible that  $A_q < 0$ .

<sup>3</sup>The details of this simplification is skipped for the sake of brevity. Nevertheless, one can input the secrecy rate in (4.13) with  $\sigma_q = \frac{A_q}{B_q} + \delta_q$  to a mathematical symbolic computation software such as *Mathematica* to obtain the simplified equation in (B.2).

$$C_q^{sec} = \log \left( 1 + \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \gamma_q}{\sum_{r=1, r \neq q}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r) + N_0} \right) - \log \left( 1 + \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \gamma_q}{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \delta_q + \sum_{r=1, r \neq q}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r) + N_0} \right) \quad (\text{B.2})$$

$\delta_q > 0$ . Assume that  $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \gg \sum_{r=1, r \neq q}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r) + N_0, \forall q$ , indicating low interference at each legitimate receiver. Also, assume that  $|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \delta_q \gg \sum_{r=1, r \neq q}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r) + N_0, \forall q$ , which mainly suggests low interference together with  $\delta_q > 0, \forall q$  such that  $\frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} \delta_q \geq 1$ . Note that  $\frac{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} > 1$  because the term  $\mathbf{r}_q^\dagger \mathbf{G}'_q$  is a vector of i.i.d ZMCSCG random variables and the term  $\mathbf{r}_q^\dagger \mathbf{G}_q$  is a scalar ZMCSCG [120], the norm of these two terms is expected to be larger than one<sup>4</sup>. Hence, we only require  $\delta_q > 1$ . Under these assumptions, the secrecy rate  $C_q^{scc}$  in (B.2) can be approximated to

$$C_q^{sec} \approx \log \left( \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \gamma_q}{\sum_{r=1, r \neq q}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 \sigma_r) + N_0} \right) - \log \left( 1 + \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 \gamma_q}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2 \delta_q} \right). \quad (\text{B.3})$$

<sup>4</sup>One can use the law of large numbers as in [41] to prove this for large number of transmit/receive antennas. However, we saw the same trend even for a moderate number of transmit/receive antennas.

Let  $\boldsymbol{\rho} = [\rho_q]_{q=1}^Q$  where  $\rho_q \triangleq \ln \sigma_q$ . Hence, (B.3) can be rewritten as

$$C_q^{sec}(\boldsymbol{\rho}) \approx \log \left( \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2 \gamma_q}{\sum_{r=1, r \neq q}^Q (|\mathbf{d}_q^\dagger \mathbf{H}_{rq}|^2 \gamma_r + |\mathbf{d}_q^\dagger \mathbf{H}'_{rq}|^2 e^{\rho_r}) + N_0} \right) - \log \left( 1 + \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 \gamma_q}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2 (e^{\rho_q} - \frac{A_q}{B_q})} \right). \quad (\text{B.4})$$

It is known that  $\log \left( 1 + \sum_{q=1}^Q e^{\rho_q} \right)$  is convex in  $\mathbb{R}^Q$  [89, Chap. 3.1.5]. Hence, the first term in (B.4) is a concave function of  $\boldsymbol{\rho} = [\rho_r]_{r=1}^Q$ . Also, the second term is a concave function of  $\ln \sigma_q$  for  $\ln \sigma_q > \frac{1}{2} \ln \left( \frac{A_q}{B_q} \left( \frac{A_q}{B_q} - \frac{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2 \gamma_q}{|\mathbf{r}_q^\dagger \mathbf{G}'_q|^2} \right) \right)$ . Because we already have the assumption of  $\sigma_q > \frac{A_q}{B_q}$ , then the second term in (B.4) is a concave function of  $\rho_q = \ln(\sigma_q)$ . Therefore, the approximation of  $C_q^{sec}$  is a concave function of  $\boldsymbol{\rho} = \ln \boldsymbol{\sigma}$ .  $\square$

Now, let us turn our attention to the game in (4.24). In order to show that there is a unique NE to this game (under the conditions of Proposition 3), we use contradiction. Assume that there are two NEs for the game in (4.24), namely  $\bar{\boldsymbol{\sigma}} = [\bar{\sigma}_q]_{q=1}^Q$  and  $\tilde{\boldsymbol{\sigma}} = [\tilde{\sigma}_q]_{q=1}^Q$ . Hence, they both satisfy the K.K.T. conditions of (4.24) for all  $q$ , i.e.,

$$\frac{\partial}{\partial \sigma_q} C_q^{sec}(\bar{\boldsymbol{\sigma}}) - \lambda_q + \boldsymbol{\nu}_{q1}^T \frac{\partial}{\partial \sigma_q} \mathbf{f}_q(\bar{\boldsymbol{\sigma}}) = 0 \quad (\text{B.5a})$$

$$\frac{\partial}{\partial \sigma_q} C_q^{sec}(\tilde{\boldsymbol{\sigma}}) - \lambda_q + \boldsymbol{\nu}_{q2}^T \frac{\partial}{\partial \sigma_q} \mathbf{f}_q(\tilde{\boldsymbol{\sigma}}) = 0 \quad (\text{B.5b})$$

where  $\mathbf{f}_q = [\sigma_q - \chi_q, \frac{P_q - \gamma_q}{N_q - 1} - \sigma_q]^T$ ,  $\boldsymbol{\nu}_{q1} = [\nu_{q1}^{(1)}, \nu_{q1}^{(2)}]^T$ , and  $\boldsymbol{\nu}_{q2} = [\nu_{q2}^{(1)}, \nu_{q2}^{(2)}]^T$  are the vectors of Lagrange multipliers corresponding to the Tx/FJ power constraints of Alice<sub>q</sub>.

The result of Theorem 7 suggests that equations in (B.5) can be equivalently written as

$$\nabla_{\sigma} C^{sec}(\bar{\sigma}) + \Upsilon_1 \nabla_{\sigma} f(\bar{\sigma}) = \mathbf{0} \quad (\text{B.6a})$$

$$\nabla_{\sigma} C^{sec}(\tilde{\sigma}) + \Upsilon_2 \nabla_{\sigma} f(\tilde{\sigma}) = \mathbf{0} \quad (\text{B.6b})$$

where  $\nabla_{\sigma} C^{sec}$  is the gradient of  $C^{sec}$  w.r.t.  $\sigma$ ,  $f = [f_1^T, \dots, f_Q^T]^T$ ,  $\nabla_{\sigma} f(\sigma) = [\frac{\partial}{\partial \sigma_1} f_1^T(\sigma), \dots, \frac{\partial}{\partial \sigma_Q} f_Q^T(\sigma)]^T$ ,  $\Upsilon_1$  and  $\Upsilon_2$  are block diagonal matrices with  $[\Upsilon_1]_{qq} = \nu_{q1}^T$  and  $[\Upsilon_2]_{qq} = \nu_{q2}^T$ ,  $q \in \mathcal{Q}$  where  $[\bullet]_{qq}$  denotes the block on the  $q$ th row and the  $q$ th column, and finally  $\mathbf{0}$  is a vector of zeros (of appropriate size). Multiplying both sides of equations in (B.6) by  $(\tilde{\sigma} - \bar{\sigma})^T$  and subtracting (B.6b) from (B.6a) we have

$$\begin{aligned} & (\tilde{\sigma} - \bar{\sigma})^T \nabla_{\sigma} C^{sec}(\bar{\sigma}) + (\bar{\sigma} - \tilde{\sigma})^T \nabla_{\sigma} C^{sec}(\tilde{\sigma}) + \\ & (\tilde{\sigma} - \bar{\sigma})^T \Upsilon_1 \nabla_{\sigma} f(\bar{\sigma}) + (\bar{\sigma} - \tilde{\sigma})^T \Upsilon_2 \nabla_{\sigma} f(\tilde{\sigma}) = 0. \end{aligned} \quad (\text{B.7})$$

Recalling Theorem 7, at the NE of the price-based method, a locally optimum point of  $C^{sec}$  would be found. Thus, both  $\bar{\sigma}$  and  $\tilde{\sigma}$  satisfy the following unilateral optimality for every player  $q$ :

$$C^{sec}(\bar{\sigma}_q, \bar{\sigma}_{-q}) \geq C^{sec}(\sigma_q, \bar{\sigma}_{-q}), \quad \forall \sigma_q \in \mathcal{D}_q, \quad \forall q \quad (\text{B.8a})$$

$$C^{sec}(\tilde{\sigma}_q, \tilde{\sigma}_{-q}) \geq C^{sec}(\sigma_q, \tilde{\sigma}_{-q}), \quad \forall \sigma_q \in \mathcal{D}_q, \quad \forall q \quad (\text{B.8b})$$

where  $\bar{\sigma}_{-q} = (\bar{\sigma}_1, \dots, \bar{\sigma}_{q-1}, \bar{\sigma}_{q+1}, \dots, \bar{\sigma}_Q)$  is the set of all TxFJ powers except that of the  $q$ th link (equivalent notation also holds for  $\tilde{\sigma}_{-q}$ ). Convexity of each player's strategy set (i.e., concavity of  $f_q$ ) suggests that the terms in (B.7) that are related to the constraints can

be lower-bounded as

$$\begin{aligned}
& (\tilde{\sigma} - \bar{\sigma})^T \Upsilon_1 \nabla_{\sigma} f(\bar{\sigma}) + (\bar{\sigma} - \tilde{\sigma})^T \Upsilon_2 \nabla_{\sigma} f(\tilde{\sigma}) \geq \\
& \Upsilon_1(f(\tilde{\sigma}) - f(\bar{\sigma})) + \Upsilon_2(f(\bar{\sigma}) - f(\tilde{\sigma})) = \\
& \Upsilon_1(f(\tilde{\sigma})) + \Upsilon_2(f(\bar{\sigma})) \geq 0
\end{aligned} \tag{B.9}$$

where we used the complementary slackness conditions, i.e.,  $\nu_{q_1} \circ f_q(\bar{\sigma}) = \mathbf{0}$  and  $\nu_{q_2} \circ f_q(\tilde{\sigma}) = \mathbf{0}$  with  $\circ$  and  $\mathbf{0}$  denoting the Hadamard product and a vector of zeros (of appropriate size), respectively. Under the conditions of Proposition 3, we can approximate  $C^{sec}$  as a concave function of  $\ln \bar{\sigma}$  or  $\ln \tilde{\sigma}$  where  $\ln(\bullet)$  is applied to each element of a vector (cf. Lemma 2). The second term in (B.4) shows that for all  $q$ , the utility of the  $q$ th player is a concave function of  $\ln \sigma_q$ . Moreover, the approximation in (B.4) is a strictly increasing function of  $\sigma_q$ . Next, the function  $\ln \sigma_q$  is concave w.r.t.  $\sigma_q$ . Hence, we can conclude that (B.4) is a strictly concave function of  $\sigma_q$ <sup>5</sup>. Lastly, the first two terms of (B.7) can be simplified to

$$\sum_{q=1}^Q (\tilde{\sigma}_q - \bar{\sigma}_q) \frac{\partial}{\partial \sigma_q} C^{sec}(\bar{\sigma}) + (\bar{\sigma}_q - \tilde{\sigma}_q) \frac{\partial}{\partial \sigma_q} C^{sec}(\tilde{\sigma}). \tag{B.10}$$

Therefore,

$$\begin{aligned}
& \sum_{q=1}^Q (\tilde{\sigma}_q - \bar{\sigma}_q) \frac{\partial}{\partial \sigma_q} C^{sec}(\bar{\sigma}) + (\bar{\sigma}_q - \tilde{\sigma}_q) \frac{\partial}{\partial \sigma_q} C^{sec}(\tilde{\sigma}) > \\
& \sum_{q=1}^Q (C^{sec}(\tilde{\sigma}_q, \bar{\sigma}_{-q}) - C^{sec}(\bar{\sigma})) + (C^{sec}(\bar{\sigma}_q, \tilde{\sigma}_{-q}) - C^{sec}(\tilde{\sigma})).
\end{aligned} \tag{B.11}$$

---

<sup>5</sup>Specifically, we use the fact that for a convex function  $g(x)$  and a non-decreasing convex function  $f(x)$ , the composite function  $f(g(x))$  is convex w.r.t.  $x$  [89].

Due to strictly increasing property of  $C^{sec}$  w.r.t.  $\sigma_q$  and the inequality in (B.8), one can consider that if  $C^{sec}(\tilde{\sigma}_q, \bar{\sigma}_{-q}) < C^{sec}(\bar{\sigma})$ , then  $\tilde{\sigma}_q < \bar{\sigma}_q$ . On the other hand, as the second term in the right hand side (RHS) of (B.11) suggests,  $C^{sec}(\bar{\sigma}_q, \tilde{\sigma}_{-q}) < C^{sec}(\tilde{\sigma})$  means that  $\bar{\sigma}_q < \tilde{\sigma}_q$ . This contradiction together with the result obtained in (B.9) suggests that (B.7) does not hold except only for the case where  $\bar{\sigma}_q = \tilde{\sigma}_q, \forall q \in \mathcal{Q}$ , which contradicts the assumption of existence of two different NEs. Hence, the NE of this game must be unique. Also, the approximation of  $C_q^{sec}$  is a concave function of  $\rho = \ln \sigma, \forall q \in \mathcal{Q}$ . Furthermore, Theorem 7 suggests that every NE of the price-based FJ control is a local optimum of the secrecy sum-rate maximization. Thus, the unique NE of the price-based game is the global maximum of the secrecy sum-rate maximization problem in (4.22).

The convergence of iterative optimization in (4.24), wherein  $C_q^{sec}$  is written according to (B.3) and subsequently  $\lambda_q = -\sum_{r \neq q} \frac{\partial C_r^{sec}}{\partial \sigma_q}$ , can be established by finding a Lyapunov-type function of the Tx/FJ powers for the  $q$ th player,  $\forall q \in \mathcal{Q}$ , and show that it is non-decreasing w.r.t.  $\sigma_q$  and upper-bounded. We do not go through the details of this proof for the sake of brevity (see [144], [145, Section 2.2], and [146, Appendix IV]).

### B.3 Proof of Proposition 4

In order to prove this property, we leverage the concept of Fast Lipschitz optimization introduced in [81], defined in the following:

**Definition 5.** *The following problem is said to be of Fast Lipschitz form:*

$$\begin{aligned}
 & \max_{\mathbf{x}} \mathbf{g}_0(\mathbf{x}) \\
 & \text{s.t. } x_i \leq g_i(\mathbf{x}) \quad \forall i \in \mathbb{A} \\
 & \quad x_i = g_i(\mathbf{x}) \quad \forall i \in \mathbb{B}
 \end{aligned} \tag{B.12}$$

where

- $\mathbf{x} = [x_i]_{i=1}^n$  is the vector of decision variables (not to be confused with the information signals defined in Section II).
- $\mathbf{g}_0 : \mathbb{R}^n \rightarrow \mathbb{R}^m$  is a differentiable scalar ( $m = 1$ ) or vector-valued ( $m \geq 2$ ) function.
- $\mathbb{A}$  and  $\mathbb{B}$  are complementary subsets of  $\{1, 2, \dots, n\}$ .
- $g_i : \mathbb{R}^n \rightarrow \mathbb{R}$  are differentiable functions.

For the case of  $\mathbf{g}_0$  being a vector valued function, the problem in (B.12) is sometimes called vector optimization, where the aim is to maximize all the elements of  $\mathbf{g}_0$  with respect to the non-negative orthant  $\mathbb{R}_+^m$  (i.e., a proper cone [89, Section 4.7]), indicating that all the elements of  $\mathbf{g}_0$  must remain positive. A feasible decision vector  $\mathbf{x}^*$  is said to be *Pareto-optimal* if there is no other feasible vector  $\tilde{\mathbf{x}}$  such that  $\mathbf{g}_0(\mathbf{x}^*) \geq \mathbf{g}_0(\tilde{\mathbf{x}})$  where the inequality is element-wise. If such Pareto-optimal point is unique, then  $\mathbf{x}^*$  is the best achievable decision vector. The authors in [81] proved that if some sufficient conditions (derived in [81, Theorem 7]) hold for the problem in (B.12), then a unique Pareto-optimal point for the problem in (B.12) exists and can be found via the iterative computation  $\mathbf{x}^* = \mathbf{g}(x^*)$  where  $\mathbf{g} = [g_i]_{i=1}^m$ .

If the set of feasible vectors is a convex set, then one can convert the objective in (B.12) to the following form

$$\max_{\mathbf{x}} \nu^T \mathbf{g}_0(\mathbf{x}) \quad (\text{B.13})$$

where  $\nu$  is a vector of positive weights. It can be shown that any Pareto-optimal point of (B.12) can be found by a proper choice of weights in (B.13) [105]. Looking back at



the problem where the aim was to solve (4.17), it turns out that the same scalarization technique used in (B.13) is actually used in (4.17) as well where the elements of  $\mathbf{g}_0$  were set to individual secrecy rates, the decision vector  $\mathbf{x}$  was set to the vector of TxFJ powers, and the weight vector  $\nu$ 's elements were set to 1. Moreover, the uniqueness of the Pareto-optimal point of (4.17) (i.e., uniqueness of NE of price-based FJ control defined by (4.24)) was shown in Proposition 3 for the case where the optimal TxFJ power is not necessarily the maximum TxFJ power, i.e.,  $\sigma_q = P_q^{jam}$ .

Here, we would like to show where using maximum TxFJ power is a unique Pareto-optimal operating point, which can be proved by leveraging Fast-Lipschitz optimization problems. In order to write the Fast Lipschitz form of (4.17), one can observe that because the problem in (4.17) has no equality constraints, we can assume that its Fast Lipschitz form does not have equality constraints, i.e.,  $\mathbb{B} = \emptyset$ . Furthermore, because in this proof we are trying to prove the optimality of greedy method (i.e., using maximum TxFJ power), we can set the functions  $g_q = P_q^{jam}$ ,  $q \in \mathcal{Q}$ .

Now that we have converted the greedy method into a Fast-Lipschitz optimization problem, we can use the properties of this class of optimization problems, specifically [81, Theorem 7] to comment on the conditions that guarantee the greedy method is the unique Pareto-optimal point. Because [81, Theorem 7] provides sufficient conditions (for the uniqueness of the Pareto-optimal optimal point) when the functions  $g_q(\mathbf{x})$  are assumed to be of general types, we simplify these conditions to the case where  $g_q = P_q^{jam}$  are constant values. The general qualifying conditions in [81, Theorem 7] requires the following for the uniqueness of the Pareto-optimal point:

- $\nabla \mathbf{g}_0(\mathbf{x})$  must have non-negative elements with non-zero rows where  $\nabla \mathbf{g}_0(\mathbf{x})$  is the Jacobian matrix of  $\mathbf{g}_0(\mathbf{x})$  w.r.t.  $\mathbf{x}$ , i.e., the elements in the  $q$ th column of  $\nabla \mathbf{g}_0(\mathbf{x})$  are

denoted as  $[\nabla \mathbf{g}_0(\mathbf{x})]_{:,q} = \frac{\partial \mathbf{g}_0(\mathbf{x})}{\partial x_q}$ <sup>6</sup>,  $q \in \mathcal{Q}$ .

- $\|\nabla \mathbf{g}\| < 1$  where  $\nabla \mathbf{g}$  is the Jacobian matrix of  $\mathbf{g} = [g_q]_{q=1}^Q$  w.r.t  $\mathbf{x}$ , i.e., the elements in the  $q$ th column of  $\nabla \mathbf{g}$  are denoted as  $[\nabla \mathbf{g}]_{:,q} = \frac{\partial \mathbf{g}}{\partial x_q}$ ; and  $\|\bullet\|$  is an arbitrary matrix norm.

There exists a  $k < \infty$  such that

- The  $k$ th power of  $\nabla \mathbf{g}$ , i.e.,  $(\nabla \mathbf{g})^k$  has non-negative elements.
- When  $k > 1$ , then  $\|\sum_{l=1}^{k-1} (\nabla \mathbf{g})^l\| < z(\mathbf{x}) = \min_q \frac{\min_r [\nabla \mathbf{g}_0(\mathbf{x})]_{rq}}{\max_r [\nabla \mathbf{g}_0(\mathbf{x})]_{rq}}$  where  $[\nabla \mathbf{g}_0(\mathbf{x})]_{rq}$  refers to the element in the  $r$ th row and  $q$ th column of  $\nabla \mathbf{g}_0(\mathbf{x})$ .

Considering that in our case the elements of  $\mathbf{g}_0(\mathbf{x})$  are assumed to represent the individual secrecy rates for all  $q \in \mathcal{Q}$ ,  $\mathbf{x}$  is the vector of all links' TxFJ powers, and  $\mathbf{g} = [P_q^{jam}]_{q=1}^Q$ , then the last three items of general qualifying conditions are automatically satisfied (assuming that  $z(\mathbf{x}) = 1$  in case of having zeros at both its nominator and denominator). Hence, we only need to satisfy the first item of general qualifying conditions, indicating that  $[\nabla \mathbf{g}_0(\mathbf{x})]_{rq} = \frac{\partial C_r^{sec}}{\partial \sigma_q} > 0, r, q \in \mathcal{Q}$ , is the only requirement to guarantee that the greedy FJ control is of Fast-Lipschitz form. Hence, the property is proved.

#### B.4 Proof of Proposition 5

In order to prove this property, we need to make use of the reformulation of the secrecy rate in (B.2) that we previously utilized in the proof of Proposition 3. According to the proof of Proposition 4, in order for the greedy FJ –which results in using the maximum TxFJ power at each link– to be the unique Pareto-optimal operating point,

---

<sup>6</sup>Note that  $\mathbf{g}_0(\mathbf{x})$  is in general a vector. Thus the derivative  $\frac{\partial \mathbf{g}_0(\mathbf{x})}{\partial x_q}$  is a vector whose elements are denoted by individual derivative of each element of  $\mathbf{g}_0(\mathbf{x})$  w.r.t.  $\mathbf{x}$ .

we only require every element of  $\nabla \mathbf{g}_0(\mathbf{x})$  to be non-negative with non-zero row where  $[\nabla \mathbf{g}(\mathbf{x})]_{rq} = \frac{\partial C_r^{sec}}{\partial \sigma_q}$ ,  $r, q \in \mathcal{Q}$ . Given that the secrecy rate of the  $q$ th user is a strictly increasing function of its own TxPJ, then  $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0$ ,  $r = q$ . For the case of  $r \neq q$ , the term  $\frac{\partial C_r^{sec}}{\partial \sigma_q}$  can be written as

$$\begin{aligned} \frac{\partial C_r^{sec}}{\partial \sigma_q} = & \frac{-\frac{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2} \gamma_r}{a_r (a_r + \gamma_r)} + \frac{\left( \frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2} \delta'_r + \frac{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2} \right) \gamma_r}{\left( \frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2} \delta_r + a_r \right) \left( \frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2} \delta_r + a_r + \gamma_r \right)} \end{aligned} \quad (\text{B.14})$$

where  $\delta_r = \sigma_r - \frac{A_r}{B_r}$  with  $A_r$  and  $B_r$  defined in (4.19); and  $\delta'_r = \frac{\partial \delta_r}{\partial \sigma_q}$ . Note that  $A_r$  and  $B_r$  are functions of  $\sigma_q$ , so  $\delta'_r$  is well-defined and is not trivially zero. Let  $\frac{|\mathbf{r}_r^\dagger \mathbf{G}'_r|^2}{|\mathbf{r}_r^\dagger \mathbf{G}_r|^2} = f_r$  and set  $\delta_r = \sigma_r - \frac{A_r}{B_r}$  in (B.14). Hence,  $f_r \delta'_r + \frac{|\mathbf{d}_r^\dagger \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r^\dagger \mathbf{H}_{rr}|^2} = \frac{|\mathbf{d}_r^\dagger \mathbf{G}'_q|^2}{|\mathbf{d}_r^\dagger \mathbf{G}_r|^2} > 0$ , indicating that the nominator of the second term in the RHS of (B.14) is always positive. Set the nominator of the second term to  $Z > 0$ . Given that the first term in the RHS of (B.14) is always negative, replacing  $\delta_r$  with  $\delta_r = \sigma_r - \frac{A_r}{B_r}$ , the following cases can be considered for  $\frac{\partial C_r^{sec}}{\partial \sigma_q}$ :

1. If  $\frac{A_r}{B_r} > 0$ , and  $|\frac{A_r}{B_r}| < \frac{a_r}{f_r}$ : In this case the second term in the RHS of (B.14), namely  $h(\sigma_r)$  which is a function of  $\sigma_r$ , can be written as

$$h(\sigma_r) = \frac{Z}{(\sigma_r + W)(\sigma_r + E)} \quad (\text{B.15})$$

where both  $Z > 0$ ,  $W > 0$ ,  $E > 0$  and  $E > W^7$ . The plot of  $h(\sigma_r)$  is shown in Figure 14.

It can be seen that if  $\sigma_r$  is reasonably low (which refers to a low power constraint

---

<sup>7</sup>We do not show the process of simplifying the second term in RHS of (B.14) to end up with (B.15) for the sake of brevity. One can use  $\delta_r = \sigma_r - \frac{A_r}{B_r}$  in (B.14) to end up with the same result in (B.15) for the second term in RHS of (B.14)

on TxFJ), then we may have  $\frac{\partial C_r^{sec}}{\partial \sigma_q} = \frac{-\frac{|\mathbf{d}_r \mathbf{H}'_{qr}|^2}{|\mathbf{d}_r \mathbf{H}_{rr}|^2} \gamma_r}{a_r(a_r + \gamma_r)} + h(\sigma_r) > 0$ . Note that it could be the case that if  $W$  is too large as is shown in Figure 15, indicating large interference at the  $r$ th legitimate receiver or close proximity of Alice <sub>$r$</sub>  to Eve, then even a low value for  $\sigma_r$  cannot be enough to guarantee  $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0$ . Note also that for the case of  $\frac{A_r}{B_r} < 0$ , although we can set  $\sigma_r = 0$  by following the procedure in (4.21), we can still use the above analysis to show that lower values of  $\sigma_r$  (in this case the lowest value) is more probable to make  $\frac{\partial C_r^{sec}}{\partial \sigma_q}$ .

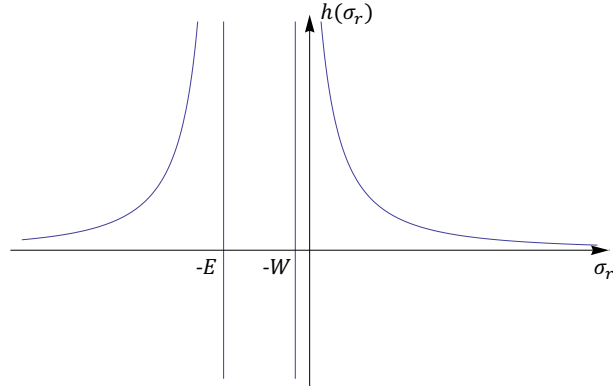


Figure 14: Plot of  $h(\sigma_r)$  when  $W$  is small.

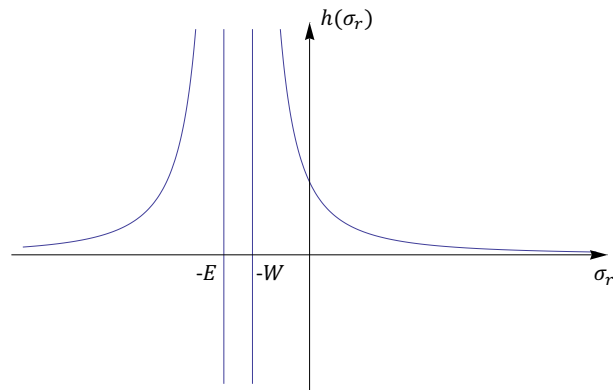


Figure 15: Plot of  $h(\sigma_r)$  when  $W$  is large.

2. If  $\frac{A_r}{B_r} > 0$  and  $\frac{a_r}{f_r} < \left| \frac{A_r}{B_r} \right| < \frac{(a_r + \gamma_r)}{f_r}$  or  $\left| \frac{A_r}{B_r} \right| > \frac{(a_r + \gamma_r)}{f_r}$ : In this case the second term

in the RHS of (B.14), namely  $h(\sigma_r)$  which is a function of  $\sigma_r$ , can be written as

$$h(\sigma_r) = \frac{Z}{(\sigma_r + W)(\sigma_r + E)} \quad (\text{B.16})$$

where  $W < 0$ , but  $E > 0$ . The plot of  $h(\sigma_r)$  is the same as Figure 14 with the rightmost root shifted to the right side of  $\sigma_r = 0$  axis because now  $W$  is considered a negative value. It can be easily deduced that for a large value of  $|W|$  a moderate/high value of  $\sigma_r$  can make  $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0$ . However, it is unlikely to have  $\frac{a_r}{f_r} < |\frac{A_r}{B_r}|$ . This can be seen from the definition of  $A_r$  and  $B_r$  in (4.19), where  $\frac{A_r}{B_r}$  has  $\frac{a_r}{f_r}$  as its first term which is then subtracted by a positive term. Thus, the case where  $\frac{a_r}{f_r} < |\frac{A_r}{B_r}|$  or  $|\frac{A_r}{B_r}| > \frac{(a_r + \gamma_r)}{f_r}$  will never occur.

Therefore, once we ensure a low constraint on  $\sigma_r$ , i.e., the maximum Tx FJ power, we can have  $\frac{\partial C_r^{sec}}{\partial \sigma_q} > 0$ ,  $\forall r, q \in \mathcal{Q}$ , and thus according to Proposition 4, the greedy FJ control approach becomes the unique Pareto-optimal operating point in the network.

## B.5 Proof of Proposition 6

Without loss of generality, assume that  $\sigma_q^*$  is a decreasing function of  $\sigma_r$  and  $\chi_q$  defined in (4.4.2) satisfies  $\Delta\sigma_q < \chi_q < \frac{P_q - \gamma_q}{N_q - 1}$ ,  $q = 1, 2$ . Furthermore, assume that the iterative use of (4.4.2) is done sequentially, i.e., Gauss-Seidel algorithm in the sense of [107, Chapter 3] is used, meaning that only one player is updating his Tx FJ power at each iteration. More specifically, let the initial Tx FJ power for the  $q$ th player be  $\sigma_q^{*(1)}$ , where the superscript  $(1)$  represents the iteration index. In the second iteration  $\sigma_r$  gets updated using (4.4.2) and  $\sigma_q^{*(2)} = \sigma_q^{*(1)}$ . In the third iteration,  $\sigma_r^{*(3)} = \sigma_r^{*(2)}$ , and  $\sigma_q$  gets updated, and so on. Since  $\sigma_q^*$  is assumed to be a decreasing function of  $\sigma_r$ . Hence, if  $\sigma_q^{*(1)} < \sigma_q^{*(3)}$  the  $r$ th player will select a smaller Tx FJ power in the fourth iteration compared to the second

iteration (i.e.,  $\sigma_r^{*(2)} > \sigma_r^{*(4)}$ ). Consequently, in the fifth iteration, the  $q$ th player selects a higher TxPJ power comparing to the third iteration. This trend continues until either the  $q$ th player reaches  $P_q^{jam}$  or the  $r$ th player reaches to  $\chi_r$ . Depending on which player reaches to either of the extreme points faster than the other, the first four forms in the RHS of (4.28) are expected to be achieved. For the case of  $(\chi_1, \chi_2)$  and  $(P_1^{jam}, P_2^{jam})$ , we first derive the price above which we always have  $\sigma_q^* = \chi_q$ . Let this price be  $\lambda_{q,1}$ . Reducing the inequality  $\sigma_q^* \leq \chi_q$ , we end up with an inequality in the form of  $\lambda_q \geq \lambda_{q,1}$ . Next, we find a price below which we have  $\sigma_q^* = P_q^{jam}$ . Let this price be  $\lambda_{q,2}$ . Reducing the inequality  $\sigma_q^* \geq P_q^{jam}$ , we end up with an inequality in the form of  $\lambda_{q,2} \geq \lambda_q$ <sup>8</sup>. Because  $\sigma_q$  is a decreasing function of  $\lambda_q$ , if  $P_q^{jam} > \chi_q$  then  $\lambda_{q,1} > \lambda_{q,2}$ . Thus, the tuples  $(\chi_1, \chi_2)$  and  $(P_1^{jam}, P_2^{jam})$  happen when  $\lambda_q > \lambda_{q,1}$ ,  $\forall q \in \{1, 2\}$  and  $\lambda_q < \lambda_{q,2}$ ,  $\forall q \in \{1, 2\}$ , respectively. An equivalent proof for when  $\sigma_q^*$  is an increasing function of  $\sigma_r$  can be given, which is skipped for the sake of brevity.

---

<sup>8</sup>Note that when  $0 < \lambda_q \leq \lambda_{q,2}$ , greedy FJ is optimal in terms of secrecy sum-rate, but it may not always be beneficial for both of the links unless  $\lambda_q \leq 0$ . The condition  $\lambda_q \leq 0$ ,  $\forall q$  found in Proposition 4 can also guarantee the optimality of greedy FJ in terms of individual secrecy rates.

## APPENDIX C

## Proofs of Chapter 5

### C.1 Proof of Theorem 7

Using [107, Proposition 6.1], the fixed point iteration in (5.36) converges to a point  $\phi^*$  from any initial point iff  $\rho(\mathbf{A} + \mathbf{B}) < 1$ . We now introduce the following theorem

**Theorem 12.** [107, Ch. 2, Proposition 6.6] *For any square matrix  $\mathbf{M}$  and any  $\epsilon > 0$ , there exists an induced norm,  $\|\bullet\|$  such that  $\rho(\mathbf{M}) \leq \|\mathbf{M}\| \leq \rho(\mathbf{M}) + \epsilon$ <sup>1</sup>.  $\square$*

Using the above theorem, since  $\rho(\mathbf{A} + \mathbf{B}) < 1$ , we can choose  $\epsilon > 0$  arbitrarily close to zero such that  $\rho(\mathbf{A} + \mathbf{B}) + \epsilon < 1$ . Hence, we can find a an induced norm  $\|\mathbf{A} + \mathbf{B}\|$  such that  $\|\mathbf{A} + \mathbf{B}\| \leq \rho(\mathbf{A} + \mathbf{B}) + \epsilon$ . Therefore, we are able to convert the condition  $\rho(\mathbf{A} + \mathbf{B})$  to an equivalent condition based on an induced norm, i.e.,  $\|\mathbf{A} + \mathbf{B}\|$ . We use this result later during this proof. To proceed with further analysis, we need the following definition:

**Definition 6.** [107] *Consider the following iteration:*

$$\Phi^{(t+1)} = \mathcal{T}(\Phi^{(t)}), \quad t = 1, 2, \dots, \quad (\text{C.1})$$

where  $\mathcal{T}$  is a mapping from  $\mathbb{A}$  (a subset of  $\mathbb{R}^Q$ ) to itself, and  $t$  indicates the index of

---

<sup>1</sup>For the sake easy presentation, we omitted introducing the weighted norm, while this is the type of norm used in [107, Ch. 2, Proposition 6.6]. Nevertheless, all of our analyses can be extended to the case of weighted norms as well.

iterations. If  $\mathcal{T}$  is continuous and

$$\|\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})\| \leq \Omega \|\Phi^{(1)} - \Phi^{(2)}\|, \quad \forall \{\Phi^{(1)}, \Phi^{(2)}\} \in \mathbb{A}^2, \quad (\text{C.2})$$

where  $\|\cdot\|$  is a norm in  $\mathbb{A}$  and  $\Omega \in [0, 1)$ , then the mapping  $\mathcal{T}$  is a contraction mapping with  $\Omega$  as the contraction modulus, and sequence  $\{\phi^{(t)}\}$  generated by iterations in (C.1) converges to the fixed point  $\phi^*$ .

Using this definition and the result of Theorem 12, we can show the iteration in (5.36) as a contraction mapping, i.e.,

$$\|\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})\| \leq \|(\mathbf{A} + \mathbf{B})(\Phi^{(1)} - \Phi^{(2)})\| \quad (\text{C.3})$$

$$\leq \|\mathbf{A} + \mathbf{B}\| \|\Phi^{(1)} - \Phi^{(2)}\| \quad (\text{C.4})$$

where  $\|\mathbf{A} + \mathbf{B}\| < 1$ , (C.4) is due to Cauchy-Schwartz inequality, and the induced norm  $\|\bullet\|$  is chosen such that for some  $\epsilon > 0$  we have  $\|\mathbf{A} + \mathbf{B}\| \leq \rho(\mathbf{A} + \mathbf{B}) + \epsilon < 1$  (cf. Theorem 12). This result will be used later in this proof.

We now focus on  $\min\{\bullet\}$  and  $\max\{\bullet\}$  functions. The operator  $\max\{\min\{\phi_0, 1\}, 0\}$ , for some  $\phi_0 > 0$ , can be equivalently shown as a Euclidean projection. Specifically, the Euclidean projection of a scalar  $\phi_0$ , denoted as  $[\phi_0]^+$ , can be written as the following optimization problem

$$\begin{aligned} & \underset{\bar{\phi}}{\text{minimize}} \quad \|\bar{\phi} - \phi_0\|^2 \\ & \text{s.t.} \quad 0 \leq \bar{\phi} \leq 1. \end{aligned} \quad (\text{C.5})$$



The KKT conditions of this problem are written as follows:

$$\bar{\phi} - \phi_0 - \nu + \lambda = 0, \quad (\text{C.6})$$

$$\nu \geq 0, \bar{\phi} \geq 0, \nu\phi = 0 \quad (\text{C.7})$$

$$\lambda \geq 0, \bar{\phi} \leq 1, \lambda(\phi - 1) = 0; \quad (\text{C.8})$$

If  $\nu > 0$ , then  $\bar{\phi} = 0$ . Hence,  $\lambda = 0$  and we have  $\nu = -\phi_0$ , or equivalently  $\phi_0 \leq 0$ . If  $\lambda > 0$ , then  $\bar{\phi} = 1$ . Hence,  $\nu = 0$ , and we have  $1 + \lambda = \phi_0$ , or equivalently  $\phi_0 \geq 1$ . If  $\lambda = 0$  and  $\nu = 0$ , then  $0 \leq \bar{\phi} \leq 1$ . Hence,  $\bar{\phi} = \phi_0$ . Summarizing these conditions, we have

$$\bar{\phi}^* = \underset{0 \leq \bar{\phi} \leq 1}{\operatorname{argmax}} ||\bar{\phi} - \phi_0||^2 = \begin{cases} 0, & \text{if } \phi_0 \leq 0, \\ 1, & \text{if } \phi_0 \geq 1, \\ \phi_0, & \text{if } 0 \leq \phi_0 \leq 1. \end{cases} \quad (\text{C.9})$$

The right hand side of (C.9) is exactly the definition of the operator  $\max\{\min\{\bullet, 1\}, 0\}$ .

Converting  $\max\{\min\{\bullet, 1\}, 0\}$  to Euclidean projection, we use the non-expansive property of Euclidean projection which is as follows [107, Ch. 3, Proposition 3.2]:

$$\left\| [\mathcal{T}(\Phi^{(1)})]^+ - [\mathcal{T}(\Phi^{(2)})]^+ \right\| \leq \|\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})\| \quad (\text{C.10})$$

The non-expansive property of Euclidean projectors can be generalized to all vector norms because all vector norms (i.e., norms in  $\mathbb{R}^n$ ) are equivalent, i.e., for any two different norm  $\|\bullet\|^1$  and  $\|\bullet\|^2 \exists \alpha_1 \in \mathbb{R}$  and  $\alpha_2 \in \mathbb{R}$  such that  $\alpha_1 \|\mathbf{x}\|^1 \leq \|\mathbf{x}\|^2 \leq \alpha_2 \|\mathbf{x}\|^1, \forall \mathbf{x} \in \mathbb{R}^n$

[95]. Hence, we have the following chain of inequalities

$$\left\| [\mathcal{T}(\Phi^{(1)})]^+ - [\mathcal{T}(\Phi^{(2)})]^+ \right\| \leq \|\mathcal{T}(\Phi^{(1)}) - \mathcal{T}(\Phi^{(2)})\| \quad (\text{C.11})$$

$$\leq \|(\mathbf{A} + \mathbf{B})(\Phi^{(1)} - \Phi^{(2)})\| \leq \|\mathbf{A} + \mathbf{B}\| \|\Phi^{(1)} - \Phi^{(2)}\| \quad (\text{C.12})$$

Hence,

$$\left\| [\mathcal{T}(\Phi^{(1)})]^+ - [\mathcal{T}(\Phi^{(2)})]^+ \right\| \leq \|\mathbf{A} + \mathbf{B}\| \|\Phi^{(1)} - \Phi^{(2)}\|. \quad (\text{C.13})$$

Setting the norm in (C.13) as the same norm in (C.4), the best response of each player is a contraction map, and thus has a unique fixed point (NE).

## C.2 Proof of Theorem 9

Similar to the proof of Theorem 7, consider the following iteration:

$$\Phi^{(t+1)} = \mathcal{T}(\Phi^{(t)}), \quad t = 1, 2, \dots, \quad (\text{C.14})$$

We use the asynchronous convergence theorem [107], which is as follows:

**Theorem 13.** *The iteration in (C.14) converges asynchronously if the following conditions are satisfied:*

1. *There exists a sequence of non-empty sets  $\mathcal{X}(t)$  such that*

$$\dots \subset \mathcal{X}(t+1) \subset \mathcal{X}(t) \subset \dots \subset \mathcal{X}. \quad (\text{C.15})$$

2. *The iteration  $\mathcal{T}(\bullet)$  must satisfy  $\mathcal{T}(\Phi^{(t)}) \in (t+1)$ . Furthermore, every limit point of  $\Phi^{(t)}$  must be a fixed point of  $\mathcal{T}(\bullet)$ .*

3. For every  $t$ , we must have  $\mathcal{X}(t) = \mathcal{X}_1(t) \times \cdots \times \mathcal{X}_Q(t)$  where  $\mathcal{X}_q(t) \subset \mathcal{X}_q$ ,  $q \in \mathcal{Q}$ .

□

The first item of Theorem 13 can be proved as follows. let  $\Phi^* = [\Phi_1^*, \dots, \Phi_Q^*]^T$  be the fixed point of the iteration in (C.14). Consider the following set

$$\mathcal{X}_q(t) = \{\Phi \in \mathbb{A} : \|\Phi - \Phi^*\|_{2,\text{block}} \leq \alpha^t \|\Phi^{(0)} - \Phi^*\|_{2,\text{block}}\} \subset \mathbb{A} \quad (\text{C.16})$$

where  $\mathbb{A} = \{\Phi \in \mathbb{R}^Q : 0 \leq \Phi \leq 1\}$ ,  $\|\mathbf{a}\|_{2,\text{block}} = \max_{q \in \mathcal{Q}} \|\mathbf{a}_q\|_2$  is the vector block-maximum norm for  $\mathbf{a} = [\mathbf{a}_1, \dots, \mathbf{a}_Q]^T$  with  $\|\bullet\|_2$  defined as the Euclidean norm, and  $\alpha = \|\mathbf{A} + \mathbf{B}\|$  with  $\mathbf{A}$  and  $\mathbf{B}$  defined in (5.34) and (5.35). It can be easily seen that iff  $\alpha < 1$  we have

$$\alpha^{t+1} \|\Phi^{(0)} - \Phi^*\|_{2,\text{block}} < \alpha^t \|\Phi^{(0)} - \Phi^*\|_{2,\text{block}}, \quad \forall n = 0, 1, \dots \quad (\text{C.17})$$

Hence, we can conclude that

$$\mathcal{X}(t+1) \subset \mathcal{X}(t) \subset \mathbb{A}, \quad t = 1, 2, \dots \quad (\text{C.18})$$

The second item of Theorem 13 can be concluded from Theorem 7. As for the third item of Theorem 13, consider the following. The set  $\mathcal{X}(t) = \mathcal{X}_1(t) \times \cdots \times \mathcal{X}_Q(t)$  can be decomposed as follows for all  $t$ :

$$\mathcal{X}_q(t) = \{0 \leq \Phi_q \leq 1 : \|\Phi_q - \Phi_q^*\| \leq \alpha^t \|\Phi^{(0)} - \Phi^*\|_{2,\text{block}}\}. \quad (\text{C.19})$$

Hence, all three conditions required for asynchronous convergence of Algorithm 1 can be satisfied provided that Theorem 7 holds.

### C.3 Proof of Theorem 10

Without loss of generality assume that  $\Omega$  represents a set of multiple independent (fictitious) Eves, whose locations (inside a given area) follows the PPP distribution with density  $\lambda$ . Obviously, these multiple Eves can be simplified to one Eve provided that a certain density and a certain area are given. Denote  $e \in \Omega$  as an arbitrary Eve. Using expectation by conditioning, the probability in (5.46) can be written as

$$\Pr\{\Gamma\gamma < \nu\} = E_{\Omega} \left[ \prod_{e \in \Omega} \Pr\{\Gamma_e \gamma_e < \nu | \Omega\} \right] \quad (\text{C.20a})$$

$$= E_{\Omega} \left[ \exp \left( \sum_{e \in \Omega} \log \left( \Pr\{\Gamma_e \gamma_e < \nu | \Omega\} \right) \right) \right]. \quad (\text{C.20b})$$

In our scenario, each Bob assumes Eves are distributed according to the PPP  $\Omega$  in a circle around him with radius  $d_0$ . The relation between  $d_{qe}$  and  $d'_{qe}$  can be written as  $d_{qe} = \sqrt{d_{qq}^2 + d'_{qe}{}^2 - 2d_{qq}d'_{qe}\cos\varphi}$ , where  $\varphi$  is the angle between  $d'_{qe}$  and  $d_{qq}$  that is uniformly distributed in the range  $[0, 2\pi]$ . Thus,

$$\Gamma = \left( \frac{\beta}{\sqrt{d_{qq}^2 + \beta^2 - 2d_{qq}\beta\cos\varphi}} \right)^{\eta}. \quad (\text{C.21})$$

Let  $d'_{qe} = \beta$ . The expectation in (C.20b) is equivalent to *Laplace functional* of a point process, so (C.20a) can be reduced to [124, Ch. 7]

$$\Pr\{\Gamma\gamma < \nu\} = \exp \left( -\lambda \int_0^{d_0} \int_0^{2\pi} \Pr \left\{ \left( \frac{\beta}{\sqrt{d_{qq}^2 + \beta^2 - 2d_{qq}\beta\cos\varphi}} \right)^{\eta} \gamma > \nu \right\} \beta d\beta d\varphi \right). \quad (\text{C.22})$$

Let  $\xi_q \triangleq \left( \frac{\beta}{\sqrt{d_{qq}^2 + \beta^2 - 2d_{qq}\beta \cos \varphi}} \right)^\eta$ ,  $q \in \mathcal{Q}$ . The quantity  $\gamma$  in (C.22) is the SINR of a one-branch diversity combiner with  $N_q$  interferers whose CDF is [127]

$$F_X(\gamma) = 1 - \frac{1}{1 + \gamma}. \quad (\text{C.23})$$

Using (C.23) in (C.22), we end up with

$$\Pr\{\xi_q \gamma > \nu\} = \left(1 + \frac{|\mathbf{d}_q^\dagger \mathbf{H}_{qq}|^2}{\xi_q \tau_q |\mathbf{d}_q^\dagger \mathbf{H}'_{qq}|^2}\right)^{-N_q}. \quad (\text{C.24})$$

#### C.4 Comparison of Complexity and Signaling Overhead Between MRC and MMSE Receivers

We first would like to mention that our work may not be applicable to devices with low computing capabilities like sensors or IoT devices. Note that these devices likely do not have multiple antennas anyway. However, our solution is in fact meant/designed for multiple antenna systems, e.g., smart phone, laptops, BSs whose computing powers are reasonably strong. We also avoided imposing additional computations on nodes in our proposed algorithms. For example, in the linear receiver stage, we chose MRC receivers instead of the MMSE receivers, as the MMSE method poses negligible performance improvement at the cost of additional complexity. In the following, a brief comparison between MMSE and MRC receivers in terms of number of operations is given<sup>2</sup>

The first step to compute an MMSE receiver at each Bob is to calculate the covariance matrix of the interference at the receive chain of each Bob, which is basically a vector mul-

---

<sup>2</sup>We skipped the detailed description of an MMSE method of reception for the sake of brevity. The fundamentals of MMSE receivers can be found at [72, chapter 6].

tiplication operation. Then, each Bob needs to measure the channel between himself and his corresponding Alice and multiply it to the inverse of the interference's covariance matrix to establish the MMSE receiver. Compared to the MRC receiver, which only requires the channel between Bob and his corresponding Alice, the MMSE receiver requires three more operations (two matrix multiplications and one inverse) to be established, which can be significant depending on the number of Alice's/Bob's antennas.

Regarding the calculation of TxFJ and RxFJ powers, we first need to reintroduce the following definitions. The secrecy rate of Alice<sub>q</sub> is denoted as  $C_q^{sec}$ , and can be defined as

$$C_q^{sec} \triangleq \max\{C_q - C_{eq}, 0\} \quad (\text{C.25})$$

where  $C_q$  and  $C_{eq}$  are the information rate at Bob<sub>q</sub> and the leaked rate at Eve from Alice<sub>q</sub>, respectively.  $C_q$  is defined as

$$C_q \triangleq \log\left(1 + \frac{\phi_q P_q}{a_q + b_q p'_q}\right) \quad (\text{C.26})$$

where  $\phi_q$  is the power assignment (PA) for the information signal at Alice<sub>q</sub>,  $P_q$  is Alice<sub>q</sub>'s transmit power,  $a_q$  is the normalized multi-user interference received at Bob<sub>q</sub>,  $b_q$  is the normalized self-interference channel at Bob<sub>q</sub> and  $p'_q$  is the power of RxFJ.  $C_{eq}$  is defined as

$$C_{eq} \triangleq \log\left(1 + \frac{\phi_q P_q}{c_q + d_q p'_q}\right) \quad (\text{C.27})$$

where  $c_q$  is the normalized interference received at Eve (except the interference received from the RxFJ of Bob<sub>q</sub>),  $d_q$  is the normalized interference received from RxFJ of Bob<sub>q</sub>. To analyze the complexity of our power allocation algorithm, we first focus on the case

where full knowledge of E-CSI is available<sup>3</sup>.

#### C.4.1 Computing the Optimal RxFJ Power

The optimal value of RxFJ can be derived as follows:

$$p_q'^* = \begin{cases} P_q', & \text{if } b_q < d_q \\ 0, & \text{if } b_q > d_q. \end{cases} \quad (\text{C.28})$$

where  $P_q'$  is the total power available at Bob<sub>*q*</sub> for RxFJ. It can be seen from (C.28) that setting the optimal amount of RxFJ only involves a comparator to judge on the values of  $b_q$  and  $d_q$ . Again, we assume that in the full-ECSI scenario Alice<sub>*q*</sub> knows the channel between herself and Eve; Moreover, MUI at Eve (i.e.,  $c_q + d_q p_q'^*$ ) is also known at Alice<sub>*q*</sub>,  $q \in \mathcal{Q}$ .

#### C.4.2 Computing the Optimal Power Allocation between Information and TxFJ Signals

The optimal PA (i.e.,  $\phi_q$ ,  $\forall q$ ) can be found from optimization (5.27). The optimal solution for PA (i.e.,  $\phi_q$ ) can be found by simplifying the following equality:

$$c_q = a_q + (b_q - d_q)p_q'^* + \delta^*. \quad (\text{C.29})$$

Notice that the term  $c_q$  includes  $\phi_q$ , i.e.,

$$c_q \triangleq \frac{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}| \sigma_q}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2} + O \quad (\text{C.30})$$

---

<sup>3</sup>We need to emphasize that we use the full-ECSI scenario to build foundation for our scheme to handle the case where knowledge of E-CSI is not available. The procedure for designing the scheme that is robust to E-CSI uncertainties is given in Section V.

where  $|\mathbf{r}_q^\dagger \mathbf{G}_{jq}|$  and  $|\mathbf{r}_q^\dagger \mathbf{G}_q|^2$  are the E-CSI components,  $\sigma_q = (1 - \phi_q)P_q$  is the power allocated to TxFJ and  $O$  covers other interference terms at Eve. Hence, the simplification of the above equality w.r.t.  $\phi_q$  can be easily done. Note that (5.3.2) was derived only to proceed with the game-theoretic analysis of the problem. A detailed procedure to find the optimal value of  $\phi_q$  in a node is as follows.

At a given iteration of our algorithm, say the  $n$ th iteration, after setting the optimal value of RxFJ, in order to determine the optimal PA, Bob<sub>*q*</sub> needs to first measure the interference at his receive chain, i.e.,  $a_q^{(n-1)} + b_q^{(n-1)}p_q'^*$  must be measured, where  $a_q^{(n-1)}$  and  $b_q^{(n-1)}$  indicate the values of  $a_q$  and  $b_q$  at the previous iteration. Assuming that full knowledge of E-CSI is available, Bob<sub>*q*</sub> also knows the MUI at Eve in the previous iteration, i.e.,  $c_q^{(n-1)} + d_q^{(n-1)}p_q'^*$  is known<sup>4</sup>. Hence, Bob<sub>*q*</sub> does the following: **1)** He subtracts the term  $\frac{|\mathbf{r}_q^\dagger \mathbf{G}_{jq}| \sigma_q^{(n-1)}}{|\mathbf{r}_q^\dagger \mathbf{G}_q|^2}$  from  $c_q^{(n-1)}$ ; **2)** He adds the result of subtraction to  $d_q^{(n-1)}p_q'^*$ . Denote the result of this addition as  $g_q$ ; **3)** He finds the optimal PA in the  $n$ th iteration, which can be described as (5.4.2) It can be seen that setting the optimal PA involves simple addition, subtraction and division of scalar values. Moreover, there is no need to know all interference terms at Bob<sub>*q*</sub> and Eve, only the aggregate of these terms (i.e.,  $a_q$  and  $c_q$ ) needs to be known. Knowing the noise floor at Bob<sub>*q*</sub> can be helpful to measure the interference level. For example, in 802.11 systems, the noise level usually stays at  $-90$  dBm [29]. The computation of PA when E-CSI and MUI at Eve are not known still involves simple scalar operations, but is different in terms of the signaling it needs, i.e., the channels that Bob<sub>*q*</sub> needs to know for his computations are different from the full-ECSI scenario.

Thus, to the best of our knowledge, users with reasonably high computational capability can still perform the operations required by our algorithms with modest complexity.

---

<sup>4</sup>Notice that throughout the iterations of our algorithm,  $b_q^{(n-1)} = b_q^{(n)}$  and  $d_q^{(n-1)} = d_q^{(n)}$ . However, the values of  $a_q$  and  $c_q$  can vary across iterations.



## C.5 Detailed Analysis of the Robust Scheme

Note that we focus on no E-CSI knowledge in only Section V. However, for the purpose of laying a theoretical foundation, until Section V, we assume that E-CSI is available. In the scenario where knowledge of E-CSI is not available, we are in fact focused on optimizing the *ergodic secrecy rate*. In what follows, we give the details of our robust scheme. We first present a detailed formulation of our robust scheme to show that our robust scheme focuses on optimizing ergodic secrecy rate. Then, we provide the proofs of existence of NE as well as conditions that guarantee its uniqueness.

### C.5.1 Detailed Formulation of the Robust Scheme

We first need to revisit the main optimization problem in (26). We have

$$\begin{aligned}
& \max_{\phi_q, \delta} U_q(\phi_q, \delta, \xi) = C_q^{sec} \\
& \text{s.t. } c_q(\xi) = a_q + (b_q - d_q(\xi))p_q'^* + \delta \\
& \quad c_q(\xi) > 0 \\
& \quad 0 < \delta < (d_q(\xi) - b_q)P_q' + J(1 - t_q(\xi)) \\
& \quad 0 \leq \phi_q \leq 1.
\end{aligned} \tag{C.31}$$

where  $\xi$  is a parameter that indicates all E-CSI components. Note that the terms  $c_q$ ,  $d_q$  and  $t_q$  are shown as functions of  $\xi$ , as they depend on E-CSI components. When knowledge of E-CSI is not available, the parameter  $\xi$  can be treated as a random variable, i.e.,  $\xi$  represents a random variable that maps the elements of a (continuous) set of random events  $\Omega$  to a real-valued vector which is referred to as E-CSI components. Now, we should optimize the expected value of  $U_q$  w.r.t. E-CSI components (i.e.,  $E_\xi[U_q(\phi_q, \delta, \xi)]$ ),

which is the same as optimizing the ergodic secrecy rate, (i.e.,  $E_\xi[C_q^{sec}]$ ). However, taking the expected value of the objective in (C.31) is not enough to convert problem (C.31) into a stochastic programming problem because the constraints of (C.31) also depend on E-CSI components. Without loss of generality, let  $\Omega$  be a set of infinitely many discrete events  $\omega_i, i = 1, 2, \dots$ , which are mapped to random variables  $\xi_i, i = 1, 2, \dots$ . Thus, the stochastic programming formulation of (C.31) can be written as [124]

$$\begin{aligned} \max_{\phi_q, \delta} \quad & E_\xi[U_q(\cdot, \phi_q, \delta, \xi)] = \sum_{i=1} \Pr(\xi_i) U_q(\cdot, \phi_q, \delta, \xi_i) \\ \text{s.t.} \quad & 0 \leq \phi_q \leq 1. \\ & \left. \begin{aligned} c_q(\xi_i) &= a_q + (b_q - d_q(\xi_i))p_q'^* + \delta \\ c_q(\xi_i) &> 0 \\ 0 < \delta &< (d_q(\xi_i) - b_q)P_q' + J(1 - t_q(\xi_i)) \end{aligned} \right\} \forall i = 1, 2, \dots \quad (\text{C.32}) \end{aligned}$$

Removing the slack variable  $\delta$  gives us the following formulation:

$$\begin{aligned} \max_{\phi_q} \quad & \sum_{i=1} \Pr(\xi_i) U_q(\cdot, \phi_q, \xi_i) \\ \text{s.t.} \quad & 0 \leq \phi_q \leq 1. \\ & \left. \begin{aligned} c_q(\xi_i) &\geq a_q + (b_q - d_q(\xi_i))p_q'^* \\ c_q(\xi_i) &> 0 \end{aligned} \right\} \forall i = 1, 2, \dots \quad (\text{C.33}) \end{aligned}$$

Notice that in (C.32), the constraints need to hold for all  $\xi_i$  (i.e., all realization of E-CSI). In the jargon of stochastic programming, the first constraint in (C.33) is known as *first-stage constraints*, and the set of constraints that depend on  $\xi_i$  are referred to as *second-stage constraints*. In the case of finite set of random events (i.e., finite realizations of  $\xi_i$ ) or some special types of objective functions, one can use *two-stage stochastic program-*

ming approaches to efficiently solve (C.33) [124]. However, the set of random events is not finite in our case because the variations of the wireless environment are usually modeled as continuous distributions. Thus, the formulation in (C.33) becomes prohibitively difficult to solve with two-stage stochastic programming approaches. Therefore, we need to settle with a sub-optimal solution that is easier to achieve. To do this, we look at (C.33) again.

Recall that we already explained that the first second-stage constraint is mainly to do with allocating enough power to TxFJ to achieve positive secrecy. Ensuring that this constraint is satisfied across all  $\xi_i$  (i.e., all realizations of E-CSI) can be limiting. For example, for some (less probable) realizations of E-CSI, the channel between Alice<sub>q</sub> and Eve can be a lot stronger than that between Alice<sub>q</sub> and Bob<sub>q</sub>. Thus, ensuring positive secrecy for this realization can force Alice<sub>q</sub> to allocate most of her power to TxFJ, which may be too conservative. We aim to avoid this issue by ensuring positive secrecy with a certain probability, i.e., positive secrecy is ensured across a subset of E-CSI realizations. In other words, the  $q$ th link needs to satisfy the following:

$$\Pr\left((c_q(\xi_i) \geq a_q + (b_q(\xi_i) - d_q(\xi_i))p_q'^*)\right) \geq \varepsilon \quad (\text{C.34})$$

where  $\varepsilon$  is a given probability for ensuring positive secrecy.

## REFERENCES

- [1] “Cisco visual networking index: Forecast and trends, 2017–2022,” Accessed 2019-08-01. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html>
- [2] C. Neumann, O. Heen, and S. Onno, “An empirical study of passive 802.11 device fingerprinting,” in *Proc. 2012 Int. Conf. Distributed Computing Syst. Workshops*, Jun. 2012, pp. 593–602.
- [3] D. Singelee and B. Preneel, “Location privacy in wireless personal area networks,” in *Proc. ACM WiSec 2006 Conf.*, 2006, pp. 11–18.
- [4] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, “SoK: Security and privacy in implantable medical devices and body area networks,” in *2014 IEEE Symp. Security and Privacy*, May 2014, pp. 524–539.
- [5] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, “LTEInspector: A systematic approach for adversarial testing of 4G LTE,” in *NDSS 2018 Conf.*, Feb. 2018.
- [6] H. Rahbari, M. Krunz, and L. Lazos, “Swift jamming attack on frequency offset estimation: The achilles’ heel of OFDM systems,” *IEEE Trans. Mobile Computing*, vol. 15, no. 5, pp. 1264–1278, May 2016.
- [7] H. Rahbari and M. Krunz, “Secrecy beyond encryption: obfuscating transmission signatures in wireless communications,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 54–60, 2015.
- [8] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, “Privacy attacks to the 4G and 5G cellular paging protocols using side channel information.”

- [9] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.
- [10] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
- [11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
- [12] S. R. Aghdam, A. Nooraiepour, and T. M. Duman, "An overview of physical layer security with finite-alphabet signaling," *IEEE Commun. Surveys Tutorials*, pp. 1–1, 2018.
- [13] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [14] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT 2007 Conf.*, Jun. 2007, pp. 2466–2470.
- [15] 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.
- [16] 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.
- [17] ———, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [18] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

- [19] W. Yang, R. F. Schaefer, and H. V. Poor, "Finite-blocklength bounds for wiretap channels," in *Proc. IEEE ISIT 2016 Conf.*, Jul. 2016, pp. 3087–3091.
- [20] A. Goldsmith and S.-G. Chua, "Variable-rate variable-power MQAM for fading channels," *IEEE Trans. Commun.*, vol. 45, no. 10, pp. 1218–1230, Oct. 1997.
- [21] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
- [22] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [23] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP Conf.*, Apr. 2009, pp. 2437–2440.
- [24] A. Mukherjee and A. L. 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.
- [25] P. Lin, S. Lai, S. Lin, and H. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.
- [26] Q. Li, M. Hong, H. Wai, Y. Liu, W. Ma, and Z. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE Journal Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.
- [27] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

- [28] G. Zheng, I. Krikidis, J. Li, A. P. 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.
- [29] D. Bharadia, E. McMilin, and S. Katti, “Full duplex radios,” in *Proc. ACM SIGCOMM Conference*, 2013, pp. 375–386.
- [30] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, “Achieving single channel, full duplex wireless communication,” in *Proc. ACM MOBICOM 2010 Conf.*, Sep. 2010.
- [31] D. Bharadia and S. Katti, “Full duplex MIMO radios,” in *Proc. USENIX NSDI 2014 Conf.*, 2014, pp. 359–372.
- [32] T. Chen, J. Zhou, N. Grimwood, R. Fogel, J. Marasevic, H. Krishnaswamy, and G. Zussman, “Full-duplex wireless based on a small-form-factor analog self-interference canceller: Demo,” in *Proc. ACM MobiHoc 2016 Conf.*, 2016, pp. 357–358.
- [33] M. B. Dastjerdi, N. Reiskarimian, T. Chen, G. Zussman, and H. Krishnaswamy, “Full duplex circulator-receiver phased array employing self-interference cancellation via beam-forming,” in *Proc. IEEE RFIC 2018 Conf.*, Jun. 2018, pp. 108–111.
- [34] G. Zheng, I. Krikidis, J. Li, A. P. 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.
- [35] R. D. Yates, “A framework for uplink power control in cellular radio systems,” *IEEE J. Sel. Areas Commun.*, vol. 13, no. 7, pp. 1341–1347, Sep. 1995.
- [36] C. U. Saraydar, N. B. Mandayam, and D. J. Goodman, “Efficient power control via pricing in wireless data networks,” *IEEE Trans. Commun.*, vol. 50, no. 2, pp. 291–303, Feb. 2002.

- [37] J. Huang, R. A. Berry, and M. L. Honig, "Distributed interference compensation for wireless networks," *IEEE Journal Sel. Areas Commun.*, vol. 24, no. 5, pp. 1074–1084, May 2006.
- [38] G. Scutari, D. P. Palomar, and S. Barbarossa, "Optimal linear precoding strategies for wide-band non-cooperative systems based on game theory—part II: Algorithms," *IEEE Trans. Signal Process.*, vol. 56, no. 3, pp. 1250–1267, Mar. 2008.
- [39] S. Kim and G. B. Giannakis, "Optimal resource allocation for MIMO ad hoc cognitive radio networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3117–3131, May 2011.
- [40] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "On the secure degrees of freedom in the K-user Gaussian interference channel," in *Proc. IEEE ISIT 2008 Conf.*, Jul. 2008, pp. 384–388.
- [41] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference-assisted secret communication," in *Proc. IEEE Inf. Theory Workshop*, May 2008, pp. 164–168.
- [42] 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.
- [43] D. Park, "Weighted sum rate maximization of MIMO broadcast and interference channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 1742–1753, Mar. 2016.
- [44] ———, "Secrecy rate improvement based on joint decoding in MIMO wiretap channels with a helping interferer," *To appear in IEEE Transactions on Vehicular Technology*, 2016.
- [45] L. Li, A. P. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *IEEE J. Select. Topics Signal Process.*, vol. 10, no. 8, pp. 1433–1448, Dec. 2016.



- [46] Z. Zhang, K. C. Teh, and K. H. Li, "Distributed optimization for resilient transmission of confidential information in interference channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 494–501, Jan. 2017.
- [47] 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.
- [48] L. Ruan, V. K. N. Lau, and M. Z. Win, "Generalized interference alignment ;part II: Application to wireless secrecy," *IEEE Trans. Signal Process.*, vol. 64, no. 10, pp. 2688–2701, May 2016.
- [49] A. Alvarado, G. Scutari, and J.-S. Pang, "A new decomposition method for multiuser dc-programming and its applications," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2984–2998, Jun. 2014.
- [50] S. Fakoorian and A. Swindlehurst, "MIMO interference channel with confidential messages: Game theoretic beamforming designs," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Nov. 2010, pp. 2099–2103.
- [51] 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.
- [52] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 885–899, Feb. 2017.
- [53] Q. Li, Y. Zhang, J. Lin, and S. X. Wu, "Full-duplex bidirectional secure communications under perfect and distributionally ambiguous eavesdropper's CSI," *IEEE Trans. Signal Process.*, vol. 65, no. 17, pp. 4684–4697, Sep. 2017.

- [54] N. H. Mahmood, I. S. Ansari, P. Popovski, P. Mogensen, and K. A. Qaraqe, "Physical-layer security with full-duplex transceivers and multiuser receiver at eve," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4392–4405, Oct. 2017.
- [55] X. Tang, P. Ren, and Z. Han, "Distributed power optimization for security-aware multi-channel full-duplex communications: A variational inequality framework," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 4065–4079, Sep. 2017.
- [56] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5511–5526, Aug. 2016.
- [57] H. Shariatmadari, R. Ratasuk, S. Iraji, A. Laya, T. Taleb, R. J  ntti, and A. Ghosh, "Machine-type communications: current status and future perspectives toward 5G systems," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 10–17, Sep. 2015.
- [58] D. Niyato, P. Wang, and D. I. Kim, "Performance modeling and analysis of heterogeneous machine type communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2836–2849, May 2014.
- [59] G. Wunder, P. Jung, M. Kasparick, T. Wild, F. Schaich, Y. Chen, S. T. Brink, I. Gaspar, N. Michailow, A. Festag, L. Mendes, N. Cassiau, D. Ktenas, M. Dryjanski, S. Pietrzyk, B. Eged, P. Vago, and F. Wiedmann, "5GNow: non-orthogonal, asynchronous waveforms for future mobile applications," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 97–105, Feb. 2014.
- [60] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.
- [61] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

- [62] Y. Zou, “Intelligent interference exploitation for heterogeneous cellular networks against eavesdropping,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1453–1464, Jul. 2018.
- [63] J. Hu, N. Yang, and Y. Cai, “Secure downlink transmission in the internet of things: How many antennas are needed?” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1622–1634, Jul. 2018.
- [64] P. Siyari, M. Krunz, and D. N. Nguyen, “A game theoretic design of artificial-noise aided transmissions in MIMO wiretap interference network,” in *Proc. IEEE GLOBECOM 2016 Conf.*, Dec. 2016, pp. 1–6.
- [65] —, “Friendly jamming in a MIMO wiretap interference network: A nonconvex game approach,” *IEEE Journal Sel. Areas Commun.*, vol. 35, no. 3, pp. 601–614, Mar. 2017.
- [66] —, “Price-based friendly jamming in a MISO interference wiretap channel,” in *Proc. IEEE INFOCOM 2016 Conf.*, Apr. 2016, pp. 1–9.
- [67] —, “Power games for secure communications in single-stream MIMO interference networks,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5759–5773, Sep. 2018.
- [68] —, “Joint transmitter- and receiver-based friendly jamming in a MIMO wiretap interference network,” in *Proc. IEEE ICC 2017 Conf. Workshops*, May 2017, pp. 1323–1328.
- [69] —, “Distributed power control in single-stream MIMO wiretap interference networks with full-duplex jamming receivers,” *IEEE Trans. Signal Process.*, vol. 67, no. 3, pp. 594–608, Feb. 2019.
- [70] P. Siyari and M. Krunz, “Linear precoding with friendly jamming in overloaded MU-MIMO wiretap networks,” in *Proc. IEEE CNS 2019 Conf. Workshops*, Jun. 2019.
- [71] X. Zhou and M. R. McKay, “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

- [72] T. M. Duman and A. Ghrayeb, *Coding for MIMO Communication Systems*. New York, NY, USA: John Wiley and Sons, Ltd, 2007.
- [73] S. Lasaulce and H. Tembine, *Game Theory and Learning for Wireless Networks: Fundamentals and Applications*. Orlando, FL, USA: Academic Press, Inc., 2011.
- [74] S. Kassam and H. Poor, "Robust signal processing for communication systems," *IEEE Commun. Mag.*, vol. 21, no. 1, pp. 20–28, Jan. 1983.
- [75] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.
- [76] Z. Han, D. Niyato, W. Saad, T. Baar, and A. Hjrungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. New York, NY, USA: Cambridge University Press, 2012.
- [77] G. Scutari, F. Facchinei, J. Pang, and L. Lampariello, "Equilibrium selection in power control games on the interference channel," in *Proc. IEEE INFOCOM 2012 Conf.*, Mar. 2012, pp. 675–683.
- [78] M. J. Osborne and A. Rubinstein, *A course in game theory*. Cambridge, MA, USA: MIT Press, 1994.
- [79] D. T. Hoang, X. Lu, D. Niyato, P. Wang, D. I. Kim, and Z. Han, "Applications of repeated games in wireless networks: A survey," *IEEE Commun. Surveys Tutorials*, vol. 17, no. 4, pp. 2102–2135, Fall 2015.
- [80] K. Akkarajitsakul, E. Hossain, D. Niyato, and D. I. Kim, "Game theoretic approaches for multiple access in wireless networks: A survey," *IEEE Commun. Surveys Tutorials*, vol. 13, no. 3, pp. 372–395, Mar. 2011.
- [81] M. Jakobsson, S. Magnusson, C. Fischione, and P. C. Weeraddana, "Extensions of Fast-Lipschitz optimization," *IEEE Trans. Automat. Control*, vol. 61, no. 4, pp. 861–876, Apr. 2016.

- [82] J. R. Correa, A. S. Schulz, and N. E. Stier-Moses, “Selfish routing in capacitated networks,” *Math. Oper. Res.*, vol. 29, no. 4, pp. 961–976, Nov. 2004.
- [83] J.-S. Pang and G. Scutari, “Nonconvex games with side constraints,” *SIAM J. Optimization*, vol. 21, no. 4, pp. 1491–1522, 2011.
- [84] F. Facchinei and J. Pang, *Finite-Dimensional Variational Inequalities and Complementarity Problems*. New York, NY, USA: Springer New York, 2007.
- [85] L. Li, C. Huang, and Z. Chen, “Cooperative secrecy beamforming in wiretap interference channels,” *IEEE Signal Process. Letters*, vol. 22, no. 12, pp. 2435–2439, Dec. 2015.
- [86] X. Huang, B. Beferull-Lozano, and C. Botella, “Quasi-Nash equilibria for non-convex distributed power allocation games in cognitive radios,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3326–3337, Jul. 2013.
- [87] G. Scutari and J. S. Pang, “Joint sensing and power allocation in nonconvex cognitive radio games: Nash equilibria and distributed algorithms,” *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4626–4661, Jul. 2013.
- [88] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wiretap channels,” *EURASIP J. Wireless Commun. Networks*, no. 5, pp. 1–12, Mar. 2009.
- [89] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.
- [90] J. Nocedal and S. J. Wright, *Numerical Optimization*. Berlin, DE: World Scientific, 2006.
- [91] G. Scutari, F. Facchinei, J.-S. Pang, and D. Palomar, “Real and complex monotone communication games,” *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4197–4231, Jul. 2014.
- [92] R. T. Rockafellar, “Applications of convex variational analysis to Nash equilibrium,” in *Proc. 7th Int. Nonlinear Anal. and Convex Anal. Conf.*, 2011, pp. 173–183.

- [93] J. Abadie, *Nonlinear Programming*. North-Holland, 1967.
- [94] G. Scutari, D. Palomar, F. Facchinei, and J.-S. Pang, “Convex optimization, game theory, and variational inequality theory,” *IEEE Signal Process Mag.*, vol. 27, no. 3, pp. 35–49, May 2010.
- [95] R. A. Horn and C. R. Johnson, Eds., *Matrix Analysis*. New York, NY, USA: Cambridge University Press, 1986.
- [96] A. Kannan and U. V. Shanbhag, “Distributed computation of equilibria in monotone nash games via iterative regularization techniques,” *SIAM J. Optimization*, vol. 22, no. 4, pp. 1177–1205, 2012.
- [97] D. Kapetanovic, G. Zheng, and F. Rusek, “Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks,” *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
- [98] A. Mukherjee and A. L. Swindlehurst, “Detecting passive eavesdroppers in the MIMO wiretap channel,” in *Proc. IEEE ICASSP Conf.*, Mar. 2012, pp. 2809–2812.
- [99] C. Shin, R. W. Heath, and E. J. Powers, “Blind channel estimation for MIMO-OFDM systems,” *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 670–685, Mar. 2007.
- [100] S. Yatawatta and A. P. Petropulu, “Blind channel estimation in MIMO-OFDM systems with multiuser interference,” *IEEE Trans. Signal Process.*, vol. 54, no. 3, pp. 1054–1068, Mar. 2006.
- [101] D. Bertsekas, *Nonlinear Programming*. Belmont, MA, USA: Athena Scientific, 1999.
- [102] L. Grippo and M. Sciandrone, “On the convergence of the block nonlinear Gauss-Seidel method under convex constraints,” *Operation Research Lett.*, vol. 26, no. 3, pp. 127–136, Apr. 2000.

- [103] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE J. Select. Areas Commun.*, vol. 21, no. 5, pp. 684–702, Jun. 2003.
- [104] X. He and A. Yener, "The interference wiretap channel with an arbitrarily varying eavesdropper: Aligning interference with artificial noise," in *Proc. 50th Annu. Allerton Conf. Commun., Contr., and Comput.*, Oct. 2012, pp. 204–211.
- [105] G. Eichfelder and J. Jahn, *Vector and Set Optimization*. New York, NY, USA: Springer New York, 2016.
- [106] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.
- [107] D. P. Bertsekas and J. N. Tsitsiklis, Eds., *Parallel and Distributed Computation: Numerical Methods*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1989.
- [108] J. F. Nash, "Equilibrium points in N-person games," *National Academy of Sciences*, vol. 36, no. 1, pp. 48–49, 1950.
- [109] H. Peters, *Finite Games*. Berlin, Heidelberg: Springer Berlin, 2015.
- [110] A. Lozano, A. Tulino, and S. Verdu, "High-snr power offset in multiantenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134–4151, Dec. 2005.
- [111] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.
- [112] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers," in *Proc. IEEE ICC Conf.*, Jun. 2011, pp. 1–5.

- [113] Y. Fujikoshi, V. V. Ulyanov, and R. Shimizu, *Wishart Distribution*. John Wiley & Sons, Inc., 2011, pp. 29–46.
- [114] C. Rao, *Linear statistical inference and its applications*, 2nd ed. New York, NY: Wiley, 1973.
- [115] G. Pederzoli, “On the ratio of generalized variances,” *Commun. in Stat. - Theory and Methods*, vol. 12, no. 24, pp. 2903–2909, Jan. 1983.
- [116] M. Boon, “Generating random variables,” Accessed 2019-09-03. [Online]. Available: <http://www.win.tue.nl/~marko/2WB05/lecture8.pdf>
- [117] W. Yu, G. Ginis, and J. Cioffi, “Distributed multiuser power control for digital subscriber lines,” *IEEE J. Sel. Areas Commun.*, vol. 20, no. 5, pp. 1105–1115, Jun. 2002.
- [118] J. Zheng, Y. Wu, N. Zhang, H. Zhou, Y. Cai, and X. Shen, “Optimal power control in ultra-dense small cell networks: A game-theoretic approach,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4139–4150, Jul. 2017.
- [119] X. Tang, P. Ren, and Z. Han, “Hierarchical competition as equilibrium program with equilibrium constraints towards security-enhanced wireless networks,” *IEEE J. Sel. Areas Commun.*, 2018.
- [120] S. H. Tsai and H. V. Poor, “Power allocation for artificial-noise secure MIMO precoding systems,” *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
- [121] N. Li, X. Tao, H. Wu, J. Xu, and Q. Cui, “Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: Ergodic secrecy sum rate and optimal power allocation,” *IEEE Trans. on Veh. Technol.*, vol. 65, no. 9, pp. 7036–7050, Sep. 2016.
- [122] A. C. Cirik, Y. Rong, and Y. Hua, “Achievable rates of full-duplex MIMO radios in fast fading channels with imperfect channel estimation,” *IEEE Trans. Signal Process.*, vol. 62, no. 15, pp. 3874–3886, Aug. 2014.



- [123] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, “Full-duplex MIMO relaying: Achievable rates under limited dynamic range,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1541–1553, Sep. 2012.
- [124] M. Haenggi, *Stochastic Geometry for Wireless Networks*. New York, NY, USA: Cambridge University Press, 2012.
- [125] T. X. Zheng, H. M. Wang, J. Yuan, Z. Han, and M. H. Lee, “Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.
- [126] S. Loyka and C. D. Charalambous, “Rank-deficient solutions for optimal signaling over wiretap MIMO channels,” *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2400–2411, Jun. 2016.
- [127] H. Gao, P. J. Smith, and M. V. Clark, “Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels,” *IEEE Trans. Commun.*, vol. 46, pp. 666–672, May 1998.
- [128] S. Ross, *Introduction to Probability and Statistics for Engineers and Scientists*. Elsevier Science, 2009.
- [129] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY, USA: Cambridge University Press, 2005.
- [130] A. D. Dabbagh and D. J. Love, “Precoding for multiple antenna gaussian broadcast channels with successive zero-forcing,” *IEEE Trans. Signal Process.*, vol. 55, no. 7, pp. 3837–3850, Jul. 2007.
- [131] H. Sung, S. R. Lee, and I. Lee, “Generalized channel inversion methods for multiuser MIMO systems,” *IEEE Trans. Commun.*, vol. 57, no. 11, pp. 3489–3499, Nov. 2009.

- [132] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. Allerton Conf. Commun., Control, Computing*, Sep. 2009, pp. 1134–1141.
- [133] E. Ekrem and S. Ulukus, "Secure broadcasting using multiple antennas," *J. Commun. Networks*, vol. 12, no. 5, pp. 411–432, Oct. 2010.
- [134] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. 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.
- [135] N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Confidential broadcasting via linear precoding in non-homogeneous MIMO multiuser networks," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2515–2530, Jul. 2014.
- [136] E. Bjornson, M. Kountouris, M. Bengtsson, and B. Ottersten, "Receive combining vs. multi-stream multiplexing in downlink systems with multi-antenna users," *IEEE Trans. Signal Process.*, vol. 61, no. 13, pp. 3431–3446, Jul. 2013.
- [137] H. A. A. Saleh, A. F. Molisch, T. Zemen, S. D. Blostein, and N. B. Mehta, "Receive antenna selection for time-varying channels using discrete prolate spheroidal sequences," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2616–2627, Jul. 2012.
- [138] Y. Gao, H. Vinck, and T. Kaiser, "Massive MIMO antenna selection: Switching architectures, capacity bounds, and optimal antenna selection algorithms," *IEEE Trans. Signal Process.*, vol. 66, no. 5, pp. 1346–1360, Mar. 2018.
- [139] A. F. Molisch, M. Z. Win, Y.-S. Choi, and J. H. Winters, "Capacity of MIMO systems with antenna selection," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1759–1772, Jul. 2005.
- [140] S. Yu, L.-C. Tranchevent, B. De Moor, and Y. Moreau, *Rayleigh Quotient-Type Problems in Machine Learning*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 27–37.

- [141] P. Patcharamaneepakorn, S. Armour, and A. Doufexi, "On the equivalence between SLNR and MMSE precoding schemes with single-antenna receivers," *IEEE Commun. Lett.*, vol. 16, pp. 1034–1037, Jul. 2012.
- [142] X.-D. Zhang, *Matrix Analysis and Applications*. Cambridge, UK: Cambridge University Press, 2017.
- [143] C. Shi, R. A. Berry, and M. L. Honig, "Monotonic convergence of distributed interference pricing in wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2009, pp. 1619–1623.
- [144] R. A. Iltis, S.-J. Kim, and D. A. Hoang, "Noncooperative iterative MMSE beamforming algorithms for ad-hoc networks," *IEEE Trans. Commun.*, vol. 54, no. 4, pp. 748–759, Apr. 2006.
- [145] G. Scutari, S. Barbarossa, and D. P. Palomar, "Potential games: A framework for vector power control problems with coupled constraints," in *Proc. IEEE ICASSP Conf.*, vol. 4, May 2006, pp. IV–IV.
- [146] D. Nguyen and M. Krunz, "Spectrum management and power allocation in MIMO cognitive networks," University of Arizona, Tech. Rep. TR-UA-ECE-2011-2, Tech. Rep., 2011. [Online]. Available: [http://www.ece.arizona.edu/~krunz/TR/MIMOCognitiveTR\\_Aug2011.pdf](http://www.ece.arizona.edu/~krunz/TR/MIMOCognitiveTR_Aug2011.pdf)