Fundamental Limits of Communication in Interference Limited Environments

A Thesis

Submitted for the Degree of

Doctor of Philosophy

in the Faculty of Engineering

by

Parthajit Mohapatra

Electrical Communication Engineering
Indian Institute of Science, Bangalore
Bangalore – 560 012 (INDIA)

February 2015

TO

My Parents

Smt. A. Mohapatra and Sri. P. K. Mohapatra

and

My Wife

Smt. S. Mishra

Acknowledgements

I would like to express my deep gratitude to my thesis advisor *Dr. Chandra R. Murthy* whose continuous guidance and encouragement have been a driving force to reach my goal. His commitment and dedication to work and patience has motivated me a lot during my Ph. D. He has not only taught me how to pursue research but also how to write research papers and present results in an elegant way. I would also like to thank him for his support and advice, whenever I faced problems. I thank the faculty members of ECE and Math departments, where I have attended many courses. I would also like to thank my M.Ṫech. advisor *Dr. Pradipta Kumar Nanda* for motivating me to pursue a career in research.

I would like to thank my colleague *Nissar K. E.* for the collaboration on the problem of interference alignment algorithms for the K-user MIMO Gaussian interference channel. I would also like to thank *K. G. Nagananda* for the collaborative work on multiuser cognitive radio networks.

The journey as a Ph. D. student would not have been enjoyable without my lab-mates *Venu, Sanjeev, Abhay, Bharath, Ranjitha, Nirmal, Gana, Saurabh, Mohit, Geethu,* and *Suma*. Also, I would like to thank my friends *Shilpa, Jobin, Tirupathaiah, and Praveen* from next generation wireless lab for a variety of discussions, both technical and non-technical. I would like to thank *Shilpa* for helping me in many occasions and alerting me to interesting happenings and events on campus. Special thanks to *Tirupathaiah* for making us to laugh on many occasions. I thank *Suma* in helping me with a variety of administrative tasks. I would like to thank *Venu* for many useful discussions ranging from mundane technical points to deep philosophical questions. I would also like to thank *Sanjeev* and *Venu* for introducing me to many great Kannada poets and writers. This

has helped me recreate my interest in literature and has given another new dimension to my life. I would like to thank *Jyoti* didi for providing nice tea at Janta Bazar, which prevented me from falling asleep during the afternoons. My thanks also go to my friend *Sanat* and my colleague *Priyadarshi* at C. V. Raman college of engineering for their support during a difficult period of my life.

My dream of getting a Ph. D. would not have been fulfilled without the support and encouragement of my family members. I thank my father and mother for everything. Also, I like to thank my sister *Preeti* and nephew *Sloak* for being with me. My thanks also go to my in-laws for their good wishes and support. Finally, I want to thank my wife *Sanghamitra* whose continuous support and unconditional love has helped me overcome many difficult situations. Especially towards the end of my Ph. D. when my mother was struggling with health problems, it would have indeed been very difficult for me to concentrate on my research without her support.

There is no doubt that the experience gained during the Ph. D. will play a crucial role in shaping my career. I also believe that it will help me take a better outlook towards life and the world in general.

Abstract

In multiuser wireless communications, interference not only limits the performance of the system, but also allows users to eavesdrop on other users' messages. Hence, interference management in multiuser wireless communication has received significant attention in the last decade, both in the academia and industry. The interference channel (IC) is one of the simplest information theoretic models to analyze the effect of interference on the throughput and secrecy of individual messages in a multiuser setup. In this thesis, the IC is studied under different settings with and without the secrecy constraint. The main contributions of the thesis are as follows:

- The generalized degrees of freedom (GDOF) has emerged as a useful approximate measure of the potential throughput of a multiuser wireless system. Also, multiple antennas at the transmitter and receiver can provide additional dimension for signaling, which can in turn improve the GDOF performance of the IC. In the initial part of the thesis, a K-user MIMO Gaussian IC (GIC) is studied from an achievable GDOF perspective. An inner bound on GDOF is derived using a combination of techniques such as treating interference as noise, zero-forcing receiving, interference alignment (IA), and extending the Han-Kobayashi (HK) scheme to K users. Also, outer bounds on the sum rate of the K-user MIMO GIC are derived, under different assumptions of cooperation and providing side information to the receivers. The derived outer bounds are simplified to obtain outer bounds on the GDOF. The relative performance of these bounds yields insight into the performance limits of the multiuser MIMO GIC and the relative merits of different schemes for interference management.

- Then, the problem of designing the precoding and receive filtering matrices for IA is explored for K-user MIMO $(M \times N)$ GIC. Two algorithms for designing

the precoding and receive filtering matrices for IA in the block fading or constant MIMO IC with a finite number of symbol extensions are proposed. The first algorithm for IA is based on aligning a subset of the interfering signal streams at each receiver. As the first algorithm requires global channel knowledge at each node, a distributed algorithm is proposed which requires only limited channel knowledge at each node. A new performance metric is proposed, that captures the possible loss in signal dimension while designing the precoders. The performance of the algorithms are evaluated by comparing them with existing algorithms for IA precoder design.

- In the later part of the thesis, a 2-user IC with limited-rate transmitter cooperation is studied, to investigate the role of cooperation in managing interference and ensuring secrecy. First, the problem is studied in the deterministic setting, and achievable schemes are proposed, which use a combination of interference cancelation, relaying of the other user's data bits, time sharing, and transmission of random bits, depending on the rate of the cooperative link and the relative strengths of the signal and the interference. Outer bounds on the secrecy rate are derived, under different assumptions of providing side information to receivers and partitioning the encoded message/output depending on the relative strength of the signal and the interference. The achievable schemes and outer bounds are extended to the Gaussian case. For example, while obtaining outer bounds, for the Gaussian case, it is not possible to partition the encoded message or output as performed in the deterministic case, and the novelty lies in finding the analogous quantities for the Gaussian case. The proposed achievable scheme for the Gaussian case uses a combination of cooperative and stochastic encoding along with dummy message transmission. For both the models, one of the key techniques used in the achievable scheme is interference cancelation, which has two benefits: it cancels interference and ensures secrecy simultaneously. The results show that limited-rate transmitter cooperation can greatly facilitate secure communications over 2-user ICs.

Glossary

AEP	:	Asymptotic Equipartition Property
AWGN	:	Additive White Gaussian Noise
BC	:	Broadcast Channel
DOF	:	Degrees of Freedom
GDOF	:	Generalized Degrees of Freedom
GIC	:	Gaussian Interference Channel
GMBC	:	Gaussian MIMO Broadcast Channel
GSIC	:	Gaussian Symmetric Interference Channel
HK-scheme	:	Han-Kobayashi scheme
IA	:	Interference Alignment
IB	:	Inner Bound
IC	:	Interference Channel
INR	:	Interference-to-Noise Ratio
LDIC	:	Linear Deterministic IC
MAC	:	Multiple Access Channel
MIMO	:	Multiple-Input Multiple-Output
OB	:	Outer Bound
RHS	:	Right Hand Side
SIMO	:	Single-Input Multiple-Output
SISO	:	Single-Input-Single-Output
SLDIC	:	Symmetric Linear Deterministic IC
SNR	:	Signal-to-Noise Ratio
ZF	:	Zero-Forcing

Notation

Boldface lower case letters	:	Vectors
Boldface upper case letters	:	Matrices
$\mathcal{C}$	:	Field of complex numbers
$\mathcal{CN}(\mu, \sigma^2)$	:	Circularly symmetric complex Gaussian distribution with mean μ and variance σ^2
$\mathcal{CN}(\mu, \Sigma)$	:	Circularly symmetric complex Gaussian distribution with mean vector μ and covariance Σ
$E[.]$	:	Expectation operator
$\mathcal{F}_2$	:	Binary field
$\mathbf{H}_{ij}$	:	$N_j \times M_i$ channel gain matrix for transmitter i to receiver j
$H(\mathbf{x})$	:	Shannon entropy of discrete random variable $\mathbf{x}$
$h(\mathbf{x})$	:	Differential entropy of continuous random variable $\mathbf{x}$
$I(\mathbf{x}; \mathbf{y})$	:	Mutual information between random variables $\mathbf{x}$ and $\mathbf{y}$
$\mathbf{I}_N$	:	Identity matrix of dimension $N \times N$
K	:	Number of users in the interference channel
M	:	Number of transmit antennas at the transmitter
M_i	:	Number of transmit antennas at the transmitter i
N	:	Number of receive antennas at the receiver
N_j	:	Number of receive antennas at the receiver j
P_i	:	Average power constraint at the i^{th} transmitter
T_ϵ^N	:	Weak typical set with respect to P_X
$[a : b]$	:	Sequence of numbers from $a, a+1, \ldots, b$ and $a \leq b$
$\mathbf{1}_A$	:	Indicator function, equal to 1 if A is true, and equal to 0 otherwise
$(.)^T$	:	Transposition
$(.)^H$	:	Hermitian transposition
$\|.\|$	:	Determinant of a matrix
$\oplus$	:	XOR operation

Contents

List of Figures

List of Tables

Chapter 1

Introduction

With the ever-increasing demand for high data rates and better quality of service in a multiuser wireless communication system, interference is one of the major factors limiting the performance of the system. Interference arises in a wireless environment, when multiple uncoordinated users share a common resource and the users do not have a priori information on the resource being shared. When the strength of interference is higher than the strength of the thermal noise at the receiver, the impairments caused by interference become more significant than that caused by noise. Under this condition, the system is said to operate in the interference-limited regime, as the performance of the system is mainly limited by interference rather than by noise. In order to mitigate the effect of interference, most of the current wireless communication systems use the following two techniques:

1. *Orthogonalize the communication links*: In this case, the communication links are orthogonalized in time/frequency, so that the transmitters do not cause interference to unintended users. But, with increase in the number of users, the performance of the system deteriorates. Also, this kind of scheme does not take strength of the

interference into account.

2. *Treat interference as noise*: In this case, receiver treats interference as noise, and performs decoding considering the sum of the interference and thermal noise as the effective noise. However, this ignores the signal structure inherent in the interference. In particular, when the interference is strong enough to be decodable at an unintended receiver, the receiver can completely cancel the interference, which could outperform treating interference as noise.

Hence, both of the above approaches can be suboptimal depending on the strength of interference or the number of users present in the system. One way to improve the performance of the system is to use multiple antennas at transmitter and receiver. These multiple antennas can be used, among other things, to nullify interference by orthogonalizing users, to suppress noise, or to increase the data rate by transmitting multiple parallel data streams. This leads to several interesting questions related to how the available spatial resources in a multiuser multi-antenna system should be shared among the users to effectively manage the interference, and thereby maximize the overall system performance.

Another important issue in multiuser wireless communications is that the users are susceptible to eavesdropping due to the broadcast nature of the wireless medium. Hence, interference not only limits the overall throughput of the system, but also allows users to eavesdrop on other users' messages. The interference channel (IC) is one of the simplest information theoretic models to analyze the effect of interference on the throughput and secrecy of individual messages in a multiuser setup. Recently, the IC has been studied extensively without [7–10] and with secrecy constraints [6, 11, 12].

This, in turn, has given useful insights on the fundamental limits of communication and different techniques to manage interference for various communication models.

1.1 Background

A model of a K-user multiple-input multiple-output (MIMO) Gaussian IC (GIC) with M antennas at each transmitter and N antennas at each receiver is shown in Fig. 1.1. In this model, K transmitters communicate with K receivers, with each transmitter having an independent message for its corresponding receiver. Let $\mathbf{H}_{ij}$ represent the $N \times M$ channel gain matrix from transmitter i to receiver j. The channel coefficients are assumed to be drawn from a continuous distribution such as the Gaussian distribution. The received signal at the j-th receiver, denoted by $\mathbf{y}_j$, is modeled as:

$$\mathbf{y}_j = \mathbf{H}_{jj}\mathbf{x}_j + \sum_{i=1, i\neq j}^{K} \mathbf{H}_{ji}\mathbf{x}_i + \mathbf{z}_j, \tag{1.1}$$

where $\mathbf{z}_j$ is the complex symmetric Gaussian noise vector, distributed as $\mathbf{z}_j \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$ and $\mathbf{x}_i$ is the signal transmitted by the i-th user.

1.1.1 Approximate capacity characterization

Generalized degrees of freedom (GDOF)

The study of an information theoretic model similar to IC dates back to 1961 [13], where the two-way communication channel was studied. Since then, the IC has been studied extensively, and under different scenarios (see, for example, [1,7–10,14]). However, the capacity of the IC has remained an open problem even in the 2-user case, except for some special cases like strong/very strong interference regimes [15, 16]. Due to this,

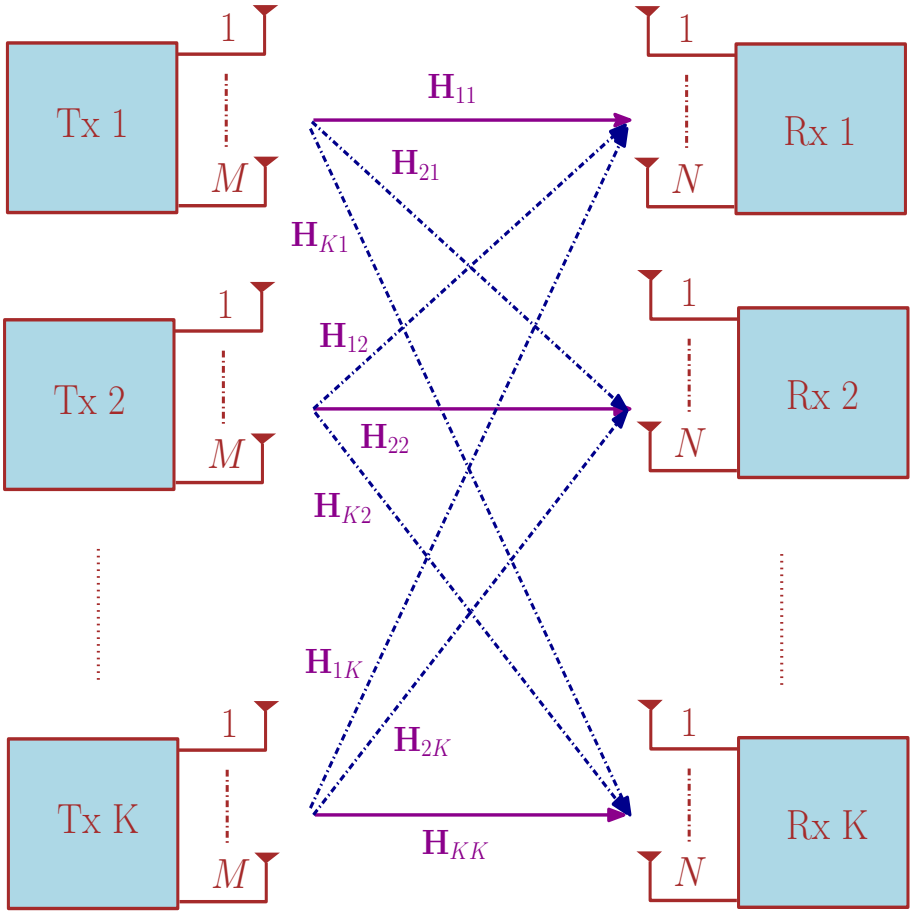


Figure 1.1: The K-user MIMO Gaussian interference channel.

approximate characterization of the capacity has recently received significant research attention. In turn, this has resulted in new, useful insights into the performance limits of communication systems and how to achieve them. Towards this, the so-called generalized degrees of freedom (GDOF), introduced in [8], has been used as an approximation of capacity at high signal-to-noise ratio (SNR) and interference-to-noise ratio (INR). The degrees of freedom (DOF), defined in [17], has been used as an approximate measure of capacity at high SNR, when the signal and interference powers are linearly related.

For a point-to-point MIMO system with M antennas at transmitter and N antennas

at receiver, the DOF of the system is $\min\{M, N\}$. For a 2-user Gaussian IC (GIC) with M_i antennas at the i^{th} $(i = 1, 2)$ transmitter and N_i antennas at the i^{th} receiver, the sum DOF is given by $\min\{M_1+M_2, N_1+N_2, \max\{M_1, N_2\}, \max\{M_2, N_1\}\}$ [17]. Hence, for the symmetric case, when the transmitters and receivers are equipped with M antennas, then each user can achieve $\frac{M}{2}$ DOF by time sharing between the two user pairs. For the K-user MIMO Gaussian symmetric IC, time sharing can only achieve a DOF of $\frac{M}{K}$ per user, while IA can continue to achieve a DOF of $\frac{M}{2}$ per user regardless of K [9]. Many other interesting results on the GDOF/DOF of the K-user IC can be found in [1, 2, 14].

The deterministic model

Another communication model which has been used as a high SNR approximation for multiuser wireless communication systems is the so-called *deterministic model*, first introduced in [18]. The deterministic model captures three key features of wireless communication: channel strength, broadcast, and superposition. Initially, it was introduced for a single source and a single destination with an arbitrary number of relay nodes. The importance of the deterministic model is that it is sufficiently simple, so that the tight achievable schemes and outer bounds can be obtained relatively easily, and yet sufficiently accurate, so that the techniques and results translate well to yield corresponding achievable schemes and outer bounds in the Gaussian channel case. The deterministic model of a 2-user Gaussian symmetric IC (GSIC) for the symmetric case is shown in Fig. 1.2. In this case, noise is modeled by truncation and interference is

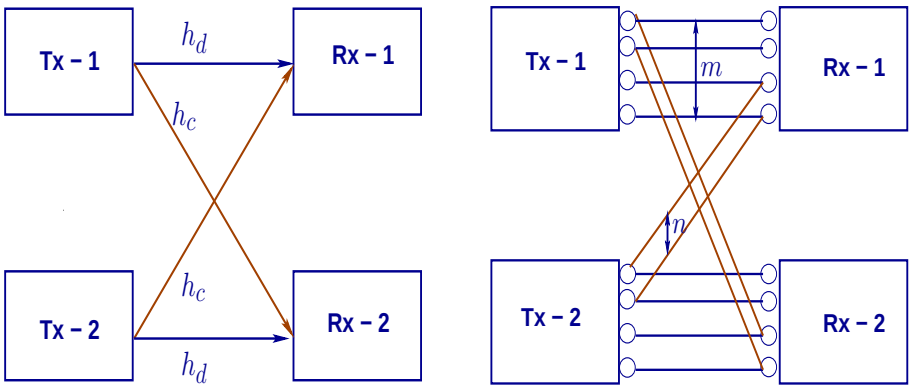


Figure 1.2: 2-user IC: (a) Gaussian case and (b) deterministic case.

modeled by XOR operation [18]. The signals at the receivers are modeled as:

$$\begin{aligned} \mathbf{y}_1 &= \mathbf{D}^{q-m}\mathbf{x}_1 \oplus \mathbf{D}^{q-n}\mathbf{x}_2, \\ \mathbf{y}_2 &= \mathbf{D}^{q-m}\mathbf{x}_2 \oplus \mathbf{D}^{q-n}\mathbf{x}_1, \end{aligned} \tag{1.2}$$

where summation and multiplication are in $\mathcal{F}_2$, $\mathbf{x}_i$ and $\mathbf{y}_i$ are binary vectors of length $q \triangleq \max\{m, n\}$, $\mathbf{D}$ is a $q \times q$ downshift matrix with elements $d_{j',j''} = 1$ if $2 \leq j' = j'' + 1 \leq q$ and $d_{j',j''} = 0$ otherwise, and $\oplus$ stands for XOR operation.

The deterministic model is completely specified by the parameters m and n. These parameters are related to GSIC in the following way: $m \triangleq (\lfloor \log \text{SNR} \rfloor)^+$ and $n \triangleq (\lfloor \log \text{INR} \rfloor)^+$, where $\text{SNR} \triangleq Ph_d^2$ and $\text{INR} \triangleq Ph_c^2$. Here, for the Gaussian case, it is assumed that P is the power in the signal $\mathbf{x}_i$ $(i = 1, 2)$ and that the noise is distributed as $\mathcal{CN}(0, 1)$.

In recent years, the deterministic model has been used to study various communication scenarios to get insights into the achievable schemes and outer bounds for their Gaussian counterparts [19, 20]. In [19], the capacity region of the deterministic IC is

characterized. The study of the deterministic IC gives sound mathematical backing for the near-optimality of some well-known achievable schemes in the Gaussian case [8]. In [20], the capacity of the deterministic model for 2-user IC with limited-rate transmitter cooperation is characterized. Also, the deterministic model has been used to study communication models with secrecy constraints [21–23].

1.1.2 Schemes for managing interference

Among different possible methods to mitigate the effect of interference, two major approaches have emerged:

1. The Han-Kobayashi (HK) scheme [7,8]

2. Interference alignment (IA) [9,24]

The above schemes are explained briefly in the following.

Han-Kobayashi (HK) scheme

The HK-scheme, proposed in [7], is known to achieve the largest possible rate region for the 2-user single-input-single-output (SISO) IC. The HK-scheme is based on splitting the message into private and common parts. The private part of the message is required to be decodable at the intended receiver, whereas the common part of the message is required to be decodable at both the receivers. The HK-scheme allows arbitrary splits of each user's transmit power over the private and common part of the message, as well as time sharing between multiple such splits. However, the optimization over different power splits and time sharing is not completely understood. Also, exactly how close the achievable scheme can come to the capacity of the channel is not known.

Recently, in [8], it was shown that a special case of the HK-scheme can achieve a rate within 1 bits/s/Hz of the capacity for all values of the channel parameters. One of the important aspects of this scheme is that the power of the private part of the message is chosen such that it is received at the noise floor of the unintended receiver. Hence, the interference caused by the private part of the message will have a relatively small effect on the performance. If the direct channel is strong, then the private part of the message can convey a significant amount of information to the intended receiver. The common part of the message can be decoded, and its effect can be canceled at the unintended receiver. The outer bounds derived in [8] help to establish that the HK-scheme can achieve within 1 bits/s/Hz of the capacity for all values of the channel parameters, and also, that the scheme is GDOF optimal. Some of the works analyzing the performance of the HK scheme for an IC and under different settings include [1–3].

Interference alignment (IA)

Interference alignment (IA) is a precoding technique that attempts to align interfering signals to a reduced dimensional subspace at each receiver. The interference can be aligned in space, time, or, frequency. It was recently shown that with IA, the sum rate achieved in the K-user IC scales linearly with the number of users [9, 25]. In [9], it is shown that the sum DOF for the K-user GIC with $M \geq 1$ antennas at each transmitter and receiver is $\frac{KM}{2}$, if the channel coefficients are time-varying and drawn from a continuous distribution. Hence, with IA, every user can achieve half the DOF that can be achieved without interference, irrespective of the number of users. More results on IA used in various communication models can be found in [14, 26–28].

Most of the aforementioned achievable DOF results require long symbol extensions

(that is, the interference is aligned when one considers a large number of symbols together) or global channel knowledge at each node, which make these methods unsuitable for practical implementation. Hence, an important problem is to devise algorithms for computing the transmit precoding matrices and the receive filtering matrices for aligning the interference at all receivers that require a limited number of symbol extensions, or require only local channel state information at each node. Some of the algorithms which approximately achieve IA can be found in [29–31].

1.1.3 Information theoretic secrecy

The notion of information theoretic secrecy was first introduced in [11], where secure communication is considered between a legitimate transmitter and receiver pair, in the presence of an eavesdropper. The transmitter and receiver share a secret key, which is unknown at the eavesdropper. It is shown that perfect secrecy of the message can be ensured if and only if the length of the key is greater than or equal to the length of the message. This is a negative result, since it implies that the length of the key, and therefore the compulsory overhead in communicating in sharing it securely, increases as the length of the data increases. In this model, both the legitimate receiver and eavesdropper listen through the same channel. But, in most physical scenarios of interest, the channel to the legitimate receiver will be different from the channel to the eavesdropper. In [32], a wiretap channel is considered, where the legitimate receiver and eavesdropper receive their signals through different channels. In this case, a nonzero secrecy rate is achieved without sharing a secret key, when the channel to the eavesdropper is more noisy than the channel to the legitimate receiver. More results on wiretap channel with

different settings can be found in [6, 33–35].

The interference channel has been analyzed under different eavesdropper settings, to understand the impact of interference on the achievable rate performance and secrecy of the system [12, 21, 36, 37]. In [12], the broadcast and IC with independent and confidential messages are considered. The achievable scheme for the IC is based on stochastic encoding, and the achievable scheme for the broadcast channel (BC) uses double-binning scheme. In [36], the communication limits of the 2-user IC is investigated in the presence of an external eavesdropper. In this case, both the users design their randomized codebooks cooperatively. Also, IA precoding along with the secrecy constraint is considered in [37], and the goal is to ensure secrecy of individual messages in the case of a frequency/time selective K-user GIC with confidential messages. The role of cooperative relaying in ensuring secrecy under different communication models can be found in [38–40].

1.1.4 Outer bounds on capacity

An important step in characterizing the capacity of any communication system, when the exact capacity is intractable, is to derive tight outer bounds. These outer bounds provide limits on the rate-tuples of the users in the system beyond which it is not possible to achieve arbitrarily low probabilities of decoding error at the receivers. Deriving outer bounds thus helps in obtaining insights into the performance limits of the system, and to establish the optimality or otherwise of any proposed achievable scheme. Most of the existing literature uses the celebrated Fano's inequality [41] to obtain outer bounds on the rates achievable in a given communication system. Mathematically,

Fano's inequality is stated as follows.

Theorem 1 ([41]). *Given an arbitrary code* $(2^{nR}, n)$ *consisting of code words* $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(2^{nR})}$, *let* $\mathbf{X} = (X_1, X_2, \ldots, X_n)$ *be a random vector that equals* $\mathbf{x}^{(i)}$ *with probability* $p(\mathbf{x}^{(i)})$, $i = 1, 2, \ldots, 2^{nR}$, *where* $\sum_{i=1}^{2^{nR}} p(\mathbf{x}^{(i)}) = 1$. *Let* $\mathbf{Y} = (Y_1, Y_2, \ldots, Y_n)$ *be the corresponding output sequence when* $\mathbf{X}$ *is transmitted over a channel. If* $p(e)$ *is the probability of error of the code, computed for the given input distribution, then*

$$H(\mathbf{X}|\mathbf{Y}) \leq H(p(e)) + p(e) \log \left(2^{nR} - 1\right), \tag{1.3}$$

where $H(p(e)) = -p(e) \log p(e) - (1 - p(e)) \log(1 - p(e))$ *and* $H(X|Y)$ *is the conditional entropy.*

Along with Fano's inequality, obtaining outer bound typically involves bounding the entropy terms or providing side information to receiver. The side information provided to receiver depends on the system model under consideration. Determining the form of side information to be provided to transmitter/receiver plays a crucial role in obtaining tight outer bounds. Giving too much side information to transmitter/receiver may result in a loose outer bound. Giving too little information may render the outer bound analytically intractable.

A seminal paper on deriving outer bounds on the 2-user IC is [8], which helps to establish that a simple variant of the HK-scheme can achieve rate within 1 bits/s/Hz of the outer bound for all values of the channel parameter. Outer bounds on the DOF and GDOF for multiuser ICs can be found in [1, 9, 14, 17, 25]. In [17], the outer bound helps to establish that a zero-forcing (ZF) receiving/precoding can achieve the optimal

sum DOF. In [9], the outer bound helps to establish the optimality of IA for the K-user SISO GIC. Also, outer bounds on DOF for the K-user MIMO GIC can be found in [14,25]. Outer bounds on DOF/GDOF for other communication models can be found in [2,26,42].

For communication models where secrecy of the message is also an issue, the basis for developing outer bounds are the twin considerations of data recoverability at the intended receiver and the security constraints at the unintended receivers. In general, the derivation of the outer bound on the secrecy rate involves use of Fano's inequality along with imposing the constraints imposed by the secrecy requirement. Outer bounds for different communication models with the secrecy constraint can be found in [6,12,36,43].

1.2 Challenges in interference-limited multiuser wireless communication systems

As mentioned earlier, the capacity of 2-user IC is not known even in the Gaussian case. The difficulty lies in obtaining capacity achieving schemes and deriving tight outer bounds. One of the ways to make headway into this problem is to approximate the capacity, rather than attempting an exact characterization. In this thesis, the following key issues are addressed:

- In a multiuser MIMO setup, the use of multiple antennas at the transmitters and receivers can provide additional dimensions for signaling, which can, in turn, improve the GDOF performance of the IC. Characterizing the GDOF performance of a multiuser MIMO IC is therefore an important problem (Chapters 2-4).

- Linear precoding at the transmitters and zero-forcing filtering at the receivers is one way to achieve the sum DOF promised by IA. An important problem is thus to devise algorithms for computing the transmit precoding matrices and the receive filtering matrices that align the interferences at all the receivers (Chapter 5).

- As mentioned earlier, wireless communication is susceptible to eavesdropping owing to the broadcast nature of the medium. The past works on IC have shown that cooperation between the transmitters/receivers can increase the achievable rate significantly [20, 44]. However, the effectiveness of transmitter cooperation in managing interference and ensuring secrecy has not been analyzed in the literature. Hence, exploring the role of transmitter cooperation in managing interference and ensuring secrecy in 2-user IC is of significant importance and can provide useful insights into system performance (Chapters 6-9).

1.3 Outline of the thesis and summary of contributions

Chapter 2 of this dissertation proposes achievable schemes for the K-user MIMO GSIC. The K-user MIMO GSIC where each transmitter has M antennas and each receiver has N antennas is studied from a generalized degrees of freedom (GDOF) perspective. An inner bound on the GDOF is derived using a combination of techniques such as treating interference as noise, zero forcing (ZF) at the receivers, IA, and extending the HK-scheme to K users, as a function of the number of antennas and the $\log \text{INR}/\log \text{SNR}$ level. Several interesting conclusions are drawn from the derived bounds. It is shown, for example, that when $K > \frac{N}{M} + 1$, a combination of the HK and IA schemes performs the best among the schemes considered.

Chapter 3 of the thesis proposes outer bounds on the sum rate for the K-user MIMO GIC. Three outer bounds are derived, under different assumptions of cooperation and providing side information to receivers. The novelty in the derivation lies in the careful selection of side information, which results in the cancellation of the negative differential entropy terms containing signal components, leading to a tractable outer bound. The overall outer bound is obtained by taking the minimum of the three outer bounds. The derived bounds are simplified for the MIMO GSIC to obtain outer bounds on the GDOF.

Chapter 4 of the thesis compares the achievable schemes derived in Chapter 2 with the outer bounds derived on the GDOF in Chapter 3. The bounds yield insight into the performance limits of multiuser MIMO GICs and the relative merits of different schemes for interference management. These insights are confirmed by establishing the optimality of the bounds in specific cases using an inner bound on the GDOF derived in the second chapter. It is also shown that many of the existing results on the GDOF of the GIC can be obtained as special cases of the bounds, e.g., by setting $K = 2$ or the number of antennas at each user to 1.

Chapter 5 of the thesis proposes novel precoder design algorithms for IA in the case of the K-user MIMO $(M \times N)$ GIC. A new performance metric for evaluating the efficacy of IA algorithms is proposed, which measures the extent to which the desired signal dimensionality is preserved after zero-forcing the interference at the receiver. Inspired by the metric, two algorithms are proposed for designing the linear precoders and receive filters for IA in the constant MIMO IC with a finite number of symbol extensions.

The first algorithm uses an eigenbeamforming method to align sub-streams of the interference to reduce the dimensionality of the interference at all the receivers. The second algorithm is iterative, and is based on minimizing the interference leakage power while preserving the dimensionality of the desired signal space at the intended receivers. The improved performance of the algorithms is illustrated by comparing them with existing algorithms for IA using Monte Carlo simulations.

Chapters 6-9 of the thesis explore the role of cooperation on managing interference and ensuring secrecy of individual messages in the case of IC. Chapter 6 of the thesis presents novel achievable schemes for the 2-user symmetric linear deterministic interference channel (SLDIC) with limited-rate transmitter cooperation and perfect secrecy constraints at the receivers. The proposed achievable scheme uses a combination of interference cancelation, relaying of the other user's data bits, time sharing, and transmission of random bits, depending on the rate of the cooperative link and the relative strengths of the signal and the interference. The results show, for example, that the proposed scheme achieves the same rate as the capacity without the secrecy constraints, in the initial part of the weak interference regime. Also, sharing random bits through the cooperative link can achieve a higher secrecy rate compared to sharing data bits, in the very high interference regime. The results highlight the importance of limited transmitter cooperation in facilitating secure communications over 2-user interference channels.

In the seventh chapter, outer bounds are presented for the 2-user SLDIC with limited-rate transmitter cooperation and perfect secrecy constraints at the receivers. Five outer

bounds are derived, under different assumptions of providing side information to receivers and partitioning the encoded message/output depending on the relative strength of the signal and the interference. The usefulness of these outer bounds is shown by comparing the bounds with the inner bound on the achievable secrecy rate derived in the previous chapter. Also, the outer bounds help to establish that sharing random bits through the cooperative link can achieve the optimal rate in the very high interference regime.

Chapter 8 proposes achievable schemes for the 2-user GSIC with limited-rate transmitter cooperation and weak secrecy constraints at the receivers. The achievable schemes are derived using the intuitions gained from studying the SLDIC in Chapter 6. The proposed achievable scheme uses a combination of cooperative and stochastic encoding, along with dummy information transmission. The schemes differ in their construction depending on the interference regime (weak/moderate/high), and the chapter provides details of the differences as well as their corresponding performance. For example, in contrast to the achievable scheme for the weak/moderate interference regime, the dummy message sent by one of the users i is required to be decodable at the receiver j in the high interference regime.

Chapter 9 presents the outer bounds for the 2-user GSIC with limited-rate transmitter cooperation and weak secrecy constraints at the receivers. The difficulty in deriving these bounds lies in translating the ideas from the deterministic case to the GSIC. Three outer bounds are derived on the achievable secrecy rate in this chapter. In some of the cases, it is not possible to partition the encoded message or output as done in the case of SLDIC, and, hence, the side-information provided to the receivers is modified to obtain

analytically tractable and tight outer bounds. Finally, the achievable secrecy rates are compared with the outer bounds to illustrate the benefits of transmitter cooperation for ensuring secrecy and achieving high throughput.

A birds eye view of the thesis is shown pictorially in Fig. 1.3. In summary, this thesis studies a variety of related problems in multiuser information theory, and explores the fundamental limits of communication in each case, through the lenses of deterministic approximations and degrees of freedom characterizations. These limits are then translated to the corresponding Gaussian channels, leading to new and important insights into near-optimal transmission schemes, their corresponding performance, and fundamental limits of communications in multiuser interference-limited environments.

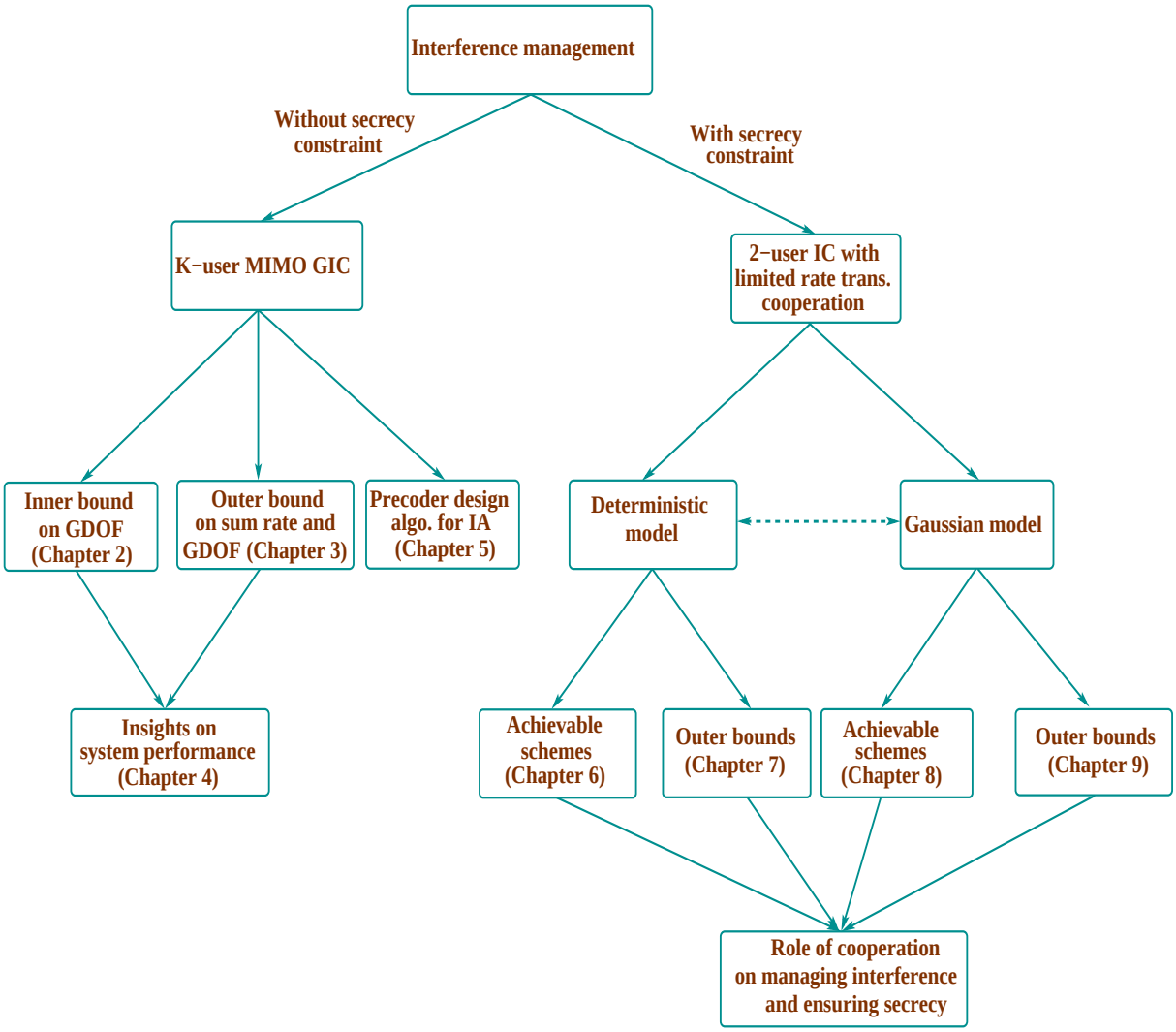


Figure 1.3: Overview of the thesis.

List of Publications from this Thesis

Journal Papers

1. **P. Mohapatra**, K. E. Nissar, and C. R. Murthy, "Interference Alignment Algorithms for the K-User Constant MIMO Interference Channel," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5499–5508, Nov. 2011.

2. **P. Mohapatra** and C. R. Murthy, "Inner Bound on the GDOF of the K-User MIMO Gaussian Symmetric Interference Channel," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 187–196, Jan. 2013.

3. **P. Mohapatra** and C. R. Murthy, "Outer Bounds on the Sum Rate of the K-User MIMO Gaussian Interference Channel," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 176–186, Jan. 2013.

4. **P. Mohapatra** and C. R. Murthy, "On the Capacity of the 2-User Interference Channel with Transmitter Cooperation and Secrecy Constraints," *submitted to IEEE Transactions on Information Theory* (Also available at: www.arxiv.org/abs/1402.5359).

Conference Papers

1. **P. Mohapatra** and C. R. Murthy, "Generalized Degrees of Freedom of the K-User Symmetric MIMO Interference Channel," *Proc. IEEE International Symposium on*

Information Theory (ISIT), St. Petersburg, Russia, Aug. 2011.

2. **P. Mohapatra** and C. R. Murthy, "Secrecy in the 2-User Symmetric Deterministic Interference Channel with Transmitter Cooperation," *Proc. IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Darmstadt, Germany, Jun. 2013. (Also accepted for Poster Presentation at the Comm. Theory Workshop, Phuket, Thailand, Jun. 2013.)

3. **P. Mohapatra** and C. R. Murthy, "Outer Bounds on the Secrecy Rate of the 2-User Symmetric Deterministic Interference Channel with Transmitter Cooperation," *Proc. IEEE National Conference on Communications (NCC)*, IIT Kanpur, India, Feb. 2014.

Chapter 2

Inner Bound on the GDOF of the K-User MIMO Gaussian Symmetric Interference Channel

Approximate capacity characterization of the interference channel has recently received considerable research attention, both as a means to analyze the capacity scaling behavior as well as to obtain guidelines for interference management in a multi-user environment. Towards this, the concept of generalized degrees of freedom (GDOF) was introduced in [8] as a means of quantifying the extent of interference management in terms of the number of interference-free signaling dimensions in a 2-user interference channel (IC). In a multiuser MIMO setup, the use of multiple antennas at the transmitters and receivers can provide additional dimensions for signaling, which can, in turn, improve the GDOF performance of the IC. Characterizing the GDOF performance of a multiuser MIMO IC is therefore an important problem, and is the focus of this chapter.

Among the different possible methods to mitigate the effect of interference, two main

approaches have typically been adopted in the literature. The first is based on the notion of splitting the message into private and public parts (also known as the Han-Kobayashi (HK) scheme) [7], [8]. The second is based on the idea of interference alignment [9, 10, 24]. These schemes are based on different ideas: the former allows part of the interference to be decoded and canceled at the unintended receivers, while the latter makes the interfering signals cast *overlapping shadows* [9] at the unintended receivers, allowing them to project the received signal in an orthogonal direction and remove the effect of interference.

The HK-scheme proposed in [7] is known to achieve the largest possible rate region for the 2-user single input single output (SISO) IC. Further, it can achieve a rate that is within 1 bit/s/Hz of the capacity of the channel for all values of the channel parameters in the case of GIC [8]. Different variants of the HK-scheme for the 2-user IC can be found in [3, 45, 46]. The concept of interference alignment (IA) originated from the work of Maddah-Ali *et al.* in [24], and was subsequently used in the DOF analysis of the X-channel in [10] and [47]. This notion of IA was crystallized by Cadambe and Jafar in [9]. Here, the precoding matrix is designed such that the interfering signals occupy a reduced dimension at all of the unintended receivers, while the desired signal remains decodable at the intended receiver. The idea of IA was extended to the K- user MIMO scenario in [14]. Other recent studies on IA include [26–28, 48, 49].

The GDOF performance of the 2-user MIMO IC was characterized in [3]. It was extended to the X-channel and the K-user SISO IC in [50] and [1], respectively. In [2], the idea of message splitting was used to derive the GDOF in a SIMO setting when $K = N + 1$, where N is the number of receive antennas at each user. However, none

of the existing studies consider the GDOF performance of the K-user MIMO Gaussian IC for $K > 2$. Moreover, the achievable GDOF performance of the HK-scheme and IA has not been contrasted in the literature. These are the main issues addressed in this chapter.

In this chapter, an inner bound on the GDOF performance is derived for the MIMO Gaussian symmetric IC (GSIC) as a combination of the HK-scheme, IA, zero forcing (ZF)-receiving, and treating interference as noise. Such a compilation of results would be useful to a system designer faced with having to make a choice between the different techniques. Together, they represent the tightest known inner bound on the GDOF performance of the K-user time-varying MIMO GSIC. In particular, the extension of the HK-scheme to K-users (where $K > 2$) is non-trivial and non-unique. Here, the GDOF performance of the HK-scheme is derived and the conditions under which it is GDOF optimal are studied. To the best of the authors' knowledge, the extension of the HK-scheme to the multiuser MIMO scenario presented here is new. Also, the interplay between the HK-scheme and IA is explored from an achievable GDOF perspective.

2.1 Preliminaries

2.1.1 System model

Consider a MIMO Gaussian IC with K transmitter-receiver pairs, with M antennas at each transmitter and N antennas at each receiver shown in Fig. 2.1. Let $\mathbf{H}_{ji}$ represent the $N \times M$ channel gain matrix from transmitter i to receiver j. The channel coefficients are assumed to be drawn from a continuous distribution such as the Gaussian

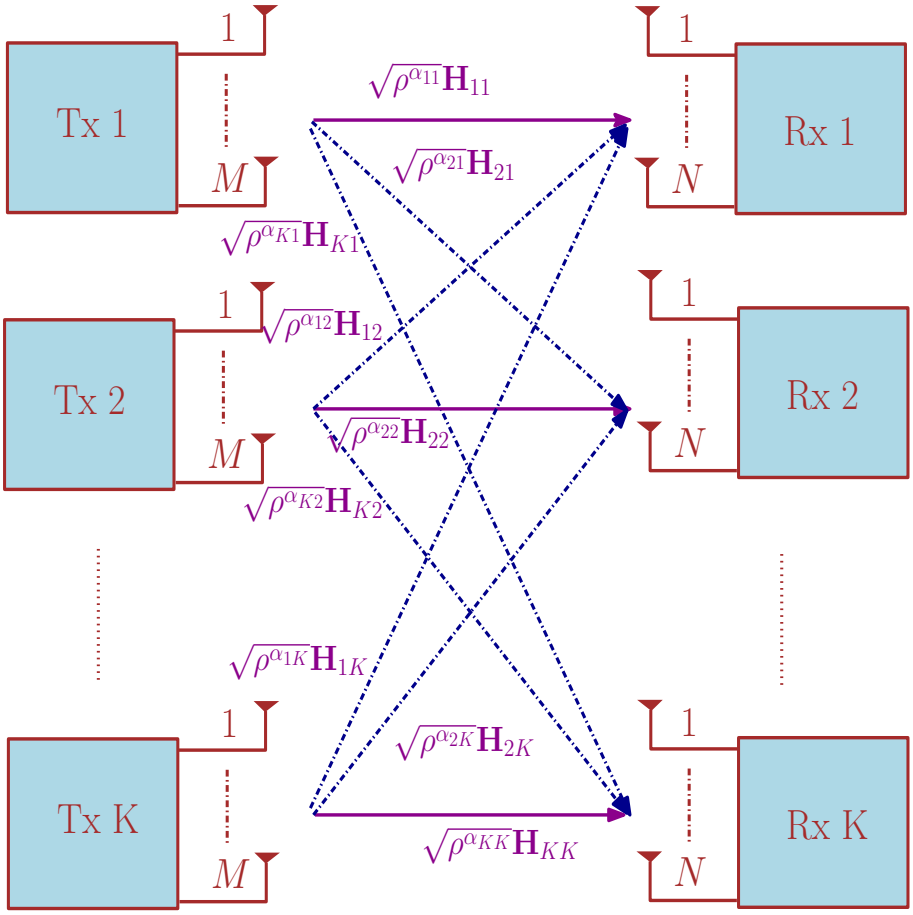


Figure 2.1: The K-user MIMO interference channel model.

distribution. The received signal at the j-th receiver, denoted $\mathbf{y}_j$, is modeled as

$$\mathbf{y}_j = \sqrt{\rho^{\alpha_{jj}}}\mathbf{H}_{jj}\mathbf{x}_j + \sum_{i=1, i\neq j}^{K} \sqrt{\rho^{\alpha_{ji}}}\mathbf{H}_{ji}\mathbf{x}_i + \mathbf{z}_j, \tag{2.1}$$

where $\mathbf{z}_j$ is the complex symmetric Gaussian noise vector, distributed as $\mathbf{z}_j \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$ and $\mathbf{x}_i$ is the signal transmitted by the i-th user, satisfying $\mathbb{E}\left\{\mathbf{x}_i^H \mathbf{x}_i\right\} = 1$. In deriving the inner bounds, it is assumed that $\mathbb{E}\left\{\mathbf{x}_i \mathbf{x}_i^H\right\}$ is full rank. The primary utility of the full rank condition is that it helps in simplifying the achievable GDOF expressions. Moreover, in many of the cases, it maximizes the achievable GDOF, because $\log\det(\cdot)$

is an increasing function on the cone of positive-definite Hermitian matrices. Also, $\rho^{\alpha_{ji}}$ represents the received signal power relative to the noise power at receiver j due to the signal from user i. In this chapter, for analytical tractability, attention is restricted to the Gaussian *Symmetric* IC (GSIC), where $\alpha_{jj} = 1$, and $\alpha_{ji} = \alpha, i \neq j$, for $i, j = 1, \ldots, K$. This assumption has been made in past work also [1–3]. Here, $\alpha > 0$ represents the ratio of the logarithm of the Interference to Noise Ratio (INR) to the logarithm of the SNR. For simplicity, it is assumed that $M \leq N$.

2.1.2 Generalized degrees of freedom

The generalized degrees of freedom (GDOF), introduced in [8], is an asymptotic quantity in the limit of high SNR and INR. For symmetric case, the per-user GDOF is defined as

$$d(\alpha) = \frac{1}{K} \lim_{\rho \to \infty} \frac{C_\Sigma(\rho, \alpha)}{\log \rho}, \tag{2.2}$$

and $C_\Sigma(\rho, \alpha)$ is the sum capacity of the K-user MIMO GSIC defined above. When $\alpha = 1$, the GDOF reduces to the degrees of freedom (DOF) defined in [14].

2.2 Inner bound

In this section, an inner bound is derived for the K-user MIMO ($M \leq N$ and $KM > N$)[1] GSIC. The main results are stated as theorems; and the proofs are provided in the Appendix. The detailed discussion and interpretation of the results is relegated to the

[1]Note that, if $KM \leq N$, one can trivially achieve the interference-free GDOF of M per user, by using a ZF receiver.

Chapter 4. For vector space IA, the channel is required to be time-varying [14]. The results for the HK-scheme, treating interference as noise and ZF-receiving are applicable in both the time-varying and the constant-channel cases.

Before stating the inner bounds, the following known results on the achievable DOF using IA and ZF-receiving are recapitulated.

2.2.1 Known results

Interference alignment

In [14], it is shown that using vector space IA, the achievable per user DOF for a K-user MIMO GSIC is

$$d_{\text{IA}} = \frac{R}{R+1} \min\{M, N\}, \text{ when } K > R, \text{ and } R \triangleq \left\lfloor \frac{\max\{M, N\}}{\min\{M, N\}} \right\rfloor. \tag{2.3}$$

Zero-forcing (ZF) receiving

The achievable DOF by ZF-receiving is given by:

$$d_{\text{ZF}} = \min\left\{M, \frac{N}{K}\right\}. \tag{2.4}$$

Note that, for vector space IA and ZF-receiving, the relative strength between the signal and interference does not matter, and hence the above DOF is achievable for all values of α. Also, vector space IA requires global channel knowledge at every node.

2.2.2 Treating interference as noise

The following theorem summarizes the GDOF obtained by treating interference as noise.

Theorem 2. *The following per user GDOF is achievable for the K-user MIMO GSIC when interference is treated as noise:*

$$d(\alpha) \geq \begin{cases} M + (N - KM)\alpha & \text{for } \frac{N}{M} < K \leq \frac{N}{M} + 1 \\ M(1-\alpha) & \text{for } K > \frac{N}{M} + 1. \end{cases} \tag{2.5}$$

Proof. See Appendix A.1. □

2.2.3 Han-Kobayashi (HK) scheme

In this section, an achievable GDOF is derived by extending the HK-scheme to the K-user MIMO GSIC. As in past work in the two-user and SIMO case [2,3,8], three different interference regimes are considered: strong, moderate, and weak interference. A key idea in the proof is to minimize the achievable GDOF per user from the common part of the message over all possible subsets of users, which does not enter into the picture in the 2-user case considered in past work. Also, the results stated in this subsection are applicable even when $\frac{N}{M}$ is not an integer.

Strong interference case $(\alpha \geq 1)$

When $\alpha \geq 1$, each receiver can decode both the unintended messages as well as the intended message. Hence, a K-user MAC channel is formed at each receiver, and the achievable rate region is the intersection of the K MAC regions obtained. This results in the following inner bound on the per user GDOF.

Theorem 3. *In the strong interference case $(\alpha \geq 1)$, the following per user GDOF is achievable*

by the HK-scheme:

$$d(\alpha) \geq \begin{cases} \min\left\{M, \frac{1}{K}\left[(K-1)M\alpha + N - (K-1)M\right]\right\} & \textit{for } \frac{N}{M} < K \leq \frac{N}{M} + 1 \\ \min\left\{M, \frac{N\alpha}{K}\right\} & \textit{for } K > \frac{N}{M} + 1. \end{cases} \tag{2.6}$$

Proof. See Appendix A.2. □

Moderate interference case $(1/2 \leq \alpha \leq 1)$

In the moderate interference regime, an achievable scheme based on HK-type message splitting is as follows. The transmitter j splits its message W_j into two sub-messages: a common message $W_{c,j}$ that is decodable at every receiver, and a private message $W_{p,j}$ that is required to be decodable only at the desired receiver. The common message is encoded using a Gaussian code book with rate $R_{c,j}$ and power $P_{c,j}$. Similarly, the private message is encoded using a Gaussian code book with rate $R_{p,j}$ and power $P_{p,j}$. Further, it is assumed that the rates are symmetric, i.e., $R_{c,j} = R_c$ and $R_{p,j} = R_p$. Also, $P_{c,j} = P_c$ and $P_{p,j} = P_p$. The powers on the private and common messages satisfy the constraint $P_c + P_p = 1$. The codewords are transmitted using superposition coding, and hence, the transmitted signal X_j is a superposition of the private message and the public message.

Similar to [3], the power in the private message is set such that it is received at the noise floor of the unintended receivers, resulting in $\text{INR}_p = 1$. Coupled with the transmit power constraint at each of the transmitters, the SNRs of the common and private parts at the desired receiver (denoted SNR_c and SNR_p) and the INRs of the common and private parts at unintended receivers (denoted INR_c and INR_p) are given by

$$\text{SNR}_c = \rho - \rho^{(1-\alpha)}, \ \ \text{SNR}_p = \rho^{(1-\alpha)}, \text{INR}_c = \rho^{\alpha} - 1, \ \text{ and } \ \text{INR}_p = 1. \tag{2.7}$$

The transmit covariance of the common message is assumed to be the same as that of the private message. The decoding order is such that the common message is decoded first, followed by the private message. While decoding the common message, all the users' private messages are treated as noise (including its own private message). The rate achievable from the private message is obtained by treating all the other users' private messages as noise.

The GDOF is contributed by both the private and public parts of the message:

$$d(\alpha) \triangleq d_p(\alpha) + d_c(\alpha), \tag{2.8}$$

where $d_p(\alpha)$ and $d_c(\alpha)$ are the GDOF contributed by the private and public parts of the message, respectively. The following theorem summarizes the per user GDOF achievable by this scheme.

Theorem 4. *In the moderate interference regime ($1/2 \leq \alpha \leq 1$), the proposed scheme achieves the following per user GDOF for the K-user MIMO GSIC*

$$d(\alpha) \geq \begin{cases} M(1-\alpha) + \min\left\{\frac{N\alpha}{K}, \frac{[M\{(2K-1)\alpha - K\} + N(1-\alpha))]}{K-1}\right\} & \text{for } \frac{N}{M} < K \leq \frac{N}{M} + 1 \\ M(1-\alpha) + \min\left\{\frac{N\alpha}{K}, \frac{[N\alpha - M(1-\alpha)]}{K-1}\right\} & \text{for } K > \frac{N}{M} + 1. \end{cases} \tag{2.9}$$

Proof. See Appendix A.3. □

Weak interference case $(0 \leq \alpha \leq 1/2)$

In this case, the received SNR and INR of the common and private messages are set the same way as in the moderate interference regime. The per user GDOF achieved is summarized in the following theorem.

Theorem 5. *In the weak interference regime* $\left(0 \leq \alpha \leq \frac{1}{2}\right)$*, the proposed scheme achieves the following per user GDOF for the* K*-user MIMO GSIC*

$$d(\alpha) \geq M(1-\alpha) + \frac{1}{K-1}(N-M)\alpha. \tag{2.10}$$

Proof. See Appendix A.4. □

Remark: The expressions for the GDOF in (2.9) and (2.10) are different because $\alpha \geq 1-\alpha$ in the former case while $\alpha \leq 1-\alpha$ the latter case, and this has been used to simplify the equations.

2.2.4 Achievable GDOF as a combination of the HK-scheme, IA, ZF-receiving and treating interference as noise

In this subsection, the performance of the various schemes considered above is consolidated in terms of the parameters α, K, M and N. Here, the channel is assumed to be time-varying in order to include IA along with the other schemes considered in this chapter. Further, to simplify the presentation, it is assumed that $\frac{N}{M}$ is an integer in Theorems 6, 7 and 8. It is straightforward to extend the result to non-integer values of $\frac{N}{M}$; however, the expressions become cumbersome with the floor of $\frac{N}{M}$ appearing in the expressions, and offer little additional insight on the achievable GDOF. In Theorem 9, the achievable GDOF for the case where $K \geq \frac{N}{M}+4$ is presented without assuming that $\frac{N}{M}$ is an integer.

Theorem 6. *The achievable per user GDOF in the strong interference case* $(\alpha \geq 1)$ *obtained by taking the maximum of all the schemes considered in this chapter is*

1. *When* $\frac{N}{M} < K \leq \frac{N}{M} + 1$,

$$d(\alpha) \geq \begin{cases} \frac{1}{K}[\alpha(K-1)M + N - (K-1)M] & \text{for } 1 \leq \alpha < \frac{M(2K-1)-N}{M(K-1)} \\ M & \text{for } \alpha \geq \frac{M(2K-1)-N}{M(K-1)}. \end{cases} \tag{2.11}$$

2. *When* $K > \frac{N}{M} + 1$,

$$d(\alpha) \geq \begin{cases} \frac{MN}{M+N} & \text{for } 1 \leq \alpha \leq \frac{KM}{M+N} \\ \frac{N\alpha}{K} & \text{for } \frac{KM}{M+N} < \alpha < \frac{KM}{N} \\ M & \text{for } \alpha \geq \frac{KM}{N}. \end{cases} \tag{2.12}$$

Proof. See Appendix A.5. □

Theorem 7. *The achievable per user GDOF in the moderate interference case* $\left(\frac{1}{2} \leq \alpha \leq 1\right)$ *obtained by taking the maximum of all the achievable schemes considered in this chapter is*

1. *When* $\frac{N}{M} < K \leq \frac{N}{M} + 1$,

$$d(\alpha) \geq \begin{cases} M(1-\alpha) + \frac{M(\alpha(2K-1)-K)+N(1-\alpha)}{K-1} & \text{for } \frac{1}{2} \leq \alpha \leq \frac{K}{2K-1} \\ M(1-\alpha) + \frac{N\alpha}{K} & \text{for } \frac{K}{2K-1} \leq \alpha \leq 1. \end{cases} \tag{2.13}$$

2. *When* $\frac{N}{M} + 1 < K \leq \frac{N}{M} + 2$,

$$d(\alpha) \geq \begin{cases} M(1-\alpha) + \frac{N\alpha - M(1-\alpha)}{K-1} & \text{for } \frac{1}{2} \leq \alpha \leq \frac{KM}{N+KM} \\ M(1-\alpha) + \frac{N\alpha}{K} & \text{for } \frac{KM}{N+KM} \leq \alpha \leq \frac{KM^2}{(M+N)(KM-N)} \\ \frac{MN}{M+N} & \text{for } \frac{KM^2}{(M+N)(KM-N)} < \alpha \leq 1. \end{cases} \tag{2.14}$$

3. *When* $K > \frac{N}{M} + 2$, $d(\alpha) \geq \frac{MN}{M+N}$.

Proof. See Appendix A.6. □

Theorem 8. *The achievable per user GDOF in the weak interference case* $\left(0 \leq \alpha \leq \frac{1}{2}\right)$ *obtained by taking the maximum of all the achievable schemes considered in this chapter is*

1. *When* $K > \frac{N}{M} + 2$,

$$d(\alpha) \geq \begin{cases} M(1-\alpha) + \frac{1}{K-1}(N-M)\alpha & \text{for } 0 \leq \alpha \leq \frac{M^2}{M(N+M)-\frac{N^2-M^2}{K-1}} \\ \frac{NM}{N+M} & \text{for } \frac{M^2}{M(N+M)-\frac{N^2-M^2}{K-1}} < \alpha \leq \frac{1}{2}. \end{cases} \tag{2.15}$$

2. *When* $\frac{N}{M} < K \leq \frac{N}{M} + 2$,

$$d(\alpha) \geq M(1-\alpha) + \frac{1}{K-1}(N-M)\alpha. \tag{2.16}$$

Proof. See Appendix A.7. □

From the expressions in the previous section, it is easy to see that the maximum of the achievable GDOF from the HK-scheme and IA outperforms the achievable GDOF from treating interference as noise or ZF-receiving for all values of M, N, K and α. The following result follows from carefully comparing the achievable GDOF from the HK-scheme and IA in the weak, moderate, and strong interference cases.

Theorem 9. *Recall that* $R \triangleq \left\lfloor \frac{N}{M} \right\rfloor$. *When* $K \geq \frac{N}{M} + 4$, *the proposed scheme for the* K*-user MIMO GSIC achieves the following per-user GDOF.*

1. *When* $R = 1$*:*

   (a) *The HK-scheme is active in the weak interference case and in the initial part of the moderate interference case, and achieves*

$$d(\alpha) \geq \begin{cases} M(1-\alpha) + \frac{(N-M)\alpha}{K-1} & \text{for } 0 \leq \alpha \leq \frac{1}{2} \\ M(1-\alpha) + \frac{N\alpha - M(1-\alpha)}{K-1} & \text{for } \frac{1}{2} < \alpha \leq \frac{(K-1)-(R+1)}{(R+1)((K-1)-\mu)}, \end{cases} \tag{2.17}$$

   where $\mu \triangleq \frac{N}{M} + 1$.

(b) IA is active in the later part of the moderate interference case and the initial part of the strong interference case, and achieves

$$d(\alpha) \geq \frac{MR}{R+1} \quad \textit{for } \frac{(K-1)-(R+1)}{(R+1)((K-1)-\mu)} < \alpha \leq \frac{MKR}{N(R+1)}.$$

(c) The HK-scheme is active in the later part of the strong interference case, and achieves

$$d(\alpha) \geq \begin{cases} \frac{N\alpha}{K} & \textit{for } \frac{MKR}{N(R+1)} < \alpha \leq \frac{MK}{N} \\ M & \textit{for } \alpha > \frac{MK}{N}. \end{cases} \tag{2.18}$$

2. When $R > 1$:

(a) The HK-scheme is active in the initial part of the weak interference case, and achieves

$$d(\alpha) \geq M(1-\alpha) + \frac{(N-M)\alpha}{K-1} \quad \textit{for } 0 \leq \alpha \leq \frac{(K-1)}{(R+1)\left(K-\frac{N}{M}\right)}.$$

(b) IA is active in the later part of the weak interference case, in the moderate interference case, and in the initial part of the strong interference case, and achieves

$$d(\alpha) \geq \frac{MR}{R+1} \quad \textit{for } \frac{(K-1)}{(R+1)\left(K-\frac{N}{M}\right)} < \alpha \leq \frac{MKR}{N(R+1)}. \tag{2.19}$$

(c) The HK-scheme is active for the later part of the strong interference case, and achieves

$$d(\alpha) \geq \begin{cases} \frac{N\alpha}{K} & \textit{for } \frac{MKR}{N(R+1)} < \alpha \leq \frac{MK}{N} \\ M & \textit{for } \alpha > \frac{MK}{N}. \end{cases} \tag{2.20}$$

Proof. See Appendix A.8. □

The above theorem is interesting because it exactly characterizes the regimes of α where the HK-scheme and IA are active for $K \geq \frac{N}{M} + 4$, even when $\frac{N}{M}$ is not an integer.

It can be used, for example, to study the effect of varying the number of transmit and receive antennas on the achievable GDOF, or the scaling of the achievable GDOF as the number of transmit and receive antennas per user is increased while keeping their ratio fixed.

2.3 Conclusions

In this chapter, a K-user MIMO GSIC was considered where each transmitter and receiver had M and N antennas, respectively. Inner bounds on the GDOF for the K-user MIMO GSIC were derived using a combination of ZF-receiving, treating interference as noise, IA, and extending the HK-scheme to K users, as a function of the number of antennas and α. Also, the relative performance of these schemes were characterized from an achievable GDOF perspective, when $K > \frac{N}{M}$ ($\frac{N}{M}$ is an integer) and $K \geq \frac{N}{M} + 4$. The usefulness of these derived bounds and their relation to the past results are discussed in Chapter 4. In the following chapter, outer bounds on the sum rate for the K-user MIMO GIC and GDOF per user for the K-user MIMO GSIC are derived.

Chapter 3

Outer Bounds on the Sum Rate of the K-User MIMO Gaussian Interference Channel

As mentioned earlier, IC is an information theoretic model where K transmitters communicate with K receivers, with each transmitter having an independent message for its corresponding receiver. Although the GIC is one of the best studied models in network information theory, its capacity region remains an open problem even in the 2-user case, except in the so-called strong interference regime [15]. Due to this, there has been an active research interest in approximately characterizing the capacity in terms of the number of interference-free signaling dimensions accessible in the GIC, also known as the generalized degrees of freedom (GDOF) [8]. The GDOF is typically characterized by deriving inner or outer bounds on the capacity, and analyzing their behavior when the INR and SNR go to infinity, but their ratio in the log-domain is held constant. In particular, outer bounds have been derived in the literature for several cases of two-user ICs and the K-user single- input single-output (SISO) IC. This chapter focuses on

developing outer bounds on the sum rate for the K-user MIMO GIC, and, using them, obtaining bounds on the GDOF in the symmetric case.

In the seminal work by Etkin, Tse, and Wang [8], the capacity of a 2-user GIC was characterized to within 1 bit/s/Hz of the capacity. The key to the characterization lies not only in devising novel achievable schemes, but also in deriving tight outer bounds. The outer bound was obtained by providing receivers with side information, and deriving outer bounds on the capacity of the resulting improved GIC. Other outer bounds for the 2-user discrete memoryless channel and GIC were presented in [51–53]. One of the bounds in [53] is obtained by using a genie to provide one of the receivers with just enough information to decode both messages. Among the 2-user sum rate outer bounds, the bounds in [8] are tightest, followed by [53], which is tighter than those in [51, 52]. Outer bounds on the sum rate and GDOF for the 2-user MIMO GIC can be found in [54] and [42], respectively. The sum rate and GDOF outer bound for the $N+1$ user single-input multiple-output (SIMO) GIC with N receive antennas at each user can be found in [2].

Past work by several researchers has provided bounds on the degrees of freedom (DOF) and GDOF for multiuser ICs (e.g., [1, 9, 14, 17, 25]). In [17], a MIMO multiple access channel (MAC) outer bound on the sum capacity of the MIMO GIC was derived, and simplified to obtain a bound on the DOF. It was also shown that zero forcing (ZF) receiving/precoding is sufficient to achieve all the available DOF. In [9], an outer bound on the DOF for the K-user SISO GSIC was presented, and the novel idea of interference alignment (IA) developed in this work was found to be DOF optimal.

Subsequently, in [14], an outer bound on the DOF for the K-user MIMO GSIC was developed, and shown to be tight when $R = \frac{\max(M,N)}{\min(M,N)}$ is an integer, where M and N are the number of transmitting and receiving antennas, respectively. The outer bound in [14] was improved in [25] by considering multiple ways of cooperation among users. The achievable scheme derived in [25] was shown to be tight when $K \geq \frac{M+N}{\gcd(M,N)}$, where $\gcd(M,N)$ denotes the greatest common divisor of M and N. Recently, some results on the GDOF of the 3-user MIMO GIC were reported in [55]. However, although several outer bounds have been derived for the DOF/GDOF, general outer bounds on the sum rate for the K-user MIMO GIC for $K > 2$ that are valid for all values of the channel parameters are not available in the existing literature. Deriving such bounds can offer important insight into the performance limits of multiuser ICs, and is therefore the focus of this chapter.

In this chapter, three new outer bounds on the sum rate are proposed, which are valid for all values of channel parameters. Further, these outer bounds are simplified to obtain outer bounds on the GDOF in the symmetric case. The overall outer bound on the GDOF is obtained by taking the minimum of the three bounds and the interference-free GDOF of $\min(M,N)$ per user. The first outer bound is based on using a combination of user cooperation similar in flavor to [25], in conjunction with providing a subset of receivers with side information. The other two outer bounds are based on providing carefully selected side information to the receivers in such a way that the the negative differential entropy terms in the sum rate bound that contain a signal component cancel out, due to which, it is possible to obtain a single letter characterization.

The three bounds on the GDOF perform differently, depending on the values of the

parameters α, M, N and K. Further, the outer bounds are compared with the inner bounds presented in Chapter 2. This, in turn, provides insights into the performance limits of different schemes for interference management. In summary, the main contributions of this chapter are:

- Three outer bounds on the sum rate are derived, presented as Theorems 10, 11 and 12. These theorems apply to all channel conditions when the channel coefficients are drawn from a continuous distribution.

- The three theorems are specialized to the MIMO GSIC to obtain outer bounds on the per user GDOF, stated as Lemmas 1, 2 and 3. To the best of the authors' knowledge, result derived here represents the tightest known outer bound on the per user GDOF of the K $(K > 2)$ user MIMO GSIC, except for some specific cases mentioned in Section 4.1.

- The scheme for providing side information employed in Theorem 11 is new. The corresponding GDOF result in Lemma 2 establishes that treating interference as noise is GDOF optimal when $M = N$ and for all K, in the weak interference regime.

- Lemmas 1 and 3 are used to establish the optimality of the achievable scheme in Chapter 2, when $\frac{N}{M} < K \leq \frac{N}{M} + 1$.

The following notation is used in this chapter. Lower case or upper case letters are used to represent scalars. Small boldface letters represent vectors, whereas capital boldface letters represent matrices. $\mathbf{x}^n = \left[\mathbf{x}_1^T, \mathbf{x}_2^T, \ldots, \mathbf{x}_n^T\right]^T$ represents a long vector consisting of the sequence of vectors $\mathbf{x}_i$, $i = 1, 2, \ldots, n$. $h(.)$ represents differential

entropy, $I(\cdot;\cdot)$ represents mutual information, $\mathbf{I}_L$ is the $L \times L$ identity matrix, and blkdiag$(\mathbf{H}_{11}, \mathbf{H}_{22}, \ldots, \mathbf{H}_{L,L})$ represents a matrix which is obtained by the block diagonal concatenation of matrices $\mathbf{H}_{11}, \mathbf{H}_{22}, \ldots, \mathbf{H}_{L,L}$.

3.1 Preliminaries

Consider a MIMO GIC with K transmitter-receiver pairs, with M_i antennas at the i-th transmitter and N_j antennas at the j-th receiver. Let $\mathbf{H}_{ji}$ represents the $N_j \times M_i$ channel gain matrix from transmitter i to receiver j. The channel coefficients are assumed to be drawn from a continuous distribution such as the Gaussian distribution. The received signal at the j-th receiver, denoted $\mathbf{y}_j$, is modeled as

$$\mathbf{y}_j = \mathbf{H}_{jj}\mathbf{x}_j + \sum_{i=1, i\neq j}^{K} \mathbf{H}_{ji}\mathbf{x}_i + \mathbf{z}_j, \tag{3.1}$$

where $\mathbf{z}_j$ is the complex symmetric Gaussian noise vector, distributed as $\mathbf{z}_j \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_j})$, and $\mathbf{x}_i$ is the signal transmitted by the i-th user, satisfying the power constraint $\mathbb{E}\left\{\mathbf{x}_i^H \mathbf{x}_i\right\} = P_i$. As in past work on the MIMO GIC, global channel state information is assumed to be available at every node. For the symmetric case considered later in the chapter, with a slight abuse of notation, $\mathbf{H}_{ji}$ $(j \neq i)$ is replaced with $\sqrt{\rho^{\alpha}}\mathbf{H}_{ji}$ and $\mathbf{H}_{jj}$ is replaced with $\sqrt{\rho}\mathbf{H}_{jj}$. The symmetric model considered here, is same as mentioned in Chapter 2.

3.2 Outer bounds

In this section, three outer bounds on the sum rate of the K-user MIMO GIC are stated as Theorems 10, 11 and 12. The bounds are general in the sense that they are valid for all values of the channel parameters. Then, the bounds are specialized to the case

of the MIMO GSIC to obtain outer bounds on the per user GDOF; these are stated as Lemmas 1, 2 and 3. Finally, the overall outer bound on the GDOF is obtained by taking the minimum of the three outer bounds and the interference free GDOF bound of $\min(M, N)$ per user.

The first outer bound is obtained by considering cooperation among subsets of users. The idea of using cooperation among users has been explored in [25] for obtaining outer bounds on the DOF of the K-user MIMO GIC. However, it turns out that cooperation by itself is not sufficient for obtaining outer bounds on the sum rate of the K-user MIMO GIC. When $\alpha \neq 1$, the symmetric assumption on the resulting 2-user GIC is no longer valid when the users are allowed to cooperate among themselves. Hence, this technique cannot be directly used to obtain an outer bound on the GDOF or the sum rate. It is necessary to provide a judiciously chosen signal as side information to a subset of the receivers in addition to cooperation, to convert the system into a MIMO Z-GIC, whose capacity cannot be worse than the original MIMO GIC. Then, an outer bound on the Z-GIC is derived. Taking the minimum of the outer bounds obtained by considering all possible combinations of cooperating users results in an outer bound on the sum rate of the MIMO GIC.

Thus, the K-user system is divided into two disjoint groups; group-1 containing L_1 $(0 \leq L_1 \leq K)$ users, and group-2 containing L_2 $(0 \leq L_2 \leq K)$ users, with $L \triangleq L_1 + L_2$ such that $0 < L \leq K$. Users not in either group are provided globally known, predetermined sequences for transmission, and hence, they play no role in the sum rate. The receivers within a given group are provided the messages of the other users in the same group, due to which, interference between users within a group is eliminated.

In group-1, all L_1 users are allowed to cooperate among themselves but they experience interference from group-2. Similarly, users in group-2 are allowed to cooperate among themselves. In group-2, all the receivers are given the messages of users $1, \ldots, L_1$ by a genie as side information. As a result, group-2 does not see any interference from the users in group-1. To simplify the equation, it is assumed that each transmitter is equipped with M antennas and each receiver is equipped with N antennas, in stating Theorem 10.

Theorem 10. *The sum rate of the K-user MIMO GIC is upper bounded as follows:*

$$\sum_{i=1}^{L} R_i \leq \log \left| \mathbf{I}_{L_1 N} + \overline{\mathbf{H}}_{11} \overline{\mathbf{P}}_1 \overline{\mathbf{H}}_{11}^H + \overline{\mathbf{H}}_{12} \overline{\mathbf{P}}_2 \overline{\mathbf{H}}_{12}^H \right| + \log \left| \mathbf{I}_{L_2 N} + \overline{\mathbf{H}}_{22} \overline{\mathbf{P}}_2^{1/2} \left\{ \mathbf{I}_{L_2 M} + \overline{\mathbf{P}}_2^{1/2} \overline{\mathbf{H}}_{12}^H \overline{\mathbf{H}}_{12} \overline{\mathbf{P}}_2^{1/2} \right\}^{-1} \overline{\mathbf{P}}_2^{1/2} \overline{\mathbf{H}}_{22}^H \right|, \tag{3.2}$$

where

$\overline{\mathbf{H}}_{11} \triangleq$ *blkdiag*$(\mathbf{H}_{11}, \ldots, \mathbf{H}_{L_1, L_1}), \overline{\mathbf{H}}_{22} \triangleq$ *blkdiag*$(\mathbf{H}_{L_1+1, L_1+1}, \ldots, \mathbf{H}_{L,L}), \overline{\mathbf{H}}_{ij} \in \mathbb{C}^{L_i N \times L_j M}$,

$\mathbf{H}_{ij} \in \mathbb{C}^{N \times M}, \overline{\mathbf{P}}_j \in \mathbb{C}^{L_j M \times L_j M}, \overline{\mathbf{P}}_1 \triangleq$ *blkdiag*$(\mathbf{P}_1, \ldots, \mathbf{P}_{L_1}), \overline{\mathbf{P}}_2 \triangleq$ *blkdiag*$(\mathbf{P}_{L_1+1}, \ldots \mathbf{P}_{L_2})$,

$\mathbf{P}_j \in \mathbb{C}^{M \times M}$: *input covariance matrix of* $j^{th} (j = 1, 2)$ *user,* $L_1 + L_2 \triangleq L \leq K$,

$0 < L_1, L_2 \leq K$, *and* $\overline{\mathbf{H}}_{12} \triangleq \begin{bmatrix} \mathbf{H}_{1,L_1+1} & \mathbf{H}_{1,L_1+2} & \cdots & \mathbf{H}_{1,L} \\ & \vdots & \vdots & \\ \mathbf{H}_{L_1,L_1+1} & \mathbf{H}_{L_1,L_1+2} & \cdots & \mathbf{H}_{L_1,L} \end{bmatrix}$.

Proof. See Appendix B.1. □

Recall that, in order to obtain (3.2), L_1 and L_2 users are allowed to cooperate in groups-1 and 2, respectively. There are $3^K - 1$ ways of choosing the user groups for cooperation. Hence, the minimum sum rate obtained out of all possible ways of cooperation leads to the tightest outer bound on the sum rate obtainable from this method. Since the users

have different power constraints and users see different SNRs and INRs, obtaining a closed-form outer bound becomes a formidable task. However, for the symmetric case, a simplified solution exists, as given by the following Lemma.

Lemma 1. *In the symmetric case, the upper bound of Theorem 10 can be expressed as an upper bound on the per user GDOF as follows:*

1. *When* $M \leq N$,

$$d(\alpha) \leq \min_{L_1,L_2} \begin{cases} \frac{1}{L}\left[L_1 M + \min\left\{r, L_1(N-M)\right\}\alpha + L_r \right. \\ \qquad \left. + \min\left\{r, L_2 N - L_r\right\}(1-\alpha)\right] & \textit{for } 0 \leq \alpha \leq 1 \\ \frac{1}{L}\left[r\alpha + \min\left\{L_1 M, L_1 N - r\right\} + L_r\right] & \textit{for } \alpha > 1. \end{cases}$$

2. *When* $M > N$,

$$d(\alpha) \leq \min_{L_1,L_2} \begin{cases} \frac{1}{L}[L_1 N + L^{'} + \min\{L^{'}, L_2 N - L^{'}\}(1-\alpha)] & \textit{for } 0 \leq \alpha \leq 1 \\ \frac{1}{L}[L_1 N + r(\alpha - 1) + L^{'}] & \textit{for } \alpha > 1, \end{cases}$$

where $r \triangleq \min\left\{L_2 M, L_1 N\right\}, L_r \triangleq L_2 M - r, L^{'} \triangleq \min\left\{L_2 N, L_r\right\}, 0 \leq L_1, L_2 \leq K$, *and* $L_1 + L_2 \triangleq L \leq K$.

Proof. See Appendix B.2. □

The result below provides another outer bound on the sum rate, by providing side information in the form of a noisy version of the intended message at the receivers. To the best of the authors' knowledge, the scheme for providing side information employed here is new. It leads to the tightest known bounds for some parameter values as mentioned in Theorem 13. Let $\mathbf{s}_{j,\mathcal{B}} \triangleq \sum_{i \in \mathcal{B}} \mathbf{H}_{ji}\mathbf{x}_i + \mathbf{z}_j$, where $\mathcal{B} \subseteq \{1, 2, \ldots, K\}$ is a subset users. Then, user 1 is provided $\mathbf{s}_{2,1}$ and user K is provided $\mathbf{s}_{K-1,K}$. Users $i = 2, 3, \ldots, K-1$ are provided $\mathbf{s}_{i-1,i}$ and $\mathbf{s}_{i+1,i}$ in succession to obtain two sets of rate bounds. It turns

out that, by doing so, all the negative differential entropy terms containing a signal component cancel out, leading to the outer bound given by Theorem 11 below. Further remarks on the choice of side information are offered in Chapter 4.

Theorem 11. *For the K-user MIMO GIC, the following rate bound is applicable:*

$$R_s \leq \sum_{i=1}^{K-1} \log \left| \mathbf{I}_{N_i} + \sum_{j=1,\, j\neq i}^{K} \boldsymbol{\phi}_{i,j} + \boldsymbol{\psi}_{i,i+1} \right| + \sum_{i=2}^{K} \log \left| \mathbf{I}_{N_i} + \sum_{j=1,\, j\neq i}^{K} \boldsymbol{\phi}_{i,j} + \boldsymbol{\psi}_{i,i-1} \right|, \tag{3.3}$$

where $R_s \triangleq R_1 + 2\sum_{i=2}^{K-1} R_i + R_K$, $\boldsymbol{\psi}_{i,j} \triangleq \mathbf{H}_{ii}\mathbf{P}_i^{1/2}(\mathbf{I}_{M_i} + \mathbf{P}_i^{1/2}\mathbf{H}_{ij}^H\mathbf{H}_{ij}\mathbf{P}_i^{1/2})^{-1}\mathbf{P}_i^{1/2}\mathbf{H}_{ii}^H$, *and* $\boldsymbol{\phi}_{i,j} \triangleq \mathbf{H}_{ij}\mathbf{P}_j\mathbf{H}_{ij}^H$.

Proof. See Appendix B.3. □

Remark: Note that the above theorem presents a bound on $R_1 + 2\sum_{i=2}^{K-1} R_i + R_K$, rather than on the sum rate, i.e., $\sum_{i=1}^{K} R_i$. Clearly, one can obtain $\frac{K(K-1)}{2}$ inequalities of the form (3.3), for each possible choice of the first and K^{th} user. Bounds on the sum rate can then be obtained from the above by summing all such inequalities and dividing by $\frac{3K(K-1)}{2}$.

Lemma 2. *In the symmetric case, the upper bound of Theorem 11 can be reduced to the following per user GDOF upper bound:*

$$d(\alpha) \leq \begin{cases} r_{\min}(1-\alpha) + \min\{r', r_{\max} - r_{\min}\}\alpha & \text{for } 0 \leq \alpha \leq \dfrac{1}{2} \\ r'\alpha + \min\{r_{\min}, r_{\max} - r'\}(1-\alpha) & \text{for } \dfrac{1}{2} \leq \alpha \leq 1, \end{cases} \tag{3.4}$$

where $r_{\min} \triangleq \min\{M, N\}$, $r_{\max} \triangleq \max\{M, N\}$, *and* $r' \triangleq \min\{N, (K-1)M\}$.

Proof. See Appendix B.4. □

Theorem 12. *For the K-user MIMO GIC, the following rate bound is applicable:*

$$R_s \leq \log\left|\mathbf{I}_{N_1} + \sum_{j=1,\, j\neq i}^{K} \boldsymbol{\phi}_{1,j} + \boldsymbol{\psi}_{1,K}\right| + \sum_{i=2}^{K-1} \log\left|\mathbf{I}_{N_i} + \overline{\mathbf{H}}_{i1}\overline{\mathbf{P}}_{i1}^{1/2}\left\{\mathbf{I}_{M_{r_i}} + \overline{\mathbf{P}}_{i1}^{1/2}\overline{\mathbf{H}}_{Ki}^{H}\overline{\mathbf{H}}_{Ki}\overline{\mathbf{P}}_{i1}^{1/2}\right\}^{-1}\right.$$
$$\left.\overline{\mathbf{P}}_{i1}^{1/2}\overline{\mathbf{H}}_{i1}^{H} + \overline{\mathbf{H}}_{i,i+1}\overline{\mathbf{P}}_{i2}^{1/2}\left\{\mathbf{I}_{M_{s_i}} + \overline{\mathbf{P}}_{i2}^{1/2}\overline{\mathbf{H}}_{1,i+1}^{H}\overline{\mathbf{H}}_{1,i+1}\overline{\mathbf{P}}_{i2}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i2}^{1/2}\overline{\mathbf{H}}_{i,i+1}^{H}\right|$$
$$+ \sum_{i=2}^{K-1} \log\left|\mathbf{I}_{N_i} + \overline{\mathbf{H}}_{iK}\overline{\mathbf{P}}_{i3}^{1/2}\left\{\mathbf{I}_{M'_{r_i}} + \overline{\mathbf{P}}_{i3}^{1/2}\overline{\mathbf{H}}_{1i}^{H}\overline{\mathbf{H}}_{1i}\overline{\mathbf{P}}_{i3}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i3}^{1/2}\overline{\mathbf{H}}_{iK}^{H} + \overline{\mathbf{H}}_{i,K-1}\overline{\mathbf{P}}_{i4}^{1/2}\right.$$
$$\left.\left\{\mathbf{I}_{M'_{s_i}} + \overline{\mathbf{P}}_{i4}^{1/2}\overline{\mathbf{H}}_{K,i+1}^{H}\overline{\mathbf{H}}_{K,i+1}\overline{\mathbf{P}}_{i4}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i4}^{1/2}\overline{\mathbf{H}}_{i,K-1}^{H}\right| + \log\left|\mathbf{I}_{N_K} + \sum_{j=1}^{K-1}\boldsymbol{\phi}_{K,j} + \boldsymbol{\psi}_{K,1}\right|, \tag{3.5}$$

where

$$\overline{\mathbf{H}}_{i1} \triangleq [\mathbf{H}_{i1}\, \mathbf{H}_{i2} \ldots \mathbf{H}_{ii}]\,, \overline{\mathbf{H}}_{i,i+1} \triangleq [\mathbf{H}_{i,i+1}\, \mathbf{H}_{i,i+2} \ldots \mathbf{H}_{iK}]\,, \overline{\mathbf{H}}_{Ki} \triangleq [\mathbf{H}_{K1}\, \mathbf{H}_{K2} \ldots \mathbf{H}_{Ki}]\,,$$

$$\overline{\mathbf{H}}_{1,i+1} \triangleq [\mathbf{H}_{1,i+1}\, \mathbf{H}_{1,i+2} \ldots \mathbf{H}_{1K}]\,, \overline{\mathbf{H}}_{1i} \triangleq [\mathbf{H}_{1K}\, \mathbf{H}_{12} \ldots \mathbf{H}_{1i}]\,, \overline{\mathbf{H}}_{iK} \triangleq [\mathbf{H}_{iK}\, \mathbf{H}_{i2} \ldots \mathbf{H}_{ii}]\,,$$

$$\overline{\mathbf{H}}_{K,i+1} \triangleq [\mathbf{H}_{K1}\, \mathbf{H}_{K,i+1} \ldots \mathbf{H}_{K,K-1}]\,, \overline{\mathbf{H}}_{i,K-1} \triangleq [\mathbf{H}_{i1}\mathbf{H}_{i,i+1} \ldots \mathbf{H}_{i,K-1}]\,,$$

$$\overline{\mathbf{P}}_{i1} \triangleq \textit{blkdiag}\,(\mathbf{P}_1\, \mathbf{P}_2 \ldots \mathbf{P}_i)\,, \overline{\mathbf{P}}_{i2} \triangleq \textit{blkdiag}\,(\mathbf{P}_{i+2}\, \mathbf{P}_{i+3} \ldots \mathbf{P}_K)\,, \overline{\mathbf{P}}_{i3} \triangleq \textit{blkdiag}\,(\mathbf{P}_K\, \mathbf{P}_2$$
$$\ldots \mathbf{P}_i)\,, \overline{\mathbf{P}}_{i4} \triangleq \textit{blkdiag}\,(\mathbf{P}_1\, \mathbf{P}_{i+1}\, \ldots\, \mathbf{P}_{K-1})\,, M_{r_i} \triangleq \sum_{j=1}^{i} M_j, M_{s_i} \triangleq \sum_{j=i+1}^{K} M_j,$$
$$M'_{r_i} \triangleq \sum_{j=2}^{i} M_j + M_K,\;\; M'_{s_i} \triangleq M_1 + \sum_{j=i+1}^{K-1} M_j, R_s \triangleq R_1 + 2\sum_{i=2}^{K-1} R_i + R_K, \boldsymbol{\phi}_{i,j} \triangleq \mathbf{H}_{ij}\mathbf{P}_j\mathbf{H}_{ij}^{H},$$
$$\textit{and } \boldsymbol{\psi}_{i,j} \triangleq \mathbf{H}_{ii}\mathbf{P}_i^{1/2}(\mathbf{I}_{M_i} + \mathbf{P}_i^{1/2}\mathbf{H}_{ij}^{H}\mathbf{H}_{ij}\mathbf{P}_i^{1/2})^{-1}\mathbf{P}_i^{1/2}\mathbf{H}_{ii}^{H}. \tag{3.6}$$

Proof. See Appendix B.5. □

Remark: A bound on the sum rate ($\sum_{i=1}^{K} R_i$) can be obtained in a similar manner as in Theorem 11.

The above result can be used to obtain an outer bound of the GDOF of the K-user MIMO GSIC only for $\frac{N}{M} < K \leq \frac{N}{M} + 1$, because the form of the above outer bound

results in rank deficient matrices when $K > \frac{N}{M} + 1$, which make finding the inverse and computing the GDOF analytically intractable.

Lemma 3. *In the symmetric case, when $\frac{N}{M} < K \leq \frac{N}{M} + 1$, the sum rate upper bound of Theorem 12 can be expressed as an upper bound on the per user GDOF as follows:*

$$d(\alpha) \leq \begin{cases} M(1-\alpha) + \frac{1}{K-1}(N-M)\alpha & \text{for } 0 \leq \alpha \leq \frac{1}{2} \\ M\alpha + \frac{1}{K-1}(N-M)(1-\alpha) & \text{for } \frac{1}{2} \leq \alpha \leq 1. \end{cases} \tag{3.7}$$

Proof. See Appendix B.6. □

The overall outer bound is obtained by taking minimum of the outer bounds in Lemmas 1, 2 and 3. Due to minimization involved in Lemma 1, analytical characterization of the outer bound is not possible in all cases. However, in Theorem 13 below, an expression for the combined outer bound is obtained when $K \geq N + M$ and $\frac{N}{M} < K \leq \frac{N}{M} + 1$. Also, a unified expression is presented for case $\frac{N}{M} + 1 < K < M + N$, when $\frac{N}{M}$ is integer-valued. In stating the theorem, three interference regimes are considered, as in the past work [2, 3, 8]. The result follows by first analytically solving the minimization in Lemma 1 and then carefully comparing the three outer bounds to determine which bound is tightest for different K, M, N and α.

Theorem 13. *The outer bound on the per user GDOF of the K-user MIMO $(M \leq N)$ GSIC, obtained by taking the minimum of the outer bounds derived in this chapter, is*

1. *When $(K \geq M + N)$ or $(\frac{N}{M} + 1 < K < M + N$, where $\frac{N}{M}$ is an integer):*

   (a) *Weak interference regime $(0 \leq \alpha \leq \frac{1}{2})$: When $MN < N^2 - M^2$, Lemma 1 is active,*

otherwise Lemma 2 is active, and the outer bound is of the following form:

$$d(\alpha) \leq \begin{cases} M - \frac{M^2\alpha}{M+N} & \text{for } MN < N^2 - M^2 \\ M(1-\alpha) + (N-M)\alpha & \text{for } MN \geq N^2 - M^2. \end{cases} \tag{3.8}$$

(b) Moderate interference regime ($\frac{1}{2} \leq \alpha \leq 1$)*:*

i. When $MN < N^2 - M^2$*, Lemma 1 is active, and the outer bound is of the following form:*

$$d(\alpha) \leq M - \frac{M^2\alpha}{M+N}. \tag{3.9}$$

ii. When $MN \geq N^2 - M^2$*, Lemma 2 is active for* $\frac{1}{2} \leq \alpha \leq \frac{M(M+N)}{N(M+N)+M^2}$*, whereas Lemma 1 is active for* $\frac{M(M+N)}{N(M+N)+M^2} < \alpha \leq 1$*, and the outer bound becomes*

$$d(\alpha) \leq \begin{cases} N\alpha & \text{for } \frac{1}{2} \leq \alpha \leq \frac{M(M+N)}{N(M+N)+M^2} \\ M - \frac{M^2\alpha}{M+N} & \text{for } \frac{M(M+N)}{N(M+N)+M^2} < \alpha \leq 1. \end{cases} \tag{3.10}$$

(c) High interference regime ($\alpha \geq 1$)*: In this case, Lemma 1 is active and the outer bound is of the following form:*

$$d(\alpha) \leq \begin{cases} \frac{MN\alpha}{M+N} & \text{for } 1 \leq \alpha \leq \frac{M+N}{N} \\ M & \text{for } \alpha > \frac{M+N}{N}. \end{cases} \tag{3.11}$$

2. When $\frac{N}{M} < K \leq \frac{N}{M} + 1$*:*

(a) Weak interference regime ($0 \leq \alpha \leq \frac{1}{2}$)*: In this case, Lemma 3 is active and the outer bound is of the following form:*

$$d(\alpha) \leq M(1-\alpha) + \frac{1}{K-1}(N-M)\alpha. \tag{3.12}$$

(b) Moderate interference regime ($\frac{1}{2} \leq \alpha \leq 1$)*: Lemma 3 is active for* $\frac{1}{2} \leq \alpha \leq \frac{K}{2K-1}$*,*

and Lemma 1 is active for $\frac{K}{2K-1} < \alpha \leq 1$. *The outer bound becomes*

$$d(\alpha) \leq \begin{cases} M\alpha + \frac{1}{K-1}(N-M)(1-\alpha) & \text{for } \frac{1}{2} \leq \alpha \leq \frac{K}{2K-1} \\ M(1-\alpha) + \frac{N\alpha}{K} & \text{for } \frac{K}{2K-1} < \alpha \leq 1. \end{cases} \tag{3.13}$$

(c) *High interference regime* ($\alpha \geq 1$)*: In this case, Lemma 1 is active and the outer bound is of the following form:*

$$d(\alpha) \leq \begin{cases} \frac{1}{K}\left[N + (K-1)M(\alpha-1)\right] & \text{for } 1 \leq \alpha \leq \frac{2KM-(M+N)}{(K-1)M} \\ M & \text{for } \alpha \geq \frac{2KM-(M+N)}{(K-1)M}. \end{cases} \tag{3.14}$$

Proof. See Appendix B.7. □

3.3 Conclusions

This chapter derived outer bounds on the sum rate of the K-user MIMO GIC. The outer bounds were simplified for the MIMO GSIC to obtain the GDOF as a function of $\alpha = \log \text{INR} / \log \text{SNR}$. The outer bound was obtained by taking the minimum of three bounds, one of the bounds being derived using the notion of cooperation and providing side information, and the other two based on providing carefully selected partial side information at the receivers. The novelty of the derivation lies in the careful selection of the side information, which results in the negative differential entropy terms containing signal components canceling out from the sum rate bounds. The usefulness of these outer bounds and their relation to the past results are discussed from a GDOF perspective in the next chapter.

Chapter 4

Discussion on the Bounds on the GDOF for the K-User MIMO GSIC

In this chapter, the proposed achievable schemes in Chapter 2 are compared with the outer bounds on the per user GDOF derived in the previous chapter. For example, in the weak interference regime ($0 \leq \alpha \leq \frac{1}{2}$), when $M = N$, the outer bound in Theorem 11 that provides each receiver with a noisy version of the interference caused by only one unintended transmitter is the tightest, and its GDOF coincides with that of the achievable scheme where each receiver treats interference as noise. Hence, treating interference as noise is GDOF optimal in the weak interference regime. When $\frac{N}{M} < K \leq \frac{N}{M} + 1$, the outer bound coincides with the inner bound for all values of α. This indicates that decoding part of the interference as in the Han-Kobayashi (HK) scheme ([7, 8]) is optimal for this range of K; and how much of interference to decode depends on the interference level. This, in turn, provides insights into the performance limits of different schemes for interference management. Note that all the comparisons are against the special case of the HK-scheme where the interference is leveled against noise.

The results also bring out the improvement in the achievable GDOF that can be obtained by adding antennas at the transmitters or receivers and can be used to answer questions related to the allocation of antennas between the transmitters and receivers to maximize the achievable GDOF. For example, when $K > \frac{N}{M} + 1$, neither the HK-scheme nor IA can uniformly outperform the other; which scheme is the better of the two depends on the $\log \text{INR}/\log \text{SNR}$ level and the values of M, N and K. In particular, these insights do not follow from past work on the 2-user SISO/MIMO [3, 8] or the K-user SISO/SIMO [1, 2] cases. Also, relation of the derived bounds with past results are discussed in this chapter.

4.1 Comparison with existing results

Some observations on how the bounds on the GDOF derived in Chapters 2 and 3 in relation to existing work are as follows:

1. When $M = 1$ and $K = N + 1$, the HK-scheme in Section 2.2.3 in Chapter 2 and the outer bound in Lemma 3 in Chapter 3 reduce to the corresponding SIMO GDOF result in [2] (see Fig. 4.1 and 4.2).

2. When $K = 2$, the inner bound derived in Section 2.2.3 in Chapter 2 and the outer bound in Chapter 3 reduce to the corresponding 2-user symmetric GDOF result in [3].

3. When $M = N = 1$ and $K = 2$, the inner bound in Section 2.2.3 in Chapter 2 and the outer bound in Chapter 3 reduce to the corresponding GDOF result for the symmetric case in [8] (see Fig. 4.1 and 4.2).

4. When $M = N = 1$, the inner bound matches with the result in [1] only in the weak interference regime. In [1], under the SISO constant channel setting, a higher GDOF is achieved using multi-level coding with a nested lattice structure. However, the outer bound derived in chapter 3 reduces to the K-user SISO GSIC GDOF result in [1].

5. When $\alpha = 1$, the cooperative outer bound of Lemma 1 matches with the DOF outer bound in [25] for many cases of K, M and N (e.g., $K = 3, M = 2, N = 5$). Theorem 1 uses genie-aided message sharing in addition to cooperation, to handle the $\alpha \neq 1$ cases. The bound in [25] only requires cooperation, due to which it is lower for some values of M, N and K. Hence, when $\alpha = 1$, the minimum of the outer bound derived here and the one in [25] is plotted in the graphs presented in the next subsection. The outer bound derived here does not match with the DOF-optimal outer bound in [56] for the $K = 3$ and $\frac{N}{M} + 1 < K \leq \frac{M+N}{\text{gcd}(M,N)}$ case. The outer bound in [56] uses the concept of subspace alignment chains to identify the extra dimension to be provided by a genie to a receiver, which does not easily generalize to arbitrary K, M, N and α.

6. When $K = 2$, the outer bound in Lemma 1 reduces to the DOF outer bound on MIMO Z-GIC in [57].

In Figs. 4.1 and 4.2, the inner bound and outer bound derived in previous chapters are compared with some of the existing results mentioned above. In Fig. 4.1, the achievable per-user GDOF is plotted against α for the $K = 3$ user GSIC with various antenna configurations and compared with existing results. The inner bound derived in Chapter 2 is compared with the result in [1] for the SISO GSIC case and with the result in [2]

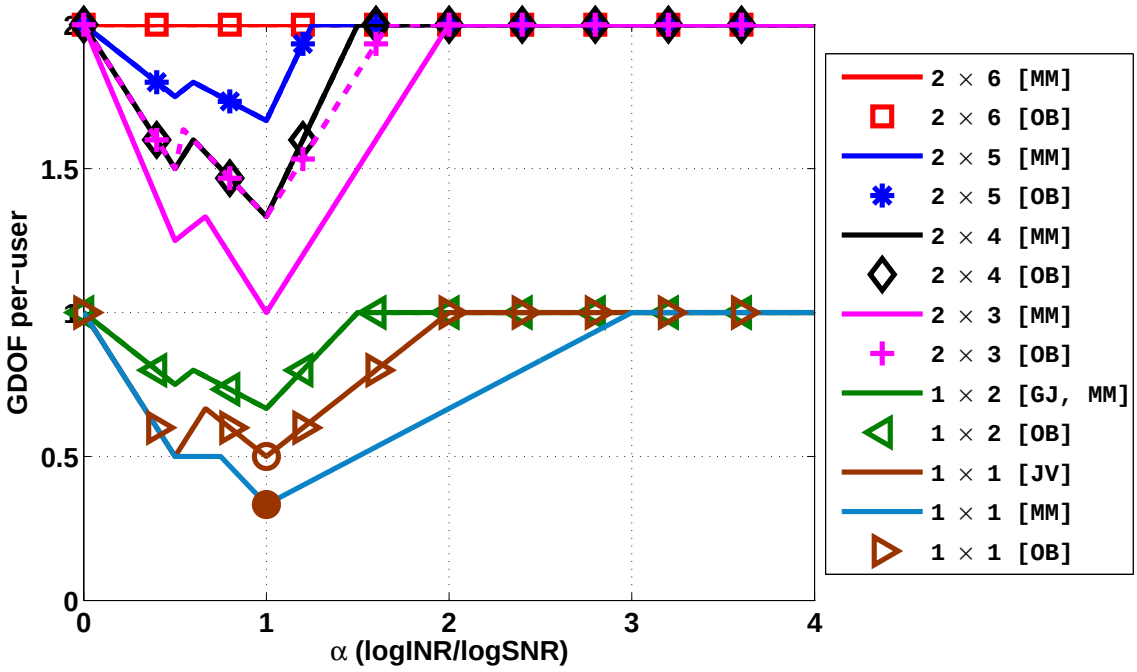


Figure 4.1: The achievable GDOF for the $K = 3$ user GSIC with different antenna configurations. In the legend, MM stands for inner bound derived in Chapter 2, JV stands for the achievable GDOF in [1], GJ stands for the achievable GDOF in [2], and OB stands for the outer bound derived in Chapter 3.

for the SIMO GSIC with $K = N + 1$. Since the achievable GDOF in [1] is discontinuous at $\alpha = 1$, it is represented by the filled circle in the plot. Note that the scheme in [1] assumes that the channel remains constant over time. Hence, the performance of IA is not included in the comparison. Further, the achievable GDOF is plotted for the $2 \times 3, 2 \times 4, 2 \times 5$ and $2\ times6$ antenna configurations. Also, the outer bound derived in Chapter 3 is plotted for these antenna configurations to verify the optimality of the inner bound.

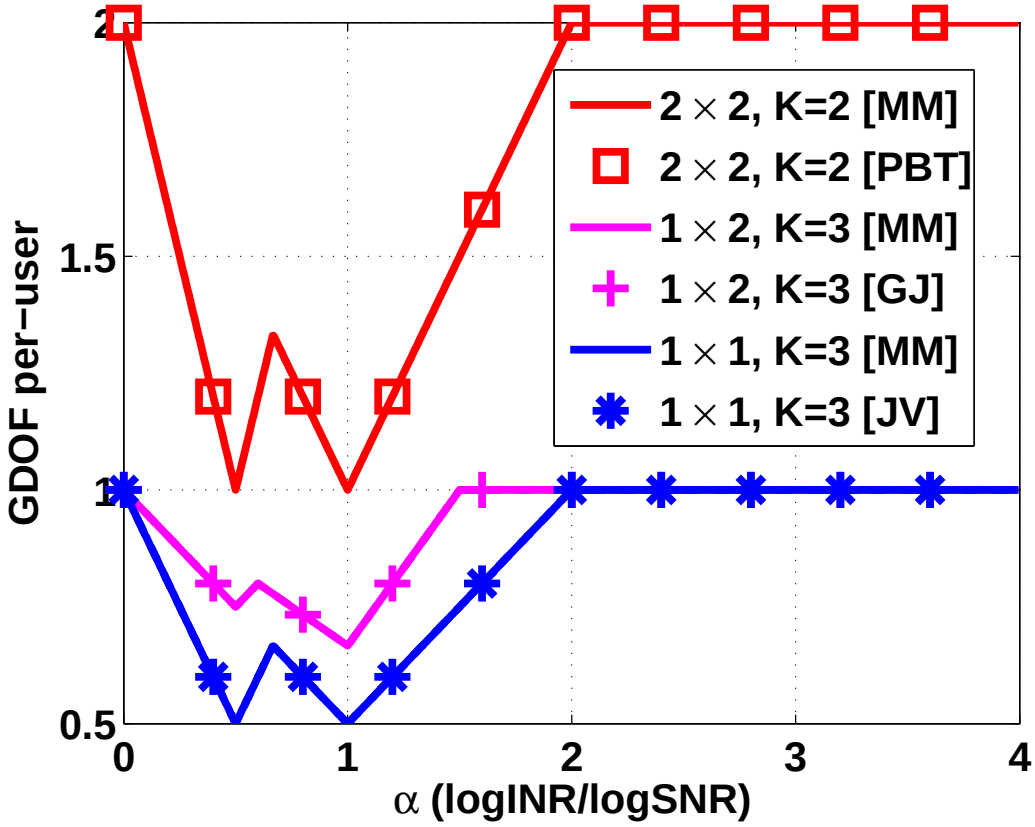


Figure 4.2: Outer bound on per user GDOF for MIMO GSIC with different antenna configuration and number of users. In the legend, MM stands for the outer bound derived in Chapter 3, PBT stands for the outer bound on GDOF in [3], GJ stands for the outer bound on GDOF in [2], and JV stands for the outer bound on GDOF in [1].

4.2 Numerical examples

Now, some numerical examples are considered to get better insight into the bounds for various values of K, M, N, and α. The channel is assumed to be time-varying since IA is considered, except for Fig. 4.1, which considers a constant channel to facilitate comparison with past work.

In Fig. 4.3, the outer bounds on the per user GDOF in Lemmas 1, 2 and 3 are contrasted as a function α, for $(M, N) = (2, 2)$ and $(2, 4)$. When $K = 3$ and $(M, N) = (2, 2)$,

the outer bound in Lemma 2 is active in the weak interference regime and the initial part of the moderate interference regime. The outer bound in Lemma 1 is not tight in this regime, as a result of the genie giving too much information to the receiver. As the interference level increases, it is necessary to provide the unintended message completely as in Theorem 10 to obtain a tractable outer bound; and hence Lemma 1 is active in the later part of the moderate interference regime and the high interference regime. As the number of receive dimensions increases $(N = 4)$, the outer bound in Lemma 2 is found to be loose. Hence, another outer bound is derived, where a carefully chosen part of the interference is provided as side information to the receiver, as in Theorem 12. The corresponding GDOF outer bound in Lemma 3 is tight in the weak interference regime $(0 \leq \alpha \leq \frac{1}{2})$ and in the initial part of the moderate interference regime $(\frac{1}{2} \leq \alpha \leq \frac{3}{5})$. For $\alpha > \frac{3}{5}$, the outer bound in Lemma 1 is active, as in the previous case.

Figure 4.1 illustrates the benefits of having additional antennas at the transmitter and receiver in improving the achievable GDOF. For the SISO GSIC, the proposed inner bound matches with the result in [1] in the weak interference case. There exists a gap between the two schemes in the moderate interference case and in the initial part of the strong interference case, as noted in the previous subsection. For the SIMO case, the achievable GDOF of the proposed scheme matches with that of the scheme in [2] and is also GDOF optimal. As receive antennas are added, in the strong interference regime, the HK-scheme achieves the interference-free GDOF at a smaller value of α. In the 2×6 system, as $N = KM$, ZF-receiving achieves the interference free GDOF for all values of α. Finally, note that the inner bound is GDOF optimal for the 2×4, 2×5 and 2×6

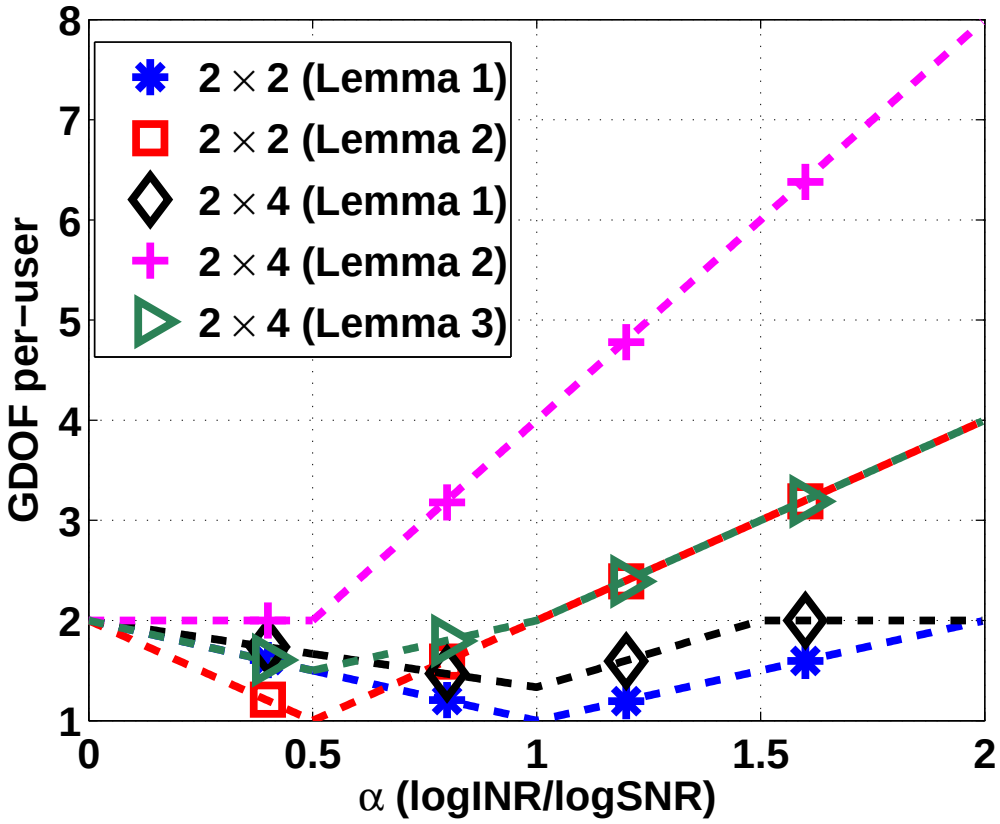


Figure 4.3: Comparison of the different outer bounds on per user GDOF for the $K = 3$ user GSIC with $(M, N) = (2, 2)$ and $(2, 4)$.

MIMO GSIC cases.

In Fig. 4.4, the per user GDOF is plotted against α for $K = 3$ and $M = N = 2$. In the weak interference regime, treating interference as noise coincides with the outer bound in Chapter 3. In this case, treating interference as noise performs as well as the HK-scheme. IA is seen to be GDOF optimal at $\alpha = 1/2$ and 1. In the strong interference regime, IA initially performs the best, and as α increases, the HK-scheme performs the best, and finally achieves the interference free GDOF. There exists a gap between the inner and outer bounds in the moderate and strong interference regimes.

In Figs. 4.5 and 4.6, the outer bound on the per user GDOF is plotted against α for

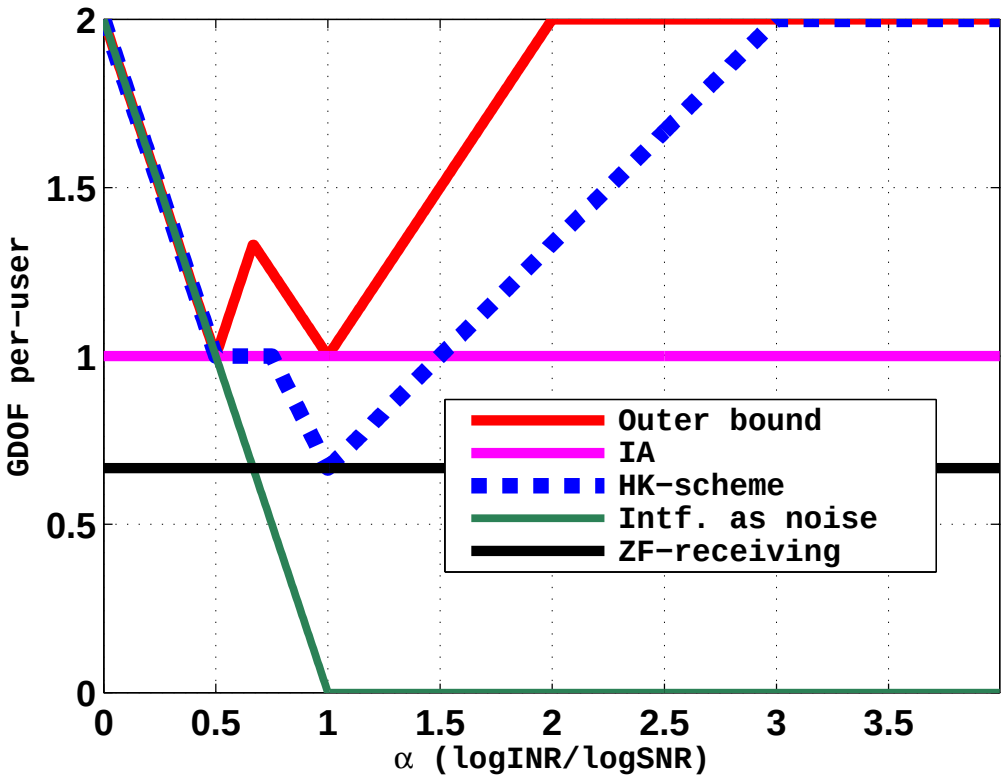


Figure 4.4: The achievable GDOF for the $K = 3$ user GSIC with $M = N = 2$. The figure shows the achievable GDOF by IA (curve labeled as `IA`), the HK-scheme (curve labeled as `HK-scheme`), treating interference as noise (curve labeled as `Intf. as noise`) and ZF-receiving (curve labeled as `ZF-receiving`), along with the outer bound (curve labeled as `Outer bound`).

$K = 3$ and 4, respectively, and for various values of M and N. The outer bound is compared with the inner bound on the per user GDOF. In the high interference regime, the outer bound increases linearly with α until it saturates at $\min(M, N)$. Such a behavior is exhibited by the achievable scheme based on decoding the interference. As α increases, more and more of the interference becomes decodable, until it achieves the interference free GDOF. Hence, decoding the interference may be necessary to obtain optimal performance in high interference regime. In the moderate interference case, there is a gap between the inner bound and the outer bound, when $(M, N) = (2, 2)$ and $(3, 6)$. The

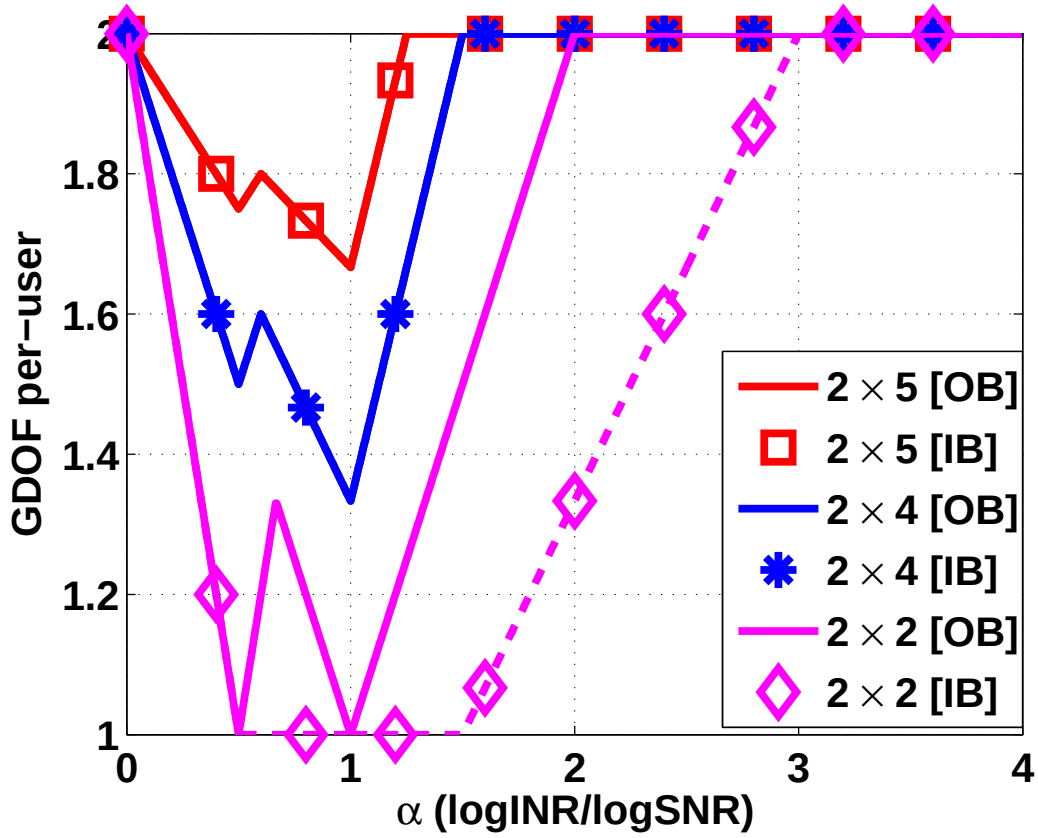


Figure 4.5: Outer bound (OB) and inner bound (IB) on the per user GDOF for $K = 3$ user MIMO GSIC with different antenna configurations.

best achievable scheme is based on IA, and is known to be optimal at $\alpha = 1$ [14] when $\frac{N}{M}$ is an integer. For other regimes of α, it may be useful to employ an HK-type scheme ([7, 8]) where the message is split into private and public parts. On the other hand, in the weak interference regime, treating interference as noise is GDOF optimal when $(M, N) = (2, 2)$. Hence, in this regime, the achievable GDOF decreases as α increases. The figures also show several cases, e.g., $(M, N) = (2, 4), (2, 5)$ and $(3, 10)$, where the inner and outer bounds match.

In Figs. 4.7 and 4.8, the per user achievable GDOF performance is compared for different antenna configurations with a total of 7 and 10 antennas per user pair, respectively.

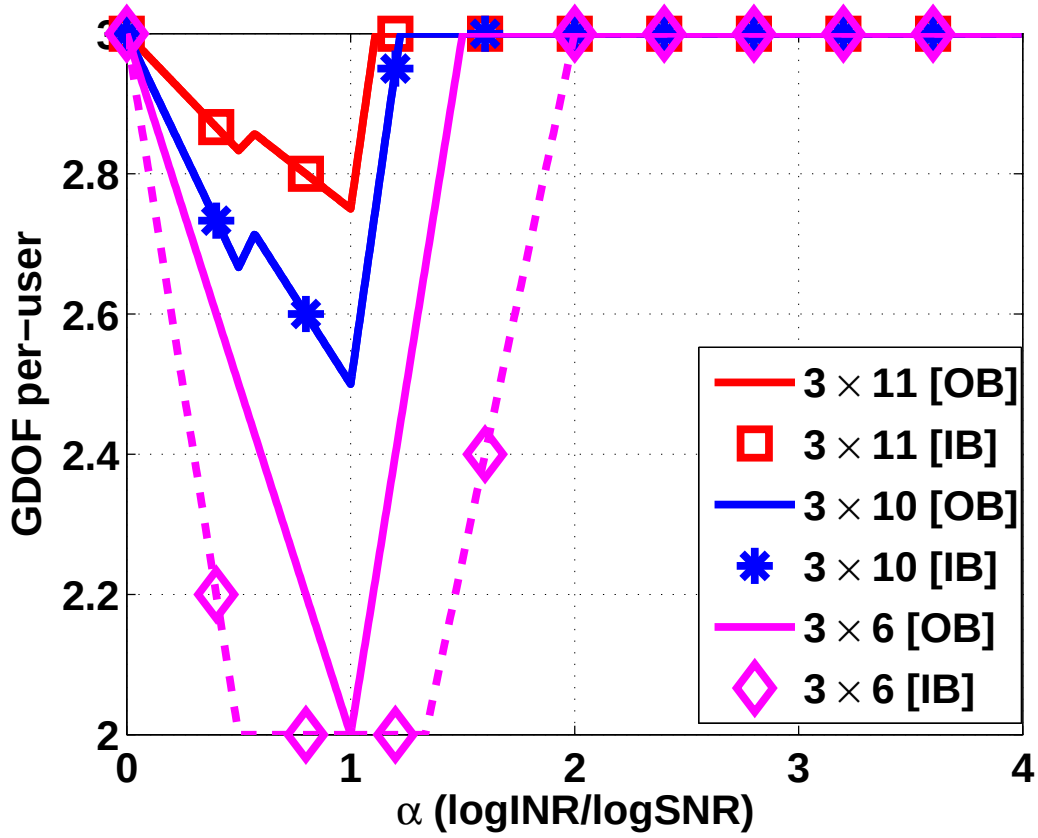


Figure 4.6: Outer bound (OB) and inner bound (IB) on the per user GDOF for $K = 4$ user MIMO GSIC with different antenna configurations.

The figures illustrate the effect of different combinations of the number of antennas at the transmitter and receiver on the achievable GDOF. When the interference is either low or very high, an equal or nearly equal (in Fig. 4.7) distribution of antennas achieves the best GDOF. The behavior for intermediate values of α depends on the specific values of M, N, K and α.

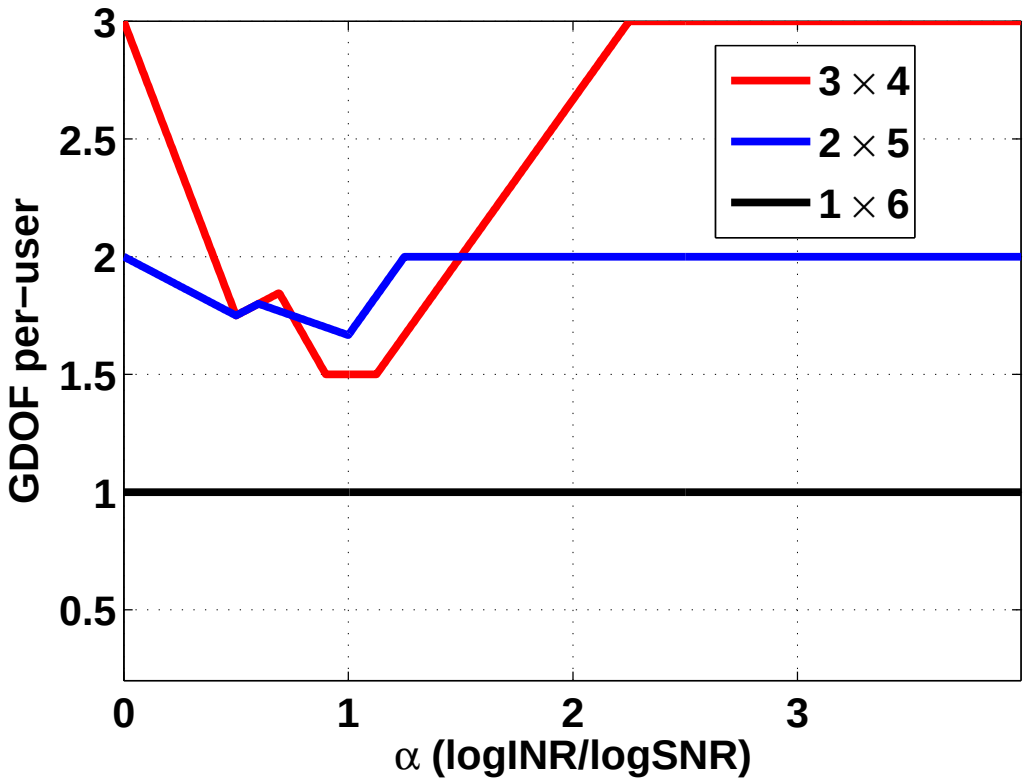


Figure 4.7: The achievable GDOF for the $K = 3$ user GSIC with different antenna configurations such that $M + N = 7$.

4.3 Further remarks

From the derived bounds, the following useful observations can be made. In particular, these insights are not be obtainable from the existing results for the 2-user MIMO GSIC or the K-user SIMO GSIC.

1. Treating interference as noise was known to be GDOF optimal in the weak interference regime in the 2-user SISO case [8], 2-user symmetric MIMO case [3] and the K-user SISO real-valued constant channel case [1]. The outer bound in Lemma 2 establishes that treating interference as noise is GDOF optimal in the weak interference regime for all K, when $M = N$. When $N > M$, the HK-scheme

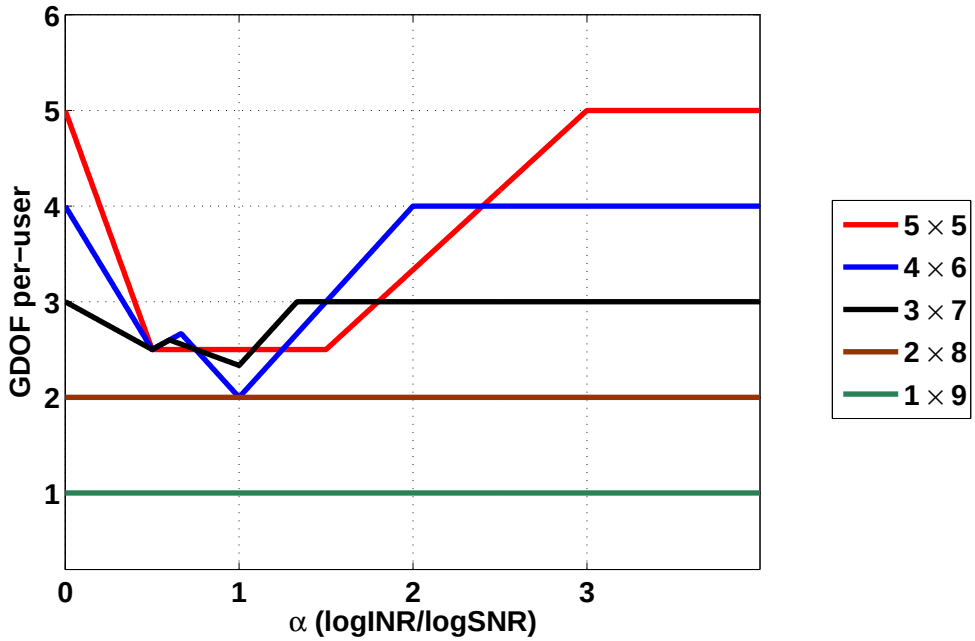


Figure 4.8: The achievable GDOF for the $K = 3$ user GSIC with different antenna configurations such that $M + N = 10$.

performs better. Moreover, the maximum of the HK-scheme and IA outperforms treating interference as noise and ZF-receiving for all values of M, N, α and K.

2. When $K > 3$ and $M = N$, IA outperforms the HK-scheme for $\frac{1}{2} \leq \alpha \leq 1$. Also, IA is GDOF optimal at $\alpha = \frac{1}{2}$ when $M = N$.

3. When $K > \frac{N}{M} + 1$, depending on the value of α, one or the other of the HK-scheme and IA performs the best. When $K \geq \frac{N}{M} + 4$, Theorem 9 characterizes the interplay between the two schemes and determines the range of α for which either scheme is active.

4. When $\frac{N}{M} < K \leq \frac{N}{M} + 1$, Theorem 13 establishes that the HK-scheme is GDOF optimal. Moreover, the HK-scheme does not assume a time-varying channel, and

hence it is optimal even for the constant channel case.

5. When $\frac{N}{M} < K \leq \frac{N}{M} + 1$, ZF-receiving coincides with the HK-scheme only at $\alpha = 1$ when $K > 2$. In contrast, when $K = 2$, ZF-receiving is optimal for $\alpha = \frac{1}{2}$ and 1 (see [3]).

6. The outer bounds on the sum rate in Theorems 11 and 12 hold for any number of transmit and receive antennas. Although Theorem 10 was presented for M antennas at each transmitter and N antennas at each receiver, it is straightforward to extend it to the case of arbitrary number of antennas at each transmitter and receiver. These results are new as there are no existing outer bounds on the sum rate of the MIMO GIC for $K \geq 3$.

7. No single outer bound on the GDOF is universally the tightest among the three. Theorem 13 characterizes the performance of the outer bounds as a function of K, M, N and α when $K \geq M+N$ and $\frac{N}{M} < K \leq \frac{N}{M}+1$, and when $\frac{N}{M}+1 < K < N+M$ for integer-valued $\frac{N}{M}$.

In general, it is found that IA performs well over a fairly wide range of parameters around $\alpha = 1$, and it offers a performance that does not depend on the interference level. Hence, it may be a good approach for managing the interference, especially when the number of receive antennas is comparable to the number of transmit antennas. As the number of receive dimensions increases, the HK-scheme becomes a better choice for interference management.

4.4 Conclusions

In this chapter, several interesting insights were obtained from the inner and outer bounds derived in Chapters 2 and 3. The outer bound was shown to be tight in the weak interference case ($0 \leq \alpha \leq \frac{1}{2}$) when $M = N$ for any K, and for all values of α when $\frac{N}{M} < K \leq \frac{N}{M} + 1$. The tightness of the bounds led to interesting insights on the performance limits of multiuser MIMO GIC and the relative efficacy of different techniques for interference management. For example, it was found that when $M = N$, treating interference as noise performs as well as the HK-scheme and outperforms both IA and ZF-receiving. However, when $N > M$, treating interference as noise is always suboptimal. The maximum of the HK-scheme and IA outperforms both treating interference as noise and ZF-receiving, for all values of M, N, α and K. When $\frac{N}{M} < K \leq \frac{N}{M} + 1$, the HK-scheme is GDOF optimal for all values of α. Also, the relation of the derived bounds to existing work were discussed. In the next chapter, a specific value of α is considered, i.e., $\alpha = 1$ and two algorithms are proposed for designing the linear precoders and receive filters for IA in the constant K-user MIMO IC. The $\alpha = 1$ case is interesting as both the signal power and interference power are equally strong.

Chapter 5

Interference Alignment Algorithms for the K-User Constant MIMO Interference Channel

As mentioned earlier, interference management is one of the key issues that need to be addressed in current and future wireless networks. One measure of the potential throughput of a wireless network with multiple transmitters and receivers is the degrees of freedom (DOF) [9, 10, 24], [47], [17], which is obtained as a special case of GDOF as mentioned in Chapter 2. It represents the number of interference-free signaling streams that are simultaneously admissible in the system. The goal of IA is to align the interferences caused at each receiver from all the transmitters into a common subspace of the total receive signal space, and to keep the interference subspace linearly independent of the desired signal subspace. In this case, a simple ZF receiver that projects the desired signal onto an interference-free subspace suffices for signal detection and decoding.

It is well-known that the DOF for a MIMO system with one transmitter and receiver

pair and M antennas at the transmitter and N antennas at the receiver is $\min(M, N)$. In the 2-user symmetric MIMO $(M \times N)$ IC (i.e., where both transmitters have M antennas and both receivers have N antennas), the maximum symmetric DOF achievable by each user with single-user zero-forcing receivers is $\min\left(\max(M, N)/2, M, \ N\right)$ [17]. In [9], Cadambe and Jafar introduced the idea of IA for a K-user SISO IC and showed that a sum DOF of $K/2$ is achievable, which represents a significant improvement over the single DOF achievable using orthogonal transmission schemes. This novel idea of overlapping interference spaces originated from the work of Maddah-Ali *et al.* in [24], [58]. This was subsequently used in the DOF analysis for the 2-user X channel in [10], [47]. Recent works that consider the DOF of wireless networks under different network settings include [59], [26], [60] and [61]. Outer bounds on the DOF were derived in [14] and [25]. Other aspects such as the feasibility of IA, the performance with limited feedback and imperfect channel knowledge, etc have been studied in [62–67].

In [14], Gou and Jafar proposed an IA scheme for a K-user symmetric MIMO $(M \times N)$ time varying IC and derived an inner bound and outer bound on the total DOF. Their proposed scheme requires a long symbol extension to achieve the IA. The achievable *symmetric DOF per user* using IA was shown to be

$$d = \frac{R}{R+1} \min(M, N), \tag{5.1}$$

where $R \triangleq \left\lfloor \frac{\max(M,N)}{\min(M,N)} \right\rfloor$. For the K-user IC, the authors showed that using $\mu_n \triangleq (R+1)(n+1)^{\Gamma}$ symbol extensions, where $\Gamma = KMR(KM - R - 1)$, one can obtain the DOF given by (5.1) as $n \to \infty$. The achievable DOF for a constant SISO and MIMO channel was characterized in [68] and [25]. However, the extent to which the DOF can

be achieved using linear beamforming schemes with finite symbol extensions is not yet fully known [62].

Linear precoding at the transmitters and zero-forcing filtering at the receivers is one way to achieve the sum DOF promised by IA. The idea is to find a pre-coding matrix at each user that aligns the interference at all receivers to within $N - d$ dimensions per symbol, while keeping the d-dimensional desired signal space linearly independent of the interference subspace, for an appropriately chosen d. An important problem is thus to devise algorithms for computing the transmit precoding matrices and the receive filtering matrices that align the interferences at all the receivers, given the channel state information. Iterative algorithms for designing precoders that approximately achieve IA were proposed in [29] and [30]. The two algorithms are similar in that they iteratively minimize the trace of the interference covariance matrix at the receivers and the covariance of the interference caused due to the precoding at the transmitters. In [31], a least squares method for designing the precoding matrices was proposed by writing a sufficient condition for IA as a set of linear equations. An iterative algorithm based on this has appeared in [69].

In general, the aforementioned algorithms are based on minimizing a performance metric that quantifies the interference signal leakage into the desired signal subspace of each receiver, and therefore may not guarantee exact IA in all cases. Another drawback is that they do not explicitly consider the desired signal *dimension* while designing the precoders, which is the key to determining the DOF achieved. To this end, this chapter proposes the use of another metric – the relative power of the weakest data

stream, in addition to the interference leakage into the desired signal space, to quantitatively evaluate the performance of IA algorithms. In addition, this chapter proposes two algorithms for designing the precoding and receive filtering matrices for IA in the block fading or constant MIMO $M \times N$ IC with a finite number of symbol extensions. Restricting the number of symbol extensions is important from the point of view of design complexity and fast convergence of iterative algorithms. The first algorithm is based on expressing a sufficient condition for sub-stream IA at each receiver as a set of linear equations similar to [31], but without the loss of signal dimension in that method. The second algorithm is iterative in nature, and requires the same channel knowledge as the distributed algorithms proposed in [29] and [30] at the transmitters and receivers, but again with the advantage that the desired signal dimension is preserved. The convergence of the algorithm to a locally optimum solution is established. The simulation results illustrate the performance benefits offered by the proposed algorithms relative to existing IA algorithms in terms of performance metrics such as the fraction of the interference power in the desired signal space, the relative power in the weakest data stream and the achieved sum rate.

The following notation is used in this chapter. A vertical stacking of matrices $\mathbf{A}$ and $\mathbf{B}$ with the same number of columns is written using a semi-colon, as $[\mathbf{A}; \mathbf{B}]$. The $d \times d$ identity matrix is denoted $\mathbf{I}_d$, and $\mathbf{A}^H$ denotes the conjugate-transpose of $\mathbf{A}$.

5.1 System model

Consider the symmetric K-user MIMO $(M \times N)$ complex GIC. There are K transmitter-receiver pairs with M antennas at each transmitter and N antennas at each receiver. The

receiver of user k only needs to correctly decode the signal from transmitter k, using zero forcing. There are therefore $K-1$ interfering signals at every receiver. The signal $\mathbf{y}_k(n) \in \mathbb{C}^{(N\times 1)}$ received at k^{th} receiver at time n can be expressed as

$$\mathbf{y}_k(n) = \sum_{t=1}^{K} \mathbf{H}_{kt}(n)\mathbf{x}_t(n) + \mathbf{z}_k(n), \qquad k = 1, 2, \ldots, K. \tag{5.2}$$

In the above, the additive noise at the receiver, $\mathbf{z}_k(n) \in \mathbb{C}^{(N\times 1)}$, is modeled as a spatially and temporally white process with independent and identically distributed $(i.i.d.)$, zero mean and unit variance circularly symmetric complex Gaussian entries. $\mathbf{x}_t(n) \in \mathbb{C}^{(M\times 1)}$ is the signal from transmitter t and $\mathbf{H}_{kt}(n) \in \mathbb{C}^{(N\times M)}$ represents the complex channel gain matrix from transmitter t to receiver k.

One way to achieve a fractional DOF in a constant MIMO IC is through symbol extension. With an S symbol extension of the channel, S consecutive symbols each of length d_k at transmitter and receiver k are collected to form a super symbol of length Sd_k. The extended channel matrix from transmitter j to receiver k is a block diagonal matrix of size $NS \times MS$ with the $n^{th} - (N \times M)$ block containing $\mathbf{H}_{kj}(n)$. Also, the channel output $\mathbf{y}_k$ and the additive noise $\mathbf{z}_k$ at receiver k both have a dimension $NS \times 1$. For a time varying MIMO IC, the channel matrix at each time slot n is different, so each block in the extended channel matrix is different. For the constant MIMO IC considered here, the channel matrix is assumed to remain constant for the duration of one extended symbol, i.e., each block in the extended channel matrix is the same. The constant channel assumption can be relaxed, when the channel is frequency selective and the symbol extension can be done across the carriers. Thus, the algorithms developed in Secs. 5.2 and 5.3 can be applied in the case of multicarrier modulations (OFDM). The channel

coefficients are assumed to be drawn $i.i.d.$ from a continuous distribution such as the complex Gaussian distribution, which implies that the IC is fully connected with probability one. Initially, all transmitters and receivers are assumed to have global channel knowledge of all links.

The receiver k pre-multiplies $\mathbf{y}_k(n)$ with a linear filter $\mathbf{W}_k^H \in \mathbb{C}^{Sd_k \times NS}$ to obtain

$$\hat{\mathbf{y}}_k = \mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{x}_k + \sum_{j=1, j\neq k}^{K} \mathbf{W}_k^H \mathbf{H}_{kj} \mathbf{x}_j + \mathbf{W}_k^H \mathbf{z}_k, \tag{5.3}$$

where the time index n has been dropped for simplicity.[1] The first term in the above represents the desired signal, the second term represents the interference from the other transmitters, and the last term is due to the AWGN at the receiver. Finally, the receiver estimates the transmitted symbols from $\hat{\mathbf{y}}_k$.

5.1.1 Problem setup

Consider assigning $d_k \leq \min(M, N)$ DOF to transmitter k. Then, associating a linearly independent set of d_k beamforming vectors with the d_k data streams, the transmitted signal is represented as

$$\mathbf{x}_k = \sum_{d=1}^{d_k} \mathbf{V}_k^d s_k^d = \mathbf{V}_k \mathbf{s}_k, \tag{5.4}$$

where $\mathbf{V}_k = [\mathbf{V}_k^1, \mathbf{V}_k^2, \ldots, \mathbf{V}_k^{d_k}]$ is the $M \times d_k$ precoding matrix of transmitter k, and $\mathbf{s}_k = [s_k^1; s_k^2; \ldots; s_k^{d_k}]$ is the $d_k \times 1$ set of symbols at transmitter k. The desired signal subspace of the k^{th} user receiver is spanned by the columns of $\mathbf{H}_{kk}\mathbf{V}_k$ with dimension d_k and the interfering signal subspace is spanned by the columns of $\mathbf{H}_{kj}\mathbf{V}_j, j = 1, 2, \ldots, K, j \neq k$.

[1] Note that, with a slight abuse of notation, $\mathbf{H}_{kj}$ in (5.3) represents the $NS \times MS$ block diagonal channel matrix when S symbol extensions are employed.

The interfering signal is restricted to occupy a total dimension up to $N - d_k$, and the desired signal subspace is required to be linearly independent of the interfering signal subspace. Then, it would be possible to recover the d_k independent streams at the k-th receiver using a zero-forcing beamforming matrix. Thus, the problem is to construct a set of matrices $\mathbf{V}_k, k = 1, 2, \ldots, K$, such that the above conditions are satisfied.

5.1.2 Performance measure

The performance of the proposed IA algorithms can be evaluated and compared with existing algorithms using the following two metrics. The choice of the metrics is intuitive; they provide insight into the efficacy of the IA algorithms in terms of the interference leakage and the preservation of the desired signal dimensions. The need for a performance measure arises because practical IA algorithms rarely align interferences perfectly, most commonly due to numerical round-off errors in the matrix computations.

Performance measure 1

This measure has been proposed in [29]. Let $(d_1, d_2, ..., d_K)$ denote the DOF of the users $1, 2, \ldots, K$, respectively. If the receive filter at the k^{th} receiver projects the signal onto the subspace spanned by the d_k smallest eigenvalues of the received interference covariance matrix, the fraction of the interfering signal power in the desired signal subspace is defined as

$$p_{\text{avg}} \triangleq \frac{1}{K} \sum_{k=1}^{K} p_k, \text{ where } p_k \triangleq \frac{\sum_{j=1}^{d_k} \lambda_j[\mathbf{Q}_k]}{\text{trace}\,(\mathbf{Q}_k)}, \tag{5.5}$$

where $\mathbf{Q}_k$ is the interference covariance matrix at receiver k, and $\lambda_j[\mathbf{Q}_k]$ denotes the j^{th} *smallest* eigen value of $\mathbf{Q}_k$. It is clear that the above represents a lower bound on the fractional interference power in the desired signal space, i.e., if the receive filter projects the signal into any d_k dimensional subspace, the fraction of the interference power in the desired signal space would be at least as large as p_k. Note that $p_k \in [0, 1]$, and when the IA is perfect, $p_k = 0$. A small value of p_{avg} thus indicates a better IA. However, one limitation of this performance measure is that it does not reflect the dimension of the desired signal space, which is captured by the metric below.

Performance measure 2

The effective channel for the desired signal at receiver k, after receive filtering, is given by $\mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k$. The power of the d_k^{th} data stream of the desired signal of user k is given by the square of the d_k^{th} largest singular value of $\mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k$. Thus, the relative power of the weakest desired data stream, denoted q_{avg}, can be written as

$$q_{\text{avg}} \triangleq \frac{1}{K} \sum_{k=1}^{K} q_k, \text{ where } q_k \triangleq \frac{\sigma_{d_k}^2 \left[\mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k\right]}{\sum_{j=1}^{d_k} \sigma_j^2 \left[\mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k\right]} \tag{5.6}$$

where $\sigma_l\left[\mathbf{A}\right]$ represents the l^{th} *largest* singular value of $\mathbf{A}$. Note that $q_k \in [0, 1/d_k]$, and a large value of q_k indicates that approximately the same data rate can be achieved in all the d_k data streams. When $q_k = 0$, there is a loss of signal dimension due to the receive filtering, and the DOF achieved by the k^{th} user is strictly less than d_k.

The next two sections propose two algorithms for the IA precoder design. It will be seen that they provide better performance in aligning and suppressing the interference

than existing algorithms, while at the same time preserving the desired signal dimensions, compared to previous methods. The first algorithm provides an IA solution that reduces the total dimension occupied by the interfering signals at all receivers by aligning some of the interfering signal sub-streams. The second is a distributed algorithm that can approximately align any number of interferers, as it designed only to minimize the interference leakage power, while maintaining the dimensionality of the desired signal at the receiver.

5.2 Algorithm 1: The eigenbeamforming method

This algorithm considers the case where $M \leq N$ and starts by writing the sufficient conditions for the IA as a set of linear equations. At every receiver, one of the interfering signal streams is aligned to lie in the span of the other $K-2$ interfering signals. The form of the solution obtained here is similar to the algorithms in [66] and [31]; but it differs from them in the following way. The algorithm proposed in [66] requires $M = N$, $K = N + 1$ and $d = 1$ whereas the proposed algorithm is applicable when $M \leq N$ and for a range of values for K and d (the feasible combinations are derived below). Also, in [31], the entire interference subspace from one user is aligned to the interference subspace from another user, whereas the proposed algorithm is based on aligning a subset of the data streams transmitted by a given interfering user within the span of the interference caused by the other $K-2$ interfering signals. First, a few examples are presented, to illustrate the central idea in the proposed method.

A sufficient condition for one data stream IA for the $K = 4$ user IC can be written as

$$\begin{aligned}
\mathbf{H}_{14}\mathbf{V}_4^{(1)} &= \mathbf{H}_{12}\mathbf{V}_2^{(3)} + \mathbf{H}_{13}\mathbf{V}_3^{(3)}, \\
\mathbf{H}_{21}\mathbf{V}_1^{(1)} &= \mathbf{H}_{23}\mathbf{V}_3^{(2)} + \mathbf{H}_{24}\mathbf{V}_4^{(2)}, \\
\mathbf{H}_{32}\mathbf{V}_2^{(1)} &= \mathbf{H}_{31}\mathbf{V}_1^{(2)} + \mathbf{H}_{34}\mathbf{V}_4^{(3)}, \\
\mathbf{H}_{43}\mathbf{V}_3^{(1)} &= \mathbf{H}_{41}\mathbf{V}_1^{(3)} + \mathbf{H}_{42}\mathbf{V}_2^{(2)}.
\end{aligned} \tag{5.7}$$

The four equations above correspond to the IA conditions at receivers $1, 2, 3$ and 4, respectively. Note that the above equations require at least three data streams to be assigned to each user. If the users are assigned more than three streams each, the remaining beamforming vectors can be chosen to be arbitrary linearly independent vectors, as long as they are linearly independent of the beamforming vectors determined from the equations above. This ensures that the rank condition on the desired data signal is satisfied, while still aligning one of the data streams from each user in the space spanned by the other interfering users. The system of equations in (5.7) can be written in the form

$$\tilde{\mathbf{H}}\mathbf{V} = \mathbf{0}, \tag{5.8}$$

where $\mathbf{V} \triangleq [\mathbf{V}_1^{(1)}; \mathbf{V}_1^{(2)}; \mathbf{V}_1^{(3)}; \mathbf{V}_2^{(1)}; \mathbf{V}_2^{(2)}; \mathbf{V}_2^{(3)}; \mathbf{V}_3^{(1)}; \mathbf{V}_3^{(2)}; \mathbf{V}_3^{(3)}; \mathbf{V}_4^{(1)}; \mathbf{V}_4^{(2)}; \mathbf{V}_4^{(3)}]$, and

$$\tilde{\mathbf{H}} \triangleq \begin{bmatrix}
\mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{12} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{13} & -\mathbf{H}_{14} & \mathbf{0} & \mathbf{0} \\
-\mathbf{H}_{21} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{23} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{24} & \mathbf{0} \\
\mathbf{0} & \mathbf{H}_{31} & \mathbf{0} & -\mathbf{H}_{32} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{H}_{34} \\
\mathbf{0} & \mathbf{0} & \mathbf{H}_{41} & \mathbf{0} & \mathbf{H}_{42} & \mathbf{0} & -\mathbf{H}_{43} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0}
\end{bmatrix} \tag{5.9}$$

A non-trivial solution to (5.8) is given by any linear combination of the eigenvectors

corresponding to the zero eigenvalue of $\tilde{\mathbf{H}}^H\tilde{\mathbf{H}}$. Note that for an IA solution to be feasible with this method, $\tilde{\mathbf{H}}^H\tilde{\mathbf{H}}$ must be rank deficient, i.e., its smallest eigenvalue should be equal to zero. A feasibility condition for this is derived in the next subsection.

In a similar manner, the two stream alignment for the $K = 4$ user case can be described as follows:

$$\begin{aligned}
\mathbf{H}_{14}\begin{bmatrix}\mathbf{V}_4^{(1)} & \mathbf{V}_4^{(2)}\end{bmatrix} &= \mathbf{H}_{12}\begin{bmatrix}\mathbf{V}_2^{(5)} & \mathbf{V}_2^{(6)}\end{bmatrix} + \mathbf{H}_{13}\begin{bmatrix}\mathbf{V}_3^{(5)} & \mathbf{V}_3^{(6)}\end{bmatrix}, \\
\mathbf{H}_{21}\begin{bmatrix}\mathbf{V}_1^{(1)} & \mathbf{V}_1^{(2)}\end{bmatrix} &= \mathbf{H}_{23}\begin{bmatrix}\mathbf{V}_3^{(3)} & \mathbf{V}_3^{(4)}\end{bmatrix} + \mathbf{H}_{24}\begin{bmatrix}\mathbf{V}_4^{(3)} & \mathbf{V}_4^{(4)}\end{bmatrix}, \\
\mathbf{H}_{32}\begin{bmatrix}\mathbf{V}_2^{(1)} & \mathbf{V}_2^{(2)}\end{bmatrix} &= \mathbf{H}_{31}\begin{bmatrix}\mathbf{V}_1^{(3)} & \mathbf{V}_1^{(4)}\end{bmatrix} + \mathbf{H}_{34}\begin{bmatrix}\mathbf{V}_4^{(5)} & \mathbf{V}_4^{(6)}\end{bmatrix}, \\
\mathbf{H}_{43}\begin{bmatrix}\mathbf{V}_3^{(1)} & \mathbf{V}_3^{(2)}\end{bmatrix} &= \mathbf{H}_{41}\begin{bmatrix}\mathbf{V}_1^{(5)} & \mathbf{V}_1^{(6)}\end{bmatrix} + \mathbf{H}_{42}\begin{bmatrix}\mathbf{V}_2^{(3)} & \mathbf{V}_2^{(4)}\end{bmatrix}.
\end{aligned} \tag{5.10}$$

Again, the four equations above correspond to the IA conditions at the four receivers. The above can now be expressed in the following compact form:

$$\bar{\mathbf{H}}\bar{\mathbf{V}} = \mathbf{0}, \tag{5.11}$$

where $\bar{\mathbf{H}}$ is in a form similar to (5.9), $\bar{\mathbf{V}} \triangleq [\mathbf{V}_{11};\ \mathbf{V}_{13};\ \mathbf{V}_{15};\ \mathbf{V}_{21};\ \mathbf{V}_{23};\ \mathbf{V}_{25};\ \mathbf{V}_{31};\ \mathbf{V}_{33};\ \mathbf{V}_{35};\ \mathbf{V}_{41};\ \mathbf{V}_{43};\ \mathbf{V}_{45}]$, and $\mathbf{V}_{kl} \triangleq \begin{bmatrix}\mathbf{V}_k^{(l)} & \mathbf{V}_k^{(l+1)}\end{bmatrix}$.

As a final example, the one stream alignment in the $K = 5$ user case is described below.

$$\mathbf{H}_{15}\mathbf{V}_5^{(1)} = \mathbf{H}_{12}\mathbf{V}_2^{(4)} + \mathbf{H}_{13}\mathbf{V}_3^{(4)} + \mathbf{H}_{14}\mathbf{V}_4^{(4)}, \tag{5.12}$$

$$\mathbf{H}_{21}\mathbf{V}_1^{(1)} = \mathbf{H}_{23}\mathbf{V}_3^{(2)} + \mathbf{H}_{24}\mathbf{V}_4^{(2)} + \mathbf{H}_{25}\mathbf{V}_5^{(2)}, \tag{5.13}$$

$$\mathbf{H}_{32}\mathbf{V}_2^{(1)} = \mathbf{H}_{31}\mathbf{V}_1^{(2)} + \mathbf{H}_{34}\mathbf{V}_4^{(3)} + \mathbf{H}_{35}\mathbf{V}_5^{(3)}, \tag{5.14}$$

$$\mathbf{H}_{43}\mathbf{V}_3^{(1)} = \mathbf{H}_{41}\mathbf{V}_1^{(3)} + \mathbf{H}_{42}\mathbf{V}_2^{(2)} + \mathbf{H}_{45}\mathbf{V}_5^{(4)}, \tag{5.15}$$

$$\mathbf{H}_{54}\mathbf{V}_4^{(1)} = \mathbf{H}_{51}\mathbf{V}_1^{(4)} + \mathbf{H}_{52}\mathbf{V}_2^{(3)} + \mathbf{H}_{53}\mathbf{V}_3^{(3)}. \tag{5.16}$$

As before, each of the above equations correspond to the IA condition at each of the five receivers.

Generalizing the above, consider an S symbol extension of the channel. Let $\mathbf{V}_i^{(j)} \in \mathbb{C}^{MS\times 1}$ represent the beamforming vector corresponding to the j^{th} data stream of the i^{th} user. Then, a set of equations for aligning p data streams per user within the interference subspace spanned by the remaining interfering users in the K-user IC can be written as

$$\textbf{Rx } 1\textbf{: } \mathbf{H}_{1K}\mathbf{V}_K^{(n)} = \sum_{j=2}^{K-1} \mathbf{H}_{1j}\mathbf{V}_j^{((K-2)p+n)}, \tag{5.17}$$

$$\textbf{Rx } 2\textbf{: } \mathbf{H}_{21}\mathbf{V}_1^{(n)} = \sum_{j=3}^{K} \mathbf{H}_{2j}\mathbf{V}_j^{(p+n)}, \tag{5.18}$$

$$\begin{aligned}\textbf{Rx } j=3 \textbf{ to } K\textbf{: } \mathbf{H}_{j(j-1)}\mathbf{V}_{j-1}^{(n)} = \mathbf{H}_{j1}\mathbf{V}_1^{((j-2)p+n)} + \sum_{r=2}^{j-2} \mathbf{H}_{jr}\mathbf{V}_r^{((j-3)p+n)} \\ + \sum_{r=j+1}^{K} \mathbf{H}_{jr}\mathbf{V}_r^{((j-1)p+n)},\end{aligned} \tag{5.19}$$

for $n = 1, 2, \ldots, p$. To obtain the above equations, each user must be assigned at least $(K-1)p$ streams, and p of these streams are aligned with the remaining interference at each receiver. If each user is assigned more than $(K-1)p$ streams, the remaining streams can be chosen at random from any continuous distribution to ensure their linear independence from the first $(K-1)p$ streams. The above equations can be re-written to obtain the IA conditions for all cases are expressed in the form

$$\tilde{\mathbf{H}}\tilde{\mathbf{V}} = \mathbf{0}, \tag{5.20}$$

where $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{V}}$ are obtained by appropriately stacking the channel and beamforming matrices, respectively. A non-trivial solution to (5.20) is given by any linear combination of the eigenvectors corresponding to the null space of $\tilde{\mathbf{H}}^{\mathbf{H}}\tilde{\mathbf{H}}$. The necessary conditions under which a solution exists to the above is derived in the following subsection.

5.2.1 Feasibility conditions

The size of the matrix $\tilde{\mathbf{H}}$ is $KNSp \times K(K-1)MSp$, where p is the number of data streams aligned at each receiver. First, for $\tilde{\mathbf{H}}$ to have a non-trivial null space, it must be column rank-deficient, which leads to

$$K > \frac{N}{M} + 1. \tag{5.21}$$

Second, there must be sufficiently many linearly independent beamforming vectors at the transmitters to achieve the desired DOF. Since each user must be assigned at least $(K-1)p$ data streams, this requires

$$\begin{aligned} (K-1)p \leq dS \leq MS, \\ \text{or } p \leq \frac{dS}{K-1} \leq \frac{MS}{K-1}. \end{aligned} \tag{5.22}$$

In the above equation, MS is the maximum possible DOF that can be assigned to a user, and dS is the DOF assigned to the user, both over the S symbol extension of the channel. Third, there must be sufficiently many linearly independent receive beamforming vectors to be able to separate the desired signal from the interference. The number of dimensions available at each receiver is NS, and the number of dimensions occupied by the desired signal is dS. The remaining number of dimensions, $(N-d)S$

must be greater than or equal to the number of interfering signal dimensions, which is $(K-1)dS - p$. This results in the condition

$$p \geq (Kd - N)S, \tag{5.23}$$

on the number of streams that need to be aligned to achieve d DOF per user per symbol extension. Combining (5.22) and (5.23), one obtains,

$$(Kd - N)S \leq \frac{dS}{K-1}. \tag{5.24}$$

Finally, incorporating the condition $d \leq M$, the maximum DOF achievable by this scheme is upper bounded by the following quantity:

$$d \leq \min\left(\frac{(K-1)N}{K(K-1)-1}, M\right). \tag{5.25}$$

Note that achieving the DOF given by the right hand side in the above equation requires $S = K(K-1)-1$ symbol extensions. For example, when $M = 3, N = 7$ and $K = 4$, (5.1) achieves a DOF of $d = 2$ with a very long symbol extension and a time-varying channel, while the eigenbeamforming method achieves $d = 1.91$ with $S = 11$ symbol extensions and even for constant MIMO channels. However, the achievable DOF decreases with K, making this method more suitable when the number of users K is relatively small. More examples on this are provided in Sec. 5.4.

Note that in the above eigenbeamforming method, global knowledge of all K^2 links is required in order to compute the precoding matrices. This computation could happen at a central controller, which then shares the optimum precoding matrices with the K transmitters and the optimum receive filtering matrices with the K receivers. In the

next section, a distributed algorithm that only requires knowledge of the received interference covariance matrix at each receiver and knowledge of the reciprocal interference covariance matrix obtained by reversing the direction of all links at each transmitter, is presented. The interference covariance matrix is reflective of the interference caused by each transmitter at all the receivers. The price paid for not requiring global channel knowledge is that the algorithm is iterative in nature.

5.3 Algorithm 2: Iterative algorithm for IA

In this section, a distributed and iterative algorithm is presented for designing the IA precoding matrices for a constant IC, such that the necessary and sufficient conditions for IA are satisfied. The algorithm is similar in flavor to the distributed IA algorithms in [29] and [30]. It iterates between two objective functions with a common interference leakage term, to find the locally optimum $\mathbf{V}_k$ and $\mathbf{W}_k$. One key difference between this and past work is that the minimization of the interference leakage is performed subject to a constraint on the dimension of the desired signal subspace. For example, although the Max-SINR algorithm proposed in [29] tries to maximize the received SINR at the desired user, there is no guarantee that the signal dimension is preserved when symbol extension is considered over a constant channel. Yet another difference is that previous iterative algorithms impose a quadratic constraint on the $\mathbf{V}_k$ and $\mathbf{W}_k$ matrices, while the algorithm below imposes a linear constraint on them to preserve the desired signal dimensionality. For clarity, the derivation mentioned below assumes $S = 1$ and its extension to any finite number of symbol extensions is straightforward.

First, consider the design of the receive filter matrices $\mathbf{W}_k$, for a fixed $\mathbf{V}_k$ at all the

transmitters. The interference and the noise term at the receiver k after receive filtering is given by,

$$\mathbf{IR}_k = \sum_{j=1, j\neq k}^{K} \mathbf{W}_k{}^H \mathbf{H}_{kj} \mathbf{V}_j \mathbf{s}_j + \mathbf{W}_k{}^H \mathbf{z}_k. \tag{5.26}$$

When all the interfering signals are aligned, one needs to find a $\mathbf{W}_k$ such that $\sum_{j=1,j\neq k}^{K}$ $\mathbf{W}_k{}^H \mathbf{H}_{kj} \mathbf{V}_j = 0$. A judicious choice for $\mathbf{W}_k$ is one that minimizes the interference leakage power at receiver k. There is also a constraint on the dimensionality of the desired signal: rank $\left(\mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k\right) = d_k$, where d_k is the DOF assigned to k^{th} transmitter. Thus, given the channel matrices $\mathbf{H}_{kk}$ and the precoding matrices $\mathbf{V}_k$, the optimal receive filter $\mathbf{W}_k$ is designed to minimize the cost function

$$J_k \triangleq \text{trace}(\mathbf{W}_k^H \mathbf{Q}_k \mathbf{W}_k) \quad \text{subject to} \quad \mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k = \alpha \mathbf{I}_{d_k}, \tag{5.27}$$

where $\mathbf{Q}_k$ is the interference plus noise covariance matrix at receiver k, given by,

$$\mathbf{Q}_k = \sum_{j=1, j\neq k}^{K} P_j [\mathbf{H}_{kj} \mathbf{V}_j][\mathbf{H}_{kj} \mathbf{V}_j]^H + \mathbf{I}_N, \tag{5.28}$$

and $\alpha > 0$ is selected such that trace $\left(\mathbf{W}_k^H \mathbf{W}_k\right) = 1$. Here, P_j is the transmit power of user j. The solution to (5.27) is given by

$$\mathbf{W}_k^{opt} = \alpha \mathbf{Q}_k^{-1} \mathbf{U}_k [\mathbf{U}_k^H \mathbf{Q}_k^{-1} \mathbf{U}_k]^{-1}, \tag{5.29}$$

where $\mathbf{U}_k = \mathbf{H}_{kk} \mathbf{V}_k$ is the desired signal subspace of the k^{th} user, and

$$\alpha = \frac{1}{\sqrt{\text{trace}\left([\mathbf{Q}_k^{-1} \mathbf{U}_k [\mathbf{U}_k^H \mathbf{Q}_k^{-1} \mathbf{U}_k]^{-1}]^H [\mathbf{Q}_k^{-1} \mathbf{U}_k [\mathbf{U}_k^H \mathbf{Q}_k^{-1} \mathbf{U}_k]^{-1}]\right)}}. \tag{5.30}$$

The proof of the above is stated as Lemma 4 below.

Lemma 4. *For the constrained optimization problem,*

$$\min_{\mathbf{G}} J(\mathbf{G}) \triangleq \textit{trace}\left(\mathbf{G}^H\mathbf{Q}\mathbf{G}\right) \quad \textit{subject to} \quad \mathbf{A}\mathbf{G} = \alpha\mathbf{I_d}, \tag{5.31}$$

where $\mathbf{G}$ *is an* $M \times d$ *matrix,* $\mathbf{Q}$ *is an* $M \times M$ *positive definite matrix and* $\mathbf{A}$ *is a* $d \times M$ *matrix, the optimum solution is given by*

$$\mathbf{G_0} = \alpha\mathbf{Q}^{-1}\mathbf{A}^H[\mathbf{A}\mathbf{Q}^{-1}\mathbf{A}^H]^{-1}. \tag{5.32}$$

Proof. It is sufficient to show that $J(\mathbf{G}_0) = \text{trace}\left(\mathbf{G}_0^H\mathbf{Q}\mathbf{G}_0\right)$ is the minimum value of the objective function, subject to the constraint. Suppose the optimum solution is $\mathbf{G}_p = \mathbf{G}_0 + \Delta, \Delta \neq 0$. Then, the objective function becomes,

$$\begin{aligned} J(\mathbf{G}_p) &= \text{trace}\left([\mathbf{G}_0 + \Delta]^H\mathbf{Q}[\mathbf{G}_0 + \Delta]\right), \\ &= \text{trace}\left(\mathbf{G}_0^H\mathbf{Q}\mathbf{G}_0 + \Delta^H\mathbf{Q}\Delta + \Delta^H\mathbf{Q}\mathbf{G}_0 + \mathbf{G}_0^H\mathbf{Q}\Delta\right). \end{aligned} \tag{5.33}$$

From the constraint $\mathbf{A}\mathbf{G}_p = \alpha\mathbf{I}$, one obtains $\mathbf{A}\Delta = \mathbf{0}$, and the cross terms get simplified as,

$$\Delta^H\mathbf{Q}\mathbf{G}_0 = \alpha\Delta^H\mathbf{Q}\mathbf{Q}^{-1}\mathbf{A}^H[\mathbf{A}\mathbf{Q}^{-1}\mathbf{A}^H]^{-1} = \mathbf{0}, \tag{5.34}$$

and similarly, $\mathbf{G}_0^H\mathbf{Q}\Delta = \mathbf{0}$. Now, the quadratic term trace$(\Delta^H\mathbf{Q}\Delta) \geq 0$ since $\mathbf{Q}$ is positive definite. Hence, $J(\mathbf{G}_0) \leq J(\mathbf{G}_p)$, which is a contradiction. Hence, $\mathbf{G}_0$ is the optimum solution. □

Now consider designing the precoding matrices $\mathbf{V}_k$ at the K transmitters, given the receive filtering matrices $\mathbf{W}_k$ at the receivers. The interfering signal due to transmitter

k at the unintended receivers is given by

$$\mathbf{T}_{kj} = \mathbf{W}_j^H \mathbf{H}_{jk} \mathbf{V}_k \mathbf{s}_k, \quad j = 1, 2, \ldots, K, j \neq k. \tag{5.35}$$

From the feasibility condition for perfect IA, one requires

$$\mathbf{W}_j^H \mathbf{H}_{jk} \mathbf{V}_k = \mathbf{0}, \quad j = 1, 2, \ldots, K, j \neq k. \tag{5.36}$$

Again, a judicious choice for the precoding matrices would be to select $\mathbf{V}_k$ such that the total interference power at the unintended receivers due to transmitter k is minimized. The interference power due to transmitter k at receiver j is obtained from the squared Frobenius norm of $\mathbf{W}_j^H \mathbf{H}_{jk} \mathbf{V}_k$ as,

$$L_{kj} = \text{trace}\left(P_k \mathbf{V}_k^H [\mathbf{W}_j^H \mathbf{H}_{jk}]^H [\mathbf{W}_j^H \mathbf{H}_{jk}] \mathbf{V}_k\right). \tag{5.37}$$

Thus, the total interference power due to the transmitter k is given by

$$L'_k = \text{trace}\left(\mathbf{V}_k^H \mathbf{R}'_k \mathbf{V}_k\right), \tag{5.38}$$

where

$$\mathbf{R}'_k = P_k \sum_{j=1, j\neq k}^{K} [\mathbf{W}_j^H \mathbf{H}_{jk}]^H [\mathbf{W}_j^H \mathbf{H}_{jk}]. \tag{5.39}$$

The objective here is to choose $\mathbf{V}_k$ such that L'_k is minimized, subject to the desired signal dimension constraint, i.e., rank $\left(\mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k\right) = d_k$. Including a regularization

term,[2] the objective function is modified as,

$$L_k = \text{trace}\left(\mathbf{V}_k^H \mathbf{R}_k' \mathbf{V}_k + \mathbf{V}_k^H \mathbf{V}_k\right). \tag{5.40}$$

Thus, the constrained optimization is given by,

$$\min_{\mathbf{V}_k} L_k = \text{trace}\left(\mathbf{V}_k^H \mathbf{R}_k \mathbf{V}_k\right), \quad \text{subject to} \quad \mathbf{W}_k^H \mathbf{H}_{kk} \mathbf{V}_k = \beta \mathbf{I}_{d_k}, \tag{5.41}$$

where $\beta > 0$ is selected to obtain trace $\left(\mathbf{V}_k^H \mathbf{V}_k\right) = 1$, and

$$\mathbf{R}_k = P_k \sum_{j=1, j\neq k}^{K} [\mathbf{W}_j^H \mathbf{H}_{jk}]^H [\mathbf{W}_j^H \mathbf{H}_{jk}] + \mathbf{I}_M. \tag{5.42}$$

Notice that $\mathbf{R}_k$ is the reflected covariance matrix of a virtual channel obtained by interchanging the transmitters and receivers. The optimum solution for $\mathbf{V}_k$ is obtained using Lemma 4 as

$$\mathbf{V}_k^{opt} = \beta \mathbf{R}_k^{-1} \mathbf{T}_k^H [\mathbf{T}_k \mathbf{R}_k^{-1} \mathbf{T}_k^H]^{-1}, \quad k = 1, 2, \ldots, K, \tag{5.43}$$

where $\mathbf{T}_k = \mathbf{W}_k^H \mathbf{H}_{kk}$ and

$$\beta = \frac{1}{\sqrt{\text{trace}\left([\mathbf{R}_k^{-1} \mathbf{T}_k^H [\mathbf{T}_k \mathbf{R}_k^{-1} \mathbf{T}_k^H]^{-1}]^H [\mathbf{R}_k^{-1} \mathbf{T}_k^H [\mathbf{T}_k \mathbf{R}_k^{-1} \mathbf{T}_k^H]^{-1}]\right)}}. \tag{5.44}$$

The iterative precoder design algorithm is summarized in Table 5.1. The algorithm requires knowledge of $\mathbf{Q}_k$ and $\mathbf{U}_k$ at the k^{th} receiver and $\mathbf{R}_k$ and $\mathbf{T}_k$ at the k^{th} transmitter rather than full information of all K^2 channels.

One issue that needs to be addressed is the convergence of the above algorithm; this

[2]The purpose of the regularization term is merely to guarantee the invertibility of $\mathbf{R}_k$. In practice, if $\mathbf{R}_k'$ is invertible, the regularization can be eliminated.

Step. No.	Action
1	Initialize $\mathbf{V}_k, k = 1, 2, \ldots, K$ to be arbitrary precoding matrices
2	Compute the matrix $\mathbf{Q}_k$ in (5.28) for $k = 1, 2, \ldots, K$
3	Obtain $\mathbf{W}_k, k = 1, 2, \ldots, K$ using (5.29)
4	Compute the matrix $\mathbf{R}_k$ from (5.42)
5	Obtain $\mathbf{V}_k, k = 1, 2, \ldots, K$ using (5.43)
6	Repeat steps $2 - 5$ until convergence of $\sum_{k=1}^{K} J_k$ and $\sum_{k=1}^{K} L_k$

Table 5.1: The iterative precoder design algorithm

is discussed next.

5.3.1 Convergence of the algorithm

First, it can be shown that the objective functions to be minimized in the algorithm at *Step 3* and *Step 5* are identical. The objective function minimized in the *Step 3* is the total interference plus noise power at receiver k. The total interference plus noise power across all the receivers is obtained as,

$$P_R = \sum_{k=1}^{K} \text{trace}\left(\mathbf{W}_k^H \left[\sum_{j=1, j\neq k}^{K} P_j [\mathbf{H}_{kj}\mathbf{V}_j][\mathbf{H}_{kj}\mathbf{V}_j]^H + \mathbf{I}_N\right] \mathbf{W}_k\right). \tag{5.45}$$

As the trace is a linear operator, the above reduces to

$$\begin{aligned} P_R &= \text{trace}\left(\sum_{k=1}^{K}\left[\sum_{j=1, j\neq k}^{K} P_j \mathbf{W}_k^H [\mathbf{H}_{kj}\mathbf{V}_j][\mathbf{H}_{kj}\mathbf{V}_j]^H \mathbf{W}_k + \mathbf{W}_k^H \mathbf{W}_k\right]\right), \\ &= \text{trace}\left(\sum_{k=1}^{K}\left[\sum_{j=1, j\neq k}^{K} P_j [\mathbf{W}_k^H \mathbf{H}_{kj}\mathbf{V}_j][\mathbf{W}_k^H \mathbf{H}_{kj}\mathbf{V}_j]^H\right]\right) + K. \end{aligned} \tag{5.46}$$

The objective function minimized at *Step 5* of the algorithm is the total interference power due to transmitter k, with a regularization term. The total interference power

due to all the transmitters is given by,

$$P_T = \sum_{k=1}^{K} \text{trace}\left(\mathbf{V}_k^H \left[P_k \sum_{j=1, j\neq k}^{K} [\mathbf{W}_j^H \mathbf{H}_{jk}]^H [\mathbf{W}_j^H \mathbf{H}_{jk}] + \mathbf{I}_M\right] \mathbf{V}_k\right). \tag{5.47}$$

Again, using the linearity property of the trace, the above is simplified as,

$$\begin{aligned} P_T &= \text{trace}\left(\sum_{k=1}^{K}\left[\sum_{j=1, j\neq k}^{K} P_k \mathbf{V}_k^H [\mathbf{W}_j^H \mathbf{H}_{jk}]^H [\mathbf{W}_j^H \mathbf{H}_{jk}] \mathbf{V}_k + \mathbf{V}_k^H \mathbf{V}_k\right]\right), \\ &= \text{trace}\left(\sum_{k=1}^{K}\left[\sum_{j=1, j\neq k}^{K} P_k [\mathbf{W}_j^H \mathbf{H}_{jk} \mathbf{V}_k]^H [\mathbf{W}_j^H \mathbf{H}_{jk} \mathbf{V}_k]\right]\right) + K. \end{aligned} \tag{5.48}$$

Since the objective functions in both P_T and P_R are the same, minimizing one does not increase the other objective function. Moreover, at each iteration, the objective functions decrease, and are bounded below by zero. This proves the convergence of both the objective functions across all transmitter-receiver pairs to a local optimum.

Note that the algorithm may not result in a zero objective function, even when the interferences are aligned perfectly and noise variance is zero, because of numerical round off errors. However, the numerical issues encountered are similar to other algorithms proposed in the literature that attempt to align interferences. Also, in the above, the constraint on the desired signal dimension is key to ensuring that there is no loss in DOF when the interfering signals are aligned.

5.4 Simulation results

Now, the performance of the proposed IA algorithms are evaluated in terms of p_{avg} and q_{avg} in (5.5) and (5.6), respectively, and are compared with existing algorithms. In addition, the algorithms are compared in terms of the sum rates of the users at different

values of SNR.

The setup consists of a symmetric MIMO $(M \times N)$ constant IC. The channel coefficients were generated from the i.i.d. complex circularly symmetric Gaussian distribution with zero mean and unit variance. The values of p_{avg} and q_{avg} were averaged using 1000 independent channel realizations, and the results were plotted as a function of the DOF obtained per user, per symbol extension. The solution from the eigenbeamforming method in (5.20) is plotted as the curve labeled `Eig-bf`. The iterative algorithm in Table 5.1 is plotted as the curve labeled `Iterative algorithm`. These algorithms are compared to the alternating minimization based IA (curves labeled `Alter-IA`) [30], the distributed IA (curves labeled `Dist-IA`) [29], the least-squares IA (curves labeled `Least squares algo`) [31] algorithms.

Figures 5.1, 5.2 and 5.3 show the fraction of the interference power in the desired signal (denoted p_{avg} above), versus the DOF per user for the 4-user (Figs. 5.1, 5.2) and 5-user (Fig. 5.3) IC with $M \times N = 3 \times 6, 3 \times 7$, and 2×6, and $K = 4, 4$ and 5, respectively. The rank of the desired signal subspace, $\mathbf{H}_{kk}\mathbf{V}_k, k = 1, 2, \ldots, K$, gives the DOF achieved by the user k. In terms of performance measure p_{avg}, the iterative algorithm gives a low value of the leakage for the DOF values considered. The distributed IA algorithm exhibits a similar performance in terms of p_{avg}. However, its performance is poor in terms of the relative power in the weakest data stream (q_{avg}), as seen in Fig. 5.4. In the 5-user case (Fig. 5.3), the distributed IA outperforms the eigenbeamforming algorithm and iterative algorithm with respect to the performance metric p_{avg}. The performance of the distributed IA in terms of q_{avg} is poor compared to the proposed methods, as seen in Fig. 5.6. In the case of the least-squares method proposed in [31], it is seen that

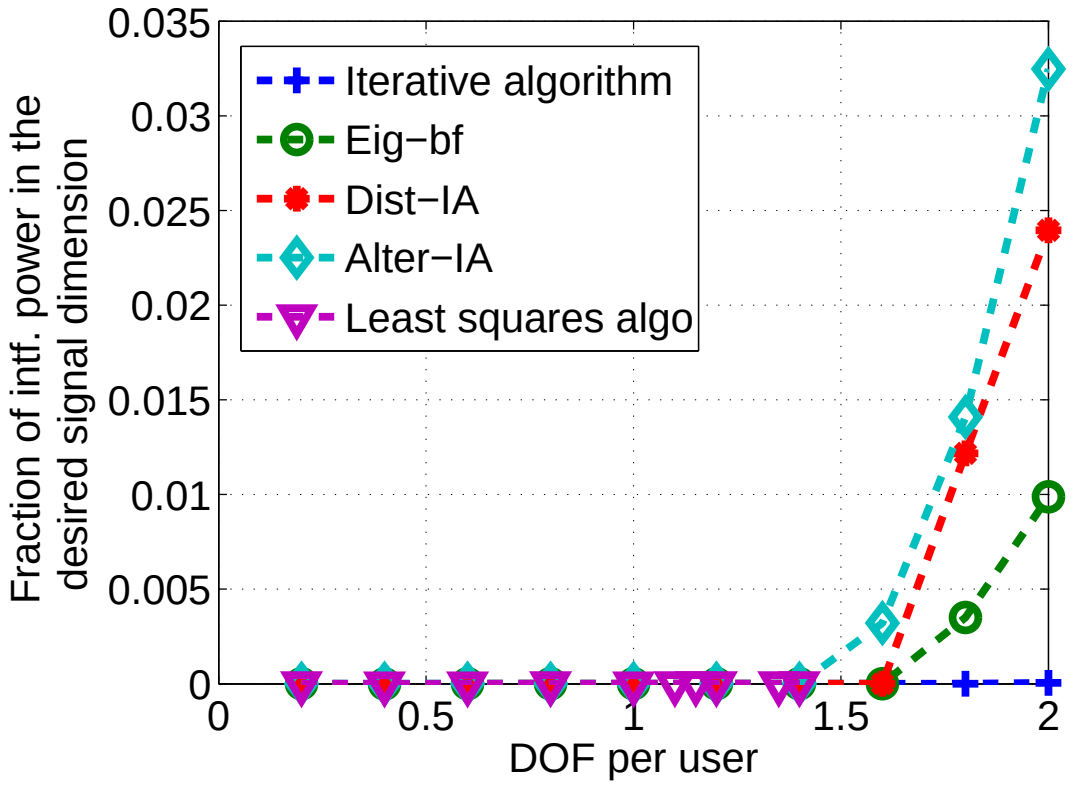


Figure 5.1: Fraction of the interference power in the desired signal space for the $K = 4$ user IC with configuration $M = 3$, $N = 6$, and $S = 5$.

the algorithm is unable to reach the target DOF for larger values of the DOF. For the eigenbeamforming method, $p = 2$ streams are aligned in the 3×6 case (Fig. 5.1) and $p = 1$ stream is aligned in the other two cases. The maximum per user DOF achievable by this scheme, from (5.25), are upper bounded by 1.64, 1.91, and 1.26, for the $(3\times6, K = 4)$, $(3 \times 7, K = 4)$ and $(2 \times 6, K = 5)$ cases, respectively and the following simulation results demonstrate that the achievable DOF are close to the maximum DOF achievable by this scheme. In order to achieve the maximum DOF (1.64, 1.91, and 1.26) exactly, the eigenbeamforming algorithm requires large symbol extensions but finite. The DOF achievable when $p = 2, 1$ and 1,

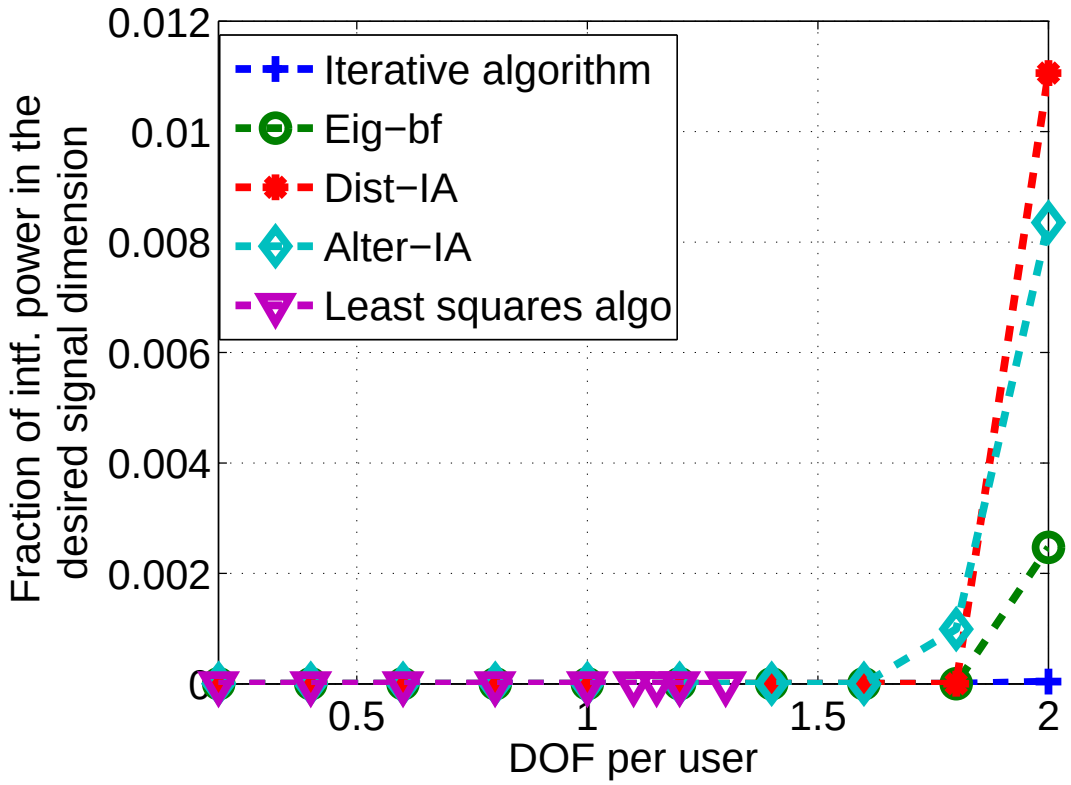


Figure 5.2: Fraction of the interference power in the desired signal space for the $K = 4$ user IC with configuration $M = 3$, $N = 7$, and $S = 5$.

from (5.23), reduce to 1.6, 1.8 and 1.25, respectively. Thus, the eigenbeamforming method is able to achieve very near to the DOF values predicted by the feasibility conditions derived in Sec. 5.2.1.

Figures 5.4, 5.5 and 5.6 show the relative power in the weakest desired data stream (denoted q_{avg} above) in the $\log_{10}$ scale versus the DOF per user for the 4-user (Figs. 5.4, 5.5) and 5-user (Fig. 5.6) IC with $M \times N = 3 \times 6$, 3×7, and 2×6, respectively. The non-zero value of q_{avg} confirms that the DOF of the desired signal is preserved. For the iterative algorithm, q_{avg} is proportional to $1/Sd$, where d is the DOF per user, due to the scaled identity constraint on the effective channel matrix in (5.27) and (5.41). The

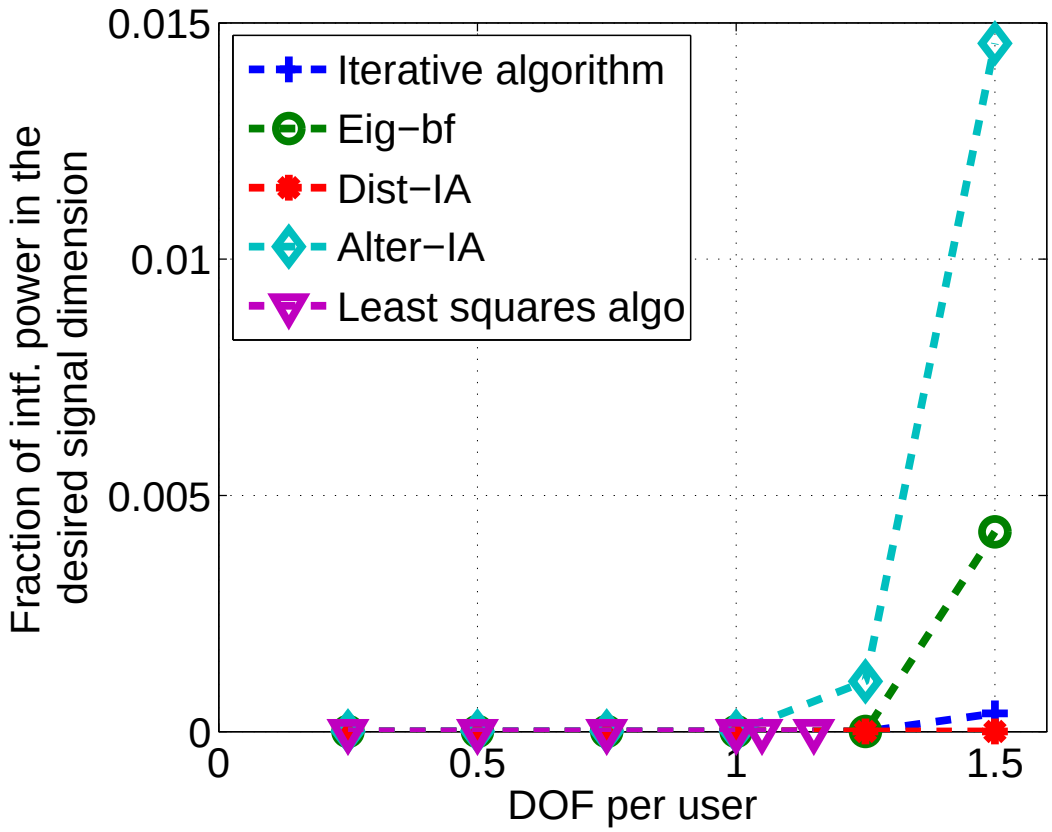


Figure 5.3: Fraction of the interference power in the desired signal space for the $K = 5$ user IC with configuration $M = 2$, $N = 6$ and $S = 4$.

utility of the second performance metric (q_{avg}) is clear from the graphs, as it captures the possible loss of desired signal dimension when the interference is aligned at all the receivers (e.g., Fig. 5.6, as mentioned above).

Fig. 5.7 shows the sum rate of the users per channel use versus the power in dB for the $K = 4$ user IC with $M = 3$, $N = 6$. In this example, each user transmits 8 streams over $S = 5$ symbol extensions, which represents a target sum DOF of 6.4 per symbol extension. The eigenbeamforming algorithm aligns two interfering data streams at each receiver, and it outperforms all the other algorithms in terms of sum rate and achieves

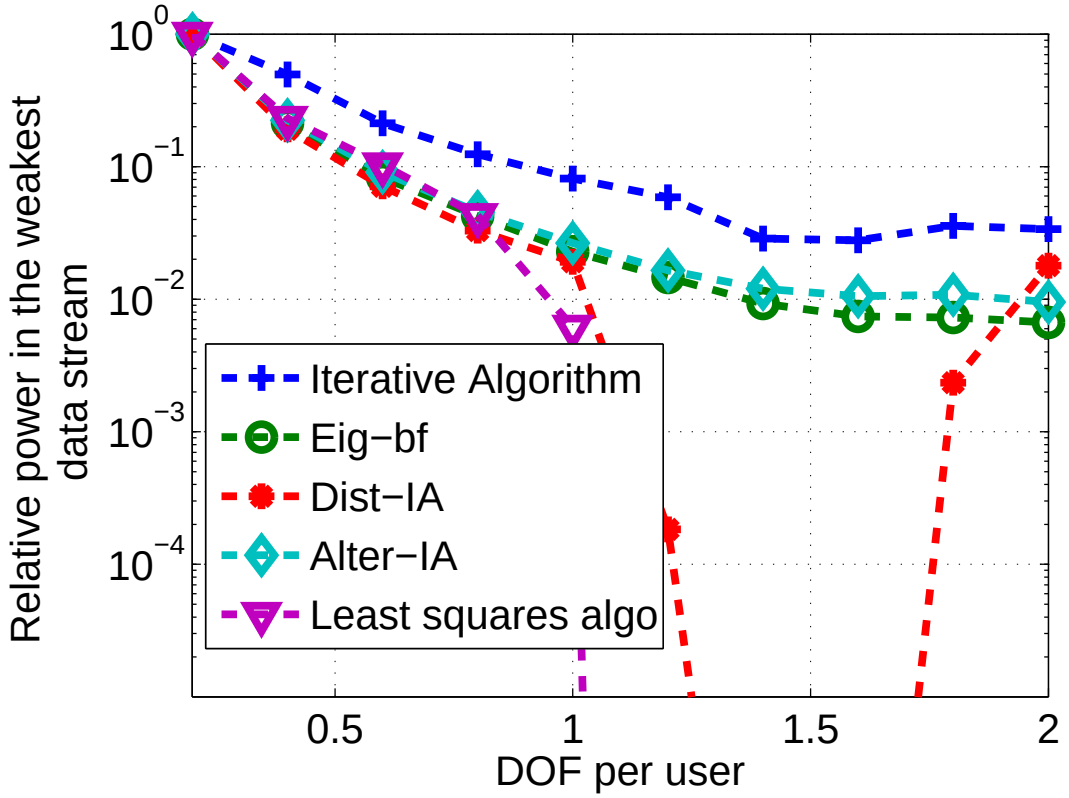


Figure 5.4: Relative power in the weakest desired signal data stream for the $K = 4$ user IC with configuration $M = 3$, $N = 6$, and $S = 5$.

a sum DOF of about 6.38. In the high SNR regime, the iterative algorithm performs the second best, and has the same performance as the Alter-IA algorithm. As the least-squares method is unable to attain the target desired signal dimension (as also seen in Fig. 5.4), its sum rate fails to achieve the target DOF. Thus, the proposed algorithms are able to handle the block-diagonal structure of the channel matrices resulting from the channel extension, which is contrary to existing algorithms which converge to local minima without achieving zero interference leakage. In summary, the above examples illustrate the performance benefits offered by the proposed algorithms relative to existing algorithms, in terms of the performance metrics considered in this chapter.

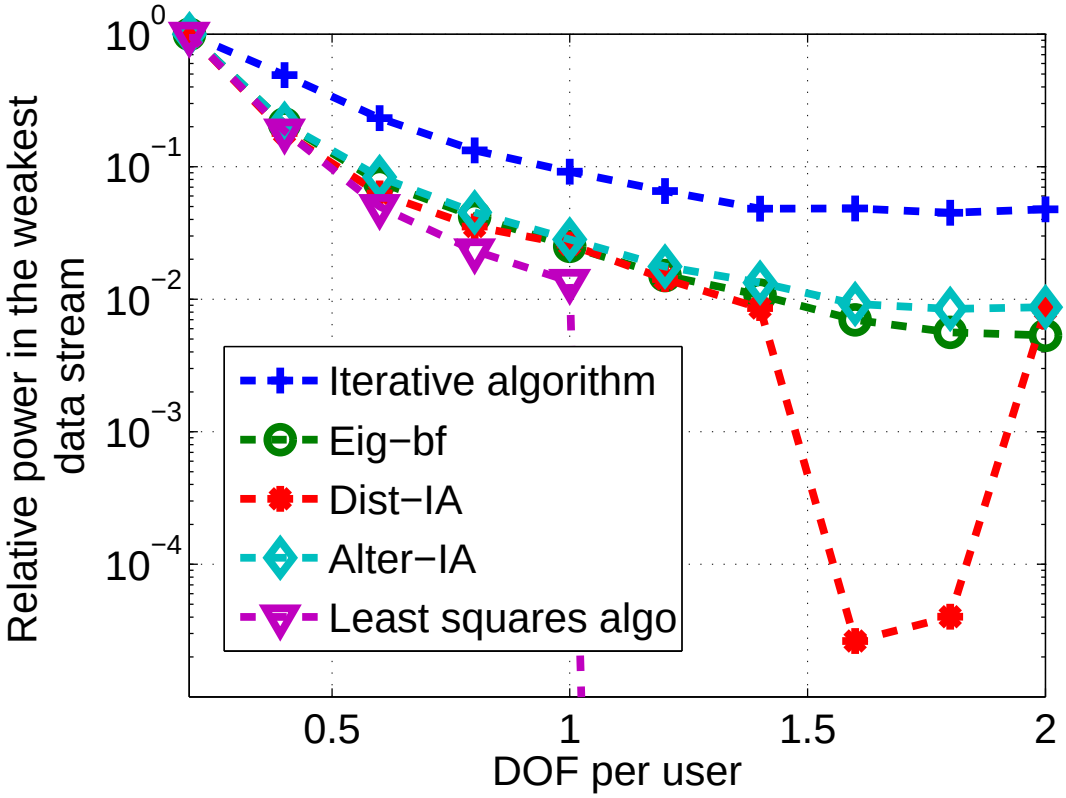


Figure 5.5: Relative power in the weakest desired signal data stream for the $K = 4$ user IC with configuration $M = 3$, $N = 7$, and $S = 5$.

5.5 Conclusions

This chapter explored the construction of precoding and receive filtering matrices for IA for constant or quasi-static MIMO channels with finite symbol extensions. Most precoder and receive filter design algorithms in the literature formulate the IA problem as an interference leakage minimization problem, and thus may not achieve perfect IA or may not achieve the required desired signal dimensionality. A new metric was proposed to measure the performance of IA algorithms, that captured the possible loss in signal dimension when the desired signal is aligned with the interference. Inspired by the metric, two algorithms for finding the precoding and receive filtering matrices for

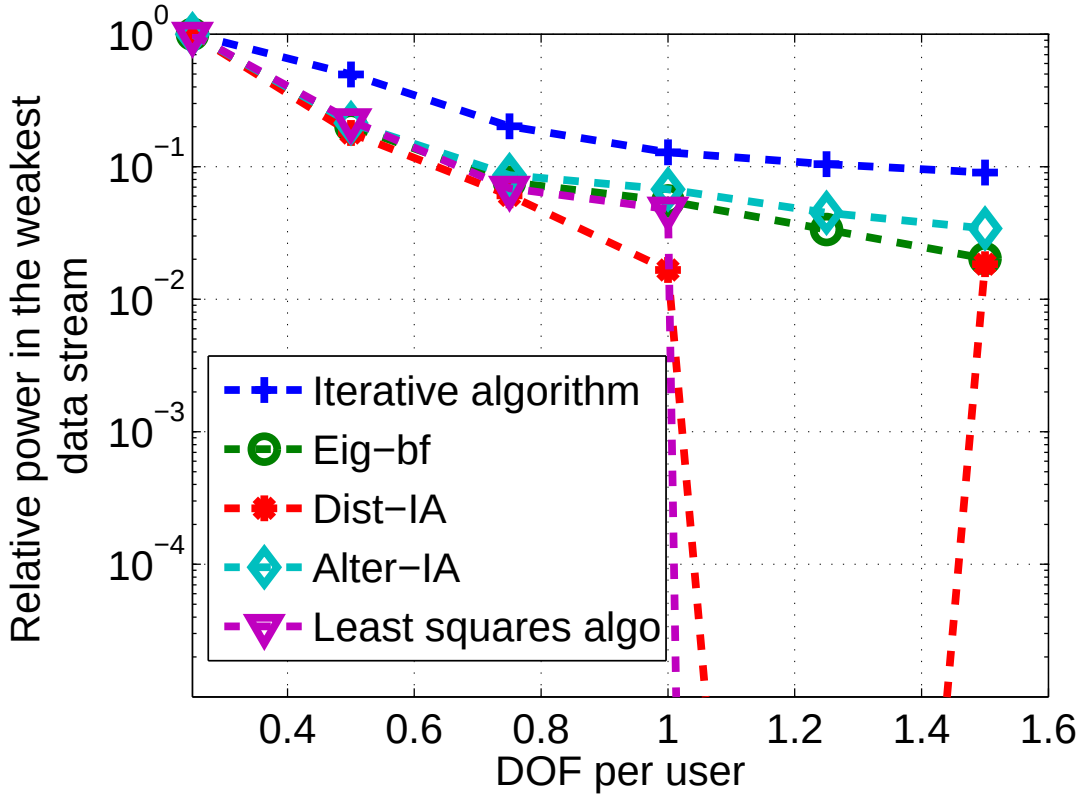


Figure 5.6: Relative power in the weakest desired signal data stream for the $K = 5$ user IC with configuration $M = 2$, $N = 6$, and $S = 4$.

IA were proposed. The first algorithm was based on sub-stream alignment at all the receivers, and the second algorithm was designed to ensure that the desired signal dimension is maintained, while minimizing the interference leakage power. The second algorithm had the added advantage of requiring limited channel knowledge at each terminal, at the price of an iterative solution. The performance of the algorithms were evaluated using Monte Carlo simulations and compared with the existing algorithms for IA precoder design. It was illustrated that the proposed algorithms outperform the existing IA algorithms in terms of the performance metrics considered. In the next

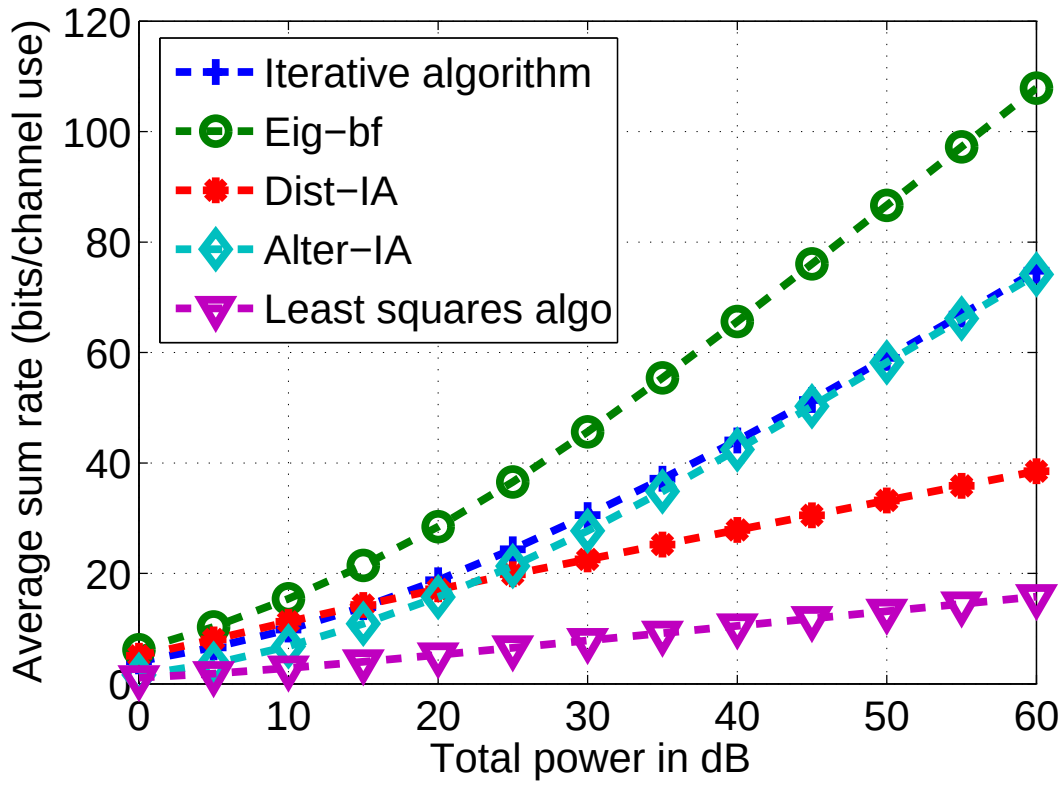


Figure 5.7: Sum rate of the $K = 4$ user IC with configuration $M = 3$, $N = 6$, and $S = 5$.

chapter, the role of transmitter cooperation on managing interference and ensuring secrecy is studied in depth, in the context of the 2-user IC.

Chapter 6

Achievable Schemes for Secrecy in SLDIC with Limited-rate Transmitter Cooperation

As mentioned earlier, in a multiuser wireless communication system, users experience interference due to the broadcast and superposition nature of the medium. Interference not only limits the performance of the system, but also allows users to eavesdrop on the other users' messages. For example, in a cellular network, when users have subscribed to different contents, it is important for the service provider to support high throughput, as well as secure its transmissions, in order to maximize its own revenue. In these scenarios, the transmitters (e.g., base stations) are not completely isolated from each other, and cooperation among them is possible. Such cooperation can potentially provide significant gains in the achievable throughput in the presence of interference, while simultaneously guaranteeing security. Hence, the objective of this chapter is to explore the role of transmitter cooperation in managing interference and ensuring secrecy in the case of 2-user symmetric linear deterministic IC (SLDIC) with limited-rate

transmitter cooperation and secrecy constraints at the receivers.

The notion of information theoretic secrecy was introduced in [11], where secret communication between the transmitter and receiver in the presence of an eavesdropper was considered. Subsequently, in [32], the wiretap channel was introduced, where the legitimate transmitter and receiver communicate in the presence of an eavesdropper, and the eavesdropper listens through a degraded channel. The wiretap channel is generalized in [70], where a general (non-degraded) broadcast channel is assumed, and the transmitter sends common information to the legitimate receiver and eavesdropper along with a confidential message intended for the legitimate receiver. These works exploit the fact that even though the signal has originated from the same source, the signal may arrive at the legitimate receiver and the eavesdropper through different channels.

A linear deterministic model for relay network was introduced in [18], which led to insights on the achievable schemes in Gaussian relay networks. The deterministic model has subsequently been used for studying the achievable rates with the secrecy constraints in [21–23]. In [21], secret communication over the IC is analyzed with two types of secrecy constraints: in the first case, the secrecy constraint is specific to the agreed-upon signaling strategy, and in the second case, the secrecy constraint takes into account the fact that the other users may deviate from the agreed-upon strategy. The deterministic model has also been studied under different eavesdropper settings in [22,23,71].

However, the role of limited transmitter-side cooperation on secrecy in an IC has not been explored in literature, and is the focus of this chapter. Due to the cooperation between the transmitters and the secrecy constraints at the receivers, the encoding at

the transmitter becomes complex and even deriving outer bounds become difficult. In order to make headway into this problem, first, the related problem of the linear deterministic setting is considered. For the symmetric linear deterministic IC (SLDIC) with cooperating transmitters and secrecy constraints at the receivers, achievable schemes are obtained in this chapter. Outer bounds on the secrecy rate are derived in Chapter 7.

In this chapter, novel transmission schemes for the 2-user SLDIC with limited transmitter cooperation and secrecy constraints at the receivers are proposed, and their achievable secrecy rates are derived. The transmission scheme depends on the capacity of the cooperative link (denoted by C) and value of $\alpha \triangleq \frac{n}{m}$, where $m \triangleq (\lfloor \log \mathsf{SNR} \rfloor)^+$ and $n \triangleq (\lfloor \log \mathsf{INR} \rfloor)^+$. The key features of the proposed schemes are:

1. In the weak interference regime[1] $(0 < \alpha \leq \frac{2}{3})$, the scheme involves precoding of a user's own data bits with the bits received through cooperation, to simultaneously cancel the interference and ensure secrecy.

2. In the moderate interference regime $(\frac{2}{3} < \alpha < 1)$, the scheme uses interference cancelation, random bit transmission, or both. The novel idea behind the random bit transmission scheme is explained in Sec. 6.2.2.

3. In the high interference regime $(1 < \alpha < 2)$, the scheme involves relaying of the other user's data bits obtained at the transmitters through the cooperative links, in addition to the techniques used for $(\frac{2}{3} < \alpha < 1)$.

4. In the very high interference regime $(\alpha \geq 2)$, the scheme uses time sharing, along with the techniques used for $(1 < \alpha < 2)$. Unlike the other interference regimes,

[1]Note that the definition of the weak interference regime here is different from the more typical $(0 < \alpha \leq \frac{1}{2})$ [8]. It will turn out that $(0 < \alpha \leq \frac{2}{3})$ is more appropriate for the discussion in this chapter.

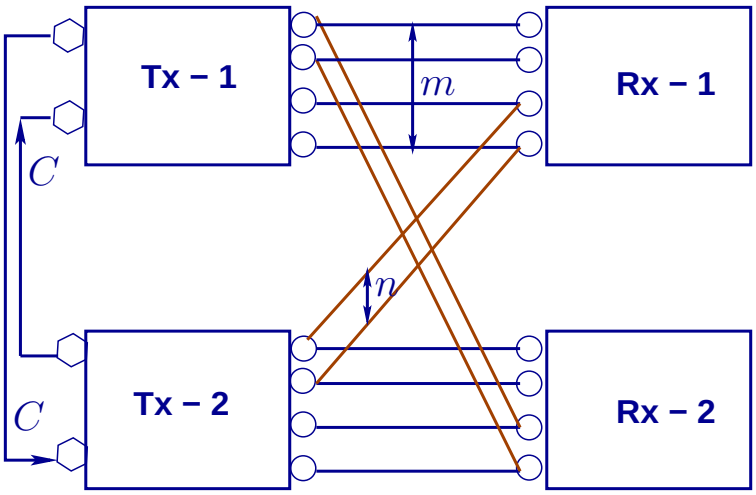


Figure 6.1: 2-user SLDIC with transmitter cooperation.

when $\alpha \geq 2$ and for small values of C, sharing random bits along with the data bits is strictly better than sharing only data bits, in terms of the achievable secrecy rate.

6.1 System model

The deterministic model of 2-user symmetric IC with limited-rate transmitter cooperation [20] is shown in Fig. 6.1. The received signals at the receivers are modeled as follows:

$$\mathbf{y}_1 = \mathbf{D}^{q-m}\mathbf{x}_1 \oplus \mathbf{D}^{q-n}\mathbf{x}_2;\ \mathbf{y}_2 = \mathbf{D}^{q-m}\mathbf{x}_2 \oplus \mathbf{D}^{q-n}\mathbf{x}_1, \tag{6.1}$$

where $\mathbf{x}_i$ and $\mathbf{y}_i$ are binary vectors of length $q \triangleq \max\{m, n\}$, $\mathbf{D}$ is a $q \times q$ downshift matrix with elements $d_{j',j''} = 1$ if $2 \leq j' = j'' + 1 \leq q$ and $d_{j',j''} = 0$ otherwise, and $\oplus$ stands for modulo-2 addition (XOR operation). Both the transmitters cooperate through a loss less and secure link but of finite capacity. The quantity $\alpha \triangleq \frac{n}{m}$ captures the amount of

coupling between the signal and the interference, and is central to characterizing the achievable rates in the case of SLDIC.

The convention followed for denoting the bits transmitted over the LDIC is the same as that presented in [20]. The bits $a_i, b_i \in \mathcal{F}_2$ denote the information bits of transmitters 1 and 2, respectively, sent on the i^{th} level, with the levels numbered starting from the bottom-most entry. The data bits transmitted on the different levels of SLDIC are chosen to be equiprobable Bernoulli distributed, denoted $\mathrm{Bern}\left(\frac{1}{2}\right)$.

The transmitter i has a message W_i, which should be decodable at the intended receiver i, but needs to be kept secret from the other, unintended receiver j, $j \neq i$. The encoded message is a function of its own data bits, the bits received through the cooperative link, and possibly some random data bits. The encoding at the transmitter should satisfy the causality constraint, i.e., it cannot depend on future cooperative bits. The decoding is based on solving the linear equation in (6.1) at each receiver. For secrecy, it is required to satisfy $I(W_i, \mathbf{y}_j) = 0, i, j \in \{1, 2\}$ [11]. Also, it is assumed that the transmitters trust each other completely and that they do not deviate from the agreed scheme.

6.2 SLDIC: Achievable schemes

6.2.1 Weak interference regime $(0 \leq \alpha \leq \frac{2}{3})$

In this regime, the proposed scheme uses interference cancelation. It is easy to see that data bits transmitted on the lower $m - n$ levels $[1 : m - n]$ remain secure, as these data bits do not cause interference at the unintended receiver. Hence, $m - n$ bits can be sent securely, when $C = 0$, as shown in Fig. 6.2. However, with cooperation $(C > 0)$, the

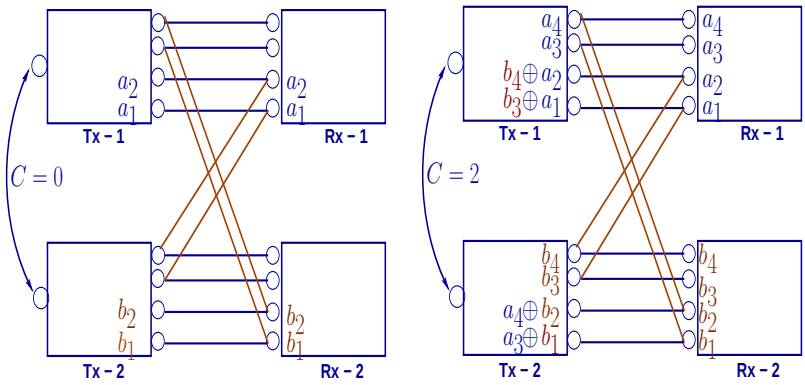


Figure 6.2: SLDIC with $m = 4$ and $n = 2$: (a) $C = 0$ and $R_s = 2$ and (b) $C = 2$ and $R_s = 4$.

top levels $[m - n + 1 : m]$ can be used for data transmission by appropriately xoring the data bits with the cooperative bits in the lower levels prior to transmission. These cooperative bits are precoded (xored) with the data bits at the levels $[1 : \min\{n, C\}]$ to cancel interference caused by the data bits sent by the other transmitter. When $C = n$, it can be shown that the proposed scheme achieves the maximum possible rate of $\max\{m, n\}$ bits. When $C > n$, $C - n$ bits can be discarded and n cooperative bits can be used for encoding as above, to achieve $\max\{m, n\}$ bits. Hence, in the sequel, it will not be explicitly mentioned that $C \leq n$. The proposed encoding scheme achieves the following symmetric secrecy rate:

$$R_s = m - n + C. \tag{6.2}$$

The details of the encoding scheme and the derivation of (6.2) can be found in Appendix C.1.

6.2.2 Moderate interference regime $(\frac{2}{3} < \alpha < 1)$

In this regime, the proposed scheme uses interference cancelation along with the transmission of random bits. Without transmitter cooperation, at least $m-n$ bits can be sent securely, as in the weak interference regime. Depending on the value of C, with the help of transmission of random bits, additional data bits on the higher levels $[m-n+1:m]$ are sent by carefully placing data bits along with zero bits and random bits.

The proposed scheme achieves the following symmetric secrecy rate:

$$R_s = m - n + B(m-n) + q + C, \tag{6.3}$$

where $B \triangleq \left\lfloor \frac{g}{3r_2} \right\rfloor$, $g \triangleq \{n-(r_2+C)\}^+$, $r_2 \triangleq m-n$, $q \triangleq \min\{(t-r_2)^+, r_2\}$ and $t \triangleq g\%\{3r_2\}$.

In the above equation, the first term corresponds to the number of data bits transmitted securely without using random bits transmission or cooperation. The term $B(m-n)+q$ corresponds to the number of data bits that can be securely transmitted using the help of random bits transmission. The last term C represents the gain in rate achievable due to cooperation. The details of the encoding scheme and the derivation of (6.3) can be found in Appendix C.2.

6.2.3 Interference is as strong as the signal $(\alpha = 1)$

In this case, from Theorem 17 in Chapter 7, it is not possible to achieve a nonzero secrecy rate.

6.2.4 High interference regime $(1 < \alpha < 2)$

The achievable scheme is similar to that proposed for the moderate interference regime, but it differs in the manner the encoding of the message is performed at each transmitter. The proposed scheme achieves the following secrecy rate:

1. When $(1 < \alpha \leq 1.5)$:

$$R_s = B(n-m) + q + C, \tag{6.4}$$

where $B \triangleq \left\lfloor \frac{g}{3r_2} \right\rfloor$, $g \triangleq (m-C)^+$, $q \triangleq \min\{(t-r_2)^+, r_2\}$, $t \triangleq g\%\{3r_2\}$ and $r_2 \triangleq n-m$.

2. When $(1.5 < \alpha < 2)$:

$$R_s = \begin{cases} 2m - n + C & \text{for } 0 \leq C \leq 4n-6m \\ 4n - 6m + C_{T_1} + C_{T_2} + C_{T_3} + r_d & \text{for } 4n-6m < C \leq n, \end{cases} \tag{6.5}$$

where $C_{T_1} \triangleq \min\left\{\left\lceil \frac{C_{\text{rem}}}{2} \right\rceil, 2m-n\right\}$, $C_{\text{rem}} \triangleq (C' - C_{T_3})^+$, $C_{T_3} \triangleq \min\{2m-n, C''\}$, $C' \triangleq C - (4n-6m)$, $C'' \triangleq \left\lceil \frac{C'}{3} \right\rceil$, $C_{T_2} \triangleq \min\{2m-n, (C_{\text{rem}} - C_{T_1})^+\}$ and $r_d \triangleq \min\{2m-n-C_{T_3}, 2m-n-C_{T_2}\}$.

The details of the encoding scheme and some illustrative examples can be found in Appendix C.3.

Remark: One can note that the achievable schemes for the moderate (Sec. 6.2.2) and high interference regime (Sec. 6.2.4) use a combination of interference cancelation and transmission of a jamming signal (random bits transmission). When precoding is done using the other user's signal, it cancels the interference and also ensures secrecy. In the technique based on random bits transmission, the transmitter self-jams its own receiver,

so that the receiver cannot decode the other user's data. But, in this process, transmitter causes interference to the other receiver, thereby adversely impairing the achievable rate of secure communication. Thus, self jamming in that form only helps if the benefit to the secrecy rate due to the interference caused at the own receiver outweighs the negative impact of the interference caused at the other receiver. However, when the jamming signal can be canceled at an unintended receiver by transmission of the same random bits by the other transmitter, its adverse impact is completely alleviated, leading to larger achievable rates.

6.2.5 Very high interference regime $(\alpha \geq 2)$

In this case, when $C = 0$, it is not possible to achieve nonzero secrecy rate as established by the outer bound in Theorem 15. However, with cooperation $(C > 0)$, the proposed scheme can achieve a nonzero secrecy rate. The proposed scheme uses interference cancelation, time sharing, and relaying the other user's data bits. In contrast to the achievable schemes for other interference regimes, the transmitters exchange data bits, random bits, or both, depending on the capacity of the cooperative link. For example, when $0 < C \leq \lceil \frac{m}{2} \rceil$, the transmitters exchange only random bits. The proposed scheme achieves the following secrecy rate:

1. When m is even:

$$R_s = \begin{cases} 2C & \text{for } 0 < C \leq \frac{m}{2} \\ \frac{m}{2} + C & \text{for } \frac{m}{2} < C \leq n - \frac{3m}{2} \\ \frac{n}{2} - \frac{m}{4} + \frac{C}{2} & \text{for } n - \frac{3m}{2} < C < n - \frac{m}{2} \\ C & \text{for } n - \frac{m}{2} \leq C \leq n. \end{cases} \tag{6.6}$$

2. When m is odd:

$$R_s = \begin{cases} \min\{2C, m\} & \text{for } 0 < C \leq \frac{m+1}{2} \\ m + \min\left\{C - \frac{m+1}{2}, n - 2m\right\} & \text{for } \frac{m+1}{2} < C \leq \frac{2n-3m+1}{2} \\ n - 2m + \frac{1}{2}\left[C_1^{ul} + 2C_1^{uu} + C_2^{uu} + C_1^{lu} + C_2^{ul}\right] & \text{for } \frac{2n-3m+1}{2} < C \leq n, \end{cases} \tag{6.7}$$

where $C_1^{uu} \triangleq \left\lceil \frac{C}{2} \right\rceil$, $C_1^{ul} \triangleq (m - C_1^{uu})^+$, $C_2^{uu} \triangleq (C - C_2^{lu} - C_2^r)^+$, $C_1^{lu} \triangleq (C - C_1^{uu} - C_1^r)^+$, $C_2^{ul} \triangleq C_1^{ll}$, $C_1^{ll} \triangleq \min\{2C_1^r, (m - C_1^{lu})^+)\}$, $C_2^{ll} \triangleq C_1^{ul}$ and $C_2^r \triangleq \max\left\{\left\lceil \frac{C_2^{ll}}{2} \right\rceil, \left\lfloor \frac{C_2^{ul}}{2} \right\rfloor\right\}$, $C_1^r \triangleq \left\lceil \frac{C_1^{ul}}{2} \right\rceil$.

The details of the achievable scheme, and examples, can be found in Appendix C.4.

Remark: When $0 < C \leq \lceil \frac{m}{2} \rceil$, the capacity achieving scheme involves exchanging only random bits through the cooperative links. This is useful in scenarios where the transmitters trust each other to follow the agreed-upon scheme, but are not allowed to share their data bits through the cooperative link.

6.3 Conclusions

This chapter proposed novel achievable schemes for the 2-user SLDIC with transmitter cooperation. The achievable scheme used a combination of interference cancelation, random bit transmission, relaying of the other user's data bits, and time sharing, depending on the values of α and C. Several interesting results were obtained from the proposed achievable schemes. For example, when $\frac{2}{3} < \alpha < 1$ and $1 < \alpha < 2$, random bit transmission helps ensure secrecy. With further increase in the strength of the interference ($\alpha \geq 2$), random bit transmission is rendered ineffective. But, with cooperation, it is possible to achieve a nonzero secrecy rate, even when the interference is very strong.

In the next chapter, outer bounds on the secrecy rate are derived for the SLDIC and the achievable results derived in this chapter are compared with the outer bounds.

Chapter 7

Outer Bounds on the Secrecy Rate of the 2-User SLDIC with Limited-rate Transmitter Cooperation

In the previous chapter, achievable schemes were obtained for the 2-user SLDIC with limited-rate transmitter cooperation with secrecy constraints at the receivers. Deriving outer bounds on the achievable secrecy rate, which is the focus of this chapter, can provide useful insights on the performance limits of the system. Further, in cases where the inner and outer bounds match, one obtains the capacity region of the 2-user SLDIC in those scenarios.

The deterministic model is a good starting point, as it provides critical insight into outer bounds for more general models [19, 20]. Also, the outer bounds derived in [19] helps to establish the capacity region for the deterministic IC. In [20], outer bounds are obtained for the deterministic IC with limited-rate transmitter cooperation without any secrecy constraints at receivers. The outer bounds are found to coincide with the achievable rate region and thereby establishing the optimality of the proposed scheme

in [20]. In [23], the outer bounds derived for the wiretap channel with side information establishes that the proposed scheme achieves capacity. However, outer bounds on the achievable secrecy rate for the 2-user deterministic IC with limited-rate transmitter cooperation have not been derived in the literature, and is the focus of this chapter.

In this chapter, four new outer bounds on the achievable rates are derived for the 2-user SLDIC with limited-rate transmitter cooperation and secrecy constraints at the receivers. The derivation of the outer bounds differ from each other in the way side-information is provided to receiver or the encoded message/output is partitioned based on the value of α, where α captures the amount of coupling between the signal and the interference. The main contributions of this chapter are:

1. Outer bounds on the secrecy rate are derived under different interference regimes for the SLDIC with limited-rate transmitter cooperation (Theorems 14-17).

2. The derivation of the outer bounds is based on providing side information to receivers in a carefully chosen manner, using the secrecy conditions at the receivers and partitioning the encoded message/output depending on the value α. For example, in the moderate interference regime ($\frac{2}{3} \leq \alpha < 1$), the encoded message is partitioned into two parts: one which causes interference at the unintended receiver, and another part which does not cause any interference at the unintended receiver.

3. The outer bound in Theorem 14 helps to establish that sharing *random* bits through the cooperative link can achieve the optimal rate under certain conditions, as mentioned in Section 7.2.1.

The derived outer bounds are compared with the achievable secrecy rate in Chapter 6, to illustrate their usefulness. It is also observed that the proposed outer bounds are tighter than the outer bound without the secrecy constraint [20], in all interference regimes, except for the initial part of the weak interference regime. Further, an outer bound on the capacity of the 2-user SLDIC in the absence of transmitter cooperation is obtained as a special case of the results in this chapter, by setting the capacity of the cooperative link to zero. The corresponding result represents the best known outer bound in this case also.

7.1 SLDIC: Outer bounds

In this section, four outer bounds on the symmetric rate for the 2-user SLDIC with limited-rate cooperation between transmitters and perfect secrecy constraints at the receivers are stated as Theorems 14-17. Theorem 14 is valid for all $\alpha \geq 0$, while Theorems 15, 16, and 17 are valid for $\alpha \geq 2$, $1 < \alpha < 2$, and $\alpha = 1$, respectively. The derivation of the outer bound involves using Fano's inequality, providing side information to receivers in a carefully chosen manner, and using the secrecy constraints at receivers. One of the difficulties faced in deriving these bounds is that the encoded messages at the transmitters are no longer independent due to the cooperation between the transmitters. In order to overcome this problem, one of the key techniques used in obtaining the outer bounds in Theorems 14- refth:theoremSLDIC-outer3 is to partition the encoded message, output, or both, depending on the value of α. This helps to simplify or bound the entropies terms involved in the outer bounds. Also, the following relation helps to establish these outer bounds: conditioned on the cooperating signals,

denoted by $(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N)$, the encoded signals and the messages at the two transmitters are independent [20,72]. This is represented as the following Markov chain relationship:[1]

$$(W_1, \mathbf{x}_1^N) - (\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) - (W_2, \mathbf{x}_2^N). \tag{7.1}$$

Finally, the overall outer bound on the symmetric secrecy rate is obtained by taking the minimum of these outer bounds. The best performing outer bound depends on the value of α and the outer bound on the symmetric secrecy rate $\max(m,n)\mathbf{1}_{\{C>0\}} + \min(m,n)\mathbf{1}_{\{C=0\}}$, where $\mathbf{1}_A$ is the indicator function, equal to 1 if A is true, and equal to 0 otherwise.

In the derivation of the first outer bound, the encoded message $\mathbf{x}_i$ $(i = 1, 2)$ is partitioned into two parts: one part ($\mathbf{x}_{ia}$) which causes interference to the unintended receiver, and another part ($\mathbf{x}_{ib}$) which is not received at the unintended receiver. Partitioning the message in this way helps to obtain an outer bound on $2R_1 + R_2$, which leads to an outer bound on the symmetric secrecy rate. The following theorem gives the outer bound on the symmetric secrecy rate.

Theorem 14. *The symmetric rate of the 2-user SLDIC with limited-rate transmitter cooperation and secrecy constraints at the receivers is upper bounded as:*

$$R_s \leq \begin{cases} \frac{1}{3}\left[2C + 3m - 2n\right] & \text{for } \alpha \leq 1 \\ \frac{1}{3}\left[2C + n\right] & \text{for } \alpha > 1. \end{cases} \tag{7.2}$$

Proof. The proof is provided in Appendix D.1. □

The next outer bound, stated as Theorem 15, focuses on the very high interference

[1] In Chapters 7-9, N denotes the number of channel uses, and not the number of antennas at each receiver as mentioned in the previous chapters.

regime, i.e., for $\alpha \geq 2$. In the derivation of the bound, the encoded message $\mathbf{x}_i$ $(i = 1, 2)$ at each transmitter is partitioned into three parts, as shown in Fig. 7.1a. The partitioning is based on whether (a) the bits are received at the intended receiver, and are received at the other receiver without interference, (b) the bits are not received at the desired receiver, and received without interference at the other receiver, and (c) the bits are not received at the intended receiver, and are received with interference at the other receiver. To motivate the development of the following outer bound, first consider the $C = 0$ case. If receiver 1 can decode $\mathbf{x}_{1a}$ sent by transmitter 1, then receiver 2 can decode $\mathbf{x}_{1a}$ as well, since it gets these data bits without any interference. Hence, data bits cannot be sent securely on those levels. Data transmitted at the remaining levels are not received by receiver 1, so they cannot be used for secure data transmission either. Now, suppose a genie provides receiver 1 with the part of the signal sent by transmitter 1 that is received without any interference at receiver 2, i.e., $\mathbf{y}_{2a}^N \triangleq (\mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N)$. Then, by using the secrecy constraint for the receiver 2, the rate of user 1 is upper bounded by $I(W_1; \mathbf{y}_1^N | \mathbf{y}_{2a}^N)$. When $\alpha \geq 2$, the following holds:

$$\begin{aligned} & I(W_1; \mathbf{y}_2^N) = 0, \\ \text{or } & I(W_1; \mathbf{y}_{2a}^N, \mathbf{y}_{2b}^N) = 0, \text{ where } \mathbf{y}_{2b}^N = \mathbf{x}_{2a}^N \oplus \mathbf{x}_{1c}^N, \\ \text{or } & I(W_1; \mathbf{y}_{2a}^N) + I(W_1; \mathbf{y}_{2b}^N | \mathbf{y}_{2a}^N) = 0. \end{aligned} \tag{7.3}$$

When $C > 0$, by using the above mentioned approach and the relation in (7.1), an outer bound on the symmetric secrecy rate is derived for $\alpha \geq 2$, and is stated as the following theorem.

Theorem 15. *In the very high interference regime, i.e., for $\alpha \geq 2$, the symmetric rate of the*

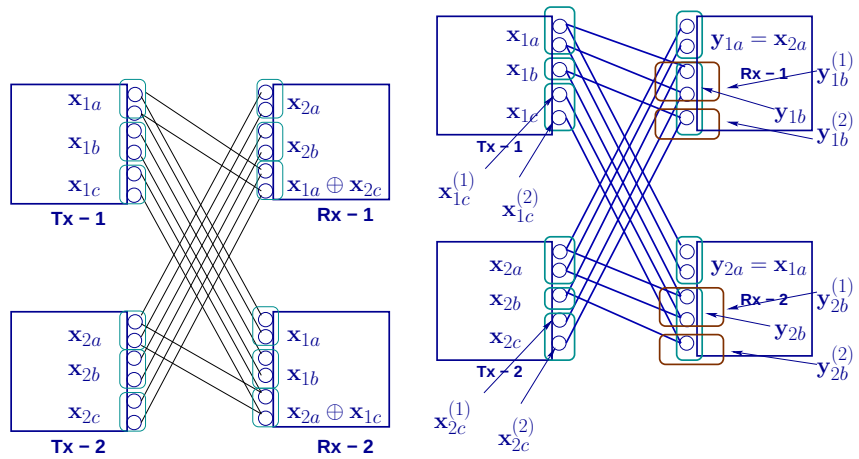


Figure 7.1: (a) SLDIC with $m = 2$ and $n = 6$ and (b) SLDIC with $m = 3$ and $n = 5$: Illustration of partitioning of the encoded message/output.

2-user SLDIC with limited-rate transmitter cooperation and secrecy constraints at the receivers is upper bounded as: $R_s \leq 2C$.

Proof. The proof is provided in Appendix D.2. □

Remark: Theorem 15 implies that, for $\alpha \geq 2$, a rate greater than $2C$ cannot be achieved, regardless of m and n. In particular, when $C = 0$, i.e., without cooperation, it is not possible to achieve a nonzero rate. The third outer bound, stated as Theorem 16 below, is applicable in the high interference regime, i.e., $1 < \alpha < 2$. The derivation of the outer bound involves partitioning of the output and the encoded message based on whether the bits are received with interference at the intended receiver, or causes interference to the other receiver, as shown in Fig. 7.1b. The outer bound on the symmetric secrecy rate for the high interference regime is stated in the following theorem.

Theorem 16. *In the high interference regime, i.e., for* $1 < \alpha < 2$, *the symmetric rate of the 2-user SLDIC with limited-rate transmitter cooperation and secrecy constraints at the receivers is upper bounded as:* $R_s \leq 2C + 2m - n$.

Proof. The proof is provided in Appendix D.3. □

The following theorem gives the outer bound on the symmetric secrecy rate for the $\alpha = 1$ case. In this case, both the receivers see the same signal. Hence, it is possible for receiver 2 decode any message that receiver 1 is able to decode, and vice-versa. Therefore, a nonzero secrecy rate cannot be achieved, irrespective of C.

Theorem 17. *When $\alpha = 1$, the symmetric rate of the 2-user SLDIC with limited-rate transmitter cooperation and secrecy constraints at the receivers is upper bounded as: $R_s = 0$.*

Proof. The proof is provided in Appendix D.4. □

A consolidated expression for the outer bound, obtained by taking minimum of the outer bounds in Theorems 14-17, is stated as the following corollary. In particular, the minimum of the outer bounds in Theorems 14 and 16 is taken for the high interference regime, and the minimum of the outer bounds in Theorems 14 and 15 is taken in the very high interference regime.

Corollory 1. *An outer bound on the symmetric secrecy rate of the SLDIC obtained, by taking the minimum of the outer bounds derived in this work, is:*

$$\frac{R_s}{m} \leq \begin{cases} \frac{2\beta}{3} - \frac{2\alpha}{3} + 1 & \textit{for } \alpha < 1 \\ 0 & \textit{for } \alpha = 1 \\ \frac{2\beta}{3} + \frac{\alpha}{3} & \textit{for } 1 < \alpha < 2, \beta > \alpha - \frac{3}{2} \textit{ or } \alpha \geq 2, \beta > \frac{\alpha}{4} \\ 2\beta - \alpha + 2 & \textit{for } \frac{3}{2} < \alpha < 2, 0 \leq \beta < \alpha - \frac{3}{2} \\ 2\beta & \textit{for } \alpha \geq 2, 0 \leq \beta \leq \frac{\alpha}{4}, \end{cases} \tag{7.4}$$

where $\beta \triangleq \frac{C}{m}$.

7.2 Results and discussion

Now, some numerical examples are considered for the deterministic case, to get insights into the bounds for different values of C, over different interference regimes.

In Fig. 7.2, the outer bound in Theorem 14 is plotted along with the achievable secrecy rate given in (6.3) for the $(m, n) = (5, 4)$ case. Also plotted is the per user capacity of the SLDIC with transmitter cooperation, but without the secrecy constraints [20]. It can be observed that the proposed scheme is optimal, when $C = 1$ and $C \geq 4$. However, it is not possible to achieve the capacity without the secrecy constraint, when $C \leq 3$. When $C \geq 4$, there is no loss in the achievable rate due to the secrecy constraint at receivers.

In Fig. 7.3, the minimum of the outer bounds in Theorems 14 and 15 is plotted as a function of C, with $(m, n) = (3, 6)$. Also plotted is the achievable secrecy rate in (6.7). From the plot, it can be observed that a nonzero secrecy rate cannot be achieved without cooperation between the transmitters, i.e., when $C = 0$. The achievable scheme, which uses random bits sharing through the cooperative link and interference cancelation, is optimal for $C = 1$. It can be observed the secrecy constraint results in a positive rate penalty, in the sense that it is not possible to achieve the capacity without the secrecy constraint, for $C \leq 5$.

In Figs. 7.4 and 7.5, the outer bound on the symmetric rate is plotted against α for a given value of C, along with the per user capacity of the SLDIC with transmitter cooperation, but without the secrecy constraints [20], and the inner bounds for the SLDIC with secrecy constraints at the receiver. In order to generate these plots, m is chosen to be 400 and n is varied from 0 to $4m$, and the rates are normalized by m.

In Fig. 7.4, the achievable secrecy rate and the capacity without secrecy constraints [20]

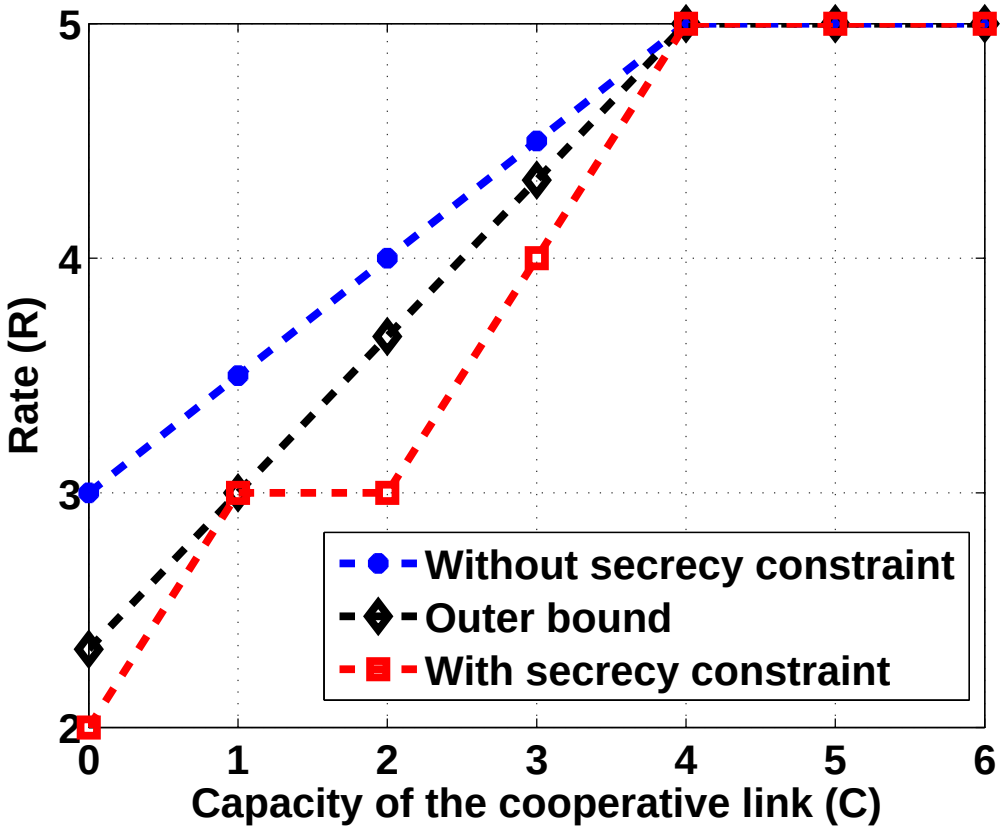


Figure 7.2: Bounds on the secrecy rate of the SLDIC with $m = 5$ and $n = 4$.

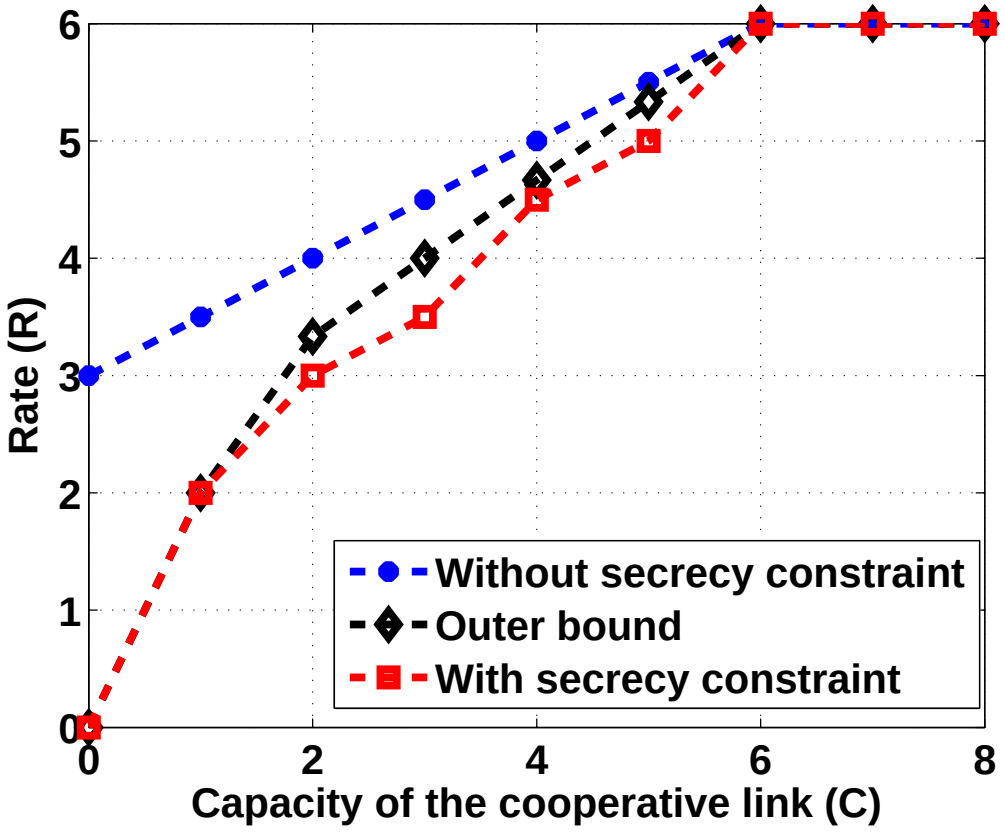


Figure 7.3: Bounds on the secrecy rate of the SLDIC with $m = 3$ and $n = 6$.

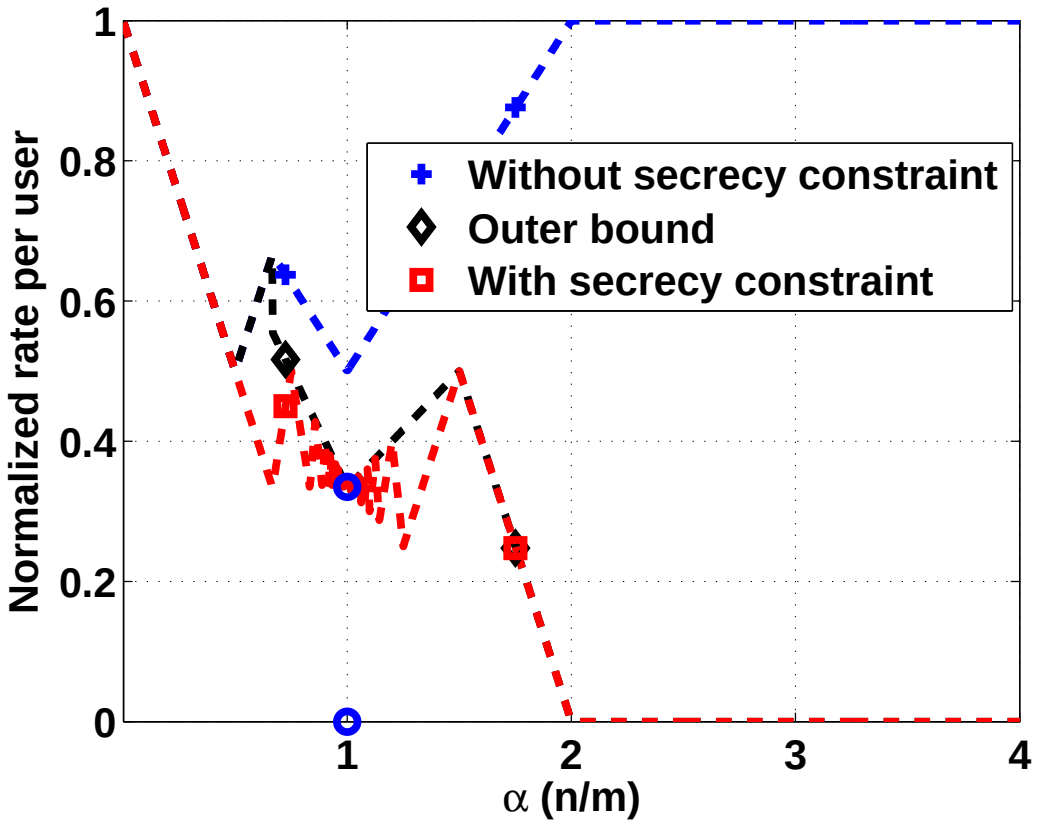


Figure 7.4: Normalized rate for the SLDIC with $C = 0$.

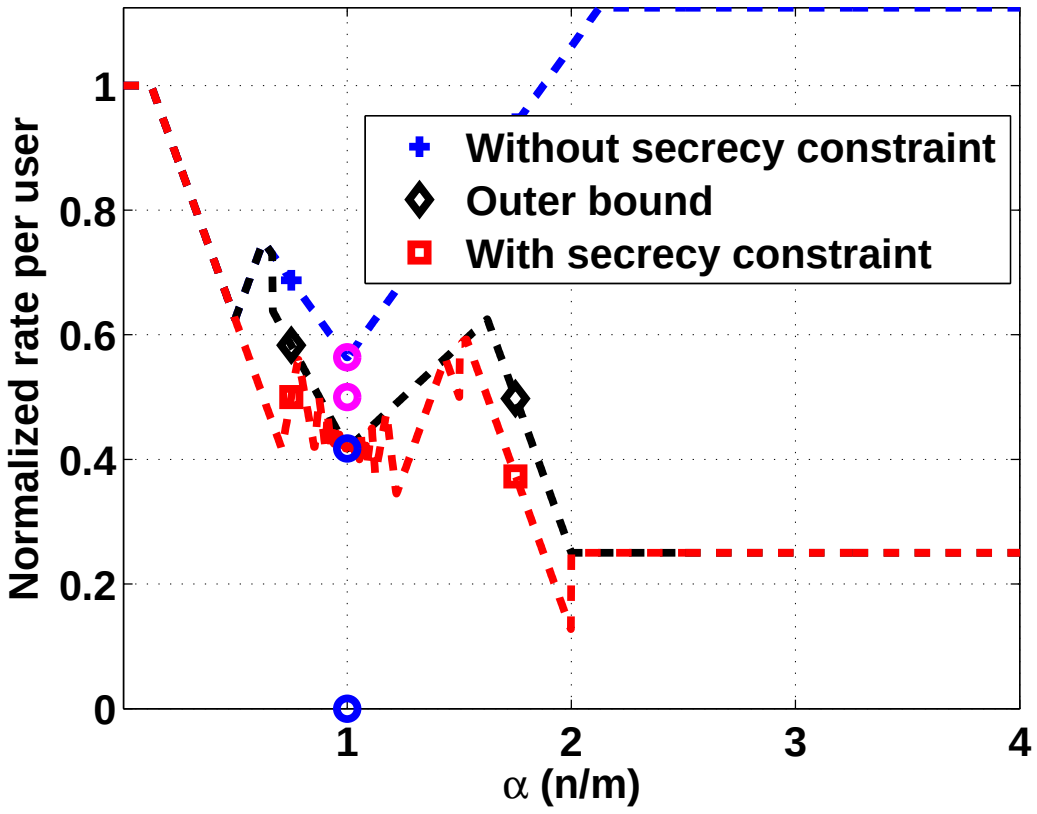


Figure 7.5: Normalized rate for the SLDIC with $C = 50$.

match when $0 \leq \alpha \leq \frac{1}{2}$. Hence, for this regime, it is not required to derive an outer bound. When $\frac{1}{2} < \alpha \leq \frac{2}{3}$, in the absence of the secrecy constraint, the capacity increases with increase in the value of α, as the receivers are able to decode some part of the interference. However, with the secrecy constraint, the receiver cannot decode the other user's message, and, hence, the achievable rate decreases with α. When $\frac{2}{3} < \alpha < 1$, the achievable secrecy rate meets the outer bound at some of the points and the fluctuating behavior of the achievable rate is due to the floor-operation involved in the rate expression. In this regime, the transmission of random bits help to compensate for the loss in rate, to some extent. At $\alpha = 1$, there exists a point of discontinuity, as no nonzero secrecy rate is achievable. Intuitively, one would expect that the achievable secrecy rate should monotonically decrease with α, because of the reasoning mentioned above. Interestingly, the achievable secrecy rate increases with increase in the value of α, when $1 < \alpha \leq 1.5$, although the increase is not monotonic in nature due to the floor operation involved in the rate expression. The increase in the achievable secrecy rate arises due to the improved ability of the transmitters to jam the data bits at the unintended receivers by sending random bits as, α increases. However, when $1.5 < \alpha < 2$, the achievable secrecy rate decreases with increase in the value of α and the outer bound meets the inner bound. When $\alpha \geq 2$, it is no longer possible to achieve a nonzero secrecy rate.

In Fig. 7.5, compared to the $C = 0$ case, the achievable secrecy rate is higher in all the interference regimes due to the cooperation, except when $\alpha = 1$. The cooperation between the transmitters not only eliminates the interference, but at the same time ensures secrecy. Also, the need of transmitting random bits decreases with increase in the value of C. Interestingly, the proposed scheme can achieve a nonzero secrecy rate even

when $\alpha \geq 2$, and the achievable scheme is optimal in this case.

7.2.1 Further remarks

From the derived bounds, the following observations can be made:

1. When $C = 0$ and $\alpha = \frac{1}{2}$, the achievable rate result for the SLDIC in Sec. 6.2.1 reduces to the achievable rate result for the SLDIC in [21] with semi-secret constraint at each receiver. The semi-secret constraint at each receiver depends on trusting the other transmitters.

2. When $(0 \leq \alpha \leq \frac{1}{2})$, the achievable rate result for the SLDIC in Sec 6.2.1 is found to match with the achievable result for the SLDIC in [20] (See Figs. 7.4 and 7.5). As α increases, in [20], the receiver can decode some part of interference and can achieve higher rate. Here, due to the secrecy constraints, the receivers cannot decode other users' messages, and hence, the achievable scheme is completely different. Also, for some values of α, the achievable scheme proposed in Chapter 6 for the SLDIC requires the exchange of only random bits through the cooperative link, in contrast with the achievable scheme in [20].

3. When $(0 \leq \alpha \leq \frac{1}{2})$, the proposed achievable scheme is found to be optimal for all values of C in the SLDIC (See Figs. 7.4 and 7.5).

4. When $(\frac{2}{3} < \alpha < 1)$, data bits are transmitted securely in the higher levels by intelligently choosing the placement of data and random bits, in addition to interference cancelation.

5. When $1 < \alpha < 2$ and $C = 0$, it is not possible to ensure secrecy without transmission of random bits in the case of SLDIC.

6. In all the interference regimes, the proposed scheme always achieves nonzero secrecy rate with cooperation (i.e., $C > 0$), except for the $\alpha = 1$ case.

7. When $C = n$ and $\alpha \neq 1$, i.e., when the cooperative link is as strong as the strength of the interference, the proposed scheme achieves the maximum possible rate of $\max\{m, n\}$ in the case of SLDIC.

8. The outer bound in Theorem 15 for $\alpha \geq 2$ helps to establish that sharing random bits through the cooperative link can achieve the optimal rate when $(0 < C \leq \lceil \frac{m}{2} \rceil)$ in the case of SLDIC. From this outer bound, one can also conclude that it is not possible to achieve a per-user rate greater than $2C$, when $\alpha \geq 2$. However, in the other interference regimes, rates greater than $2C$ can be achieved (See Figs. 7.4 and 7.5).

7.3 Conclusions

In this chapter, novel outer bounds on the achievable secrecy rate were derived for the 2-user SLDIC with transmitter cooperation. The derivation of the outer bound was based on providing side information to receiver in a carefully chosen manner, use of the secrecy constraints at the receivers, and partitioning of the encoded message/output, depending on the value of α. The usefulness of these outer bounds was illustrated by comparing them with the achievable secrecy rate derived in Chapter 6. When $0 < \alpha \leq \frac{1}{2}$, the achievable scheme is found to be optimal for all values of C.

When $\alpha \geq 2$, sharing random bits, or data bits, or both, outperforms sharing only data bits through the cooperative links. The derived outer bounds establish that sharing random bits through the cooperative link can achieve the optimal rate when $\alpha \geq 2$ and $(0 < C \leq \lceil \frac{m}{2} \rceil)$. In the next chapter, achievable schemes for the Gaussian symmetric IC with limited-rate transmitter cooperation and secrecy constraints at the receivers are presented.

Chapter 8

Inner Bounds on the Secrecy Rate of the 2-User GSIC with Limited-rate Transmitter Cooperation

As mentioned earlier, the capacity region of the Gaussian IC (GIC) without secrecy constraints at receiver remains an open problem, even in the $K = 2$ user case, except for some special cases like strong/very strong interference regimes [15], [16]. In [12], the broadcast and IC with independent confidential messages are considered and the achievable scheme is based on random binning techniques. The work in [6] demonstrates that with the help of an independent interferer, the secrecy capacity region of the wiretap channel can be enhanced. Intuitively, although the use of an independent interferer increases the interference at both the legitimate receiver and the eavesdropper, the benefit from the latter outweighs the rate loss due to the former. Some more results on the IC under different eavesdropper settings can be found in [36,37,43].

The effect of cooperation on secrecy has been explored in [73–76]. In [73], the effects of user cooperation on the secrecy of multiple access channel with generalized feedback

is analyzed, where the message of each sender needs to be kept secret from each other. In [74], the effects of user cooperation on the secrecy of BC, where the receivers can cooperate with each other is considered. The achievable scheme uses a combination of Marton's coding scheme for BC and a compress and forward scheme for the relay channel. Also, outer bounds on the rate-equivocation region are presented. The role of a relay in ensuring secrecy under different wireless network settings has been studied in [38–40].

The proposed transmission/coding strategy in the Gaussian setting is inspired by the schemes proposed for the 2-user SLDIC in Chapter 6. It uses a superposition of a non-cooperative private codeword and a cooperative private codeword. For the non-cooperative private part, stochastic encoding is used [32], and for the cooperative private part, the cooperative encoding scheme described in Sec. 8.2.1 is used. The codewords corresponding to the cooperate private part are precoded such that the interference caused by the cooperative private codeword of the other user is completely canceled out. This approach is different from the one used in [20], where the interference caused by the unwanted codeword is approximately canceled. Further, one of the users transmits dummy information to enhance the achievable secrecy rate.

8.1 System model

Consider a 2-user GSIC with cooperating transmitters. The signals at the receivers are modeled as

$$y_1 = h_d x_1 + h_c x_2 + z_1; \quad y_2 = h_d x_2 + h_c x_1 + z_2, \tag{8.1}$$

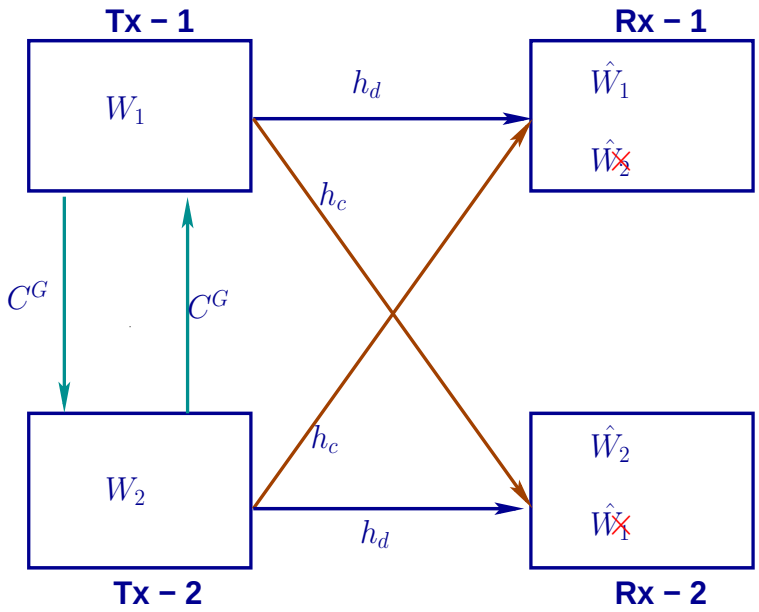


Figure 8.1: The 2-user GSIC with transmitter cooperation.

where z_j $(j = 1, 2)$ is complex Gaussian, distributed as $z_j \sim \mathcal{CN}(0, 1)$. The input signals are required to satisfy the power constraint: $E[|\mathbf{x}_i|^2] \leq P$. Here, h_d and h_c are the channel gains of the direct and cross links, respectively. The transmitters cooperate through a noiseless secure link of finite rate (C_G). The parameters m and n used for the SLDIC are related to the GSIC as $m = (\lfloor \log P|h_d|^2 \rfloor)^+$, $n = (\lfloor \log P|h_c|^2 \rfloor)^+$, while the capacity of the cooperative link is $C = \lfloor C_G \rfloor$.

The transmitter i has a message W_i, which should be decodable at the intended receiver i, but needs to be kept secret from the other, unintended receiver j, $j \neq i$. The notion of weak secrecy is considered for the Gaussian case, in contrast to the perfect secrecy constraint used in the deterministic case. Also, it is assumed that the transmitters trust each other completely and that they do not deviate from the agreed scheme. The details of the encoding and decoding scheme can be found for the weak/moderate interference regime and high/very high interference regime in Secs. 8.2.1 and 8.2.2,

respectively.

In the following section, achievable schemes for the GSIC are presented.

8.2 GSIC: Achievable schemes

8.2.1 Weak/moderate interference regime $(0 \leq \alpha \leq 1)$

The achievable scheme is based on the approach used in Secs. 6.2.1 and 6.2.2, for the SLDIC. In the case of the SLDIC, the achievable scheme used a combination of interference cancelation, transmission of random bits, or both, depending on the value of α and C. That scheme is extended to the Gaussian setting, as follows.

The message at transmitter i is split into two parts: a *non-cooperative private* part (w_{pi}) and a *cooperative private* part (w_{cpi}). The non-cooperative private message is encoded using stochastic encoding [32], and the cooperative private part is encoded using cooperative encoding scheme. For the SLDIC, data bits transmitted at the lower levels $[1 : m-n]$ are not received at the unintended receiver. Hence, these data bits remain secure. However, there is no one-to-one analogue of this in the GSIC, so the scheme does not extend directly. In the Gaussian case, for the non-cooperative private part, stochastic encoding is used to ensure secrecy. The transmitter i encodes the non-cooperative part $w_{pi} \in \mathcal{W}_{pi} = \{1, 2, \ldots, 2^{NR_{pi}}\}$ into $\mathbf{x}_{pi}^N$. A stochastic encoder is specified by a conditional probability density $f_{pi}(x_{pi,k}|w_{pi})$ $(i = 1, 2)$, where $x_{pi} \in \mathcal{X}_{pi}$ and $w_{pi} \in \mathcal{W}_{pi}$, and it satisfies the following condition:

$$\sum_{x_{pi,k} \in \mathcal{X}_{pi}} f_{pi}(x_{pi,k}|w_{pi}) = 1, \qquad k = 1, 2, \ldots, N, \tag{8.2}$$

where $f_{pi}(x_{pi,k}|w_{pi})$ is the probability that $x_{pi,k}$ is output by the stochastic encoder, when

message w_{pi} is to be transmitted.

The cooperative private message $w_{cp1} \in \mathcal{W}_{cp1} = \{1, 2, \ldots, 2^{NR_{cp1}}\}$ and $w_{cp2} \in \mathcal{W}_{cp2} = \{1, 2, \ldots, 2^{NR_{cp2}}\}$ at transmitters 1 and 2 are encoded using cooperative encoding scheme, as described in the later part of this section. One of the key aspects of the achievable scheme is the precoding of the cooperative private messages such that the codeword carrying the cooperative private message is completely canceled at the unintended receiver. This corresponds to the scheme used for interference cancelation in the case of SLDIC. This serves two purposes: it cancels interference over the air, and simultaneously ensures secrecy. This scheme is termed as *cooperative encoding scheme*. The transmitter 2 sends a dummy message along with the cooperative private message and the non-cooperative private message. Note that stochastic encoding is sufficient to ensure secrecy of the non-cooperative private message. However, the additional dummy message sent by the transmitter 2 can enhance the achievable secrecy rate, depending on the values of α and C. In this case, both the receivers treat the dummy message as noise.

Encoding and decoding

For the non-cooperative private part, transmitter i $(i = 1, 2)$ generates $2^{N(R_{pi}+R'_{pi})}$ i.i.d. sequences of length N at random according to

$$P(\mathbf{x}_{pi}^N) = \prod_{k=1}^{N} P(x_{pi,k}). \tag{8.3}$$

The $2^{N(R_{pi}+R'_{pi})}$ codewords in the codebook C_{pi} are randomly grouped into $2^{NR_{pi}}$ bins, with each bin containing $2^{NR'_{pi}}$ codewords. Any codeword in C_{pi} is indexed as $\mathbf{x}_{pi}^N(w_{pi}, w'_{pi})$

for $w_{pi} \in \mathcal{W}_{pi}$ and $w'_{pi} \in \mathcal{W}'_{pi} = \{1, 2, \ldots, 2^{NR'_{pi}}\}$. In order to transmit w_{pi}, transmitter i selects a $w'_{pi} \in \mathcal{W}'_{pi}$ randomly and transmits the codeword $\mathbf{x}_{pj}^N(w_{pi}, w'_{pi})$.

In order to transmit a dummy message, transmitter 2 generates $2^{NR_{d2}}$ i.i.d. sequences of length N at random according to

$$P(\mathbf{x}_{d2}^N) = \prod_{k=1}^{N} P(x_{d2,k}). \tag{8.4}$$

The $2^{NR_{d2}}$ codewords in codebook C_{d2} are randomly grouped into $2^{NR'_{d2}}$ bins, with each bin containing $2^{NR''_{d2}}$ codewords (and thus $R_{d2} = R'_{d2} + R''_{d2}$). Any codeword in C_{d2} is indexed as $\mathbf{x}_{d2}^N(w'_{d2}, w''_{d2})$, where $w'_{d2} \in \mathcal{W}'_{d2} = \{1, 2, \ldots, 2^{NR'_{d2}}\}$ and $w''_{d2} \in W''_{d2} = \{1, 2, \ldots, 2^{NR''_{d2}}\}$. During encoding, transmitter 2 selects $w'_{d2} \in \mathcal{W}'_{d2}$ and $w''_{d2} \in \mathcal{W}''_{d2}$ independently at random and sends the codeword $\mathbf{x}_{d2}^N(w'_{d2}, w''_{d2})$.

For the cooperative private message, the transmitter i $(i = 1, 2)$ generates the cooperative private codeword $\mathbf{w}_{iz}^N(w_{\text{cpi}})$ according to

$$P(\mathbf{w}_{iz}^N) = \prod_{k=1}^{N} P(\mathbf{w}_{iz,k}), \text{where } i = 1, 2. \tag{8.5}$$

Each transmitter communicates its shared message to the other transmitter over the cooperative links. The cooperative messages at the transmitters are precoded in such way that the cooperative private messages at the unintended receivers are completely canceled, as described below:

$$\begin{aligned} \mathbf{x}_{cp1} &= \mathbf{w}_{1z} h_d - \mathbf{w}_{2z} h_c, \\ \mathbf{x}_{cp2} &= \mathbf{w}_{2z} h_d - \mathbf{w}_{1z} h_c. \end{aligned} \tag{8.6}$$

Finally, the non-cooperative private codeword and cooperative private codeword are

superimposed to form the transmit codeword at the transmitter 1 and the non-cooperative private codeword, cooperative private codeword and the dummy message codeword are superimposed to form the transmit codeword at the transmitter 2:

$$\begin{aligned}\mathbf{x}_1^N(w_{cp1}, w_{cp2}, w_{p1}, w'_{p1}) &= \mathbf{x}_{cp1}^N + \mathbf{x}_{p1}^N,\\ \text{and } \mathbf{x}_2^N(w_{cp1}, w_{cp2}, w_{p2}, w'_{p2}, w'_{d2}, w''_{d2}) &= \mathbf{x}_{cp2}^N + \mathbf{x}_{p2}^N + \mathbf{x}_{d2}^N. \end{aligned} \tag{8.7}$$

This not only eliminates the interference caused by the cooperative private part, but also ensures secrecy of the cooperative private message. The outputs at the receivers are:

$$y_1 = u_1 + h_c x_{d2} + h_c x_{p1} + z_2, y_2 = u_2 + h_d x_{d2} + h_c x_{p1} + z_2. \tag{8.8}$$

where $u_i = (h_d^2 - h_c^2)\mathbf{w}_{iz}, i = 1, 2$. The quantity σ_{iz}^2 $(i = 1, 2)$ corresponds to the variance of $\mathbf{w}_{iz}$.

For decoding, receiver i looks for a unique message tuple such that $(\mathbf{y}_i^N, \mathbf{u}_i^N(\hat{w}_{cpi}),$ $\mathbf{x}_{pi}^N(\hat{w}_{pi}, \hat{w}'_{pi}))$ is jointly typical. Based on the above coding strategy, the following theorem gives the achievable result on the secrecy rate.

Theorem 18. *In the weak/moderate interference regime, the following rate is achievable for the GSIC with limited-rate transmitter cooperation and secrecy constraints at the receivers:*

$$\begin{aligned} R_1 + R'_{p1} &\leq I(\mathbf{u}_1, \mathbf{x}_{p1}; \mathbf{y}_1),\\ R_1 + R'_{p1} &\leq I(\mathbf{x}_{p1}; \mathbf{y}_1|\mathbf{u}_1) + \min\left\{C_G, I(\mathbf{u}_1; \mathbf{y}_1|\mathbf{x}_{p1})\right\}, \end{aligned} \tag{8.9}$$

where $R'_{p1} = I(\mathbf{x}_{p1}; \mathbf{y}_2|\mathbf{x}_{p2}, \mathbf{u}_2)$. *The achievable secrecy rate for the user* 2 *can be obtained by*

exchanging the indices 1 *and* 2 *in (8.9).*

Proof. The proof involves analyzing the error probability at decoder along with equivocation computation. One of the novelties in obtaining the achievable scheme lies in the precoding of the codewords carrying the cooperative private part of the message (w_{cpi}) which is canceled at the unintended receiver. This simultaneously eliminates interference and ensures secrecy of the cooperate private message. For ensuring secrecy of the non-cooperative private message, it is required to show that the weak secrecy constraint is satisfied at the receiver j, i.e., $H(W_{pi}|\mathbf{y}_j^N) \geq N[R_{pi} - \epsilon_s]$. In the equivocation computation, the main novelty lies in choosing the value of the rate sacrificed in confusing the unintended receiver (R'_{pi}) and rate of the dummy message (R_{di}) so that the weak secrecy constraint is satisfied.

Equivocation computation: The equivocation at receiver 2 is bounded as follows.

$$\begin{aligned} H(W_1|\mathbf{y}_2^N) &= H(W_{p1}, W_{cp1}|\mathbf{y}_2^N), \\ &= H(W_{p1}|\mathbf{y}_2^N) + H(W_{cp1}|\mathbf{y}_2^N, W_{p1}). \end{aligned} \tag{8.10}$$

First consider the term $H(W_{cp1}|\mathbf{y}_2^N, W_{p1})$. The output at receiver 2 is

$$y_2 = u_2 + h_d x_{d2} + h_c x_{p1} + z_2. \tag{8.11}$$

As $\mathbf{u}_1$ and $\mathbf{u}_2$ are independent of each other, i.e., $I(\mathbf{u}_1; \mathbf{u}_2) = 0$, and w_{cp1} is chosen independent of w_{p1}, the following holds:

$$H(W_{cp1}|\mathbf{y}_2^N, W_{p1}) = H(W_{cp1}). \tag{8.12}$$

Hence, it is only required to show the following:

$$H(W_{p1}|\mathbf{y}_2^N) \geq N\left[R_{p1} - \epsilon_s\right]. \tag{8.13}$$

Consider the following:

$$\begin{aligned}
&H(W_{p1}|\mathbf{y}_2^N)\\
&\geq H(W_{p1}|\mathbf{y}_2^N, \mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}''),\\
&\overset{(a)}{=} H(W_{p1}, \mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}'') - H(\mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}''),\\
&\overset{(b)}{=} H(W_{p1}, \mathbf{y}_2^N, \mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}'') - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{y}_2^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{p1}, W_{d2}'')\\
&\qquad - H(\mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}''),\\
&= H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{x}_{p2}^N, W_{d2}'') + H(W_{p1}, \mathbf{y}_2^N|\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{d2}'') - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{y}_2^N, \mathbf{x}_{p2}^N, W_{p1}, W_{d2}'')\\
&\qquad\qquad - H(\mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}''),\\
&\geq H(\mathbf{x}_{p1}^N) + H(\mathbf{x}_{d2}^N|W_{d2}'') + H(\mathbf{y}_2^N|\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{d2}'') - H(\mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N)\\
&\qquad\qquad - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{y}_2^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{p1}, W_{d2}''),\\
&\overset{(c)}{=} H(\mathbf{x}_{p1}^N) + H(\mathbf{x}_{d2}^N|W_{d2}'') + H(\mathbf{y}_2^N|\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N) - H(\mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N)\\
&\qquad\qquad - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{y}_2^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{p1}, W_{d2}''),\\
&= N\left[R_{p1} + R_{p1}' + R_{d2}'\right] - I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N|\mathbf{u}_2^N, \mathbf{x}_{p2}^N) - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{y}_2^N, \mathbf{u}_2^N, \mathbf{x}_{p2}^N, W_{p1}, W_{d2}''),
\end{aligned} \tag{8.14}$$

where (a) and (b) are obtained using the relation:

$H(W_{p1}, \mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}'') = H(\mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}'') + H(W_{p1}|\mathbf{y}_2^N, \mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}'')$ and

$H(W_{p1}, \mathbf{y}_2^N, \mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}'') = H(W_{p1}, \mathbf{y}_2^N|\mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{d2}'')+$

$H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{y}_2^N, \mathbf{x}_{p2}^N, \mathbf{u}_2^N, W_{p1}, W_{d2}'')$, respectively; and (c) is obtained using the fact that

$W''_{d2} \to (\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \mathbf{x}_{p2}^N, \mathbf{u}_2^N) \to \mathbf{y}_2^N$ forms a Markov chain. This can be shown with the help of a functional dependency graph [77].

Using Lemma 5 in Appendix E.2, it can be shown that

$$I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{u}_2^N, \mathbf{x}_{p2}^N) \leq NI(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{u}_2, \mathbf{x}_{p2}) + N\epsilon'. \tag{8.15}$$

Thus the remaining key step in showing that the condition in (8.13) is satisfied is to bound the last term in (8.14). To bound this term, consider the joint decoding of W'_{p1} and W'_{d2} at receiver 2 assuming that a genie has given W_{p1} and W''_{d2} as side information to receiver 2. For a given $W_{p1} = w_{p1}$ and $W''_{d2} = w''_{d2}$, assume that w'_{p1} and w'_{d2} are sent by transmitters 1 and 2, respectively and receiver 2 knows the sequence $\mathbf{y}_2^N = y_2^N$ and $\mathbf{u}_2^N = u_2^N$. For a given $W_{p1} = w_{p1}$ and $W''_{d2} = w''_{d2}$, receiver 2 declares that j and l was sent if $(\mathbf{x}_{p1}^N(w_{p1}, j), \mathbf{x}_{d2}^N(l, w''_{d2}), \mathbf{y}_2^N)$ is jointly typical and such (j, l) exists and is unique. Otherwise, an error is declared. Now, define the following event

$$E_{jl}^1 = \left\{ (\mathbf{x}_{p1}^N(w_{p1}, j), \mathbf{x}_{d2}^N(l, w''_{d2}), \mathbf{y}_2^N) \in T_\epsilon^N(P_{\mathbf{x}_{p1}, \mathbf{x}_{d2}, \mathbf{y}_2 | \mathbf{u}_2, \mathbf{x}_{p2}}) \right\}, \tag{8.16}$$

where $T_\epsilon^N(P_{X_{p1}X_{d2}Y_2|U_2X_{p2}})$ denotes, for given typical sequences $\mathbf{u}_2$ and $\mathbf{x}_{p2}$, the set of jointly typical sequences $\mathbf{y}_1, \mathbf{x}_{p1}$, and $\mathbf{u}_1$ with respect to $P_{X_{p1}X_{d2}Y_2|U_2X_{p2}}$. Without loss of generality, assume that $\mathbf{x}_{p1}^N(w_{p1}, 1)$ and $\mathbf{x}_{d2}^N(1, w''_{d2})$ were sent. Then, by the union of events bound, the following is obtained:

$$\begin{aligned} P_{e1}^N &= P\left(E_{11}^{1^c} \bigcup \cup_{j\neq 1, l\neq 1} E_{jl}^1\right), \\ &\leq P(E_{11}^{1^c}) + \sum_{j\neq 1} P(E_{j1}^1) + \sum_{l\neq 1} P(E_{1l}^1) + \sum_{j\neq 1, l\neq 1} P(E_{jl}^1), \end{aligned}$$

$$\leq P(E_{11}^{1^c}) + 2^{NR'_{p1}} 2^{-N[I(\mathbf{x}_{p1};\mathbf{y}_2|\mathbf{x}_{d2},\mathbf{u}_2,\mathbf{x}_{p2})-3\epsilon]} + 2^{NR'_{d2}} 2^{-N[I(\mathbf{x}_{d2};\mathbf{y}_2|\mathbf{x}_{p1},\mathbf{u}_2,\mathbf{x}_{p2})-3\epsilon]}$$
$$+ 2^{N\left(R'_{p1}+R'_{d2}\right)} 2^{-N[I(\mathbf{x}_{p1},\mathbf{x}_{d2};\mathbf{y}_2|\mathbf{u}_2,\mathbf{x}_{p2})-3\epsilon]}. \tag{8.17}$$

Hence, the probability of error P_{e1}^N is arbitrarily small for large N, provided the following conditions are satisfied.

$$R'_{P1} \leq I(\mathbf{x}_{p1};\mathbf{y}_2|\mathbf{x}_{d2},\mathbf{u}_2,\mathbf{x}_{p2}), \;\; R'_{d2} \leq I(\mathbf{x}_{d2};\mathbf{y}_2|\mathbf{x}_{p1},\mathbf{u}_2,\mathbf{x}_{p2}),$$
$$R'_{p1} + R'_{d2} \leq I(\mathbf{x}_{p1},\mathbf{x}_{d2};\mathbf{y}_2|\mathbf{u}_2,\mathbf{x}_{p2}). \tag{8.18}$$

When the conditions in (8.18) are satisfied and for sufficiently large N, the following bound is obtained using Fano's inequality:

$$\frac{1}{N}H(\mathbf{x}_{p1}^N,\mathbf{x}_{d2}^N|\mathbf{y}_1^N,\mathbf{u}_2^N,\mathbf{x}_{p2}^N,W_{p1}=w_{p1},W''_{d2}=w''_{d2}) \leq \frac{1}{N}[1+P_{e1}^N \log 2^{N[R'_{p1}+R'_{d2}]}] \leq \delta_1. \tag{8.19}$$

Using the above, the last term in (8.14) is bounded as follows:

$$H(\mathbf{x}_{p1}^N,\mathbf{x}_{d2}^N|\mathbf{y}_2^N,\mathbf{u}_2^N,\mathbf{x}_{p2}^N,W_{p1},W''_{d2})$$
$$= \sum_{w_{p1},w''_{d2}} P(w_{p1},w''_{d2}) H(\mathbf{x}_{p1}^N,\mathbf{x}_{d2}^N|\mathbf{y}_2^N,\mathbf{u}_2^N,\mathbf{x}_{p2}^N,W_{p1}=w_{p1},W''_{d2}=w''_{d2}),$$
$$\leq N\delta_1. \tag{8.20}$$

Using (8.15) and (8.20), (8.14) becomes

$$H(W_{p1}|\mathbf{y}_2^N) \geq N\left[R_{p1} + R'_{p1} + R'_{d2} - I(\mathbf{x}_{p1},\mathbf{x}_{d2};\mathbf{y}_2|\mathbf{u}_2,\mathbf{x}_{p2}) - \epsilon_1\right], \tag{8.21}$$

where $\epsilon_1 = \epsilon' + \delta_1$. By choosing $R'_{p1} + R'_{d2} = I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2|\mathbf{u}_2, \mathbf{x}_{p2}) - \epsilon_{11}$, (8.21) becomes

$$H(W_{p1}|\mathbf{y}_2^N) \geq N\left[R_{p1} - \epsilon_s\right], \text{ where } \epsilon_s = \epsilon_1 + \epsilon_{11}. \tag{8.22}$$

Hence, by choosing $R'_{p1} = I(\mathbf{x}_{p1}; \mathbf{y}_2|\mathbf{x}_{p2}, \mathbf{u}_2) - \epsilon'_{11}$ and $R'_{d2} = I(\mathbf{x}_{d2}; \mathbf{y}_2|\mathbf{x}_{p1}, \mathbf{x}_{p2}, \mathbf{u}_2) - \epsilon''_{11}$, secrecy is ensured for the non-cooperative private message of transmitter 1, and also, the achievability condition in (8.18) is satisfied.

For receiver 1, also, it is only required to show that the non-cooperative private message of transmitter 2 remains secure. To bound the equivocation at receiver 1, consider the following:

$$H(W_{p2}|\mathbf{y}_1^N) \geq H(W_{p2}|\mathbf{y}_1^N, \mathbf{x}_{p1}^N, \mathbf{u}_1^N, W'_{d2}). \tag{8.23}$$

Then, by following similar steps as used in case of receiver 2, it can be shown that the choice of $R'_{p2} = I(\mathbf{x}_{p2}; \mathbf{y}_1|\mathbf{x}_{p1}, \mathbf{u}_1) - \epsilon'_2$ and $R''_{d2} = I(\mathbf{x}_{d2}; \mathbf{y}_1|\mathbf{x}_{p1}, \mathbf{x}_{p2}, \mathbf{u}_1) - \epsilon''_2$, ensures secrecy for the non-cooperative private message of transmitter 2. This completes the proof. □

Using the achievable rate result in Theorem 18 and time-sharing, the achievable *symmetric* secrecy rate is stated in the following Corollary.

Corollory 2. *Using the achievable result in Theorem 18 and time-sharing between transmitters, following symmetric secrecy rate is achievable for the GSIC with limited-rate transmitter cooperation:*

$$R_s = \frac{1}{2}\left[R_i^*(1) + R_i^*(2)\right], \tag{8.24}$$

where $i = 1, 2$ and $R_i^*(1)$ and $R_i^*(2)$ are the achievable secrecy rate for the transmitter i in the first and second time slot, respectively, which is obtained by maximizing the rate given in the following equations:

$$R_1(1) \leq \begin{cases} 0.5\log\left(1+\frac{\sigma_u^2+h_d^2P_{p1}}{1+h_c^2P_{d2}+h_c^2P_{p2}}\right) - R'_{p1}, \\ 0.5\log\left(1+\frac{h_d^2P_{p1}}{1+h_c^2P_{d2}+h_c^2P_{p2}}\right) + \min\left\{C_G, 0.5\log\left(1+\frac{\sigma_u^2}{1+h_c^2P_{d2}+h_c^2P_{p2}}\right)\right\} - R'_{p1}, \end{cases} \tag{8.25}$$

$$R_2(1) \leq \begin{cases} 0.5\log\left(1+\frac{\sigma_u^2+h_d^2P_{p2}}{1+h_d^2P_{d2}+h_c^2P_{p1}}\right) - R'_{p2}, \\ 0.5\log\left(1+\frac{h_d^2P_{p2}}{1+h_d^2P_{d2}+h_c^2P_{p1}}\right) + \min\left\{C_G, 0.5\log\left(1+\frac{\sigma_u^2}{1+h_d^2P_{d2}+h_c^2P_{p1}}\right)\right\} - R'_{p2}, \end{cases} \tag{8.26}$$

where $R'_{p1} = 0.5\log\left(1+\frac{h_c^2P_{p1}}{1+h_d^2P_{d2}}\right)$, $R'_{p2} = 0.5\log\left(1+\frac{h_c^2P_{p2}}{1+h_c^2P_{d2}}\right)$, $\sigma_u^2 \triangleq (h_d^2-h_c^2)^2\sigma_z^2$, $\sigma_z^2 \triangleq \frac{\theta_1}{\theta_1+\theta_2}\frac{P_1}{h_d^2+h_c^2}$, $P_{p1} \triangleq \frac{\theta_2}{\theta_1+\theta_2}P_1$, $P_{p2} = \frac{\eta_1}{\eta_1+\eta_2}P'$, $P_{d2} = \frac{\eta_2}{\eta_1+\eta_2}P'$, $P' = (P_2-(h_d^2+h_c^2)\sigma_z^2)$, $P_i \triangleq \beta_i P$ $(i = 1, 2)$ and $0 \leq (\theta_i, \eta_i, \beta_i) \leq 1$. The rate equations for the second time slot can be obtained by exchanging indices 1 and 2 in (8.25) and (8.26).

Proof. In the first and second time slots, transmitters 1 and 2 send the following encoded messages:

$$\begin{aligned} &\mathbf{x}_1(1) = \mathbf{x}_{cp1}(1) + \mathbf{x}_{p1}(1), \text{ and } \mathbf{x}_2(1) = \mathbf{x}_{cp2}(1) + \mathbf{x}_{p2}(1) + \mathbf{x}_{d2}(1), \\ &\mathbf{x}_1(2) = \mathbf{x}_{cp1}(2) + \mathbf{x}_{p1}(2) + \mathbf{x}_{d1}(2), \text{ and } \mathbf{x}_2(2) = \mathbf{x}_{cp2}(2) + \mathbf{x}_{p2}(2), \end{aligned} \tag{8.27}$$

where $\mathbf{x}_{cpi}$ $(i = 1, 2)$ is as defined in (8.6). In the following, the achievable secrecy rate and power allocation for different messages are discussed in the case of the first time slot. Hence, for simplicity, the time index is omitted. The mutual information terms given in Theorem 18 are evaluated as follows. From Theorem 18, R'_{p1} and R'_{p2} are set as $0.5\log\left(1+\frac{h_c^2P_{p1}}{1+h_d^2P_{d2}}\right)$ and $0.5\log(1+\frac{h_c^2P_{p2}}{1+h_c^2P_{d2}})$, respectively. The first equation in (8.9)

becomes

$$R_1 \leq 0.5 \log\left(1 + \frac{\sigma_u^2 + h_d^2 P_{p1}}{1 + h_c^2 P_{d2} + h_c^2 P_{p2}}\right) - R'_{p1}. \tag{8.28}$$

The second equation in (8.9) becomes

$$R_1 \leq 0.5 \log\left(1 + \frac{h_d^2 P_{p1}}{1 + h_c^2 P_{d2} + h_c^2 P_{p2}}\right) + \min\left\{C_G, 0.5 \log\left(1 + \frac{\sigma_u^2}{1 + h_c^2 P_{d2} + h_c^2 P_{p2}}\right)\right\} - R'_{p1}. \tag{8.29}$$

The achievable rate for user 2 becomes

$$R_2 \leq 0.5 \log\left(1 + \frac{\sigma_u^2 + h_d^2 P_{p2}}{1 + h_d^2 P_{d2} + h_c^2 P_{p1}}\right) - R'_{p2}, \tag{8.30}$$

$$R_2 \leq 0.5 \log\left(1 + \frac{h_d^2 P_{p2}}{1 + h_d^2 P_{d2} + h_c^2 P_{p1}}\right) + \min\left\{C_G, 0.5 \log\left(1 + \frac{\sigma_u^2}{1 + h_d^2 P_{d2} + h_c^2 P_{p1}}\right)\right\} - R'_{p2}. \tag{8.31}$$

The encoded message at transmitters 1 and 2 are

$$\mathbf{x}_1 = h_d \mathbf{w}_{1z} - h_c \mathbf{w}_{2z} + \mathbf{x}_{p1}, \text{ and } \mathbf{x}_2 = h_d \mathbf{w}_{2z} - h_c \mathbf{w}_{1z} + \mathbf{x}_{p2} + \mathbf{x}_{d2}. \tag{8.32}$$

To simplify the power allocation, the variance of $\mathbf{w}_{1z}$ and $\mathbf{w}_{2z}$ are chosen to be the same, i.e, $\sigma_{1z}^2 = \sigma_{2z}^2 = \sigma_z^2$. In order to satisfy the power constraint at the transmitters, the following conditions need to be satisfied.

$$(h_d^2 + h_c^2)\sigma_z^2 + P_{p1} \leq P_1 \text{ and } (h_d^2 + h_c^2)\sigma_z^2 + P_{p2} + P_{d2} \leq P_2, \tag{8.33}$$

where $P_i = \beta_i P$ $(i = 1, 2)$, $0 \leq \beta_i \leq 1$ and P is the maximum power available at either transmitter. The power for the non-cooperative private message, cooperative private

message and dummy message are chosen as follows:

$$\sigma_z^2 = \frac{\theta_1}{\theta_1+\theta_2}\frac{P_1}{h_d^2+h_c^2}, P_{p1} = \frac{\theta_2}{\theta_1+\theta_2}P_1,$$
$$P_{p2} = \frac{\eta_1}{\eta_1+\eta_2}P', P_{d2} = \frac{\eta_2}{\eta_1+\eta_2}P', \text{ and } P' = (P_2 - (h_d^2+h_c^2)\sigma_z^2)^+. \tag{8.34}$$

where $(\theta_i, \eta_i) \in [0,1]$. The parameters θ_i and η_i act as power splitting parameters for transmitters 1 and 2, respectively. The parameter β_i acts as a power control parameter. Hence, θ_i, η_i and β_i are chosen such that the rates in (8.28)-(8.31) are maximized, and the minimum of (8.28) and (8.29) gives the achievable secrecy rate for transmitter 1 i.e., $R_1^*(1)$; and the minimum of (8.30) and (8.31) give the achievable secrecy rate for the transmitter 2 i.e., $R_2^*(1)$. This completes the proof. □

8.2.2 High/very high interference regime $(\alpha > 1)$

The achievable scheme is based on the approach used for the SLDIC in the case of the high interference regime. The achievable scheme for the SLDIC in Sec. 6.2.4 used a combination of interference cancelation, relaying of the other user's data bits, and transmission of random bits. In the case of the SLDIC, as some of the interfering links are not present to the intended receiver, the levels corresponding to these links can be directly used for the other user's data transmission. But, in the Gaussian setting, it is not possible to relay the other user's data directly in this manner. The relationship between the corresponding achievable schemes for the SLDIC and the GSIC will be made precise in the following paragraphs.

In the proposed scheme, user 1 sends a non-cooperative private message (w_{p1}) and a

cooperative private message (w_{cp1}). The other user transmits cooperative private message (w_{cp2}) along with a dummy message (w_{d2}). For the SLDIC, the achievable scheme required transmission of random bits for ensuring secrecy of data bits, in addition to the data bits that were sent with the help of cooperation. Similarly, for the GSIC, the proposed scheme requires stochastic encoding and transmission of a dummy message by the other user, in order to ensure secrecy for the non-cooperative private message sent by user 1. It is important to note that stochastic encoding alone cannot ensure secrecy for the non-cooperative private part of the message. For the cooperative private part of the message (w_{cpi}), the coding scheme is the same as that mentioned in Sec. 8.2.1.

The transmission of the dummy message x_{d2} by transmitter 2 can be considered as using another stochastic encoder f_{d2}, which is specified by a probability density $f_{d2}(x_{d2,k})$, with $x_{d2,k} \in \mathcal{X}_{d2}$ and $\sum_{x_{d2,k} \in \mathcal{X}_{d2}} f_{d2}(x_{d2,k}) = 1$. The rate R_{d2} of the dummy message sent by transmitter 2 and the rate sacrificed by transmitter 1 in stochastic encoding in order to confuse the eavesdroppers at receivers 1 and 2, respectively, are chosen such that the non-cooperative private message sent by transmitter 1 remains secure at receiver 2, and receiver 1 is able to decode the dummy message. At transmitter 1, the cooperative private message and the non-cooperative private message are superimposed to form the transmit codeword ($\mathbf{x}_1^N$). Finally, at transmitter 2, the cooperative private message and the dummy information are superimposed to form the transmit codeword ($\mathbf{x}_2^N$). In contrast to the achievable scheme for the weak/moderate interference regime, the dummy message sent by one of the transmitters i is required to be decodable at the receiver j ($i \neq j$).

Encoding and decoding

The encoding of the non-cooperative private message at transmitter 1 and the cooperative private message at both the transmitters is the same as described in Sec. 8.2.1. In order to transmit the dummy message, transmitter 2 chooses $\mathbf{x}_{d2}^N(w_{d2})$ for $w_{d2} \in \mathcal{W}_{d2}$.

The codewords transmitted from the two transmitters are given by:

$$\mathbf{x}_1^N(w_{cp1}, w_{cp2}, w_{p1}, w'_{p1}) = \mathbf{x}_{cp1}^N + \mathbf{x}_{p1}^N, \text{ and } \mathbf{x}_2^N(w_{cp1}, w_{cp2}, w_{d2}) = \mathbf{x}_{cp2}^N + \mathbf{x}_{d2}^N, \tag{8.35}$$

where $\mathbf{x}_{cpi}$ $(i = 1, 2)$ is defined in (8.6).

For decoding, receiver 1 looks for a unique message tuple such that $(\mathbf{y}_1^N, \mathbf{u}_1^N(\hat{w}_{cp1}), \mathbf{x}_{d2}^N(\hat{w}_{d2}), \mathbf{x}_{p1}^N(\hat{w}_{p1}, \hat{w}'_{p1}))$ is jointly typical. Receiver 2 looks for a index $\hat{w}_{cp2}$ such that $(\mathbf{y}_2^N, \mathbf{u}_2^N(\hat{w}_{cp2}))$ is jointly typical.

Based on the above coding strategy, the following theorem gives the achievable result on the secrecy rate.

Theorem 19. *In the high interference regime, the following rate is achievable for the GSIC with limited-rate transmitter cooperation and secrecy constraints at the receivers:*

$$\begin{aligned}
&R_1 + R'_{p1} \leq \min\left[I(\mathbf{u}_1, \mathbf{x}_{p1}; \mathbf{y}_1|\mathbf{x}_{d2}), I(\mathbf{x}_{p1}; \mathbf{y}_1|\mathbf{u}_1, \mathbf{x}_{d2}) + \min\left\{I(\mathbf{u}_1; \mathbf{y}_1|\mathbf{x}_{p1}, \mathbf{x}_{d2}), C_G\right\}\right],\\
&R_1 + R'_{p1} + R_{d2} \leq \min\left[I(\mathbf{u}_1, \mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1), I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1|\mathbf{u}_1) + \min\left\{I(\mathbf{u}_1; \mathbf{y}_1|\mathbf{x}_{p1}, \mathbf{x}_{d2}), C_G\right\},\right.\\
&\qquad\qquad \left. I(\mathbf{x}_{p1}; \mathbf{y}_1|\mathbf{u}_1, \mathbf{x}_{d2}) + I(\mathbf{u}_1, \mathbf{x}_{d2}; \mathbf{y}_1|\mathbf{x}_{p1})\right],\\
&R_1 + R'_{p1} + 2R_{d2} \leq I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1|\mathbf{u}_1) + I(\mathbf{u}_1, \mathbf{x}_{d2}; \mathbf{y}_1|\mathbf{x}_{p1}),\\
&R_2 \leq \min\left\{I(\mathbf{u}_2; \mathbf{y}_2), C_G\right\}, R_{d2} \leq I(\mathbf{x}_{d2}; \mathbf{y}_1|\mathbf{u}_1, \mathbf{x}_{p1}),
\end{aligned} \tag{8.36}$$

where $R_1 \triangleq R_{p1} + R_{cp1}$, $R_2 \triangleq R_{cp2}$, $R'_{p1} \triangleq I(\mathbf{x}_{p1}; \mathbf{y}_2|\mathbf{u}_2)$, *and* $R_{d2} \triangleq I(\mathbf{x}_{d2}; \mathbf{y}_2|\mathbf{x}_{p1}, \mathbf{u}_2)$.

Proof. The proof is provided in Appendix E.3. □

The achievable symmetric secrecy rate is stated in the following Corollary.

Corollory 3. *Using the achievable result in Theorem 19 and time-sharing between transmitters, the following symmetric secrecy rate is achievable for the GSIC with limited-rate transmitter cooperation:*

$$R_s = \frac{1}{2}\left[R_1^*(1) + R_1^*(2)\right], \tag{8.37}$$

where $R_1^*(1)$ *and* $R_1^*(2)$ *are the achievable secrecy rates for transmitter* 1 *in the first and second time slots, respectively, which are obtained by maximizing* R_s *over parameters* θ_i, η_i *and* β_i $(i = 1, 2)$*. The achievable rates for users* 1 *and* 2 *in the first time slot are as follows:*

$$R_1(1) \leq \begin{cases} \min\left[0.5\log(1+\sigma_u^2+h_d^2P_{p1}), 0.5\log(1+h_d^2P_{p1}) + \min\left\{0.5\log(1+\sigma_u^2), C_G\right\}\right] - R'_{p1}, \\ \min\left[0.5\log(1+\sigma_u^2+h_d^2P_{p1}+h_c^2P_{d2}), 0.5\log(1+\sigma_u^2+h_c^2P_{d2}) + \right. \\ \quad \left. \min\left\{0.5\log(1+\sigma_u^2), C_G\right\}, 0.5\left\{\log(1+h_d^2P_{p1}) + \log(1+\sigma_u^2+h_c^2P_{d2})\right\}\right] \\ \qquad -(R'_{p1}+R_{d2}), \\ 0.5\log(1+h_d^2P_{p1}+h_c^2P_{d2}) + 0.5\log(1+\sigma_u^2+h_c^2P_{d2}) - (R'_{p1}+2R_{d2}) \end{cases}$$

$$\text{and } R_2(1) = \min\left\{0.5\log\left(1+\frac{\sigma_u^2}{1+h_d^2P_{d2}+h_c^2P_{p1}}\right), C_G\right\}, \tag{8.38}$$

where $R'_{p1} = 0.5\log\left(1+\frac{h_c^2P_{p1}}{1+h_d^2P_{d2}}\right)$, $R_{d2} = 0.5\log(1+h_d^2P_{d2})$, $\sigma_u^2 \triangleq (h_d^2-h_c^2)^2\sigma_z^2$, $\sigma_z^2 \triangleq \frac{\theta_1}{\theta_1+\theta_2}\frac{P_1}{h_d^2+h_c^2}$, $P_{p1} \triangleq \frac{\theta_2}{\theta_1+\theta_2}P_1$, $P_{d2} \triangleq (P_2-(h_d^2+h_c^2)\sigma_z^2)^+$, $P_i \triangleq \beta_i P$ *and* $0 \leq (\theta_i, \beta_i) \leq 1$*. The achievable rate equation for the second time slot can be obtained by exchanging indices* 1 *and* 2 *in (8.38).*

Proof. The proof is provided in Appendix E.4. □

8.3 Conclusions

In this chapter, achievable schemes were proposed for the GSIC with limited-rate transmitter cooperation and secrecy constraints at the receivers. The achievable scheme used a combination of cooperative encoding scheme and stochastic encoding along with dummy message transmission. However, in the high interference regime, it was possible to ensure secrecy for the non-cooperative part of the message with the help of dummy message transmission. In the next chapter, outer bounds on the secrecy rate for the GSIC with limited-rate transmitter cooperation are presented. The rates achieved by the schemes proposed in this chapter are compared with the outer bounds for different values of C_G and in different interference regimes.

Chapter 9

Outer Bounds on the Secrecy Rate of the 2-User GSIC with Limited-rate Transmitter Cooperation

In the previous chapters, the achievable schemes for the SLDIC and GSIC were obtained, along with outer bounds for the SLDIC. In this chapter, using the intuitions gained from the deterministic model, outer bounds for the GSIC are derived. Before going into the details of the outer bounds, some of the past results on outer bounds for various communication models with secrecy constraints are discussed below.

In general, deriving outer bounds on the secrecy rate involves use of Fano's inequality along with the secrecy constraints at receivers. The outer bounds and achievable schemes have given useful insights on the performance limits of the system for various communication models [6, 12, 36, 43]. In [12], the broadcast and IC with independent confidential messages are considered. For a special case of the IC, termed as the switch channel, the outer bound helps to establish the optimality of the proposed scheme.

In [6], outer bounds on the secrecy capacity of the wiretap channel with a helping interferer are given for both discrete memoryless and Gaussian channels. The outer bounds derived in [36] helps to establish the optimality of the cooperative encoding scheme for specific cases, in the case of 2-user IC with an external eavesdropper. In [43], a K-user Gaussian many-to-one IC is considered and nested-lattice code is used to obtain achievable secrecy sum-rate. It is shown that under specific cases, the gap between the outer bound and achievable secrecy sum rate is only a function of the number of users.

The effects of cooperation on secrecy has been studied under different system models in [38, 39, 73, 74]. In [73], the effects of user cooperation on the secrecy of multiple access channel with generalized feedback is analyzed and outer bounds on the achievable equivocation rates are obtained. Outer bounds on the rate-equivocation region are proposed using auxiliary random variables for cooperative relay broadcast channel in [74]. Also, outer bounds for relay-eavesdropper channel can be found in [38, 39].

In this chapter, three outer bounds are presented on the achievable secrecy rate in Theorems 20-22. The novelty in deriving these bounds lies in the way the outer bounds are extended from the deterministic case to the Gaussian case. The derived outer bounds are compared with achievable results derived in the previous chapter to illustrate the usefulness of these outer bounds.

9.1 GSIC: Outer bounds

In this section, the outer bounds on the secrecy rate for the GSIC with limited-rate transmitter cooperation are stated as Theorems 20-22. In the derivation of these outer bounds, the main difficulty lies in translating the ideas from the SLDIC to the Gaussian

case.

The outer bound derived in Theorem 14 for the SLDIC partitions the encoded message into two parts: $\mathbf{x}_{ia}^N$ (received at receiver j, $j \neq i$) and $\mathbf{x}_{ib}^N$ (not received at receiver j, $j \neq i$). However, it is not possible to partition the message in this way for the Gaussian case. Hence, in the derivation of Theorem 20, $\mathbf{s}_i^N = h_c \mathbf{x}_i^N + \mathbf{z}_j^N$ $(j \neq i)$ is used as a proxy for $\mathbf{x}_{ia}^N$. In this section, the following notation is used: SNR $\triangleq h_d^2 P$, INR $\triangleq h_c^2 P$ and $\rho \triangleq E[\mathbf{x}_1 \mathbf{x}_2]$.

Theorem 20. *The symmetric rate of the 2-user GSIC with limited-rate transmitter cooperation and secrecy constraints at the receiver is upper bounded as follows:*

$$R_s \leq \max_{0 \leq |\rho| \leq 1} \frac{1}{3} \left[2C_G + 0.5 \log \left(1 + SNR + INR + 2\rho\sqrt{SNR\, INR} \right) + 0.5 \log det \left(\Sigma_{\bar{\mathbf{y}}|\bar{\mathbf{s}}} \right) \right], \tag{9.1}$$

where $\Sigma_{\bar{\mathbf{y}}|\bar{\mathbf{s}}} = \Sigma_{\bar{\mathbf{y}}} - \Sigma_{\bar{\mathbf{y}},\bar{\mathbf{s}}} \Sigma_{\bar{\mathbf{s}}}^{-1} \Sigma_{\bar{\mathbf{y}},\bar{\mathbf{s}}}^T$,

$$\Sigma_{\bar{\mathbf{y}}} = \begin{bmatrix} 1 + SNR + INR + 2\rho\sqrt{SNR\, INR} & 2\sqrt{SNR\, INR} + \rho(SNR + INR) \\ 2\sqrt{SNR\, INR} + \rho(SNR + INR) & 1 + SNR + INR + 2\rho\sqrt{SNR\, INR} \end{bmatrix},$$

$$\Sigma_{\bar{\mathbf{y}},\bar{\mathbf{s}}} = \begin{bmatrix} \sqrt{SNR\, INR} + \rho INR & INR + \rho\sqrt{SNR\, INR} \\ INR + \rho\sqrt{SNR\, INR} & \sqrt{SNR\, INR} + \rho INR \end{bmatrix}, \text{ and } \Sigma_{\bar{\mathbf{s}}} = \begin{bmatrix} 1 + INR & \rho INR \\ \rho INR & 1 + INR \end{bmatrix},$$

and $\det(\cdot)$ *represents the determinant of a matrix.*

Proof. The proof is provided in Appendix F.1. □

The outer bound on the secrecy rate presented in the following theorem is based on the idea used in deriving outer bounds in Theorems 15 and 16 for case of the SLDIC. But, in the Gaussian setting, it is not possible to partition the encoded message as was done for the SLDIC. For example, in Theorem 15, a part of the output at receiver 2

which does not contain the signal sent by transmitter 1 is provided as side information to receiver 1. Hence, the approach used in the derivation of the outer bound in the case of the SLDIC cannot be directly used for the Gaussian case. To overcome this problem, for the Gaussian case, first $\mathbf{x}_2^N$ is provided as side information to receiver 1; this eliminates the interference caused by transmitter 2. Then, the receiver 1 is provided with $\mathbf{y}_2^N$ as side-information. The outer bound on the symmetric secrecy rate is stated in the following theorem.

Theorem 21. *The symmetric rate of the 2-user GSIC with limited-rate transmitter cooperation and secrecy constraints at the receiver is upper bounded as follows:*

$$R_s \leq \max_{0\leq|\rho|\leq 1} \left[2C_G + 0.5 \log \left(1 + \frac{SNR + SNR^2(1-\rho^2)}{1 + SNR + INR + 2\rho\sqrt{SNR\, INR}} \right) \right]. \tag{9.2}$$

Proof. The proof is provided in Appendix F.2. □

The outer bound presented in the following theorem is similar to the outer bound presented in Theorem 17 in the case of the SLDIC. This kind of outer bound exists in the literature (see, for example, [23]), but for the sake of completeness, it is presented in the following theorem. Unlike the results in Theorems 20 and 21, this outer bound does not depend on the capacity of the cooperative link.

Theorem 22. *The symmetric rate of the 2-user GSIC with limited-rate transmitter cooperation and secrecy constraints at the receiver is upper bounded as follows:*

$$R_s \leq \max_{0\leq|\rho|\leq 1} 0.5 \log \left[1 + SNR + INR + 2\rho\sqrt{SNR\, INR} - \frac{(2\sqrt{SNR\, INR} + \rho(SNR + INR))^2}{1 + SNR + INR + 2\rho\sqrt{SNR\, INR}} \right]. \tag{9.3}$$

Proof. The proof is provided in Appendix F.3. □

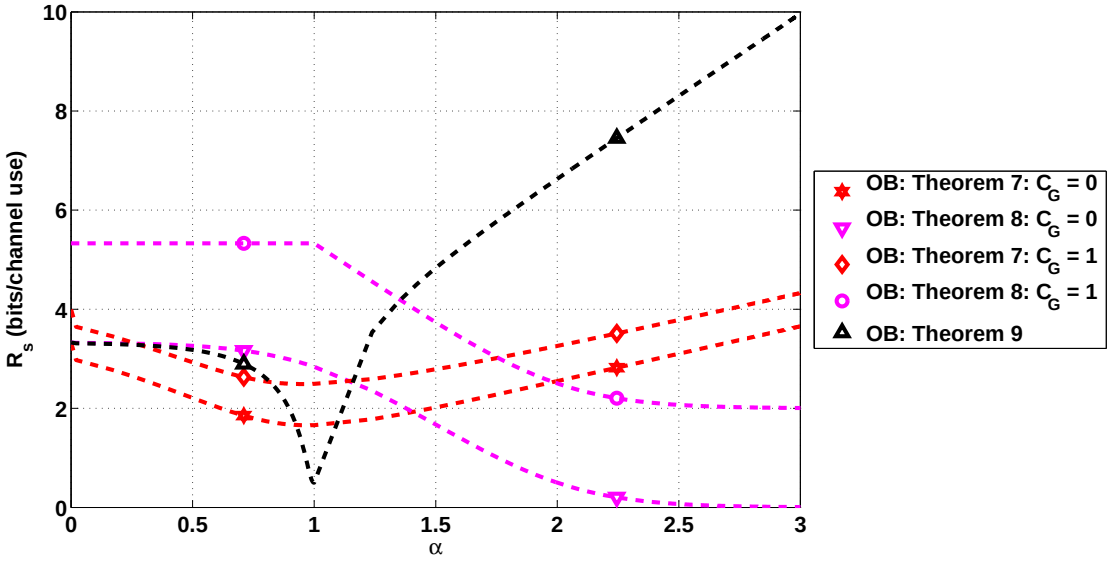


Figure 9.1: Comparison of different outer bounds on the achievable secrecy rate for the GSIC with $P = 100$ and $h_d = 1$.

9.1.1 Relation between the outer bounds for SLDIC and GSIC

In the following, it is shown that at high SNR and INR, the outer bounds developed for the Gaussian case (Theorems 20 and 21) are approximately equal to the outer bounds for the SLDIC, when $C = 0$.[1] In Fig. 9.1, the outer bounds on the achievable secrecy rate in Theorems 20-22 are compared as a function of α, for $C_G = 0$ and $C_G = 1$, when $P = 100$ and $h_d = 1$.

In the following, for ease of presentation, it is assumed that $\log \mathrm{SNR}$ and $\log \mathrm{INR}$ are integers. Recall that, the parameters m and n of the SLDIC are related to the GSIC as $m = (\lfloor 0.5 \log \mathrm{SNR} \rfloor)^+$ and $n = (\lfloor 0.5 \log \mathrm{INR} \rfloor)^+$, respectively.

[1] When $C \neq 0$, from Fig. 9.1, it appears that the approximate equivalence of the bounds for the GSIC and SLDIC will still hold.

Outer bound in Theorem 20

Consider the following bound in the proof of Theorem 20, when $C = 0$:

$$N[R_1 + 2R_2] \leq h(\mathbf{y}_1^N) + h(\mathbf{y}_1^N, \mathbf{y}_2^N | \widetilde{\mathbf{s}}_1^N, \widetilde{\mathbf{s}}_2^N) - h(\widetilde{\mathbf{z}}_1^N) - h(\widetilde{\mathbf{z}}_2^N) - h(\mathbf{z}_1^N) + N\epsilon'', \tag{9.4}$$

$$\leq h(\mathbf{y}_1^N) + h(\mathbf{y}_1^N | \widetilde{\mathbf{s}}_1^N) + h(\mathbf{y}_2^N | \widetilde{\mathbf{s}}_2^N) - h(\widetilde{\mathbf{z}}_1^N) - h(\widetilde{\mathbf{z}}_2^N) - h(\mathbf{z}_1^N) + N\epsilon'',$$

$$\text{or } R_1 + 2R_2 \leq 0.5 \left[\log(1 + \text{SNR} + \text{INR}) + 2 \log \left(1 + \frac{\text{SNR} + \text{INR}}{1 + \text{INR}} \right) \right],$$

$$\approx 0.5[\log(\text{SNR} + \text{INR}) + 2 \log(\text{SNR} + \text{INR}) - 2 \log \text{INR}], \tag{9.5}$$

where the last equation is obtained for high SNR and INR. Using the above mentioned definitions of m and n, (9.5) reduces to:

$$R_s \leq \begin{cases} \frac{1}{3}[3m - 2n] & \text{for } \alpha \leq 1 \\ \frac{n}{3} & \text{for } \alpha > 1. \end{cases} \tag{9.6}$$

The above is the same as the outer bound for the SLDIC in Theorem 14, when $C = 0$.

Outer bound in Theorem 21

When $C = 0$, the outer bound in Theorem 21 reduces to the following, in the high SNR and high INR regime:

$$R_s \leq 0.5 \log \left(1 + \frac{\text{SNR} + \text{SNR}^2}{1 + \text{SNR} + \text{INR}} \right),$$

$$\approx 0.5 \left[\log \left(\text{INR} + \text{SNR}^2 \right) - \log(\text{SNR} + \text{INR}) \right]. \tag{9.7}$$

Using the above mentioned definitions of m and n, (9.7) reduces to:

$$R_s \leq \begin{cases} 2m - n & \text{for } 1 < \alpha < 2 \\ 0 & \text{for } \alpha \geq 2. \end{cases} \tag{9.8}$$

The above is the same as the outer bound for the SLDIC in Theorem 15, when $C = 0$.

9.2 Discussion and numerical examples

9.2.1 Comparison with existing results

Some observations on how the bounds derived in this work stand in relation to existing works are as follows:

1. When $C_G = 0$, the system reduces to the 2-user GSIC without cooperation, which was studied in [12]. The achievable rate result in Theorem 18 and Corollary 2 reduce to the results reported in [12] in this case.

2. When $C_G = 0$, the achievable result in Theorem 19 reduces to the achievable result in [6, Theorem 3] for the high/very high interference regime $(\alpha > 1)$ for the wiretap channel with a helping interferer.

3. When the capacity of the cooperative links are sufficiently large, then the GSIC with transmitter cooperation reduces to a 2-user Gaussian MIMO broadcast channel (GMBC) with two antennas at transmitter and one antenna at each receiver. The achievable rate result in Corollaries 2 and 3 are found to be very close to the achievable rate result in [4, Theorem 1] for the GMBC, as shown in Fig. 9.2.

4. The proposed outer bounds for the GSIC with limited rate transmitter cooperation in Theorems 20-22 are compared with existing outer bounds for the GSIC with

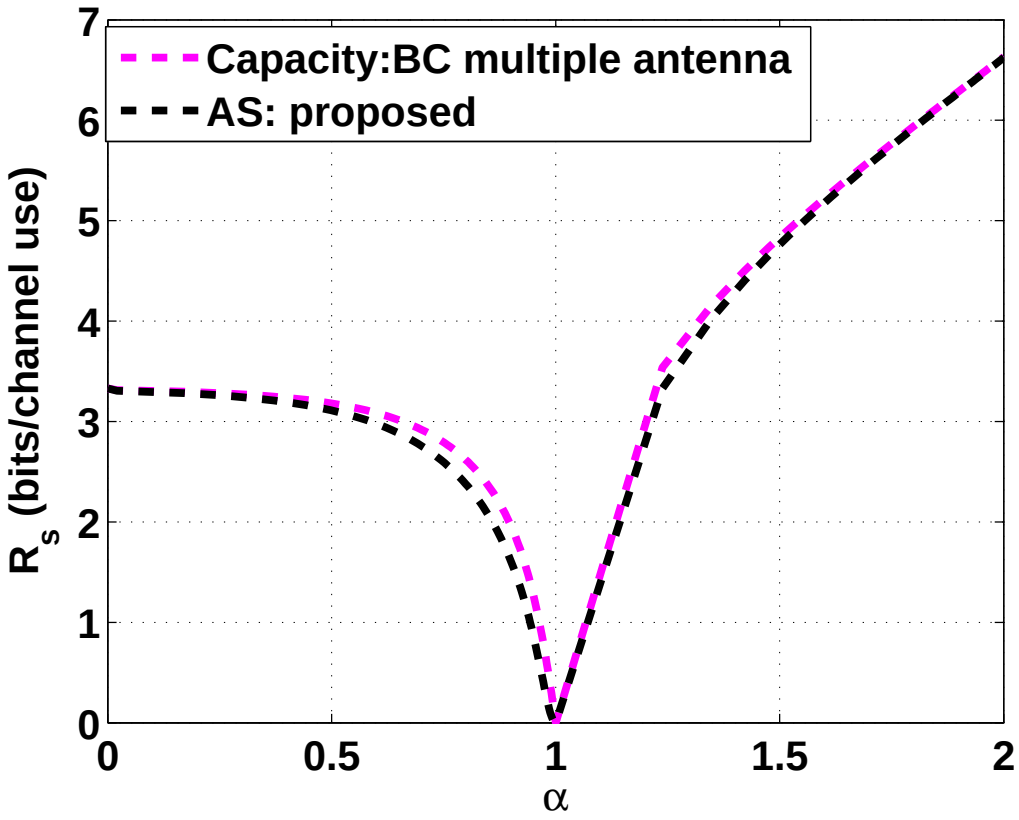


Figure 9.2: Achievable secrecy rate for the GSIC with C_G sufficiently large, and the capacity of the GMBC with two transmit antennas and one receive antenna at each receiver [4]. For the GSIC and GMBC the individual power constraints at each transmitter are $P = 100$ and $P = 200$, respectively. The channel gain to the intended receivers in the case of the GSIC and GMBC: $h_d = 1$.

secrecy constraints at each receiver [5, 6], when $C_G = 0$, in Fig. 9.3. It can be observed that the outer bounds derived in this chapter improve over the best known outer bounds in the literature even in the absence of cooperation $(C_G = 0)$.

In the following section, some numerical examples are considered for the Gaussian cases, to get insights into the bounds for different values of C_G, over different interference regimes.

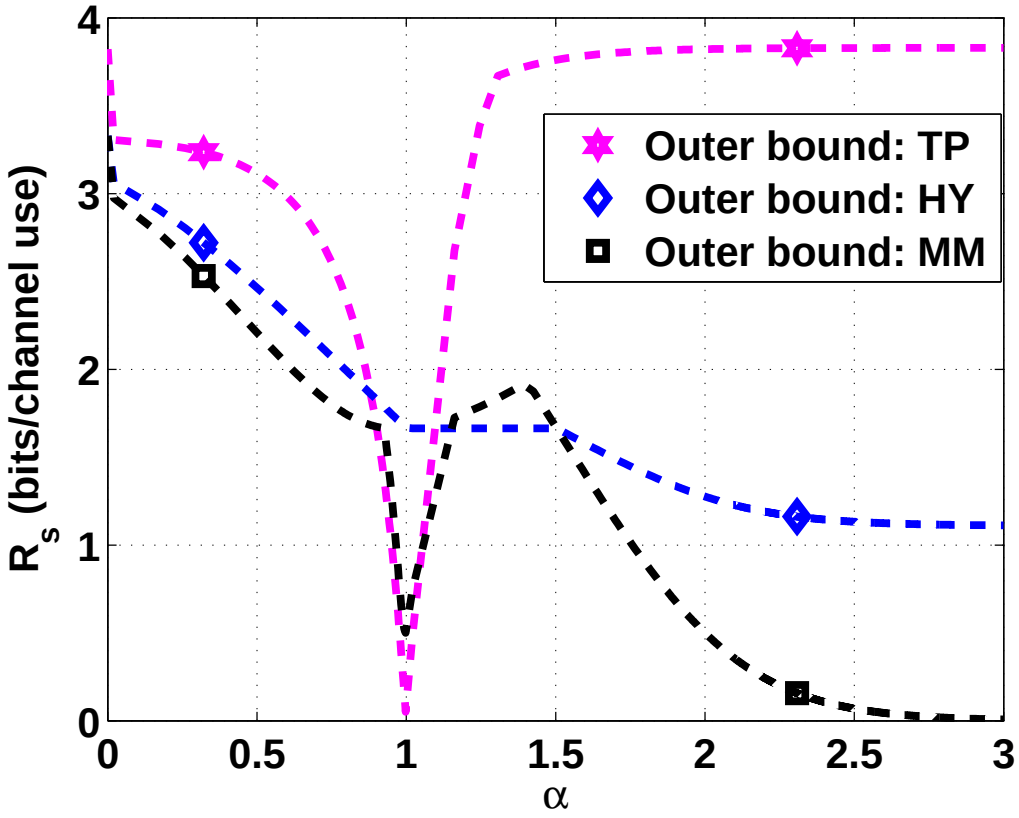


Figure 9.3: Outer bound on the symmetric secrecy rate for the GSIC with $C_G = 0$, $P = 100$ and $h_d = 1$. In the legend, MM stands for the outer bound derived in this work, HY stands for the outer bound on secrecy rate in [5] and TP stands for the outer bound derived in [6].

9.2.2 Numerical examples in the case of the GSIC

In Fig. 9.4, the achievable result in Corollary 2 in Chapter 8 is plotted against α, for different values of C_G, with two types of power allocations. In the first case, no power is alloted for transmitting the dummy message. The power allocations for the non-cooperative private message and cooperative private message are discussed below. For the SLDIC, in the weak and moderate interference regimes, the data bits transmitted on the lower levels $[1 : m-n]$ will not be received at the unintended receiver. For the GSIC,

this corresponds to transmitting the non-cooperative private message such that it is received at the noise floor of the unintended receiver. In the existing literature, this type of power allocation has been used for the private message[2] in the Han-Kobayashi (HK)-scheme [8], and hence, this special case is termed as HKPA (HK-type power allocation) scheme in this chapter. The remaining power is alloted for transmitting the cooperative private message. In the second case, the achievable result in Corollary 2, which involves transmission of a dummy message, is plotted. When $C_G = 0$ and $\alpha > 0.4$, the scheme in Corollary 2 outperforms the HKPA scheme. The gain in the achievable rate largely arises from the transmission of the dummy message. When $C_G = 1$, the gap between the two schemes decreases, except for the initial part of the weak interference regime.

In Fig. 9.5, the achievable symmetric secrecy rate in Corollaries 2 and 3 are plotted against α, for $C_G = 0$ and $P = 100$. Also plotted is the outer bound on the symmetric rate in the case of GSIC without the secrecy constraint at receiver [20]. While plotting the outer bound with secrecy constraint, the minimum of the outer bounds derived in this work and outer bounds in [5, 6, 20] is taken for the $C_G = 0$ case. When $(0 \leq \alpha \leq 1)$, the achievable secrecy rate decreases with increase in the value α. At $\alpha = 1$, the achievable secrecy rate becomes zero. But, with further increase in the value of α, it remains an increasing function of α till around $\alpha = 1.5$, after which the achievable secrecy rate starts to decrease with α. This is due to the fact that the rate of the dummy message sent by one of the users, say user j, is chosen such that it can be decoded and subtracted from the received signal at the receiver i $(i \neq j)$, but the other receiver j is not able to decode the dummy message. As the value of α increases beyond 1.5, the

[2] In [8], there is no secrecy constraint at the receiver and the terminology *private* arises due to the fact that this part of the message is not required to be decodable at the unintended receiver.

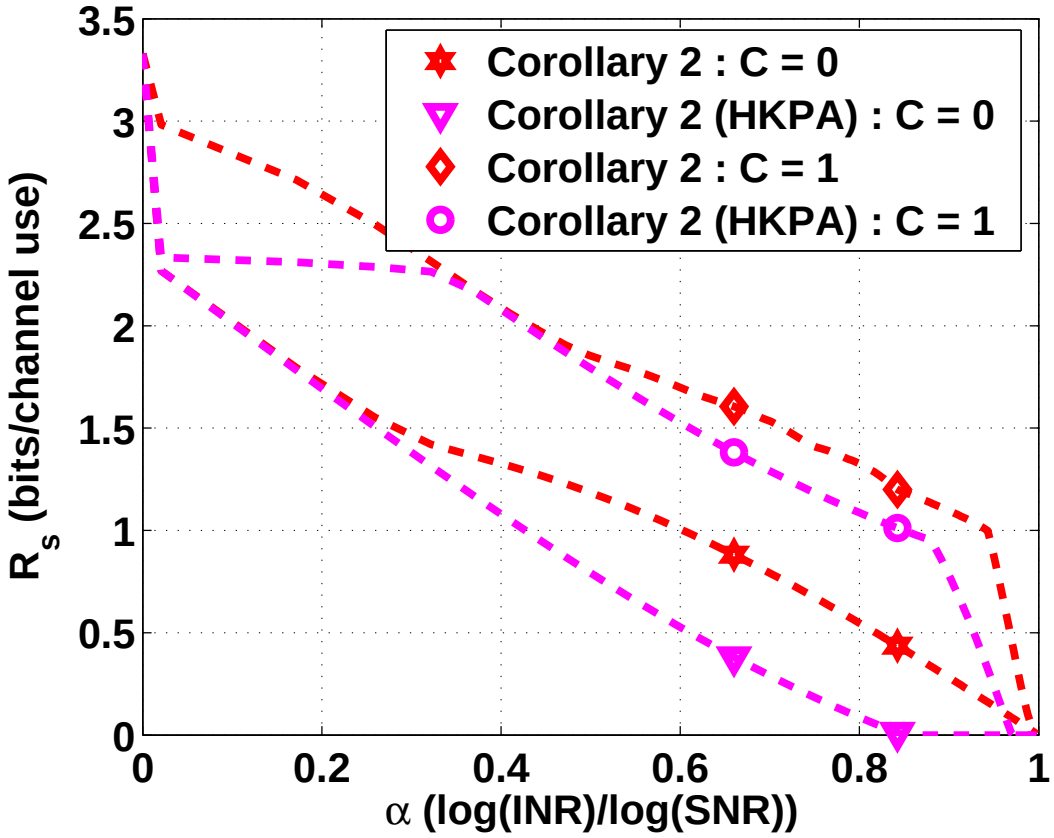


Figure 9.4: Comparison of achievable schemes in Corollary 2 with different power allocations: $P = 100$ and $h_d = 1$.

dummy message does not help much in ensuring secrecy of the non-cooperate private message at receiver j. Also, there is a positive penalty in the achievable rate due to the secrecy constraint at receivers (compared to the rate achievable without the secrecy constraints), except in the weak interference regime.

In Fig. 9.6, the achievable symmetric secrecy rate is plotted against α for $P = 100$ and $C_G = 1$, along with the outer bounds. For plotting the outer bound with secrecy constraints, the minimum of the outer bounds derived in this work and the outer bound in [20] is used. When $\alpha > 1$, the achievable secrecy rate initially increases, and later

decreases with α. Finally, the achievable secrecy rate saturates when $(\alpha \geq 2)$, and this is due to the fact that it is no longer possible to transmit any non-cooperative private message and the gain in the achievable secrecy rate as compared to $C_G = 0$ case is due to cooperation only. Hence, when $C_G > 0$, the proposed scheme achieves nonzero secrecy rate in all the interference regimes except for the $\alpha = 1$ case. Hence, as the value of C_G increases, it is required to assign lower powers for transmitting the dummy message and the non-cooperative private message. By assigning lower power to the non- cooperative private message, the penalty in the achievable secrecy rate due to stochastic encoding also decreases. In the following example, no power is allocated for transmitting the non-cooperative private message and the dummy message.

In Fig. 9.7, the achievable symmetric secrecy rate is plotted against α for $P = 100$ and $C_G = 10$, along with the outer bounds. Here, the achievable secrecy rate and outer bounds are very close to each other. In this case, both the users transmit cooperative private messages only.

9.2.3 Further remarks

1. In the Gaussian case, there is a gap between the inner bound and outer bound. In the Gaussian case, it was not possible to send the non-cooperative private message directly as in the case of SLDIC, and some part of the rate is sacrificed in confusing the unintended receiver.

2. In contrast to the deterministic case, only one of the users transmits dummy information in the Gaussian case. The transmission of dummy information helps to improve the achievable secrecy rate as compared to the case where no dummy

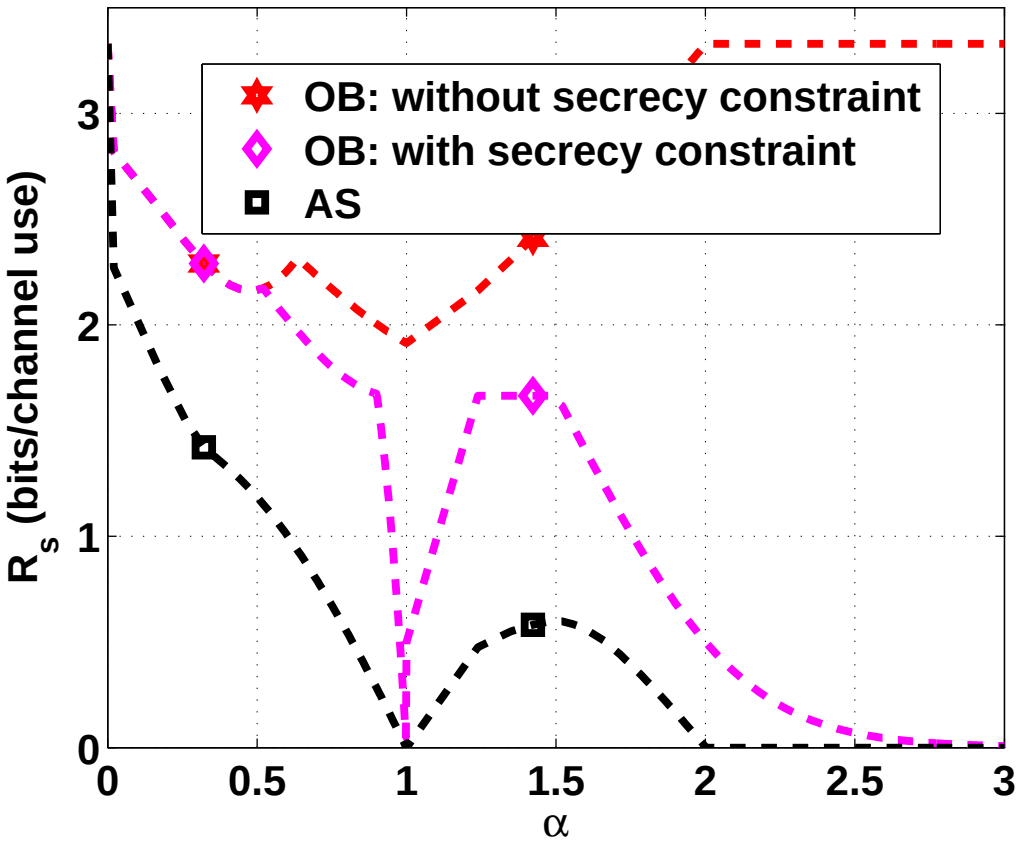


Figure 9.5: Secrecy rate in the case of the GSIC with $P = 100$ and $C_G = 0$.

information is sent.

3. When $1 < \alpha < 2$ and $C_G = 0$, it is not possible to ensure secrecy without transmission of dummy information in the case of GSIC.

4. In all the interference regimes, the proposed scheme always achieves nonzero secrecy rate with cooperation $(\text{i.e.}, C_G > 0)$ in the case of GSIC, except for the $\alpha = 1$ case.

5. In the GSIC, when $C_G \approx \lceil 0.5 \log(1 + h_c^2 P) \rceil$, the achievable secrecy rate is very close to the outer bound (See Fig. 9.7).

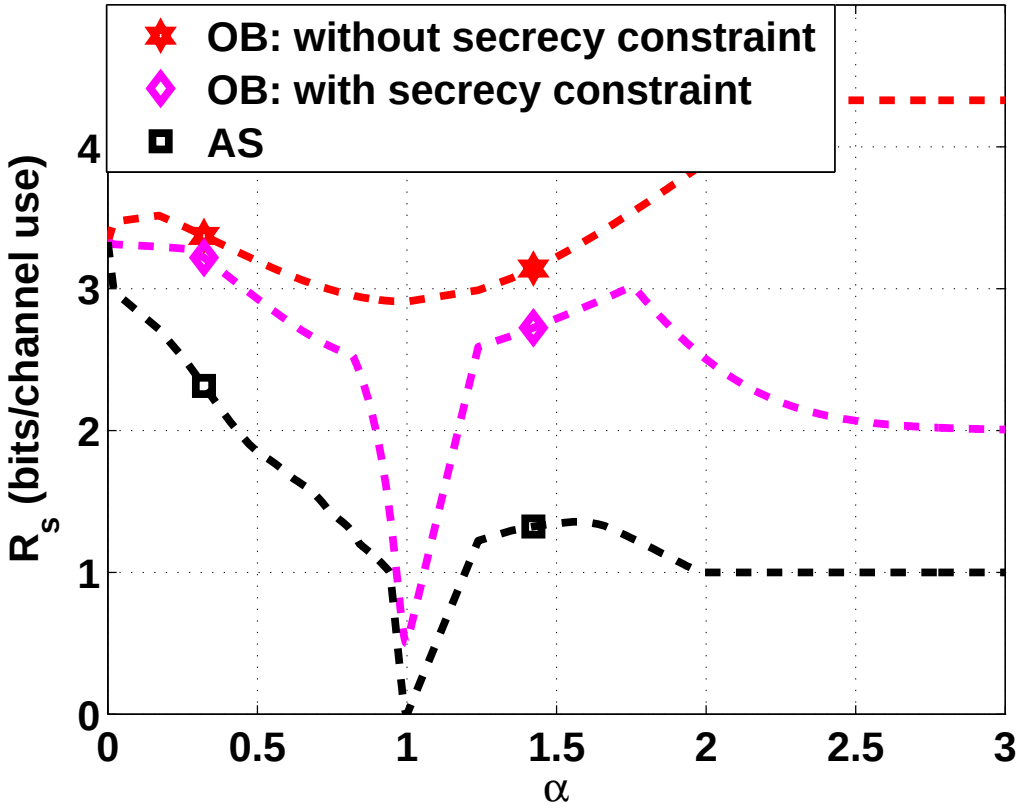


Figure 9.6: Secrecy rate in the case of the GSIC with $P = 100$ and $C_G = 1$.

9.3 Conclusions

In this chapter, the outer bounds on the achievable secrecy rate were presented for the GSIC with limited-rate transmitter cooperation and secrecy constraints at receivers. The outer bounds were compared with the achievable results derived in the previous chapter, which gave interesting insights into the performance limits of the system. It was found that when $C_G \approx \lceil 0.5 \log(1 + h_c^2 P) \rceil$, the achievable secrecy rate is very close to the outer bound. Also, it was observed that, with cooperation, a nonzero secrecy rate can be achieved in almost all cases, except for the $\alpha = 1$ case. These results demonstrate

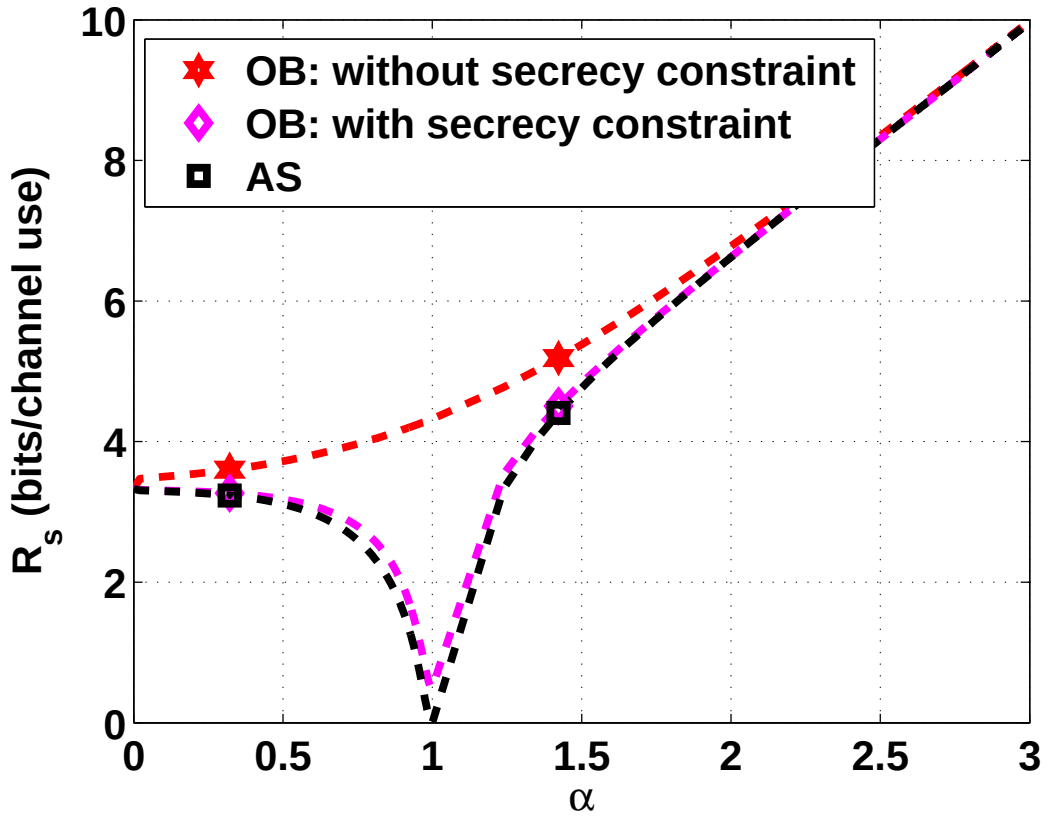


Figure 9.7: Secrecy rate in the case of the GSIC with $P = 100$ and $C_G = 10$.

that having a secure communication link in a network can significantly improve the achievable secrecy rate.

Chapter 10

Conclusions and Future Work

In this thesis, the IC was studied under different settings with and without secrecy constraints, from an information theoretic perspective. The main contributions of this thesis are summarized below.

10.1 Summary of contributions

Chapter 2 proposed an inner bound on the achievable GDOF for the K-user MIMO GSIC, where each transmitter and receiver had M and N antennas, respectively. Inner bounds on the GDOF were derived using a combination of ZF-receiving, treating interference as noise, IA and HK-scheme. The HK-scheme was extended to K-users as a function of M, N and α. The relative performance of these schemes were characterized from an achievable GDOF perspective, when $K > \frac{N}{M}$ ($\frac{N}{M}$ is an integer) and $K \geq \frac{N}{M} + 4$. Also, the interplay between the HK-scheme and IA was explored.

In Chapter 3, three outer bounds on the sum rate were derived for the K-user MIMO GIC. One of the bounds was derived using the notion of cooperation and providing side information, and the other two were based on providing carefully selected partial side

information at the receivers. The novelty of the derivation lies in the careful selection of the side information, which results in the negative differential entropy terms containing signal components canceling out from the sum rate bounds. The outer bounds were simplified for the MIMO GSIC to obtain corresponding outer bounds on the GDOF as a function of K, M, N, and α. The overall outer bound on the GDOF was obtained by taking the minimum of the three bounds and the interference-free GDOF of $\min(M, N)$ per user.

In Chapter 4, the proposed achievable schemes in Chapter 2 were compared with the outer bounds on the per user GDOF derived in the previous chapter. The comparison of the bounds led to interesting insights on the performance limits of the multiuser MIMO GIC and the relative efficacy of different techniques for interference management. For example, it was found that when $M = N$, treating interference as noise performs as well as the HK-scheme and outperforms both IA and ZF-receiving. However, when $N > M$, treating interference as noise is always suboptimal. The maximum of the HK-scheme and IA outperforms both treating interference as noise and ZF-receiving, for all values of K, M, N, and α. When $\frac{N}{M} < K \leq \frac{N}{M} + 1$, the HK-scheme was found to be GDOF optimal for all values of α. Treating interference as noise was found to be GDOF optimal in the weak interference case $(0 \leq \alpha \leq \frac{1}{2})$ when $M = N$ for any K.

Chapter 5 explored the construction of precoding and receive filtering matrices for IA for constant or quasi-static MIMO channels with finite symbol extensions. A new metric was proposed to measure the performance of IA algorithms, that captured the possible loss in signal dimension while designing the precoders. Inspired by the metric, two algorithms for finding the precoding and receive filtering matrices for IA were

proposed. The first algorithm for IA was based on aligning some of the interfering signal sub-streams at each receiver. Also, the necessary conditions for solution to exist was derived. As the first algorithm required global channel knowledge at each node, a distributed algorithm was proposed which required limited channel knowledge and also preserved the dimensionality of the desired signal at the intended receiver. It was shown that the algorithms outperform existing algorithms achieving IA using linear precoding at the transmitters.

In Chapters 2-5, the issue of ensuring security of individual messages arising due to the broadcast nature of the wireless medium was not taken into consideration. In the remaining chapters of the thesis, the 2-user IC with security constraints was considered, where individual messages need to be kept secret from the unintended receiver. Also, the transmitters were allowed to cooperate through a noiseless link of finite rate.

In Chapters 6-9, the role of limited-rate transmitter cooperation in facilitating secure communication over the 2-user IC was explored. In Chapter 6, novel achievable schemes were proposed for the 2-user SLDIC with transmitter cooperation. The achievable scheme used a combination of interference cancelation, random bits transmission, relaying of the other user's data bits, and time sharing, depending on the values of α and C. Several useful insights were obtained from the proposed achievable schemes. For example, it was found that when $\frac{2}{3} < \alpha < 1$ and $1 < \alpha < 2$, random bit transmission can enhance the achievable secrecy rate. However, when $\alpha \geq 2$ and $C = 0$, it was not possible to ensure secrecy. But, with cooperation (i.e., when $C > 0$), it was possible to achieve a nonzero secrecy rate and the proposed scheme which involved sharing random bits, or data bits, or both, outperformed sharing only data bits through

the cooperative links. Finally, when $0 < \alpha \leq \frac{1}{2}$, the achievable scheme was found to be optimal for all values of C.

Chapter 7 proposed novel outer bounds on the achievable secrecy rate for the 2-user SLDIC with transmitter cooperation. The derivation of the outer bounds was based on providing side information to receiver in a carefully chosen manner, the use of the secrecy constraints at the receivers, and partitioning of the encoded message/output. The outer bounds were compared with the achievable schemes obtained in the previous chapter. These bounds gave useful insights on the performance limits of the system under security constraints. For example, it was observed that, there is a nonzero loss in the achievable rate relative to the capacity without the secrecy constraint when $C < n$, except when $0 \leq \alpha \leq \frac{1}{2}$. Also, the derived outer bounds helped to establish that sharing random bits through the cooperative link can achieve the optimal rate when $\alpha \geq 2$ and $(0 < C \leq \lceil \frac{m}{2} \rceil)$.

In Chapter 8, achievable schemes were proposed for the GSIC with limited-rate transmitter cooperation and secrecy constraints at receivers, using the intuitions obtained from study of SLDIC in Chapter 6. The achievable scheme used a combination of stochastic encoding and cooperative encoding scheme, along with dummy information transmission. The achievable scheme for the high interference regime required the dummy information sent by one of the users to be decodable at the other receiver, in contrast to the achievable scheme for the weak/moderate interference regime.

In Chapter 9, the outer bounds on the achievable secrecy rate were presented for the GSIC with limited-rate transmitter cooperation and secrecy constraints at receivers. The novelty in deriving these bounds was in the translation of the ideas obtained from the

deterministic case to the Gaussian case. The outer bounds were compared with the achievable results derived in the previous chapter, which gave useful insights on the performance limits of the system. It was found that when $C_G \approx \lceil 0.5 \log (1 + h_c^2 P) \rceil$, the achievable secrecy rate is very close to the outer bound.Also, it was observed that, with cooperation, a nonzero secrecy rate can be achieved in almost all cases, except for the $\alpha = 1$ case.

10.2 Future work

Future work could study the following issues:

1. The achievable results and outer bounds on GDOF in Chapter 2 and 3, respectively, assume knowledge of global CSI at transmitters and receivers. It will be interesting to conduct more detailed analysis on the effect of imperfect or outdated CSI on the achievable GDOF or the outer bound on the GDOF for K-user MIMO GIC. Some initial results related to this can be found in [78,79].

2. In Chapter 6-9, it is assumed that transmitters trust each other completely and they do not deviate from the agreed-upon scheme. When there is lack of trust between the transmitters, it would be pertinent to analyze the IC under a robust notion of secrecy, where user i must preserve its secrecy even when user j $(j \neq i)$ deviates from the agreed-upon scheme.

3. Also, studying the IC channel with rate-limited transmitter or receiver cooperation in the presence of an external eavesdroppers from an information theoretic view is an interesting direction for future work.

Appendix A

Appendix for Chapter 2

A.1 Proof of Theorem 2

When interference is treated as noise, the rate achieved by user j for the MIMO GSIC is bounded as

$$\begin{aligned} R_j &\geq \log \left| \mathbf{I}_N + \rho \mathbf{H}_{jj} \mathbf{P}_j \mathbf{H}_{jj}^H + \rho^\alpha \sum_{i=1, i\neq j}^{K} \mathbf{H}_{ji} \mathbf{P}_i \mathbf{H}_{ji}^H \right| - \log \left| \mathbf{I}_N + \rho^\alpha \sum_{i=1, i\neq j}^{K} \mathbf{H}_{ji} \mathbf{P}_i \mathbf{H}_{ji}^H \right|, \\ &= \left[r + \min \left\{ r^{'}, N - r \right\} \alpha - \alpha r^{'} \right] \log \rho + \mathcal{O}(1), \end{aligned} \tag{A.1}$$

where $r \triangleq \text{rank}(\mathbf{H}_{jj} \mathbf{P}_j \mathbf{H}_{jj}^H)$ and $r^{'} \triangleq \text{rank}(\sum_{i=1, i\neq j}^{K} \mathbf{H}_{ji} \mathbf{P}_i \mathbf{H}_{ji}^H)$. The last equation is obtained using Lemma 4 in [42]. As the input covariance matrix $\mathbf{P}_i$ is full rank, (A.1) becomes:

$$R_j \geq \left[M + \min \left\{ \min \left\{ (K-1)M, N \right\}, N - M \right\} \alpha \; - \min \left\{ (K-1)M, N \right\} \alpha \right] \log \rho + \mathcal{O}(1). \tag{A.2}$$

When $\frac{N}{M} < K \leq \frac{N}{M} + 1$, $N - M \leq (K-1)M \leq N$, and hence, (A.2) becomes

$$R_j \geq \left[M + (N - M)\alpha - (K-1)M\alpha \right] \log \rho + \mathcal{O}(1). \tag{A.3}$$

Thus, the per user GDOF that can be achieved in this case is

$$d(\alpha) \geq M + (N - KM)\alpha. \tag{A.4}$$

When $K > \frac{N}{M} + 1$, $\min\{(K-1)M, N\} = N$, and hence, (A.2) becomes

$$R_j \geq [M + \min\{N, N - M\}\,\alpha - N\alpha] \log \rho + \mathcal{O}(1). \tag{A.5}$$

The achievable per user GDOF in this case is $d(\alpha) \geq M(1-\alpha)$. Combining this with (A.4) results in Theorem 2.

A.2 Proof of Theorem 3

Due to the symmetry of the problem, it is sufficient to derive the GDOF achieved by any particular user, say user 1. Consider a user subset $S \subseteq \{2, \ldots, K\}$, and let $S' \triangleq S \cup \{1\}$, i.e., S is a subset of users excluding user 1, while S' always includes user 1. The number of users in the set S is denoted by $|S| \leq K-1$ and number of users in S' is $|S|+1$. The following two cases are considered.

When $(\frac{N}{M} < K \leq \frac{N}{M} + 1)$

Now, using the MAC channel formed at the receiver of user 1 with the signals from the user set S, the achievable sum rate is bounded as:

$$\sum_{j \in S} R_j \leq \log |\mathbf{I}_N + \rho^\alpha \sum_{j \in S} \mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H| = \min\{|S|M, N\}\,\alpha \log \rho + \mathcal{O}(1),$$
$$\text{or } R_j \leq M\alpha \log \rho + \mathcal{O}(1). \tag{A.6}$$

To get the last equation above, note that $|S|_{\max} = K - 1$. Since $\frac{N}{M} < K \leq \frac{N}{M} + 1$, this implies $\min\{|S|M, N\} = |S|M$. Similarly, using the MAC channel formed at the receiver of user 1 with signals from the user set S', the achievable sum rate is bounded as:

$$\begin{aligned}\sum_{j\in S'} R_j &\leq \log|\mathbf{I}_N + \rho\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H + \rho^\alpha \sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H|, \\ &= [|S|M\alpha + \min\{M, N - |S|M\}]\log\rho + \mathcal{O}(1). \end{aligned} \tag{A.7}$$

Again, Lemma 4 in [42] is used to obtain the last equation above.

Now, when $\min\{M, N - |S|M\} = N - |S|M$, since $K \leq \frac{N}{M} + 1$, the condition becomes $\frac{N}{M} \leq 1 + |S| \leq \frac{N}{M} + 1$ and (A.7) reduces to the following form:

$$R_j \leq \frac{|S|M(\alpha - 1) + N}{1 + |S|}\log\rho + \mathcal{O}(1). \tag{A.8}$$

The right hand side above is minimized when $|S| = |S|_{\max} = K - 1$; and recall that $K \leq \frac{N}{M} + 1$. Hence, (A.8) becomes

$$R_j \leq \frac{(K-1)M(\alpha - 1) + N}{K}\log\rho + \mathcal{O}(1). \tag{A.9}$$

When $\min\{M, N - |S|M\} = M$, $1 + |S| \leq \frac{N}{M}$, and (A.7) becomes:

$$R_j \leq \frac{|S|\alpha + 1}{|S| + 1}M\log\rho + \mathcal{O}(1). \tag{A.10}$$

The term in the right hand side of the above equation is minimized when $|S| = 0$ and

this results in following equation:

$$R_j \leq M \log \rho + \mathcal{O}(1). \tag{A.11}$$

The achievable rate is obtained by taking the minimum of (A.6), (A.9) and (A.11). It can be observed that (A.6) becomes superfluous given (A.11). Finally, taking the minimum of (A.9) and (A.11) results in case 1 of Theorem 3.

When $(K > \frac{N}{M} + 1)$

Now, using the MAC channel formed at the receiver of user 1 with the signals from the user set S, the achievable sum rate is bounded as:

$$\sum_{j \in S} R_j \leq \log |\mathbf{I}_N + \rho^{\alpha} \sum_{j \in S} \mathbf{H}_{1j} \mathbf{P}_j \mathbf{H}_{1j}^H| = \min \{|S|M, N\} \, \alpha \log \rho + \mathcal{O}(1). \tag{A.12}$$

If $\min \{|S|M, N\} = |S|M$, then the above equation simplifies to:

$$R_j \leq M\alpha \log \rho + \mathcal{O}(1). \tag{A.13}$$

If $\min \{|S|M, N\} = N$, then (A.12) simplifies to:

$$R_j \leq \frac{N\alpha}{|S|} \log \rho + \mathcal{O}(1), \text{ where } |S| \leq K - 1. \tag{A.14}$$

Similarly, using the MAC channel formed at the receiver of user 1 with the signals from the user set S', the achievable sum rate is bounded as:

$$\begin{aligned}\textstyle\sum_{j\in S'} R_j &\leq \log|\mathbf{I}_N + \rho\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H + \rho^\alpha \sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H|, \\ &= [\min\{|S|M, N\}\alpha + \min\{M, N - \min(|S|M, N)\}]\log\rho + \mathcal{O}(1). \end{aligned} \quad \text{(A.15)}$$

Again, Lemma 4 in [42] is used to obtain the last equation above. The above equation is simplified under the following cases.

Case a): When $\min\{|S|M, N\} = |S|M$, (A.15) becomes:

$$\sum_{j\in S'} R_j \leq |S|M\alpha\log\rho + \min\{M, N - |S|M\}\log\rho + \mathcal{O}(1), \quad \text{(A.16)}$$

When $\min\{M, N - |S|M\} = N - |S|M$, then it results in the condition $\frac{N}{M} - 1 \leq |S| \leq \frac{N}{M}$ and (A.16) becomes:

$$R_j \leq \frac{|S|M(\alpha - 1) + N}{1 + |S|}\log\rho + \mathcal{O}(1). \quad \text{(A.17)}$$

The value of $|S|$ which minimizes the RHS of the above equation is discussed in the later part of the proof. When $\min\{M, N - |S|M\} = M$, it results in the condition $|S| \leq \frac{N}{M} - 1 < \frac{N}{M}$ and (A.16) becomes

$$R_j \leq \frac{|S|\alpha + 1}{|S| + 1}M\log\rho + \mathcal{O}(1). \quad \text{(A.18)}$$

The right hand side in the above equation is minimized when $|S| = 0$. This results in

$$R_j \leq M\log\rho + \mathcal{O}(1). \quad \text{(A.19)}$$

Case b: When $\min\{|S|M, N\} = N$, (A.15) reduces to:

$$R_j \leq \frac{N\alpha}{|S|+1}\log\rho + \mathcal{O}(1), \tag{A.20}$$

Above equation is minimized when $|S| = K-1$ and (A.20) becomes:

$$R_j \leq \frac{N\alpha}{K}\log\rho + \mathcal{O}(1). \tag{A.21}$$

Finally, taking minimum of (A.13), (A.14), (A.17), (A.19) and (A.21) the achievable GDOF is obtained as follows. Given (A.19), the equation in (A.13) becomes superfluous as $\alpha > 1$. Similarly, given (A.21), the equation in (A.14) is redundant. Also, (A.17) is redundant given (A.19) and (A.21) as explained below, when $\frac{N}{M}$ is an integer. There are two possible values of $|S|$ which satisfies the condition: $\frac{N}{M} - 1 \leq |S| \leq \frac{N}{M}$. When $|S| = \frac{N}{M} - 1$, (A.17) reduces to following form:

$$R_j \leq \frac{\left(\frac{N}{M}-1\right)M(\alpha-1)+N}{\frac{N}{M}}\log\rho + \mathcal{O}(1). \tag{A.22}$$

It is not difficult to observe that given (A.19), (A.22) is redundant. When $|S| = \frac{N}{M}$, (A.17) becomes

$$R_j \leq \frac{N\alpha}{\frac{N}{M}+1}\log\rho + \mathcal{O}(1). \tag{A.23}$$

As $K > \frac{N}{M} + 1$, given (A.21), the rate in (A.23) becomes superfluous. When $\frac{N}{M}$ is not an integer, then with some algebraic manipulations, it can be shown that (A.17) is redundant given (A.21). Finally by taking minimum of (A.19) and (A.21) results in the second case of Theorem 3. This completes the proof.

A.3 Proof of Theorem 4

First, the rate obtained due to the private part of the message is obtained. As the private message is decoded last, the rate of the private message is obtained by treating all remaining users' private messages as noise. Due to symmetry of the problem, it is sufficient to consider only one particular user. The rate achieved by the private part is

$$\begin{aligned} R_{p,j} &\leq \log \left| \mathbf{I}_N + \left(\mathbf{I}_N + \sum_{j=1, j\neq i}^{K} \mathbf{H}_{ji} \mathbf{P}_i \mathbf{H}_{ji}^H \right)^{-1} \rho^{1-\alpha} \mathbf{H}_{jj} \mathbf{P}_j \mathbf{H}_{jj}^H \right|, \\ &= M(1-\alpha) \log \rho + \mathcal{O}(1). \end{aligned} \tag{A.24}$$

For obtaining the rate due to the common part of the message, the following two cases are considered. In both the cases, different subsets of users are considered, as in Appendix A.2. Consider the set $S^{'} \subseteq \{1, 2, \ldots, K\}$, where user 1 is always included in the subset. Since common messages need to be decodable at every receiver, user 1 should be able to decode the other users' common messages as well as its own common message. While decoding the common message, it should treat all other users' private messages as well as its own private message as noise.

When $(\frac{N}{M} < K \leq \frac{N}{M} + 1)$

The common messages form a MAC channel at Receiver 1. The achievable rate due to the signals from $S^{'}$ is:

$$\sum_{j \in S'} R_{c,j} \leq \log |\mathbf{I}_N + (\mathbf{I}_N + \sum_{j \in S} \mathbf{H}_{1j} \mathbf{P}_j \mathbf{H}_{1j}^H + \rho^{(1-\alpha)} \mathbf{H}_{11} \mathbf{P}_1 \mathbf{H}_{11}^H)^{-1} \sum_{j \in S'} P_{c,j} \mathbf{H}_{1j} \mathbf{P}_j \mathbf{H}_{1j}^H|. \tag{A.25}$$

Here, $P_{c,j} \triangleq \rho^{\alpha} - 1$ when $j \neq 1$ and $P_{c,j} \triangleq \rho - \rho^{(1-\alpha)}$ when $j = 1$. Now, (A.25) becomes:

$$\begin{aligned}\sum_{j\in S'} R_{c,j} &\leq \log|\mathbf{I}_N + \sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H + \rho^{(1-\alpha)}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H + \left(\rho - \rho^{(1-\alpha)}\right)\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H \\ &\quad + (\rho^{\alpha}-1)\sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H| - \log\left|\mathbf{I}_N + \rho^{(1-\alpha)}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H\right|, \\ &= \log|\mathbf{I}_N + \rho\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H + \rho^{\alpha}\sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H| - \log\left|\mathbf{I}_N + \rho^{(1-\alpha)}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H\right| + \mathcal{O}(1), \\ &= \left[M\alpha + \min\left\{|S|M, N-M\right\}\alpha\right]\log\rho + \mathcal{O}(1). \end{aligned} \tag{A.26}$$

Equation (A.26) is obtained using Lemma 4 in [42] and $|S|M \leq (K-1)M \leq N$. The above equation is simplified under the following cases.

Case a: When $\min\{|S|M, N-M\} = N-M$, we have $N \leq (1+|S|)M$. Since $\frac{N}{M} < K \leq \frac{N}{M} + 1$ and $|S| \leq K-1$, the inequality can only be satisfied for $|S| = K-1$, and hence (A.26) becomes:

$$R_{c,j} \leq \frac{N\alpha}{K}\log\rho + \mathcal{O}(1). \tag{A.27}$$

Case b: When $\min\{|S|M, N-M\} = |S|M$, we have $(1+|S|)M \leq N$. This condition is satisfied when $|S| < K-1$, and (A.26) simplifies to

$$R_{c,j} \leq M\alpha\log\rho + \mathcal{O}(1). \tag{A.28}$$

Now consider the user subset $S \subseteq \{2,\ldots,K\}$. A MAC channel is formed at Receiver 1 due to the signals from users in S. The achievable sum rate in this case is:

$$\begin{aligned}\sum_{j\in S} R_{c,j} &\leq \log|\mathbf{I}_N + (\mathbf{I}_N + \sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H + \rho^{(1-\alpha)}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H)^{-1}(\rho^{\alpha}-1)\sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H|, \\ &= \left[|S|M\alpha + \min\left\{M, N-|S|M\right\}(1-\alpha) - M(1-\alpha)\right]\log\rho + \mathcal{O}(1), \end{aligned} \tag{A.29}$$

where, to obtain the last equation above, Lemma 4 in [42] and the inequality $\alpha \geq (1-\alpha)$ was used. Equation (A.29) is simplified under the following cases:

Case b(i): When $\min\{M, N-|S|M\} = N-|S|M$, then $N-|S|M \leq M$. This condition is satisfied when $|S| = K-1$, and (A.29) reduces to:

$$R_{c,j} \leq \frac{1}{K-1}\left[M\left\{\alpha\left(2K-1\right)-K\right\}+N(1-\alpha)\right]\log\rho+\mathcal{O}(1). \tag{A.30}$$

Case b(ii): When $\min\{M, N-|S|M\} = M$, it results in $(1+|S|)M \leq N$. Under this condition, (A.29) reduces to

$$R_{c,j} \leq M\alpha\log\rho+\mathcal{O}(1). \tag{A.31}$$

The achievable rate is obtained by taking the minimum of (A.27), (A.28), (A.30) and (A.31). As $N < KM$, (A.28) and (A.31) become superfluous given (A.27). The achievable GDOF by the common part of the message is thus given by

$$d_c(\alpha) \geq \min\left\{\frac{N\alpha}{K}, \frac{1}{K-1}\left[M\left\{\alpha\left(2K-1\right)-K\right\}+N(1-\alpha)\right]\right\}. \tag{A.32}$$

From (A.24), one obtains $d_p(\alpha) \geq M(1-\alpha)$. Adding this and (A.32), the total GDOF achievable by the private part and the common part together is obtained, resulting in the first case of the right hand side in (2.9). This completes the proof for the first case of Theorem 4.

When $(K > \frac{N}{M} + 1)$

The achievable rate due to the signals from S' is:

$$\sum_{j \in S'} R_{c,j} \leq \log |\mathbf{I}_N + \rho \mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H + \rho^{\alpha} \sum_{j \in S} \mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H| - \log \left|\mathbf{I}_N + \rho^{1-\alpha}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H\right| + \mathcal{O}(1),$$
$$= \left[M + \min\left\{\min\left\{N, |S|M\right\}, N - M\right\}\alpha - M(1-\alpha)\right]\log\rho + \mathcal{O}(1). \quad \text{(A.33)}$$

The above equation is obtained using Lemma 4 in [42]. It can be simplified under the following cases.

Case a: When $\min\{N, |S|M\} = N$, then $\frac{N}{M} \leq |S|$ and the maximum value of $|S|$ which satisfies this condition is $K - 1$. Under this condition, (A.33) becomes:

$$R_{c,j} \leq \frac{N\alpha}{K}\log\rho + \mathcal{O}(1). \quad \text{(A.34)}$$

Case b: When $\min\{N, |S|M\} = |S|M$, then $|S| \leq \frac{N}{M}$. Under this condition, (A.33) becomes:

$$\sum_{j \in S'} R_{c,j} \leq M\log\rho + \min\left\{|S|M, N - M\right\}\alpha\log\rho - M(1-\alpha)\log\rho + \mathcal{O}(1). \quad \text{(A.35)}$$

When $\min\left\{|S|M, N - M\right\} = N - M$, then $\frac{N}{M} \leq |S| + 1$. The achievable rate becomes

$$R_{c,j} \leq \frac{N\alpha}{1 + |S|}\log\rho + \mathcal{O}(1). \quad \text{(A.36)}$$

The above equation is minimized by taking largest integer value of $|S|$ which satisfies the condition: $\frac{N}{M} \leq |S| + 1 \leq \frac{N}{M} + 1$.

When $\min\{|S|M, N-M\} = |S|M$, then $|S| < 1 + |S| \leq \frac{N}{M}$ and (A.35) becomes:

$$R_{c,j} \leq M\alpha \log \rho + \mathcal{O}(1). \tag{A.37}$$

Now consider the user set $S \subseteq \{2, 3, \ldots, K\}$. As this forms a MAC channel at receiver 1, from (A.29), the following rate equation is obtained:

$$\begin{aligned}\sum_{j\in S} R_{c,j} &\leq \log|\mathbf{I}_N + \rho^{\alpha}\sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H + \rho^{1-\alpha}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H| - \log|\mathbf{I}_N + \rho^{1-\alpha}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H|, \\ &= [\min\{N, |S|M\}\,\alpha + \min\{M, N - \min(N, |S|M)\}\,(1-\alpha) - M(1-\alpha)]\log\rho \\ &\quad + \mathcal{O}(1),\end{aligned} \tag{A.38}$$

where the above uses the fact that $\alpha > 1 - \alpha$ in the moderate interference regime. The above equation is simplified under the following cases.

Case a: When $\min\{N, |S|M\} = |S|M$, then $|S| \leq \frac{N}{M}$. Under this condition, (A.38) becomes

$$\sum_{j\in S} R_{c,j} \leq [|S|M\alpha + \min\{M, N - |S|M\}\,(1-\alpha) - M(1-\alpha)]\log\rho + \mathcal{O}(1). \tag{A.39}$$

Above equation is further simplified as follows. When $\min\{M, N - |S|M\} = N - |S|M$, then $\frac{N}{M} - 1 \leq |S| \leq \frac{N}{M}$ and (A.39) becomes:

$$R_{c,j} \leq M(2\alpha - 1)\log\rho + \frac{(N-M)(1-\alpha)}{|S|}\log\rho + \mathcal{O}(1). \tag{A.40}$$

The above equation is required to be minimized by taking largest possible integer value of $|S|$, which also satisfies $\frac{N}{M} - 1 \leq |S| \leq \frac{N}{M}$. To simplify the analysis, consider $\frac{N}{M}$ is an integer. When $\frac{N}{M}$ is not an integer, it is straightforward to see that the arguments to

follow remain valid, as $\lfloor \frac{N}{M} \rfloor < \frac{N}{M}$. Hence, (A.40) is minimized by taking $|S| = \frac{N}{M}$ and (A.40) becomes:

$$R_{c,j} \leq M(2\alpha - 1)\log\rho + \frac{(N-M)(1-\alpha)}{\frac{N}{M}}\log\rho + \mathcal{O}(1). \tag{A.41}$$

When $\min\{M, N - |S|M\} = M$, then $|S| \leq \frac{N}{M} - 1 < \frac{N}{M}$ and (A.39) becomes:

$$R_{c,j} \leq M\alpha\log\rho + \mathcal{O}(1). \tag{A.42}$$

Case b: When $\min\{N, |S|M\} = N$, then $\frac{N}{M} \leq |S|$. Under this condition, (A.38) becomes:

$$R_{c,j} \leq \frac{N\alpha - M(1-\alpha)}{|S|}\log\rho + \mathcal{O}(1). \tag{A.43}$$

The above equation is minimized when $|S| = K - 1$ and (A.43) becomes:

$$R_{c,j} \leq \frac{N\alpha - M(1-\alpha)}{K-1}\log\rho + \mathcal{O}(1). \tag{A.44}$$

The achievable rate by the common part when $K > \frac{N}{M} + 1$ of the message is obtained by taking minimum of (A.34), (A.36), (A.37), (A.41), (A.42) and (A.44). It can be observed that (A.37) and (A.42) are redundant given (A.34) as $N < KM$. As $K > \frac{N}{M} + 1$, (A.41) is redundant given (A.44). Also, (A.36) is redundant given (A.34). Now the achievable GDOF obtained by the common part of the message is:

$$d_c(\alpha) \geq \min\left\{\frac{N\alpha}{K}, \frac{N\alpha - M(1-\alpha)}{K-1}\right\}. \tag{A.45}$$

From (A.24), one obtains $d_p(\alpha) \geq M(1-\alpha)$. Adding this and (A.45), the total GDOF achievable by the private part and the common part together is obtained, resulting in

the second case of the right hand side in (2.9). This completes the proof for the second case of Theorem 4.

A.4 Proof of Theorem 5

The GDOF achieved by the private part is the same as in the moderate interference case:

$$d_p(\alpha) \geq M(1-\alpha). \tag{A.46}$$

To obtain the rate for the common part of the message, the same procedure is followed as described in the moderate interference case. The following two cases are considered:

When $\left(\frac{N}{M} < K \leq \frac{N}{M} + 1\right)$

In order to obtain the rate for the common part, consider the MAC channel formed at Receiver 1 due to the users in $S \subseteq \{2, \ldots, K\}$. The sum rate constraint leads to

$$\begin{aligned}\sum_{j\in S} R_{c,j} &\leq \log|\mathbf{I}_N + \rho^{\alpha}\sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H + \rho^{(1-\alpha)}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H| - \log|\mathbf{I}_N + \rho^{(1-\alpha)}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H|,\\ &= \min\{|S|M, N-M\}\,\alpha\log\rho + \mathcal{O}(1).\end{aligned} \tag{A.47}$$

When $\min\{|S|M, N-M\} = N-M$, then $N \leq (1+|S|)M$. This implies $|S| = K-1$, and (A.47) becomes:

$$R_{c,j} \leq \frac{N-M}{K-1}\alpha\log\rho + \mathcal{O}(1). \tag{A.48}$$

When $\min\{|S|M, N-M\} = |S|M$, then $(1+|S|)M \leq N$. This condition results when $|S| < K-1$, and hence, (A.47) reduces to:

$$R_{c,j} \leq M\alpha \log \rho + \mathcal{O}(1). \tag{A.49}$$

Now consider the user set $S^{'} = S \cup \{1\}$, where user 1 is always included. The sum rate constraint for the common part of the message is given by:

$$\begin{aligned}\sum_{j\in S'} R_{c,j} &\leq \log\left|\mathbf{I}_N + \rho\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H + \rho^{\alpha}\sum_{j\in S}\mathbf{H}_{1j}\mathbf{P}_j\mathbf{H}_{1j}^H\right| - \log\left|\mathbf{I}_N + \rho^{(1-\alpha)}\mathbf{H}_{11}\mathbf{P}_1\mathbf{H}_{11}^H\right| + \mathcal{O}(1),\\ &= \left[M\alpha + \min\left\{\min\left\{N, |S|M\right\}, N-M\right\}\alpha\right]\log\rho + \mathcal{O}(1).\end{aligned} \tag{A.50}$$

As $K \leq \frac{N}{M} + 1$, we have $(K-1)M \leq N$ or $|S|M \leq N$, and (A.50) further simplifies to

$$\sum_{j\in S'} R_{c,j} \leq \left[M\alpha + \min\left\{|S|M, N-M\right\}\alpha\right]\log\rho + \mathcal{O}(1). \tag{A.51}$$

It can be seen that (A.26) and (A.51) are the same, and hence, the above can be simplified as in (A.26). When $\min\{|S|M, N-M\} = N-M$, (A.51) becomes

$$R_{c,j} \leq \frac{N\alpha}{K}\log\rho + \mathcal{O}(1). \tag{A.52}$$

When $\min\{|S|M, N-M\} = |S|M$, (A.51) becomes

$$R_{c,j} \leq M\alpha \log\rho + \mathcal{O}(1). \tag{A.53}$$

The rate achievable by the common part of the message is obtained by taking the minimum of (A.48), (A.49), (A.52) and (A.53). With some algebraic manipulation, it can be

shown that given (A.48), all the remaining equations become superfluous. The achievable GDOF due to the common part of the message is thus given by

$$d_c(\alpha) \geq \frac{N-M}{K-1}\alpha. \tag{A.54}$$

The per user GDOF achievable in this case is obtained by adding (A.46) and (A.54), resulting in the expression given by (2.10).

When $\left(K > \frac{N}{M} + 1\right)$

As in the previous case, first consider the MAC channel formed at Receiver 1, due to the users in $S \subseteq \{2, \ldots, K\}$. The sum rate constraint in this case becomes:

$$\sum_{j \in S} R_{c,j} \leq \min\left\{\min\left\{N, |S|M\right\}, N-M\right\}\alpha \log \rho + \mathcal{O}(1). \tag{A.55}$$

When $\min\left\{N, |S|M\right\} = N$, then $N \leq |S|M$. Under this condition and for $|S| = K-1$, (A.55) reduces to:

$$R_{c,j} \leq \frac{N-M}{K-1}\alpha \log \rho + \mathcal{O}(1). \tag{A.56}$$

When $\min\left\{N, |S|M\right\} = |S|M$, then $|S| \leq \frac{N}{M}$, and (A.55) becomes:

$$\sum_{j \in S} R_{c,j} \leq \min\left\{|S|M, N-M\right\}\alpha \log \rho + \mathcal{O}(1). \tag{A.57}$$

When $\min\left\{|S|M, N-M\right\} = N-M$, then $N \leq (1+|S|)M$. Under this condition and for $|S| = K-1$, (A.55) becomes

$$R_{c,j} \leq \frac{N-M}{K-1}\alpha \log \rho + \mathcal{O}(1). \tag{A.58}$$

When $\min\{|S|M, N-M\} = |S|M$, then $(1+|S|)M \leq N$, and (A.55) becomes

$$R_{c,j} \leq M\alpha \log \rho + \mathcal{O}(1). \tag{A.59}$$

Now consider the user set $S^{'} = S \cup \{1\}$, where user 1 is always included. By following the same procedure as in the previous case, the following equation similar to (A.50) is obtained

$$\sum_{j \in S'} R_{c,j} \leq M\alpha \log \rho + \min\left\{\min\left\{N, |S|M\right\}, N-M\right\} \alpha \log \rho + \mathcal{O}(1). \tag{A.60}$$

When $\min\{N, |S|M\} = |S|M$, then following equation is obtained:

$$\sum_{j \in S'} R_{c,j} \leq M\alpha \log \rho + \min\left\{|S|M, N-M\right\} \alpha \log \rho + \mathcal{O}(1). \tag{A.61}$$

By using the same procedure as in the previous case, above equation is further simplified and the following rate constraints are obtained under the following conditions.

When $\frac{N}{M} - 1 \leq |S| \leq \frac{N}{M}$, then (A.61) becomes

$$R_{c,j} \leq \frac{N\alpha}{1+|S|} \log \rho + \mathcal{O}(1). \tag{A.62}$$

The above equation is minimized when $|S| = \frac{N}{M}$ (assume $\frac{N}{M}$ is an integer) and (A.62) becomes:

$$R_{c,j} \leq \frac{N\alpha}{1+\frac{N}{M}} \log \rho + \mathcal{O}(1). \tag{A.63}$$

When $|S| < 1 + |S| \leq \frac{N}{M}$, (A.61) reduces to:

$$R_{c,j} \leq M\alpha \log \rho + \mathcal{O}(1). \tag{A.64}$$

When $N - M \leq |S|M$, using $|S| = K - 1$, (A.61) becomes

$$R_{c,j} \leq \frac{N\alpha}{K} \log \rho + \mathcal{O}(1). \tag{A.65}$$

When $\min\{N, |S|M\} = N$, then $N \leq |S|M$. Under this condition, for $|S| = K-1$, (A.60) becomes

$$R_{c,j} \leq \frac{N\alpha}{K} \log \rho + \mathcal{O}(1). \tag{A.66}$$

Finally, the achievable rate by common part of the message is obtained by taking minimum of (A.56), (A.58), (A.59), (A.63), (A.64), (A.65) and (A.66). Given (A.65), (A.63) becomes redundant as $K > \frac{N}{M} + 1$. It is not difficult to see that the above results remain same, even if $\frac{N}{M}$ is not an integer. Given (A.56) and (A.58), (A.59), (A.65) and (A.66) become redundant. Finally, the GDOF achievable by the common part of the message is:

$$d_c(\alpha) \geq \frac{N - M}{K - 1}\alpha. \tag{A.67}$$

The per user GDOF achievable in this case is obtained by adding (A.46) and (A.67), resulting in the expression given by (2.10).

A.5 Proof of Theorem 6

Following two cases are considered.

When $\left(\frac{N}{M} < K \leq \frac{N}{M} + 1\right)$: In this case, the HK-scheme achieves the GDOF given by (2.6). The HK-scheme achieves the interference free GDOF provided

$$\alpha \geq \frac{M(2K-1) - N}{M(K-1)}. \tag{A.68}$$

Hence, (2.6) can also be expressed as (2.11) in the statement of the theorem. Comparing (2.11) with (2.4), it is easy to see that the HK-scheme outperforms ZF-receiving for all $\alpha \geq 1$. The HK-scheme also outperforms treating interference as noise.

When $\left(K > \frac{N}{M} + 1\right)$: In this case, from Theorem 3, the HK-scheme achieves a per user GDOF given by (2.6). Comparing the HK-scheme with IA, it is easy to show that the former outperforms the latter for $\alpha > \frac{KM}{N+M}$. Hence, we obtain (2.12) in the statement of the theorem. Also, the HK-scheme always outperforms ZF-receiving and treating interference as noise. This completes the proof.

A.6 Proof of Theorem 7

The following two cases are considered in this regime.

When $\left(\frac{N}{M} < K \leq \frac{N}{M} + 1\right)$: In this case, from Theorem 4, the per user GDOF achievable by the HK-scheme is

$$d_{\text{HK}}(\alpha) = \begin{cases} M(1-\alpha) + \frac{1}{K-1}\left[M\left\{\alpha(2K-1) - K\right\} + N(1-\alpha)\right] & \text{for } \frac{1}{2} \leq \alpha \leq \frac{K}{2K-1} \\ M(1-\alpha) + \frac{N\alpha}{K} & \text{for } \frac{K}{2K-1} \leq \alpha \leq 1. \end{cases} \tag{A.69}$$

It can be shown that the HK-scheme performs better than treating interference as noise and ZF-receiving, with their performance coinciding at $\alpha = 1$. In this case, IA is not applicable.

When $\left(K > \frac{N}{M} + 1\right)$: In this case, the HK-scheme as well as IA perform better than ZF-receiving and treating interference as noise and at $\alpha = 1$, the HK-scheme coincides with ZF-receiving. In this regime, the achievable per user GDOF in Theorem 4 simplifies to

$$d_{\text{HK}}(\alpha) = \begin{cases} M(1-\alpha) + \frac{N\alpha - M(1-\alpha)}{K-1} & \text{for } \frac{1}{2} \leq \alpha \leq \frac{KM}{N+KM} \\ M(1-\alpha) + \frac{N\alpha}{K} & \text{for } \frac{KM}{N+KM} < \alpha \leq 1. \end{cases} \tag{A.70}$$

When $\frac{1}{2} \leq \alpha \leq \frac{KM}{N+KM}$, the HK-scheme outperforms IA for

$$\alpha\left[N - M(K-2)\right] \geq M\left[\frac{N - M(K-2)}{M+N}\right]. \tag{A.71}$$

When $N - M(K-2) \geq 0$, the following condition on α is obtained:

$$\alpha \geq \frac{M}{M+N}, \tag{A.72}$$

which is satisfied for all α in the moderate interference regime and hence the HK-scheme always performs better than IA.

When $N - M(K-2) < 0$, then following condition is obtained:

$$\alpha < \frac{M}{M+N} \leq \frac{1}{2}. \tag{A.73}$$

In this case, it is not possible to find an α which satisfies the above condition, and hence, IA always outperforms the HK-scheme.

When $\frac{KM}{N+KM} < \alpha \leq 1$, from (A.70), the HK-scheme outperforms IA when

$$\alpha \leq \frac{KM^2}{(M+N)(KM-N)}. \tag{A.74}$$

From (A.72), (A.73) and (A.74), the following conditions are obtained.

1. When $N - M(K-2) \geq 0$ i.e., $K < 2 + \frac{N}{M}$, then we have following conditions:

   (a) When $\frac{1}{2} \leq \alpha \leq \frac{KM}{N+KM}$, the HK-scheme performs better than IA and it achieves a per user GDOF of

   $$d(\alpha) \geq M(1-\alpha) + \frac{N\alpha - M(1-\alpha)}{K-1}. \tag{A.75}$$

   (b) When $\frac{KM}{N+KM} < \alpha \leq \frac{KM^2}{(M+N)(KM-N)}$, the HK-scheme outperforms IA and achieves a per user GDOF of

   $$d(\alpha) \geq M(1-\alpha) + \frac{N\alpha}{K}. \tag{A.76}$$

   (c) When $\frac{KM^2}{(M+N)(KM-N)} < \alpha \leq 1$, IA performs the best and the following per user GDOF is achievable:

   $$d(\alpha) \geq \frac{MN}{M+N}. \tag{A.77}$$

2. When $N - M(K-2) < 0$, i.e., $K > 2 + \frac{N}{M}$, IA performs better than the HK-scheme for $\frac{1}{2} \leq \alpha \leq 1$, and the following per user GDOF is achievable:

   $$d(\alpha) \geq \frac{NM}{N+M}. \tag{A.78}$$

This completes the proof.

A.7 Proof of Theorem 8

When $K > \frac{N}{M}+1$, from (2.10) and (2.5), it can be observed that the HK-scheme performs better than treating interference as noise. The per user GDOF achievable by the HK-scheme is

$$d_{\text{HK}}(\alpha) = M + \frac{1}{K-1}(N - KM)\alpha. \tag{A.79}$$

When $\frac{N}{M} < K \leq \frac{N}{M} + 1$, from (2.10) and (2.5), it can be observed that the HK-scheme again performs better than treating interference as noise in this case, since $\frac{1}{K-1}(N - KM)\alpha > (N - KM)\alpha$. Now, the HK-scheme outperforms IA whenever

$$\alpha > \frac{M^2}{M(N+M) - \frac{N^2-M^2}{K-1}}. \tag{A.80}$$

Since $\alpha < \frac{1}{2}$, the right hand side is less than $\frac{1}{2}$, which requires

$$K > 2 + \frac{N}{M}. \tag{A.81}$$

Thus, when $K > 2 + \frac{N}{M}$ and (A.80) is satisfied, the HK-scheme performs better than IA. Comparing the HK-scheme with ZF-receiving, it is easy to show that the HK-scheme outperforms ZF-receiving for $\alpha \leq \frac{1}{2}$. The two schemes coincide at $\alpha = \frac{1}{2}$, when $K = 2$.

To summarize, when $K > 2 + \frac{N}{M}$, the per user GDOF that can be achieved in the weak interference regime is:

$$d(\alpha) \geq \begin{cases} M(1-\alpha) + \frac{1}{K-1}(N-M)\alpha & \text{for } 0 \leq \alpha \leq \frac{M^2}{M(N+M) - \frac{N^2-M^2}{K-1}} \\ \frac{NM}{N+M} & \text{for } \frac{M^2}{M(N+M) - \frac{N^2-M^2}{K-1}} < \alpha \leq \frac{1}{2}. \end{cases} \tag{A.82}$$

When $K \leq 2 + \frac{N}{M}$, the HK-scheme outperforms the other schemes and the per user

GDOF achievable by this scheme is as given in (2.10). This completes the proof.

A.8 Proof of Theorem 9

First, recall that the maximum of the achievable GDOF from the HK-scheme and IA outperforms the achievable GDOF from treating interference as noise or ZF-receiving for all values of M, N, K and α. Hence, the above result follows from carefully comparing the achievable GDOF from the HK-scheme and IA in the weak, moderate, and strong interference cases.

Weak interference case $(0 \leq \alpha \leq \frac{1}{2})$**:** Comparing the achievable GDOF using IA, given by (2.3), with that achievable using the HK-scheme, given by (2.10), it follows that the HK-scheme is active when

$$\alpha \leq \frac{(K-1)}{(R+1)\left(K-\frac{N}{M}\right)}. \tag{A.83}$$

When $R = 1$, since $\frac{N}{M} \geq 1$, it is clear that the right hand side above exceeds $\frac{1}{2}$. Hence, the HK-scheme is active throughout the weak interference case. When $R > 1$, the right hand side above is $\leq \frac{1}{2}$, provided

$$K \geq \frac{N}{M} + 2\frac{\frac{N}{M}-1}{R-1}. \tag{A.84}$$

Notice that, in the last term above, the denominator is the floor of the numerator. Hence, the ratio is bounded above by 2. Hence, for $K \geq \frac{N}{M} + 4$, the HK-scheme is active for the initial part of the weak interference case. IA is active in the later part of the weak interference case. This completes the proof in the weak interference case.

Moderate interference case $(\frac{1}{2} \leq \alpha \leq 1)$**:** Consider the achievable GDOF using the

HK-scheme given by (2.9) for $K > \frac{N}{M} + 1$. The expression can be equivalently written as

$$d(\alpha) \geq \begin{cases} M(1-\alpha) + \frac{N\alpha + M(1-\alpha)}{K-1} & \text{for } \frac{1}{2} \leq \alpha < \frac{1}{1+\frac{N}{MK}} \\ M(1-\alpha) + \frac{N\alpha}{K} & \text{for } \frac{1}{1+\frac{N}{MK}} \leq \alpha < 1. \end{cases} \tag{A.85}$$

Consider the first case above, i.e., when $\frac{1}{2} \leq \alpha < \frac{1}{1+\frac{N}{MK}}$. It can be shown that the above achievable GDOF exceeds that achievable by IA, provided

$$\alpha \leq \frac{(K-1) - (R+1)}{(R+1)\left((K-1) - \left(\frac{N}{M} + 1\right)\right)}. \tag{A.86}$$

Now, the right hand side above is smaller than $\frac{1}{1+\frac{N}{MK}}$ when $K \geq \frac{N}{M} + 2\frac{N}{RM}$, which is always satisfied when $K \geq \frac{N}{M} + 4$. When $R = 1$, it is immediate to see that the right hand side above exceeds $\frac{1}{2}$, and hence, the HK-scheme is active for an initial portion of $\frac{1}{2} \leq \alpha < \frac{1}{1+\frac{N}{MK}}$. When $R > 1$, the right hand side above is smaller than $\frac{1}{2}$ and hence IA is active throughout this range of α, provided

$$K \geq \frac{N}{M} + 2\frac{\frac{N}{M} - 1}{R-1}, \tag{A.87}$$

which is satisfied when $K \geq \frac{N}{M} + 4$.

Next, consider the second case above, i.e., when $\frac{1}{1+\frac{N}{MK}} \leq \alpha < 1$. In this case, the HK-scheme outperforms IA when

$$\alpha \leq \frac{1}{(R+1)\left(1 - \frac{N}{MK}\right)}. \tag{A.88}$$

When the right hand side above is $\leq \frac{1}{1+\frac{N}{MK}}$, IA is active throughout this range of α. This leads to

$$K \geq \frac{N}{M} + 2\frac{N}{RM}, \tag{A.89}$$

which is satisfied when $K \geq \frac{N}{M} + 4$. This completes the proof in the moderate interference case.

Strong interference case $(\alpha \geq 1)$**:** In this case, from (2.6), the achievable GDOF from the HK-scheme when $K \geq \frac{N}{M} + 4$ is given by

$$d(\alpha) \geq \begin{cases} \frac{N\alpha}{K} & \text{for } 1 \leq \alpha < \frac{MK}{N} \\ M & \text{for } \alpha \geq \frac{MK}{N}. \end{cases} \tag{A.90}$$

Comparing the above achievable GDOF using IA given by (2.3), one obtains

$$d(\alpha) \geq \begin{cases} \frac{RM}{R+1} & \text{for } 1 \leq \alpha \leq \frac{MKR}{N(R+1)} \\ \frac{N\alpha}{K} & \text{for } \frac{MKR}{N(R+1)} < \alpha \leq \frac{MK}{N} \\ M & \text{for } \alpha > \frac{MK}{N}. \end{cases} \tag{A.91}$$

The statements of the theorem are now easily obtained by consolidating the above results.

Appendix B

Appendix for Chapter 3

B.1 Proof of Theorem 10

Given the stated assumptions on user cooperation and the genie-provided side information, the system model becomes:

$$\overline{\mathbf{y}}_1 = \overline{\mathbf{H}}_{11}\overline{\mathbf{x}}_1 + \overline{\mathbf{H}}_{12}\overline{\mathbf{x}}_2 + \overline{\mathbf{z}}_1, \text{ and } \overline{\mathbf{y}}_2 = \overline{\mathbf{H}}_{22}\overline{\mathbf{x}}_2 + \overline{\mathbf{z}}_2, \tag{B.1}$$

where

$$\overline{\mathbf{y}}_1 \triangleq \left[\mathbf{y}_1^T, \cdots, \mathbf{y}_{L_1}^T\right]^T, \ \overline{\mathbf{y}}_2 \triangleq \left[\mathbf{y}_{L_1+1}^T, \cdots, \mathbf{y}_{L}^T\right]^T, \overline{\mathbf{x}}_1 \triangleq \left[\mathbf{x}_1^T, \cdots, \mathbf{x}_{L_1}^T\right]^T,$$

$$\overline{\mathbf{x}}_2 \triangleq \left[\mathbf{x}_{L_1+1}^T, \cdots, \mathbf{x}_{L}^T\right]^T, \overline{\mathbf{z}}_1 \triangleq \left[\mathbf{z}_1^T, \cdots, \mathbf{z}_{L_1}^T\right]^T, \text{ and } \overline{\mathbf{z}}_2 \triangleq \left[\mathbf{z}_{L_1+1}^T, \cdots, \mathbf{z}_{L}^T\right]^T.$$

Here, $\overline{\mathbf{H}}_{ij}$ are stacked channel matrices, as defined in the statement of the theorem. The above system model is equivalent to a 2-user MIMO Z-GIC with the two transmitters having L_1M and L_2M antennas and the two receivers having L_1N and L_2N antennas. The outer bound derived for this modified system is clearly an outer bound for the K-user MIMO GIC. By using Fano's inequality, the sum rate of the modified system is

upper bounded as:

$$n\sum_{i=1}^{L} R_i - n\epsilon_n \overset{(a)}{\leq} I\left(\overline{\mathbf{x}}_1^n; \overline{\mathbf{y}}_1^n\right) + I\left(\overline{\mathbf{x}}_2^n; \overline{\mathbf{y}}_2^n, \overline{\mathbf{s}}^n\right),$$
$$\text{or } \sum_{i=1}^{L} R_i \overset{(b)}{\leq} h\left(\overline{\mathbf{y}}_1^*\right) - h\left(\overline{\mathbf{z}}_1\right) + h\left(\overline{\mathbf{y}}_2^* | \overline{\mathbf{s}}^*\right) - h\left(\overline{\mathbf{z}}_2\right), \tag{B.2}$$

where *(a)* is due to the genie giving side information to receiver 2 and where, $\overline{\mathbf{s}}^n \triangleq \overline{\mathbf{H}}_{12}\overline{\mathbf{x}}_2^n + \overline{\mathbf{z}}_1^n$; and *(b)* follows from the Lemma 2 in [80]. In the above equation, the superscript $*$ indicates that the inputs are i.i.d. Gaussian i.e., $\overline{\mathbf{x}}_i^* \sim CN(\mathbf{0}, \overline{\mathbf{P}}_i)$ and the quantities $\overline{\mathbf{s}}^*, \overline{\mathbf{y}}_1^*$ and $\overline{\mathbf{y}}_2^*$ are the signals obtained due to Gaussian inputs, and $h(\overline{\mathbf{z}}_j) = L_j N \log(\pi e)$, $j = 1, 2$. Each term in (B.2) is simplified as follows:

$$h\left(\overline{\mathbf{y}}_1^*\right) = \log\left|\pi e\left[\mathbf{I}_{L_1 N} + \overline{\mathbf{H}}_{11}\overline{\mathbf{P}}_1\overline{\mathbf{H}}_{11}^H + \overline{\mathbf{H}}_{12}\overline{\mathbf{P}}_2\overline{\mathbf{H}}_{12}^H\right]\right|, \tag{B.3}$$

$$h\left(\overline{\mathbf{y}}_2^* | \overline{\mathbf{s}}^*\right) = \log\left|\pi e \Sigma_{\overline{\mathbf{y}}_2^* | \overline{\mathbf{s}}^*}\right|, \tag{B.4}$$

where

$$\Sigma_{\overline{\mathbf{y}}_2^* | \overline{\mathbf{s}}^*} \triangleq \mathbf{E}\left[\overline{\mathbf{y}}_2^* \overline{\mathbf{y}}_2^{*H}\right] - \mathbf{E}\left[\overline{\mathbf{y}}_2^* \overline{\mathbf{s}}^{*H}\right]\mathbf{E}\left[\overline{\mathbf{s}}^* \overline{\mathbf{s}}^{*H}\right]^{-1}\mathbf{E}\left[\overline{\mathbf{s}}^* \overline{\mathbf{y}}_2^{*H}\right],$$
$$= \mathbf{I}_{L_2 N} + \overline{\mathbf{H}}_{22}\overline{\mathbf{P}}_2^{1/2}\left\{\mathbf{I}_{L_2 M} + \overline{\mathbf{P}}_2^{1/2}\overline{\mathbf{H}}_{12}^H\overline{\mathbf{H}}_{12}\overline{\mathbf{P}}_2^{1/2}\right\}^{-1}\overline{\mathbf{P}}_2^{1/2}\overline{\mathbf{H}}_{22}^H. \tag{B.5}$$

In the above, (B.5) is obtained using the Woodbury matrix identity [81]. The conditional differential entropy in (B.4) thus reduces to:

$$h\left(\overline{\mathbf{y}}_2^* | \overline{\mathbf{s}}^*\right) = \log\left|\pi e\left[\mathbf{I}_{L_2 N} + \overline{\mathbf{H}}_{22}\overline{\mathbf{P}}_2^{1/2}\left\{\mathbf{I}_{L_2 M} + \overline{\mathbf{P}}_2^{1/2}\overline{\mathbf{H}}_{12}^H\overline{\mathbf{H}}_{12}\overline{\mathbf{P}}_2^{1/2}\right\}^{-1}\overline{\mathbf{P}}_2^{1/2}\overline{\mathbf{H}}_{22}^H\right]\right|. \tag{B.6}$$

From (B.3) and (B.6), the sum rate bound in (B.2) reduces to (3.2), which concludes the proof.

B.2 Proof of Lemma 1

In the symmetric case, with a slight abuse of notation, the system model in (B.1) reduces to

$$\overline{\mathbf{y}}_1 = \sqrt{\rho}\overline{\mathbf{H}}_{11}\overline{\mathbf{x}}_1 + \sqrt{\rho^{\alpha}}\overline{\mathbf{H}}_{12}\overline{\mathbf{x}}_2 + \overline{\mathbf{z}}_1, \text{ and } \overline{\mathbf{y}}_2 = \sqrt{\rho}\overline{\mathbf{H}}_{22}\overline{\mathbf{x}}_2 + \overline{\mathbf{z}}_2. \tag{B.7}$$

Under the symmetric assumption, the sum rate in (3.2) in Theorem 10 is bounded as follows:

$$\sum_{i=1}^{L} R_i \leq \log\left|\mathbf{I}_{L_1N} + \rho\overline{\mathbf{H}}_{11}\overline{\mathbf{H}}_{11}^H + \rho^{\alpha}\overline{\mathbf{H}}_{12}\overline{\mathbf{H}}_{12}^H\right| + \log\left|\mathbf{I}_{L_2N} + \rho\overline{\mathbf{H}}_{22}\left\{\mathbf{I}_{L_2M} + \rho^{\alpha}\overline{\mathbf{H}}_{12}^H\overline{\mathbf{H}}_{12}\right\}^{-1}\overline{\mathbf{H}}_{22}^H\right|. \tag{B.8}$$

Equation (B.8) is obtained using Lemma 6 in [82] and the fact that $\log|\cdot|$ is monotonically increasing on the cone of positive definite matrices. Consider the following term in (B.8):

$$\begin{aligned}
&\mathbf{I}_{L_2N} + \rho\overline{\mathbf{H}}_{22}\left\{\mathbf{I}_{L_2M} + \rho^{\alpha}\overline{\mathbf{H}}_{12}^H\overline{\mathbf{H}}_{12}\right\}^{-1}\overline{\mathbf{H}}_{22}^H \\
&\overset{(a)}{=} \mathbf{I}_{L_2N} + \rho\overline{\mathbf{H}}_{22}\left\{\mathbf{I}_{L_2M} + \rho^{\alpha}\overline{\mathbf{U}}_{12}\overline{\Sigma}_{12}\overline{\mathbf{U}}_{12}^H\right\}^{-1}\overline{\mathbf{H}}_{22}^H, \\
&= \mathbf{I}_{L_2N} + \rho\widetilde{\mathbf{H}}_{22}\left\{\mathbf{I}_{L_2M} + \rho^{\alpha}\overline{\Sigma}_{12}\right\}^{-1}\widetilde{\mathbf{H}}_{22}^H, \qquad \text{where } \widetilde{\mathbf{H}}_{22} \triangleq \overline{\mathbf{H}}_{22}\overline{\mathbf{U}}_{12}, \\
&\overset{(b)}{=} \mathbf{I}_{L_2N} + \rho\begin{bmatrix}\widetilde{\mathbf{H}}_{22}^{(a)} & \widetilde{\mathbf{H}}_{22}^{(b)}\end{bmatrix}\begin{bmatrix}\left(\mathbf{I}_r + \rho^{\alpha}\Sigma_r\right)^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{L_2M-r}\end{bmatrix}\begin{bmatrix}\widetilde{\mathbf{H}}_{22}^{(a)} & \widetilde{\mathbf{H}}_{22}^{(b)}\end{bmatrix}^H, \\
&= \mathbf{I}_{L_2N} + \rho\widetilde{\mathbf{H}}_{22}^{(a)}\left(\mathbf{I}_r + \rho^{\alpha}\Sigma_r\right)^{-1}\widetilde{\mathbf{H}}_{22}^{(a)H} + \rho\widetilde{\mathbf{H}}_{22}^{(b)}\mathbf{I}_{L_2M-r}\widetilde{\mathbf{H}}_{22}^{(b)H},
\end{aligned} \tag{B.9}$$

where *(a)* is obtained by taking eigen value decomposition (EVD) of $\overline{\mathbf{H}}_{12}^H\overline{\mathbf{H}}_{12}$, $\overline{\mathbf{U}}_{12} \in \mathbb{C}^{L_2M \times L_2M}$; in *(b)* Σ_r contains the nonzero singular values of $\overline{\mathbf{H}}_{12}^H\overline{\mathbf{H}}_{12}$ and $\mathbf{0}_{L_2M-r}$ is a zero matrix of dimension $(L_2M - r) \times (L_2M - r)$, where $r \triangleq \min\{L_2M, L_1N\}$ and $\widetilde{\mathbf{H}}_{22}$

is partitioned into two sub-matrices $\widetilde{\mathbf{H}}_{22}^{(a)}$ and $\widetilde{\mathbf{H}}_{22}^{(b)}$ of dimensions $L_2N \times r$ and $L_2N \times (L_2M - r)$, respectively. Substituting (B.9) in (B.8), one obtains the following outer bound on the sum rate:

$$\sum_{i=1}^{L} R_i \leq \log \left| \mathbf{I}_{L_1N} + \rho \overline{\mathbf{H}}_{11} \overline{\mathbf{H}}_{11}^H + \rho^{\alpha} \overline{\mathbf{H}}_{12} \overline{\mathbf{H}}_{12}^H \right| + \log \left| \mathbf{I}_{L_2N} + \rho^{1-\alpha} \widetilde{\mathbf{H}}_{22}^{(a)} \Sigma_r^{-1} \widetilde{\mathbf{H}}_{22}^{(a)H} + \rho \widetilde{\mathbf{H}}_{22}^{(b)} \mathbf{I}_{L_2M-r} \widetilde{\mathbf{H}}_{22}^{(b)H} \right| + \mathcal{O}(1). \tag{B.10}$$

The above bound holds at high SNR, and is further simplified depending on the values of M, N and α.

Case 1 ($M \leq N$ **and** $0 \leq \alpha \leq 1$**):** Using Lemma 4 in [42], the outer bound in (B.10) becomes

$$\sum_{i=1}^{L} R_i \leq \left[r_{11} + \min\{r_{12}, L_1N - r_{11}\}\alpha + r_{22}^{(b)} + \min\{r_{22}^{(a)}, L_2N - r_{22}^{(b)}\}(1-\alpha) \right] \log \rho + \mathcal{O}(1), \tag{B.11}$$

where $r_{ij} \triangleq \text{rank}(\overline{\mathbf{H}}_{ij})$, $r_{22}^{(a)} \triangleq \text{rank}(\widetilde{\mathbf{H}}_{22}^{(a)})$ and $r_{22}^{(b)} \triangleq \text{rank}(\widetilde{\mathbf{H}}_{22}^{(b)})$. As the channel coefficients are drawn from a continuous distribution such as the Gaussian distribution, the channel matrices are full rank with probability one. Hence, the outer bound in (B.11) reduces to the following form:

$$\sum_{i=1}^{L} R_i \leq \left[L_1M + \min\left\{r, L_1N - L_1M\right\}\alpha + L_r + \min\left\{r, L_2N - L_r\right\}(1-\alpha) \right] \log \rho + \mathcal{O}(1),$$

where $r \triangleq \min\{L_2M, L_1N\}$ and $L_r \triangleq L_2M - r$. Hence, the sum GDOF of the L users is upper bounded as

$$d_{i_1} + \ldots + d_{i_L} \leq L_1M + \min\{r, L_1(N-M)\}\,\alpha + L_r + \min\{r, L_2N - L_r\}\,(1-\alpha). \tag{B.12}$$

Note that L users can be chosen among K-users in $\binom{K}{L}$ different ways, and any given user appears in $\binom{K-1}{L-1}$ of these ways. By adding all inequalities like (B.12) and dividing by K, the following upper bound on the per user GDOF is obtained:

$$d(\alpha) \leq \frac{1}{L}\left[L_1M + \min\{r, L_1(N-M)\}\,\alpha + L_r + \min\{r, L_2N - L_r\}\,(1-\alpha)\right]. \tag{B.13}$$

Taking the minimum of (B.13) over all possible values of L_1 and L_2 results in Case 1 of Lemma 1.

Case 2 ($M \leq N$ **and** $\alpha > 1$): Hence, the outer bound in (B.10) is simplified to following form using Lemma 4 in [42]:

$$\sum_{i=1}^{L} R_i \leq r\alpha\log\rho + \min\{L_1M, L_1N - r\}\log\rho + (L_2M - r)\log\rho + \mathcal{O}(1). \tag{B.14}$$

By following the same steps as in the previous case, the per user GDOF is upper bounded as given below:

$$d(\alpha) \leq \frac{1}{L}\left[r\alpha + \min\{L_1M, L_1N - r\} + (L_2M - r)\right]. \tag{B.15}$$

By taking minimum of (B.15) over all possible values of L_1 and L_2 results in Case 2 of Lemma 1.

Case 3 ($M > N$ **and** $0 \leq \alpha \leq 1$): When $M > N$ and $0 \leq \alpha \leq 1$, the sum rate in (B.10)

reduces to following form by using Lemma 4 in [42]:

$$\sum_{i=1}^{L} R_i \leq L_1 N \log\rho + \min\left\{L_2 N, L_2 M - r\right\}\log\rho + \min\left\{\min\left\{L_2 N, r\right\}, L_2 N - \min\left\{L_2 N, L_2 M - r\right\}\right\}(1-\alpha)\log\rho + \mathcal{O}(1). \quad \text{(B.16)}$$

Following the same steps as in Case 1, the per user GDOF is upper bounded as given below by using (B.16):

$$d(\alpha) \leq \frac{1}{L}\left[L_1 N + \min\left\{L_2 N, L_2 M - r\right\} + \min\left\{\min\left\{L_2 N, r\right\}, L_2 N - \min\left\{L_2 N, L_2 M - r\right\}\right\}(1-\alpha)\right]. \quad \text{(B.17)}$$

By taking minimum of (B.17) over all possible values of L_1 and L_2 results in Case 3 of Lemma 1.

Case 4 ($M > N$ **and** $\alpha \geq 1$):

Under this condition the outer bound in (B.10) is simplified to following form by using Lemma 4 in [42]:

$$\begin{aligned}\sum_{i=1}^{L} R_i &\leq r\alpha\log\rho + \min\left\{L_1 N, L_1 N - r\right\}\log\rho + \min\left\{L_2 N, L_2 M - r\right\}\log\rho + \mathcal{O}(1),\\ &= r\alpha\log\rho + (L_1 N - r)\log\rho + \min\left\{L_2 N, L_2 M - r\right\}\log\rho + \mathcal{O}(1). \quad \text{(B.18)}\end{aligned}$$

Following the same steps as in case 1, the per user GDOF is upper bounded as:

$$d(\alpha) \leq \frac{1}{L}\left[L_1 N + r(\alpha - 1) + \min\left\{L_2 N, L_2 M - r\right\}\right]. \quad \text{(B.19)}$$

Taking minimum of (B.19) over all possible values of L_1 and L_2 results in Case 4 of Lemma 1. This completes the proof of Lemma 1.

B.3 Proof of Theorem 11

Define the quantity $\mathbf{s}_{j,\mathcal{B}} \triangleq \sum_{i\in\mathcal{B}} \mathbf{H}_{ji}\mathbf{x}_i + \mathbf{z}_j$, where $\mathcal{B} \subseteq \{1, 2, \ldots, K\}$ is a subset of the K-users. The rate of the first user is upper bounded as follows:

$$\begin{aligned}
nR_1 &\overset{(a)}{\leq} I(\mathbf{x}_1^n; \mathbf{y}_1^n, \mathbf{s}_{2,1}^n) + n\epsilon_n, \\
&\overset{(b)}{=} h(\mathbf{s}_{2,1}^n) - h(\mathbf{z}_2^n) + h(\mathbf{y}_1^n|\mathbf{s}_{2,1}^n) - h(\mathbf{y}_1^n|\mathbf{s}_{2,1}^n, \mathbf{x}_1^n) + n\epsilon_n, \\
&= h(\mathbf{s}_{2,1}^n) - h(\mathbf{z}_2^n) + h(\mathbf{y}_1^n|\mathbf{s}_{2,1}^n) - h(\mathbf{y}_1^n|\mathbf{x}_1^n) + n\epsilon_n, \\
&\overset{(c)}{\leq} h(\mathbf{s}_{2,1}^n) - h(\mathbf{z}_2^n) + h(\mathbf{y}_1^n|\mathbf{s}_{2,1}^n) - h(\mathbf{y}_1^n|\{\mathbf{x}_i^n\}_{i=1,i\neq 2}^K) + n\epsilon_n, \\
&= h(\mathbf{s}_{2,1}^n) - h(\mathbf{z}_2^n) + h(\mathbf{y}_1^n|\mathbf{s}_{2,1}^n) - h(\mathbf{s}_{1,2}^n) + n\epsilon_n, \qquad \text{(B.20)}
\end{aligned}$$

where *(a)* is due to the genie giving side information to receiver 1; *(b)* follows from the chain rule of mutual information, and *(c)* follows by using the fact that the differential entropy cannot increase by additional conditioning to provide $\mathbf{x}_i^n, i = 1, \ldots, K, i \neq 2$, to receiver 1. Given $\{\mathbf{x}_i^n\}_{i=1,i\neq 2}^K$, the remaining uncertainty in $\mathbf{y}_1^n$ is due to that in $\mathbf{x}_1^n$ and $\mathbf{z}_1^n$, and it is simply given by $h(\mathbf{s}_{1,2}^n)$.

The rate of the K^{th} user is upper bounded by giving side information of the form $\mathbf{s}_{K-1,K}$ to its receiver and using similar arguments as in the case of the first user, to get

$$nR_K \leq h(\mathbf{s}_{K-1,K}^n) - h(\mathbf{z}_{K-1}^n) + h(\mathbf{y}_K^n|\mathbf{s}_{K-1,K}^n) - h(\mathbf{s}_{K,K-1}^n) + n\epsilon_n. \qquad \text{(B.21)}$$

The rates of users $i = 2, 3, \ldots, K-1$ are upper bounded as

$$\begin{aligned}
nR_i &\leq I(\mathbf{x}_i^n; \mathbf{y}_i^n, \mathbf{s}_{i-1,i}^n) + n\epsilon_n, \\
&= h(\mathbf{s}_{i-1,i}^n) - h(\mathbf{z}_{i-1}^n) + h(\mathbf{y}_i^n|\mathbf{s}_{i-1,i}^n) - h(\mathbf{y}_i^n|\mathbf{s}_{i-1,i}^n, \mathbf{x}_i^n) + n\epsilon_n,
\end{aligned}$$

$$\leq h(\mathbf{s}_{i-1,i}^n) - h(\mathbf{z}_{i-1}^n) + h(\mathbf{y}_i^n|\mathbf{s}_{i-1,i}^n) - h(\mathbf{s}_{i,i+1}^n) + n\epsilon_n. \tag{B.22}$$

Another way to upper bound the rates of users $i = 2, 3, \ldots, K-1$ is by providing $\mathbf{s}_{i+1,i}$ as side information. This results in

$$nR_i \leq h(\mathbf{s}_{i+1,i}^n) - h(\mathbf{z}_{i+1}^n) + h(\mathbf{y}_i^n|\mathbf{s}_{i+1,i}^n) - h(\mathbf{s}_{i,i-1}^n) + n\epsilon_n. \tag{B.23}$$

Summing the inequalities in (B.20), (B.21), (B.22) and (B.23), and using Lemma 2 in [80] , the sum rate is bounded as follows:

$$R_{\text{s}} \leq \sum_{i=1}^{K-1} h(\mathbf{y}_i^*|\mathbf{s}_{i+1,i}^*) + \sum_{i=2}^{K} h(\mathbf{y}_i^*|\mathbf{s}_{i-1,i}^*) - h(\mathbf{z}_1) - 2\sum_{i=2}^{K-1} h(\mathbf{z}_i) - h(\mathbf{z}_K), \tag{B.24}$$

where $R_{\text{s}} \triangleq R_1 + 2\sum_{i=2}^{K-1} R_i + R_K$. The conditional differential entropy terms in (B.24) are simplified as follows:

$$h(\mathbf{y}_i^*|\mathbf{s}_{i+1,i}^*) = \log\left|\pi e \Sigma_{\mathbf{y}_i^*|\mathbf{s}_{i+1,i}^*}\right|, \tag{B.25}$$

where

$$\Sigma_{\mathbf{y}_i^*|\mathbf{s}_{i+1,i}^*} \triangleq \mathbf{E}\left[\mathbf{y}_i^*\mathbf{y}_i^{*H}\right] - \mathbf{E}\left[\mathbf{y}_i^*\mathbf{s}_{i+1,i}^{*H}\right]\mathbf{E}\left[\mathbf{s}_{i+1,i}^*\mathbf{s}_{i+1,i}^{*H}\right]^{-1}\mathbf{E}\left[\mathbf{s}_{i+1,i}^*\mathbf{y}_i^{*H}\right]. \tag{B.26}$$

The individual terms in $\Sigma_{\mathbf{y}_i^*|\mathbf{s}_{i+1,i}^*}$ are obtained as

$$\begin{aligned}
\mathbf{E}\left[\mathbf{y}_i^*\mathbf{y}_i^{*H}\right] &= \mathbf{I}_{N_i} + \mathbf{H}_{ii}\mathbf{P}_i\mathbf{H}_{ii}^H + \sum_{j=1,\, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{P}_j\mathbf{H}_{ij}^H, \\
\mathbf{E}\left[\mathbf{y}_i^*\mathbf{s}_{i+1,i}^{*H}\right] &= \mathbf{H}_{ii}\mathbf{P}_i\mathbf{H}_{i+1,i}^H, \\
\text{and } \mathbf{E}\left[\mathbf{s}_{i+1,i}^*\mathbf{s}_{i+1,i}^{*H}\right] &= \mathbf{I}_{N_i} + \mathbf{H}_{i+1,i}\mathbf{P}_i\mathbf{H}_{i+1,i}^H.
\end{aligned} \tag{B.27}$$

Using the Woodbury matrix identity [81] to simplify $\Sigma_{\mathbf{y}_i^*|\mathbf{s}_{i+1,i}^*}$, and substituting in (B.25), one obtains

$$h(\mathbf{y}_i^*|\mathbf{s}_{i+1,i}^*) = \log\left|\pi e\left[\mathbf{I}_{N_i} + \sum_{j=1,\, j\neq i}^{K} \boldsymbol{\phi}_{i,j} + \boldsymbol{\psi}_{i,i+1}\right]\right|. \tag{B.28}$$

In a similar manner, it can be shown that

$$h(\mathbf{y}_i^*|\mathbf{s}_{i-1,i}^*) = \log\left|\pi e\left[\mathbf{I}_{N_i} + \sum_{j=1,\, j\neq i}^{K} \boldsymbol{\phi}_{i,j} + \boldsymbol{\psi}_{i,i-1}\right]\right|. \tag{B.29}$$

In the above equations, $\boldsymbol{\phi}_{i,j}$ and $\boldsymbol{\psi}_{i,j}$ are as defined in the statement of the Theorem. Finally, the sum rate is upper bounded using (B.28) and (B.29) in (B.24) to get (3.3), which completes the proof.

B.4 Proof of Lemma 2

The following two cases are considered to simplify the outer bound stated in Theorem 11.

Case 1 $(M \leq N)$: For the symmetric case, applying Lemma 6 in [82] and simplifying (3.3) for high SNR, the outer bound of Theorem 11 becomes

$$\begin{aligned} R_{\mathrm{s}} \leq & \sum_{i=1}^{K-1} \log\left|\mathbf{I}_N + \rho^{\alpha} \sum_{j=1,\, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^H + \rho^{(1-\alpha)}\mathbf{H}_{ii}\left(\mathbf{H}_{i+1,i}^H\mathbf{H}_{i+1,i}\right)^{-1}\mathbf{H}_{ii}^H\right| \\ & + \sum_{i=2}^{K} \log\left|\mathbf{I}_N + \rho^{\alpha} \sum_{j=1,\, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^H + \rho^{(1-\alpha)}\mathbf{H}_{ii}\left(\mathbf{H}_{i-1,i}^H\mathbf{H}_{i-1,i}\right)^{-1}\mathbf{H}_{ii}^H\right| + \mathcal{O}(1). \end{aligned} \tag{B.30}$$

Weak Interference Case $(0 \leq \alpha \leq \frac{1}{2})$: Using Lemma 4 in [42] and with $r^{'}$ as defined in the statement the Lemma, (B.30) leads to the following upper bound on the per user GDOF

$$d(\alpha) \leq M(1-\alpha) + \min\{r^{'}, N-M\}\alpha. \tag{B.31}$$

Moderate Interference Case $\left(\frac{1}{2} \leq \alpha \leq 1\right)$: Using Lemma 4 in [42] and with $r^{'}$ as defined in the statement the Lemma, (B.30) leads to the following upper bound on the per user GDOF

$$d(\alpha) \leq r^{'}\alpha + \min\left\{M, N - r^{'}\right\}(1-\alpha). \tag{B.32}$$

High Interference Case $(\alpha \geq 1)$: Using Lemma 4 in [42] and with $r^{'}$ as defined in the statement the Lemma, (B.30) leads to the following upper bound on the per user GDOF

$$d(\alpha) \leq \min\{N, (K-1)M\}\,\alpha. \tag{B.33}$$

As the per user GDOF in this case exceeds the interference free GDOF, this bound is not helpful for high interference regime.

Case 2 $(M > N)$: By employing a procedure similar to that used to obtain (B.10), one can simplify (B.30) to get

$$\begin{aligned} R_{\text{s}} \leq & \sum_{i=1}^{K-1} \log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=1, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^{H} + \rho^{(1-\alpha)} \tilde{\mathbf{H}}_{ii}^{(a)} \left(\Sigma_N^{i+1,i}\right)^{-1} \tilde{\mathbf{H}}_{ii}^{(a)H} + \rho \tilde{\mathbf{H}}_{ii}^{(b)} \mathbf{I}_{M-N} \tilde{\mathbf{H}}_{ii}^{(b)H} \right| \\ & + \sum_{i=2}^{K} \log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=1, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^{H} + \rho^{(1-\alpha)} \tilde{\mathbf{H}}_{ii}^{(a)} \left(\Sigma_N^{i-1,i}\right)^{-1} \tilde{\mathbf{H}}_{ii}^{(a)H} + \rho \tilde{\mathbf{H}}_{ii}^{(b)} \mathbf{I}_{M-N} \tilde{\mathbf{H}}_{ii}^{(b)H} \right| + \mathcal{O}(1), \end{aligned} \tag{B.34}$$

where $\tilde{\mathbf{H}}_{ii} \triangleq \mathbf{H}_{ii}\mathbf{U}_{ij}$ and $\Sigma_N^{j,i}$ contains N nonzero singular values of $\mathbf{H}_{ij}^{H}\mathbf{H}_{ij}$, and $\tilde{\mathbf{H}}_{ii}$ is partitioned into submatrices $\tilde{\mathbf{H}}_{ii}^{(a)}$ and $\tilde{\mathbf{H}}_{ii}^{(b)}$ of dimension $N \times N$ and $N \times (M-N)$, respectively.

Weak Interference Case $(0 \leq \alpha \leq \frac{1}{2})$: Consider a specific i in (B.34):

$$\log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=1, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^H + \rho^{(1-\alpha)} \tilde{\mathbf{H}}_{ii}^{(a)} \left(\Sigma_N^{i+1,i}\right)^{-1} \tilde{\mathbf{H}}_{ii}^{(a)H} + \rho \tilde{\mathbf{H}}_{ii}^{(b)} \mathbf{I}_{M-N} \tilde{\mathbf{H}}_{ii}^{(b)H} \right|$$
$$= [\min\{N, M-N\} + (N - \min\{N, M-N\})(1-\alpha)] \log \rho + \mathcal{O}(1), \tag{B.35}$$

The above equation is obtained by using Lemma 5 in [42]. Thus, from (B.34) and (B.35), the per user GDOF is upper bounded as

$$d(\alpha) \leq N(1-\alpha) + \min\{N, M-N\}\alpha. \tag{B.36}$$

Moderate Interference Case $\left(\frac{1}{2} \leq \alpha \leq 1\right)$: Consider a specific i in (B.34):

$$\log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=1, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^H + \rho^{1-\alpha} \tilde{\mathbf{H}}_{ii}^{(a)} \left(\Sigma_N^{i+1,i}\right)^{-1} \tilde{\mathbf{H}}_{ii}^{(a)H} + \rho \tilde{\mathbf{H}}_{ii}^{(b)} \mathbf{I}_{M-N} \tilde{\mathbf{H}}_{ii}^{(b)H} \right|$$
$$= \min\{N, M-N\} \log \rho + \min\{N, N - \min\{N, M-N\}\} \alpha \log \rho + \mathcal{O}(1). \tag{B.37}$$

The above equation is obtained by using Lemma 5 in [42]. Thus, from (B.34) and (B.37), the per user GDOF is upper bounded as

$$d(\alpha) \leq N\alpha + \min\{N, M-N\}(1-\alpha). \tag{B.38}$$

High Interference Case $(\alpha \geq 1)$:

In this case, the outer bound in (B.34) simplifies as follows:

$$R_{\text{s}} \leq \sum_{i=1}^{K-1} \log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=1, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^H + \rho \tilde{\mathbf{H}}_{ii}^{(b)} \mathbf{I}_{M-N} \tilde{\mathbf{H}}_{ii}^{(b)H} \right|$$
$$+ \sum_{i=2}^{K} \log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=1, j\neq i}^{K} \mathbf{H}_{ij}\mathbf{H}_{ij}^H + \rho \tilde{\mathbf{H}}_{ii}^{(b)} \mathbf{I}_{M-N} \tilde{\mathbf{H}}_{ii}^{(b)H} \right| + \mathcal{O}(1),$$

$$\text{or } R_i \leq N\alpha \log \rho + \mathcal{O}(1), \tag{B.39}$$

The above equation is obtained by using Lemma 4 in [42]. Hence, the per user GDOF in case of high interference is upper bounded as follows:

$$d(\alpha) \leq N\alpha. \tag{B.40}$$

But the outer bound in this case exceeds the interference free GDOF i.e. N as $\alpha \geq 1$. Hence, this outer bound is not useful when $\alpha \geq 1$. By combining (B.31), (B.32), (B.36) and (B.38) results in Lemma 2. This completes the proof.

B.5 Proof of Theorem 12

Define $\mathbf{s}_{j,\mathcal{B}}$ as in the proof of Theorem 11. Let $\mathcal{A} = \{1, 2, \ldots, K\}$ be the set of all transmitters, and let $\mathcal{A} - \mathcal{B}$ be the complement of $\mathcal{B}$ in $\mathcal{A}$. Following the procedure in [2] and using Lemma 2 in [80], the sum rate can be bounded as

$$\begin{aligned} R_{\text{s}} \leq\ & h\left(\mathbf{y}_1^* | \mathbf{s}_{K,1}^*\right) + \sum_{i=2}^{K-1} h\left(\mathbf{y}_i^* | \mathbf{s}_{K,\{1,2,\ldots,i\}}^*, \mathbf{s}_{1,\{i+1,\ldots,K\}}^*\right) + h\left(\mathbf{y}_K^* | \mathbf{s}_{1,K}^*\right) \\ & + \sum_{i=2}^{K-1} h\left(\mathbf{y}_i^* | \mathbf{s}_{1,\{K,2,\ldots,i\}}^*, \mathbf{s}_{K,\mathcal{A}-\{K,2,3,\ldots,i\}}^*\right) - h\left(\mathbf{z}_1\right) - 2n \sum_{i=2}^{K-1} h\left(\mathbf{z}_i\right) - h\left(\mathbf{z}_K\right). \end{aligned} \tag{B.41}$$

The above expression is simplified for the SIMO case in [2]. Here, since the transmitters can have multiple antennas, the individual terms in (B.41) need to be evaluated as follows. The first two terms in (B.41) are similar to the evaluation of conditional

differential entropy in the proof of Theorem 11. On simplification, these terms become

$$h\left(\mathbf{y}_1^*|\mathbf{s}_{K,1}^*\right) = \log\left|\beta\left[\mathbf{I}_{N_1} + \sum_{j=2}^{K}\boldsymbol{\phi}_{1,j} + \boldsymbol{\psi}_{1,K}\right]\right|,$$
$$h\left(\mathbf{y}_K^*|\mathbf{s}_{1,K}^*\right) = \log\left|\beta\left[\mathbf{I}_{N_K} + \sum_{j=1}^{K-1}\boldsymbol{\phi}_{K,j} + \boldsymbol{\psi}_{K,1}\right]\right|. \tag{B.42}$$

where $\beta \triangleq \pi e$. In the above equations, $\boldsymbol{\phi}_{i,j}$ and $\boldsymbol{\psi}_{i,j}$ are as defined in the statement of the Theorem. Now consider the term $h\left(\mathbf{y}_i^*|\mathbf{s}_{K,\{1,2,\ldots,i\}}^*, \mathbf{s}_{1,\{i+1,\ldots,K\}}^*\right)$. In this case, $\mathbf{y}_i^* = \mathbf{H}_{ii}\mathbf{x}_i^* + \sum_{j=1, j\neq i}^{K}\mathbf{H}_{ij}\mathbf{x}_j^* + \mathbf{z}_i$, $\mathbf{s}_{K,\{1,2,\ldots,i\}}^* = \sum_{j\in\{1,2,\ldots,i\}}\mathbf{H}_{Kj}\mathbf{x}_j^* + \mathbf{z}_K$, and $\mathbf{s}_{1,\{i+1,\ldots,K\}}^* = \sum_{j\in\{i+1,\ldots,K\}}\mathbf{H}_{1j}\mathbf{x}_j^* + \mathbf{z}_1$. The conditional differential entropy becomes

$$h\left(\mathbf{y}_i^*|\mathbf{s}_{K,\{1,2,\ldots,i\}}^*, \mathbf{s}_{1,\{i+1,\ldots,K\}}^*\right) = \log\left|\pi e\Sigma_{\mathbf{y}_i^*|\mathbf{s}_{K,\{1,2,\ldots,i\}}^*, \mathbf{s}_{1,\{i+1,\ldots,K\}}^*}\right|, \tag{B.43}$$

where

$$\Sigma_{\mathbf{y}_i^*|\mathbf{s}_{K,\{1,2,\ldots,i\}}^*, \mathbf{s}_{1,\{i+1,\ldots,K\}}^*} \triangleq \mathbf{E}\left[\mathbf{y}_i^*\mathbf{y}_i^{*H}\right] - \mathbf{E}\left[\mathbf{y}_i^*\overline{\mathbf{s}}^{*H}\right]\mathbf{E}\left[\overline{\mathbf{s}}^*\overline{\mathbf{s}}^{*H}\right]^{-1}\mathbf{E}\left[\overline{\mathbf{s}}^*\mathbf{y}_i^{*H}\right],$$
$$\text{and } \overline{\mathbf{s}}^* \triangleq \left[\begin{array}{cc}\mathbf{s}_{K,\{1,2,\ldots,i\}}^{*T} & \mathbf{s}_{K,\{1,\ldots,i\}}^{*T}\end{array}\right]^T.$$

The output at receiver i $(i \neq 1, K)$ can be expressed as

$$\mathbf{y}_i^* = \overline{\mathbf{H}}_{i1}\overline{\mathbf{x}}_1 + \overline{\mathbf{H}}_{i,i+1}\overline{\mathbf{x}}_2 + \mathbf{z}_i, \tag{B.44}$$

where $\overline{\mathbf{x}}_1 \triangleq [\mathbf{x}_1^{*T} \ldots \mathbf{x}_i^{*T}]^T$, $\overline{\mathbf{x}}_2 \triangleq [\mathbf{x}_{i+1}^{*T} \ldots \mathbf{x}_K^{*T}]^T$. Here, $\overline{\mathbf{H}}_{i1}$ and $\overline{\mathbf{H}}_{i,i+1}$ are defined after (3.5). The two side information terms can be expressed as $\mathbf{s}_{K,\{1,2,\ldots,i\}} = \overline{\mathbf{H}}_{Ki}\overline{\mathbf{x}}_1 + \mathbf{z}_K$, and $\mathbf{s}_{1,\{i+1,\ldots,K\}} = \overline{\mathbf{H}}_{1,i+1}\overline{\mathbf{x}}_2 + \mathbf{z}_1$. Now consider the evaluation of the individual terms in

$\Sigma_{\mathbf{y}_i^*|\mathbf{s}^*_{K,\{1,2,\ldots,i\}},\mathbf{s}^*_{1,\{i+1,\ldots,K\}}}$:

$$\mathbf{E}\left[\mathbf{y}_i^*\mathbf{y}_i^{*H}\right] = \mathbf{I}_{N_i} + \overline{\mathbf{H}}_{i1}\overline{\mathbf{P}}_{i1}\overline{\mathbf{H}}_{i1}^H + \overline{\mathbf{H}}_{i,i+1}\overline{\mathbf{P}}_{i2}\overline{\mathbf{H}}_{i,i+1}^H,$$

$$\mathbf{E}\left[\mathbf{y}_i^*\overline{\mathbf{s}}^{*H}\right] = \left[\overline{\mathbf{H}}_{i1}\overline{\mathbf{P}}_{i1}\overline{\mathbf{H}}_{Ki}^H \quad \overline{\mathbf{H}}_{i,i+1}\overline{\mathbf{P}}_{i2}\overline{\mathbf{H}}_{1,i+1}^H\right],$$

$$\mathbf{E}\left[\mathbf{s}_{1,K}^*\mathbf{s}_{1,K}^{*H}\right] = \text{blkdiag}\left(\mathbf{I}_{N_i} + \overline{\mathbf{H}}_{Ki}\overline{\mathbf{P}}_{i1}\overline{\mathbf{H}}_{Ki}^H,\ \mathbf{I}_{N_i} + \overline{\mathbf{H}}_{1,i+1}\overline{\mathbf{P}}_{i2}\overline{\mathbf{H}}_{1,i+1}^H\right).$$

Hence, $\Sigma_{\mathbf{y}_i^*|\mathbf{s}^*_{K,\{1,2,\ldots,i\}},\mathbf{s}^*_{1,\{i+1,\ldots,K\}}}$ becomes

$$\begin{aligned}\Sigma_{\mathbf{y}_i^*|\mathbf{s}^*_{K,\{1,2,\ldots,i\}},\mathbf{s}^*_{1,\{i+1,\ldots,K\}}} &= \mathbf{I}_{N_i} + \overline{\mathbf{H}}_{i1}\overline{\mathbf{P}}_{i1}^{1/2}\left\{\mathbf{I}_{M_{r_i}} + \overline{\mathbf{P}}_{i1}^{1/2}\overline{\mathbf{H}}_{Ki}^H\overline{\mathbf{H}}_{Ki}\overline{\mathbf{P}}_{i1}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i1}^{1/2}\overline{\mathbf{H}}_{i1}^H \\ &\quad + \overline{\mathbf{H}}_{i,i+1}\overline{\mathbf{P}}_{i2}^{1/2}\left\{\mathbf{I}_{M_{s_i}} + \overline{\mathbf{P}}_{i2}^{1/2}\overline{\mathbf{H}}_{1,i+1}^H\overline{\mathbf{H}}_{1,i+1}\overline{\mathbf{P}}_{i2}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i2}^{1/2}\overline{\mathbf{H}}_{i,i+1}^H.\end{aligned}$$

where $M_{r_i} \triangleq \sum_{j=1}^{i} M_j$, $M_{s_i} \triangleq \sum_{j=i+1}^{K} M_j$, and the last equation follows from the Woodbury matrix identity [81]. The quantities $\overline{\mathbf{P}}_{i1}$ and $\overline{\mathbf{P}}_{i2}$ are as defined after (3.5). Hence, (B.43) becomes

$$\begin{aligned}h\left(\mathbf{y}_i^*|\mathbf{s}^*_{K,\{1,2,\ldots,i\}}, \mathbf{s}^*_{1,\{i+1,\ldots,K\}}\right) = \log\Bigg|\pi e\Bigg[&\mathbf{I}_{N_i} + \overline{\mathbf{H}}_{i1}\overline{\mathbf{P}}_{i1}^{1/2}\left\{\mathbf{I}_{M_{r_i}} + \overline{\mathbf{P}}_{i1}^{1/2}\overline{\mathbf{H}}_{Ki}^H\overline{\mathbf{H}}_{Ki}\overline{\mathbf{P}}_{i1}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i1}^{1/2}\overline{\mathbf{H}}_{i1}^H \\ &+ \overline{\mathbf{H}}_{i,i+1}\overline{\mathbf{P}}_{i2}^{1/2}\left\{\mathbf{I}_{M_{s_i}} + \overline{\mathbf{P}}_{i2}^{1/2}\overline{\mathbf{H}}_{1,i+1}^H\overline{\mathbf{H}}_{1,i+1}\overline{\mathbf{P}}_{i2}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i2}^{1/2}\overline{\mathbf{H}}_{i,i+1}^H\Bigg]\Bigg|.\end{aligned} \tag{B.45}$$

In a similar manner, it can be shown that

$$\begin{aligned}h\left(\mathbf{y}_i^*|\mathbf{s}^*_{1,\{K,2,\ldots,i\}}, \mathbf{s}^*_{K,\mathcal{A}-\{K,2,3,\ldots,i\}}\right) = \log\Bigg|\pi e\Bigg[&\mathbf{I}_{N_i} + \overline{\mathbf{H}}_{iK}\overline{\mathbf{P}}_{i3}^{1/2}\left\{\mathbf{I}_{M'_{r_i}} + \overline{\mathbf{P}}_{i3}^{1/2}\overline{\mathbf{H}}_{1i}^H\overline{\mathbf{H}}_{1i}\overline{\mathbf{P}}_{i3}^{1/2}\right\}^{-1} \\ &\overline{\mathbf{P}}_{i3}^{1/2}\overline{\mathbf{H}}_{iK}^H + \overline{\mathbf{H}}_{i,K-1}\overline{\mathbf{P}}_{i4}^{1/2}\left\{\mathbf{I}_{M'_{s_i}} + \overline{\mathbf{P}}_{i4}^{1/2}\overline{\mathbf{H}}_{K,i+1}^H\overline{\mathbf{H}}_{K,i+1}\overline{\mathbf{P}}_{i4}^{1/2}\right\}^{-1}\overline{\mathbf{P}}_{i4}^{1/2}\overline{\mathbf{H}}_{i,K-1}^H\Bigg|\Bigg],\end{aligned} \tag{B.46}$$

where $M_{r_i}^{'} \triangleq \sum_{j=2}^{i} M_j + M_K$ and $M_{s_i}^{'} \triangleq M_1 + \sum_{j=i+1}^{K-1} M_j$, and $\overline{\mathbf{P}}_{i3}$ and $\overline{\mathbf{P}}_{i4}$ are as defined after (3.5). Combining (B.42), (B.45) and (B.46) results in Theorem 12.

B.6 Proof of Lemma 3

For the symmetric case, using Lemma 6 in [82], the sum rate outer bound in Theorem 12 reduces to the following form:

$$\begin{aligned}
R_{\mathrm{s}} \leq & \log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=2}^{K} \mathbf{H}_{1j} \mathbf{H}_{1j}^H + \rho \mathbf{H}_{11} \left\{ \mathbf{I}_M + \rho^{\alpha} \mathbf{H}_{K1}^H \mathbf{H}_{K1} \right\}^{-1} \mathbf{H}_{11}^H \right| \\
& + \sum_{i=2}^{K-1} \log \left| \mathbf{I}_N + \overline{\mathbf{H}}_{i1} \left\{ \mathbf{I}_{M_{r_i}} + \overline{\mathbf{H}}_{Ki}^H \overline{\mathbf{H}}_{Ki} \right\}^{-1} \overline{\mathbf{H}}_{i1}^H + \overline{\mathbf{H}}_{i,i+1} \left\{ \mathbf{I}_{M_{r_i}} + \overline{\mathbf{H}}_{1,i+1}^H \overline{\mathbf{H}}_{1,i+1} \right\}^{-1} \overline{\mathbf{H}}_{i,i+1}^H \right| \\
& + \sum_{i=2}^{K-1} \log \left| \mathbf{I}_N + \overline{\mathbf{H}}_{iK} \left\{ \mathbf{I}_{M_{r_i}} + \overline{\mathbf{H}}_{1i}^H \overline{\mathbf{H}}_{1i} \right\}^{-1} \overline{\mathbf{H}}_{iK}^H + \overline{\mathbf{H}}_{i,K-1} \left\{ \mathbf{I}_{M_{r_i}} + \overline{\mathbf{H}}_{K,i+1}^H \overline{\mathbf{H}}_{K,i+1} \right\}^{-1} \overline{\mathbf{H}}_{i,K-1}^H \right| \\
& + \log \left| \mathbf{I}_N + \rho^{\alpha} \sum_{j=1}^{K-1} \mathbf{H}_{Kj} \mathbf{H}_{Kj}^H + \rho \mathbf{H}_{KK} \left\{ \mathbf{I}_M + \rho^{\alpha} \mathbf{H}_{1K}^H \mathbf{H}_{1K} \right\}^{-1} \mathbf{H}_{KK}^H \right|, \text{ where } M_{r_i} \triangleq iM.
\end{aligned} \tag{B.47}$$

Consider the following term in the above equation

$$\begin{aligned}
& \log \left| \mathbf{I}_N + \overline{\mathbf{H}}_{i1} \left\{ \mathbf{I}_{M_{r_i}} + \overline{\mathbf{H}}_{Ki}^H \overline{\mathbf{H}}_{Ki} \right\}^{-1} \overline{\mathbf{H}}_{i1}^H + \overline{\mathbf{H}}_{i,i+1} \left\{ \mathbf{I}_{M_{r_i}} + \overline{\mathbf{H}}_{1,i+1}^H \overline{\mathbf{H}}_{1,i+1} \right\}^{-1} \overline{\mathbf{H}}_{i,i+1}^H \right| \\
& = \log \left| \mathbf{I}_N + \left[\mathbf{H}_{i1} \, \mathbf{H}_{i2} \ldots \, \sqrt{\rho^{(1-\alpha)}} \mathbf{H}_{ii} \right] \left\{ \left[\mathbf{H}_{K1} \, \mathbf{H}_{K2} \ldots \mathbf{H}_{Ki} \right]^H \left[\mathbf{H}_{K1} \, \mathbf{H}_{K2} \, \ldots \, \mathbf{H}_{Ki} \right] \right\}^{-1} \right. \\
& \left[\mathbf{H}_{i1} \, \mathbf{H}_{i2} \ldots \, \sqrt{\rho^{(1-\alpha)}} \mathbf{H}_{ii} \right]^H + \left[\mathbf{H}_{i,i+1} \, \mathbf{H}_{i,i+2} \, \ldots \, \mathbf{H}_{iK} \right] \left\{ \left[\mathbf{H}_{1,i+1} \, \mathbf{H}_{1,i+2} \, \ldots \, \mathbf{H}_{1K} \right]^H \right. \\
& \left. \left. \left[\mathbf{H}_{1,i+1} \, \mathbf{H}_{1,i+2} \, \ldots \, \mathbf{H}_{1K} \right] \right\}^{-1} \left[\mathbf{H}_{i,i+1} \, \mathbf{H}_{i,i+2} \, \ldots \, \mathbf{H}_{iK} \right]^H \right| + \mathcal{O}(1), \\
& \overset{(a)}{=} \log \left| \mathbf{I}_N + \left[\mathbf{H}_{i1} \, \mathbf{H}_{i2} \ldots \, \sqrt{\rho^{(1-\alpha)}} \mathbf{H}_{ii} \right] \left[\mathbf{H}_{i1} \, \mathbf{H}_{i2} \ldots \, \sqrt{\rho^{(1-\alpha)}} \mathbf{H}_{ii} \right]^H \right| + \mathcal{O}(1), \\
& \overset{(b)}{=} \log \left| \mathbf{I}_N + \rho^{(1-\alpha)} \mathbf{H}_{ii} \mathbf{H}_{ii}^H \right| + \mathcal{O}(1),
\end{aligned} \tag{B.48}$$

where *(a)* is obtained by using the fact that the terms containing inverses are independent of α and are invertible when $\frac{N}{M} < K \leq \frac{N}{M} + 1$, and *(b)* is obtained by taking the constant terms into the $\mathcal{O}(1)$ approximation.

Similarly, it can be shown that

$$\begin{aligned}&\log\left|\mathbf{I}_N+\overline{\mathbf{H}}_{iK}\left\{\mathbf{I}_{M_{r_i}}+\overline{\mathbf{H}}_{1i}^H\overline{\mathbf{H}}_{1i}\right\}^{-1}\overline{\mathbf{H}}_{iK}^H+\overline{\mathbf{H}}_{i,K-1}\left\{\mathbf{I}_{M_{r_i}}+\overline{\mathbf{H}}_{K,i+1}^H\overline{\mathbf{H}}_{K,i+1}\right\}^{-1}\overline{\mathbf{H}}_{i,K-1}^H\right|\\&=\log\left|\mathbf{I}_N+\rho^{(1-\alpha)}\mathbf{H}_{ii}\mathbf{H}_{ii}^H\right|+\mathcal{O}(1).\end{aligned}\tag{B.49}$$

Using (B.48) and (B.49), for large ρ, the sum rate bound in (B.47) reduces to

$$\begin{aligned}R_{\mathrm{s}}\leq&\log\left|\mathbf{I}_N+\rho^{\alpha}\sum_{j=2}^{K}\mathbf{H}_{1j}\mathbf{H}_{1j}^H+\rho^{(1-\alpha)}\mathbf{H}_{11}\left\{\mathbf{H}_{K1}^H\mathbf{H}_{K1}\right\}^{-1}\mathbf{H}_{11}^H\right|\\&+\sum_{i=2}^{K-1}\log\left|\mathbf{I}_N+\rho^{(1-\alpha)}\mathbf{H}_{ii}\mathbf{H}_{ii}^H\right|+\sum_{i=2}^{K-1}\log\left|\mathbf{I}_N+\rho^{(1-\alpha)}\mathbf{H}_{ii}\mathbf{H}_{ii}^H\right|\\&+\log\left|\mathbf{I}_N+\rho^{\alpha}\sum_{j=1}^{K-1}\mathbf{H}_{Kj}\mathbf{H}_{Kj}^H+\rho^{(1-\alpha)}\mathbf{H}_{KK}\left\{\mathbf{H}_{1K}^H\mathbf{H}_{1K}\right\}^{-1}\mathbf{H}_{KK}^H\right|+\mathcal{O}(1).\end{aligned}\tag{B.50}$$

The outer bound in (B.50) is further simplified based on the range of α.

Weak Interference Case $(0 \leq \alpha \leq \frac{1}{2})$: Using Lemma 4 in [42], (B.50) becomes

$$R_{\mathrm{s}} \leq \left[2\min\left\{\min\left(N,(K-1)M\right),N-M\right\}\alpha+2(K-1)M(1-\alpha)\right]\log\rho+\mathcal{O}(1).\tag{B.51}$$

Thus, the per user GDOF is upper bounded as given below:

$$d(\alpha)\leq M(1-\alpha)+\frac{1}{K-1}\left(N-M\right)\alpha.\tag{B.52}$$

This results in the first case of Lemma 3.

Moderate Interference Case $\left(\frac{1}{2} \leq \alpha \leq 1\right)$: Using Lemma 4 in [42], (B.50) simplifies to

$$R_{\mathrm{s}} \leq [2\alpha \min\{N, (K-1)M\} + 2\min\{M, N - \min\{N, (K-1)M\}\}(1-\alpha) \\ +2(K-2)M(1-\alpha)]\log\rho + \mathcal{O}(1). \tag{B.53}$$

Hence, the per user GDOF is upper bounded as given below:

$$d(\alpha) \leq M\alpha + \frac{1}{K-1}(N-M)(1-\alpha). \tag{B.54}$$

This results in the second case of Lemma 3.

High Interference Case $(\alpha \geq 1)$:

In this case, it can be shown that the sum rate bound in (B.50) leads to $d(\alpha) \leq \alpha M$, which exceeds the interference free GDOF. Hence, the upper bound reduces to $d(\alpha) \leq M$.

Finally, combining (B.52) and (B.54) results in Lemma 3.

B.7 Proof of Theorem 13

In the initial part of the proof, the outer bound in Lemma 1 is simplified. Then, in specific cases, the performance of the outer bound is characterized as a function of K, M, N and α.

Weak $(0 \leq \alpha \leq \frac{1}{2})$ *and moderate* $(\frac{1}{2} \leq \alpha \leq 1)$ *interference regime:*

When $M \leq N$, for a specific L_1 and L_2 $(0 < L_1 + L_2 \leq K)$, the outer bound in Lemma 1 is of the following form:

$$d(\alpha) \leq \frac{1}{L}\left[L_1 M + \min\{r, L_1(N-M)\}\alpha + L_r + \min\{r, L_2 N - L_r\}(1-\alpha)\right], \tag{B.55}$$

where $r \triangleq \min\{L_2M, L_1N\}$ and $L_r \triangleq L_2M - r$. The RHS in (B.55) is simplified under the following cases.

Case 1: When $\min\{L_2M, L_1N\} = L_2M$, then it results in the following condition:

$$\frac{L_2}{L_1} \leq \frac{N}{M}. \tag{B.56}$$

Under this condition, (B.55) becomes

$$\begin{aligned} d(\alpha) &\leq \frac{1}{L}\left[L_1M + \min\{L_2M, L_1(N-M)\}\,\alpha + \min\{L_2M, L_2N\}\,(1-\alpha)\right], \\ &= \frac{1}{L}\left[LM + \min\{L_2M, L_1(N-M)\}\,\alpha - L_2M\alpha\right]. \end{aligned} \tag{B.57}$$

Equation (B.57) is simplified under the following cases:

Case 1(a): When $\min\{L_2M, L_1(N-M)\} = L_1(N-M)$, then

$$\frac{L_2}{L_1} \geq \frac{N}{M} - 1. \tag{B.58}$$

Combining this with (B.56), results in the following condition

$$\frac{N}{M} - 1 \leq \frac{L_2}{L_1} \leq \frac{N}{M}. \tag{B.59}$$

Under this condition, (B.57) becomes

$$d(\alpha) \leq M(1-\alpha) + \frac{L_1}{L}N\alpha. \tag{B.60}$$

Case 1(b): When $\min\{L_2M, L_1(N-M)\} = L_2M$, then (B.57) becomes

$$d(\alpha) \leq M. \tag{B.61}$$

This case is not useful, as the RHS is equal to the interference free GDOF.

Case 2: When $\min\{L_2M, L_1N\} = L_1N$, then

$$\frac{L_2}{L_1} \geq \frac{N}{M}. \tag{B.62}$$

In this case, (B.55) becomes

$$\begin{aligned} d(\alpha) &\leq \frac{1}{L}\left[L_1M + \min\{L_1N, L_1(N-M)\}\alpha + L_2M - L_1N \right. \\ &\qquad \left. + \min\{L_1N, L_2N - L_2M + L_1N\}(1-\alpha)\right], \\ &= M - \frac{L_1}{L}M\alpha. \end{aligned} \tag{B.63}$$

High interference regime ($\alpha \geq 1$)*:*

In the high interference regime, for a specific L_1 and L_2 ($0 < L_1 + L_2 \leq K$), Lemma 1 is of the following form:

$$d(\alpha) \leq \frac{1}{L}\left[r\alpha + \min\{L_1M, L_1N - r\} + L_r\right]. \tag{B.64}$$

The above equation is simplified under the following cases.

Case 1: When $\min\{L_2M, L_1N\} = L_2M$, then

$$\frac{L_2}{L_1} \leq \frac{N}{M}, \tag{B.65}$$

Under this condition (B.64) becomes

$$d(\alpha) \leq \frac{1}{L}\left[L_2M\alpha + \min\{L_1M, L_1N - L_2M\}\right]. \tag{B.66}$$

The above equation is further simplified under following cases.

Case 1(a): When $\min\{L_1M, L_1N - L_2M\} = L_1N - L_2M$, then the following condition is obtained:

$$\frac{L_2}{L_1} \geq \frac{N}{M} - 1. \tag{B.67}$$

In this case, (B.66) becomes

$$\begin{aligned} d(\alpha) &\leq \frac{1}{L}\left[L_2M\alpha + L_1N - L_2M\right], \\ &= N + \frac{L_2}{L}\left[M(\alpha - 1) - N\right]. \end{aligned} \tag{B.68}$$

Case 1(b): When $\min\{L_1M, L_1N - L_2M\} = L_1M$, (B.66) becomes

$$d(\alpha) \leq \frac{L_2\alpha + L_1}{L}M. \tag{B.69}$$

As $\alpha \geq 1$, this case is not useful as the RHS in the above equation exceeds the interference free GDOF.

Case 2: When $\min\{L_2M, L_1N\} = L_1N$,

$$\frac{L_2}{L_1} \geq \frac{N}{M}, \tag{B.70}$$

and (B.64) becomes

$$\begin{aligned} d(\alpha) &\leq \frac{1}{L}\left[L_1N\alpha + L_2M - L_1N\right] \\ &= N(\alpha - 1) + \frac{L_2}{L}\left[M - N(\alpha - 1)\right]. \end{aligned} \tag{B.71}$$

Due to the minimization involved in Lemma 1, it is not possible to characterize the performance of the outer bounds in all the cases. However, a tractable solution exists

in the following cases.

Case a $(K \geq N + M)$**:** It is required to determine the value of L_1 and L_2, such that the outer bound in Lemma 1 is minimized. First, the weak and moderate interference regimes are considered, followed by the high interference regime in the later part of the proof.

The RHS in (B.60) is minimized when $\frac{L_1}{L}$ is minimized, under the constraint in (B.59). In other words, $\frac{L}{L_1}$ or $\frac{L_2}{L_1}$ is required to be maximized to minimize the RHS in (B.60). From (B.59), it can be noticed that $\frac{L_2}{L_1}$ is maximized when $\frac{L_2}{L_1} = \frac{N}{M}$. As $K \geq M + N$, it is always possible to choose $L_1 = M$ and $L_2 = N$, and (B.60) becomes

$$d(\alpha) \leq M - \frac{M^2}{M+N}\alpha. \tag{B.72}$$

The RHS in (B.63) is minimized by choosing $\frac{L_1}{L}$ as large as possible, under the constraint in (B.62). Maximizing $\frac{L_1}{L}$ is the same as minimizing $\frac{L_2}{L_1}$. By choosing $L_1 = M$ and $L_2 = N$, the RHS in (B.63) is minimized, and the outer bound reduces to following from:

$$d(\alpha) \leq M - \frac{M^2}{M+N}\alpha, \tag{B.73}$$

which is same as that in (B.72). Hence, the outer bound in Lemma 1 is minimized by choosing $L_1 = M$ and $L_2 = N$ and is given by (B.73).

Now, the outer bounds are compared in the following interference regimes. As $K \geq M + N$, the condition $\frac{N}{M} < K \leq \frac{N}{M} + 1$ is not satisfied, and hence, the outer bound in Lemma 3 is not applicable.

Weak interference regime $(0 \leq \alpha \leq \frac{1}{2})$*:* In this case, the outer bound on the per user GDOF

in Lemma 2 reduces to:

$$d(\alpha) \leq M(1-\alpha) + (N-M)\alpha. \tag{B.74}$$

The outer bound in (B.74) exceeds that in (B.73), when $MN < N^2 - M^2$ and which results in (3.8).

Moderate interference regime ($\frac{1}{2} \leq \alpha \leq 1$)*:* In this case, the outer bound in Lemma 2 reduces to

$$d(\alpha) \leq N\alpha. \tag{B.75}$$

The outer bound in (B.73) is active compared to (B.75), when

$$\alpha > \frac{M(M+N)}{N(M+N)+M^2}. \tag{B.76}$$

Note that $\frac{M(M+N)}{N(M+N)+M^2} \leq 1$. The outer bound in (B.73) is active for the entire moderate interference regime, if

$$\begin{aligned} \frac{M(M+N)}{N(M+N)+M^2} &< \frac{1}{2}, \\ \text{or } MN &< N^2 - M^2. \end{aligned} \tag{B.77}$$

Otherwise, when $\frac{1}{2} \leq \alpha \leq \frac{M(M+N)}{N(M+N)+M^2}$, the outer bound in (B.75) is active, and when $\frac{M(M+N)}{N(M+N)+M^2} < \alpha \leq 1$, the outer bound in (B.73) is active. Combining these results together leads to (3.9) and (3.10).

High interference regime ($\alpha \geq 1$)*:* The RHS in (B.68) and (B.71) need to be minimized in cases 1 and 2 discussed in a previous page, respectively. Consider the minimization of (B.68) first. When $M(\alpha-1) - N \geq 0$, the RHS in (B.68) exceeds the interference free GDOF, and hence this case is not useful. When $M(\alpha-1) - N < 0$, the RHS in (B.68) is

minimized by choosing $\frac{L_2}{L}$ as large as possible. From (B.65), it can be noticed that (B.68) is minimized by choosing $L_1 = M$ and $L_2 = N$, and (B.68) becomes

$$d(\alpha) \leq \frac{MN\alpha}{M+N}. \tag{B.78}$$

Now, the RHS in (B.71) is required to be minimized. When $M - N(\alpha - 1) < 0$, $\frac{L_2}{L}$ should be chosen as large as possible. By choosing $L_1 = 0$ and $L_2 > 0$, $\frac{L_2}{L}$ is maximized, and (B.71) becomes

$$d(\alpha) \leq M, \tag{B.79}$$

which is not useful. When $M - N(\alpha - 1) \geq 0$, $\frac{L_2}{L}$ or $\frac{L_2}{L_1}$ should be as low as possible. From (B.70), it can be noticed that (B.71) is minimized by choosing $L_1 = M$ and $L_2 = N$, and it reduces to

$$d(\alpha) \leq \frac{MN\alpha}{M+N}. \tag{B.80}$$

It can be noticed that in both the cases, the RHS are the same. But, (B.78) and (B.80) are active when $1 \leq \alpha \leq \frac{M+N}{M}$ and $1 \leq \alpha \leq \frac{M+N}{N}$, respectively. As $M \leq N$ and the RHS in (B.80) exceeds the interference free GDOF per user, i.e., M, when $\alpha > \frac{M+N}{N}$, it is not required to consider the case $\frac{M+N}{N} < \alpha \leq \frac{M+N}{M}$. The outer bound in Lemmas 2 and 3 exceed the interference free GDOF in this case as mentioned in the proofs of these lemmas, and hence, these bounds are not taken into account in the high interference regime. Finally, taking the minimum of (B.80) and M results in (3.11).

Case b ($\frac{N}{M} + 1 < K < M + N$**, where** $\frac{N}{M}$ **is an integer**)**:** In this case, (B.60) and (B.63) are minimized by choosing $L_1 = 1$ and $L_2 = \frac{N}{M}$. This can be shown by following a similar procedure as in the previous case. Hence, the outer bound in Lemma 1 in

weak/moderate interference regime and high interference regime is of the same form as given in the first case of the Theorem.

Case c ($\frac{N}{M} < K \leq \frac{N}{M} + 1$)**:** In this case, (B.60) is minimized by choosing $L_1 = 1$ and $L_2 = K - 1$. It is easy to verify that this choice of L_1 and L_2 maximizes $\frac{L_1}{L}$ and also satisfies the constraint in (B.59). Hence, (B.60) becomes

$$d(\alpha) \leq M(1-\alpha) + \frac{N\alpha}{K}. \tag{B.81}$$

In this case, the condition $\frac{L_2}{L_1} \geq \frac{N}{M}$ implies that (B.63) arises only when $(K-1)M = N$. The RHS in (B.63) is minimized by choosing $L_1 = 1$ and $L_2 = K-1$, and (B.63) becomes

$$d(\alpha) \quad \leq M - \frac{M\alpha}{K}. \tag{B.82}$$

With some algebraic manipulation, it can be shown that (B.82) reduces to (B.81) when $(K-1)M = N$. Hence, choosing $L_1 = 1$ and $L_2 = K - 1$ minimizes the outer bound in Lemma 1, and it is given by (B.81).

The following interference regimes are considered for comparison with other outer bounds.

Weak interference regime ($0 \leq \alpha \leq \frac{1}{2}$)*:* In the weak interference regime, the outer bound in Lemma 2 reduces to:

$$d(\alpha) \leq M(1-\alpha) + (N-M)\alpha. \tag{B.83}$$

Comparing (B.83) with (B.81), results in the condition $2M \leq N$, which is always satisfied in this case. Hence, the outer bound in (B.83) is loose compared to the outer bound in (B.81). When, the outer bound in (B.81) is compared with the outer bound in Lemma 3, it results in the condition $KM \leq N$, which is satisfied in this case. Hence,

Lemma 3 is active in the entire weak interference regime, which results in (3.12).

Moderate interference regime ($\frac{1}{2} \leq \alpha \leq 1$)*:* In the moderate interference regime, it is easy to see that the outer bound in Lemma 2 is loose compared to the outer bound in Lemma 1. Lemma 3 is tighter than the outer bound in (B.81), when $\alpha \leq \frac{K}{2K-1}$. Consequently, Lemma 1 is active when $\frac{K}{2K-1} < \alpha \leq 1$. Taking the minimum of these two outer bounds results in (3.13).

High interference regime ($\alpha \geq 1$)*:* By employing the similar procedure as followed in the weak/moderate interference regime, it can be shown that the outer bound in Lemma 1 is minimized by choosing $L_1 = 1$ and $L_2 = K - 1$. Also, the outer bound in Lemma 2 and 3 are loose compared to Lemma 1, as they exceed the interference free GDOF per user, i.e., M. In this case, Lemma 1 reduces to

$$d(\alpha) \leq \frac{1}{K}\left[N + (K-1)M(\alpha - 1)\right]. \tag{B.84}$$

Finally, taking the minimum of (B.84) and M results in (3.14), which completes the proof.

Remark: There are a few other cases where it is possible to exactly characterize the performance of these outer bounds. For example, when $K < M + N < aK$, and integer $a \geq 2$, $\frac{M}{a}$ and $\frac{N}{a}$ are integers, choosing $L_1 = \frac{M}{a}$ and $L_2 = \frac{N}{a}$ minimizes the outer bound in Lemma 1, and the outer bound is the same as given in the first case of the Theorem. In this case, $\frac{N}{M}$ need not be an integer.

Appendix C

Appendix for Chapter 6

C.1 Details of the achievable scheme when $(0 < \alpha \leq \frac{2}{3})$

Recall that data bits transmitted on the the lower $m-n$ levels $[1 : m-n]$ remain secure even without transmitter cooperation. When $C = 0$, if all the bottom $m-n$ levels are used for transmission, it is easy to see that transmitting on the remaining n levels either reduces the rate or violates secrecy. But, with cooperation, the upper levels can be used for data transmission using the scheme proposed below. In this scheme, the transmitters exchange the C bits they intend to transmit on the levels $[m-n+1 : m-n+C]$, through the cooperative link. Each transmitter precodes the cooperative bits received from the other transmitter by xoring them with the data bits at the levels $[1 : C]$. This serves a dual purpose: it cancels the interference caused by the data bits sent by the other transmitter, and also ensures that data bits from the other transmitter remain secure. This scheme is illustrated for $C = 0$ and 2 in Fig. 6.2. Mathematically,

the message of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(m-(r+C))^+ \times 1} \\ \mathbf{a}_{(r+C)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-C)\times 1} \\ \mathbf{b}^c_{C\times 1} \end{bmatrix}, \tag{C.1}$$

where $\mathbf{a} \triangleq [a_{r+C}, a_{r+C-1}, \ldots, a_1]^T$ are the own transmitter 1's data bits, $\mathbf{b}^c \triangleq [b_{r+C}, b_{r+C-1}, \ldots, b_{r+1}]^T$ are the cooperative data bits received from transmitter 2, and $r \triangleq m - n$. The message of transmitter 2 is encoded in an analogous fashion. The proposed encoding scheme thus achieves the following symmetric secrecy rate:

$$R_s = m - n + C. \tag{C.2}$$

C.2 Details of the achievable scheme when $(\frac{2}{3} < \alpha < 1)$

First, note that the links in the SLDIC can be classified into three categories: Type I, Type II, and Type III, as shown in Fig. C.1a. The classification is based on whether the data bits are received without interference or with interference at the intended receiver, and whether or not they cause interference at the unintended receiver. The number of Type I (r_1) and Type II (r_2) links are $r_1 = r_2 = \frac{m-l}{2} = m - n$, where l is the number of Type III links, which is given by $l = 2n - m$. In this case, the achievable scheme uses interference cancelation in addition to random bit transmission.

As the bits transmitted on the Type II links $[1 : m - n]$ are not received at the unintended receiver, at least r_2 bits can be sent securely. Data bits transmitted on the Type III/I links (levels $[m - n + 1 : n]/[n + 1 : m]$) will cause interference at the unintended receiver, and it is not possible to ensure secrecy with uncoded data transmission on these levels. As the Type II links are already used up for data transmission,

the remaining $g \triangleq \{n-(r_2+C)\}^+$ levels can be used for transmission with the help of random bits sent by each transmitter. Transmitter i sends the random bits in such a way that they superimpose with the data bits sent by the other transmitter, at receiver i. Thus, the random bits are a form of jamming signal sent by each transmitter to ensure that its own receiver is unable to decode the other transmitter's message. Such a transmission scheme truly exploits the cooperative nature of the transmitters, and works because the transmitters do not deviate from the agreed- upon scheme. Note that, the receiver does not require the knowledge of these random bits in order to decode its own message.

Now, it is required to determine the number of levels of Type I/III links that can be used for data transmission. Notice that bits transmitted on any level get shifted down by $m-n$ levels at the unintended receiver. In the scheme proposed below, transmission occurs in blocks of size $3(m-n)$ levels, with each block consisting of a sequence of data bits, random bits and zero-bits of size $m-n$ each, sent on consecutive levels. Such a scheme ensures that the intended data bits are received without interference at the desired receiver, and, data received at the unintended receiver remains secure. The total number of blocks of size $3r_2$ that can be sent is $B \triangleq \left\lfloor \frac{g}{3r_2} \right\rfloor$. Out of the remaining $t \triangleq g\%\{3r_2\}$ levels, one can use $q \triangleq \min\{(t-r_2)^+, r_2\}$ levels to send data bits securely; the remaining levels are unused.

Mathematically, the signal $\mathbf{x}_1$ of transmitter 1 is encoded as follows:

Case 1 ($q=0$)*:*

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(m-(r_2+C))^+\times 1} \\ \mathbf{a}_{(r_2+C)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-C)\times 1} \\ \mathbf{b}^c_{C\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{a}^u_{p\times 1} \\ \mathbf{0}_{p'\times 1} \end{bmatrix}, \tag{C.3}$$

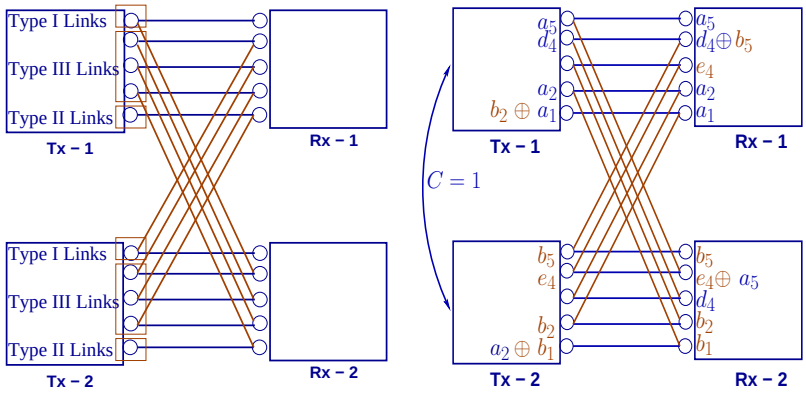


Figure C.1: SLDIC with $m = 5$ and $n = 4$: (a) Different types of links, (b) $C = 1$ and $R_S = 3$.

where $\mathbf{a} \triangleq [a_{r_2+C}, a_{r_2+C-1}, \ldots, a_1]^T$, $\mathbf{b}^c \triangleq [b_{r_2+C}, b_{r_2+C-1}, \ldots, b_{r_2+1}]^T$, $\mathbf{a}^u \triangleq [\mathbf{u}_1, \mathbf{d}_2, \mathbf{z}_3, \mathbf{u}_4, \mathbf{d}_5, \mathbf{z}_6, \ldots, \mathbf{u}_{3B-2}, \mathbf{d}_{3B-1}, \mathbf{z}_{3B},]^T$, $\mathbf{u}_l \triangleq \left[a_{m-(l-1)r_2}, a_{m-(l-1)r_2-1}, \ldots, a_{m-lr_2+1}\right]$, $\mathbf{d}_l \triangleq \left[d_{m-(l-1)r_2}, d_{m-(l-1)r_2-1}, \ldots, d_{m-lr_2+1}\right]$, $\mathbf{z}_l$ is a zero vector of size $1 \times r_2$, $p \triangleq 3B(m-n)$ and $p' \triangleq m-p$. The encoding at transmitter 2 is similar.

Case 2 ($q \neq 0$): The number of data bits that can be sent on the remaining t levels is $q = \min\{(t - r_2)^+, r_2\}$. In this case, the message of transmitter 1 is encoded as follows.

$$\mathbf{x}_1^{\text{mod}} = \mathbf{x}_1 \oplus \begin{bmatrix} \mathbf{0}_{p\times 1} \\ \mathbf{a'}_{t\times 1} \\ \mathbf{0}_{(m-(p+t))\times 1} \end{bmatrix}, \tag{C.4}$$

where $\mathbf{x}_1$ is as defined in (C.3), $\mathbf{a}' \triangleq [\mathbf{u}_{11}, \mathbf{u}_{12}, \mathbf{d}_{11}, \mathbf{d}_{12}, \mathbf{z}]^T$, $\mathbf{u}_{11} \triangleq [a_{m-p}, a_{m-p-1}, \ldots, a_{m-p-q+1}]$, $\mathbf{d}_{11} \triangleq [d_{m-w}, d_{m-w-1}, \ldots, d_{m-w-q+1}]$. Also, $\mathbf{u}_{12}$, $\mathbf{d}_{12}$ and $\mathbf{z}$ are zero vectors of size $1 \times v$, $1 \times f$, and $1 \times v'$, respectively. Here, $v \triangleq (r_2 - q)$, $f \triangleq (t - (r_2 + q))^+$, $w \triangleq p + r_2$ and $v' \triangleq (t - 2r_2)^+$.

As mentioned earlier, the data bits transmitted on the lower levels $[1 : m - n]$ are inherently secure as they are not received by the unintended receiver. With the help of

cooperation and transmission of random bits, it possible to transmit at the higher levels $[m-n+1:m]$. To determine the achievable rate, it is required to find the number of data bits that can be transmitted securely on the higher levels. With the help of interference cancellation, the unintended user's data bits can be completely canceled at the unintended receiver, thereby preventing it from being able to decode these data bits. Hence, cooperation between the users can provide a rate gain of C bits. The number of data bits that can be transmitted securely with the help of transmission of random bits is $B(m-n)+q$ (See (C.3) and (C.4)). By choosing the random bits independent of the data bits and from a $\mathcal{B}(\frac{1}{2})$ distribution, the secrecy of data bits can be ensured, i. e., $H(b_i|d_i \oplus b_i) = H(b_i)$ at receiver 1. Hence, the proposed scheme in (C.3) and (C.4) achieves the following secrecy rate:

$$R_s = m - n + B(m-n) + q + C. \tag{C.5}$$

Depending on the encoding schemes for different interference regimes, the achievable secrecy rate can be obtained in a similar way as mentioned above, and hence, these details are omitted for the remaining cases.

C.3 Details of the achievable scheme when $(1 < \alpha < 2)$

When $(1 < \alpha \leq 1.5)$

The achievable scheme uses transmission of random bits, interference cancelation, or both, depending on the capacity of the cooperative link. The bits received through the cooperative links are transmitted on the levels $[1:C]$. As the links corresponding to

the levels $[1 : n - m]$ are not present at the intended receiver, these links can be directly used to securely relay the other user's data bits. Any data bits transmitted on the levels higher than $n - m$ will cause interference. The cooperative data bits transmitted by transmitter i on the levels higher than $n - m$, namely, on levels $[n - m + 1 : C]$, can be canceled by transmitter j by sending the same data bits along with the data bits of user i $(i \neq j)$. Precoding the data with the other user's data bits thus serves a dual purpose: it cancels interference, and simultaneously ensures secrecy, since one does not want the interfering signal to be decodable.

In the remaining higher levels, the transmission of data bits along with random bits happen in a similar way as mentioned for the moderate interference regime. Define the following quantities: $g \triangleq (m - C)^+$, $B \triangleq \lfloor \frac{g}{3r_2} \rfloor$, $t \triangleq g\%3r_2$ and $q \triangleq \min\{(t - r_2)^+, r_2\}$. Mathematically, the signal of transmitter 1 is encoded as follows:

Case 1 $(q = 0)$:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{a}^e_{p\times 1} \\ \mathbf{0}_{s\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-C)\times 1} \\ \mathbf{b}_{C\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{v\times 1} \\ \mathbf{a}^l_{(C-r_2)^+\times 1} \end{bmatrix}, \tag{C.6}$$

where $\mathbf{a}^e \triangleq [\mathbf{d}_1, \mathbf{u}_2, \mathbf{z}_3, \mathbf{d}_4, \mathbf{u}_5, \mathbf{z}_6, \ldots, \mathbf{d}_{3B-2}, \mathbf{u}_{3B-1}, \mathbf{z}_{3B},]^T$, $\mathbf{u}_l \triangleq [a_{n-(l-1)r_2}, a_{n-(l-1)r_2-1}, \ldots, a_{n-lr_2+1}]$, $\mathbf{d}_l \triangleq \left[d_{n-(l-1)r_2}, d_{n-(l-1)r_2-1}, \ldots, d_{n-lr_2+1}\right]$, $\mathbf{z}_l$ is a zero vector of size $1 \times r_2$, $\mathbf{b} \triangleq [b_C, b_{C-1}, \ldots, b_1]^T$, $\mathbf{a}^l \triangleq [a_C, a_{C-1}, \ldots, a_{r_2+1}]^T$ $p \triangleq 3Br_2$, $s \triangleq n - p$ and $v \triangleq (n - (C - r_2)^+)$.

Case 2 $(q \neq 0)$:

$$\mathbf{x}_1^{\text{mod}} = \mathbf{x}_1 \oplus \begin{bmatrix} \mathbf{0}_{w\times 1} \\ \mathbf{a'}_{t\times 1} \\ \mathbf{0}_{s\times 1} \end{bmatrix}, \tag{C.7}$$

where $\mathbf{x}_1$ is as defined in (C.6), $\mathbf{a}' \triangleq [\mathbf{d}_{11}, \mathbf{d}_{12}, \mathbf{u}_{11}, \mathbf{u}_{12}, \mathbf{z}']^T$, $\mathbf{u}_{11} \triangleq [a_{n-3Br_2-q-v'}, a_{n-3Br_2-q-v'-1}, \ldots, a_{n-3Br_2-2q-v'+1}]$, $\mathbf{d}_{11} \triangleq [d_{n-3Br_2}, d_{n-3Br_2-1}, \ldots, d_{n-3Br_2-q+1}]$. Also, $\mathbf{d}_{12}$, $\mathbf{u}_{12}$ and $\mathbf{z}'$ are zero vectors of length $1 \times v'$, $1 \times (t-(2q+f+v'))^+$ and $1 \times f$, respectively. Here, $v' \triangleq (n-m-q)^+$, $f \triangleq (t-2(q+v'))^+$, $s \triangleq n-m+C$ and $w \triangleq (n-t-s)^+$.

The proposed encoding scheme achieves the following symmetric secrecy rate:

$$R_s = B(n-m) + q + C. \tag{C.8}$$

When $(1.5 < \alpha < 2)$

The links in the SLDIC can be classified into three categories: Type I, Type II, and Type III, as shown in Fig. C.2a. The classification is based on whether the data bits are received with or without interference at the intended receiver, and whether or not they are received at the intended receiver.

Case 1 *When* $(0 \leq C \leq 2(2n-3m))$*:* In this case, the achievable scheme uses a combination of interference cancelation, transmission of random bits and relaying of the other user's data bits. The data bits transmitted by transmitter i on the levels associated with Type II links $[n-m+1:m]$ will be received at the unintended receiver j $(j \neq i)$. In order to ensure secrecy, transmitter j transmits random bits on the levels $[2(n-m)+1:n]$. The remaining levels can be used for transmitting the other user's data bits received through cooperation. The cooperative bits are transmitted on the levels corresponding to Type I and Type III links. The $C_1 \triangleq \lfloor \frac{C}{2} \rfloor$ data bits obtained through cooperation are sent by transmitter i for transmitter j $(i \neq j)$ on the levels corresponding to Type III links. As these links are not present at receiver i $(i \neq j)$, these bits will remain secure. However, the remaining $C_2 \triangleq C - C_1$ cooperative bits sent on the levels corresponding

to Type I links by transmitter i will cause interference at receiver i. The interference caused at receiver i is eliminated by sending the same C_2 data bits on Type III links by transmitter j $(i \neq j)$ and this simultaneously cancels interference and ensures secrecy. The achievable scheme is shown for $m = 5$, $n = 8$ and $C = 2$ in Fig. C.2b.

The signal of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{d}_{l\times 1} \\ \\ \\ \mathbf{0}_{(n-l)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-m)\times 1} \\ \\ \mathbf{a}_{l\times 1} \\ \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-m-C_2)\times 1} \\ \mathbf{b}^u_{C_2\times 1} \\ \mathbf{0}_{l\times 1} \\ \mathbf{b}^l_{C_1\times 1} \\ \mathbf{0}_{(n-m-C_1)^+\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-l-C_2)^+\times 1} \\ \\ \mathbf{a'}_{C_2\times 1} \\ \\ \mathbf{0}_{l\times 1} \end{bmatrix}, \tag{C.9}$$

where $\mathbf{d} \triangleq [d_n, d_{n-1}, \ldots, d_{n-l+1}]^T$, $\mathbf{a} \triangleq [a_l, a_{l-1}, \ldots, a_1]^T$, $\mathbf{b}^l \triangleq [b_{n-m}, b_{n-m-1}, \ldots, b_{n-m-C_1+1}]^T$, $\mathbf{b}^u \triangleq [b_{m+C_2}, b_{m+C_2-1}, \ldots, b_{m+1}]^T$, $\mathbf{a'} \triangleq [a_{m+C_2}, a_{m+C_2-1}, \ldots, a_{m+1}]^T$ and $l \triangleq 2m - n$.

The proposed scheme achieves the following secrecy rate:

$$R_s = 2m - n + C. \tag{C.10}$$

Case 2 *When* $(2(2n - 3m) < C \leq n)$*:* In this case, $2(2n - 3m)$ cooperative data bits out of C cooperative bits obtained through cooperation are used in an analogous way as in the previous case. Define $C_1 \triangleq C_2 \triangleq 2n - 3m$. The remaining cooperative bits $C' \triangleq C - (4n - 6m)$ are used as explained below. Let $C'' \triangleq \left\lceil \frac{C'}{3} \right\rceil$. The cooperative data bits sent by transmitter i on the levels corresponding to Type III links will remain secure, as these links are present to the receiver j $(i \neq j)$ only. The number of data bits that can be relayed by transmitter i for transmitter j on the levels corresponding to Type III links are: $C_{T_3} = \min\{2m - n, C''\}$. The remaining cooperative bits $C_{\text{rem}} \triangleq (C' - C_{T_3})^+$ are transmitted on the levels corresponding to Type I and II links as explained

below. The $C_{T_1} \triangleq \min\left\{\left\lceil \frac{C_{\text{rem}}}{2} \right\rceil, 2m-n\right\}$ cooperative bits sent by transmitter i cause interference at receiver i. The interference caused at receiver i is eliminated by sending the same C_{T_1} bits on Type II/III links by transmitter j $(j \neq i)$. The remaining $C_{T_2} \triangleq \min\{2m-n, (C_{\text{rem}} - C_{T_1})^+\}$ bits are transmitted on the Type II links by transmitter i. These data bits cause interference at receiver i, which is canceled by transmitter j $(i \neq j)$, by sending the same C_{T_2} data bits on the Type III links. Depending on the number of levels used, the number of data bits that can be sent on the Type II links with the help of transmission of random bits is $r_d \triangleq \min\{(2m-n-C_{T_3})^+, 2m-n-C_{T_2}\}$. The achievable scheme is shown for $m=5$, $n=8$ and $C=4$ in Fig. C.2c.

Mathematically, the signal of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(2m-n)\times 1} \\ \mathbf{b}^u_{(2n-3m)\times 1} \\ \mathbf{0}_{(2m-n)\times 1} \\ \mathbf{b}^l_{(2n-3m)\times 1} \\ \mathbf{0}_{(2m-n)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(2m-n-C_{T_1})\times 1} \\ \mathbf{b'}^u_{C_{T_1}\times 1} \\ \\ \mathbf{0}_{(2(n-m)-C_{T_3})\times 1} \\ \mathbf{b'}^l_{C_{T_3}\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-C_{T_2})\times 1} \\ \\ \mathbf{b'}^m_{C_{T_2}\times 1} \\ \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{m\times 1} \\ \\ \mathbf{a}^u_{(2n-3m)\times 1} \\ \mathbf{0}_{(2m-n-C_{T_2})\times 1} \\ \mathbf{a}^m_{C_{T_2}\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-C_{T_1})\times 1} \\ \\ \mathbf{a'}^u_{C_{T_1}\times 1} \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{d}_{r_d\times 1} \\ \mathbf{0}_{(n-m-r_d)\times 1} \\ \mathbf{a}^e_{r_d\times 1} \\ \mathbf{0}_{(m-r_d)\times 1} \end{bmatrix}, \tag{C.11}$$

where $\mathbf{b}^l \triangleq [b_{n-m}, b_{n-m-1}, \ldots, b_{2m-n+1}]^T$, $\mathbf{b}^u \triangleq [b_{2(n-m)}, b_{2(n-m)-1}, \ldots, b_{m+1}]^T$, $\mathbf{b'}^l \triangleq [b_{C_{T_3}}, b_{C_{T_3}-1}, \ldots, b_1]^T$, $\mathbf{b'}^u \triangleq [b_{2(n-m)+C_{T_1}}, b_{2(n-m)+C_{T_1}-1}, \ldots, b_{2(n-m)+1}]^T$, $\mathbf{b'}^m \triangleq [b_{n-m+C_{T_2}}, b_{n-m+C_{T_2}-1}, \ldots, b_{n-m+1}]^T$, $\mathbf{a}^u \triangleq [a_{2(n-m)}, a_{2(n-m)-1}, \ldots, a_{m+1}]^T$, $\mathbf{a}^m \triangleq [a_{n-m+C_{T_2}}, a_{n-m+C_{T_2}-1}, \ldots, a_{n-m+1}]^T$, $\mathbf{a'}^u \triangleq [a_{2(n-m)+C_{T_1}}, a_{2(n-m)+C_{T_1}-1}, \ldots, a_{2(n-m)+1}]^T$, $\mathbf{d} \triangleq [d_n, d_{n-1}, \ldots, d_{n-r_d+1}]^T$

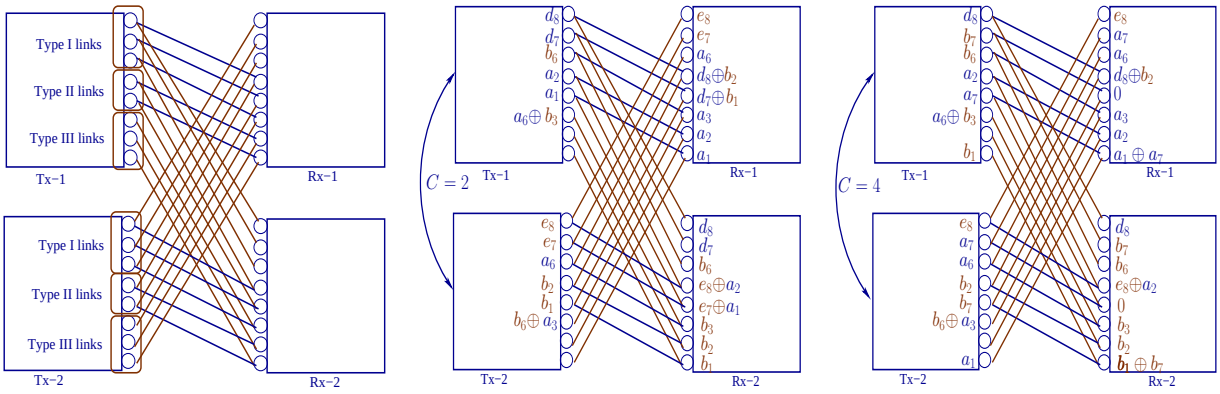


Figure C.2: SLDIC with $m = 5$ and $n = 8$: (a) Different types of links, (b) $C = 2$, $R_S = 4$ (c) $C = 4$, $R_S = 5$.

and $\mathbf{a}^e \triangleq [a_{2m-n}, a_{2m-n-1}, \ldots, a_{2m-n-r_d+1}]^T$. The proposed scheme achieves the following secrecy rate:

$$R_s = 2(2n - 3m) + C_{T_1} + C_{T_2} + C_{T_3} + r_d. \tag{C.12}$$

C.4 Details of the achievable scheme when $(\alpha \geq 2)$

When $0 < C \leq \frac{m}{2}$ and m is even

In this case, interestingly, transmitters share only random bits through the cooperative links. Each transmitter generates C random bits independent of data bits with $\mathrm{Bern}\left(\frac{1}{2}\right)$. The achievable scheme involves transmitting the data bits xored with the random bits. The same random bits are transmitted by the other transmitter, so as to cancel them out at the desired receiver. In contrast to the achievable schemes in Secs. 6.2.2 and 6.2.4, the random bits transmission causes jamming to the unintended receiver only. Through careful observation it is found that sharing random bits through the cooperative links

can achieve higher secrecy rate compared to sharing data bits only. The achievable scheme is illustrated for random bits sharing and data bits sharing for $C = 1$ in Figs. C.3a and C.3b, respectively.

In this case, the signal of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(m-2C)^+ \times 1} \\ \mathbf{a}_{2C \times 1} \\ \mathbf{0}_{(n-m) \times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-2C) \times 1} \\ \\ \mathbf{d}^1_{2C \times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-2C)^+ \times 1} \\ \mathbf{d}^2_{2C \times 1} \\ \mathbf{0}_{(n-m) \times 1} \end{bmatrix}, \tag{C.13}$$

where $\mathbf{a} \triangleq [a_{2C}, a_{2C-1}, \ldots, a_1]^T$, $\mathbf{d}^1 \triangleq [e_C, d_C, \ldots, e_1, d_1]^T$ and $\mathbf{d}^2 \triangleq [d_C, e_C, \ldots, d_1, e_1]^T$. The proposed scheme achieves the following secrecy rate:

$$R_s = 2C. \tag{C.14}$$

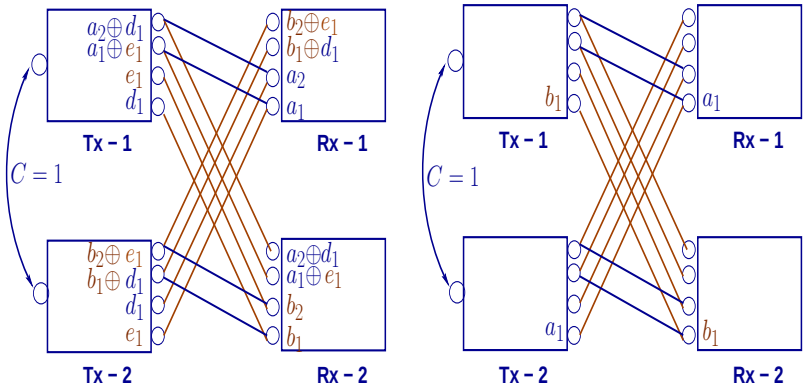
Note that, with data bits sharing, the achievable scheme achieves

$$R_s = C. \tag{C.15}$$

Hence, under the proposed scheme, one can achieve higher rate by sharing random bits than by sharing the data bits.

When $(\frac{m}{2} < C \leq n - \frac{3m}{2})$ and m is even

In this case, the transmitters exchange $\frac{m}{2}$ random bits and $(C - \frac{m}{2})$ data bits. The random bits are used in an analogous fashion as described in the previous subsection. The links corresponding to the levels from $[m + 1 : n - m]$ are present only at the unintended receiver and data bits transmitted on these levels are received without interference at the unintended receiver. Hence, any data bits of the other user relayed using these



(a) Random bits sharing: $R_s = 2$. (b) Data bits sharing: $R_s = 1$.

Figure C.3: SLDIC with $m = 2$ and $n = 4$

levels will remain secure. In this case, the signal of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{a}_{m\times 1} \\ \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-m)\times 1} \\ \\ \mathbf{d}^1_{m\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{d}^2_{m\times 1} \\ \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-C-\frac{m}{2})\times 1} \\ \mathbf{b}^c_{(C-\frac{m}{2})\times 1} \\ \mathbf{0}_{m\times 1} \end{bmatrix}, \tag{C.16}$$

where $\mathbf{a} \triangleq [a_m, a_{m-1}, \ldots, a_1]^T$, $\mathbf{d}^1 \triangleq [e_{\frac{m}{2}}, d_{\frac{m}{2}}, \ldots, e_1, d_1]^T$, $\mathbf{d}^2 \triangleq [d_{\frac{m}{2}}, e_{\frac{m}{2}}, \ldots, d_1, e_1]^T$ and $\mathbf{b}^c \triangleq [b_{\frac{m}{2}+C}, b_{\frac{m}{2}+C-1}, \ldots, b_{m+1}]^T$.

The proposed scheme achieves the following secrecy rate:

$$R_s = \frac{m}{2} + C. \tag{C.17}$$

When $(n - \frac{3m}{2} < C < n - \frac{m}{2})$ and m is even

The novelty of the proposed scheme is in precoding the data bits of the user partly with the other user's data bits and/or with random bits. The random bits used for precoding may be generated at its own transmitter or obtained from the other transmitter through the cooperative link. Then, by appropriately transmitting data bits or random bits on the levels of the SLDIC, the random bits are canceled at the intended receiver, or the

data bits of the other user are canceled out at the unintended receiver. The details of the achievable scheme are as follows.

The achievable scheme uses transmission of random bits, interference cancelation, time sharing and relaying of the other user's data bits. The transmitters share a combination of random bits and data bits through the cooperative links. To simplify the understanding of the achievable scheme, first consider the $\alpha = 2$ case. In this case, both the transmitters share $\frac{m}{2}$ random bits along with $C_1 \triangleq C - \frac{m}{2}$ data bits. In the first time slot, transmitter 1 sends m random bits (d_i and e_i) on alternate levels in $[1 : m]$. In order to eliminate the interference caused by these random bits at receiver 2, the data bits of transmitter 2 are precoded (xored) with these m random bits and transmitted on the levels from $[m + 1 : 2m]$ from transmitter 2. The random bits are not canceled at receiver 1. Further, receiver 1 has no knowledge of these random bits. Hence, it cannot decode the bits intended to receiver 2. Also, the data bits of transmitter 2 received through the cooperative link are transmitted at the upper levels $[n - C_1 + 1 : n]$ from transmitter 1. Again, in order to ensure secrecy at receiver 1, transmitter 2 sends the same data bits at levels $[m - C_1 + 1 : m]$ along with the C_1 data bits of transmitter 1, also received through cooperation. This not only cancels the interference due to the bits sent on levels $[n - C_1 + 1 : n]$ at receiver 1, but also enables transmitter 2 to relay the data bits of transmitter 1.

In the remaining upper levels $[m + 1 : n - C_1]$, transmitter 1 sends its own data bits xored with random bits. Transmitter 2 transmits the same random bits on levels $[1 : C_1]$ to cancel the random bits at receiver 1. In this way, transmitter 1 sends $m - C_1$ data bits of its own and C_1 data bits of transmitter 2, in the first time slot. Simultaneously,

transmitter 2 is able to send m data bits of its own and C_1 data bits of transmitter 1. In the second time slot, the roles of transmitters 1 and 2 are reversed.

In contrast to the achievable schemes for other interference regimes, transmitters exchange both random bits and data bits through the cooperative links. However, as the capacity of the cooperative links increases, it is required to exchange fewer number of random bits. Figures C.4a and C.4b illustrate the scheme for $m = 2$ and $n = 4$, with $C = 2$ bits.

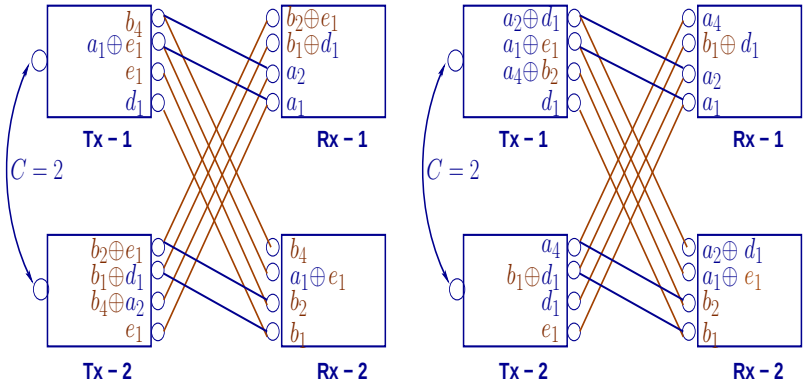
When $\alpha > 2$, it is straightforward to extend the achievable scheme described above. Both the transmitter exchanges $\frac{m}{2}$ random bits and $C' \triangleq C - \frac{m}{2}$ data bits. Out of C' data bits obtained through cooperation, $n - 2m$ data bits are securely relayed using the levels $[m+1 : n-m]$. The m random bits and the remaining $C_1 \triangleq C' - n + 2m$ data bits obtained through cooperation are used in a similar manner as explained for the $\alpha = 2$ case. The signal of transmitter 1 in the first time slot is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(n-m)\times 1} \\ \\ \mathbf{d}^1_{m\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{b}^c_{C_1\times 1} \\ \mathbf{a}_{(m-C_1)\times 1} \oplus \mathbf{d}^2_{(m-C_1)\times 1} \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{m\times 1} \\ \mathbf{b'}^c_{(n-2m)\times 1} \\ \mathbf{0}_{m\times 1} \end{bmatrix}, \tag{C.18}$$

where $\mathbf{d}^1 \triangleq [e_{m/2}, d_{m/2}, \ldots, e_1, d_1]^T$, $\mathbf{b}^c \triangleq [b_n, b_{n-1}, \ldots, b_{n-C_1+1}]^T$, $\mathbf{a} \triangleq [a_{m-C_1}, \ldots, a_2, a_1]^T$, $\mathbf{d}^2 \triangleq [d_q, e_q, \ldots, d_1, e_1]^T$ if $m - C_1$ is even, $\mathbf{d}^2 \triangleq [e_{q+1}, d_q, e_q, \ldots, d_1, e_1]^T$ if $m - C_1$ is odd, $q \triangleq \lfloor \frac{m-C_1}{2} \rfloor$ and $\mathbf{b'}^c \triangleq [b_{n-m}, b_{n-m-1} \ldots, b_{m+1}]^T$.

The signal of transmitter 2 in the first time slot is encoded as follows:

$$\mathbf{x}_2 = \begin{bmatrix} \mathbf{b}_{m\times 1} \oplus \mathbf{e}^2_{m\times 1} \\ \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-m)\times 1} \\ \mathbf{b}^l_{C_1\times 1} \oplus \mathbf{a}^c_{C_1\times 1} \\ \mathbf{e}^1_{(m-C_1)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{m\times 1} \\ \mathbf{a'}^c_{(n-2m)\times 1} \\ \mathbf{0}_{m\times 1} \end{bmatrix}, \tag{C.19}$$



(a) First slot: $(R_1, R_2) = (2, 3)$. (b) Second slot: $(R_1, R_2) = (3, 2)$.

Figure C.4: SLDIC with $m = 2$ and $n = 4$: $C = 2$ and $R_s = 2.5$.

where $\mathbf{b} \triangleq [b_m, b_{m-1}, \ldots, b_1]^T$, $\mathbf{e}^2 \triangleq [e_{m/2}, d_{m/2}, \ldots, e_1, d_1]^T$, $\mathbf{b}^l \triangleq [b_n, b_{n-1}, \ldots, b_{n-C_1+1}]^T$, $\mathbf{a}^c \triangleq [a_m, a_{m-1}, \ldots, a_{m-C_1+1}]^T$, $\mathbf{e}^1 \triangleq [d_q, e_q, \ldots, d_1, e_1]^T$ if $m - C_1$ is even, $\mathbf{e}^1 \triangleq [e_{q+1}, d_q, e_q, \ldots, d_1, e_1]^T$ if $m - C_1$ is odd, $q \triangleq \lfloor \frac{m-C_1}{2} \rfloor$ and $\mathbf{a}'^c \triangleq [a_{n-m}, a_{n-m-1}, \ldots, a_{m+1}]^T$. In the second time slot, the encoding for transmitters 1 and 2 is reversed. The proposed scheme achieves the following secrecy rate:

$$R_s = \frac{n}{2} - \frac{m}{4} + \frac{C}{2}. \tag{C.20}$$

When $(n - \frac{m}{2} \leq C \leq n)$ and m is even

In this case, both the transmitters share C data bits and the achievable scheme uses interference cancelation. The signal of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{0}_{(n-C+m)^+ \times 1} \\ \\ \mathbf{a}_{(C-m)\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-C)^+ \times 1} \\ \\ \mathbf{b}_{C\times 1} \end{bmatrix}, \tag{C.21}$$

where $\mathbf{a} = [a_C, a_{C-1}, \ldots, a_{m+1}]^T$ and $\mathbf{b} = [b_C, b_{C-1}, \ldots, b_1]^T$. The proposed scheme achieves the following secrecy rate.

$$R_s = C. \tag{C.22}$$

When $0 < C \leq \frac{m+1}{2}$ and m is odd

The achievable scheme and encoding of the message are analogous to that mentioned for the $(0 < C \leq \frac{m}{2})$ and even valued m case. The proposed scheme achieves the following secrecy rate:

$$R_s = \min\{2C, m\}. \tag{C.23}$$

When $\frac{m+1}{2} < C \leq \frac{2n-3m+1}{2}$ and m is odd

In this case, the achievable scheme is analogous to that mentioned for the $(\frac{m}{2} < C \leq n - \frac{3m}{2})$ and even valued m case. The signal of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{d}^u_{m\times 1} \oplus \mathbf{a}^u_{m\times 1} \\ \mathbf{0}_{(n-2m)\times 1} \\ \mathbf{d}^l_{m\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-m-C')\times 1} \\ \mathbf{b}^c_{C'\times 1} \\ \mathbf{0}_{m\times 1} \end{bmatrix}, \tag{C.24}$$

where $\mathbf{d}^u \triangleq [e_{\frac{m+1}{2}}, \ldots, d_1, e_1]^T$, $\mathbf{a}^u \triangleq [a_m, a_{m-1}, \ldots, a_1]^T$, $\mathbf{d}^l \triangleq [d_{\frac{m+1}{2}}, \ldots, e_1, d_1]^T$, $\mathbf{b}^c \triangleq [b_{m+C'}, b_{m+C'-1}, \ldots, b_{m+1}]^T$ and $C' \triangleq C - \frac{m+1}{2}$. The proposed scheme achieves the following secrecy rate:

$$R_s = m + \min\left\{C - \frac{m+1}{2}, n - 2m\right\}. \tag{C.25}$$

When $\frac{2n-3m+1}{2} < C \leq n$ and m is odd

In this case, the achievable scheme is similar to that described for the $(n - \frac{3m}{2} < C < n - \frac{m}{2})$ and even valued m case, with minor differences in the way the encoding is performed. For simplicity of exposition, the encoding scheme is explained for the $\alpha = 2$ case. Now define the following quantities: $C_1^{uu} = \left\lceil \frac{C}{2} \right\rceil$, $C_2^{lu} = C_1^{uu}$, $C_1^{ul} = (m - C_1^{uu})^+$, $C_2^{ll} = C_1^{ul}$, $C_1^r = \left\lceil \frac{C_1^{ul}}{2} \right\rceil$, $C_1^{lu} = (C - C_1^{uu} - C_1^r)^+$, $C_1^{ll} = \min\{2C_1^r, (m - C_1^{lu})^+)\}$, $C_2^{ul} = C_1^{ll}$, $C_2^r = \max\left\{ \left\lceil \frac{C_2^{ll}}{2} \right\rceil, \left\lfloor \frac{C_2^{ul}}{2} \right\rfloor \right\}$, $C_2^{uu} = (C - C_2^{lu} - C_2^r)^+$. In the first time slot, transmitter 1 sends C_1^{uu} data bits of transmitter 2 received through cooperation on the upper levels $[n - C_1^{uu} + 1 : n]$. In order to ensure secrecy at receiver 1, transmitter 2 sends the same data bits at levels $[m - C_2^{lu} + 1 : m]$ along with the C_2^{lu} data bits of transmitter 1, also received through cooperation. In the remaining upper levels $[m + 1 : n - C_1^{uu}]$, transmitter 1 sends C_1^{ul} of its own data bits, xored with random bits. Transmitter 2 sends the same random bits on levels $[1 : C_2^{ll}]$ to cancel the random bits at receiver 1. The number of random cooperative bits in such a transmission is C_1^r. Also, transmitter 1 relays C_1^{lu} data bits of transmitter 2 received through cooperation on the levels $[m - C_1^{lu} + 1 : m]$. As the links corresponding to these levels are not present to receiver 1, these data bits remain secure. Transmitter 1 sends C_1^{ll} random bits on the levels $[1 : C_1^{ll}]$ to ensure secrecy of user 2's data. Transmitter 2 sends its $C_2^{ul} = C_1^{ll}$ data bits precoded with the same random bits transmitted on the levels $[1 : C_1^{ll}]$, to eliminate the random bits at receiver 2. The number of cooperative random bits used by transmitter 2 is C_2^r. Then, transmitter 2 can relay the remaining C_2^{uu} cooperative data bits on the upper levels $[n - C_2^{uu} + 1 : n]$. As these bits will cause interference at receiver 2, transmitter 1 sends the same data bits on the levels $[m - C_2^{uu} + 1 : m]$ to cancel the interference at receiver 2.

When $\alpha > 2$, it is straightforward to extend the achievable scheme described above. In the first time slot, the signal of transmitter 1 is encoded as follows:

$$\mathbf{x}_1 = \begin{bmatrix} \mathbf{b}'^{uu}_{C_1^{uu}\times 1} \\ \mathbf{a}^{ul}_{C_1^{ul}\times 1} \oplus \mathbf{d}^{ul}_{C_1^{ul}\times 1} \\ \\ \mathbf{0}_{(n-C_1^{uu}-C_1^{ul})\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-m)\times 1} \\ \mathbf{b}'^{lu}_{C_1^{lu}\times 1} \\ \mathbf{0}_{(m-C_1^{lu}-C_1^{ll})^+\times 1} \\ \mathbf{d}^{ll}_{C_1^{ll}\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{m\times 1} \\ \mathbf{b}'^{c}_{(n-2m)\times 1} \\ \mathbf{a}^{lu}_{C_2^{uu}\times 1} \\ \mathbf{0}_{(m-C_2^{uu})^+\times 1} \end{bmatrix}, \tag{C.26}$$

where $\mathbf{b}'^{uu} \triangleq [b_n, b_{n-1}, \ldots, b_{n-C_1^{uu}+1}]^T$, $\mathbf{b}'^{lu} \triangleq [b_m, b_{m-1}, \ldots, b_{m-C_1^{lu}+1}]^T$, $\mathbf{a}^{ul} \triangleq [a_{C_1^{ul}}, a_{C_1^{ul}-1}, \ldots, a_1]^T$, $\mathbf{d}^{ul} \triangleq [d_{C_1^r}, e_{C_1^r}, \ldots, d_1, e_1]^T$ if C_1^{ul} is even, $\mathbf{d}^{ul} \triangleq [e_{C_1^r}, d_{C_1^r-1}, e_{C_1^r-1}, \ldots, d_1, e_1]^T$ if C_1^{ul} is odd, $\mathbf{a}^{lu} \triangleq [a_n, a_{n-1}, \ldots, a_{n-C_2^{uu}+1}]^T$, $\mathbf{d}^{ll} \triangleq [e_{\frac{C_1^{ll}}{2}}, d_{\frac{C_1^{ll}}{2}}, \ldots, e_1, d_1]^T$ if C_1^{ll} is even, $\mathbf{d}^{ll} \triangleq [d_{\left\lceil \frac{C_1^{ll}}{2} \right\rceil}, e_{\lceil C_1^{ll} \rceil - 1}, d_{\lceil C_1^{ll} \rceil - 1} \ldots, e_1, d_1]^T$ if C_1^{ll} is odd and $\mathbf{b}'^{c} \triangleq [b_{n-m}, b_{n-m-1}, \ldots, b_{m+1}]^T$. The signal of transmitter 2 is encoded as follows:

$$\mathbf{x}_2 = \begin{bmatrix} \mathbf{0}^{uu}_{(m-C_2^{ul})\times 1} \\ \mathbf{b}^{ul}_{C_2^{ul}\times 1} \\ \mathbf{0}_{(n-2m)\times 1} \\ \mathbf{b}^{lu}_{C_2^{lu}\times 1} \\ \mathbf{0}_{(m-C_2^{lu})\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{a}'^{uu}_{C_2^{uu}\times 1} \\ \mathbf{0}_{(m-C_2^{uu})\times 1} \\ \mathbf{a}^{c}_{(n-2m)\times 1} \\ \mathbf{a}'^{lu}_{C_2^{lu}\times 1} \\ \mathbf{0}_{(m-C_2^{lu})\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(n-C_2^{ll})\times 1} \\ \\ \\ \\ \mathbf{e}^{ll}_{C_2^{ll}\times 1} \end{bmatrix} \oplus \begin{bmatrix} \mathbf{0}_{(m-C_2^{ul})\times 1} \\ \\ \mathbf{e}^{ul}_{C_2^{ul}\times 1} \\ \\ \mathbf{0}_{(n-m)\times 1} \end{bmatrix}, \tag{C.27}$$

where $\mathbf{b}^{ul} \triangleq [b_{C_2^{ul}}, b_{C_2^{ul}-1}, \ldots, b_1]^T$, $\mathbf{b}^{lu} \triangleq [b_n, b_{n-1}, \ldots, b_{n-C_2^{lu}+1}]^T$, $\mathbf{a}'^{uu} \triangleq [a_n, a_{n-1}, \ldots, a_{n-C_2^{uu}+1}]^T$, $\mathbf{a}^{c} \triangleq [a_{n-m}, a_{n-m-1}, \ldots, a_{m+1}]^T$, $\mathbf{a}'^{lu} \triangleq [a_m, a_{m-1}, \ldots, a_{m-C_2^{lu}+1}]^T$, $\mathbf{e}^{ll} \triangleq [d_{\frac{C_2^{ll}}{2}}, e_{\frac{C_2^{ll}}{2}}, \ldots, d_1, e_1]^T$ if C_2^{ll} is even, $\mathbf{e}^{ll} \triangleq [e_{\left\lceil \frac{C_2^{ll}}{2} \right\rceil}, d_{\left\lceil \frac{C_2^{ll}}{2} \right\rceil - 1}, \ldots, d_1, e_1]^T$ if C_2^{ll} is odd, $\mathbf{e}^{ul} \triangleq [e_{\frac{C_2^{ul}}{2}}, d_{\frac{C_2^{ll}}{2}}, \ldots, e_1, d_1]^T$ if C_2^{ul} is even and $\mathbf{e}^{ul} \triangleq [d_{\left\lceil \frac{C_2^{ul}}{2} \right\rceil}, e_{\left\lceil \frac{C_2^{ul}}{2} \right\rceil - 1}, \ldots, e_1, d_1]^T$ if C_2^{ul} is odd.

In the second time slot, the encoding scheme is reversed for transmitters 1 and 2. The proposed scheme achieves the following secrecy rate:

$$R_s = n - 2m + \frac{1}{2}\left[C_1^{ul} + 2C_1^{uu} + C_2^{uu} + C_1^{lu} + C_2^{ul}\right]. \tag{C.28}$$

Appendix D

Appendix for Chapter 7

D.1 Proof of Theorem 14

Using Fano's inequality, the rate of user 1 is upper bounded as

$$\begin{aligned}
NR_1 &\leq I(W_1; \mathbf{y}_1^N) + N\epsilon_1, \\
&= H(\mathbf{y}_1^N) - H(\mathbf{y}_1^N|W_1) + N\epsilon_1, \\
&\overset{(a)}{\leq} H(\mathbf{y}_1^N) - H(\mathbf{y}_1^N|W_1, \mathbf{x}_1^N) + N\epsilon_1, \\
&= H(\mathbf{y}_1^N) - H(\mathbf{x}_{2a}^N|W_1, \mathbf{x}_1^N) + N\epsilon_1, \text{ where, } \mathbf{x}_{2a}^N \triangleq \mathbf{D}^{q-n}\mathbf{x}_2^N, \\
&\leq H(\mathbf{y}_1^N) - H(\mathbf{x}_{2a}^N|W_1, \mathbf{x}_1^N, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + N\epsilon_1, \\
&\overset{(b)}{=} H(\mathbf{y}_1^N) - H(\mathbf{x}_{2a}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + N\epsilon_1, \\
\text{or } H(\mathbf{x}_{2a}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) &\leq H(\mathbf{y}_1^N) - NR_1 + N\epsilon_1, \qquad \text{(D.1)}
\end{aligned}$$

where (a) follows by using the fact that the entropy cannot increase by additional conditioning and (b) follows by using the relation in (7.1).

Adopting similar steps for user 2, it follows that

$$H(\mathbf{x}_{1a}^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) \leq H(\mathbf{y}_2^N) - NR_2 + N\epsilon_2, \text{ where, } \mathbf{x}_{1a}^N \triangleq \mathbf{D}^{q-n}\mathbf{x}_1^N. \tag{D.2}$$

Note that in obtaining the outer bounds in (D.1) and (D.2), the secrecy constraint at receiver has not been used. Using the secrecy constraint at receiver 2, the rate of user 1 can also be bounded as follows:

$$\begin{aligned}
NR_1 &\leq I(W_1;\mathbf{y}_1^N) + N\epsilon_1, \\
&\overset{(a)}{\leq} I(W_1;\mathbf{y}_1^N,\mathbf{y}_2^N) + N\epsilon_1, \\
&\overset{(b)}{=} I(W_1;\mathbf{y}_1^N|\mathbf{y}_2^N) + N\epsilon_1, \\
&\leq H(\mathbf{y}_1^N|\mathbf{y}_2^N) + N\epsilon_1, \\
&\overset{(c)}{=} H(\mathbf{y}_1^N,\mathbf{y}_2^N) - H(\mathbf{y}_2^N) + N\epsilon_1, \\
&\overset{(d)}{\leq} H(\mathbf{y}_1^N,\mathbf{y}_2^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N) - H(\mathbf{y}_2^N) + N\epsilon_1, \\
&\overset{(e)}{=} H(\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N) + H(\mathbf{y}_1^N,\mathbf{y}_2^N|\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N) - H(\mathbf{y}_2^N) + N\epsilon_1, \qquad \text{(D.3)} \\
&\overset{(f)}{\leq} H(\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N,\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + H(\mathbf{y}_1^N,\mathbf{y}_2^N|\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N) - H(\mathbf{y}_2^N) + N\epsilon_1, \\
&\overset{(g)}{\leq} H(\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + H(\mathbf{x}_{1a}^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + H(\mathbf{x}_{2a}^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + H(\mathbf{y}_1^N,\mathbf{y}_2^N|\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N) \\
&\qquad - H(\mathbf{y}_2^N) + N\epsilon_1, \qquad \text{(D.4)}
\end{aligned}$$

where (a) is due to a genie providing $\mathbf{y}_2^N$ to receiver 1; (b) is due to the perfect secrecy condition at receiver 2, i.e., $I(W_1;\mathbf{y}_2^N) = 0$; (c) is obtained from the joint entropy relation: $H(\mathbf{y}_1^N,\mathbf{y}_2^N) = H(\mathbf{y}_2^N) + H(\mathbf{y}_1^N|\mathbf{y}_2^N)$; (d), (e) and (f) follow from the chain rule for joint entropy; and (g) is obtained using the fact that removing conditioning cannot decrease the entropy.

In deriving the bounds in (D.1)-(D.4), one of the difficulties is that the encoded messages are no longer independent due to the cooperation between the transmitters. This problem is overcome by cleverly using $\mathbf{v}_{12}$ and $\mathbf{v}_{21}$ in a manner that allows one to bound the different entropy terms.

Using (D.1) and (D.2), (D.4) becomes

$$\begin{aligned} NR_1 &\leq H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{y}_1^N) - N\left[R_1 + R_2\right] + H(\mathbf{y}_1^N, \mathbf{y}_2^N | \mathbf{x}_{1a}^N, \mathbf{x}_{2a}^N) + N\epsilon_1, \\ \text{or } N[2R_1 + R_2] &\leq H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{y}_1^N) + H(\mathbf{D}^{q-m}\mathbf{x}_1^N | \mathbf{x}_{1a}^N) + H(\mathbf{D}^{q-m}\mathbf{x}_2^N | \mathbf{x}_{2a}^N) + N\epsilon_1. \end{aligned} \tag{D.5}$$

The above equation is simplified under the following cases.

Case 1 $(m \geq n)$: In this case, $q = m$ and (D.5) becomes

$$\begin{aligned} N[2R_1 + R_2] &\leq H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{y}_1^N) + H(\mathbf{x}_1^N | \mathbf{x}_{1a}^N) + H(\mathbf{x}_2^N | \mathbf{x}_{2a}^N) + N\epsilon_1, \\ \text{or } R &\leq \frac{1}{3}\left[2C + 3m - 2n\right]. \end{aligned} \tag{D.6}$$

The above equation is obtained using the fact that the entropies $H(\mathbf{v}_{12}, \mathbf{v}_{21})$, $H(\mathbf{y}_i)$ and $H(\mathbf{x}_i|\mathbf{x}_{ia})$ are upper bounded by $2C$, m and $m - n$, respectively.

Case 2 $(m < n)$: In this case, $q = n$ and (D.5) becomes

$$\begin{aligned} N[2R_1 + R_2] &\leq H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{y}_1^N) + H(\mathbf{D}^{n-m}\mathbf{x}_1^N | \mathbf{x}_1^N) + H(\mathbf{D}^{n-m}\mathbf{x}_2^N | \mathbf{x}_2^N) + N\epsilon_1, \\ \text{or } R &\leq \frac{1}{3}\left[2C + n\right]. \end{aligned} \tag{D.7}$$

The above equation is obtained using the fact that the entropies $H(\mathbf{v}_{12}, \mathbf{v}_{21})$ and $H(\mathbf{y}_1)$ are upper bounded by $2C$ and n, respectively. Also, given $\mathbf{x}_i^N$, there is no uncertainty about $\mathbf{D}^{n-m}\mathbf{x}_i^N$. Combining (D.6) and (D.7) results in (7.2). This completes the proof.

D.2 Proof of Theorem 15

Using Fano's inequality, the rate of user 1 is upper bounded as

$$\begin{aligned} NR_1 &\leq I(W_1; \mathbf{y}_1^N) + N\epsilon_1, \\ &\overset{(a)}{\leq} I(W_1; \mathbf{y}_1^N, \mathbf{y}_{2a}^N) + N\epsilon_1, \text{ where } \mathbf{y}_{2a}^N \triangleq (\mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N), \\ &= I(W_1; \mathbf{y}_{2a}^N) + I(W_1; \mathbf{y}_1^N | \mathbf{y}_{2a}^N) + N\epsilon_1, \end{aligned} \tag{D.8}$$

where (a) is due to a genie providing $\mathbf{y}_{2a}^N$ to receiver 1. From the secrecy constraint at receiver 2, the following holds:

$$\begin{aligned} & I(W_1; \mathbf{y}_2^N) = 0, \\ \text{or } & I(W_1; \mathbf{y}_{2a}^N, \mathbf{y}_{2b}^N) = 0, \text{ where } \mathbf{y}_{2b}^N = \mathbf{x}_{2a}^N \oplus \mathbf{x}_{1c}^N, \\ \text{or } & I(W_1; \mathbf{y}_{2a}^N) + I(W_1; \mathbf{y}_{2b}^N | \mathbf{y}_{2a}^N) = 0. \end{aligned} \tag{D.9}$$

As mutual information cannot be negative, $I(W_1; \mathbf{y}_{2a}^N) = 0$, and (D.8) becomes

$$\begin{aligned} NR_1 &\leq I(W_1; \mathbf{y}_1^N | \mathbf{y}_{2a}^N) + N\epsilon_1, \\ &= H(\mathbf{y}_1^N | \mathbf{y}_{2a}^N) - H(\mathbf{y}_1^N | \mathbf{y}_{2a}^N, W_1) + N\epsilon_1, \\ &\overset{(a)}{=} H(\mathbf{x}_{2a}^N, \mathbf{x}_{2b}^N, \mathbf{x}_{1a}^N \oplus \mathbf{x}_{2c}^N | \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N) - H(\mathbf{x}_{2a}^N, \mathbf{x}_{2b}^N, \mathbf{x}_{1a}^N \oplus \mathbf{x}_{2c}^N | \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N, W_1) + N\epsilon_1, \\ &= H(\mathbf{x}_2^N | \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N) - H(\mathbf{x}_2^N | \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N, W_1) + N\epsilon_1, \end{aligned} \tag{D.10}$$

where (a) is obtained by partitioning the message into three parts as shown in Fig. 7.1a.

The encoded messages at the transmitters are correlated due to the cooperation between the transmitters. Because of this, it is not straightforward to upper bound or

simplify (D.10). To overcome this problem, $H(\mathbf{x}_2^N|\mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N)$ is upper bounded by $H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_2^N|\mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N)$, and the latter is further upper bounded as explained below.

$$\begin{aligned}
NR_1 &\leq H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_2^N|\mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N) - H(\mathbf{x}_2^N|\mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N, W_1) + N\epsilon_1, \\
&\overset{(a)}{\leq} H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N) + H(\mathbf{x}_2^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N) - H(\mathbf{x}_2^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N, W_1) \\
&\qquad + N\epsilon_1, \\
&\overset{(b)}{\leq} H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{x}_2^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N) - H(\mathbf{x}_2^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{1b}^N, W_1) + N\epsilon_1, \\
&\overset{(c)}{\leq} H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + N\epsilon_1, \\
\text{or } R_1 &\leq 2C,
\end{aligned} \tag{D.11}$$

where (a) is due to the fact that conditioning cannot increase the entropy; (b) is due to the fact that removing conditioning cannot decrease the entropy; and (c) is obtained using the relationship in (7.1). This completes the proof.

D.3 Proof of Theorem 16

Using Fano's inequality, rate of user 1 is bounded as

$$\begin{aligned}
NR_1 &\leq I(W_1; \mathbf{y}_1^N) + N\epsilon_1, \\
&\overset{(a)}{\leq} I(W_1; \mathbf{y}_1^N, \mathbf{y}_{2a}^N) + N\epsilon_1, \\
&\overset{(b)}{=} I(W_1; \mathbf{y}_1^N|\mathbf{y}_{2a}^N) + N\epsilon_1, \\
&= H(\mathbf{y}_1^N|\mathbf{x}_{1a}^N) - H(\mathbf{y}_1^N|\mathbf{x}_{1a}^N, W_1) + N\epsilon_1, \\
&\leq H(\mathbf{y}_1^N, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{x}_{1a}^N) - H(\mathbf{y}_1^N|\mathbf{x}_{1a}^N, W_1) + N\epsilon_1, \\
&\leq H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{x}_{1a}^N) + H(\mathbf{y}_1^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N) - H(\mathbf{y}_1^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, W_1) + N\epsilon_1,
\end{aligned}$$

$$
\begin{aligned}
&\leq H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{y}_1^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N) - H(\mathbf{y}_1^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, W_1) + N\epsilon_1, \\
&\overset{(c)}{=} H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{x}_{2a}^N, \mathbf{y}_{1b}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N) - H(\mathbf{x}_{2a}^N, \mathbf{y}_{1b}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, W_1) + N\epsilon_1, \\
&= H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{x}_{2a}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N) + H(\mathbf{y}_{1b}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{2a}^N) \\
&\qquad\qquad - H(\mathbf{x}_{2a}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, W_1) - H(\mathbf{y}_{1b}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{2a}^N, W_1) + N\epsilon_1, \\
&\overset{(d)}{=} H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + H(\mathbf{y}_{1b}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{2a}^N) - H(\mathbf{y}_{1b}^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_{1a}^N, \mathbf{x}_{2a}^N, W_1) + N\epsilon_1, \quad \text{(D.12)}
\end{aligned}
$$

where (a) is due to a genie providing $\mathbf{y}_{2a}^N$ to receiver 1; (b) is obtained using the secrecy constraint at receiver 2; (c) is obtained by partitioning of the encoded message and output as shown in Fig. 7.1b; and (d) is obtained using the relation in (7.1).

Once again, as the encoded messages at transmitters are correlated, it is not straightforward to bound or simplify the entropy terms in (D.12). To overcome this problem, the output $\mathbf{y}_{1b}$ is partitioned into two parts as follows:

- $\mathbf{y}_{1b}^{(1)}$: contains $\mathbf{x}_{1a}$ sent by transmitter 1 and the interference caused by transmitter 2 due to transmission on the levels $[2m - n + 1 : m]$
- $\mathbf{y}_{1b}^{(2)}$: contains $\mathbf{x}_{1b}$ sent by transmitter 1 and the interference caused by transmitter 2 due to transmission on the levels $[1 : 2m - n]$

The partitioning of $\mathbf{y}_{1b} = (\mathbf{y}_{1b}^{(1)}, \mathbf{y}_{1b}^{(2)})$ is illustrated in the Fig. 7.1b. Now consider the

second term in (D.12):

$$\begin{aligned}
&H(\mathbf{y}_{1b}^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N)\\
&= H(\mathbf{y}_{1b}^{(1)N},\mathbf{y}_{1b}^{(2)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N)\\
&= H(\mathbf{x}_{2b}^N,\mathbf{x}_{2c}^{(1)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N) + H(\mathbf{y}_{1b}^{(2)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N,\mathbf{y}_{1b}^{(1)N})\\
&= H(\mathbf{x}_{2b}^N,\mathbf{x}_{2c}^{(1)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{2a}^N) + H(\mathbf{y}_{1b}^{(2)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N,\mathbf{y}_{1b}^{(1)N}). \qquad \text{(D.13)}
\end{aligned}$$

The above equation is obtained using the fact that $I(\mathbf{x}_{2b}^N,\mathbf{x}_{2c}^{(1)N};\mathbf{x}_{1a}^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{2a}^N)=0$. This can be obtained using the relation in (7.1). In a similar way, the third term in (D.12) can be simplified as follows:

$$\begin{aligned}
&H(\mathbf{y}_{1b}^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N,W_1)\\
&= H(\mathbf{x}_{2b}^N,\mathbf{x}_{2c}^{(1)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{2a}^N) + H(\mathbf{y}_{1b}^{(2)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N,\mathbf{y}_{1b}^{(1)N},W_1). \qquad \text{(D.14)}
\end{aligned}$$

From (D.13) and (D.14), and dropping the last term in (D.14), (D.12) becomes

$$\begin{aligned}
&NR_1 \le H(\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + H(\mathbf{y}_{1b}^{(2)N}|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N,\mathbf{x}_{1a}^N,\mathbf{x}_{2a}^N,\mathbf{y}_{1b}^{(1)N}) + N\epsilon_1,\\
&\text{or } R_1 \le H(\mathbf{v}_{12},\mathbf{v}_{21}) + H(\mathbf{y}_{1b}^{(2)}) \le 2C + 2m - n. \qquad \text{(D.15)}
\end{aligned}$$

In the above equation, the term $H(\mathbf{v}_{12},\mathbf{v}_{21})$ is upper bounded by $2C$. From the definition of $\mathbf{y}_{1b}^{(2)}$, it can be seen that the term $H(\mathbf{y}_{1b}^{(2)})$ can be upper bounded by $2m-n$. This completes the proof.

D.4 Proof of Theorem 17

Using Fano's inequality, the rate of user-1 is upper bounded as

$$\begin{aligned} NR_1 &\leq I(W_1; \mathbf{y}_1^N) + N\epsilon_1 \overset{(a)}{=} I(W_1; \mathbf{y}_2^N) + N\epsilon_1, \\ \text{or } R_1 &\overset{(b)}{=} 0, \end{aligned} \tag{D.16}$$

where (a) is obtained using the fact that $\mathbf{y}_1 = \mathbf{y}_2$ and (b) is obtained using the perfect secrecy constraint at receiver 2. This completes the proof.

Appendix E

Appendix for Chapter 8

E.1 Analysis of the probability of error in the proof of Theorem 18

Define the following event

$$E_{ijk} = \left\{ \left(\mathbf{y}_1^N, \mathbf{x}_{p1}^N(i,j), \mathbf{u}_1^N(k) \right) \in T_\epsilon^N(P_{Y_1 X_{p1} U_1}) \right\}, \tag{E.1}$$

where $T_\epsilon^N(P_{Y_1 X_{p1} U_1})$ denotes the set of jointly typical sequences $\mathbf{y}_1, \mathbf{x}_{p1}$, and $\mathbf{u}_1$ with respect to $P(\mathbf{y}_1, \mathbf{x}_{p1}, \mathbf{u}_1)$. Without loss of generality, assume that transmitters 1 and 2 sends $\mathbf{x}_1^N(1,1,1,1)$ and $\mathbf{x}_2^N(1,1,1,1,1,1)$, respectively. An error occurs if the transmitted and received codewords are not jointly typical or a wrong codeword is jointly typical with the received codewords. By the union of events bounds

$$\lambda_e^{(N)} = P\left(E_{111}^c \bigcup \cup_{i\neq 1, j\neq 1, k\neq 1} E_{ijk} \right) \leq P(E_{111}^c) + P(\cup_{i\neq 1, j\neq 1, k\neq 1} E_{ijk}). \tag{E.2}$$

From the joint AEP [83], $P(E_{111}^c) \to 0$ as $N \to \infty$. When $i \neq 1, j \neq 1$, and $k = 1$, then

$$\begin{aligned}\lambda_{ij1} = \sum_{i\neq 1, j\neq 1} P(E_{ij1}) &\leq 2^{N\left[R_{p1}+R'_{p1}\right]} \sum_{(\mathbf{y}_1^N, \mathbf{x}_{p1}^N, \mathbf{u}_1^N)\in T_\epsilon^{(N)}} P(\mathbf{x}_{p1}^N) P(\mathbf{u}_1^N) P(\mathbf{y}_1^N|\mathbf{u}_1^N), \\ &\leq 2^{N\left[R_{p1}+R'_{p1}-I(\mathbf{x}_{p1};\mathbf{y}_1|\mathbf{u}_1)+4\epsilon\right]}. \end{aligned} \tag{E.3}$$

Hence, $\lambda_{ij1} \to 0$ as $N \to \infty$, if

$$R_{p1} + R'_{p1} \leq I(\mathbf{x}_{p1}; \mathbf{y}_1|\mathbf{u}_1). \tag{E.4}$$

When the above condition is satisfied, also, the probability of error λ_{1j1} and λ_{i11} also go to zero as $N \to \infty$. When $k \neq 1$ and $(i, j) = (1, 1)$

$$\begin{aligned}\lambda_{11k} = \sum_{k\neq 1} P(E_{11k}) &\leq 2^{NR_{cp1}} \sum_{(\mathbf{y}_1^N, \mathbf{x}_{p1}^N, \mathbf{u}_1^N)\in T_\epsilon^{(N)}} P(\mathbf{x}_{p1}^N) P(\mathbf{u}_1^N) P(\mathbf{y}_1^N|\mathbf{x}_{p1}^N), \\ &\leq 2^{N[R_{cp1}-I(\mathbf{u}_1;\mathbf{y}_1|\mathbf{x}_{p1})+4\epsilon]}. \end{aligned} \tag{E.5}$$

Hence, $\lambda_{11k} \to 0$ as $N \to \infty$, if

$$R_{cp1} \leq I(\mathbf{u}_1; \mathbf{y}_1|\mathbf{x}_{p1}). \tag{E.6}$$

Due to limited-rate transmitter cooperation, the following holds:

$$R_{\text{cp1}} \leq C_G. \tag{E.7}$$

From (E.6) and (E.7), the following constraint is obtained on the rate for the cooperative private message

$$R_{\text{cp1}} \leq \min\{I(\mathbf{u}_1; \mathbf{y}_1|\mathbf{x}_{p1}), C_G\}. \tag{E.8}$$

When $i \neq 1$, $j \neq 1$, and $k \neq 1$, then

$$\lambda_{ijk} = \sum_{i\neq 1, j\neq 1, k\neq 1} P(E_{ijk}) \leq 2^{N\left[R_{cp1}+R_{p1}+R'_{p1}\right]} \sum_{(\mathbf{y}_1^N, \mathbf{x}_{p1}^N, \mathbf{u}_1^N)\in T_\epsilon^{(N)}} P(\mathbf{x}_{p1}^N) P(\mathbf{u}_1^N) P(\mathbf{y}_1^N),$$
$$\leq 2^{N\left[R_{cp1}+R_{p1}+R'_{p1}-I(\mathbf{u}_1,\mathbf{x}_{p1};\mathbf{y}_1)+4\epsilon\right]}. \tag{E.9}$$

Hence, $\lambda_{ijk} \to 0$ as $N \to \infty$, if

$$R_{cp1} + R_{p1} + R'_{p1} \leq I(\mathbf{u}_1, \mathbf{x}_{p1}; \mathbf{y}_1). \tag{E.10}$$

The above condition also ensures that λ_{i1k} and λ_{1jk} go to zero as $N \to \infty$. Hence, $\lambda_e^{(n)}$ in (E.2) goes to 0 as $N \to \infty$, when the conditions in (E.4), (E.8) and (E.10) are satisfied.

Now, using the Fourier-Motzkin procedure [84], the achievable rate in Theorem 18 is obtained. The choice of R'_{p1} is discussed in the proof of Theorem 18.

The following lemma is useful in bounding the mutual information in the proof of Theorem 18.

E.2 Useful Lemma

Lemma 5.

$$I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) \leq N\left[I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2) + \epsilon_3\right], \tag{E.11}$$

where ϵ_3 is small for sufficiently large N.

Proof. Let $T_\epsilon^{(N)}(P_{X_{p1},X_{p2},X_{d2},U_2,Y_2})$ denote the set of typical sequences $(\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N)$

with respect to $P(x_{p1}, x_{p2}, x_{d2}, u_2, y_2)$. Define the following indicator random variable.

$$\psi(\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N) = \begin{cases} 1 & (\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N) \notin T_\epsilon^N \\ 0 & \text{otherwise.} \end{cases} \tag{E.12}$$

Now, $I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N)$ is bounded as follows:

$$\begin{aligned} I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) &\leq I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \psi; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N), \\ &= I(\psi; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) + I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N, \psi). \end{aligned} \tag{E.13}$$

Consider the first term in (E.13).

$$I(\psi; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) \leq H(\psi) \leq 1. \tag{E.14}$$

Consider the second term in (E.13).

$$I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N, \psi) = \sum_{j=0}^{1} P(\psi = j) I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N, \psi = j). \tag{E.15}$$

When $j = 1$, $(\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N) \notin T_\epsilon^{(N)}$, and the following bound is obtained:

$$\begin{aligned} P(\psi = 1) I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N, \psi = 1) &\leq P\left\{(\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N) \notin T_\epsilon^{(N)}\right\} H(\mathbf{y}_2^N), \\ &\leq N\epsilon_3 \log |\mathcal{Y}_2|. \end{aligned} \tag{E.16}$$

When $j=0$, $(\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N) \in T_\epsilon^{(N)}$, and the following bound is obtained.

$$
\begin{aligned}
&P(\psi=0) I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N, \psi=0) \\
&\leq I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N, \psi=0), \\
&\leq \sum_{(\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N) \in T_\epsilon^{(N)}} P(\mathbf{x}_{p1}^N, \mathbf{x}_{p2}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N, \mathbf{y}_2^N) \left[\log P(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) \right. \\
&\qquad \left. - \log P(\mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) - \log P(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) \right], \\
&\leq N \left[H(\mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2) + H(\mathbf{x}_{p1}, \mathbf{x}_{d2} | \mathbf{x}_{p2}, \mathbf{u}_2) - H(\mathbf{x}_{p1}, \mathbf{x}_{d2}, \mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2) + 3\epsilon_3 \right], \\
&= N \left[I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2) + 3\epsilon_2 \right]. \qquad \text{(E.17)}
\end{aligned}
$$

From (E.14)-(E.17), (E.13) is bounded as follows:

$$
I(\mathbf{x}_{p1}^N; \mathbf{y}_2^N | \mathbf{x}_{p2}^N, \mathbf{u}_2^N) \leq N I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{x}_{p2}, \mathbf{u}_2) + N\epsilon_3', \qquad \text{(E.18)}
$$

where $\epsilon_3' = \epsilon_3' \log |\mathcal{Y}_2| + 3\epsilon_2 + \frac{1}{N}$ and $|\mathcal{Y}_2|$ is the cardinality of the output alphabet $\mathcal{Y}_2$. This completes the proof. □

E.3 Proof of Theorem 19

In contrast to the achievable scheme for the weak/moderate interference regime, the dummy message sent by one of the users i is required to be decodable at the receiver j $(j \neq i)$. Intuitively, since the cross links are stronger than the direct links, stochastic encoding alone is not sufficient to ensure secrecy of the non-cooperative private message. Hence, the dummy message sent by transmitter i acts as a self-jamming signal, preventing receiver i from decoding the message from the other transmitter $j \neq i$. At the same time, ensuring that the dummy message is decodable at receiver j enables receiver j to

cancel the interference caused by the dummy message, allowing it to decode its own message. Thus, although the cross-links are strong, receiver i is unable to decode the message from transmitter j because of the jamming signal; and this helps user j achieve a better rate. In the next time slot, user i can achieve a better rate by exchanging the roles of users i and j. The proof involves analyzing the error probability at the decoder along with equivocation computation.

E.3.1 Analysis of the probability of error

Define the following event

$$E_{ijkl} = \left\{ \left(\mathbf{y}_1^N, \mathbf{x}_{p1}^N(i,j), \mathbf{u}_1^N(k), \mathbf{x}_{d2}^N(l) \right) \in T_\epsilon^N \right\}. \tag{E.19}$$

Without loss of generality, assume that transmitters 1 and 2 send $\mathbf{x}_1^N(1,1,1,1)$ and $\mathbf{x}_2^N(1,1,1,1)$, respectively. An error occurs if the transmitted and received codewords are not jointly typical or a wrong codeword is jointly typical with the received codewords. Then by the union of events bounds

$$\lambda_e^{(n)} = P\left(E_{1111}^c \bigcup \cup_{i\neq 1, j\neq 1, k\neq 1, l\neq 1} E_{ijkl} \right) \leq P(E_{1111}^c) + P(\cup_{i\neq 1, j\neq 1, k\neq 1, l\neq 1} E_{ijkl}). \tag{E.20}$$

From the joint AEP [83], $P(E_{1111}^c) \to 0$ as $N \to \infty$. When $i \neq 1$, $j \neq 1$, and $(k,l) = (1,1)$, then

$$\begin{aligned}
\lambda_{ij11} &= \sum_{i\neq 1, j\neq 1} P(E_{ij11}), \\
&\leq 2^{N\left[R_{p1} + R'_{p1}\right]} \sum_{(\mathbf{y}_1^N, \mathbf{x}_{p1}^N, \mathbf{u}_1^N, \mathbf{x}_{d2}^N) \in T_\epsilon^{(N)}} P(\mathbf{x}_{p1}^N) P(\mathbf{u}_1^N) P(\mathbf{x}_{d2}^N) P(\mathbf{y}_1^N | \mathbf{u}_1^N, \mathbf{x}_{d2}^N), \\
&\leq 2^{N\left[R_{p1} + R'_{p1} - I(\mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{u}_1, \mathbf{x}_{d2}) + 5\epsilon\right]}.
\end{aligned} \tag{E.21}$$

Hence, $\lambda_{ij11} \to 0$ as $N \to \infty$, if

$$R_{p1} + R'_{p1} \leq I(\mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{u}_1, \mathbf{x}_{d2}). \tag{E.22}$$

Thus, if the condition in (E.22) is satisfied, then the probabilities of error λ_{i111} and λ_{1j11} also go to zero. When $k \neq 1$ and $(i, j, l) = (1, 1, 1)$, then

$$\begin{aligned} \lambda_{11k1} &= \sum_{k \neq 1} P(E_{11k1}), \\ &\leq 2^{N[R_{cp1} - I(\mathbf{u}_1; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{x}_{d2}) + 5\epsilon]}. \end{aligned} \tag{E.23}$$

Hence, $\lambda_{11k1} \to 0$ as $N \to \infty$, if

$$R_{cp1} \leq I(\mathbf{u}_1; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{x}_{d2}). \tag{E.24}$$

Due to limited-rate transmitter cooperation, the following holds:

$$R_{\text{cp1}} \leq C_G. \tag{E.25}$$

From (E.24) and (E.25), the following constraint is obtained on the rate for the cooperative private message

$$R_{\text{cp1}} \leq \min\{I(\mathbf{u}_1; \mathbf{y}_1 | \mathbf{x}_{p1}), C_G\}. \tag{E.26}$$

When $l \neq 1$ and $(i, j, k) = (1, 1, 1)$, then

$$\begin{aligned} \lambda_{111l} &= \sum_{l \neq 1} P(E_{111l}), \\ &\leq 2^{N[R_{d2} - I(\mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{u}_1) + 5\epsilon]}. \end{aligned} \tag{E.27}$$

Thus, $\lambda_{111l} \to 0$ as $N \to \infty$, if

$$R_{d2} \leq I(\mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{x}_{p1}, \mathbf{u}_1). \tag{E.28}$$

When $i \neq 1, j \neq 1, k \neq 1$, and $l = 1$, then

$$\begin{aligned} \lambda_{ijk1} &= \sum_{i \neq 1, j \neq 1, k \neq 1} P(E_{ijk1}), \\ &\leq 2^{N\left[R_{cp1} + R_{p1} + R'_{p1} - I(\mathbf{u}_1, \mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{x}_{d2}) + 5\epsilon\right]}. \end{aligned} \tag{E.29}$$

Hence, $\lambda_{ijk1} \to 0$ as $N \to \infty$, if

$$R_{cp1} + R_{p1} + R'_{p1} \leq I(\mathbf{u}_1, \mathbf{x}_{p1}; \mathbf{y}_1 | \mathbf{x}_{d2}). \tag{E.30}$$

Thus, if the condition in (E.30) is satisfied, then the probabilities of error λ_{i1k1} and λ_{1jk1} also go to zero. When $k \neq 1, l \neq 1$, and $(i, j) = (1, 1)$, then

$$\begin{aligned} \lambda_{11kl} &= \sum_{k \neq 1, l \neq 1} P(E_{11kl}), \\ &\leq 2^{N[R_{cp1} + R_{d2} - I(\mathbf{u}_1, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{x}_{p1}) + 5\epsilon]}. \end{aligned} \tag{E.31}$$

Hence, $\lambda_{11kl} \to 0$ as $N \to \infty$, if

$$R_{cp1} + R_{d2} \leq I(\mathbf{u}_1, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{x}_{p1}). \tag{E.32}$$

When $i \neq 1, j \neq 1, l \neq 1$, and $k = 1$, then

$$\begin{aligned} \lambda_{ij1l} &= \sum_{i \neq 1, j \neq 1, l \neq 1} P(E_{ij1l}), \\ &\leq 2^{N\left[R_{p1} + R'_{p1} + R_{d2} - I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{u}_1) + 5\epsilon\right]}. \end{aligned} \tag{E.33}$$

Hence, $\lambda_{ij1l} \to 0$ as $N \to \infty$, if

$$R_{p1} + R'_{p1} + R_{d2} \leq I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1 | \mathbf{u}_1). \tag{E.34}$$

Thus, if the condition in (E.34) is satisfied, then the probabilities of error λ_{i11l} and λ_{1j1l} also go to zero. When $i \neq 1, j \neq 1, k \neq 1,$ and $l \neq 1$, then

$$\begin{aligned} \lambda_{1jkl} &= \sum_{i\neq 1, j\neq 1, k\neq 1, l\neq 1} P(E_{ijkl}), \\ &\leq 2^{N\left[R_{p1}+R'_{p1}+R_{cp1}+R_{d2}-I(\mathbf{u}_1,\mathbf{x}_{p1},\mathbf{x}_{d2};\mathbf{y}_1)+5\epsilon\right]}. \end{aligned} \tag{E.35}$$

Hence, $\lambda_{ijkl} \to 0$ as $N \to \infty$, if

$$R_{p1} + R'_{p1} + R_{cp1} + R_{d2} \leq I(\mathbf{u}_1, \mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_1). \tag{E.36}$$

If the condition in (E.36) is satisfied, then the probabilities of error λ_{i1kl} and λ_{1jkl} also go to zero.

In a similar way, it can be shown that the probability of decoding error at receiver 2 goes to zero if the following condition is satisfied.

$$R_{cp2} \leq \min\{I(\mathbf{u}_2; \mathbf{y}_2), C_G\}. \tag{E.37}$$

Thus, the probabilities of encoding and decoding error go to 0 as $N \to \infty$, if (E.22), (E.26), (E.28), (E.30), (E.32), (E.34), (E.36) and (E.37) are satisfied. Then, by applying Fourier-Motzkin procedure [84] to these equations and the conditions for encoding error, the achievable rate in Theorem 19 can be obtained.

E.3.2 Equivocation computation

The equivocation at receiver 2 is bounded as follows. As the non-intended cooperative private message is canceled completely at receiver 2, it suffices to show the following, as mentioned in the proof of Theorem 18.

$$H(W_{p1}|\mathbf{y}_2^N) \geq N\left[R_{p1} - \epsilon_s\right]. \tag{E.38}$$

Consider the following:

$$\begin{aligned}
H(W_{p1}|\mathbf{y}_2^N) &\geq H(W_{p1}|\mathbf{y}_2^N, \mathbf{u}_2^N), \\
&= H(W_{p1}, \mathbf{y}_2^N|\mathbf{u}_2^N) - H(\mathbf{y}_2^N|\mathbf{u}_2^N), \\
&\overset{(a)}{=} H(W_{p1}, \mathbf{y}_2^N, \mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{u}_2^N) - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|W_{p1}, \mathbf{y}_2^N, \mathbf{u}_2^N) - H(\mathbf{y}_2^N|\mathbf{u}_2^N), \\
&= H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{u}_2^N) + H(W_{p1}, \mathbf{y}_2^N|\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N) - H(\mathbf{y}_2^N|\mathbf{u}_2^N) \\
&\qquad - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|W_{p1}, \mathbf{y}_2^N, \mathbf{u}_2^N), \\
&\geq H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{u}_2^N) + H(\mathbf{y}_2^N|\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N, \mathbf{u}_2^N) - H(\mathbf{y}_2^N|\mathbf{u}_2^N) \\
&\quad - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|W_{p1}, \mathbf{y}_2^N, \mathbf{u}_2^N), \\
&= R_{p1} + R'_{p1} + R_{d2} - I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N|\mathbf{u}_2^N) - H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|W_{p1}, \mathbf{y}_2^N, \mathbf{u}_2^N),
\end{aligned} \tag{E.39}$$

where (a) is obtained using the relation: $H(W_{p1}, \mathbf{y}_2^N, \mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|\mathbf{u}_2^N) = H(W_{p1}, \mathbf{y}_2^N|\mathbf{u}_2^N) + H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N|W_{p1}, \mathbf{y}_2^N, \mathbf{u}_2^N)$. The second term in (E.39) is upper bounded as follows.

$$I(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N; \mathbf{y}_2^N|\mathbf{u}_2^N) \leq NI(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2|\mathbf{u}_2) + N\epsilon'. \tag{E.40}$$

The above bound can be obtained by using similar steps as used in the proof of Lemma 5 in Appendix E.2. To bound the last term in (E.39), consider the joint decoding of W'_{p1}

and W_{d2}, assuming that the receiver 2 is given W_{p1} and $\mathbf{u}_2^N$ as side information. By following similar steps as in the equivocation computation in the proof of Theorem 18, the probability of error can be made arbitrarily small for large N, provided the following conditions are satisfied:

$$\begin{aligned} &R'_{P1} \leq I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{x}_{d2}, \mathbf{u}_2), \;\; R_{d2} \leq I(\mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{x}_{p1}, \mathbf{u}_2), \\ &R'_{p1} + R_{d2} \leq I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{u}_2). \end{aligned} \tag{E.41}$$

When the conditions in (E.41) are satisfied and for sufficiently large N, the following bound is obtained using Fano's inequality:

$$H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N | W_{p1} = w_{p1}, \mathbf{y}_1^N, \mathbf{u}_2^N) \leq N\delta_2. \tag{E.42}$$

Finally, the last term in (E.39) is bounded as follows.

$$\begin{aligned} H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N | W_{p1}, \mathbf{y}_2^N, \mathbf{u}_2^N) &= \sum_{w_{p1}} P(w_{p1}) H(\mathbf{x}_{p1}^N, \mathbf{x}_{d2}^N | W_{p1} = w_{p1}, \mathbf{y}_1^N, \mathbf{u}_2^N), \\ &\leq N\delta_2. \end{aligned} \tag{E.43}$$

Using (E.40) and (E.43), (E.39) becomes

$$H(W_{p1} | \mathbf{y}_2^N) \geq N \left[R_{p1} + R'_{p1} + R_{d2} - I(\mathbf{x}_{p1}, \mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{u}_2) - (\delta_2 + \epsilon') \right], \tag{E.44}$$

By choosing $R'_{p1} = I(\mathbf{x}_{p1}; \mathbf{y}_2 | \mathbf{u}_2) - \epsilon'_2$ and $R_{d2} = I(\mathbf{x}_{d2}; \mathbf{y}_2 | \mathbf{x}_{p1}, \mathbf{u}_2) - \epsilon''_2$ secrecy of the non-cooperative private part is ensured. Thus,

$$H(W_{p1} | \mathbf{y}_2^N) \geq N \left[R_{p1} - \epsilon_2 \right]. \tag{E.45}$$

This completes the proof.

E.4 Proof of Corollary 3

In the first and second time slots, transmitters 1 and 2 send the following encoded messages.

$$\begin{aligned}
&\mathbf{x}_1(1) = \mathbf{x}_{cp1}(1) + \mathbf{x}_{p1}(1), \text{ and } \mathbf{x}_2(1) = \mathbf{x}_{cp2}(1) + \mathbf{x}_{d2}(1),\\
&\mathbf{x}_1(2) = \mathbf{x}_{cp1}(2) + \mathbf{x}_{d1}(2), \text{ and } \mathbf{x}_2(2) = \mathbf{x}_{cp2}(2) + \mathbf{x}_{p2}(2).
\end{aligned} \tag{E.46}$$

In the following, the achievable secrecy rate and power allocation for different messages are discussed in case of the first time slot. Hence, for simplicity, the time index is omitted here. The mutual information given in Theorem 19 is evaluated as follows. From Theorem 19, R'_{p1} and R_{d2} are set as $0.5\log\left(1+\frac{h_c^2P_{p1}}{1+h_d^2P_{d2}}\right)$ and $0.5\log(1+h_d^2P_{d2})$, respectively. The first four inequalities in (8.36) lead, respectively, to

$$R_1 \leq \min\left[0.5\log(1+\sigma_{u1}^2+h_d^2P_{p1}), 0.5\log(1+h_d^2P_{p1}) + \min\left\{0.5\log(1+\sigma_{u1}^2), C_G\right\}\right] - R'_{p1}, \tag{E.47}$$

$$\begin{aligned}
R_1 \leq \min\Big[&0.5\log(1+\sigma_{u1}^2+h_d^2P_{p1}+h_c^2P_{d2}), 0.5\log(1+\sigma_{u1}^2+h_c^2P_{d2})\\
&+\min\left\{0.5\log(1+\sigma_{u1}^2), C_G\right\}, 0.5\log(1+h_d^2P_{p1}) + 0.5\log(1+\sigma_{u1}^2+h_c^2P_{d2})\Big]\\
&-(R'_{p1}+R_{d2}),
\end{aligned} \tag{E.48}$$

$$R_1 \leq 0.5\log(1+h_d^2P_{p1}+h_c^2P_{d2}) + 0.5\log(1+\sigma_{u1}^2+h_c^2P_{d2}) - (R'_{p1}+2R_{d2}), \tag{E.49}$$

$$R_2 = \min\left\{0.5\log\left(1+\frac{\sigma_{u2}^2}{1+h_d^2P_{d2}+h_c^2P_{p1}}\right), C_G\right\}. \tag{E.50}$$

As $R_{d2} = 0.5\log(1 + h_d^2 P_{d2}) < 0.5\log(1 + h_c^2 P_{d2})$, R_{d2} satisfies the last inequality in (8.36). Now, consider the power allocation for the private cooperative message, non-cooperative private message and dummy message as shown below. The encoded messages at transmitters 1 and 2 are:

$$\mathbf{x}_1 = h_d \mathbf{w}_{1z} - h_c \mathbf{w}_{2z} + \mathbf{x}_{p1}, \text{ and } \mathbf{x}_2 = h_d \mathbf{w}_{2z} - h_c \mathbf{w}_{1z} + \mathbf{x}_{d2}. \tag{E.51}$$

To simplify the power allocation, the variance of $\mathbf{w}_{1z}$ and $\mathbf{w}_{2z}$ are chosen to be the same. In order to satisfy the power constraint, the following conditions need to be satisfied.

$$(h_d^2 + h_c^2)\sigma_z^2 + P_{p1} \leq P_1, \text{ and } (h_d^2 + h_c^2)\sigma_z^2 + P_{d2} \leq P_2, \tag{E.52}$$

where $P_i = \beta_i P$ $(i = 1, 2)$ and $0 \leq \beta_i \leq 1$. The power for the non-cooperative private message, cooperative private message and dummy message are chosen as follows:

$$\sigma_z^2 = \frac{\theta_1}{\theta_1 + \theta_2} \frac{P_1}{h_d^2 + h_c^2}, P_{p1} = \frac{\theta_2}{\theta_1 + \theta_2} P_1, \text{ and } P_{d2} = (P_2 - (h_d^2 + h_c^2)\sigma_z^2)^+. \tag{E.53}$$

where $\theta_i \in [0, 1]$. The parameters θ_i and β_i are the power splitting and power control parameter, respectively. Hence, θ_i and β_i are chosen such that the rates in (E.47)-(E.50) are maximized and the minimum of (E.47)-(E.49) gives the achievable secrecy rate for the transmitter 1 i.e., $R_1^*(1)$ and (E.50) gives the achievable secrecy rate for the transmitter 2. i.e., $R_2^*(1)$. In a similar way, the achievable secrecy rate $R_1^*(2)$ and $R_1^*(2)$ can be determined in the second time slot. This completes the proof.

Appendix F

Appendix for Chapter 9

F.1 Proof of Theorem 20

Using Fano's inequality, the rate of user 1 is upper bounded as

$$\begin{aligned} NR_1 &\leq I(W_1; \mathbf{y}_1^N) + N\epsilon_N, \\ &\overset{(a)}{\leq} h(\mathbf{y}_1^N) - h(\mathbf{y}_1^N | W_1, \mathbf{x}_1^N) + N\epsilon_N, \\ &\overset{(b)}{\leq} h(\mathbf{y}_1^N) - h(h_c\mathbf{x}_2^N + \mathbf{z}_1^N | \mathbf{v}_{12}^N, \mathbf{v}_{21}^N, W_1, \mathbf{x}_1^N) + N\epsilon_N, \\ &\overset{(c)}{=} h(\mathbf{y}_1^N) - h(h_c\mathbf{x}_2^N + \mathbf{z}_1^N | \mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + N\epsilon_N, \\ &\overset{(d)}{=} h(\mathbf{y}_1^N) - h(h_c\mathbf{x}_2^N + \widetilde{\mathbf{z}}_1^N | \mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + N\epsilon_N, \\ \text{or } h(\widetilde{\mathbf{s}}_2^N | \mathbf{v}_{12}^N, \mathbf{v}_{21}^N) &\leq h(\mathbf{y}_1^N) - NR_1 + N\epsilon_N, \text{ where } \widetilde{\mathbf{s}}_2^N \triangleq h_c\mathbf{x}_2^N + \widetilde{\mathbf{z}}_1^N, \end{aligned} \tag{F.1}$$

where (a) and (b) follow by using the fact that the entropy cannot increase by additional conditioning; (c) follows by using the relation in (7.1), and (d) is obtained using the fact that the secrecy capacity region of an interference channel with confidential messages is invariant under any joint channel noise distribution $P(z1, z2)$ that leads to the same marginal distributions $P(z_1)$ and $P(z_2)$ [5]. Although this invariance property is stated

for GIC in [5], it is not difficult to see that this property holds for the GIC with limited-rate transmitter cooperation also.

Adopting similar steps as was used to obtain (F.1), the following bound on the conditional entropy is obtained.

$$h(\widetilde{\mathbf{s}}_1^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) \leq h(\mathbf{y}_2^N) - NR_2 + N\epsilon_N, \text{ where } \widetilde{\mathbf{s}}_1^N \triangleq h_c\mathbf{x}_1^N + \widetilde{\mathbf{z}}_2^N, \tag{F.2}$$

The rate of user 1 can also be bounded as

$$\begin{aligned}
NR_1 &\leq I(W_1;\mathbf{y}_1^N) + N\epsilon, \\
&\overset{(a)}{\leq} I(W_1;\mathbf{y}_1^N) - I(W_1;\mathbf{y}_2^N) + N\epsilon', \\
&\overset{(b)}{\leq} I(W_1;\mathbf{y}_1^N,\mathbf{y}_2^N) - I(W_1;\mathbf{y}_2^N) + N\epsilon', \\
&= I(W_1;\mathbf{y}_1^N|\mathbf{y}_2^N) + N\epsilon', \\
&= h(\mathbf{y}_1^N|\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon', \\
&= h(\mathbf{y}_1^N,\mathbf{y}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon', \\
&\overset{(c)}{=} h(\mathbf{y}_1^N,\mathbf{y}_2^N,\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N) - h(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N|\mathbf{y}_1^N,\mathbf{y}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon', \\
&= h(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N) + h(\mathbf{y}_1^N,\mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N) - h(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N|\mathbf{y}_1^N,\mathbf{y}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon', \\
&= I(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N;\mathbf{y}_1^N,\mathbf{y}_2^N) + h(\mathbf{y}_1^N,\mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon', \\
&\overset{(d)}{\leq} I(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N;\mathbf{y}_1^N,\mathbf{y}_2^N,\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + h(\mathbf{y}_1^N,\mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon', \\
&\leq H(\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + I(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N;\mathbf{y}_1^N,\mathbf{y}_2^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) + h(\mathbf{y}_1^N,\mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N) \\
&\qquad - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon', \\
&\leq H(\mathbf{v}_{12}^N) + H(\mathbf{v}_{21}^N) + h(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N|\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) - h(\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N|\mathbf{y}_1^N,\mathbf{y}_2^N,\mathbf{v}_{12}^N,\mathbf{v}_{21}^N) \\
&\qquad + h(\mathbf{y}_1^N,\mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N,\widetilde{\mathbf{s}}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N,W_1) + N\epsilon',
\end{aligned}$$

$$\begin{aligned}
&\overset{(e)}{\leq} H(\mathbf{v}_{12}^N) + H(\mathbf{v}_{21}^N) + h(\widetilde{\mathbf{s}}_1^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + h(\widetilde{\mathbf{s}}_2^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) - h(\widetilde{\mathbf{s}}_1^N, \widetilde{\mathbf{s}}_2^N|\mathbf{y}_1^N, \mathbf{y}_2^N, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N, \mathbf{x}_1^N, \mathbf{x}_2^N) \\
&\qquad + h(\mathbf{y}_1^N, \mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N, \widetilde{\mathbf{s}}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{y}_1^N|\mathbf{y}_2^N, W_1, \mathbf{x}_1^N, \mathbf{x}_2^N) + N\epsilon', \\
&= H(\mathbf{v}_{12}^N) + H(\mathbf{v}_{21}^N) + h(\widetilde{\mathbf{s}}_1^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + h(\widetilde{\mathbf{s}}_2^N|\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) - h(\widetilde{\mathbf{z}}_1^N, \widetilde{\mathbf{z}}_2^N) \\
&\qquad + h(\mathbf{y}_1^N, \mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N, \widetilde{\mathbf{s}}_2^N) - h(\mathbf{y}_2^N) - h(\mathbf{z}_1^N) + N\epsilon', \qquad \text{(F.3)}
\end{aligned}$$

where (a) is obtained using the secrecy constraint at receiver 2; (b) is due to the genie providing $\mathbf{y}_2^N$ to receiver 1; (c) is obtained using the relation $h(\mathbf{y}_1^N, \mathbf{y}_2^N, \widetilde{\mathbf{s}}_1^N, \widetilde{\mathbf{s}}_2^N) = h(\mathbf{y}_1^N, \mathbf{y}_2^N) + h(\widetilde{\mathbf{s}}_1^N, \widetilde{\mathbf{s}}_2^N|\mathbf{y}_1^N, \mathbf{y}_2^N)$; (d) is obtained using chain rule for mutual information, and (e) is obtained using the fact that removing conditioning cannot decrease the entropy and conditioning cannot increase the entropy. Using (F.1) and (F.2), (F.3) becomes

$$\begin{aligned}
N[2R_1 + R_2] \leq\ & H(\mathbf{v}_{12}^N) + H(\mathbf{v}_{21}^N) + h(\mathbf{y}_1^N) + h(\mathbf{y}_1^N, \mathbf{y}_2^N|\widetilde{\mathbf{s}}_1^N, \widetilde{\mathbf{s}}_2^N) \\
& - h(\widetilde{\mathbf{z}}_1^N) - h(\widetilde{\mathbf{z}}_2^N) - h(\mathbf{z}_1^N) + N\epsilon'',
\end{aligned}$$

$$\text{or } R \leq \max_{0\leq|\rho|\leq 1} \frac{1}{3}\left[2C_G + 0.5\log\left(1 + \text{SNR} + \text{INR} + 2\rho\sqrt{\text{SNR INR}}\right) + 0.5\log\det\left(\Sigma_{\bar{\mathbf{y}}|\bar{\mathbf{s}}}\right)\right]. \qquad \text{(F.4)}$$

In the above equation, ρ, det(.) and $\Sigma_{\bar{\mathbf{y}}|\bar{\mathbf{s}}}$ are as defined in the statement of the theorem. The second term in (F.4) is obtained using the fact that differential entropy is maximized by the Gaussian distribution for a given power constraint. Hence, the following holds.

$$h(\mathbf{y}_1) \leq 0.5\log\left(2\pi e\left(1 + \text{SNR} + \text{INR} + 2\rho\sqrt{\text{SNR INR}}\right)\right), \qquad \text{(F.5)}$$

where SNR and INR are as defined in the statement of the theorem. The last term in

(F.4) is obtained as follows.

$$h(\mathbf{y}_1, \mathbf{y}_2|\widetilde{\mathbf{s}}_1, \widetilde{\mathbf{s}}_2) \leq 0.5 \log \det \left(2\pi e \Sigma_{\bar{\mathbf{y}}|\bar{\mathbf{s}}}\right), \tag{F.6}$$

where $\Sigma_{\bar{\mathbf{y}}|\bar{\mathbf{s}}} = \Sigma_{\bar{\mathbf{y}}} - \Sigma_{\bar{\mathbf{y}},\bar{\mathbf{s}}}\Sigma_{\bar{\mathbf{s}}}^{-1}\Sigma_{\bar{\mathbf{y}},\bar{\mathbf{s}}}^T$, $\Sigma_{\bar{\mathbf{y}}} = E[\bar{\mathbf{y}}\bar{\mathbf{y}}^T]$, $\Sigma_{\bar{\mathbf{y}},\bar{\mathbf{s}}} = E[\bar{\mathbf{y}}\bar{\mathbf{s}}^T]$, $\Sigma_{\bar{\mathbf{s}}} = E[\bar{\mathbf{s}}\bar{\mathbf{s}}^T]$, $\bar{\mathbf{y}} \triangleq [\mathbf{y}_1 \ \mathbf{y}_2]^T$, and $\bar{\mathbf{s}} \triangleq [\widetilde{\mathbf{s}}_1 \widetilde{\mathbf{s}}_2]^T$. The evaluation of these terms are given in the statement of the theorem. This completes the proof.

F.2 Proof of Theorem 21

Using Fano's inequality, the rate of user 1 is upper bounded as

$$\begin{aligned}
NR_1 &\leq I(W_1; \mathbf{y}_1^N) + N\epsilon_N, \\
&\overset{(a)}{\leq} I(W_1; \mathbf{y}_1^N, \mathbf{x}_2^N) + N\epsilon_N, \\
&= I(W_1; \mathbf{x}_2^N) + I(W_1; \mathbf{y}_1^N|\mathbf{x}_2^N) + N\epsilon_N, \\
&= I(W_1; \mathbf{x}_2^N) + h(\mathbf{s}'^N_1|\mathbf{x}_2^N) - h(\mathbf{s}'^N_1|\mathbf{x}_2^N, W_1) + N\epsilon_N, \text{ where } \mathbf{s}'^N_1 \triangleq h_d\mathbf{x}_1^N + \mathbf{z}_1^N, \\
&= I(W_1; \mathbf{x}_2^N) + I(W_1; \mathbf{s}'^N_1|\mathbf{x}_2^N) + N\epsilon_N, \\
&\overset{(b)}{=} I(W_1; \mathbf{x}_2^N, \mathbf{s}'^N_1) + N\epsilon_N, \\
&\overset{(c)}{\leq} I(W_1; \mathbf{s}'^N_1) - I(W_1; \mathbf{y}_2^N) + I(W_1; \mathbf{x}_2^N|\mathbf{s}'^N_1) + N\epsilon'_N, \\
&\overset{(d)}{\leq} I(W_1; \mathbf{s}'^N_1, \mathbf{y}_2^N) - I(W_1; \mathbf{y}_2^N) + I(W_1; \mathbf{x}_2^N|\mathbf{s}'^N_1) + N\epsilon'_N, \\
&= I(W_1; \mathbf{s}'^N_1|\mathbf{y}_2^N) + I(W_1; \mathbf{x}_2^N|\mathbf{s}'^N_1) + N\epsilon'_N, \\
&\overset{(e)}{\leq} I(W_1; \mathbf{s}'^N_1|\mathbf{y}_2^N) + I(W_1; \mathbf{x}_2^N, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{s}'^N_1) + N\epsilon'_N, \\
&= I(W_1; \mathbf{s}'^N_1|\mathbf{y}_2^N) + I(W_1; \mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{s}'^N_1) + I(W_1; \mathbf{x}_2^N|\mathbf{s}'^N_1, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + N\epsilon'_N,
\end{aligned}$$

$$\leq I(W_1; \mathbf{s'}_1^N|\mathbf{y}_2^N) + H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{s'}_1^N) + h(\mathbf{x}_2^N|\mathbf{s'}_1^N, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N)$$

$$- h(\mathbf{x}_2^N|\mathbf{s'}_1^N, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N, W_1) + N\epsilon'_N,$$

$$\overset{(f)}{\leq} h(\mathbf{s'}_1^N|\mathbf{y}_2^N) - h(\mathbf{s'}_1^N|\mathbf{y}_2^N, W_1) + H(\mathbf{v}_{12}^N, \mathbf{v}_{21}^N) + N\epsilon'_N,$$

$$\text{or } R_1 \leq \max_{0\leq|\rho|\leq 1} \left[2C_G + 0.5 \log \Sigma_{\mathbf{s'}|\mathbf{y}_2}\right], \tag{F.7}$$

where (a) is due to the genie providing $\mathbf{x}_2^N$ to receiver 1; (b) is obtained using chain rule for mutual information; (c) is obtained using secrecy constraint at receiver 2; (d) is due to the genie providing $\mathbf{y}_2^N$ as side information to receiver 1, where $\mathbf{x}_2^N$ is eliminated, (e) is obtained using the relation $I(W_1; \mathbf{x}_2^N, \mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{s'}_1^N) = I(W_1; \mathbf{x}_2^N|\mathbf{s'}_1^N) + I(W_1; \mathbf{v}_{12}^N, \mathbf{v}_{21}^N|\mathbf{s'}_1^N, \mathbf{x}_2^N)$ and (f) is obtained using the relation in (7.1) and the fact that removing conditioning does not decrease the entropy. The last inequality is obtained using the fact that the differential entropy is maximized by the Gaussian distribution for a given power constraint. The term $\Sigma_{\mathbf{s'}|\mathbf{y}_2}$ is evaluated as follows.

$$\Sigma_{\mathbf{s'}|\mathbf{y}_2} = E[\mathbf{s'}_1^2] - E[\mathbf{s'}\mathbf{y}_2]^2 E[\mathbf{y}_2^2]^{-1} = 1 + \frac{\text{SNR} + \text{SNR}^2(1-\rho^2)}{1 + \text{SNR} + \text{INR} + 2\rho\sqrt{\text{SNR}\,\text{INR}}}. \tag{F.8}$$

This completes the proof.

F.3 Proof of Theorem 22

Using Fano's inequality, the rate of user 1 is upper bounded as

$$NR_1 \leq I(W_1; \mathbf{y}_1^N) + N\epsilon_N,$$

$$\begin{aligned}
&\overset{(a)}{\leq} I(W_1;\mathbf{y}_1^N) - I(W_1;\mathbf{y}_2^N) + N\epsilon'_N,\\
&\leq I(W_1;\mathbf{y}_1^N,\mathbf{y}_2^N) - I(W_1;\mathbf{y}_2^N) + N\epsilon'_N,\\
&\leq h(\mathbf{y}_1^N|\mathbf{y}_2^N) - h(\mathbf{z}_1^N) + N\epsilon'_N,\\
\text{or } R_1 &\leq \max_{0\leq|\rho|\leq 1} 0.5\log\Sigma_{\mathbf{y}_1|\mathbf{y}_2},
\end{aligned} \tag{F.9}$$

where (a) is obtained using the secrecy constraint at receiver 2 and $\Sigma_{\mathbf{y}_1|\mathbf{y}_2}$ is evaluated as follows:

$$\begin{aligned}
\Sigma_{\mathbf{y}_1|\mathbf{y}_2} &= E[\mathbf{y}_1^2] - E[\mathbf{y}_1\mathbf{y}_2]^2 E[\mathbf{y}_2^2]^{-1},\\
&= 1 + \text{SNR} + \text{INR} + 2\rho\sqrt{\text{SNR INR}} - \frac{(2\sqrt{\text{SNR INR}} + \rho(\text{SNR}+\text{INR}))^2}{1+\text{SNR}+\text{INR}+2\rho\sqrt{\text{SNR INR}}}.
\end{aligned} \tag{F.10}$$

Substituting the value of $\Sigma_{\mathbf{y}_1|\mathbf{y}_2}$ from (F.10) in (F.9) results in (9.3), and this completes the proof.

Bibliography

[1] S. Jafar and S. Vishwanath, "Generalized degrees of freedom of the symmetric Gaussian K user interference channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3297–3303, Jul. 2010.

[2] T. Gou and S. Jafar, "Sum capacity of a class of symmetric SIMO Gaussian Interference Channels within $O(1)$," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1932–1958, Apr. 2011.

[3] P. Parker, D. Bliss, and V. Tarokh, "On the degrees-of-freedom of the MIMO interference channel," in *Proc. Conf. on Information Sciences and Systems*, Mar. 2008, pp. 62–67.

[4] R. Liu and H. Poor, "Secrecy capacity region of a multiple-antenna gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, March 2009.

[5] X. He and A. Yener, "A new outer bound for the gaussian interference channel with confidential messages," in *Proc. Conf. on Information Sciences and Systems*, 2009, pp. 318–323.

[6] X. Tang, R. Liu, P. Spasojević, and H. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[7] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

[8] R. Etkin, D. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5534–5562, Dec. 2008.

[9] V. Cadambe and S. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[10] M. Maddah-Ali, A. Motahari, and A. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3457–3470, Aug. 2008.

[11] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[12] R. Liu, I. Maric, P. Spasojević, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[13] C. E. Shannon, "Two-Way Communication Channels," in *4th Berkeley Symp. on Mathematical Statistics and Probability*, vol. 1. Univ. California Press, 1961, pp. 611–644.

[14] T. Gou and S. Jafar, "Degrees of freedom of the K user $M \times N$ MIMO interference channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6040–6057, Dec. 2010.

[15] A. Carleial, "A case where interference does not reduce capacity," *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 569–570, Sep. 1975.

[16] H. Sato, "The capacity of the gaussian interference channel under strong interference (corresp.)," *IEEE Trans. Inf. Theory*, vol. 27, no. 6, pp. 786–788, 1981.

[17] S. Jafar and M. Fakhereddin, "Degrees of freedom for the MIMO interference channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2637–2642, Jul. 2007.

[18] A. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: A deterministic approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.

[19] G. Bresler and D. Tse, "The two-user gaussian interference channel: a deterministic view." *European Transactions on Telecommunications*, vol. 19, no. 4, pp. 333–354, 2008.

[20] I. Wang and D. Tse, "Interference mitigation through limited transmitter cooperation," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2941–2965, May 2011.

[21] R. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 374–378.

[22] E. Perron, S. Diggavi, and E. Telatar, "On cooperative wireless network secrecy," in *Proc. IEEE INFOCOM' 2009*, Apr. 2009, pp. 1935–1943.

[23] M. El-Halabi, T. Liu, C. Georghiades, and S. Shamai, "Secret writing on dirty paper: A deterministic view," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3419–3429, Jun. 2012.

[24] M. Maddah-Ali, A. Motahari, and A. Khandani, "Signaling over MIMO multi-base systems: Combination of multi-access and broadcast schemes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2104–2108.

[25] A. Ghasemi, A. Motahari, and A. Khandani, "Interference alignment for the K user MIMO interference channel," *CoRR*, vol. abs/0909.4604, Sep. 2009. [Online]. Available: http://arxiv.org/abs/0909.4604

[26] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of wireless X networks," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3893–3908, Sep. 2009.

[27] V. Cadambe, S. Jafar, and C. Wang, "Interference alignment with asymmetric complex signaling−settling the Høst-Madsen–Nosratinia conjecture," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4552–4565, Sep. 2010.

[28] S. H. Chae and S.-Y. Chung, "Blind interference alignment for a class of K-user line-of-sight interference channels," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1177–1181, 2012.

[29] K. Gomadam, V. Cadambe, and S. Jafar, "Approaching the capacity of wireless networks through distributed interference alignment," in *Proc. IEEE Global Telecomm. Conference*, Nov 2008, pp. 1–6.

[30] S. Peters and R. Heath, "Interference alignment via alternating minimization," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, April 2009, pp. 2445–2448.

[31] H. Yu, J. Park, Y. Sung, and Y. H. Lee, "A least squares approach to joint beam design for interference alignment in multiuser interference channels," in *Proc. IEEE Workshop on Signal Processing Advances in Wireless Comm.*, 2009, pp. 593–597.

[32] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1334–1387, Oct. 1975.

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

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

[35] E. Ekrem and S. Ulukus, "The secrecy capacity region of the gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.

[36] O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[37] O. Koyluoglu, H. El Gamal, L. Lai, and H. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[38] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[39] A. Vaneet, S. Lalitha, and C. A Robert, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, 2009.

[40] E. Perron, S. Diggavi, and I. Telatar, "On cooperative secrecy for discrete memoryless relay networks," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2010, pp. 2573–2577.

[41] R. Ash, *Information Theory*, ser. Dover Books on Mathematics Series. Dover Publications, 1990.

[42] S. Karmakar and M. Varanasi, "The generalized degrees of freedom region of the MIMO interference channel and its achievability," *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7188–7203, 2012.

[43] X. He and A. Yener, "The gaussian many-to-one interference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2730–2745, May 2011.

[44] I.-H. Wang and D. Tse, "Interference mitigation through limited receiver cooperation," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2913–2940, May 2011.

[45] E. Telatar and D. Tse, "Bounds on the capacity region of a class of interference channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2871 –2874.

[46] S. Karmakar and M. K. Varanasi, "The generalized degrees of freedom of the MIMO interference channel," *CoRR*, vol. abs/1103.1672, Mar. 2011.

[47] S. Jafar and S. Shamai, "Degrees of freedom region of the MIMO X channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 151–170, Jan. 2008.

[48] V. Cadambe, S. Jafar, and S. Shamai, "Interference alignment on the deterministic channel and application to fully connected AWGN interference networks," in *Information Theory Workshop*, 2008, pp. 41–45.

[49] K. Lee, N. Lee, and I. Lee, "Achievable degrees of freedom on K-user Y channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1210–1219, 2012.

[50] C. Huang, V. R. Cadambe, and S. A. Jafar, "On the capacity and generalized degrees of freedom of the X channel," *CoRR*, vol. abs/0810.4741, Oct. 2008.

[51] A. Carleial, "Outer bounds on the capacity of interference channels (corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, no. 4, pp. 602–606, Jul. 1983.

[52] H. Sato, "Two-user communication channels," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 295–304, May 1977.

[53] G. Kramer, "Outer bounds on the capacity of Gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 581–586, Mar. 2004.

[54] S. Karmakar and M. K. Varanasi, "Capacity of the MIMO interference channel to within a constant gap," *CoRR*, vol. abs/1102.0267, 2011.

[55] J. Bae, J. Lee, and I. Kang, "The GDOF of 3-user MIMO gaussian interference channel," *Arxiv preprint arXiv:1207.5010*, 2012.

[56] C. Wang, T. Gou, and S. A. Jafar, "Subspace alignment chains and the degrees of freedom of the three-user MIMO interference channel," *CoRR*, vol. abs/1109.4350, 2011.

[57] L. Ke and Z. Wang, "Degrees of freedom regions of two-user MIMO Z and full interference channels: The benefit of reconfigurable antennas," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3766 –3779, June 2012.

[58] M. A. Maddah-Ali, *Communication over X channel: Signalling and multiplexing gain*. Tech Rep., 2006.

[59] V. Cadambe and S. Jafar, "Multiple access outerbounds and the inseparability of parallel interference channels," in *Proc. IEEE Global Telecomm. Conference*, Nov 2008, pp. 1–5.

[60] C. Suh and D. Tse, "Interference alignment for cellular networks," in *Proc. Allerton Conf. on Comm., Control, and Computing*, Sept 2008, pp. 1037–1044.

[61] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wireless networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Sept 2005, pp. 2065–2069.

[62] C. Yetis, T. Gou, S. Jafar, and A. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4771–4782, Sept 2010.

[63] F. Negro, S. Shenoy, I. Ghauri, and D. T. M. Slock, "Interference alignment feasibility in constant coefficient MIMO interference channels," in *Proc. IEEE Workshop on Signal Processing Advances in Wireless Comm.*, June 2010, pp. 1–5.

[64] H. Bolcskei and I. Thukral, "Interference alignment with limited feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2009, pp. 1759–1763.

[65] R. Tresch and M. Guillaud, "Cellular interference alignment with imperfect channel knowledge," in *Proc. IEEE Int. Conf. on Communications*, June 2009, pp. 1–5.

[66] R. Tresch, M. Guillaud, and E. Riegler, "On the achievability of interference alignment in the K-user constant MIMO interference channel," in *Proc. IEEE Workshop on Statistical Signal Processing*, Aug 2009, pp. 277–280.

[67] S. Gollakota, S. D. Perli, and D. Katabi, "Interference alignment and cancellation," *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 4, pp. 159–170, Aug. 2009.

[68] A. S. Motahari, S. O. Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real interference alignment," *CoRR*, vol. abs/1001.3403, 2010.

[69] H. Yu and Y. Sung, "Iterative algorithm for interference alignment in multiuser MIMO interference channels," in *Proc. IEEE Workshop on Signal Processing Advances in Wireless Comm.*, June 2010, pp. 1–5.

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

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

[72] F. M. J. Willems, "The discrete memoryless multiple access channel with partially cooperating encoders (corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 441–445, 1983.

[73] E. Ekrem and S. Ulukus, "Effects of cooperation on the secrecy of multiple access

channels with generalized feedback," in *Proc. Conf. on Information Sciences and Systems*, Mar. 2008, pp. 791–796.

[74] ——, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[75] Z. H. Awan, A. Zaidi, and L. Vandendorpe, "Multiaccess channel with partially cooperating encoders and security constraints," *CoRR*, vol. abs/1205.6852, 2012.

[76] E. Tekin, "The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming," in *Information Theory and Applications Workshop, 2007*, Jan 2007, pp. 404–413.

[77] G. Kramer, "Topics in multi-user information theory," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 45, pp. 265–444, 2008.

[78] C. Vaze, S. Karmakar, and M. Varanasi, "On the generalized degrees of freedom region of the MIMO interference channel with no CSIT," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2011, pp. 757–761.

[79] C. Vaze and M. Varanasi, "The degrees of freedom region and interference alignment for the MIMO interference channel with delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4396–4417, July 2012.

[80] X. Shang, B. Chen, G. Kramer, and H. Poor, "Capacity regions and sum-rate capacities of vector gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 5030–5044, Oct. 2010.

[81] G. Seber, *A matrix handbook for statisticians*. Wiley-Interscience, 2008.

[82] S. Karmakar and M. Varanasi, "The capacity region of the MIMO interference channel and its reciprocity to within a constant gap," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4781–4797, 2013.

[83] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[84] A. El Gamal and Y.-H. Kim, *Network information theory*. Cambridge University Press, 2011.