ABSTRACT

Title of dissertation: SECURE DEGREES OF FREEDOM OF WIRELESS NETWORKS

Jianwei Xie, Doctor of Philosophy, 2014

Dissertation directed by: Professor Şennur Ulukuş
Department of Electrical and Computer Engineering

This dissertation studies the security of wireless interference networks from an information-theoretic point of view. In this setting, several transmitter-receiver pairs wish to have secure communication against the eavesdropper(s). The central goal of this dissertation is to develop a framework based on information-theoretic principles to determine the complete solutions for the signaling schemes in different wireless interference networks with large transmit powers, and derive the corresponding fundamental limits in terms of the secure degrees of freedom (s.d.o.f.).

First, we study one-hop wireless networks by considering four fundamental wireless network structures: Gaussian wiretap channel with helpers, Gaussian broadcast channel (BC) with confidential messages, Gaussian interference channel (IC) with confidential messages, and Gaussian multiple access (MAC) wiretap channel. The secrecy capacity of the canonical Gaussian wiretap channel does not scale with the transmit power, and hence, the s.d.o.f. of the Gaussian wiretap channel with no helpers is zero. We show that the exact s.d.o.f. of the Gaussian wiretap channel with a helper is $\frac{1}{2}$. Our achievable scheme is based on real interference alignment

and cooperative jamming, which renders the message signal and the cooperative jamming signal *separable* at the legitimate receiver, but *aligns* them perfectly at the eavesdropper preventing any reliable decoding of the message signal. Our converse is based on two key lemmas. The first lemma quantifies the *secrecy penalty* by showing that the net effect of an eavesdropper on the system is that it eliminates one of the independent channel inputs. The second lemma quantifies the *role of a helper* by developing a direct relationship between the cooperative jamming signal of a helper and the message rate. We extend this result to the case of M helpers, and show that the exact s.d.o.f. in this case is $\frac{M}{M+1}$. We then generalize this approach to more general network structures with *multiple messages*. We show that the sum s.d.o.f. of the Gaussian BC with confidential messages and M helpers is 1, the sum s.d.o.f. of the two-user IC with confidential messages is $\frac{2}{3}$, the sum s.d.o.f. of the two-user IC with confidential messages and M helpers is 1, and the sum s.d.o.f. of the K-user MAC wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$.

Next, we study the sum s.d.o.f. of multi-receiver networks. In this dissertation, we determine the exact sum s.d.o.f. of the K-user Gaussian IC. We consider three different secrecy constraints: 1) K-user IC with one external eavesdropper (IC-EE), 2) K-user IC with confidential messages (IC-CM), and 3) K-user IC with confidential messages and one external eavesdropper (IC-CM-EE). We show that for all of these three cases, the exact sum secure d.o.f. is $\frac{K(K-1)}{2K-1}$. We show converses for IC-EE and IC-CM, which imply a converse for IC-CM-EE. We show achievability for IC-CM-EE, which implies achievability for IC-EE and IC-CM. We develop the converses by relating the channel inputs of interfering users to the reliable rates of the interfered

users, and by quantifying the secrecy penalty in terms of the eavesdroppers' observations. Our achievability uses structured signaling, structured cooperative jamming, channel prefixing, and asymptotic real interference alignment. While the traditional interference alignment provides some amount of secrecy by mixing unintended signals in a smaller sub-space at every receiver, in order to attain the optimum sum s.d.o.f., we incorporate structured cooperative jamming into the achievable scheme, and intricately design the structure of all of the transmitted signals jointly.

Then, we study the *entire s.d.o.f. regions* of multi-user network structures. In this dissertation, we determine the *entire s.d.o.f. regions* of the K-user MAC wiretap channel and the K-user IC with secrecy constraints. The converse for the MAC follows from a middle step in the converse of the sum s.d.o.f. The converse for the IC includes constraints both due to secrecy as well as due to interference. Although the portion of the region close to the optimum sum s.d.o.f. point is governed by the upper bounds due to secrecy constraints, the other portions of the region are governed by the upper bounds due to interference constraints. Different from the existing literature, in order to fully understand the characterization of the s.d.o.f. region of the IC, one has to study the 4-user case, i.e., the 2 or 3-user cases do not illustrate the generality of the problem. In order to prove the achievability, we use the polytope structure of the converse region. In both MAC and IC cases, we develop explicit schemes that achieve the extreme points of the polytope region given by the converse. Specifically, the extreme points of the MAC region are achieved by an m-user MAC wiretap channel with $K-m$ helpers, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers. The extreme points

of the IC region are achieved by a $(K-m)$-user IC with confidential messages, m helpers, and N external eavesdroppers, for $m \geq 1$ and a finite N. As a byproduct of determining the entire s.d.o.f. regions of MAC and IC channels, we show that the sum s.d.o.f. is achieved *only at one extreme point* of the s.d.o.f. region, which is the symmetric-rate extreme point, for both MAC and IC channel models.

Next, we determine the sum s.d.o.f. of two-unicast layered wireless networks. Without any secrecy constraints, the sum d.o.f. of this class of networks was shown to take only one of three possible values: $1, \frac{3}{2}$ and 2, for all network configurations. We consider the setting where, in addition to being reliably transmitted, each message is required to be kept information-theoretically secure from the unintended receiver. We show that the sum s.d.o.f. can only take one of five possible values: $0, \frac{2}{3}, 1, \frac{3}{2}, 2$, for all network configurations. To determine the sum s.d.o.f., we divide the class of two-unicast layered networks into several sub-classes, and propose an achievable scheme based on the specific structure of the networks in each sub-class. Our achievable schemes are based on real interference alignment, cooperative jamming, interference neutralization and cooperative jamming neutralization techniques.

Then, we consider the Gaussian wiretap channel with M helpers, where no eavesdropper channel state information (CSI) is available at the legitimate entities. One of the key ingredients of our optimal achievable scheme with perfect CSI is to align cooperative jamming signals with the information symbols at the eavesdropper to limit the information leakage rate. This requires perfect eavesdropper CSI at the transmitters. We propose a new achievable scheme in which cooperative jamming signals span the *entire space* of the eavesdropper, but are not exactly aligned with

the information symbols. We show that this scheme achieves the same s.d.o.f. of $\frac{M}{M+1}$ but does not require any eavesdropper CSI; the transmitters *blindly* cooperative jam the eavesdropper.

Next, we study the separability of the parallel MAC wiretap channel. Separability, when exists, is useful as it enables us to code separately over parallel channels, and still achieve the optimum overall performance. It is well-known that the parallel single-user channel, parallel MAC and parallel BC are all separable, however, the parallel IC is not separable in general. In this dissertation, we show that, while MAC is separable MAC wiretap channel is not separable in general. We prove this via a specific linear deterministic MAC wiretap channel. We then show that even the Gaussian MAC wiretap channel is inseparable in general. Finally, we show that, when the channel gains are drawn from continuous distributions, and when the s.d.o.f. region is considered, then the Gaussian MAC wiretap channel is almost surely separable.

Finally, we study the two-user one-sided IC with confidential messages. In this IC, in addition to the usual selfishness of the users, the relationship between the users is adversarial in the sense of both receivers' desires to eavesdrop on the communication of the other pair. We develop a game-theoretic model for this setting. We start with a model where each pair's payoff is their own secrecy rate. We then propose a refinement for the payoff function by explicitly accounting for the desire of the receiver to eavesdrop on the other party's communication. This payoff function captures the adversarial relationship between the users better. We determine the Nash equilibria for the binary deterministic channel for both payoff functions.

SECURE DEGREES OF FREEDOM OF WIRELESS NETWORKS

by

Jianwei Xie

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2014

Advisory Committee:
Professor Şennur Ulukuş, Chair/Advisor
Professor Prakash Narayan
Professor Gang Qu
Professor Adrian Papamarcou
Professor Lawrence C. Washington

DEDICATION

To my wife Yanqi Wang.

ACKNOWLEDGEMENT

First of all, I would like to express my sincerest gratitude to my advisor, Prof. Sennur Ulukus. It was really a tough time at the beginning stage of my PhD study. Without her help, patience, and open-mindedness, I may not be able to complete my PhD and start a new career life. In the past six years, she taught me many many things, not only the academic knowledge supporting my research, but also the methodology helping me solve all challenging problems in all areas of my life.

I would like to thank Professors Prakash Narayan, Gang Qu, Adrian Papamarcou and Lawrence C. Washington for being in my dissertation committee and providing me useful comments about my work. I am especially grateful to Professor Prakash Narayan for the conversations we had on various topics, including the nonsense issue like coffee. I also want to thank Professors Alexander Barg and Prakash Narayan for the wonderful teaching assistant experiences with them, which help me a lot.

I would also like to thank my wife, Yanqi Wang, for her kindly unconditioned support and love. She takes care of my life, respects my decisions, tolerates my bad temper, and understands me. Even during our most difficult time, the only words I heard from her were encouragement and hope. I really appreciate the offer from her which allowed me to sit on the chair and write my paper inside the Metropolitan Museum of Art at New York for the whole afternoon, while she was taking the pictures alone.

I would like to thank all friends in CSPL lab. My thanks go to Jing Yang,

Beiyu Rong, Ravi Tandon, Raef Bassily, Ersen Ekrem, Himanshu Tyagi, Shalab Jain, Omur Ozel, Pritam Mukherjee, Berk Gurakan, Praneeth Boda for their nice company. I give special thanks to Jing Yang and her husband Weiqiang Wu, who have helped me so much since the first day I came to U.S.A. I owe so many thanks to them, for their advises in school, their supports in Maryland, and their company in Boston. I feel proud to meet Himanshu Tyagi, who is one of most brilliant guys I have ever met. Thanks him for our growing friendship, insightful discussions, and the farewell party at his home. I am also grateful to Omur for our annual travel to ISIT crossing Europe, North America, and Asia. Especially, thanks for his welcome treat, which started my fantastic journal in Istanbul, Turkey. I would like to thank Pritam Mukherjee, Berk Gurakan, Praneeth Boda, and many other friends who made my stay at office just fun.

Finally, I thank my father Zhenming Xie, my mother Weirong Wei for theirs love. It was really an unforgettable travel in New York before my graduation. Mum played with the seagull at the Liberty Island. Dad named the Wall Street as the "poor street" due to the terrible environment after heavy snow. And, we took a "I love New York" photo together before a van in the snowing night of my 30th birthday. I shall treasure this memory for ever.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Overview

In this dissertation, we study secure communications in wireless interference networks from an information-theoretic point of view. Security of communication was first considered by Shannon in [1], where a legitimate pair wishes to have secure communication in the presence of an eavesdropper over a noiseless channel, leading to the necessity of secure keys and the one-time-pad encryption method, in that model. Wyner introduced the noisy wiretap channel, and demonstrated that secure communication can be attained by stochastic encoding without using any keys, if the eavesdropper is degraded with respect to the legitimate receiver [2]. Csiszar and Korner generalized his result to arbitrary, not necessarily degraded, wiretap channels, and showed that secure communication is still possible, even when the eavesdropper is not degraded [3]. Csiszar and Korner introduced channel prefixing and rate splitting into the achievable scheme in addition to Wyner's stochastic encoding. Leung-Yan-Cheong and Hellman obtained the capacity-equivocation region of the Gaussian wiretap channel [4], which is degraded. They showed that a Gaussian input signal is optimum, and in particular, secrecy capacity equals the difference of the capacities of the legitimate and eavesdropping links in this case.

Multi-user versions of the wiretap channel have been studied recently, e.g.,

broadcast channels (BC) with confidential messages [5, 6], multi-receiver wiretap channels [7–10] (see also a survey on extensions of these to MIMO channels [11]), two-user interference channels (IC) with confidential messages [5, 12], two-user IC with external eavesdroppers [13], multiple access (MAC) wiretap channels [14–18], relay eavesdropper channels [19–24], compound wiretap channels [25, 26]. Since in most multi-user scenarios it is difficult to obtain the exact secrecy capacity region, achievable secure degrees of freedom (s.d.o.f.) at high signal-to-noise ratio (SNR) cases have been studied for several channel structures, such as the K-user Gaussian IC with confidential messages [27, 28], the K-user IC with external eavesdroppers [27, 29], the Gaussian wiretap channel with one helper [30–33], the Gaussian MAC wiretap channel [34, 35], and the wireless X network [36]. In this dissertation, we focus on the s.d.o.f. of various wireless networks and determine the exact s.d.o.f. for several different channel models.

In the Gaussian wiretap channel, the secrecy capacity is the difference between the channel capacities of the transmitter-receiver and the transmitter-eavesdropper pairs. It is well-known that this difference does not scale with the SNR, and hence the s.d.o.f. of the Gaussian wiretap channel is zero, indicating a severe penalty due to secrecy in this case. Fortunately, this does not hold in multi-user scenarios. In a multi-user wireless network, focusing on a specific transmitter-receiver pair, other (independent) transmitters can be understood as helpers which can improve the individual secrecy rate of this specific pair by cooperatively jamming the eavesdropper [14, 15, 18, 37].[1] However, these cooperative jamming signals also limit the decod-

[1]Note that, if reliability was the only concern, then in order to maximize the reliable rate of a

ing performance of the legitimate receiver. It is also known that if the helper nodes transmit independent identically distributed (i.i.d.) Gaussian cooperative jamming signals in a Gaussian wiretap channel, then the s.d.o.f. is still zero [14, 15, 35, 37]. Such i.i.d. Gaussian signals, while maximally jam the eavesdropper, also maximally hurt the legitimate user's decoding capability. Therefore, we expect that strictly positive s.d.o.f. may be achieved with some *weak* jamming signals. Confirming this intuition, [30, 31] achieved positive s.d.o.f. by using nested lattice codes in a Gaussian wiretap channel with a helper.

In this dissertation, we develop a unified framework based on information-theoretic principles to completely determine s.d.o.f. of several different kinds of wireless communication channel models, and provide the corresponding optimal signaling designs at high SNR. Toward this end, in Chapter 2, we start with the Gaussian wiretap channel with one helper, which provides us a basic framework to understand the role of an independent transmitter (helper) from an information-theoretic secrecy point of view in a wireless network. Then, in Chapter 2, we study the *sum* s.d.o.f. of *one-hop* wireless networks by considering three other fundamental network structures in addition to the Gaussian wiretap channel with helpers: Gaussian BC with confidential messages, two-user Gaussian IC with confidential messages, and Gaussian MAC wiretap channel [38–40]. In Chapter 3, we extend our problem setting to a K-user IC, and determine the exact sum s.d.o.f. of the K-user Gaussian IC with three different secrecy constraints in a unified framework [41, 42]. In Chapter

given transmitter-receiver pair, all other independent transmitters must remain silent. However, when secrecy in addition to reliability is a concern, then independent helpers can improve the secrecy rate of a given transmitter-receiver pair by transmitting signals [14, 15, 18, 37].

4, we broaden our problem formulation and develop a technique to determine the *entire s.d.o.f. regions* of K-user Gaussian MAC wiretap channel and K-user IC with secrecy constraints [43, 44]. In Chapter 5, we consider *multi-hop* networks and determine the sum s.d.o.f. of two-unicast layered wireless networks [45, 46]. In Chapter 6, we consider the case where eavesdropper's channel state information (CSI) is not available at the legitimate entities in an M-helper Gaussian wiretap channel, and determine the exact s.d.o.f. [47]. In Chapter 7, we consider a parallel Gaussian MAC wiretap channel, and investigate the optimality of separation: while Gaussian MAC is known to be separable, we show that, in general, Gaussian MAC wiretap channel is not separable [48]. Finally, in Chapter 8, we investigate the adversarial relationship between the transmitter-receiver pairs in a network at a deeper level by proposing a secrecy game between selfish but rational users by explicitly accounting for the desires of the users to keep their own messages secure while achieving eavesdropping on the other user's messages [49].

1.2 Outline

In Chapter 2, we obtain the exact s.d.o.f. of several important one-hop Gaussian network structures. We start by considering the Gaussian wiretap channel with a single helper, as shown in Figure 1.1. In this channel model, the s.d.o.f. with i.i.d. Gaussian cooperative signals is zero [37], and strictly positive s.d.o.f. can be obtained, for instance, by using nested lattice codes [30, 31]. Considering this model as a special case of other channel models, we can verify that $\frac{1}{4}$ s.d.o.f. can be achieved

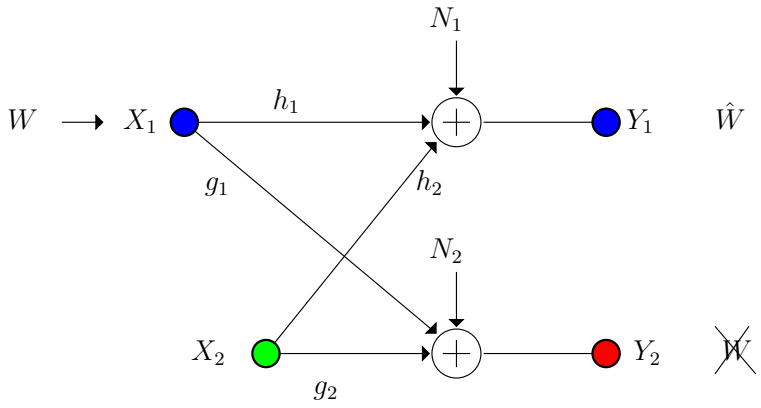


Figure 1.1: Gaussian wiretap channel with one helper.

as a symmetric individual rate on the two-user IC with external eavesdroppers [27, 29] and on the MAC wiretap channel [34]. References [50] and [31, Theorem 5.4 on page 126] showed that with integer lattice codes a s.d.o.f. of $\frac{1}{2}$ can be achieved if the channel gains are *irrational algebraic numbers.* While such class of channel gains has zero Lebesgue measure, the idea behind this achievable scheme can be generalized to much larger set of channel gains. The enabling idea behind this achievable scheme is as follows: If the cooperative jamming signal from the helper and the message signal from the legitimate user can be aligned in the same *dimension* at the eavesdropper, then the secrecy penalty due to the information leakage to the eavesdropper can be upper bounded by a constant, while the information transmission rate to the legitimate user can be made to scale with the transmit power. Following this insight, we propose an achievable scheme[2] based on real interference alignment [51, 52] and cooperative jamming to achieve $\frac{1}{2}$ s.d.o.f. for *almost all channel gains.* This constitutes the best known achievable s.d.o.f. for the Gaussian wiretap channel with

[2]In this chapter, by an *achievable scheme*, we mean that we design specific forms for the auxiliary random variables and the channel inputs, and evaluate well-known random-coding based achievable expressions with our selected random variables.

a helper. The cooperative jamming signal from the helper can be distinguished from the message signal at the legitimate receiver by properly designing the structure of the signals from both transmitters; meanwhile, they can be aligned together at the observation space of the eavesdropper to ensure undecodability of the message signal, hence secrecy (see Figure 2.1). Intuitively, the end result of $\frac{1}{2}$ s.d.o.f. comes from the facts that the cooperative jamming signal and the message signal should be of about the same size to align at the eavesdropper, and they should be separable at the legitimate receiver, who can decode at most a total of 1 d.o.f. We analyze the rate and equivocation achieved by this scheme by using the Khintchine-Groshev theorem of Diophantine approximation in number theory.

For the converse for this channel model, the best known upper bound is $\frac{2}{3}$ [31, Theorem 5.3 on page 126] which was obtained by adding virtual nodes to the system and using the upper bound developed in [53]. Reference [53] developed upper bounds for the s.d.o.f. of the multiple-antenna compound wiretap channel by exploring the correlation between the n-letter observations of a group of legitimate receivers and a group of eavesdroppers, instead of working with single-letter expressions. Our converse works with n-letter observations as well. Our converse has two key steps. First, we upper bound the secrecy rate by the difference of the sum of differential entropies of the channel inputs of the legitimate receiver and the helper and the differential entropy of the eavesdropper's observation. This shows that, the secrecy penalty due to the eavesdropper's observation is tantamount to eliminating one of the independent channel inputs. As a result, the final upper bound involves only the differential entropy of the channel input of the independent helper. In the second

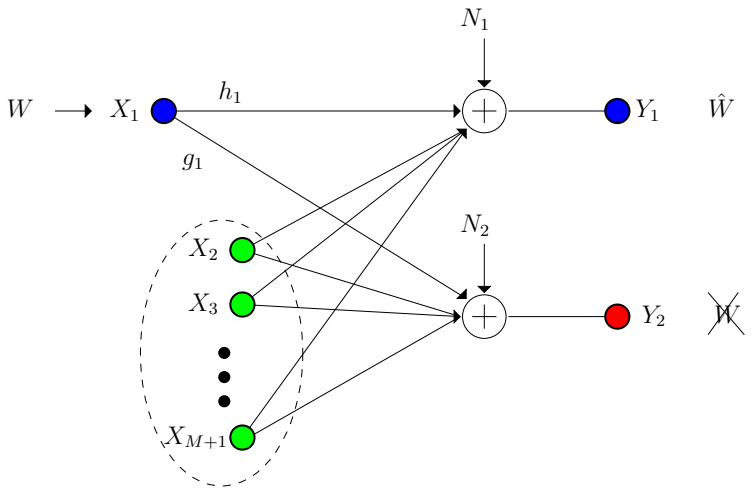


Figure 1.2: Gaussian wiretap channel with M helpers.

step, we develop a relationship between the cooperative jamming signal from the independent helper and the message rate. The goal of the cooperative jamming signal is to further confuse the eavesdropper. However, the cooperative jamming signal appears in the channel output of the legitimate user also. Intuitively, if the legitimate user is to reliably decode the message signal which is mixed with the cooperative jamming signal, there must exist a constraint on the cooperative jamming signal. Our second step identifies this constraint by developing an upper bound on the differential entropy of the cooperative jamming signal in terms of the message rate. These two steps give us an upper bound of $\frac{1}{2}$ s.d.o.f. for the Gaussian wiretap channel with a helper, which matches our achievable lower bound. This concludes that the exact s.d.o.f. of the Gaussian wiretap channel with a helper is $\frac{1}{2}$ for *almost all channel gains*.

We then generalize our result to the case of M independent helpers; see Figure 1.2. We show that the exact s.d.o.f. in this case is $\frac{M}{M+1}$. Our achievability extends our original achievability for the one-helper case in the following manner:

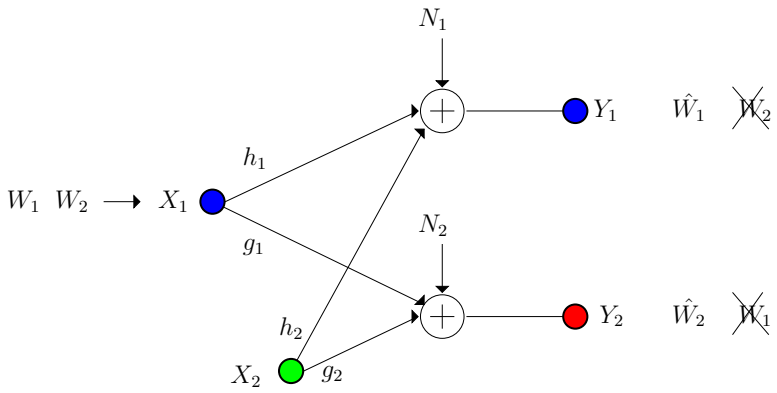


Figure 1.3: Gaussian BC with confidential messages and $M = 1$ helper.

The transmitter sends its message by employing M independent sub-messages, and the M helpers send independent cooperative jamming signals. Each cooperative jamming signal is aligned with one of the M sub-messages at the eavesdropper to ensure secrecy (see Figure 2.2). Therefore, each sub-message is protected by one of the M helpers. Our converse is an extension of the converse in the one-helper case. In particular, we upper bound the secrecy rate by the difference of the sum of the differential entropies of all of the channel inputs and the differential entropy of the eavesdropper's observation. The secrecy penalty due to the eavesdropper's observation eliminates one of the channel inputs, which we choose as the legitimate user's channel input. We then utilize the relationship we developed between the differential entropy of each of the cooperative jamming signals and the message rate. The upper bound so developed matches the achievability lower bound, giving the exact s.d.o.f. for the M-helper case.

As an important extension of the single-message one-helper problem, we consider the BC with confidential messages and one-helper (see Figure 1.3), where a transmitter wishes to send two messages securely to two users on a BC while keep-

ing each message secure from the unintended receiver. Without a helper, the sum s.d.o.f. of this channel model is zero. We show that with one helper, the exact sum s.d.o.f. is 1. The sum s.d.o.f. remains the same as more helpers are added. The achievability for the one-helper case is as follows: The transmitter sends the channel input by putting two messages on different *rational dimensions*. Meanwhile, the cooperative jamming signal from the helper is designed in such a way that it aligns with the unintended message, but leaves the intended message intact, at each receiver (see Figure 2.3). The converse for this case follows from the converse without any secrecy constraints for the Gaussian BC, which is 1.

Cooperative jamming based achievable schemes are intuitive for the independent helper problems due to the fact that the helpers do not have messages of their own. Such schemes can be extended to multiple-transmitter (with independent messages) settings, such as, IC with confidential messages and MAC wiretap channel, etc. All previous works extended this approach in the following way: Each transmitter simply sends one message signal, and the message signals from all of the transmitters are *aligned* together at the eavesdropper. Due to the mixture of the message signals, the eavesdropper is confused regarding any one of the message signals, and a positive s.d.o.f. is achievable. However, this approach is sub-optimal. To achieve optimal s.d.o.f., we need to design the structure of the channel inputs more carefully. We propose the following transmission structure: Besides the message carrying signal, each transmitter also sends a cooperative jamming signal.[3] The ex-

[3]This addition of a cooperative jamming signal to the message carrying signal can be interpreted as *channel prefixing* [3] which introduces a further randomization from the message carrying signal to the channel input on top of *stochastic encoding* [2] which maps every message to multiple codewords.

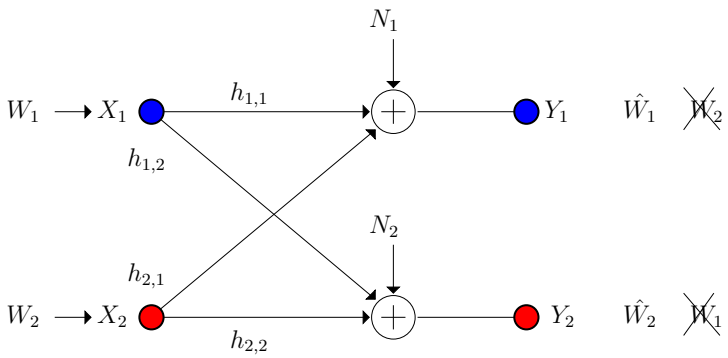


Figure 1.4: Two-user Gaussian IC with confidential messages.

act number and the structure of the message signals and the cooperative jamming signals depend on the specific network structure.

For the two-user Gaussian IC with confidential messages (see Figure 1.4), previously known lower bounds for the sum s.d.o.f. are $\frac{1}{3}$ [36] and 0 [27], which come from the general results for the K-user case: $\frac{K-1}{2K-1}$ [36] and $\frac{K(K-2)}{2K-2}$ [27]. The individual s.d.o.f. of $\frac{1}{2}$ achieved in [50] and [31, Theorem 5.4 on page 126] in the context of the wiretap channel with a helper (for the class of algebraic irrational channel gains) can also be understood as a lower bound for the sum s.d.o.f. for the two-user IC with confidential messages. We show that, by using interference alignment and cooperative jamming at both transmitters, we can achieve a sum s.d.o.f. of $\frac{2}{3}$ for *almost all channel gains*, which is better than all previously known achievable s.d.o.f. We design an achievable scheme in which each transmitter sends a mixed signal containing the message signal and a cooperative jamming signal. These two components have the same signaling structure, and are separable at the intended receiver. Furthermore, the cooperative jamming signal is perfectly *aligned* with the message signal from the other transmitter (see Figure 2.4).[4] Our converse

[4]An interesting observation here is that each transmitter jams its own receiver to protect the

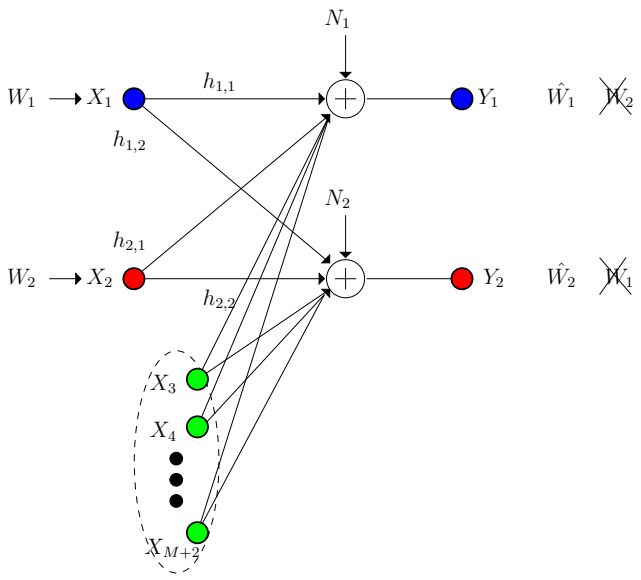


Figure 1.5: Two-user Gaussian IC with confidential messages and M helpers.

starts with considering transmitter 2 as a helper for transmitter-receiver pair 1. In contrast to the single-message case, since transmitter 2 also intends to deliver a message W_2 to receiver 2, in the second step, we treat transmitter 1 as the helper for the transmitter-receiver pair 2 and upper bound the differential entropy of its channel input by using its relationship with the message rate of W_2. The converse matches the achievability lower bound, giving the exact s.d.o.f. for the two-user IC with confidential messages as $\frac{2}{3}$.

We then generalize this result to the case with one helper, i.e., two-user Gaussian IC with confidential messages and one helper (see Figure 1.5). We show that a sum s.d.o.f. of 1 is achievable. The structure of the channel inputs in the corresponding achievable scheme is simpler than in the cases of previous channel models. Each transmitter sends a signal carrying its message. With probability one, these

message of the other transmitter. This scheme achieves the largest (optimum) sum s.d.o.f. for the system.

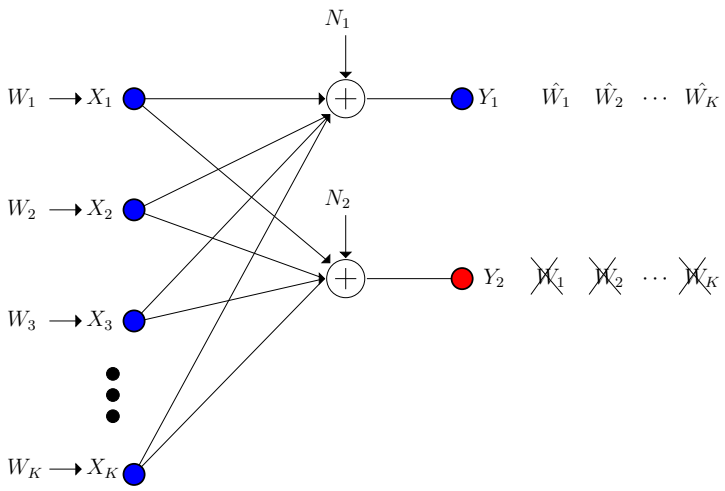


Figure 1.6: K-user MAC wiretap channel.

two signals are not in the same *rational dimension* at the receivers. On the other hand, the cooperative jamming signal from the helper can be aligned with the unintended message at each receiver while leaving the intended message intact (see Figure 2.5). The converse for this case follows from the converse without any secrecy constraints for the two-user Gaussian IC [54], which is 1. This concludes that the exact sum s.d.o.f. of the two-user Gaussian IC with confidential messages and one helper is 1. Since utilizing one helper is sufficient to achieve the upper bound, the sum s.d.o.f. remains the same for arbitrary M helpers.

For the K-user MAC wiretap channel (see Figure 1.6), the best known lower bound for the sum s.d.o.f. is $\frac{K-1}{K}$ [34] which gives $\frac{1}{2}$ for $K = 2$. In addition, for $K = 2$, the individual s.d.o.f. of $\frac{1}{2}$ achieved in [50] and [31, Theorem 5.4 on page 126] in the context of the wiretap channel with a helper (for the class of algebraic irrational channel gains) can also be understood as a lower bound for the sum s.d.o.f. for the two-user MAC wiretap channel. We show that, by using interference alignment and cooperative jamming at all transmitters simultaneously, we can achieve a sum

s.d.o.f. of $\frac{K(K-1)}{K(K-1)+1}$ for the K-user MAC wiretap channel, for *almost all channel gains*, which is better than all previously known achievable s.d.o.f. In particular, for $K = 2$, our achievable scheme gives a sum s.d.o.f. of $\frac{2}{3}$. In order to obtain this sum s.d.o.f., we need a more detailed structure for each channel input. Each transmitter sends a mixed signal containing the message signal and a cooperative jamming signal. Specifically, each transmitter divides its own message into $K-1$ sub-messages each of which having the same structure as the cooperative jamming signal. By such a scheme, the total K cooperative jamming signals from the K transmitters *span* the whole *space* at the eavesdropper's observation, in order to hide each one of the message signals from the eavesdropper. On the other hand, to maximize the sum s.d.o.f., the cooperative jamming signals from all of the transmitters are *aligned* in the same *dimension* at the legitimate receiver to occupy the smallest *space* (see Figure 2.6). Our converse is a generalization of our converse used in earlier channel models. We first show that the sum secrecy rate is upper bounded by the sum of differential entropies of all channel inputs except the one eliminated by the eavesdropper's observation. Then, we consider each channel input as the jamming signal for all other transmitters and upper bound its differential entropy by using its relationship with the sum rate of the messages belonging to all other transmitters. This gives us a matching converse and shows that the exact sum s.d.o.f. for this channel model is $\frac{K(K-1)}{K(K-1)+1}$.

In Chapter 3, we focus on the K-user IC with secrecy constraints, and determine its exact sum s.d.o.f. The K-user Gaussian IC with secrecy constraints consists of K transmitter-receiver pairs each wishing to have secure communication

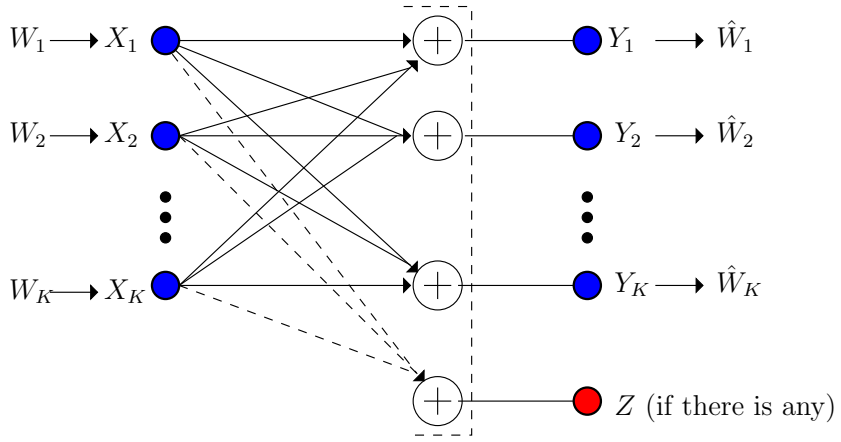


Figure 1.7: K-user Gaussian IC with secrecy constraints.

over a Gaussian IC; see Figure 1.7. We consider three different secrecy constraints: 1) K-user IC with one external eavesdropper (IC-EE), where K transmitter-receiver pairs wish to have secure communication against an external eavesdropper, see Figure 1.8(a). 2) K-user IC with confidential messages (IC-CM), where there are no external eavesdroppers, but each transmitter-receiver pair wishes to secure its communication against the remaining $K-1$ receivers, see Figure 1.8(b). 3) K-user IC with confidential messages and one external eavesdropper (IC-CM-EE), which is a combination of the previous two cases, where each transmitter-receiver pair wishes to secure its communication against the remaining $K-1$ receivers and the external eavesdropper, see Figure 1.8(c).

Reference [28] showed that nested lattice codes and layered coding are useful in providing positive sum s.d.o.f. for the K-user IC-CM; their result gave a sum s.d.o.f. of less than $\frac{3}{4}$ for $K=3$. Reference [27] used interference alignment to achieve a sum s.d.o.f. of $\frac{K(K-2)}{2K-2}$ for the K-user IC-CM, which gave $\frac{3}{4}$ for $K=3$. Based on the same idea, [27, 29] achieved a sum s.d.o.f. of $\frac{K(K-1)}{2K}$ for the K-user IC-EE, which

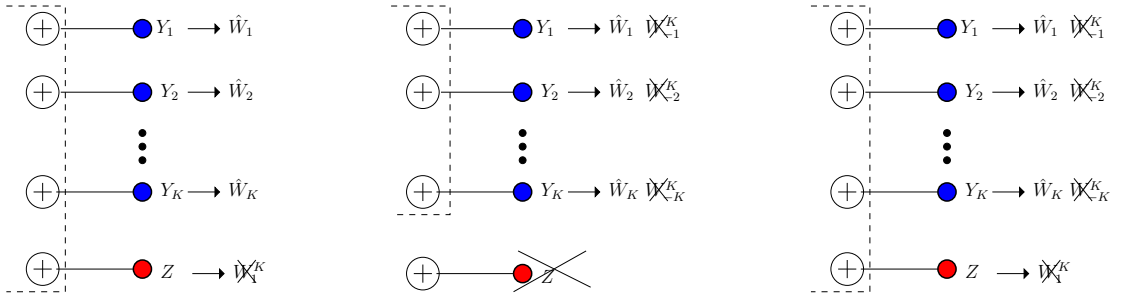


Figure 1.8: The receiver sides of the three channel models: (a) K-user IC-EE, (b) K-user IC-CM, and (c) K-user IC-CM-EE, where W_{-i}^K is the whole message set but W_i.

gave 1 for $K = 3$. The approach used in [27, 29] is basically to evaluate the secrecy performance of the interference alignment technique [55] devised originally for the K-user IC without any secrecy constraints. Since the original interference alignment scheme puts all of the interfering signals into the same reduced-dimensionality sub-space at a receiver, it naturally provides a certain amount of secrecy to those signals as an unintended byproduct, because the interference signals in this sub-space create uncertainty for one another and make it difficult for the receiver to decode them. However, since the end-goal of [55] is *only* to achieve reliable decoding of the transmitted messages at their intended receivers, the d.o.f. it provides is sub-optimal when *both* secrecy and reliability of messages are considered.

The *exact* sum s.d.o.f. of the two-user IC-CM is obtained to be $\frac{2}{3}$ in Chapter 2. It is shown that while interference alignment is a key ingredient in achieving positive s.d.o.f., a more intricate design of the signals is needed to achieve the simultaneous end-goals of reliability at the desired receivers and secrecy at the eavesdroppers. In particular, in Chapter 2, each transmitter sends both message carrying signals, as

well as cooperative jamming signals.

In Chapter 3, we generalize the results in Chapter 2 to the case of K-user IC, for $K > 2$. Our generalization has three main components:

1. While Chapter 2 considered IC-CM only, we consider both IC-CM and IC-EE and their combination IC-CM-EE in a unified framework. To this end, we show converses separately for IC-EE and IC-CM, which imply a converse for IC-CM-EE; and we show achievability for IC-CM-EE, which implies achievability for IC-EE and IC-CM. The achievability and converse meet giving an *exact* sum s.d.o.f. of $\frac{K(K-1)}{2K-1}$ for all three models.

2. For achievability: In the case of two-user IC-CM in Chapter 2, each message needs to be delivered reliably to one receiver and needs to be protected from another receiver. This requires alignment at two receivers, which is achieved in Chapter 2 by simply choosing transmission coefficients properly, which cannot be extended to the K-user case here. In the K-user IC-CM-EE case, we need to deliver each message to a receiver, while protecting it from K other receivers. This requires designing signals in order to achieve alignment at $K+1$ receivers simultaneously: at one receiver (desired receiver) we need alignment to ensure that the largest space is made available to message carrying signals for their reliable decodability, and at K other receivers, we need to align cooperative jamming signals with message carrying signals to protect them. These requirements create two challenges: i) aligning multiple signals simultaneously at multiple receivers, and ii) upper bounding the information leakage rates by

suitable functions which can be made small. We overcome these challenges by using an asymptotical approach [52], where we introduce many signals that carry each message and align them simultaneously at multiple receivers only order-wise (i.e., align most of them, but not all of them), and by developing a method to upper bound the information leakage rate by a function which can be made small. In contrast to the constant upper bound for the information leakage rate in Chapter 2, here the upper bound is not constant, but a function which can be made small. This is due to the non-perfect (i.e., only asymptotical) alignment.

3. For the converse: To the best of our knowledge, the only known upper bound for the sum s.d.o.f. of the K-user IC with secrecy constraints is $\frac{K}{2}$, which is the upper bound with no secrecy constraints [55]. The upper bounding technique for the two-user IC-CM in Chapter 2 considers one single confidential message against the corresponding unintended receiver each time, since in that case the eavesdropping relationship is straightforward: for each message there is only one eavesdropper and for each eavesdropper there is only one confidential message. However, in the case of K-user IC, each message is required to be kept secret against multiple eavesdroppers and each eavesdropper is associated with multiple unintended messages. To develop a tight converse, we focus on the eavesdropper as opposed to the message. In the converse for IC-EE, we consider the sum rate of all of the messages eavesdropped by the external eavesdropper. We sequentially apply the *role of a helper lemma* in Chapter

2 to each transmitter by treating its signal as a helper to another specific transmitter. In the converse for IC-CM, for each receiver (which also is an eavesdropper), we consider the sum rate of all unintended messages, and again apply the *role of a helper lemma* in a specific structure.

In Chapter 4, we investigate the s.d.o.f. structures of multi-user wireless networks in more depth by studying the s.d.o.f. regions of MAC wiretap channel and IC with secrecy constraints. We start with the MAC wiretap channel, where multiple legitimate transmitters wish to have secure communication with a legitimate receiver in the presence of an eavesdropper; see Figure 1.6. The converse for the sum s.d.o.f. is developed in Chapter 2 using two lemmas: the *secrecy penalty* lemma and the *role of a helper* lemma. The achievability for the sum s.d.o.f. in Chapter 2 is based on real interference alignment [51, 52] and structured cooperative jamming [15] with an emphasis on simultaneous alignments at both the legitimate receiver and the eavesdropper. We develop the converse for the *entire region* by starting from a middle step in the converse proof of Chapter 2. While Chapter 2 developed asymmetric upper bounds for the secure rates, since the sum s.d.o.f. was achieved by symmetric rates in Chapter 2, we summed up the asymmetric upper bounds to get a single symmetric upper bound to match the achievability. We revisit the converse proof in Chapter 2 and develop a converse for the entire region by keeping the developed asymmetric upper bounds. Therefore, the converse proofs developed in Chapter 2 to obtain a converse for the sum s.d.o.f. suffice to obtain a tight converse for the entire region.

The converse region for the s.d.o.f. problem has a general *polytope* structure, as opposed to the non-secrecy counterpart for the MAC which has a *polymatroid* structure [56]. Polytope is a bounded polyhedron, which is an intersection of a finite number of half-spaces. Such definition is called a half-space representation, which is exactly the way our converse is expressed. In order to show the achievability of the polytope region, we need to show the achievability of boundaries of all of the half-spaces, which is inefficient. We use Minkowski theorem [57, Theorem 2.4.5] which states that the polytope region discussed in Chapter 4 can be represented by the convex hull of all of its extreme points, which there are only finitely many. We, therefore, first determine the extreme points of this converse (polytope) region, and then develop an achievable scheme for each extreme point of the converse region; the achievability of the entire region then follows from time-sharing. In particular, each extreme point of the converse region is achieved by an m-user MAC wiretap channel with $K-m$ helpers, for $m=1,\ldots,K$, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers.

We then consider the IC with secrecy constraints; see Figure 1.7. In particular, we consider three different secrecy constraints in a unified framework as in Chapter 3: IC-EE, IC-CM, and IC-CM-EE. The converse for the sum s.d.o.f. (the sum s.d.o.f. is the same for all three models) is developed in Chapter 3 by using the *secrecy penalty* lemma and the *role of a helper* lemma in a certain way, and then by summing up the obtained asymmetric upper bounds into a single symmetric upper bound. The achievability for the sum s.d.o.f. in Chapter 3 is based on asymptotical real interference alignment [52] to enable simultaneous alignment at multiple receivers.

In order to develop a converse for the *entire region* for the IC case, in Chapter 4, similar to the MAC case, we start by re-examining the converse proof in Chapter 3 for the sum s.d.o.f. However, unlike the MAC case, the original steps used for the sum s.d.o.f. are not tight for the characterization of the entire region. There are two reasons for this: First, in the case of the MAC wiretap channel, since there is a single legitimate receiver, each transmitter (helper/interferer) impacts the total rate of all other legitimate transmitters at the legitimate receiver, and therefore, there is a single manner in which the *role of a helper* lemma is applied. In the IC case, there are many different ways in which the *role of a helper* lemma can be invoked as there are multiple receivers. In this case, by pairing up helpers (interferers) and the receivers we obtain $(K-1)^K$ upper bounds; even after removing the redundancies, we get $\left(\binom{K}{K-1}\right) = \binom{2K-2}{K-1}$ upper bounds. In order to obtain the tightest subset of these upper bounds, we choose the most binding pairing of the helpers/interferers and the receivers. In particular, we do not apply the *next one* (i.e., $k = i-1$ and $k = i+1$) selection of helpers/interferers as we have done in (3.33) and (3.61) in Chapter 3. Instead, we choose all of the transmitters as interfering with a single transmitter-receiver pair; see (4.92) and (4.108) in Chapter 4. This yields the tightest upper bounds. Second, we observe that, when we study the s.d.o.f. region, we need to consider the non-secrecy upper bounds for the underlying IC [54, 55] as additional upper bounds. We note that such upper bounds are not binding for the case of MAC wiretap channel s.d.o.f. region, or the MAC and IC sum s.d.o.f. converses. In fact, such non-secrecy upper bounds for the IC are not binding even for the cases of $K = 2$ or $K = 3$. We observe that these upper bounds are needed for the IC with

secrecy constraints starting with $K \geq 4$. To the best of our knowledge, this is the first time in network information theory that $K = 2$ or $K = 3$ do not capture the most generality of the problem, and we need to study $K = 4$ to observe a certain multi-user phenomenon to take effect.

The converse region for the IC with secrecy constraints has a *polytope* structure as well, and similar to the MAC wiretap channel case, we need to determine the extreme points of this polytope region. However, different from the MAC wiretap channel case, the converse region consists of two classes of upper bounds, due to secrecy and due to interference. This makes it difficult to identify the extreme points of the converse polytope. Finding the extreme points is related to finding full-rank sub-matrices from an overall matrix of size $2K + K(K-1)/2$. Since there are approximately K^K such matrices, an exhaustive search is intractable, and therefore we investigate the consistency of the upper bounds, which reduces the possible number of sub-matrices to examine. After determining the extreme points of the converse polytope, we develop an achievable scheme for each extreme point. In particular, each extreme point of the converse region is achieved by a $(K-m)$-user IC-CM with m helpers and N independent external eavesdroppers, for $m \geq 1$ and finite N.

Finally, after characterizing the entire s.d.o.f. regions of the MAC and IC with secrecy constraints, as a byproduct of our results in Chapter 4, we note that the sum s.d.o.f. is achieved *only at one extreme point* of the s.d.o.f. region, which is the symmetric-rate extreme point, for both MAC and IC channel models.

In Chapter 5, we consider a two-unicast layered network (see Figure 1.9) where

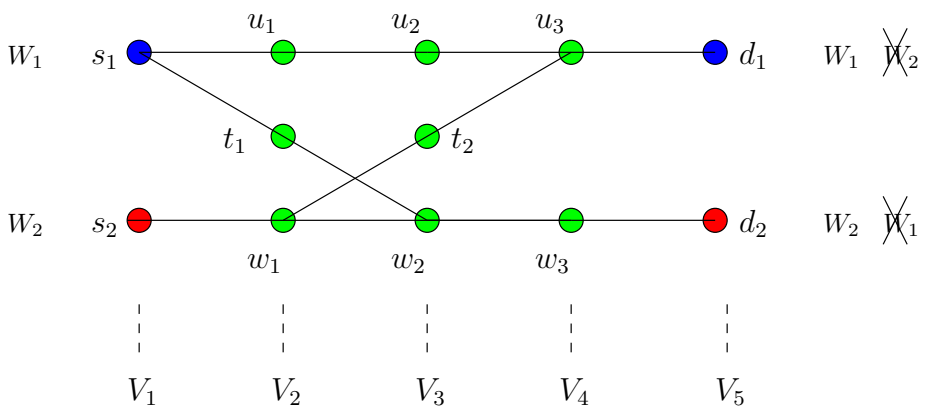


Figure 1.9: An example two-unicast layered network.

two transmitters wish to have reliable and secure communication with their respective receivers simultaneously, by utilizing a layered network in between. The two-layer (i.e., single-hop) version of this network is an IC, whose capacity is unknown in general; it is known only in certain special cases, e.g., a class of deterministic ICs [58], a class of strong ICs [59–61], a class of degraded ICs [62]. The degrees of freedom (d.o.f.) characterizations have been found for the IC in several different settings, e.g., [51, 52, 55, 63]. In particular, the sum d.o.f. of a fully connected two-user IC is 1 [54]. Recently, reference [64] showed that, if the source-destination pairs are *connected*, then with probability one, the sum d.o.f. of two-unicast layered Gaussian networks can take only one of three possible values: 1, $\frac{3}{2}$ and 2.

We extend this line of work to include security in addition to reliability for the end-to-end users. To determine the sum d.o.f. of two-unicast layered networks, reference [64] divided all network structures into five cases: A, A', B, B' and C, and found the sum d.o.f. in each case. In particular, the sum d.o.f. of all networks in cases A and A' is 1, in cases B and B' is 2, and in case C is $\frac{3}{2}$. The main challenge of

determining the sum *secure* d.o.f. is in cases A and A'. In the first part of Chapter 5, we show that although for these two cases the sum d.o.f. is exactly 1, the sum s.d.o.f. can take one of three possible values: $0, \frac{2}{3}$ and 1. To determine the s.d.o.f. in all possible cases, we further divide the layered networks in case A and A' into five sub-cases, e.g., A_1 through A_5. In the first four sub-cases, we explicitly utilize the properties of the layered network in each sub-case, and either find a node and employ it to protect the communication by having it perform cooperative jamming [14, 15] against the unintended receiver, or use the interference neutralization technique [65] to neutralize the message signal at the unintended destination and even neutralize the cooperative jamming signal at the intended receiver to mimic the wiretap channel with cooperative jamming. Achievable schemes we develop based on these two techniques match the corresponding upper bounds, giving the exact sum s.d.o.f. for the layered networks in these four sub-cases.

In the last sub-case of the cases A and A', i.e., in A_5, we note that there is an independence structure in the last layer of the network before the destination nodes. Specifically, the nodes in this last layer have mutually independent observations, and therefore as transmitters in the last hop of the network, they can only send independent signals. Due to this independence structure, we cannot simply utilize cooperative jamming and/or interference neutralization to achieve the optimal sum s.d.o.f., which makes this sub-case most challenging. To overcome this difficulty, we first reduce this problem into two simplest equivalent channel models, which are (**P1**) the two-user Gaussian IC with confidential messages and $M \geq 0$ helper(s) and (**P2**) the Gaussian BC with confidential messages and $M \geq 1$ helper(s). In

Chapter 2, we have shown that $\frac{2}{3}$ is the exact sum s.d.o.f. for the two-user Gaussian IC with confidential messages, i.e., for the case $M = 0$ in (**P1**), and 1 is the exact sum s.d.o.f. for the cases $M \geq 1$ in (**P1**) and (**P2**). Utilizing these results in the context of this two-unicast layered network, we are able to provide a complete sum s.d.o.f. characterization for all two-unicast layered networks in cases A and A'.

For the cases B and B', reference [64] showed that the trivial upper bound of 2 for the sum d.o.f. can be achieved by either obtaining a diagonal end-to-end transfer matrix with non-zero diagonal entries, or by constructing a $2 \times 2 \times 2$ condensed interference network in which the d.o.f.-optimal achievable scheme is based on real interference alignment [66]. For the first scenario, we have secrecy for free, due to the diagonal nature of the end-to-end transfer matrix. For the second scenario, we propose a modified achievable scheme for the $2 \times 2 \times 2$ interference network to achieve the upper bound of 2 for the sum s.d.o.f. The challenge in the equivocation calculation in this case is that we need to provide a precise performance analysis in terms of both reliability and secrecy. In this case, the nodes in the middle layer of the $2 \times 2 \times 2$ interference network perform hard decisions to decode the original channel inputs from the previous layer. If these hard decisions have no error, then due to the special construction of the channel inputs based on interference neutralization and interference alignment, the messages are secure. However, if errors occur during decoding in the middle layer, then the mixed signals containing both messages observed by both destination nodes may leak information. To show the optimality of the proposed achievable scheme, we observe that the message rate scales with $\log P$, but the probability of hard decision error decreases exponentially

fast with P, which makes the information leakage rate negligible at high SNR.

Finally, reference [64] showed that all layered networks in case C can be operated in a time-sharing mode between two networks which belong to cases B and B', i.e., after selecting a temporary node d' in the network, in both modes, we can find a sub-network which has the structure of case B or case B' to transmit 2 sum d.o.f. reliably, in which, node d' is one of the destinations for the first mode, which stores the information and serves as the source node in the second mode. Therefore, on average, we can achieve $\frac{3}{2}$ sum d.o.f. To achieve $\frac{3}{2}$ sum s.d.o.f. for case C, we study all possibilities for the layered network in this case, and find a node to cooperatively jam the unintended receiver to protect the messages.

In Chapter 6, we revisit the Gaussian wiretap channel with M helpers in Chapter 2 (see Figure 1.2). In Chapter 2, we show that the exact s.d.o.f. of the Gaussian wiretap channel with M helpers is $\frac{M}{M+1}$. This result is derived under the assumption that the eavesdropper's CSI is available at the transmitters. In Chapter 6, we show that the same s.d.o.f. can be achieved even when the eavesdropper's CSI is unknown at the legitimate transmitters. This result is practically significant because, generally, it is difficult or impossible to obtain the eavesdropper's CSI. Since the upper bound developed in Chapter 2 is valid for this case also, we thus determine the exact s.d.o.f. of the Gaussian wiretap channel with M helpers with no eavesdropper CSI as $\frac{M}{M+1}$. The achievable scheme in the case of no eavesdropper CSI in Chapter 6 is significantly different than the achievable scheme with eavesdropper CSI developed in Chapter 2.

In particular, in Chapter 2, the legitimate transmitter divides its message into

M sub-messages and sends them on M different *irrational dimensions*. Each one of the helpers sends a cooperative jamming signal. The message signals and the cooperative jamming signals are sent in such a way that: 1) the cooperative jamming signals are aligned at the legitimate receiver in the same irrational dimension, so that they occupy the smallest possible space at the legitimate receiver to enable the decodability of the message signals, and 2) each cooperative jamming signal is aligned exactly in the same irrational dimension with one of the message signals at the eavesdropper to protect it (see Figure 2.2). In Chapter 2, we use insights from [30, 31, 50] to show that, when a cooperative jamming signal is aligned with a message signal in the same irrational dimension at the eavesdropper, this alignment protects the message signal, and limits the information leakage rate to the eavesdropper by a constant which does not depend on the transmit power. Meanwhile, due to the alignment of the cooperative jamming signals in a small space at the legitimate receiver, the information rate to the legitimate receiver can be made to scale with the transmit power. We use this real interference alignment [51, 52] based approach to achieve a s.d.o.f. of $\frac{M}{M+1}$ for *almost all channel gains*, and develop a converse to show that it is in fact the s.d.o.f. capacity.

The achievable scheme in Chapter 6 again divides the message into M sub-messages. Each one of the helpers sends a cooperative jamming signal. As a major difference from the achievable scheme in Chapter 2, in this achievable scheme, the legitimate transmitter also sends a cooperative jamming signal (see Figure 6.1). In this case, the message signals and the cooperative jamming signals are sent in such a way that: 1) all $M+1$ cooperative jamming signals are aligned at the legitimate

receiver in the same irrational dimension, and 2) all cooperative jamming signals span the *entire space* at the eavesdropper to limit the information leakage to the eavesdropper. We use insights from [67], which developed a new achievable scheme that achieved the same s.d.o.f. as in [53] without eavesdropper CSI, to show that the information leakage to the eavesdropper is upper bounded by a function, which can be made arbitrarily small. On the other hand, since the cooperative jamming signals occupy the smallest space at the legitimate receiver, the information rate to the legitimate receiver can be made to scale with the transmit power. In this achievable scheme, we let the legitimate transmitter and the helpers *blindly* cooperative jam the eavesdropper. Because of the inefficiency of *blind* cooperative jamming, in Chapter 6, we need to use more cooperative jamming signals than in Chapter 2, i.e., in Chapter 2 we use a total of M cooperative jamming signals from the helpers, while in Chapter 6 we use $M+1$ cooperative jamming signals, one of which coming from the legitimate transmitter.

In Chapter 7, we study the separability of parallel MAC wiretap channel. Separability, when exists, is useful as it enables us to code separately over parallel channels, and still achieve the optimum overall performance. It is well-known that the parallel single-user channel [68], parallel MAC [56] and parallel BC [69] are all separable, however, the parallel IC is not separable in general [70–73]. In particular, reference [70] studied the two-user one-sided ergodic fading IC and showed that separation can be strictly sub-optimal in certain cases. Reference [71] studied the separability in a parallel Gaussian IC, and showed that the parallel Gaussian IC is not always separable by presenting a specific example where joint encoding over

the parallel channels outperforms individually optimal encoding in each parallel channel. Reference [72] further confirmed the inseparability of the parallel IC by examining the topological IC where the parallel channels correspond to different network topologies some of which had asymmetric connectivity. Recently, reference [73] showed that even symmetric parallel ICs are inseparable by characterizing the capacity region of parallel symmetric linear deterministic ICs.

In Chapter 7, we consider the MAC wiretap channel, which is a combination of a MAC to the legitimate receiver and a MAC to the eavesdropper. The MAC wiretap channel was introduced in [14, 15] and studied further in [16, 18, 30, 34, 35, 74, 75]. Even though, in the absence of any secrecy constraints, MAC is the most well-understood multi-user channel model [68], its wiretap version is significantly more complex. The secrecy capacity region of the MAC wiretap channel is still unknown today, and its s.d.o.f. region has been fully characterized in Chapter 2 and Chapter 4. In Chapter 7, we focus on the separability of the parallel MAC wiretap channel and show that it is not separable in general. Intuitively, this can be attributed to the observation that, even though MAC wiretap channel is composed of MAC legitimate and eavesdropping links, as a whole, it resembles the IC more, as it has two independent transmitters and two independent receivers.

To show the inseparability of the parallel MAC wiretap channel, we construct a specific linear deterministic MAC wiretap channel in each component channel. We find the exact secrecy capacity of each of these component MAC wiretap channels, and then determine the optimum secrecy rates achievable by separate encoding. This step is challenging as the secrecy capacity of MAC wiretap channels is unknown in

general; we provide a specific achievability and converse for the capacity of each of the component channels. We then provide an encoding scheme that codes over the parallel channels which outperforms the optimum separable scheme.

Next, we consider the parallel Gaussian MAC wiretap channel. Since the secrecy capacity region of the general MAC wiretap channel, including the Gaussian MAC wiretap channel, is unknown but the exact s.d.o.f. region is known due to Chapter 4, we investigate the sum s.d.o.f. of parallel Gaussian MAC wiretap channels and prove that it is inseparable. This implies the inseparability of the secrecy region as well. Next, we observe that, if the different channel gains which give rise to different parallel channels are drawn independently from continuous distributions, then the channel gain configurations which give rise to inseparability fall into a set with zero Lebesgue measure. To confirm this observation, and prove the almost sure s.d.o.f. separability of parallel Gaussian MAC wiretap channels, we consider the *flat channel*, where we put the individual n channel uses of each component channel into a single $2n$ channel uses. We utilize the converse techniques in Chapter 2 and Chapter 4 to show the separability in this case. Finally, we note that, while inseparability in s.d.o.f. implies inseparability in the secrecy capacity, separability in s.d.o.f. does not imply separability in secrecy capacities. The almost sure separability proved for the parallel Gaussian MAC wiretap channel in Chapter 7 holds only for the s.d.o.f., which is the pre-log factor of the secrecy capacity, and is a weaker measure of separability.

In Chapter 8, we study a secrecy game on interference networks. In the IC, multiple users share the transmission medium, and simultaneously wish to have

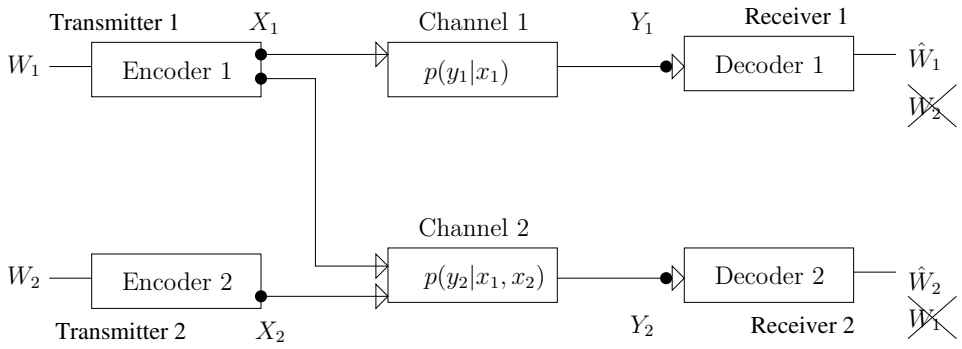


Figure 1.10: One-sided IC with confidential messages.

reliable communication with their respective receivers. In order to achieve a particular rate point on the capacity region of the IC, the transmitter-receiver pairs need to jointly choose encoding and decoding schemes, and cooperate to agree on the particular operating rate point, and coordinate their actions, e.g., time-sharing.

In actual interference networks, such kinds of cooperations may not be practical or agreeable by the users. It is reasonable to assume that all transmitter-receiver pairs in the network are selfish and rational. Moreover, each pair is only interested in transmitting their messages at the maximum reliable rate. Consequently, the information-theoretic capacity region may not be fully achievable. Reference [76] made this intuition precise by considering the IC from a game-theoretic point of view, and found the Nash equilibrium operating points on the capacity region, especially focusing on the binary deterministic IC and the Gaussian IC. Taking the reliable communication rate for each transmitter as its payoff function, [76] showed that, in a non-cooperative game, two transmitters agree only on a subset of the capacity region of the IC, which forms the set of Nash equilibria.

In Chapter 8, we focus on the two-user one-sided IC with confidential messages,

in which one transmitter-receiver pair is interference-free as shown in Figure 1.10. The best known achievable secrecy rate region for the IC with confidential messages was developed in [5]. As in the case of ICs without secrecy constraints, in [5], the two transmitter-receiver pairs need to jointly choose encoding and decoding schemes and further cooperate and coordinate their actions to achieve a secrecy rate pair in this region. In addition, the achievable scheme in [5] requires that the parties trust each other in that they will not unilaterally change their encoding-decoding schemes. Hence, even if it was known, secrecy capacity region might not be sufficient to understand the adversarial relationship in this network. Reference [77], addressed the issue of trust. In [77], the transmitters can deviate from their transmit strategies. In their definition of robust-secrecy [77], a transmitter can deviate from its strategy, however, arbitrary deviations are not allowed; a transmitter can only deviate to a strategy if the new strategy does not injure the performance of the other transmitter-receiver pair in terms of reliability. When the transmitters are selfish, such kind of behavior may not be guaranteed. Selfish transmitters would care only about their own reliability and secrecy of their own messages. Such selfish transmitters may choose any strategy to maximize the secrecy rate of their own private message, which may hurt the other user's performance.

To develop a model to characterize the adversarial relationship between the two pairs, we only assume that the two transmitter-receiver pairs are selfish and rational; other than these two, they are free to choose any transmission strategy to maximize their own payoff. Under these assumptions, in Chapter 8, we give a formal definition of the game on ICs with confidential messages and define the

Nash equilibrium in the secrecy rate region. We first consider the case where the payoff function is the reliable secrecy rate of each user. We analyze the binary deterministic IC for this payoff function. This analysis reveals that some of the Nash equilibrium secrecy rate pairs are achieved only by self-jamming of a transmitter of its own receiver. This hurts the eavesdropping ability of its own receiver, which in fact is one of the interests of the receivers. Among all the strategies achieving the same secrecy rate, a transmitter-receiver pair is more likely to choose the one that allows the receiver to more strongly eavesdrop on the other pair. To overcome this difficulty, we propose a refinement to the equilibrium. Specifically, we modify the payoff function by incorporating an information leakage measure to it in addition to the secure reliable rate. We find the Nash equilibria with both payoff functions.

In Chapter 9, we provide conclusions of this dissertation.

Chapter 2

Sum Secure Degrees of Freedom of One-hop Wireless Networks

2.1 Introduction

In this chapter, we study the sum s.d.o.f. of one-hop wireless networks. We start with the simplest channel model toward this goal, which is the Gaussian wiretap channel with one helper. The secrecy capacity of the canonical Gaussian wiretap channel does not scale with the transmit power, and hence, the s.d.o.f. of the Gaussian wiretap channel with no helpers is zero. It has been known that a strictly positive s.d.o.f. can be obtained in the Gaussian wiretap channel by using a helper which sends structured cooperative signals. In this chapter, we first show that the exact s.d.o.f. of the Gaussian wiretap channel with a helper is $\frac{1}{2}$. Our achievable scheme is based on real interference alignment and cooperative jamming, which renders the message signal and the cooperative jamming signal *separable* at the legitimate receiver, but *aligns* them perfectly at the eavesdropper preventing any reliable decoding of the message signal. Our converse is based on two key lemmas. The first lemma quantifies the *secrecy penalty* by showing that the net effect of an eavesdropper on the system is that it eliminates one of the independent channel inputs. The second lemma quantifies the *role of a helper* by developing a direct relationship between the cooperative jamming signal of a helper and the message rate of the legitimate transmitter.

Channel model	**(Sum) s.d.o.f.**
Wiretap channel with one helper	$\frac{1}{2}$
Wiretap channel with M helpers	$\frac{M}{M+1}$
Broadcast channel with CM and M helpers	1
Two-user interference channel with CM	$\frac{2}{3}$
Two-user interference channel with CM and M helpers	1
K-user multiple access wiretap channel	$\frac{K(K-1)}{K(K-1)+1}$

Table 2.1: Summary of the main results of this chapter ("CM" stands for confidential messages).

We extend this result to the case of M helpers, and show that the exact s.d.o.f. in this case is $\frac{M}{M+1}$. We then generalize this approach to more general network structures with *multiple messages*. We show that the sum s.d.o.f. of the Gaussian BC with confidential messages and M helpers is 1, the sum s.d.o.f. of the two-user IC with confidential messages is $\frac{2}{3}$, the sum s.d.o.f. of the two-user IC with confidential messages and M helpers is 1, and the sum s.d.o.f. of the K-user MAC wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$.

Table 2.1 summarizes the main results of this chapter in a tabular form.

2.2 System Model and Definitions

In this chapter, we consider four fundamental channel models: wiretap channel with helpers, BC with confidential messages and helpers, two-user IC with confidential messages and helpers, and MAC wiretap channel. In this section, we give the channel models and relevant definitions. All the channels are additive white Gaussian noise

(AWGN) channels. All the channel gains are time-invariant, and independently drawn from continuous distributions.

2.2.1 Wiretap Channel with Helpers

The Gaussian wiretap channel with helpers (see Figure 1.2) is defined by,

$$Y_1 = h_1 X_1 + \sum_{j=2}^{M+1} h_j X_j + N_1 \tag{2.1}$$

$$Y_2 = g_1 X_1 + \sum_{j=2}^{M+1} g_j X_j + N_2 \tag{2.2}$$

where Y_1 is the channel output of the legitimate receiver, Y_2 is the channel output of the eavesdropper, X_1 is the channel input of the legitimate transmitter, X_i, for $i = 2, \ldots, M+1$, are the channel inputs of the M helpers, h_i is the channel gain of the ith transmitter to the legitimate receiver, g_i is the channel gain of the ith transmitter to the eavesdropper, and N_1 and N_2 are two independent zero-mean unit-variance Gaussian random variables. All channel inputs satisfy average power constraints, $\mathrm{E}[X_i^2] \leq P$, for $i = 1, \ldots, M+1$.

Transmitter 1 intends to send a message W, uniformly chosen from a set $\mathcal{W}$, to the legitimate receiver (receiver 1). The rate of the message is $R \triangleq \frac{1}{n} \log |\mathcal{W}|$, where n is the number of channel uses. Transmitter 1 uses a stochastic function $f : \mathcal{W} \to \mathbf{X}_1$ to encode the message, where $\mathbf{X}_1 \triangleq X_1^n$ is the n-length channel input.[1] The legitimate receiver decodes the message as $\hat{W}$ based on its observation $\mathbf{Y}_1$. A

[1] We use boldface letters to denote n-length vector signals, e.g., $\mathbf{X}_1 \triangleq X_1^n$, $\mathbf{Y}_1 \triangleq Y_1^n$, $\mathbf{Y}_2 \triangleq Y_2^n$, etc.

secrecy rate R is said to be achievable if for any $\epsilon > 0$ there exists an n-length code such that receiver 1 can decode this message reliably, i.e., the probability of decoding error is less than ϵ,

$$\Pr\left[W \neq \hat{W}\right] \leq \epsilon \tag{2.3}$$

and the message is kept information-theoretically secure against the eavesdropper,

$$\frac{1}{n}H(W|\mathbf{Y}_2) \geq \frac{1}{n}H(W) - \epsilon \tag{2.4}$$

i.e., that the uncertainty of the message W, given the observation $\mathbf{Y}_2$ of the eavesdropper, is almost equal to the entropy of the message. The supremum of all achievable secrecy rates is the secrecy capacity C_s and the s.d.o.f., D_s, is defined as

$$D_s \triangleq \lim_{P\to\infty} \frac{C_s}{\frac{1}{2}\log P} \tag{2.5}$$

Note that $D_s \leq 1$ is an upper bound. To avoid trivial cases, we assume that $h_1 \neq 0$ and $g_1 \neq 0$. Without the independent helpers, i.e., $M = 0$, the secrecy capacity of the Gaussian wiretap channel is known [4]

$$C_s = \frac{1}{2}\log\left(1 + h_1^2 P\right) - \frac{1}{2}\log\left(1 + g_1^2 P\right) \tag{2.6}$$

and from (2.5) the s.d.o.f. is zero. Therefore, we assume $M \geq 1$. If there exists a j ($j = 2, \ldots, M+1$) such that $h_j = 0$ and $g_j \neq 0$, then a lower bound of 1

s.d.o.f. can be obtained for this channel by letting this helper jam the eavesdropper by i.i.d. Gaussian noise of power P and keeping all other helpers silent. This lower bound matches the upper bound, giving the s.d.o.f. On the other hand, if there exists a j ($j = 2, \ldots, M+1$) such that $h_j \neq 0$ and $g_j = 0$, then this helper can be removed from the channel model without affecting the secure d.o.f. Therefore, in the rest of the chapter, for the case of Gaussian wiretap channel with M helpers, we assume that $M \geq 1$ and $h_j \neq 0$ and $g_j \neq 0$ for all $j = 1, \cdots, M+1$.

2.2.2 Broadcast Channel with Confidential Messages and Helpers

The Gaussian BC with confidential messages and helpers (see Figure 1.3 for one helper) is defined by,

$$Y_1 = h_1 X_1 + \sum_{j=2}^{M+1} h_j X_j + N_1 \tag{2.7}$$

$$Y_2 = g_1 X_1 + \sum_{j=2}^{M+1} g_j X_j + N_2 \tag{2.8}$$

In this model, transmitter 1 has two independent messages, W_1 and W_2, intended for receivers 1 and 2, respectively. Messages W_1 and W_2 are independently and uniformly chosen from sets $\mathcal{W}_1$ and $\mathcal{W}_2$, respectively. The rates of the messages are $R_1 \stackrel{\triangle}{=} \frac{1}{n} \log |\mathcal{W}_1|$ and $R_2 \stackrel{\triangle}{=} \frac{1}{n} \log |\mathcal{W}_2|$. Transmitter 1 uses a stochastic function $f : \mathcal{W}_1 \times \mathcal{W}_2 \to \mathbf{X}_1$ to encode the messages. The messages are said to be confidential if only the intended receiver can decode each message, i.e., each receiver is an eavesdropper for the other. Transmitters $2, \cdots, M+1$ are the independent helpers.

Similar to (2.3) and (2.4), we define the reliability and secrecy of the messages as,

$$\Pr[W_1 \neq \hat{W}_1] \leq \epsilon \tag{2.9}$$

$$\Pr[W_2 \neq \hat{W}_2] \leq \epsilon \tag{2.10}$$

$$\frac{1}{n}H(W_1|\mathbf{Y}_2) \geq \frac{1}{n}H(W_1) - \epsilon \tag{2.11}$$

$$\frac{1}{n}H(W_2|\mathbf{Y}_1) \geq \frac{1}{n}H(W_2) - \epsilon \tag{2.12}$$

The sum s.d.o.f. for this channel model is defined as

$$D_{s,\Sigma} \stackrel{\triangle}{=} \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \tag{2.13}$$

where the supremum is over all achievable secrecy rate pairs (R_1, R_2).

2.2.3 Interference Channel with Confidential Messages and Helpers

The two-user Gaussian IC with confidential messages and helpers (see Figure 1.5) is defined by,

$$Y_1 = h_{1,1}X_1 + h_{2,1}X_2 + \sum_{j=3}^{M+2} h_{j,1}X_j + N_1 \tag{2.14}$$

$$Y_2 = h_{1,2}X_1 + h_{2,2}X_2 + \sum_{j=3}^{M+2} h_{j,2}X_j + N_2 \tag{2.15}$$

where $X_1, X_2, \cdots, X_{M+2}, N_1$ and N_2 are mutually independent.

One special, but important, case is the two-user Gaussian IC with confidential

messages, i.e., $M = 0$, which is shown in Figure 1.4 and defined by,

$$Y_1 = h_{1,1}X_1 + h_{2,1}X_2 + N_1 \tag{2.16}$$

$$Y_2 = h_{1,2}X_1 + h_{2,2}X_2 + N_2 \tag{2.17}$$

In the two-user IC with confidential messages, each transmitter wishes to send a confidential message to its own receiver. Transmitter 1 has message W_1 uniformly chosen from set $\mathcal{W}_1$. The rate of the message is $R_1 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_1|$. Transmitter 1 uses a stochastic function $f_1 : \mathcal{W}_1 \to \mathbf{X}_1$ to encode the message. Similarly, transmitter 2 has message W_2 (independent of W_1) uniformly chosen from set $\mathcal{W}_2$. The rate of the message is $R_2 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_2|$. Transmitter 2 uses a stochastic function $f_2 : \mathcal{W}_2 \to \mathbf{X}_2$ to encode the message. The messages are said to be confidential if only the intended receiver can decode each message, i.e., each receiver is an eavesdropper for the other. Transmitters $3, \cdots, M+2$ are the independent helpers. Similar to (2.3) and (2.4), we define the reliability and secrecy of the messages as,

$$\Pr[W_1 \neq \hat{W}_1] \leq \epsilon \tag{2.18}$$

$$\Pr[W_2 \neq \hat{W}_2] \leq \epsilon \tag{2.19}$$

$$\frac{1}{n}H(W_1|\mathbf{Y}_2) \geq \frac{1}{n}H(W_1) - \epsilon \tag{2.20}$$

$$\frac{1}{n}H(W_2|\mathbf{Y}_1) \geq \frac{1}{n}H(W_2) - \epsilon \tag{2.21}$$

The sum s.d.o.f. for this channel model is defined as

$$D_{s,\Sigma} \stackrel{\triangle}{=} \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \tag{2.22}$$

where the supremum is over all achievable secrecy rate pairs (R_1, R_2).

2.2.4 Multiple Access Wiretap Channel

The K-user Gaussian MAC wiretap channel (see Figure 1.6) is defined by,

$$Y_1 = \sum_{i=1}^{K} h_i X_i + N_1 \tag{2.23}$$

$$Y_2 = \sum_{i=1}^{K} g_i X_i + N_2 \tag{2.24}$$

In this channel model, each transmitter i has a message W_i intended for the legitimate receiver whose channel output is Y_1. All of the messages are independent. Message W_i is uniformly chosen from set $\mathcal{W}_i$. The rate of message i is $R_i \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_i|$. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ to encode its message. All of the messages are needed to be kept secret from the eavesdropper, whose channel output is Y_2.

Similar to (2.3), the reliability of the messages is defined by

$$\Pr\left[(W_1, \cdots, W_K) \neq (\hat{W}_1, \cdots, \hat{W}_K)\right] \leq \epsilon \tag{2.25}$$

and similar to (2.4) the secrecy constraint (for the entire message set) is defined as

$$\frac{1}{n}H(W_1, W_2, \cdots, W_K|\mathbf{Y}_2) \geq \frac{1}{n}H(W_1, W_2, \cdots, W_K) - \epsilon \tag{2.26}$$

Note that this definition implies the secrecy for any subset of the messages, including individual messages, i.e.,

$$\begin{aligned}\frac{1}{n}I(W_{\mathbf{S}}; \mathbf{Y}_2) &= \frac{1}{n}I(W_1, W_2, \cdots, W_K; \mathbf{Y}_2) - \frac{1}{n}I(W_{\mathbf{S}^c}; \mathbf{Y}_2|W_{\mathbf{S}}) &(2.27)\\ &\leq \frac{1}{n}I(W_1, W_2, \cdots, W_K; \mathbf{Y}_2) &(2.28)\\ &\leq \epsilon &(2.29)\end{aligned}$$

for any $\mathbf{S} \subset \{1, \cdots, K\}$. The sum s.d.o.f. for this channel model is defined as

$$D_{s,\Sigma} \stackrel{\triangle}{=} \lim_{P\to\infty} \sup \frac{\sum_{i=1}^{K} R_i}{\frac{1}{2}\log P} \tag{2.30}$$

where the supremum is over all achievable secrecy rate tuples $(R_1, \cdots, R_K)$.

2.3 General Converse Results and Preliminaries

In this section, we give two lemmas, Lemmas 2.1 and 2.2, that will be used in the converse proofs and another lemma, Lemma 2.3, that will be used in the achievability proofs in later sections.

2.3.1 Secrecy Penalty

Consider the channel model formulated in Section 2.2.1, where transmitter 1 wishes to have secure communication with receiver 1, in the presence of an eavesdropper (receiver 2) and M helpers (transmitters 2 through $M+1$). We propose a general upper bound for the secrecy rate between transmitter 1 and receiver 1 by working with n-letter signals, and introducing new mutually independent Gaussian random variables $\{\tilde{N}_i\}_{i=1}^{M}$ which are zero-mean and of variance $\tilde{\sigma}_i^2$ where $\tilde{\sigma}_i^2 < \min(1/h_i^2, 1/g_i^2)$, and are independent of all other random variables. Each vector $\tilde{\mathbf{N}}_i$ is an i.i.d. sequence of $\tilde{N}_i$.

In the following lemma, we give a general upper bound for the secrecy rate. This lemma states that the secrecy rate of the legitimate pair is upper bounded by the difference of the sum of differential entropies of all channel inputs (perturbed by small noise) and the differential entropy of the eavesdropper's observation; see (2.31). This upper bound can further be interpreted as follows: If we consider the eavesdropper's observation as the *secrecy penalty,* then the secrecy penalty is tantamount to the elimination of one of the channel inputs in the system; see (2.32).

Lemma 2.1 *The secrecy rate of the legitimate pair is upper bounded as*

$$nR \leq \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc \tag{2.31}$$

$$\leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{2.32}$$

where $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$ *for* $i = 1, \cdots, M+1$, *and* $\tilde{\mathbf{N}}_i$ *is an i.i.d. sequence (in time) of*

random variables $\tilde{N}_i$ which are independent Gaussian random variables with zero-mean and variance $\tilde{\sigma}_i^2$ with $\tilde{\sigma}_i^2 < \min(1/h_i^2, 1/g_i^2)$. In addition, c and c' are constants which do not depend on P, and $j \in \{1, \cdots, M+1\}$ can be arbitrary.

Proof: We use notation c_i, for $i \geq 1$, to denote constants which are independent of the power P. We start as follows:

$$nR = H(W) = H(W|\mathbf{Y}_1) + I(W; \mathbf{Y}_1) \tag{2.33}$$

$$\leq I(W; \mathbf{Y}_1) + nc_1 \tag{2.34}$$

$$\leq I(W; \mathbf{Y}_1) - I(W; \mathbf{Y}_2) + nc_2 \tag{2.35}$$

where we used Fano's inequality and the secrecy constraint in (2.4). By providing $\mathbf{Y}_2$ to receiver 1, we further upper bound nR as

$$nR \leq I(W; \mathbf{Y}_1, \mathbf{Y}_2) - I(W; \mathbf{Y}_2) + nc_2 \tag{2.36}$$

$$= I(W; \mathbf{Y}_1|\mathbf{Y}_2) + nc_2 \tag{2.37}$$

$$= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2, W) + nc_2 \tag{2.38}$$

$$\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_3 \tag{2.39}$$

where (2.39) is due to

$$h(\mathbf{Y}_1|\mathbf{Y}_2, W) \geq h(\mathbf{Y}_1|\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_{M+1}, \mathbf{Y}_2, W) \tag{2.40}$$

$$= h(\mathbf{N}_1|\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_{M+1}, \mathbf{Y}_2, W) \tag{2.41}$$

$$= h(\mathbf{N}_1) \tag{2.42}$$

$$= \frac{n}{2} \log 2\pi e \tag{2.43}$$

which is independent of P. Here, (2.42) is due to the fact that $\mathbf{N}_1$ is independent of $(\mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_{M+1}, \mathbf{Y}_2, W)$.

In the next step, we introduce random variables $\tilde{\mathbf{X}}_i$ which are noisy versions of

the channel inputs $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$ for $i = 1, \cdots, M+1$. Thus, starting from (2.39),

$$
\begin{aligned}
nR &\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_3 && (2.44)\\
&= h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && (2.45)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2) \\
&\quad - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}|\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_3 && (2.46)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2) \\
&\quad - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}|\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_{M+1}) - h(\mathbf{Y}_2) + nc_3 && (2.47)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2) \\
&\quad - h(\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \cdots, \tilde{\mathbf{N}}_{M+1}|\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_{M+1}) - h(\mathbf{Y}_2) + nc_3 && (2.48)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \cdots, \tilde{\mathbf{N}}_{M+1}) - h(\mathbf{Y}_2) + nc_3 \\
& && (2.49)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}, \mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_4 && (2.50)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) + h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) - h(\mathbf{Y}_2) + nc_4 && (2.51)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) - h(\mathbf{Y}_2) + nc_5 && (2.52)\\
&= \sum_{i=1}^{M+1} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_2) + nc_5 && (2.53)
\end{aligned}
$$

where (2.49) is due to the fact that $(\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \cdots, \tilde{\mathbf{N}}_{M+1})$ is independent of $(\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_{M+1})$ and (2.52) is due to $h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) \leq nc_6$. The intuition behind this is that, given all (slightly noisy versions of) the channel inputs, (at high SNR) the channel outputs can be *reconstructed*.[2] To show this formally, we

[2]By *reconstructed*, we mean that the conditional differential entropy

have

$$
\begin{aligned}
&h(\mathbf{Y}_1, \mathbf{Y}_2 | \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) \\
&\quad \le h(\mathbf{Y}_1 | \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) + h(\mathbf{Y}_2 | \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1}) && (2.54) \\
&\quad = h\left(\sum_{i=1}^{M+1} h_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1} \right) \\
&\qquad + h\left(\sum_{i=1}^{M+1} g_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1} \right) && (2.55) \\
&\quad = h\left(-\sum_{i=1}^{M+1} h_i \tilde{\mathbf{N}}_i + \mathbf{N}_1 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1} \right) \\
&\qquad + h\left(-\sum_{i=1}^{M+1} g_i \tilde{\mathbf{N}}_i + \mathbf{N}_2 \middle| \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1} \right) && (2.56) \\
&\quad \le h\left(-\sum_{i=1}^{M+1} h_i \tilde{\mathbf{N}}_i + \mathbf{N}_1 \right) + h\left(-\sum_{i=1}^{M+1} g_i \tilde{\mathbf{N}}_i + \mathbf{N}_2 \right) && (2.57) \\
&\quad \stackrel{\triangle}{=} nc_6 && (2.58)
\end{aligned}
$$

which completes the proof of (2.31).

Finally, we show (2.32). To this end, fixing a j, which can be arbitrary, we express $\mathbf{Y}_2$ in a stochastically equivalent form $\tilde{\mathbf{Y}}_2$, i.e.,

$$
\mathbf{Y}_2 = g_j \mathbf{X}_j + \sum_{i=1, i \neq j}^{M+1} g_i \mathbf{X}_i + \mathbf{N}_2 \tag{2.59}
$$

$$
\tilde{\mathbf{Y}}_2 = g_j \tilde{\mathbf{X}}_j + \sum_{i=1, i \neq j}^{M+1} g_i \mathbf{X}_i + \mathbf{N}_2' \tag{2.60}
$$

have the same distribution, where $\mathbf{N}_2'$ is an i.i.d. sequence of a random variable N_2' which is Gaussian with zero-mean and variance $(1 - g_j^2 \tilde{\sigma}_j^2)$, and is independent of

$h(\mathbf{Y}_1, \mathbf{Y}_2 | \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_{M+1})$ does not grow with P.

all other random variables. Then, we have

$$h(\mathbf{Y}_2) = h(\tilde{\mathbf{Y}}_2) \tag{2.61}$$

$$= h\left(g_j\tilde{\mathbf{X}}_j + \sum_{i=1,i\neq j}^{M+1} g_i\mathbf{X}_i + \mathbf{N}_2'\right) \tag{2.62}$$

$$\geq h\left(g_j\tilde{\mathbf{X}}_j\right) \tag{2.63}$$

$$= n\log|g_j| + h(\tilde{\mathbf{X}}_j) \tag{2.64}$$

where (2.63) is due to the differential entropy version of [68, Problem 2.14]. Substituting this into (2.31) gives us (2.32). □

2.3.2 Role of a Helper

Intuitively, a cooperative jamming signal from a helper may potentially increase the secrecy of the legitimate transmitter-receiver pair by creating extra equivocation at the eavesdropper. However, if the helper creates too much equivocation, it may also hurt the decoding performance of the legitimate receiver. Since the legitimate receiver needs to decode message W by observing $\mathbf{Y}_1$, there must exist a constraint on the cooperative jamming signal of the helper. To this end, we develop a constraint on the differential entropy of (the noisy version of) the cooperative jamming signal of any given helper, helper j in (2.65), in terms of the differential entropy of the legitimate user's channel output and the message rate $H(W)$, in the following lemma. The inequality in this lemma, (2.65), can alternatively be interpreted as an upper bound on the message rate, i.e., on $H(W)$, in terms of the difference of the

differential entropies of the channel output of the legitimate receiver and the channel input of the jth helper; in particular, the higher the differential entropy of the cooperative jamming signal the lower this upper bound will be. This motivates not using i.i.d. Gaussian cooperative jamming signals which have the highest differential entropy.

Finally, we note as an aside that, since this upper bound is derived based on the reliability of the legitimate user's decoding (not involving any secrecy constraints), it can be used in d.o.f. calculations in settings not involving secrecy. We show an application of this lemma in a non-secrecy context by developing an alternative proof for the multiplexing gain of the K-user Gaussian IC, which was originally proved in [54], in Appendix 2.12.1.

Lemma 2.2 *For reliable decoding at the legitimate receiver, the differential entropy of the input signal of helper j, $\mathbf{X}_j$, must satisfy*

$$h(\mathbf{X}_j + \tilde{\mathbf{N}}) \leq h(\mathbf{Y}_1) - H(W) + nc \tag{2.65}$$

where c is a constant which does not depend on P, and $\tilde{N}$ is a new Gaussian noise independent of all other random variables with $\sigma^2_{\tilde{N}} < \frac{1}{h_j^2}$, and $\tilde{\mathbf{N}}$ is an i.i.d. sequence of $\tilde{N}$.

Proof: To reliably decode the message at the legitimate receiver, we must

have

$$nR = H(W) \leq I(\mathbf{X}_1; \mathbf{Y}_1) \tag{2.66}$$

$$= h(\mathbf{Y}_1) - h(\mathbf{Y}_1|\mathbf{X}_1) \tag{2.67}$$

$$= h(\mathbf{Y}_1) - h\left(\sum_{i=2}^{M+1} h_i \mathbf{X}_i + \mathbf{N}_1\right) \tag{2.68}$$

$$\leq h(\mathbf{Y}_1) - h\left(h_j \mathbf{X}_j + \mathbf{N}_1\right) \tag{2.69}$$

$$\leq h(\mathbf{Y}_1) - h\left(h_j \mathbf{X}_j + h_j \tilde{\mathbf{N}}\right) \tag{2.70}$$

$$= h(\mathbf{Y}_1) - h\left(\mathbf{X}_j + \tilde{\mathbf{N}}\right) + nc \tag{2.71}$$

where (2.69) and (2.70) are due to the differential entropy version of [68, Problem 2.14]. In going from (2.69) to (2.70), we also used the infinite divisibility of Gaussian distribution and expressed $\mathbf{N}_1$ in its stochastically equivalent form as $\mathbf{N}_1 = h_j \tilde{\mathbf{N}} + \mathbf{N}'$ where $\mathbf{N}'$ is an i.i.d. sequence of random variable N' which is Gaussian with zero-mean and appropriate variance, and which is independent of all other random variables. $\square$

Note that, although we develop the inequality in (2.65) for the message of transmitter-receiver pair 1, this result also holds for the message of any transmitter-receiver pair in a multiple-message setting provided that the zero-mean Gaussian noise $\tilde{N}$ has an appropriately small variance.

2.3.3 Real Interference Alignment

In this subsection, we review pulse amplitude modulation (PAM) and real interference alignment [51, 52], similar to the review in [53, Section III]. The purpose of this subsection is to illustrate that by using real interference alignment, the transmission rate of a PAM scheme can be made to approach the Shannon achievable rate at high SNR. This provides a universal and convenient way to design capacity-achieving signalling schemes at high SNR by using PAM for different channel models as will be done in later sections.

2.3.3.1 Pulse Amplitude Modulation

For a point-to-point scalar Gaussian channel,

$$Y = X + Z \tag{2.72}$$

with additive Gaussian noise Z of zero-mean and variance σ^2, and an input power constraint $\mathrm{E}[X^2] \leq P$, assume that the input symbols are drawn from a PAM constellation,

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{2.73}$$

where Q is a positive integer and a is a real number to normalize the transmit power. Note that, a is also the minimum distance $d_{min}(C)$ of this constellation, which has

the probability of error

$$\Pr(e) = \Pr\left[X \neq \hat{X}\right] \leq \exp\left(-\frac{d_{min}^2}{8\sigma^2}\right) = \exp\left(-\frac{a^2}{8\sigma^2}\right) \tag{2.74}$$

where $\hat{X}$ is an estimate for X obtained by choosing the closest point in the constellation $C(a, Q)$ based on observation Y.

The transmission rate of this PAM scheme is

$$R = \log(2Q + 1) \tag{2.75}$$

since there are $2Q + 1$ signalling points in the constellation. For any small enough $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2}}$ and $a = \gamma P^{\frac{\delta}{2}}$, where γ is a constant independent of P, then

$$\Pr(e) \leq \exp\left(-\frac{\gamma^2 P^{\delta}}{8\sigma^2}\right) \qquad \text{and} \qquad R \geq \frac{1-\delta}{2}\log P \tag{2.76}$$

and we can have $\Pr(e) \to 0$ and $R \to \frac{1}{2}\log P$ as $P \to \infty$. That is, we can have reliable communication at rates approaching $\frac{1}{2}\log P$.

Note that the PAM scheme has small probability of error (i.e., reliability) only when P goes to infinity. For arbitrary P, the probability of error $\Pr(e)$ is a finite number. Similar to the steps in [52, 78], we connect the PAM transmission rate to the Shannon rate in the following derivation. We note that Shannon rate of $I(X;Y)$

is achieveable with arbitrary reliability using a random codebook:

$$R' = I(X;Y) \tag{2.77}$$

$$\geq I(X;\hat{X}) \tag{2.78}$$

$$= H(X) - H(X|\hat{X}) \tag{2.79}$$

$$= \log(2Q+1) - H(X|\hat{X}) \tag{2.80}$$

$$\geq \log(2Q+1) - 1 - \Pr(e)\log(2Q+1) \tag{2.81}$$

$$\geq \Big[1 - \Pr(e)\Big]\frac{1-\delta}{2}\log P - 1 \tag{2.82}$$

where we use the Markov chain $X \to Y \to \hat{X}$ and bound $H(X|\hat{X})$ using Fano's inequality. Therefore, we can achieve the rate in (2.82) with arbitrary reliability, where for any fixed P, $\Pr(e)$ in (2.82) is the probability of error of the PAM scheme given in (2.76), which is a well-defined function of P. For a finite P, while $\Pr(e)$ may not be arbitrarily small, the rate achieved in (2.82), which is smaller than the rate of PAM in (2.75), is achieved arbitrarily reliably. We finally note that as P goes to infinity $\Pr(e)$ goes to zero exponentially, and from (2.82), both PAM transmission rate and the Shannon achievable rate have the same asymptotical performance, i.e., PAM transmission rate has 1 Shannon d.o.f.

2.3.3.2 Real Interference Alignment

This PAM scheme for the point-to-point scalar channel can be generalized to multiple data streams. Let the transmit signal be

$$x = \mathbf{a}^T \mathbf{b} = \sum_{i=1}^{L} a_i b_i \tag{2.83}$$

where $a_1, \ldots, a_L$ are rationally independent real numbers[3] and each b_i is drawn independently from the constellation $C(a, Q)$ in (2.73). The real value x is a combination of L data streams, and the constellation observed at the receiver consists of $(2Q+1)^L$ signal points.

By using the Khintchine-Groshev theorem of Diophantine approximation in number theory, [51, 52] bounded the minimum distance d_{min} of points in the receiver's constellation: For any $\delta > 0$, there exists a constant k_δ, such that

$$d_{min} \geq \frac{k_\delta a}{Q^{L-1+\delta}} \tag{2.84}$$

for almost all rationally independent $\{a_i\}_{i=1}^{L}$, except for a set of Lebesgue measure zero. Since the minimum distance of the receiver constellation is lower bounded, with proper choice of a and Q, the probability of error can be made arbitrarily small, with rate R approaching $\frac{1}{2}\log P$. This result is stated in the following lemma, as in [53, Proposition 3].

Lemma 2.3 ([51, 52]) *For any small enough $\delta > 0$, there exists a positive constant*

[3] $a_1, \ldots, a_L$ are rationally independent if whenever $q_1, \ldots, q_L$ are rational numbers then $\sum_{i=1}^{L} q_i a_i = 0$ implies $q_i = 0$ for all i.

γ, which is independent of P, such that if we choose

$$Q = P^{\frac{1-\delta}{2(L+\delta)}} \qquad \textit{and} \qquad a = \gamma \frac{P^{\frac{1}{2}}}{Q} \tag{2.85}$$

then the average power constraint is satisfied, i.e., $E[X^2] \leq P$, and for almost all $\{a_i\}_{i=1}^{L}$, except for a set of Lebesgue measure zero, the probability of error is bounded by

$$\Pr(e) \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{2.86}$$

where η_γ is a positive constant which is independent of P.

Furthermore, as a simple extension, if b_i are sampled independently from different constellations $C_i(a, Q_i)$, the lower bound in (2.84) can be modified as

$$d_{min} \geq \frac{k_\delta a}{(\max_i Q_i)^{L-1+\delta}} \tag{2.87}$$

2.4 Wiretap Channel with One Helper

In this section, we consider the Gaussian wiretap channel with one helper as formulated in Section 2.2.1 for the case $M = 1$. In this section, we will show that the s.d.o.f. is $\frac{1}{2}$ for almost all channel gains as stated in the following theorem. The converse follows from the general secrecy penalty upper bound in Section 2.3.1 and the cooperative jamming signal upper bound in Section 2.3.2. The achievability is based on cooperative jamming with discrete signaling and real interference alignment.

Theorem 2.1 *The s.d.o.f. of the Gaussian wiretap channel with one helper is $\frac{1}{2}$ for*

almost all channel gains.

2.4.1 Converse

We start with (2.32) of Lemma 2.1 with $M = 1$ and by choosing $j = 1$,

$$nR \leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{2.88}$$

$$= h(\tilde{\mathbf{X}}_2) + nc' \tag{2.89}$$

$$\leq h(\mathbf{Y}_1) - H(W) + nc_7 \tag{2.90}$$

$$\leq \frac{n}{2} \log P - H(W) + nc_8 \tag{2.91}$$

where (2.90) is due to Lemma 2.2. By noting $H(W) = nR$ and using (2.5), (2.91) implies that

$$D_s \leq \frac{1}{2} \tag{2.92}$$

which concludes the converse part of the theorem.

2.4.2 Achievable Scheme

To show the achievability by interference alignment, we slightly change the notation. Let $\bar{X}_1 \triangleq g_1 X_1$, $\bar{X}_2 \triangleq g_2 X_2$, $\alpha \triangleq h_1/g_1$, and $\beta \triangleq h_2/g_2$. Then, the channel model

becomes

$$Y_1 = \alpha \bar{X}_1 + \beta \bar{X}_2 + N_1 \tag{2.93}$$

$$Y_2 = \bar{X}_1 + \bar{X}_2 + N_2 \tag{2.94}$$

Here $\bar{X}_1$ is the input signal carrying the message W of the legitimate transmitter and $\bar{X}_2$ is the cooperative jamming signal from the helper. Our goal is to properly design $\bar{X}_1$ and $\bar{X}_2$ such that they are distinguishable at the legitimate receiver, meanwhile they align together at the eavesdropper. To prevent decoding of the message signal at the eavesdropper, we need to make sure that the cooperative jamming signal occupies the same *dimensions* as the message signal at the eavesdropper; on the other hand, we need to make sure that the legitimate receiver is able to decode $\bar{X}_2$, which in fact, is not useful. Intuitively, secrecy penalty is almost *half* of the signal space, and we should be able to have a s.d.o.f. of $\frac{1}{2}$. This is illustrated in Figure 2.1, and proved formally in the sequel.

We choose both of the input symbols $\bar{X}_1$ and $\bar{X}_2$ independent and uniformly distributed over the same PAM constellation in (2.73). Since $\bar{\mathbf{X}}_2$ is an i.i.d. sequence and is independent of $\bar{\mathbf{X}}_1$, the following secrecy rate is always achievable [3]

$$C_s \geq I(\bar{X}_1; Y_1) - I(\bar{X}_1; Y_2) \tag{2.95}$$

In order to show that $D_s \geq \frac{1}{2}$, it suffices to prove that this lower bound provides $\frac{1}{2}$ s.d.o.f. To this end, we need to find a lower bound for $I(\bar{X}_1; Y_1)$ and an upper

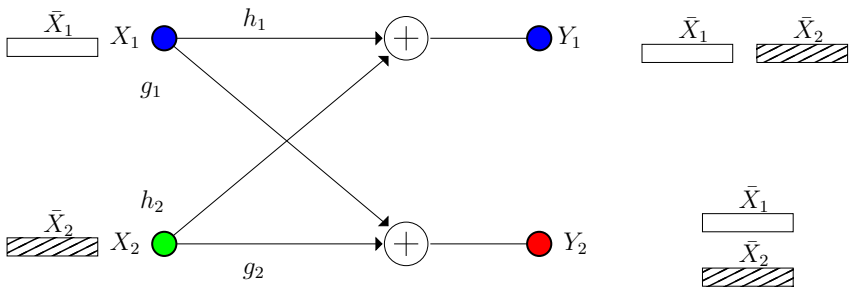


Figure 2.1: Illustration of interference alignment for the Gaussian wiretap channel with one helper.

bound for $I(\bar{X}_1; Y_2)$. It is clear that

$$H(\bar{X}_1) = H(\bar{X}_2) = \log |C(a, Q)| = \log(2Q + 1) \tag{2.96}$$

Also, note that, besides the additive Gaussian noise, the observation at receiver 1 is a linear combination of $\bar{X}_1$ and $\bar{X}_2$, i.e.,

$$Y_1 - N_1 = \alpha \bar{X}_1 + \beta \bar{X}_2 \tag{2.97}$$

where α and β are rationally independent real numbers almost surely.

By Lemma 2.3, for any small enough $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(2+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$ then the average power constraint is satisfied and the probability of error is bounded by

$$\Pr\left[\bar{X}_1 \neq \hat{X}_1\right] \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{2.98}$$

where η_γ is a positive constant which is independent of P and $\hat{X}_1$ is the estimate for $\bar{X}_1$ obtained by choosing the closest point in the constellation based on observation

Y_1.

By Fano's inequality and the Markov chain $\bar{X}_1 \to Y_1 \to \hat{X}_1$, we know that

$$H(\bar{X}_1|Y_1) \leq H(\bar{X}_1|\hat{X}_1) \tag{2.99}$$

$$\leq 1 + \exp\left(-\eta_\gamma P^\delta\right) \log(2Q+1) \tag{2.100}$$

which means that

$$I(\bar{X}_1; Y_1) = H(\bar{X}_1) - H(\bar{X}_1|Y_1) \tag{2.101}$$

$$\geq \left[1 - \exp\left(-\eta_\gamma P^\delta\right)\right] \log(2Q+1) - 1 \tag{2.102}$$

On the other hand,

$$I(\bar{X}_1; Y_2) \leq I(\bar{X}_1; \bar{X}_1 + \bar{X}_2) \tag{2.103}$$

$$= H(\bar{X}_1 + \bar{X}_2) - H(\bar{X}_2|\bar{X}_1) \tag{2.104}$$

$$= H(\bar{X}_1 + \bar{X}_2) - H(\bar{X}_2) \tag{2.105}$$

$$\leq \log(4Q+1) - \log(2Q+1) \tag{2.106}$$

$$\leq \log \frac{4Q+1}{2Q+1} \tag{2.107}$$

$$\leq 1 \tag{2.108}$$

where (2.106) is due to the fact that entropy of the sum $\bar{X}_1 + \bar{X}_2$ is maximized by the uniform distribution which takes values over a set of cardinality $4Q+1$.

Combining (2.102) and (2.108), we have

$$C_s \geq I(\bar{X}_1; Y_1) - I(\bar{X}_1; Y_2) \tag{2.109}$$

$$\geq \left[1 - \exp\left(-\eta_\gamma P^\delta\right)\right] \log(2Q+1) - 2 \tag{2.110}$$

$$= \left[1 - \exp\left(-\eta_\gamma P^\delta\right)\right] \log\left(2P^{\frac{1-\delta}{2(2+\delta)}} + 1\right) - 2 \tag{2.111}$$

$$= \frac{1-\delta}{(2+\delta)} \left(\frac{1}{2} \log P\right) + o(\log P) \tag{2.112}$$

where the $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{1}{2}$ s.d.o.f., which concludes the achievability part of the theorem.

2.5 Wiretap Channel with M Helpers

In this section, we consider the Gaussian wiretap channel with M helpers as formulated in Section 2.2.1 for general $M > 1$. In this section, we will show that the s.d.o.f. is $\frac{M}{M+1}$ for almost all channel gains as stated in the following theorem. This shows that even though the helpers are independent, the s.d.o.f. increases monotonically with the number of helpers M. The converse follows from the general secrecy penalty upper bound in Section 2.3.1 and the cooperative jamming signal upper bound in Section 2.3.2. The achievability is based on cooperative jamming of M helpers with discrete signaling and real interference alignment.

Theorem 2.2 *The s.d.o.f. of the Gaussian wiretap channel with M helpers is $\frac{M}{M+1}$ for almost all channel gains.*

2.5.1 Converse

We again start with (2.32) of Lemma 2.1 with the selection of $j = 1$

$$nR \leq \sum_{i=1, i\neq j}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{2.113}$$

$$= \sum_{i=2}^{M+1} h(\tilde{\mathbf{X}}_i) + nc' \tag{2.114}$$

$$\leq M[h(\mathbf{Y}_1) - H(W)] + nc_9 \tag{2.115}$$

where (2.115) is due to Lemma 2.2 for each jamming signal $\tilde{\mathbf{X}}_i$, $i = 2, \cdots, M+1$. By noting $H(W) = nR$, (2.115) implies that

$$(M+1)nR \leq Mh(\mathbf{Y}_1) + nc_9 \tag{2.116}$$

$$\leq M\left(\frac{n}{2}\log P\right) + nc_{10} \tag{2.117}$$

which further implies from (2.5) that

$$D_s \leq \frac{M}{M+1} \tag{2.118}$$

which concludes the converse part of the theorem.

2.5.2 Achievable Scheme

Let $\{V_2, V_3, \cdots, V_{M+1}, U_2, U_3, \cdots, U_{M+1}\}$ be mutually independent discrete random variables, each of which uniformly drawn from the same PAM constellation $C(a, Q)$

in (2.73), where a and Q will be specified later. We choose the input signal of the legitimate transmitter as

$$X_1 = \sum_{k=2}^{M+1} \frac{g_k}{g_1 h_k} V_k \tag{2.119}$$

and the input signal of the jth helper, $j = 2, \cdots, M+1$, as

$$X_j = \frac{1}{h_j} U_j \tag{2.120}$$

Then, the observations of the receivers are

$$Y_1 = \sum_{k=2}^{M+1} \frac{h_1 g_k}{g_1 h_k} V_k + \left(\sum_{j=2}^{M+1} U_j \right) + N_1 \tag{2.121}$$

$$Y_2 = \sum_{k=2}^{M+1} \frac{g_k}{h_k} \Big(V_k + U_k \Big) + N_2 \tag{2.122}$$

The intuition here is as follows. We use M independent sub-signals V_k, $k = 2, \cdots, M+1$, to represent the signals carrying the original message W. The input signal X_1 is a linear combination of V_ks. To cooperatively jam the eavesdropper, each helper k aligns the cooperative jamming signal U_k in the same *dimension* as the sub-signal V_k at the eavesdropper. At the legitimate receiver, all of the cooperative jamming signals U_ks are well-aligned such that they occupy a small portion of the signal space. Since, almost surely, $\left\{1, \frac{h_1 g_2}{g_1 h_2}, \frac{h_1 g_3}{g_1 h_3}, \cdots, \frac{h_1 g_{M+1}}{g_1 h_{M+1}}\right\}$ are rationally independent, signals $\left\{V_2, V_3, \cdots, V_{M+1}, \sum_{j=2}^{M+1} U_j\right\}$ can be distinguished by the legitimate receiver. As an example, the case of $M = 2$ is shown in Figure 2.2.

Since, for each $j \neq 1$, $\mathbf{X}_j$ is an i.i.d. sequence and independent of $\mathbf{X}_1$, the

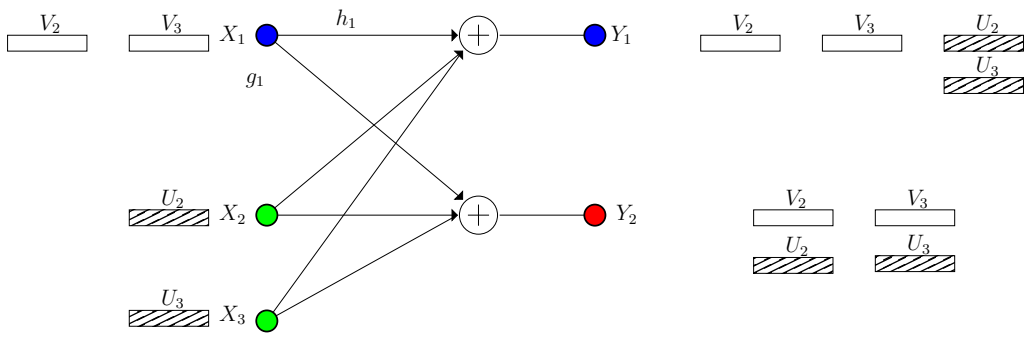


Figure 2.2: Illustration of interference alignment for the Gaussian wiretap channel with M helpers. Here, $M = 2$.

following secrecy rate is achievable [3]

$$C_s \geq I(X_1; Y_1) - I(X_1; Y_2) \tag{2.123}$$

Now, we first bound the probability of decoding error. Note that the *space* observed at receiver 1 consists of $(2Q+1)^M(2MQ+1)$ points in $M+1$ *dimensions*, and the sub-signal in each *dimension* is drawn from a constellation of $C(a, MQ)$. Here, we use the property that $C(a, Q) \subset C(a, MQ)$. By Lemma 2.3, for any small enough $\delta > 0$ and for almost all rationally independent $\left\{1, \frac{h_1 g_2}{g_1 h_2}, \frac{h_1 g_3}{g_1 h_3}, \cdots, \frac{h_1 g_{M+1}}{g_1 h_{M+1}}\right\}$, except for a set of Lebesgue measure zero, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(M+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$ then the average power constraint is satisfied and the probability of error is bounded by

$$\Pr\left[X_1 \neq \hat{X}_1\right] \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{2.124}$$

where η_γ is a positive constant which is independent of P and where $\hat{X}_1$ is the estimate of X_1 by choosing the closest point in the constellation based on observation

Y_1.

By Fano's inequality and the Markov chain $X_1 \to Y_1 \to \hat{X}_1$, we know that

$$H(X_1|Y_1) \leq H(X_1|\hat{X}_1) \tag{2.125}$$

$$\leq 1 + \exp\left(-\eta_\gamma P^\delta\right) \log(2Q+1)^M \tag{2.126}$$

which means that

$$I(X_1;Y_1) = H(X_1) - H(X_1|Y_1) \tag{2.127}$$

$$\geq \left[1 - \exp\left(\eta_\gamma P^\delta\right)\right] \log(2Q+1)^M - 1 \tag{2.128}$$

On the other hand,

$$I(X_1;Y_2) \leq I\left(X_1; \sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\right) \tag{2.129}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\middle| X_1\right) \tag{2.130}$$

$$= H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)\right) - H\left(\sum_{k=2}^{M+1} \frac{g_k}{h_k} U_k\right) \tag{2.131}$$

$$\leq \log(4Q+1)^M - \log(2Q+1)^M \tag{2.132}$$

$$\leq M \log \frac{4Q+1}{2Q+1} \tag{2.133}$$

$$\leq M \tag{2.134}$$

where (2.132) is due to the fact that entropy of the sum $\sum_{k=2}^{M+1} \frac{g_k}{h_k}(V_k + U_k)$ is maximized by the uniform distribution which takes values over a set of cardinality

$(4Q+1)^M$.

Combining (2.128) and (2.134), we have

$$C_s \geq I(X_1;Y_1) - I(X_1;Y_2) \tag{2.135}$$

$$\geq \left[1-\exp\left(-\eta_\gamma P^\delta\right)\right]\log(2Q+1)^M - (M+1) \tag{2.136}$$

$$\geq \left[1-\exp\left(-\eta_\gamma P^\delta\right)\right]\log(2P^{\frac{1-\delta}{2(M+1+\delta)}}+1)^M - (M+1) \tag{2.137}$$

$$= \frac{M(1-\delta)}{(M+1+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.138}$$

where $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{M}{M+1}$ s.d.o.f., which concludes the achievability part of the theorem.

2.6 Broadcast Channel with Confidential Messages and M Helpers

In this section, we consider the Gaussian BC with confidential messages and M helpers formulated in Section 2.2.2. When there are no helpers, i.e., $M = 0$, due to the degradedness of the underlying Gaussian BC, one of the users (stronger) has the secrecy capacity which is equal to the secrecy capacity of the Gaussian wiretap channel, and the other user (weaker) has zero secrecy capacity. Therefore, for both users, the s.d.o.f. is zero, implying that the sum s.d.o.f. of the system is zero. Therefore, we consider the case $M \geq 1$. In this section, we will show that the sum s.d.o.f. is 1 for any $M \geq 1$, as stated in the following theorem.

Theorem 2.3 *The sum s.d.o.f. of the Gaussian broadcast channel with confidential messages and $M \geq 1$ helpers is 1 for almost all channel gains.*

2.6.1 Converse

An immediate upper bound for the s.d.o.f. of this problem is 1, i.e., $D_{s,\Sigma} \leq 1$ for any M. This comes from the fact that the d.o.f. for the Gaussian BC without any secrecy constraints is 1, and this constitutes an upper for the sum s.d.o.f. also.

2.6.2 Achievable Scheme

In the following, we will show that a sum s.d.o.f. of 1 can be achieved for the case of $M = 1$. Since the achievable scheme with a single helper achieves the upper bound $D_{s,\Sigma} \leq 1$, the sum s.d.o.f. for all $M \geq 1$ is 1. Therefore, if we have more than one helper, then all but one helper may remain silent.

We use the equivalent channel expression in (2.93) and (2.94). Let V_1, V_2 and U be three mutually independent random variables which are identically and uniformly distributed over the constellation $C(a, Q)$ in (2.73), where a and Q will be specified later. We assign channel inputs as $\bar{X}_1 = V_1 + \frac{\beta}{\alpha} V_2$ and $\bar{X}_2 = U$. Then, the observations at the two receivers are:

$$Y_1 = \alpha V_1 + \beta(V_2 + U) + N_1 \tag{2.139}$$

$$Y_2 = (V_1 + U) + \frac{\beta}{\alpha} V_2 + N_2 \tag{2.140}$$

We use two independent variables V_1 and V_2 to be the signals carrying the messages W_1 and W_2 that go to the two receivers. In order to ensure that the messages are kept secure against the unintended receiver, we align the cooperative jamming signal

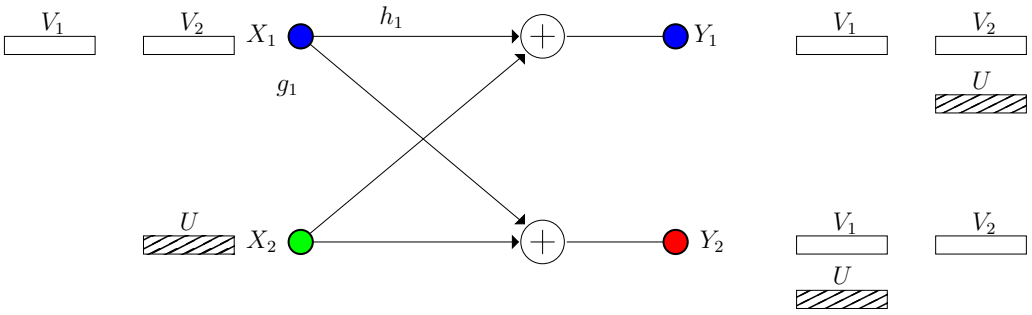


Figure 2.3: Illustration of interference alignment for the Gaussian BC with confidential messages and one helper.

U from the helper in the *dimension* of V_2 at receiver 1, and in the *dimension* of V_1 at receiver 2. This is illustrated in Figure 2.3.

Since $\bar{\mathbf{X}}_2$ is an i.i.d. sequence, the following secrecy rate pair is achievable [5, Theorem 4]

$$R_1 \geq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{2.141}$$

$$R_2 \geq I(V_2; Y_2) - I(V_2; Y_1|V_1) \tag{2.142}$$

By Lemma 2.3, it is easy to verify that receiver i can decode V_i, for $i = 1, 2$ with arbitrarily small probability of decoding error with probability one, i.e., for any small enough $\delta > 0$ and for almost all rationally independent $\{\alpha, \beta\}$, except for a set of Lebesgue measure zero, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(2+\delta)}}$, $a = \gamma P^{\frac{1}{2}}/Q$ then the average power constraint is satisfied and the probability of error is bounded by

$$\Pr\left[V_i \neq \hat{V}_i\right] \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{2.143}$$

where η_γ is a positive constant which is independent of P and $\hat{V}_i$ is the estimate for V_i by choosing the closest point in the constellation based on observation Y_i.

By Fano's inequality and the Markov chain $V_i \to Y_i \to \hat{V}_i$, we know that

$$H(V_i|Y_i) \leq H(V_i|\hat{V}_i) \tag{2.144}$$

$$\leq 1 + \exp\left(-\eta_\gamma P^\delta\right) \log(2Q+1) \tag{2.145}$$

which means that

$$I(V_i;Y_i) = H(V_i) - H(V_i|Y_i) \tag{2.146}$$

$$\geq \left[1 - \exp\left(-\eta_\gamma P^\delta\right)\right] \log(2Q+1) - 1 \tag{2.147}$$

$$= \frac{1-\delta}{2+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.148}$$

for $i = 1$ or 2.

On the other hand, for $i = 1$, we have

$$I(V_1;Y_2|V_2) \leq I\left(V_1; V_1 + U + \frac{\beta}{\alpha}V_2 \Big| V_2\right) \tag{2.149}$$

$$= H(V_1+U) - H(U) \tag{2.150}$$

$$\leq 1 \tag{2.151}$$

Similarly, for $i = 2$, we have

$$I(V_2; Y_1|V_1) \leq I\left(V_2; \alpha V_1 + \beta(V_2 + U)\Big|V_1\right) \tag{2.152}$$

$$= H(V_2 + U) - H(U) \tag{2.153}$$

$$\leq 1 \tag{2.154}$$

which implies that the following sum secrecy rate is achievable

$$R_1 + R_2 \geq \frac{2 - 2\delta}{2 + \delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.155}$$

If we choose δ small enough, then we can have $D_{s,\Sigma} \geq 1$. Combining this with the upper bound $D_{s,\Sigma} \leq 1$, we conclude that

$$D_{s,\Sigma} = 1 \tag{2.156}$$

for almost all channel gains.

2.7 Two-User Interference Channel with Confidential Messages and No Helpers

In this section, we consider the two-user Gaussian IC with confidential messages formulated in Section 2.2.3 for the case of no helpers, i.e., $M = 0$. The case of $M \geq 1$ will be presented in Section 2.8. For the case of no helpers, we show that the sum s.d.o.f. is $\frac{2}{3}$ as stated in the following theorem.

Theorem 2.4 *The sum s.d.o.f. of the two-user Gaussian interference channel with confidential messages is* $\frac{2}{3}$ *for almost all channel gains.*

2.7.1 Converse

We first start with (2.31) of Lemma 2.1 to upper bound the individual rate R_1 of message W_1

$$nR_1 \leq h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) - h(\mathbf{Y}_2) + nc \tag{2.157}$$

$$\leq h(\tilde{\mathbf{X}}_1) + h(\mathbf{Y}_1) - H(W_1) - h(\mathbf{Y}_2) + nc_{11} \tag{2.158}$$

$$\leq h(\mathbf{Y}_2) - H(W_2) + h(\mathbf{Y}_1) - H(W_1) - h(\mathbf{Y}_2) + nc_{12} \tag{2.159}$$

where (2.158) is due to applying Lemma 2.2 for $h(\tilde{\mathbf{X}}_2)$ and (2.159) is due to applying Lemma 2.2 once again for $h(\tilde{\mathbf{X}}_1)$. By noting that $H(W_1) = nR_1$ and $H(W_2) = nR_2$, from (2.159), we have

$$2nR_1 + nR_2 \leq h(\mathbf{Y}_1) + nc_{12} \tag{2.160}$$

We use the same method to get a symmetric upper bound on the individual rate R_2 of message W_2 as

$$nR_1 + 2nR_2 \leq h(\mathbf{Y}_2) + nc_{13} \tag{2.161}$$

Then, combining (2.160) and (2.161), we get

$$3(nR_1 + nR_2) \leq h(\mathbf{Y}_1) + h(\mathbf{Y}_2) + nc_{14} \tag{2.162}$$

$$\leq 2\left(\frac{n}{2}\log P\right) + nc_{15} \tag{2.163}$$

which means

$$D_{s,\Sigma} \leq \frac{2}{3} \tag{2.164}$$

which concludes the converse part of the theorem.

2.7.2 Achievable Scheme

Let $\{V_1, U_1, V_2, U_2\}$ be mutually independent discrete random variables. Each of them is uniformly and independently drawn from the same constellation $C(a, Q)$ in (2.73), where a and Q will be specified later. Here, the role of V_i is the signal carrying message W_i, and the role of U_i is the cooperative jamming signal to help the transmitter-receiver pair $j \neq i$. We choose the input signals of the transmitters as:

$$X_1 = V_1 + \frac{h_{2,1}}{h_{1,1}}U_1 \tag{2.165}$$

$$X_2 = V_2 + \frac{h_{1,2}}{h_{2,2}}U_2 \tag{2.166}$$

With these input signal selections, observations of the receivers are

$$Y_1 = h_{1,1}V_1 + h_{2,1}\big(U_1 + V_2\big) + \frac{h_{2,1}h_{1,2}}{h_{2,2}}U_2 + N_1 \tag{2.167}$$

$$Y_2 = h_{2,2}V_2 + h_{1,2}\big(U_2 + V_1\big) + \frac{h_{2,1}h_{1,2}}{h_{1,1}}U_1 + N_2 \tag{2.168}$$

Since, for each i and $j \neq i$, V_i and U_i are not in the same *dimension* at both receivers, we align U_i in the *dimension* of V_j at receiver i such that V_j is *secure* and V_i can occupy a *larger* space. This is illustrated in Figure 2.4.

By [5, Theorem 2], we know that the following secrecy rate pair is achievable

$$R_1 \geq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{2.169}$$

$$R_2 \geq I(V_2; Y_2) - I(V_2; Y_1|V_1) \tag{2.170}$$

For receiver 1, by Lemma 2.3, for any small enough $\delta > 0$ and for almost all rationally independent $\left\{h_{1,1}, h_{2,1}, \frac{h_{2,1}h_{1,2}}{h_{2,2}}\right\}$, except for a set of Lebesgue measure zero, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(3+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$ then the average power constraint is satisfied and the probability of error is bounded by

$$\Pr\left[V_1 \neq \hat{V}_1\right] \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{2.171}$$

where η_γ is a positive constant which is independent of P and $\hat{V}_1$ is the estimate of V_1 by choosing the closest point in the constellation based on observation Y_1.

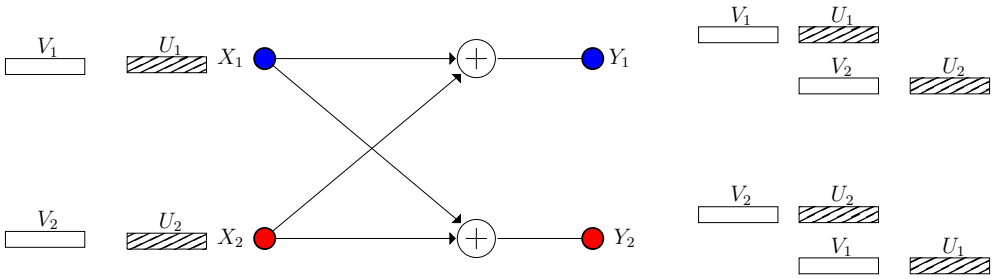


Figure 2.4: Illustration of interference alignment for the two-user Gaussian IC with confidential messages (no helpers).

To lower bound the achievable rate R_1, we first note that

$$I(V_1;Y_1) \geq I(V_1;\hat{V}_1) \tag{2.172}$$

$$= H(V_1) - H(V_1|\hat{V}_1) \tag{2.173}$$

$$\geq \left[1 - \exp\left(-\eta_\gamma P^\delta\right)\right] \log(2Q+1) - 1 \tag{2.174}$$

$$= \frac{1-\delta}{3+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.175}$$

On the other hand,

$$I(V_1;Y_2|V_2) \leq I(V_1;Y_2,U_1|V_2) \tag{2.176}$$

$$= I(V_1;Y_2|V_2,U_1) \tag{2.177}$$

$$\leq I\left(V_1;h_{1,2}(U_2+V_1)|V_2,U_1\right) \tag{2.178}$$

$$= H(U_2+V_1) - H(U_2) \tag{2.179}$$

$$\leq \log(4Q+1) - \log(2Q+1) \tag{2.180}$$

$$\leq 1 \tag{2.181}$$

Combining (2.175) and (2.181), we obtain

$$R_1 \geq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{2.182}$$

$$\geq \frac{1-\delta}{3+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.183}$$

By applying this same analysis to rate R_2, we can obtain a symmetric result for R_2. Then, by choosing δ arbitrarily small, we can achieve $\frac{2}{3}$ sum s.d.o.f.

2.8 Two-User Interference Channel with Confidential Messages and M Helpers

In this section, we consider the two-user Gaussian IC with confidential messages formulated in Section 2.2.3 for the general case of $M \geq 1$ helpers. For this general case, we show that the sum s.d.o.f. is 1 as stated in the following theorem.

Theorem 2.5 *The sum s.d.o.f. of the two-user Gaussian interference channel with confidential messages and $M \geq 1$ helpers is 1 for almost all channel gains.*

2.8.1 Converse

An immediate upper bound for the s.d.o.f. of this problem is 1, i.e., $D_{s,\Sigma} \leq 1$ for any M. This comes from the fact that the d.o.f. for the two-user IC without any secrecy constraints is 1, and this constitutes an upper for the sum s.d.o.f. also. The fact that the d.o.f. of the two-user IC is 1 was first proved in [54]. We provide an alternative proof to this fact using the techniques developed in this chapter in Appendix 2.12.1.

2.8.2 Achievable Scheme

In the following, we will show that a sum s.d.o.f. of 1 can be achieved for the case of $M = 1$. Since the achievable scheme with a single helper achieves the upper bound $D_{s,\Sigma} \leq 1$, the sum s.d.o.f. for all $M \geq 1$ is 1. Therefore, if we have more than one helper, then all but one helper may remain silent.

Let $\{V_1, V_2, U\}$ be mutually independent discrete random variables. Each of them is uniformly and independently drawn from the same constellation $C(a, Q)$ in (2.73), where a and Q will be specified later. Here, the role of V_i is the signal carrying message W_i, and the role of U is the cooperative jamming signal from the helper. We choose the input signals of the transmitters as:

$$X_1 = \frac{h_{3,2}}{h_{1,2}} V_1 \tag{2.184}$$

$$X_2 = \frac{h_{3,1}}{h_{2,1}} V_2 \tag{2.185}$$

$$X_3 = U \tag{2.186}$$

With these input signal selections, observations of the receivers are

$$Y_1 = \frac{h_{3,2}h_{1,1}}{h_{1,2}} V_1 + h_{3,1}\big(U + V_2\big) + N_1 \tag{2.187}$$

$$Y_2 = \frac{h_{3,1}h_{2,2}}{h_{2,1}} V_2 + h_{3,2}\big(U + V_1\big) + N_2 \tag{2.188}$$

For each i and $j \neq i$, we align U in the *dimension* of V_j at receiver i such that V_j is *secure* and V_i can be decoded. This is illustrated in Figure 2.5.

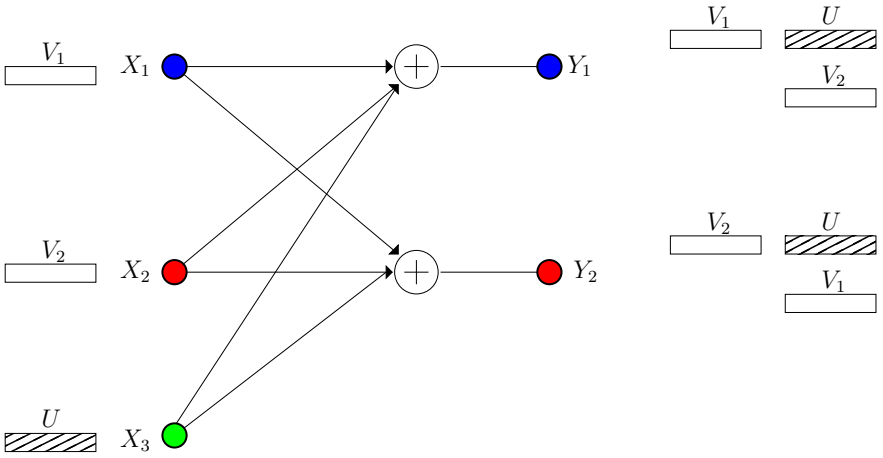


Figure 2.5: Illustration of interference alignment for the two-user Gaussian IC with confidential messages and one helper.

Since $\mathbf{U}$ is an i.i.d. sequence, by [5, Theorem 2], we know that the following secrecy rate pair is achievable

$$R_1 \geq I(V_1; Y_1) - I(V_1; Y_2|V_2) \tag{2.189}$$

$$R_2 \geq I(V_2; Y_2) - I(V_2; Y_1|V_1) \tag{2.190}$$

For receiver 1, by Lemma 2.3, for any small enough $\delta > 0$ and for almost all rationally independent $\left\{\frac{h_{3,2}h_{1,1}}{h_{1,2}}, h_{3,1}\right\}$, except for a set of Lebesgue measure zero, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(2+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$ then the average power constraint is satisfied and the probability of error is bounded by

$$\Pr\left[V_1 \neq \hat{V}_1\right] \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{2.191}$$

where η_γ is a positive constant which is independent of P and $\hat{V}_1$ is the estimate of V_1 by choosing the closest point in the constellation based on the observation Y_1.

To lower bound the achievable rate R_1, we first note that

$$I(V_1;Y_1) \geq I(V_1;\hat{V}_1) \tag{2.192}$$

$$= H(V_1) - H(V_1|\hat{V}_1) \tag{2.193}$$

$$\geq \left[1 - \exp\left(-\eta_\gamma P^\delta\right)\right] \log(2Q+1) - 1 \tag{2.194}$$

$$= \frac{1-\delta}{2+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.195}$$

On the other hand,

$$I(V_1;Y_2|V_2) \leq I\Big(V_1; h_{3,2}(U+V_1)|V_2\Big) \tag{2.196}$$

$$= H(U+V_1) - H(U) \tag{2.197}$$

$$\leq \log(4Q+1) - \log(2Q+1) \tag{2.198}$$

$$\leq 1 \tag{2.199}$$

Combining (2.195) and (2.199), we obtain

$$R_1 \geq I(V_1;Y_1) - I(V_1;Y_2|V_2) \tag{2.200}$$

$$\geq \frac{1-\delta}{2+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.201}$$

By applying this same analysis to rate R_2, we can obtain a symmetric result for R_2. Then, by choosing δ arbitrarily small, we can achieve 1 sum s.d.o.f. for almost all channel gains for the $M = 1$ case.

2.9 K-User Multiple Access Wiretap Channel

In this section, we consider the K-user MAC wiretap channel formulated in Section 2.2.4. We show that the sum s.d.o.f. of this channel is $\frac{K(K-1)}{K(K-1)+1}$ as stated in the following theorem.

Theorem 2.6 *The sum s.d.o.f. of the K-user Gaussian multiple access wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$ for almost all channel gains.*

2.9.1 Converse

We start with the sum rate and derive an upper bound similar to Lemma 2.1

$$n\sum_{i=1}^{K} R_i = \sum_{i=1}^{K} H(W_i) = H(W_1^K) \tag{2.202}$$

$$\leq I(W_1^K; \mathbf{Y}_1, \mathbf{Y}_2) - I(W_1^K; \mathbf{Y}_2) + nc_{15} \tag{2.203}$$

$$= I(W_1^K; \mathbf{Y}_1|\mathbf{Y}_2) + nc_{15} \tag{2.204}$$

$$\leq I(\mathbf{X}_1^K; \mathbf{Y}_1|\mathbf{Y}_2) + nc_{15} \tag{2.205}$$

$$= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{Y}_1|\mathbf{Y}_2, \mathbf{X}_1^K) + nc_{15} \tag{2.206}$$

$$= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{N}_1|\mathbf{Y}_2, \mathbf{X}_1^K) + nc_{15} \tag{2.207}$$

$$= h(\mathbf{Y}_1|\mathbf{Y}_2) - h(\mathbf{N}_1) + nc_{15} \tag{2.208}$$

$$\leq h(\mathbf{Y}_1|\mathbf{Y}_2) + nc_{16} \tag{2.209}$$

$$= h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{17} \tag{2.210}$$

$$= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2)$$

$$- h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K|\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{17} \tag{2.211}$$

where (2.208) is due to the fact that $\mathbf{N}_1$ is independent of $(\mathbf{Y}_2, \mathbf{X}_1^K)$. Besides, $W_1^K \stackrel{\triangle}{=} \{W_j\}_{j=1}^K$ and, for each j, $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$. Here $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence and $\tilde{N}_j$ is a Gaussian noise with variance $\sigma_j^2 < \min(1/h_j^2, 1/g_j^2)$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other random variables. Thus,

$$
\begin{aligned}
n\sum_{i=1}^{K} R_i &= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K | \mathbf{Y}_1, \mathbf{Y}_2) \\
&\quad - h(\mathbf{Y}_2) + nc_{17} && (2.212) \\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) \\
&\quad - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K | \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_K) - h(\mathbf{Y}_2) + nc_{17} && (2.213) \\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) \\
&\quad - h(\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \cdots, \tilde{\mathbf{N}}_K | \mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2, \cdots, \mathbf{X}_K) - h(\mathbf{Y}_2) + nc_{17} && (2.214) \\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{N}}_1, \tilde{\mathbf{N}}_2, \cdots, \tilde{\mathbf{N}}_K) \\
&\quad - h(\mathbf{Y}_2) + nc_{17} && (2.215) \\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K, \mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{18} && (2.216) \\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K) + h(\mathbf{Y}_1, \mathbf{Y}_2 | \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K) \\
&\quad - h(\mathbf{Y}_2) + nc_{18} && (2.217) \\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \cdots, \tilde{\mathbf{X}}_K) - h(\mathbf{Y}_2) + nc_{19} && (2.218) \\
&= \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Y}_2) + nc_{20} && (2.219) \\
&\leq \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_{21} && (2.220)
\end{aligned}
$$

where (2.215) is due to the fact that $\tilde{\mathbf{N}}_1^K$ is independent of $(\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1^K)$, (2.218) follows similar to (2.52), and (2.220) is due to

$$h(\tilde{\mathbf{X}}_1) \leq h(g_1\mathbf{X}_1 + \mathbf{N}_2) + nc_{22} \leq h(\mathbf{Y}_2) + nc_{22} \tag{2.221}$$

which is similar to going from (2.31) to (2.32) in Lemma 2.1 by using derivations in (2.59)-(2.64).

On the other hand, for each j, we have a bound similar to Lemma 2.2

$$\sum_{i\neq j} H(W_i) = H(W_{\neq j}) \tag{2.222}$$

$$\leq I(W_{\neq j}; \mathbf{Y}_1) + nc_{23} \tag{2.223}$$

$$\leq I\left(\sum_{i\neq j} h_i\mathbf{X}_i; \mathbf{Y}_1\right) + nc_{23} \tag{2.224}$$

$$= h\left(\mathbf{Y}_1\right) - h\left(\mathbf{Y}_1 \middle| \sum_{i\neq j} h_i\mathbf{X}_i\right) + nc_{23} \tag{2.225}$$

$$= h\left(\mathbf{Y}_1\right) - h\left(h_j\mathbf{X}_j + \mathbf{N}_1\right) + nc_{23} \tag{2.226}$$

$$\leq h(\mathbf{Y}_1) - h(\tilde{\mathbf{X}}_j) + nc_{24} \tag{2.227}$$

where $W_{\neq j} \stackrel{\triangle}{=} \{W_i\}_{i=1}^K \backslash \{W_j\}$ which forms the Markov chain $W_{\neq j} \rightarrow \mathbf{X}_{\neq j} \rightarrow \sum_{i\neq j} h_i\mathbf{X}_i \rightarrow \mathbf{Y}_1$. Therefore, for each j, we have

$$h(\tilde{\mathbf{X}}_j) \leq h(\mathbf{Y}_1) - \sum_{i\neq j} H(W_i) + nc_{24} \tag{2.228}$$

Now, continuing from (2.220) and incorporating (2.228), we have

$$n\sum_{i=1}^{K} R_i \leq \sum_{j=2}^{K} h(\tilde{\mathbf{X}}_j) + nc_{25} \tag{2.229}$$

$$\leq \sum_{j=2}^{K} \left[h(\mathbf{Y}_1) - \sum_{i\neq j} H(W_i) \right] + nc_{26} \tag{2.230}$$

Noting that $H(W_i) = nR_i$, this is equivalent to,

$$nR_1 + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)h(\mathbf{Y}_1) + nc_{26} \tag{2.231}$$

We then apply this upper bound for each i by eliminating a different $h(\tilde{\mathbf{X}}_i)$ each time in the same way that it was done for $h(\tilde{\mathbf{X}}_1)$ in (2.221) and have K upper bounds in total:

$$nR_i + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)h(\mathbf{Y}_1) + nc_{26}, \qquad i = 1, \cdots, K \tag{2.232}$$

Thus,

$$\Big[K(K-1)+1\Big]\sum_{j=1}^{K} nR_j \leq K(K-1)h(\mathbf{Y}_1) + nc_{27} \tag{2.233}$$

$$\leq K(K-1)\left(\frac{n}{2}\log P\right) + nc_{28} \tag{2.234}$$

that is,

$$D_{s,\Sigma} \leq \frac{K(K-1)}{K(K-1)+1} \tag{2.235}$$

which concludes the converse part of the theorem.

2.9.2 Achievable Scheme

In the Gaussian wiretap channel with M helpers, our achievability scheme divided the message signal into M parts, and each one of the M helpers protected a part at the eavesdropper. On the other hand, in the IC with confidential messages, since each user had its own message to send, each transmitter sent a combination of a message and a cooperative jamming signal. We combine these two approaches to propose the following achievability scheme in this K-user MAC wiretap channel. Each transmitter i divides its message into $(K-1)$ mutually independent sub-signals. In addition, each transmitter i sends a cooperative jamming signal U_i. At the eavesdropper Y_2, each sub-signal indexed by (i,j), where $j \in \{1,\cdots,K\}\backslash\{i\}$, is *aligned* with a cooperative jamming signal U_i. At the legitimate receiver Y_1, all of the cooperative jamming signals are *aligned* in the same dimension to *occupy* as *small* a signal space as possible. This scheme is illustrated in Figure 2.6 for the case of $K=3$.

We use in total K^2 mutually independent random variables which are

$$V_{i,j}, \quad i,j \in \{1,\cdots,K\}, j \neq i \tag{2.236}$$

$$U_k, \quad k \in \{1,\cdots,K\} \tag{2.237}$$

Each of them is uniformly and independently drawn from the same constellation $C(a,Q)$ in (2.73), where a and Q will be specified later. For each $i \in \{1,\cdots,K\}$,

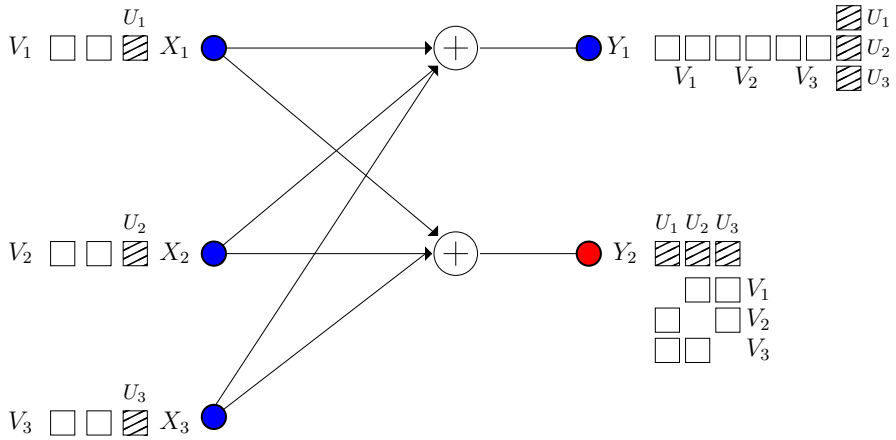


Figure 2.6: Illustration of interference alignment for the K-user MAC wiretap channel. Here, $K = 3$.

we choose the input signal of transmitter i as

$$X_i = \sum_{j=1, j\neq i}^{K} \frac{g_j}{g_i h_j} V_{i,j} + \frac{1}{h_i} U_i \tag{2.238}$$

With these input signal selections, observations of the receivers are

$$Y_1 = \sum_{i=1}^{K} \sum_{j=1, j\neq i}^{K} \frac{g_j h_i}{g_i h_j} V_{i,j} + \left[\sum_{k=1}^{K} U_k\right] + N_1 \tag{2.239}$$

$$Y_2 = \left[\sum_{i=1}^{K} \sum_{j=1, j\neq i}^{K} \frac{g_j}{h_j} V_{i,j}\right] + \sum_{j=1}^{K} \frac{g_j}{h_j} U_j + N_2 \tag{2.240}$$

$$= \sum_{j=1}^{K} \frac{g_j}{h_j} \left[U_j + \sum_{i=1, i\neq j}^{K} V_{i,j}\right] + N_2 \tag{2.241}$$

By [34, Theorem 1], we can achieve the following sum secrecy rate

$$\sup \sum_{i=1}^{K} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{2.242}$$

where $\mathbf{V} \triangleq \{V_{i,j} : i, j \in \{1, \cdots, K\}, j \neq i\}$.

Now, we first bound the probability of decoding error. Note that the *space* observed at receiver 1 consists of $(2Q+1)^{K(K-1)}(2KQ+1)$ points in $K(K-1)+1$ *dimensions*, and the sub-signal in each *dimension* is drawn from a constellation of $C(a, KQ)$. Here, we use the property that $C(a, Q) \subset C(a, KQ)$. By Lemma 2.3, for any small enough $\delta > 0$ and for almost all rationally independent factors in Y_1 except for a set of Lebesgue measure zero, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(K(K-1)+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$ then the average power constraint is satisfied and the probability of error is bounded by

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{2.243}$$

where η_γ is a positive constant which is independent of P and $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y_1.

By Fano's inequality and the Markov chain $\mathbf{V} \to Y_1 \to \hat{\mathbf{V}}$, we know that

$$H(\mathbf{V}|Y_1) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{2.244}$$

$$\leq 1 + \exp\left(-\eta_\gamma P^\delta\right) \log(2Q+1)^{K(K-1)} \tag{2.245}$$

which means that

$$I(\mathbf{V}; Y_1) = H(\mathbf{V}) - H(\mathbf{V}|Y_1) \tag{2.246}$$

$$\geq \left[1 - \exp\left(-\eta_\gamma P^\delta\right)\right] \log(2Q+1)^{K(K-1)} - 1 \tag{2.247}$$

On the other hand,

$$I(\mathbf{V};Y_2) \le I\left(\mathbf{V};\sum_{j=1}^{K}\frac{g_j}{h_j}\left[U_j+\sum_{i=1,i\neq j}^{K}V_{i,j}\right]\right) \tag{2.248}$$

$$= H\left(\sum_{j=1}^{K}\frac{g_j}{h_j}\left[U_j+\sum_{i=1,i\neq j}^{K}V_{i,j}\right]\right) - H\left(\sum_{j=1}^{K}\frac{g_j}{h_j}\left[U_j+\sum_{i=1,i\neq j}^{K}V_{i,j}\right]\middle|\mathbf{V}\right) \tag{2.249}$$

$$= H\left(\sum_{j=1}^{K}\frac{g_j}{h_j}\left[U_j+\sum_{i=1,i\neq j}^{K}V_{i,j}\right]\right) - H\left(\sum_{j=1}^{K}\frac{g_j}{h_j}U_j\right) \tag{2.250}$$

$$\le K\log\frac{2KQ+1}{2Q+1} \tag{2.251}$$

$$\le K\log K \tag{2.252}$$

where (2.250) is due to the fact that entropy is maximized by the uniform distribution which takes values over a set of cardinality $(2KQ+1)^K$.

Combining (2.247) and (2.252), we obtain

$$\sup\sum_{i=1}^{K}R_i \ge I(\mathbf{V};Y_1) - I(\mathbf{V};Y_2) \tag{2.253}$$

$$\ge \left[1-\exp\left(-\eta_\gamma P^\delta\right)\right]\log(2Q+1)^{K(K-1)} - 1 - K\log K \tag{2.254}$$

$$= \frac{K(K-1)(1-\delta)}{K(K-1)+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{2.255}$$

where $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{K(K-1)}{K(K-1)+1}$ sum s.d.o.f. for almost all channel gains.

2.10 Discussion

2.10.1 CSI of the External Eavesdropper

The results in this chapter are all critically dependent on the availability of all channel state information (CSI) at all entities. We utilize this CSI information to design the transmitter signals so that they align at the legitimate receiver and the eavesdropper in a certain desired manner. Availability of legitimate receiver's CSI can be justified by the feedback links. Availability of the eavesdropper CSI can be justified only when the eavesdropper is also a legitimate user of the system, as in the case of IC with confidential messages. For the case of external eavesdroppers, generally, the CSI of the eavesdropper link will not be available, as the eavesdropper will not feed her CSI back, and even when she does, she will not be truthful. Therefore, studying the case where eavesdropper CSI is not available is practically important (and also theoretically challenging). There have been some recent results on this topic [27, 47, 67, 79]; see also, e.g., [80, 81], for the multiple-input multiple-output (MIMO) setting.

References [27, 79] utilized interference alignment to obtain s.d.o.f. for ergodic fading channel models with secrecy constraints. Although it is infeasible to put all of the signals into the same sub-space at the eavesdropper without eavesdropper CSI, the total d.o.f. the eavesdropper can observe is limited to 1. Since mixing signals together already provides a certain amount of secrecy to those signals, even when the eavesdropper CSI is not known at the transmitter(s), s.d.o.f. can be obtained as shown in [27, 79].

More recently, references [67] and Chapter 6 introduce the concept of *blind cooperative jamming* to deal with the absence of eavesdropper CSI in a system where the legitimate receiver CSI is available. In such a system, [67] and Chapter 6 let all cooperative jamming signals span the entire space at the eavesdropper to limit the information leakage to the eavesdropper, while aligning the cooperative jamming signals in the same dimension at the legitimate receiver using **only** the legitimate receiver CSI. More specifically, as an extension of this work, Chapter 6 will show that with the new *blind cooperative jamming* scheme, for the M-helper wiretap channel described in Section 2.2.1 and analyzed in Section 2.5, the same s.d.o.f. of $\frac{M}{M+1}$ can be achieved with no eavesdropper CSI and only with legitimate receiver CSI. Since this is also an upper bound, this implies that the exact s.d.o.f. of such as system is $\frac{M}{M+1}$. However, the problem remains open in all other channel models, including the MAC wiretap channel.

2.10.2 Discontinuity of the Secure d.o.f. in the Channel Gain Space

We next comment on the term "*for almost all channel gains*" that appears in all achievability proofs in this chapter. This term is due to real interference alignment [51, 52], which is based on Diophantine approximation in number theory. The field of Diophantine approximation in number theory deals with approximation of real numbers with rational numbers. [51, Theorem 1 (Khintchine-Groshev)] states that such approximation, which is closely related to our decoding problem, has a lower bound except for a set $\mathcal{A}$ with zero Lebesgue measure. The set $\mathcal{Q}$ of all rational

numbers (channel gains) falls into the set $\mathcal{A}$. In addition, even some sets of irrational numbers (channel gains) also fall into this subset. For example, consider the Gaussian wiretap channel with one helper. If the channel between the transmitters and the eavesdropper is stochastically degraded with respect to the channel between the transmitters and the legitimate receiver, then the coefficients α and β in (2.97) are equal, which results this case falling into the set $\mathcal{Q}$ of rational channel gains[4] and thereby falling into the set $\mathcal{A}$, **even though** they are irrational numbers. In fact, the exact s.d.o.f. for this case is known to be zero due to [14]. This leads to an interesting observation: the s.d.o.f. is discontinuous along the whole $\alpha = \beta$ line in the channel gain space, in addition to at all rational number points. We note that the s.d.o.f. with rational channel gains remains unknown. We also remark that a similar discontinuity phenomenon was investigated without secrecy constraints in [78]. For the K-user fully-connected Gaussian IC, it is widely known that the sum d.o.f. is $K/2$ *for almost all channel gains* [55]. However, in [78], the d.o.f. for any Gaussian IC with nonzero rational channel gains is shown to be *strictly* smaller than $K/2$.

2.10.3 Complex Channel Gains

In the literature, wireless communication channels are generally modeled either as time-varying or time-invariant (constant), and channel gains are modeled either to come from complex numbers or real numbers. Generally, converse proofs carry over to one another in these domains. In the complex case, the scaling of rates with

[4]This is due to the approximation nature of the decoding problem (see [51, Eqn. (8)]).

$\frac{1}{2}\log P$ needs to be replaced with $\log P$ due to real and imaginary components. Achievability techniques also carry over from one setting to another. To the best of our knowledge, there almost always exists a one-to-one connection between interference alignment for time-varying complex channels (with symbol extension) and time-invariant channels (with real interference alignment). Examples include: the K-user Gaussian interference channels in [55] and [52]; the K-user Gaussian interference compound wiretap channel in [27, Section IV] and [29]; and the $2 \times 2 \times 2$ interference channel in [66, Section III.A] and [66, Section III.B]. The channel models we have investigated in this chapter fall into the class of time-invariant (constant) real channel gains. However, we believe that the techniques and results in this chapter can be applied to the models with time-varying and/or complex channel gains. In addition, [31, Theorem 5.6 on page 154] provided an interesting achievable scheme achieving the same 0.5 s.d.o.f. for the Gaussian wiretap channel with a helper where the channel gains are *complex* and *constant*.

2.11 Conclusions

In this chapter, we determined the s.d.o.f. of several fundamental channel models in one-hop wireless networks. We first considered the Gaussian wiretap channel with one helper. While the helper needs to create interference at the eavesdropper, it should not create too much interference at the legitimate receiver. Our approach is based on understanding this trade-off that the helper needs to strike. To that purpose, we developed an upper bound that relates the entropy of the cooperative

jamming signal from the helper and the message rate. In addition, we developed an achievable scheme based on real interference alignment which aligns the cooperative jamming signal from the helper in the same *dimension* as the message signal. This ensures that the information leakage rate is upper bounded by a constant which does not scale with the power. In addition, to help the legitimate user decode the message, our achievable scheme renders the message signal and the cooperative jamming signal distinguishable at the legitimate receiver. This essentially implies that the message signal can *occupy* only half of the available space in terms of the d.o.f. Consequently, we showed that the exact s.d.o.f. of the Gaussian wiretap channel with one helper is $\frac{1}{2}$ by these matching achievability and converse proofs. We then generalized our achievability and converse techniques to the Gaussian wiretap channel with M helpers, Gaussian BC with confidential messages and helpers, two-user Gaussian IC with confidential messages and helpers, and K-user Gaussian MAC wiretap channel. In the multiple-message settings, transmitters needed to send a mix of their own messages and cooperative jamming signals, which can be interpreted as applying *channel prefixing*. We determined the exact s.d.o.f. in all of these system models.

2.12 Appendix

2.12.1 An Alternative Proof for the Multiplexing Gain of the K-User Gaussian Interference Channel

The original proof for this setting is given by [54]. Here, we provide an alternative proof for the $K = 2$ case by using Lemma 2.2, and then extend it to the case of general K.

For $K = 2$, the channel model for the two-user Gaussian IC is

$$Y_1 = h_{1,1}X_1 + h_{2,1}X_2 + N_1 \tag{2.256}$$

$$Y_2 = h_{1,2}X_1 + h_{2,2}X_2 + N_2 \tag{2.257}$$

We start with the definition of the sum rate

$$
\begin{aligned}
nR_1 + nR_2 &= H(W_1, W_2) && (2.258)\\
&= H(W_1, W_2|\mathbf{Y}_1, \mathbf{Y}_2) + I(W_1, W_2; \mathbf{Y}_1, \mathbf{Y}_2) && (2.259)\\
&\leq I(W_1, W_2; \mathbf{Y}_1, \mathbf{Y}_2) + nc_{29} && (2.260)\\
&= h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_1, \mathbf{Y}_2|W_1, W_2) + nc_{29} && (2.261)\\
&\leq h(\mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_1, \mathbf{Y}_2|\mathbf{X}_1, \mathbf{X}_2, W_1, W_2) + nc_{29} && (2.262)\\
&\leq h(\mathbf{Y}_1, \mathbf{Y}_2) + nc_{30} && (2.263)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2|\mathbf{Y}_1, \mathbf{Y}_2) + nc_{30} && (2.264)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2|\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{X}_1, \mathbf{X}_2) + nc_{30} && (2.265)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \mathbf{Y}_1, \mathbf{Y}_2) + nc_{31} && (2.266)\\
&= h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + h(\mathbf{Y}_1, \mathbf{Y}_2|\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + nc_{31} && (2.267)\\
&\leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + nc_{32} && (2.268)
\end{aligned}
$$

where the last inequality follows similar to (2.52) after a derivation similar to (2.54)-(2.58), and, for each j, $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$. Here $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence of $\tilde{N}_j$, which is Gaussian with variance $\sigma_j^2 < \min(1/h_{j,1}^2, 1/h_{j,2}^2)$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other random variables.

Then, we apply Lemma 2.2 to characterize the interference from X_1 to transmitter-

receiver pair 2 and from X_2 to transmitter-receiver pair 1

$$nR_1 + nR_2 \leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2) + nc_{32} \tag{2.269}$$

$$\leq h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) + nc_{32} \tag{2.270}$$

$$\leq h(\mathbf{Y}_2) - H(W_2) + h(\mathbf{Y}_1) - H(W_1) + nc_{33} \tag{2.271}$$

By noting that $H(W_1) = nR_1$ and $H(W_2) = nR_2$, we have

$$2(nR_1 + nR_2) \leq h(\mathbf{Y}_2) + h(\mathbf{Y}_1) + nc_{33} \tag{2.272}$$

$$\leq 2\left(\frac{n}{2}\log P\right) + nc_{34} \tag{2.273}$$

which implies that

$$D_\Sigma \stackrel{\triangle}{=} \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \leq 1 \tag{2.274}$$

i.e., the multiplexing gain of the two-user Gaussian IC is not greater than 1. By the argument in [54, Proposition 1], we can conclude that the multiplexing gain of the K-user Gaussian IC is at most $\frac{K}{2}$.

Chapter 3

Sum Secure Degrees of Freedom of K-User Gaussian Interference Channels: A Unified View

3.1 Introduction

In Chapter 2, we have studied the sum s.d.o.f. of one-hop wireless networks. The common property of the networks studied in Chapter 2 is that, in all cases, there are two receivers. In this chapter, we consider networks with more than two receivers, and generalize the upper bounding techniques in Chapter 2 to these settings, and develop corresponding achievable schemes. In particular, in this chapter, we consider K-user Gaussian IC, and determine its exact sum s.d.o.f. We consider three different secrecy constraints: IC-EE, IC-CM, and IC-CM-EE. We show that for all of these three cases, the exact sum s.d.o.f. is $\frac{K(K-1)}{2K-1}$. We show converses for IC-EE and IC-CM, which imply a converse for IC-CM-EE. We show achievability for IC-CM-EE, which implies achievability for IC-EE and IC-CM. We develop the converses by relating the channel inputs of interfering users to the reliable rates of the interfered users, and by quantifying the secrecy penalty in terms of the eavesdroppers' observations. Our achievability uses structured signaling, structured cooperative jamming, channel prefixing, and asymptotic real interference alignment. While the traditional interference alignment provides some amount of secrecy by mixing unintended sig-

nals in a smaller sub-space at every receiver, in order to attain the optimum sum s.d.o.f., we incorporate structured cooperative jamming into the achievable scheme, and intricately design the structure of all of the transmitted signals jointly.

3.2 System Model, Definitions and the Result

The input-output relationships for a K-user Gaussian IC with secrecy constraints (Figure 1.7) are given by

$$Y_i = \sum_{j=1}^{K} h_{ji} X_j + N_i, \qquad i = 1, \ldots, K \tag{3.1}$$

$$Z = \sum_{j=1}^{K} g_j X_j + N_Z \tag{3.2}$$

where Y_i is the channel output of receiver i, Z is the channel output of the external eavesdropper (if there is any), X_i is the channel input of transmitter i, h_{ji} is the channel gain of the jth transmitter to the ith receiver, g_j is the channel gain of the jth transmitter to the eavesdropper (if there is any), and $\{N_1, \ldots, N_K, N_Z\}$ are mutually independent zero-mean unit-variance Gaussian random variables. All the channel gains are time-invariant, and independently drawn from continuous distributions. We further assume that all h_{ji} are non-zero, and all g_j are non-zero if there is an external eavesdropper. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_i^2\right] \leq P$, for $i = 1, \ldots, K$.

Each transmitter i intends to send a message W_i, uniformly chosen from a set $\mathcal{W}_i$, to receiver i. The rate of the message is $R_i \triangleq \frac{1}{n} \log |\mathcal{W}_i|$, where n is the number

of channel uses. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ to encode the message, where $\mathbf{X}_i \triangleq X_i^n$ is the n-length channel input of user i. We use boldface letters to denote n-length vector signals, e.g., $\mathbf{X}_i \triangleq X_i^n$, $\mathbf{Y}_j \triangleq Y_j^n$, $\mathbf{Z} \triangleq Z^n$, etc. The legitimate receiver j decodes the message as $\hat{W}_j$ based on its observation $\mathbf{Y}_j$. A rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if for any $\epsilon > 0$, there exist joint n-length codes such that each receiver j can decode the corresponding message reliably, i.e., the probability of decoding error is less than ϵ for all messages,

$$\max_j \Pr\left[W_j \neq \hat{W}_j\right] \leq \epsilon \tag{3.3}$$

and the corresponding secrecy requirement is satisfied. We consider three different secrecy requirements:

1) In IC-EE, Figure 1.8(a), all of the messages are kept information-theoretically secure against the external eavesdropper,

$$\frac{1}{n} H(W_1, \ldots, W_K | \mathbf{Z}) \geq \frac{1}{n} H(W_1, \ldots, W_K) - \epsilon \tag{3.4}$$

2) In IC-CM, Figure 1.8(b), all unintended messages are kept information-theoretically secure against each receiver,

$$\frac{1}{n} H(W_{-i}^K | \mathbf{Y}_i) \geq \frac{1}{n} H(W_{-i}^K) - \epsilon, \qquad i = 1, \ldots, K \tag{3.5}$$

where $W_{-i}^K \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$.

3) In IC-CM-EE, Figure 1.8(c), all of the messages are kept information-theoretically secure against both the $K-1$ unintended receivers and the eavesdropper, i.e., we impose both secrecy constraints in (3.4) and (3.5).

The supremum of all sum achievable secrecy rates is the sum secrecy capacity $C_{s,\Sigma}$, and the sum s.d.o.f., $D_{s,\Sigma}$, is defined as

$$D_{s,\Sigma} \triangleq \lim_{P\to\infty} \frac{C_{s,\Sigma}}{\frac{1}{2}\log P} = \lim_{P\to\infty} \sup \frac{R_1 + \cdots + R_K}{\frac{1}{2}\log P} \tag{3.6}$$

The main result of this chapter is stated in the following theorem.

Theorem 3.1 *The sum s.d.o.f. of the K-user IC-EE, IC-CM, and IC-CM-EE is $\frac{K(K-1)}{2K-1}$ for almost all channel gains.*

3.3 Preliminaries

3.3.1 Role of a Helper Lemma

For completeness, we repeat Lemma 2.2 in Chapter 2 here, which is called *role of a helper lemma*. In Chapter 2, there is only one legitimate receiver, whereas in this chapter, there are K legitimate receivers. While (2.65) in Lemma 2.2 is written for receiver 1, (3.7) in the following lemma is written for any kth receiver. This lemma identifies a constraint on the signal of a given transmitter, based on the decodability of another transmitter's message at its intended receiver.

Lemma 3.1 *For reliable decoding of the kth transmitter's signal at the kth receiver,*

the channel input of transmitter $i \neq k$, $\mathbf{X}_i$, must satisfy

$$h(\mathbf{X}_i + \tilde{\mathbf{N}}) \leq h(\mathbf{Y}_k) - nR_k + nc \tag{3.7}$$

where c is a constant which does not depend on P, and $\tilde{N}$ is a new Gaussian random variable independent of all other random variables with $\sigma^2_{\tilde{N}} < \frac{1}{h^2_{ik}}$, and $\tilde{\mathbf{N}}$ is an i.i.d. sequence of $\tilde{N}$.

Lemma 3.1 gives an upper bound on the differential entropy of (a noisy version of) the signal of any given transmitter, transmitter i in (3.7), in terms of the differential entropy of the channel output and the message rate $nR_k = H(W_k)$, of a user k, based on the decodability of message W_k at its intended receiver. The inequality in this lemma, (3.7), can alternatively be interpreted as an upper bound on the message rate, i.e., on nR_k, in terms of the difference of the differential entropies of the channel output of a receiver k and the channel input of a transmitter i; in particular, the higher the differential entropy of the signal coming from user i, the lower this upper bound will be on the rate of user k. This motivates not using i.i.d. Gaussian signals which have the highest differential entropy. Also note that this lemma does not involve any secrecy constraints, and is based only on the decodability of the messages at their intended receivers.

3.4 Converse for IC-EE

In this section, we develop a converse for the K-user IC-EE (see Figure 1.8(a)) defined in (3.1) and (3.2) with the secrecy constraint (3.4). We start with the sum rate:

$$n\sum_{i=1}^{K} R_i = \sum_{i=1}^{K} H(W_i) = H(W_1^K) \tag{3.8}$$

$$\leq I(W_1^K; \mathbf{Y}_1^K) - I(W_1^K; \mathbf{Z}) + nc_{34} \tag{3.9}$$

$$\leq I(W_1^K; \mathbf{Y}_1^K, \mathbf{Z}) - I(W_1^K; \mathbf{Z}) + nc_{34} \tag{3.10}$$

$$= I(W_1^K; \mathbf{Y}_1^K|\mathbf{Z}) + nc_{34} \tag{3.11}$$

$$\leq I(\mathbf{X}_1^K; \mathbf{Y}_1^K|\mathbf{Z}) + nc_{34} \tag{3.12}$$

$$= h(\mathbf{Y}_1^K|\mathbf{Z}) - h(\mathbf{Y}_1^K|\mathbf{Z}, \mathbf{X}_1^K) + nc_{34} \tag{3.13}$$

$$= h(\mathbf{Y}_1^K|\mathbf{Z}) - h(\mathbf{N}_1^K|\mathbf{Z}, \mathbf{X}_1^K) + nc_{34} \tag{3.14}$$

$$\leq h(\mathbf{Y}_1^K|\mathbf{Z}) + nc_{35} \tag{3.15}$$

$$= h(\mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_{35} \tag{3.16}$$

where $W_1^K \triangleq \{W_j\}_{j=1}^K$, $\mathbf{X}_1^K \triangleq \{\mathbf{X}_j\}_{j=1}^K$, $\mathbf{Y}_1^K \triangleq \{\mathbf{Y}_j\}_{j=1}^K$, and all the c_is in this chapter are constants which do not depend on P.

For each j, we introduce $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$, where $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence of $\tilde{N}_j$ which is a zero-mean Gaussian random variable with variance $\sigma_j^2 < \min(\min_i 1/h_{ji}^2, 1/g_j^2)$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other

random variables. Continuing from (3.16),

$$n\sum_{i=1}^{K} R_i \le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_{35} \tag{3.17}$$

$$\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{X}}_1^K|\mathbf{X}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_{35} \tag{3.18}$$

$$= h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\tilde{\mathbf{N}}_1^K) - h(\mathbf{Z}) + nc_{35} \tag{3.19}$$

$$\le h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K, \mathbf{Z}) - h(\mathbf{Z}) + nc_{36} \tag{3.20}$$

$$= h(\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_{36} \tag{3.21}$$

$$\le h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_{37} \tag{3.22}$$

where $\tilde{\mathbf{X}}_1^K \triangleq \{\tilde{\mathbf{X}}_j\}_{j=1}^K$, and the last inequality is due to the fact that $h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K) \le nc'$, i.e., given all the channel inputs (disturbed by small Gaussian noises), the channel outputs can be *reconstructed*, which is shown as follows

$$h(\mathbf{Y}_1^K, \mathbf{Z}|\tilde{\mathbf{X}}_1^K)$$

$$\le \left[\sum_{j=1}^{K} h(\mathbf{Y}_j|\tilde{\mathbf{X}}_1^K)\right] + h(\mathbf{Z}|\tilde{\mathbf{X}}_1^K) \tag{3.23}$$

$$= \left[\sum_{j=1}^{K} h\left(\sum_{i=1}^{K} h_{ij}(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right)\right] + h\left(\sum_{i=1}^{K} g_i(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_Z \middle| \tilde{\mathbf{X}}_1^K\right) \tag{3.24}$$

$$= \left[\sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right)\right] + h\left(-\sum_{i=1}^{K} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_Z \middle| \tilde{\mathbf{X}}_1^K\right) \tag{3.25}$$

$$\le \left[\sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j\right)\right] + h\left(-\sum_{i=1}^{K} g_i\tilde{\mathbf{N}}_i + \mathbf{N}_Z\right) \tag{3.26}$$

$$\triangleq nc_{38} \tag{3.27}$$

Next, we note

$$h(\tilde{\mathbf{X}}_j) \leq h(g_j \mathbf{X}_j + \mathbf{N}_Z) + nc_{39} \leq h(\mathbf{Z}) + nc_{39}, \qquad j = 1, \ldots, K \tag{3.28}$$

where the inequalities are due to the differential entropy version of [68, Problem 2.14]. Inserting (3.28) into (3.22), for any $j = 1, \ldots, K$, we get

$$n \sum_{i=1}^{K} R_i \leq h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Z}) + nc_3 \tag{3.29}$$

$$\leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Z}) + nc_3 \tag{3.30}$$

$$\leq \sum_{i=1, i \neq j}^{K} h(\tilde{\mathbf{X}}_i) + nc_{40} \tag{3.31}$$

which means that the net effect of the presence of an eavesdropper is to *eliminate* one of the channel inputs; we call this the *secrecy penalty*.

We apply the *role of a helper lemma*, Lemma 3.1, to each $\tilde{\mathbf{X}}_i$ with $k = i + 1$ (for $i = K$, $k = 1$), in (3.31) as

$$n \sum_{i=1}^{K} R_i \leq h(\tilde{\mathbf{X}}_1) + h(\tilde{\mathbf{X}}_2) + \cdots + h(\tilde{\mathbf{X}}_{j-1}) + h(\tilde{\mathbf{X}}_{j+1}) + \cdots + h(\tilde{\mathbf{X}}_K) + nc_{41} \tag{3.32}$$

$$\leq [h(\mathbf{Y}_2) - nR_2] + [h(\mathbf{Y}_3) - nR_3] + \cdots + [h(\mathbf{Y}_j) - nR_j]$$

$$+ [h(\mathbf{Y}_{j+2}) - nR_{j+2}] + \cdots + [h(\mathbf{Y}_K) - nR_K] + [h(\mathbf{Y}_1) - nR_1] + nc_{42} \tag{3.33}$$

By noting that $h(\mathbf{Y}_i) \leq \frac{n}{2}\log P + nc_i'$ for each i, we have

$$2n\sum_{i=1}^{K} R_i \leq (K-1)\left(\frac{n}{2}\log P\right) + nR_{(j+1) \bmod K} + nc_{43} \tag{3.34}$$

for $j = 1, \ldots, K$. Therefore, we have a total of K bounds in (3.34) for $j = 1, \ldots, K$. Summing these K bounds, we obtain:

$$(2K-1)n\sum_{i=1}^{K} R_i \leq K(K-1)\left(\frac{n}{2}\log P\right) + nc_{44} \tag{3.35}$$

which gives

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \tag{3.36}$$

completing the converse for IC-EE.

3.5 Converse for IC-CM

In this section, we develop a converse for the K-user IC-CM (see Figure 1.8(b)). We focus on the secrecy constraint (3.5) at a single receiver, say j, as an eavesdropper,

and start with the sum rate corresponding to all unintended messages at receiver j:

$$n \sum_{i=1,i\neq j}^{K} R_i = \sum_{i=1,i\neq j}^{K} H(W_i) = H(W_{-j}^K) \tag{3.37}$$

$$\leq I(W_{-j}^K; \mathbf{Y}_{-j}^K) - I(W_{-j}^K; \mathbf{Y}_j) + nc_{45} \tag{3.38}$$

$$\leq I(W_{-j}^K; \mathbf{Y}_{-j}^K, \mathbf{Y}_j) - I(W_{-j}^K; \mathbf{Y}_j) + nc_{45} \tag{3.39}$$

$$= I(W_{-j}^K; \mathbf{Y}_{-j}^K | \mathbf{Y}_j) + nc_{45} \tag{3.40}$$

$$\leq I(\mathbf{X}_{-j}^K; \mathbf{Y}_{-j}^K | \mathbf{Y}_j) + nc_{45} \tag{3.41}$$

$$= h(\mathbf{Y}_{-j}^K | \mathbf{Y}_j) - h(\mathbf{Y}_{-j}^K | \mathbf{Y}_j, \mathbf{X}_{-j}^K) + nc_{45} \tag{3.42}$$

$$\leq h(\mathbf{Y}_{-j}^K | \mathbf{Y}_j) - h(\mathbf{Y}_{-j}^K | \mathbf{Y}_j, \mathbf{X}_1^K) + nc_{45} \tag{3.43}$$

$$= h(\mathbf{Y}_{-j}^K | \mathbf{Y}_j) - h(\mathbf{N}_{-j}^K | \mathbf{Y}_j, \mathbf{X}_1^K) + nc_{45} \tag{3.44}$$

$$\leq h(\mathbf{Y}_{-j}^K | \mathbf{Y}_j) + nc_{46} \tag{3.45}$$

$$= h(\mathbf{Y}_{-j}^K, \mathbf{Y}_j) - h(\mathbf{Y}_j) + nc_{46} \tag{3.46}$$

$$= h(\mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{46} \tag{3.47}$$

where $W_{-j}^K \triangleq \{W_i\}_{i=1,i\neq j}^K$ is the message set containing all unintended messages with respect to receiver j, $\mathbf{X}_{-j}^K \triangleq \{\mathbf{X}_i\}_{i=1,i\neq j}^K$ and $\mathbf{Y}_{-j}^K \triangleq \{\mathbf{Y}_i\}_{i=1,i\neq j}^K$.

For each j, we introduce $\tilde{\mathbf{X}}_j = \mathbf{X}_j + \tilde{\mathbf{N}}_j$, where $\tilde{\mathbf{N}}_j$ is an i.i.d. sequence of $\tilde{N}_j$ which is a zero-mean Gaussian random variable with variance $\sigma_j^2 < \min_i 1/h_{ji}^2$. Also, $\{\tilde{N}_j\}_{j=1}^K$ are mutually independent, and are independent of all other random

variables. Continuing from (3.47),

$$n\sum_{i=1,i\neq j}^{K} R_i \leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{46} \tag{3.48}$$

$$\leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{X}}_1^K|\mathbf{Y}_1^K, \mathbf{X}_1^K) - h(\mathbf{Y}_j) + nc_{46} \tag{3.49}$$

$$= h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\tilde{\mathbf{N}}_1^K) - h(\mathbf{Y}_j) + nc_{46} \tag{3.50}$$

$$\leq h(\tilde{\mathbf{X}}_1^K, \mathbf{Y}_1^K) - h(\mathbf{Y}_j) + nc_{47} \tag{3.51}$$

$$= h(\tilde{\mathbf{X}}_1^K) + h(\mathbf{Y}_1^K|\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{47} \tag{3.52}$$

$$\leq h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{48} \tag{3.53}$$

where the last inequality is due to the fact that $h(\mathbf{Y}_1^K|\tilde{\mathbf{X}}_1^K) \leq nc'$, i.e., given all the channel inputs (disturbed by small Gaussian noises), the channel outputs can be *reconstructed*, which is shown as follows

$$h(\mathbf{Y}_1^K|\tilde{\mathbf{X}}_1^K) \leq \sum_{j=1}^{K} h(\mathbf{Y}_j|\tilde{\mathbf{X}}_1^K) \tag{3.54}$$

$$= \sum_{j=1}^{K} h\left(\sum_{i=1}^{K} h_{ij}(\tilde{\mathbf{X}}_i - \tilde{\mathbf{N}}_i) + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right) \tag{3.55}$$

$$= \sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j \middle| \tilde{\mathbf{X}}_1^K\right) \tag{3.56}$$

$$\leq \sum_{j=1}^{K} h\left(-\sum_{i=1}^{K} h_{ij}\tilde{\mathbf{N}}_i + \mathbf{N}_j\right) \tag{3.57}$$

$$\stackrel{\triangle}{=} nc_{49} \tag{3.58}$$

We apply the *role of a helper lemma*, Lemma 3.1, to each $\tilde{\mathbf{X}}_i$ with $k = i + 1$

(for $i = K$, $k = 1$), in (3.53) as

$$n \sum_{i=1, i\neq j}^{K} R_i \leq h(\tilde{\mathbf{X}}_1^K) - h(\mathbf{Y}_j) + nc_{14} \tag{3.59}$$

$$\leq \sum_{i=1}^{K} h(\tilde{\mathbf{X}}_i) - h(\mathbf{Y}_j) + nc_{14} \tag{3.60}$$

$$\leq \sum_{i=1}^{K-1} \Big[h(\mathbf{Y}_{i+1}) - nR_{i+1}\Big] + \Big[h(\mathbf{Y}_1) - nR_1\Big] - h(\mathbf{Y}_j) + nc_{50} \tag{3.61}$$

$$= \sum_{i=1}^{K} \Big[h(\mathbf{Y}_i) - nR_i\Big] - h(\mathbf{Y}_j) + nc_{50} \tag{3.62}$$

By noting that $h(\mathbf{Y}_i) \leq \frac{n}{2} \log P + nc_i'$ for each i, we have

$$nR_j + 2n \sum_{i=1, i\neq j}^{K} R_i \leq \sum_{i=1, i\neq j}^{K} h(\mathbf{Y}_i) + nc_{50} \tag{3.63}$$

$$\leq (K-1) \left(\frac{n}{2} \log P\right) + nc_{51} \tag{3.64}$$

for $j = 1, \ldots, K$. Therefore, we have a total of K bounds in (3.64) for $j = 1, \ldots, K$. Summing these K bounds, we obtain:

$$(2K-1)n \sum_{i=1}^{K} R_i \leq K(K-1) \left(\frac{n}{2} \log P\right) + nc_{52} \tag{3.65}$$

which gives

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \tag{3.66}$$

completing the converse for IC-CM.

3.6 Achievability

In this section, we provide achievability for the K-user IC-CM-EE (see Figure 1.8(c)), which will imply achievability for K-user IC-EE and K-user IC-CM. We will prove that, for almost all channel gains, a sum s.d.o.f. lower bound of

$$D_{s,\Sigma} \geq \frac{K(K-1)}{2K-1} \tag{3.67}$$

is achievable for the K-user IC-CM-EE.

3.6.1 Background

In this section, we will summarize the achievability scheme for the two-user IC-CM in Section 2.7, Chapter 2, motivate the need for simultaneous alignment of multiple signals at multiple receivers in this K-user case, and provide an example of simultaneously aligning two signals at two receivers via asymptotic real alignment [52]. We provide the general achievable scheme for $K > 2$ in Section 3.6.2 via cooperative jamming and asymptotic real alignment, and show that it achieves the sum s.d.o.f. in (3.67) via a detailed performance analysis in Section 3.6.3.

In the achievable scheme for $K = 2$ in Chapter 2, four mutually independent discrete random variables $\{V_1, U_1, V_2, U_2\}$ are employed (see Figure 2.4 in Chapter 2). Each of them is uniformly and independently drawn from the discrete constellation $C(a, Q)$ given in (2.73). The role of V_i is to carry message W_i, and the role of U_i is to cooperatively jam receiver i to help transmitter-receiver pair j, where $j \neq i$,

for $i, j = 1, 2$. By carefully selecting the transmit coefficients, U_1 and V_2 are aligned at receiver 1, and U_2 and V_1 are aligned at receiver 2; and therefore, U_1 protects V_2, and U_2 protects V_1. By this signalling scheme, information leakage rates are upper bounded by constants, and the message rates are made to scale with power P, reaching the s.d.o.f. capacity of the two-user IC-CM which is $\frac{2}{3}$.

Here, for the K-user IC-CM-EE, we employ a total of K^2 random variables,

$$V_{ij}, \quad i, j = 1, \ldots, K, \; j \neq i \tag{3.68}$$

$$U_k, \quad k = 1, \ldots, K \tag{3.69}$$

which are illustrated in Figure 3.1 for the case of $K = 3$. The scheme proposed here has two major differences from Chapter 2, Section 2.7: 1) Instead of using a single random variable to carry a message, we use a total of $K-1$ random variables to carry each message. For transmitter i, $K-1$ random variables $\{V_{ij}\}_{j \neq i}$, each representing a sub-message, collectively carry message W_i. 2) Rather than protecting one message at one receiver, each U_k simultaneously protects a portion of all sub-messages at all required receivers. More specifically, U_k protects $\{V_{ik}\}_{i \neq k, i \neq j}$ at receivers j, and at the eavesdropper (if there is any). For example, in Figure 3.1, U_1 protects V_{21} and V_{31} where necessary. In particular, U_1 protects V_{21} at receivers 1, 3 and the eavesdropper; and it protects V_{31} at receivers 1, 2 and the eavesdropper. As a technical challenge, this requires U_1 to be aligned with the same signal, say V_{21}, at multiple receivers simultaneously, i.e., at receivers 1, 3 and the eavesdropper. These particular alignments are circled by ellipsoids in Figure 3.1. We do these

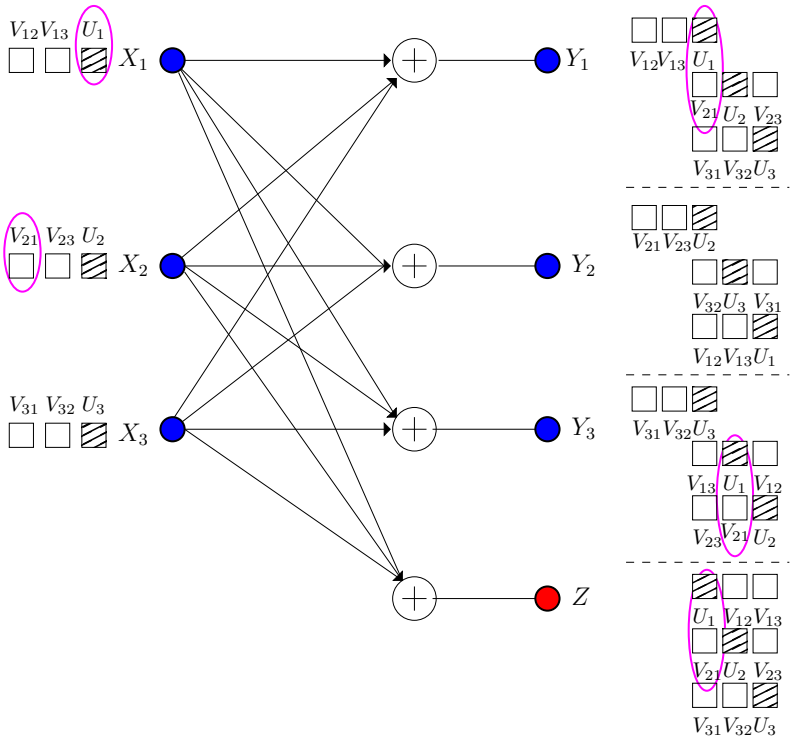


Figure 3.1: Illustration of alignment for 3-user IC-CM-EE. U_1 and V_{21} are marked to emphasize their simultaneous alignment at Y_1, Y_3 and Z.

simultaneous alignments using asymptotic real alignment technique proposed in [52] and used in [29, 53].

For illustration purposes, in the rest of this section, we demonstrate how we can align two signals at two receivers simultaneously; in particular, we will align U_1 with V_{21} at Y_1 and Y_3, simultaneously. Towards this end, we will further divide the random variable V_{21}, which represents a sub-message, into a large number of random variables denoted as $V_{21} \triangleq \{v_{21t} : t = 1, \ldots, |T_1|\}$. We then send each one of these random variables after multiplying it with one of the coefficients in the following set which serves as the set of *dimensions*:

$$T_1 = \left\{ h_{11}^{r_{11}} h_{21}^{r_{21}} h_{13}^{r_{13}} h_{23}^{r_{23}} : \ r_{11}, r_{21}, r_{13}, r_{23} \in \{1, \ldots, m\} \right\} \tag{3.70}$$

where m is a large constant. To perform the alignment, we let U_1 have the same detailed structure as V_{21}, i.e., U_1 is also divided into a large number of random variables as $U_1 \triangleq \{u_{1t} : t = 1, \ldots, |T_1|\}$. At receiver 1, the elements of U_1 from transmitter 1 occupy the dimensions $h_{11}T_1$ and the elements of V_{21} from transmitter 2 occupy the dimensions $h_{21}T_1$. Although these two sets are not the same, their intersection contains nearly as many elements as T_1, i.e.,

$$|h_{11}T_1 \cap h_{21}T_1| = m^2(m-1)^2 \approx m^4 = |T_1| \tag{3.71}$$

when m is large, i.e., almost all elements of U_1 and V_{21} are asymptotically aligned at receiver 1. The same argument applies for receiver 3. At receiver 3, the elements of U_1 from transmitter 1 occupy the dimensions $h_{13}T_1$ and the elements of V_{21} from transmitter 2 occupy the dimensions $h_{23}T_1$. Again, although these two sets are not the same, their intersection contains nearly as many elements as T_1. Therefore, almost all elements of U_1 and V_{21} are aligned at receivers 1 and 3, simultaneously. These simultaneous alignments are depicted in Figure 3.2. In the following section, we use this basic idea to align multiple signals at multiple receivers simultaneously. This will require a more intricate design of signals and dimensions.

3.6.2 General Achievable Scheme via Asymptotic Alignment

Here, we give the general achievable scheme for the K-user IC-CM-EE. Let m be a large constant. Let us define sets T_i, for $i = 1, \ldots, K$, which will represent

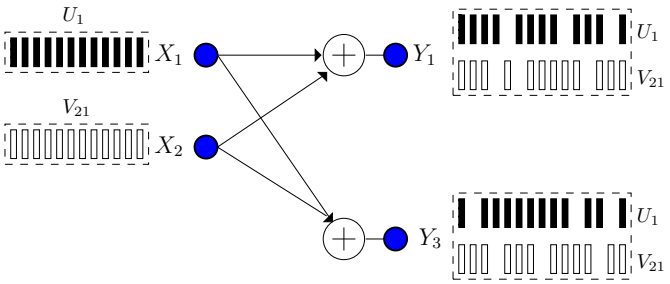


Figure 3.2: Illustration of alignment at multiple receivers.

dimensions as follows:

$$T_i \triangleq \left\{ h_{ii}^{r_{ii}} \left(\prod_{j,k=1,j\neq k}^{K} h_{jk}^{r_{jk}} \right) \left(\prod_{j=1}^{K} g_j^{s_j} \right) : \ r_{jk}, s_j \in \{1, \ldots, m\} \right\} \tag{3.72}$$

Let M_i be the cardinality of T_i. Note that all M_i are the same, thus we denote them as M,

$$M \triangleq m^{1+K(K-1)+K} = m^{K^2+1} \tag{3.73}$$

For each transmitter i, for $j \neq i$, let $\mathbf{t}_{ij}$ be the vector containing all the elements in the set T_j. Therefore, $\mathbf{t}_{ij}$ is an M-dimensional vector containing M rationally independent real numbers in T_j. The sets $\mathbf{t}_{ij}$ will represent the *dimensions* along which message signals are transmitted. In particular, for any given (i, j) with $i \neq j$, $\mathbf{t}_{ij}$ will represent the dimensions in which message signal V_{ij} is transmitted. In addition, for each transmitter i, let $\mathbf{t}_{(i)}$ be the vector containing all the elements in the set T_i. Therefore, $\mathbf{t}_{(i)}$ is an M-dimensional vector containing M rationally independent real numbers in T_i. The sets $\mathbf{t}_{(i)}$ will represent the *dimensions* along which cooperative jamming signals are transmitted. In particular, for any given i, $\mathbf{t}_{(i)}$ will represent the dimensions in which cooperative jamming signal U_i is transmitted.

Let us define a KM dimensional vector $\mathbf{b}_i$ by stacking $\mathbf{t}_{ij}$ and $\mathbf{t}_{(i)}$ as

$$\mathbf{b}_i^T = \left[\mathbf{t}_{i1}^T, \ldots, \mathbf{t}_{i,i-1}^T, \mathbf{t}_{i,i+1}^T, \ldots, \mathbf{t}_{iK}^T, \mathbf{t}_{(i)}^T\right] \tag{3.74}$$

Then, transmitter i generates a vector $\mathbf{a}_i$, which contains a total of KM discrete signals each identically and independently drawn from $C(a, Q)$. For convenience, we partition this transmitted signal as

$$\mathbf{a}_i^T = \left[\mathbf{v}_{i1}^T, \ldots, \mathbf{v}_{i,i-1}^T, \mathbf{v}_{i,i+1}^T, \ldots, \mathbf{v}_{iK}^T, \mathbf{u}_i^T\right] \tag{3.75}$$

where $\mathbf{v}_{ij}$ represents the information symbols in V_{ij}, and $\mathbf{u}_i$ represents the cooperative jamming signal in U_i. Each of these vectors has length M, and therefore, the total length of $\mathbf{a}_i$ is KM. The channel input of transmitter i is

$$x_i = \mathbf{a}_i^T \mathbf{b}_i \tag{3.76}$$

Before we investigate the performance of this signalling scheme in Section 3.6.3, we analyze the structure of the received signal at the receivers. Without loss of generality we will focus on receiver 1; by symmetry, a similar structure will exist at all other receivers. We observe that in addition to the additive Gaussian noise, receiver 1 receives all the vectors $\mathbf{v}_{jk}$ for all $j, k\,(j \neq k)$ and $\mathbf{u}_i$ for all i. All of these signals get multiplied with the corresponding channel gains before they arrive at receiver 1. Due to the specific signalling structure used at the transmitters, and the multiplications with different channel gains over the wireless communication

channel, the signals arrive at the receiver lying in various different *dimensions*.

To see the detailed structure of the received signals at the receivers, let us define $\tilde{T}_i$ as a superset of T_i, as follows

$$\tilde{T}_i \triangleq \left\{ h_{ii}^{r_{ii}} \left(\prod_{j,k=1,j\neq k}^{K} h_{jk}^{r_{jk}} \right) \left(\prod_{j=1}^{K} g_j^{s_j} \right) : \; r_{jk}, s_j \in \{1, \ldots, m+1\} \right\} \tag{3.77}$$

The information symbols coming from transmitter 1 are in vectors $\mathbf{v}_{12}, \mathbf{v}_{13}$, ..., $\mathbf{v}_{1K}$ which are multiplied by coefficients in $\mathbf{t}_{12}, \mathbf{t}_{13}, \ldots, \mathbf{t}_{1K}$ before they are sent. These coefficients come from sets $T_2, T_3, \ldots, T_K$, respectively. After going through the channel, all of these coefficients get multiplied by h_{11}. Therefore, the receiving coefficients of $\mathbf{v}_{12}, \mathbf{v}_{13}, \ldots, \mathbf{v}_{1K}$ are $h_{11}\mathbf{t}_{12}, h_{11}\mathbf{t}_{13}, \ldots, h_{11}\mathbf{t}_{1K}$, which are the *dimensions* in the sets $h_{11}T_2, h_{11}T_3, \ldots, h_{11}T_K$, respectively. By construction, since each T_i has powers of h_{ii} in it (but no h_{jj}), these dimensions are *separate*. These correspond to *separate* boxes of V_{12} and V_{13} at receiver 1 in Figure 3.1 for the example case of $K = 3$.

On the other hand, all of the cooperative jamming signals from all of the transmitters $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_K$ come to receiver 1 with received coefficients $h_{11}\mathbf{t}_{(1)}$, $h_{21}\mathbf{t}_{(2)}$, ..., $h_{K1}\mathbf{t}_{(K)}$, which are the *dimensions* in the sets $h_{11}T_1, h_{21}T_2, \ldots, h_{K1}T_K$, respectively. We note that all of these dimensions are separate among themselves, and they are separate from the dimensions of the message signals coming from transmitter 1. That is, all of the dimensions in $h_{11}T_2, h_{11}T_3, \ldots, h_{11}T_K$ and $h_{11}T_1, h_{21}T_2, \ldots, h_{K1}T_K$ are all mutually different, again owing to the fact that each T_i contains powers of h_{ii} in it. These correspond to separate boxes of V_{12}, V_{13}, U_1, U_2 and U_3 at receiver

1 in Figure 3.1 for the example case of $K = 3$.

Next, we note that each $\mathbf{u}_i$ is aligned together with all of the $\mathbf{v}_{ji}$ coming from the jth transmitter, with $j \neq i$ and $j \neq 1$, at receiver 1. Note that $\mathbf{u}_i$ occupies dimensions $h_{i1}T_i$ and $\mathbf{v}_{ji}$ (for any $j \neq i$ and $j \neq 1$) occupies dimensions $h_{j1}T_i$ at receiver 1. From the arguments in Section 3.6.1, $\mathbf{u}_i$ and $\mathbf{v}_{ji}$ (with $j \neq i$ and $j \neq 1$) are asymptotically aligned. More formally, we note that $\mathbf{u}_i$ occupies dimensions $h_{i1}T_i$ which is contained in $\tilde{T}_i$. Similarly, all $\mathbf{v}_{ji}$, with $j \neq i$ and $j \neq 1$, occupy dimensions $h_{j1}T_i$, respectively, which are all contained in $\tilde{T}_i$. Therefore, $\mathbf{u}_i$ and all $\mathbf{v}_{ji}$ (with $j \neq i$ and $j \neq 1$) are all aligned along $\tilde{T}_i$. These alignments are shown as U_1 being aligned with V_{21} and V_{31}; U_2 being aligned with V_{32}; and U_3 being aligned with V_{23} at receiver 1 in Figure 3.1 for the example case of $K = 3$. Further, we note that, since only T_i and $\tilde{T}_i$ contain powers of h_{ii}, the dimensions $h_{11}T_2, h_{11}T_3, \ldots, h_{11}T_K, \tilde{T}_1, \tilde{T}_2, \ldots, \tilde{T}_K$ are all separable. This implies that all the elements in the set

$$R_1 \triangleq \left(\bigcup_{j=2}^{K} h_{11}T_j\right) \bigcup \left(\bigcup_{j=2}^{K} \tilde{T}_j\right) \bigcup \tilde{T}_1 \tag{3.78}$$

are rationally independent, and thereby the cardinality of R_1 is

$$M_R \triangleq |R_1| = (K-1)m^{1+K(K-1)+K} + K(m+1)^{1+K(K-1)+K} \tag{3.79}$$

$$= (K-1)m^{K^2+1} + K(m+1)^{K^2+1} \tag{3.80}$$

3.6.3 Performance Analysis

We will compute the secrecy rates achievable with the asymptotic alignment based scheme proposed in Section 3.6.2 by using the following theorem.

Theorem 3.2 *For K-user interference channels with confidential messages and one external eavesdropper, the following rate region is achievable*

$$R_i \geq I(V_i; Y_i) - \max_{j \in \mathcal{K}_{0,-i}} I(V_i; Y_j | V_{-i}^K), \qquad i = 1, \ldots, K \tag{3.81}$$

where for convenience we denote Z by Y_0, $V_{-i}^K \triangleq \{V_j\}_{j=1, j\neq i}^K$ and $\mathcal{K}_{0,-i} = \{0, 1, \ldots, i-1, i+1, \ldots, K\}$. The auxiliary random variables $\{V_i\}_{i=1}^K$ are mutually independent, and for each i, we have the following Markov chain $V_i \to X_i \to (Y_1, \ldots, Y_K)$.

In developing the achievable rates in Theorem 3.2, we focus on a single transmitter, say i, and consider the compound setting associated with message W_i, where this message needs to be secured against a total of K eavesdroppers, with $K-1$ of them being the other legitimate receivers ($j \neq i$) and the remaining one being the external eavesdropper ($j = 0$). A proof of this theorem is given in Appendix 3.8.1.

We apply Theorem 3.2 to our alignment based scheme proposed in Section 3.6.2 by selecting V_i used in (3.81) as

$$V_i \triangleq (\mathbf{v}_{i1}^T, \ldots, \mathbf{v}_{i,i-1}^T, \mathbf{v}_{i,i+1}^T, \ldots, \mathbf{v}_{iK}^T) \tag{3.82}$$

for $i = 1, \ldots, K$. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(M_R+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, based on Lemma 2.3 in Chapter 2, the probability of error of estimating V_i based on Y_i can

be upper bounded by a function decreasing exponentially fast in P, by choosing a γ, a positive constant independent of P to normalize the average power of the input signals, as

$$0 < \gamma \leq \frac{1}{\sum_{t\in\mathbf{b}_i} |t|} = \frac{1}{\sum_{i=1}^{K} \sum_{t_i\in T_i} |t_i|} \tag{3.83}$$

Furthermore, by Fano's inequality, we can conclude that

$$I(V_i; Y_i) \geq \frac{(K-1)m^{K^2+1}(1-\delta)}{M_R + \delta} \left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.84}$$

$$= \frac{(K-1)(1-\delta)}{K - 1 + K\left(1+\frac{1}{m}\right)^{K^2+1} + \frac{\delta}{m^{K^2+1}}} \left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.85}$$

where $o(\cdot)$ is the little-o function. This provides a lower bound for the first term in (3.81).

Next, we need to derive an upper bound for the second item in (3.81), i.e, the secrecy penalty. For any $i \in \mathcal{K} = \{1, \ldots, K\}$ and $j \in \mathcal{K}_{-i} = \{1, \ldots, i-1, i+1, \ldots, K\}$, by the Markov chain $V_i \to (\sum_{k=1}^{K} h_{kj} X_{kj}, V_{-i}^K) \to Y_j$,

$$I(V_i; Y_j | V_{-i}^K) \leq I\left(V_i; \sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) \tag{3.86}$$

$$= H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) - H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_1^K\right) \tag{3.87}$$

where $V_1^K = \{V_1, \ldots, V_K\}$. The first term in (3.87) can be rewritten as

$$H\left(\sum_{k=1}^{K} h_{kj} X_k \Big| V_{-i}^K\right) = H\left(\sum_{k=1}^{K} h_{kj}\mathbf{u}_k^T\mathbf{t}_{(k)} + \sum_{\substack{k=1\\k\neq i}}^{K} h_{ij}\mathbf{v}_{ik}^T\mathbf{t}_{ik}\right) \tag{3.88}$$

$$= H\left(h_{ij}\mathbf{u}_i^T\mathbf{t}_{(i)} + \sum_{\substack{k=1\\k\neq i}}^{K}\left[h_{ij}\mathbf{v}_{ik}^T\mathbf{t}_{ik} + h_{kj}\mathbf{u}_k^T\mathbf{t}_{(k)}\right]\right) \tag{3.89}$$

Note that, for a given k, the vectors $\mathbf{t}_{ik}$ and $\mathbf{t}_{(k)}$ represent the same *dimensions* T_k, and $h_{ij}, h_{kj} \in T_k$ for all $k \neq i$, which implies that $h_{ij}T_k, h_{kj}T_k \in \tilde{T}_k$. In addition, for each k, we note that a large part of the two sets $h_{ij}T_k$ and $h_{kj}T_k$ are the same, i.e.,

$$\left|h_{ij}T_k \bigcap h_{kj}T_k\right| = m^{K^2-1}(m-1)^2 \triangleq M_\delta \tag{3.90}$$

Therefore, the first term in (3.87) can be further upper bounded as

$$
\begin{aligned}
&H\left(\sum_{k=1}^{K} h_{kj}X_k \Big| V_{-i}^K\right) \\
&= H\left(h_{ij}\mathbf{u}_i^T\mathbf{t}_{(i)} + \sum_{\substack{k=1\\k\neq i}}^{K}\left[h_{ij}\mathbf{v}_{ik}^T\mathbf{t}_{ik} + h_{kj}\mathbf{u}_k^T\mathbf{t}_{(k)}\right]\right) && (3.91)\\
&\leq \log\left[(2Q+1)^M(4Q+1)^{(K-1)M_\delta}(2Q+1)^{2(K-1)(M-M_\delta)}\right] && (3.92)\\
&\leq \log\left[Q^{M+(K-1)M_\delta+2(K-1)(M-M_\delta)}\right] + o(\log P) && (3.93)\\
&\leq \frac{\left[M+(K-1)M_\delta+2(K-1)(M-M_\delta)\right](1-\delta)}{(K-1)m^{K^2+1}+K(m+1)^{K^2+1}+\delta}\left(\frac{1}{2}\log P\right)\\
&\quad + o(\log P) && (3.94)\\
&\leq \frac{\left\{1+(K-1)\left(1-\frac{1}{m}\right)^2+2(K-1)\left[1-\left(1-\frac{1}{m}\right)^2\right]\right\}(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right)\\
&\quad + o(\log P) && (3.95)
\end{aligned}
$$

The second term in (3.87) is exactly the entropy of $\{\mathbf{u}_k\}_{k=1}^K$ vectors, i.e.,

$$
\begin{aligned}
H\left(\sum_{k=1}^{K} h_{kj}X_k|V_1^K\right) &= H\left(\sum_{k=1}^{K} h_{kj}\mathbf{u}_k^T\mathbf{t}_{(k)}\right) && (3.96)\\
&= \log(2Q+1)^{KM} && (3.97)\\
&= \frac{Km^{K^2+1}(1-\delta)}{(K-1)m^{K^2+1}+K(m+1)^{K^2+1}+\delta}\left(\frac{1}{2}\log P\right)\\
&\quad + o(\log P) && (3.98)\\
&= \frac{K(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P)\\
& && (3.99)
\end{aligned}
$$

Substituting (3.95) and (3.99) into (3.87), we get

$$
\begin{aligned}
&I(V_i;Y_j|V_{-i}^K) \\
&\quad\le H\left(\sum_{k=1}^{K} h_{kj}X_k\Big|V_{-i}^K\right) - H\left(\sum_{k=1}^{K} h_{kj}X_k\Big|V_1^K\right) && (3.100)\\
&\quad\le \frac{\left\{1+(K-1)\left(1-\frac{1}{m}\right)^2+2(K-1)\left[1-\left(1-\frac{1}{m}\right)^2\right]-K\right\}(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) \\
&\qquad + o(\log P) && (3.101)\\
&\quad\le \frac{K\,\frac{2m-1}{m^2}(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right)+o(\log P) && (3.102)
\end{aligned}
$$

We note that by choosing m large enough, the factor before the $\frac{1}{2}\log P$ term can be made arbitrarily small. Due to the non-perfect (i.e., only asymptotical) alignment, the upper bound for the information leakage rate is not a constant as in Section 2.7, (2.181), but a function which can be made to approach zero d.o.f.

For any $i \in \mathcal{K}$ and $j = 0$, i.e., $Y_0 = Z$ the external eavesdropper, we should derive a new upper bound for the second term in (3.87), i.e., $I(V_i; Z|V_{-i}^K)$. By similar steps, we have

$$
\begin{aligned}
I(V_i;Z|V_{-i}^K) &\le I\left(V_i;\sum_{k=1}^{K} g_kX_k\Big|V_{-i}^K\right) && (3.103)\\
&= H\left(\sum_{k=1}^{K} g_kX_k\Big|V_{-i}^K\right) - H\left(\sum_{k=1}^{K} g_kX_k\Big|V_1^K\right) && (3.104)\\
&= H\left(\sum_{k=1}^{K} g_kX_k\Big|V_{-i}^K\right) - H\left(\sum_{k=1}^{K} g_k\mathbf{u}_k^T\mathbf{t}_{(k)}\right) && (3.105)\\
&= H\left(\sum_{k=1}^{K} g_kX_k\Big|V_{-i}^K\right) - \log(2Q+1)^{KM} && (3.106)
\end{aligned}
$$

Here, we need to upper bound the first item in (3.106). We first observe that

$$H\left(\sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) = H\left(\sum_{k=1}^{K} g_k \mathbf{u}_k^T \mathbf{t}_{(k)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} g_i \mathbf{v}_{ik}^T \mathbf{t}_{ik}\right) \tag{3.107}$$

$$= H\left(g_i \mathbf{u}_i^T \mathbf{t}_{(i)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} \left[g_k \mathbf{u}_k^T \mathbf{t}_{(k)} + g_i \mathbf{v}_{ik}^T \mathbf{t}_{ik}\right]\right) \tag{3.108}$$

Firstly, note that, $\mathbf{t}_{(k)}$ and $\mathbf{t}_{ik}$ represent the same set T_k. Therefore, for different k, the *dimensions* are distinguishable. Secondly, due to reasons similar to (3.90), we conclude that

$$H\left(\sum_{k=1}^{K} g_k X_k \Big| V_{-i}^K\right) = H\left(g_i \mathbf{u}_i^T \mathbf{t}_{(i)} + \sum_{\substack{k=1 \\ k\neq i}}^{K} \left[g_k \mathbf{u}_k^T \mathbf{t}_{(k)} + g_i \mathbf{v}_{ik}^T \mathbf{t}_{ik}\right]\right) \tag{3.109}$$

$$\leq \log\left[(2Q+1)^M (4Q+1)^{(K-1)M_\delta} (2Q+1)^{2(K-1)(M-M_\delta)}\right] \tag{3.110}$$

$$\leq \log\left[Q^{M+(K-1)M_\delta+2(K-1)(M-M_\delta)}\right] + o(\log P) \tag{3.111}$$

$$\leq \frac{[M+(K-1)M_\delta+2(K-1)(M-M_\delta)]\,(1-\delta)}{(K-1)m^{K^2+1}+K(m+1)^{K^2+1}+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.112}$$

Substituting (3.112) into (3.106), we attain an upper bound which is the same as the upper bound for $I(V_i; Y_j|V_{-i}^K)$, i.e.,

$$I(V_i; Z|V_{-i}^K) \leq \frac{K\,\frac{2m-1}{m^2}(1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.113}$$

Substituting (3.85), (3.102), and (3.113) into (3.81), we obtain a lower bound for the achievable secrecy rate R_i as

$$R_i \geq \frac{\left[(K-1) - K\left(\frac{2m-1}{m^2}\right)\right](1-\delta)}{K-1+K\left(1+\frac{1}{m}\right)^{K^2+1}+\frac{\delta}{m^{K^2+1}}}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.114}$$

By choosing $m \to \infty$ and $\delta \to 0$, we can achieve secrecy sum rates arbitrarily close to $\frac{K-1}{2K-1}\left(\frac{1}{2}\log P\right)$, thereby achieving the sum s.d.o.f. lower bound in (3.67).

3.7 Conclusions

In this chapter, we studied secure communications in K-user Gaussian interference networks from an information-theoretic point of view, and addressed three important channel models: IC-EE, IC-CM and their combination IC-CM-EE in a unified framework. We showed that, for all three models, the sum s.d.o.f. is exactly $\frac{K(K-1)}{2K-1}$. Our achievability is based on structured signalling, structured cooperative jamming, channel prefixing and asymptotic real interference alignment. The key insight of the achievability is to carefully design the structure of all of the signals at the transmitters so that the signals are received at both legitimate receivers and eavesdroppers in the most desirable manner from a secure communication point of view. In particular, cooperative jamming signals protect information carrying signals via alignment, and the information carrying signals are further aligned to maximize s.d.o.f.

3.8 Appendix

3.8.1 Proof of Theorem 3.2

We first provide an outline of the proof. Our proof will combine and extend techniques from [5] and [25]. Our approach has three main components. First, as in [5], we condition the mutual information representing the secrecy leakage rate on the signals that carry the messages of other transmitter-receiver pairs. That is, for any given i, we condition the subtracted mutual information term in (3.81) on V_{-i}^K. This creates *enhanced* eavesdroppers. If we can guarantee secrecy against these enhanced eavesdroppers, we can guarantee secrecy against the original eavesdroppers. More specifically, for the leakage rate of message of transmitter i at receiver j, with $j \neq i$, we use

$$I(V_i; Y_j|V_{-i}^K) = I(V_i; Y_j, V_{-i}^K) \stackrel{\triangle}{=} I(V_i; \tilde{Y}_j) \tag{3.115}$$

where $\tilde{Y}_j \stackrel{\triangle}{=} (Y_j, V_{-i}^K)$ is the output of an *enhanced* eavesdropper with respect to message W_i. Second, as in [25], we consider the secrecy rate achievable against the *strongest* enhanced eavesdropper for each message. Therefore, as argued in [25, Appendex A], if we can guarantee a secrecy rate against the strongest eavesdropper, we can guarantee this secrecy rate against the original eavesdroppers. More specifically, let $Y^{(i)}$ be an element of the set $\{Y_1, \ldots, Y_k, Z\} \backslash \{Y_i\}$ such that

$$I(V_i; Y^{(i)}|V_{-i}^K) = \max_{j \in \mathcal{K}_{0,-i}} (V_i; Y_j|V_{-i}^K) \tag{3.116}$$

That is, $Y^{(i)}$ is the *strongest* eavesdropper with respect to transmitter i. The achievable rate in (3.81) considers the strongest eavesdropper for each message. Therefore, for each transmitter i, we construct a compound wiretap code as in [25]. Third, we prove secrecy for each message W_i, via the following equivocation inequality

$$\frac{1}{n}H(W_i|\mathbf{Y}^{(i)},\mathbf{V}_{-i}^K) \geq \frac{1}{n}H(W_i) - \epsilon^{(i)}, \qquad i=1,\ldots,K \tag{3.117}$$

for some arbitrarily small number $\epsilon^{(i)}$. Here, as in the main body of the chapter, we denote n-length sequences with boldface letters. The secrecy constraints in (3.117) fit the created equivalent view of the channel better. As we show next, secrecy constraints in (3.117) imply our original secrecy constraints in (3.4) and (3.5).

Towards this end, first note that, for each i,

$$\frac{1}{n}H(W_i|\mathbf{Y}_j,\mathbf{V}_{-i}^K) \geq \frac{1}{n}H(W_i|\mathbf{Y}^{(i)},\mathbf{V}_{-i}^K) \geq \frac{1}{n}H(W_i) - \epsilon^{(i)} \tag{3.118}$$

for all $j \in \mathcal{K}_{0,-i}$ since $Y^{(i)}$ is the *strongest* eavesdropper with respect to transmitter i and by using the enhanced eavesdropper argument in [25, Appendix A]. Then, the fact that (3.117) for all i implies the original secrecy constraints in (3.4) and (3.5)

follows from the following derivation:

$$
\begin{aligned}
H(W_{-j}^K|\mathbf{Y}_j) &\geq H(W_{-j}^K|\mathbf{Y}_j, W_j) && (3.119)\\
&\geq \sum_{i\neq j} H(W_i|\mathbf{Y}_j, W_{-i}^K) && (3.120)\\
&\geq \sum_{i\neq j} H(W_i|\mathbf{Y}_j, \mathbf{V}_{-i}^K, W_{-i}^K) && (3.121)\\
&= \sum_{i\neq j} H(W_i|\mathbf{Y}_j, \mathbf{V}_{-i}^K) && (3.122)\\
&\geq \sum_{i\neq j} H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) && (3.123)\\
&\geq \sum_{i\neq j} \left[H(W_i) - n\epsilon^{(i)}\right] && (3.124)\\
&= H(W_{-j}^K) - n\epsilon^{(-j)} && (3.125)
\end{aligned}
$$

where (3.122) is due to the Markov chain $W_{-i}^K \to (\mathbf{Y}_j, \mathbf{V}_{-i}^K) \to W_i$. Similarly,

$$
\begin{aligned}
H(W^K|\mathbf{Z}) &\geq \sum_i H(W_i|\mathbf{Z}, W_{-i}^K) && (3.126)\\
&\geq \sum_i H(W_i|\mathbf{Z}, \mathbf{V}_{-i}^K, W_{-i}^K) && (3.127)\\
&= \sum_i H(W_i|\mathbf{Z}, \mathbf{V}_{-i}^K) && (3.128)\\
&\geq \sum_i H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) && (3.129)\\
&\geq \sum_i \left[H(W_i) - n\epsilon^{(i)}\right] && (3.130)\\
&= H(W^K) - n\epsilon^{(Z)} && (3.131)
\end{aligned}
$$

where $\epsilon^{(Z)}$ is small for sufficiently large n.

We start by choosing the following rates for the secure and confusion messages of transmitter i:

$$R_i = I(V_i; Y_i) - I(V_i; Y^{(i)}|V_{-i}^K) - \epsilon \tag{3.132}$$

$$R_i^c = I(V_i; Y^{(i)}|V_{-i}^K) - \epsilon \tag{3.133}$$

Transmitter i generates $2^{n(R_i+R_i^c)}$ independent sequences each with probability

$$p(\mathbf{v}_i) = \prod_{t=1}^{n} p(v_{it}) \tag{3.134}$$

and constructs a codebook as

$$C_i \stackrel{\triangle}{=} \left\{ \mathbf{v}_i(w_i, w_i^c) \,:\, w_i \in \{1, \ldots, 2^{nR_i}\}, w_i^c \in \{1, \ldots, 2^{nR_i^c}\} \right\} \tag{3.135}$$

To transmit a message w_i, transmitter i chooses an element $\mathbf{v}_i$ from the sub-codebook $C_i(w_i)$

$$C_i(w_i) \stackrel{\triangle}{=} \left\{ \mathbf{v}_i(w_i, w_i^c) \,:\, w_i^c \in \{1, \ldots, 2^{nR_i^c}\} \right\} \tag{3.136}$$

and generates a channel input sequence based on

$$p(x_i|v_i) \tag{3.137}$$

Due to the code construction, we have $R_i + R_i^c < I(V_i; Y_i)$, for all i. Therefore,

for sufficiently large n_i, we can find a codebook such that the probability of error at the corresponding receiver i can be upper bounded by an arbitrarily small number, i.e., $\Pr(e_i)^{(n_i)} \leq \epsilon$. Then, let $n = \max_i n_i$, which gives $\max_i \Pr(e_i)^{(n)} \leq \epsilon$.

For the equivocation calculation, we consider the following conditional entropy as discussed before:

$$H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) = H(W_i, \mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) - H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) \tag{3.138}$$

$$= H(W_i, \mathbf{V}_i, \mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) - H(\mathbf{V}_i|W_i, \mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) - H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) \tag{3.139}$$

$$= H(W_i, \mathbf{V}_i|\mathbf{V}_{-i}^K) + H(\mathbf{Y}^{(i)}|W_i, \mathbf{V}_i, \mathbf{V}_{-i}^K) - H(\mathbf{V}_i|W_i, \mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) - H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) \tag{3.140}$$

$$= H(W_i, \mathbf{V}_i|\mathbf{V}_{-i}^K) - H(\mathbf{V}_i|W_i, \mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) + H(\mathbf{Y}^{(i)}|\mathbf{V}_i, \mathbf{V}_{-i}^K) - H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) \tag{3.141}$$

where the last equality is due to the Markov chain $W_i \to (\mathbf{V}_i, \mathbf{V}_{-i}^K) \to \mathbf{Y}^{(i)}$.

The first term in (3.141) is exactly the entropy of codebook C_i

$$H(\mathbf{V}_i) = n(R_i + R_i^c) \tag{3.142}$$

To bound the second term in (3.141), we have the following observation: Given the message $W_i = w_i$ and the received sequences $\mathbf{Y}^{(i)} = \mathbf{y}^{(i)}$ and genie-aided sequences $\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K$, receiver $Y^{(i)}$ can decode the codeword $\mathbf{v}_i(w_i, w_i^c)$ with arbitrarily small probability of error $\lambda(w_i)^{(n)}$ as n gets very large. More formally: by giving

$W_i = w_i, \mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K$, receiver $Y^{(i)}$ decodes $\mathbf{V}_i$ if there is a unique w_i^c such that

$$\left(\mathbf{v}_i(w_i, w_i^c), \mathbf{y}^{(i)}\right) \in T_\epsilon^{(n)}(P_{V_1, Y^{(i)}|V_{-i}^K}) \tag{3.143}$$

Otherwise, the receiver declares an error. Without loss of generality, we assume that $\mathbf{v}_i(w_i, w_1^c)$ is sent and denote the event $\left\{(\mathbf{v}_i(w_i, w_j^c), \mathbf{y}^{(i)}) \in T_\epsilon^{(n)}(P_{V_1, Y^{(i)}|V_{-i}^K})\right\}$ as E_j. Therefore, the probability of error $\lambda(w_i)^{(n)}$ can be bounded as

$$\lambda(w_i)^{(n)} \leq \Pr(E_1^c) + \sum_{j \neq 1} \Pr(E_j) \tag{3.144}$$

where the probability here is conditioned on the event that $\mathbf{v}_i(w_i, w_1^c)$ is sent. By joint typicality, we know that $\Pr(E_1^c) \leq \epsilon_1$ for sufficiently large n, and

$$\Pr(E_j) \leq 2^{nH(V_i, Y^{(i)}|V_{-i}^K) - nH(V_i) - nH(Y^{(i)}|V_{-i}^K) - n\epsilon_2} = 2^{-nI(V_I; Y^{(i)}|V_{-i}^K) - n\epsilon_2} \tag{3.145}$$

Hence,

$$\lambda(w_i)^{(n)} \leq \epsilon_1 + 2^{nR_i^c} 2^{-nI(V_I; Y^{(i)}|V_{-i}^K) - n\epsilon_2} \tag{3.146}$$

Note that $R_i^c = I(V_i; Y^{(i)}|V_{-i}^K) - \epsilon$. Therefore, we can conclude that $\lambda(w_i)^{(n)} \leq \epsilon_3$ for sufficiently large n, which by Fano's inequality further implies that

$$H(\mathbf{V}_i|W_i, \mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) = \sum_{W_i = w_i, \mathbf{Y}^{(i)} = \mathbf{y}^{(i)}, \mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K} H(\mathbf{V}_i|w_i, \mathbf{y}^{(i)}, \mathbf{v}_{-i}^K) \leq n\epsilon_4 \tag{3.147}$$

The third term in (3.141) can be lower bounded as follows:

$$H(\mathbf{Y}^{(i)}|\mathbf{V}_i,\mathbf{V}_{-i}^K)=\sum_{\mathbf{v}_i,\mathbf{v}_{-i}^K}\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)H(\mathbf{Y}^{(i)}|\mathbf{V}_i=\mathbf{v}_i,\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) \tag{3.148}$$

$$\geq \sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})}\Bigg[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) H(\mathbf{Y}^{(i)}|\mathbf{V}_i=\mathbf{v}_i,\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K)\Bigg] \tag{3.149}$$

$$\geq \sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})}\Bigg[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) \sum_{(a,b)\in\mathcal{V}_i\times\mathcal{V}_{-i}^K} N(a,b|\mathbf{v}_i,\mathbf{v}_{-i}^K)\sum_{y^{(i)}\in\mathcal{Y}^{(i)}} -p(y^{(i)}|a,b)\log p(y^{(i)}|a,b)\Bigg] \tag{3.150}$$

$$\geq \sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})}\Bigg[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) \sum_{(a,b)\in\mathcal{V}_i\times\mathcal{V}_{-i}^K} n\Big(\Pr(V_i=a,V_{-i}^K=b)-\epsilon_5\Big) \sum_{y^{(i)}\in\mathcal{Y}^{(i)}} -p(y^{(i)}|a,b)\log p(y^{(i)}|a,b)\Bigg] \tag{3.151}$$

$$\geq \sum_{(\mathbf{v}_i,\mathbf{v}_{-i}^K)\in T_\epsilon^{(n)}(P_{V_i,V_{-i}^K})} n\Big[\Pr(\mathbf{V}_i=\mathbf{v}_i)\Pr(\mathbf{V}_{-i}^K=\mathbf{v}_{-i}^K) \cdot H(Y^{(i)}|V_i,V_{-i}^K)-\epsilon_6\Big] \tag{3.152}$$

$$\geq (1-\epsilon_7)nH(Y^{(i)}|V_i,V_{-i}^K)-n\epsilon_8 \tag{3.153}$$

$$\geq nH(Y^{(i)}|V_i,V_{-i}^K)-n\epsilon_9 \tag{3.154}$$

To compute the forth term in (3.141), we define

$$\hat{\mathbf{Y}}^{(i)} = \begin{cases} \mathbf{Y}^{(i)}, & \text{if } (\mathbf{v}_{-i}^K, \mathbf{y}^{(i)}) \in T_\epsilon^{(n)}(P_{V_{-i}^K, Y^{(i)}}) \\ \text{arbitrary}, & \text{otherwise} \end{cases} \tag{3.155}$$

Then, we obtain

$$H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) = \sum_{\mathbf{v}_{-i}^K} \Pr(\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K) H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K) \tag{3.156}$$

$$\leq \sum_{\mathbf{v}_{-i}^K} \Pr(\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K) H(\mathbf{Y}^{(i)}, \hat{\mathbf{Y}}^{(i)}|\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K) \tag{3.157}$$

$$= \sum_{\mathbf{v}_{-i}^K} \Pr(\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K) \Big[H(\hat{\mathbf{Y}}^{(i)}|\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K) + H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K, \hat{\mathbf{Y}}^{(i)}) \Big] \tag{3.158}$$

$$\leq nH(Y^{(i)}|V_{-i}^K) + n\epsilon_{10} + \sum_{\mathbf{v}_{-i}^K} \Big[\Pr(\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K) H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K = \mathbf{v}_{-i}^K, \hat{\mathbf{Y}}^{(i)}) \Big] \tag{3.159}$$

Combining Fano's inequality and the fact that

$$\Pr(\mathbf{Y}^{(i)} \neq \hat{\mathbf{Y}}^{(i)}) \leq \Pr\Big\{ (\mathbf{V}_{-i}^K, \mathbf{Y}^{(i)}) \notin T_\epsilon^{(n)}(P_{V_{-i}^K, Y^{(i)}}) \Big\} \tag{3.160}$$

is arbitrarily small for sufficiently large n, (3.159) implies

$$H(\mathbf{Y}^{(i)}|\mathbf{V}_{-i}^K) \leq nH(Y^{(i)}|V_{-i}^K) + n\epsilon_{10} + n\epsilon_{11} \tag{3.161}$$

Substituting (3.142), (3.147), (3.154), and (3.161) into (3.141), we conclude

that

$$H(W_i|\mathbf{Y}^{(i)}, \mathbf{V}_{-i}^K) \geq H(W_i) - n\epsilon^{(i)} \tag{3.162}$$

where $\epsilon^{(i)}$ is small for sufficiently large n, which completes the proof.

Chapter 4

Secure Degrees of Freedom Region of Wireless Networks: The Polytope Structure

4.1 Introduction

In Chapters 2 and 3, we have studied the sum s.d.o.f. of multiple-transmitter multiple-receiver one-hop wireless networks. In this chapter, we study the *entire s.d.o.f. regions* of two important multi-user wireless network structures: The K-user Gaussian MAC wiretap channel and K-user IC with secrecy constraints. The converse for the MAC follows from a middle step in the converse of the sum s.d.o.f. in Chapter 2. The converse for the IC includes constraints both due to secrecy as well as due to interference. In order to prove the achievability, we use the polytope structure of the converse regions. In both MAC and IC cases, we develop explicit schemes that achieve the extreme points of the polytope regions given by the converse. Specifically, the extreme points of the MAC region are achieved by an m-user MAC wiretap channel with $K-m$ helpers. The extreme points of the IC region are achieved by a $(K-m)$-user IC with confidential messages, m helpers, and N external eavesdroppers, for $m \geq 1$ and a finite N.

4.2 System Model, Definitions and the Result

4.2.1 K-user Gaussian MAC Wiretap Channel

The K-user Gaussian MAC wiretap channel (see Figure 1.6) is:

$$Y_1 = \sum_{i=1}^{K} h_i X_i + N_1 \tag{4.1}$$

$$Y_2 = \sum_{i=1}^{K} g_i X_i + N_2 \tag{4.2}$$

where Y_1 is the channel output of the legitimate receiver, Y_2 is the channel output of the eavesdropper, X_i is the channel input of transmitter i, h_i and g_i are the channel gains of transmitter i to the legitimate receiver and the eavesdropper, respectively, and N_1 and N_2 are independent Gaussian random variables with zero-mean and unit-variance. All channel gains are independently drawn from continuous distributions, and are time-invariant throughout the communication session. We further assume that all h_i and g_i are non-zero. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_i^2\right] \leq P$, for $i = 1, \ldots, K$.

Each transmitter i has a message W_i intended for the legitimate receiver. For each i, message W_i is uniformly and independently chosen from set $\mathcal{W}_i$. The rate of message i is $R_i \stackrel{\triangle}{=} \frac{1}{n} \log |\mathcal{W}_i|$. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ where the n-length vector $\mathbf{X}_i \stackrel{\triangle}{=} X_i^n$ denotes the ith user's channel input in n channel uses. All messages are needed to be kept secret from the eavesdropper. A secrecy rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if for any $\epsilon > 0$ there exist n-length codes such that the legitimate receiver can decode the messages reliably, i.e., the

probability of decoding error is less than ϵ

$$\Pr\left[(W_1,\ldots,W_K)\neq(\hat{W}_1,\ldots,\hat{W}_K)\right]\leq\epsilon \tag{4.3}$$

and the messages are kept information-theoretically secure against the eavesdropper

$$\frac{1}{n}H(W_1,\ldots,W_K|\mathbf{Y}_2)\geq\frac{1}{n}H(W_1,\ldots,W_K)-\epsilon \tag{4.4}$$

where $\hat{W}_1,\ldots,\hat{W}_K$ are the estimates of the messages based on observation $\mathbf{Y}_1$, where $\mathbf{Y}_1\stackrel{\triangle}{=}Y_1^n$ and $\mathbf{Y}_2\stackrel{\triangle}{=}Y_2^n$.

The s.d.o.f. region is defined as:

$$D=\left\{\mathbf{d}:(R_1,\ldots,R_K)\text{ is achievable and }d_i\stackrel{\triangle}{=}\lim_{P\to\infty}\frac{R_i}{\frac{1}{2}\log P},\ i=1,\ldots,K\right\} \tag{4.5}$$

The sum s.d.o.f. is defined as:

$$D_{s,\Sigma}\stackrel{\triangle}{=}\lim_{P\to\infty}\sup\frac{\sum_{i=1}^{K}R_i}{\frac{1}{2}\log P} \tag{4.6}$$

where the supremum is over all achievable secrecy rate tuples $(R_1,\ldots,R_K)$. The sum s.d.o.f. of the K-user Gaussian MAC wiretap channel is characterized in Theorem 2.6 of Chapter 2 as $\frac{K(K-1)}{K(K-1)+1}$. In this chapter, we characterize the s.d.o.f. region of the K-user Gaussian MAC wiretap channel in the following theorem.

Theorem 4.1 *The s.d.o.f. region D of the K-user Gaussian MAC wiretap channel*

is the set of all $\mathbf{d}$ *satisfying*

$$Kd_i + (K-1)\sum_{j=1,j\neq i}^{K} d_j \leq K-1, \qquad i = 1,\ldots,K \tag{4.7}$$

$$d_i \geq 0, \qquad i = 1,\ldots,K \tag{4.8}$$

for almost all channel gains.

4.2.2 K-user Gaussian IC with Secrecy Constraints

The K-user Gaussian IC with secrecy constraints (see Figure 1.7) is:

$$Y_i = \sum_{j=1}^{K} h_{ji}X_j + N_i, \qquad i = 1,\ldots,K \tag{4.9}$$

$$Z = \sum_{j=1}^{K} g_j X_j + N_Z \tag{4.10}$$

where Y_i is the channel output of receiver i, Z is the channel output of the external eavesdropper (if there is any), X_i is the channel input of transmitter i, h_{ji} is the channel gain of the jth transmitter to the ith receiver, g_j is the channel gain of the jth transmitter to the eavesdropper (if there is any), and $\{N_1,\ldots,N_K,N_Z\}$ are mutually independent zero-mean unit-variance Gaussian random variables. All channel gains are independently drawn from continuous distributions, and are time-invariant throughout the communication session. We further assume that all h_{ji} are non-zero, and all g_j are non-zero if there is an external eavesdropper. All channel inputs satisfy average power constraints, $\mathrm{E}[X_i^2] \leq P$, for $i = 1,\ldots,K$.

Each transmitter i intends to send a message W_i, uniformly chosen from a set $\mathcal{W}_i$, to receiver i. The rate of message i is $R_i \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_i|$, where n is the number of channel uses. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to \mathbf{X}_i$ to encode the message, where $\mathbf{X}_i \stackrel{\triangle}{=} X_i^n$ is the n-length channel input of user i. The legitimate receiver j decodes the message as $\hat{W}_j$ based on its observation $\mathbf{Y}_j$. A secrecy rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if for any $\epsilon > 0$, there exist joint n-length codes such that each receiver j can decode the corresponding message reliably, i.e., the probability of decoding error is less than ϵ for all messages,

$$\max_j \Pr\left[W_j \neq \hat{W}_j\right] \leq \epsilon \tag{4.11}$$

and the corresponding secrecy requirement is satisfied. We consider three different secrecy requirements:

1) In IC-EE, Figure 1.8(a), all of the messages are kept information-theoretically secure against the external eavesdropper,

$$\frac{1}{n}H(W_1, \ldots, W_K|\mathbf{Z}) \geq \frac{1}{n}H(W_1, \ldots, W_K) - \epsilon \tag{4.12}$$

2) In IC-CM, Figure 1.8(b), all unintended messages are kept information-theoretically secure against each receiver,

$$\frac{1}{n}H(W_{-i}^K|\mathbf{Y}_i) \geq \frac{1}{n}H(W_{-i}^K) - \epsilon, \qquad i = 1, \ldots, K \tag{4.13}$$

where $W_{-i}^{K} \triangleq \{W_1, \ldots, W_{i-1}, W_{i+1}, \ldots, W_K\}$.

3) In IC-CM-EE, Figure 1.8(c), all of the messages are kept information-theoretically secure against both the $K-1$ unintended receivers and the eavesdropper, i.e., we impose both secrecy constraints in (4.12) and (4.13).

The s.d.o.f. region and the sum s.d.o.f. are defined as in (4.5) and (4.6). The sum s.d.o.f. of the K-user IC-EE, IC-CM, and IC-CM-EE is characterized in Theorem 3.1 of Chapter 3 as $\frac{K(K-1)}{2K-1}$. In this chapter, we characterize the s.d.o.f. region of the K-user IC-EE, IC-CM, and IC-CM-EE in the following theorem.

Theorem 4.2 *The s.d.o.f. region D of K-user IC-EE, IC-CM, and IC-CM-EE is the set of all* $\mathbf{d}$ *satisfying*

$$Kd_i + \sum_{j=1, j\neq i}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{4.14}$$

$$\sum_{i \in V} d_i \leq 1, \qquad \forall\ V \subseteq \{1, \ldots, K\},\ |V| = 2 \tag{4.15}$$

$$d_i \geq 0, \qquad i = 1, \ldots, K \tag{4.16}$$

for almost all channel gains.

4.3 Preliminaries

4.3.1 Polytope Structure and Extreme Points

Let $X \subseteq R^n$. The *convex hull* of X, $\mathrm{Co}(X)$, is the set of all convex combinations of the points in X:

$$\mathrm{Co}(X) \triangleq \left\{ \sum_i \lambda_i \mathbf{x}_i \mid \mathbf{x}_i \in X,\ \sum_i \lambda_i = 1,\ \lambda_i \in R,\ \text{and } \lambda_i \geq 0,\ \forall i \right\} \tag{4.17}$$

A set $P \subseteq R^n$ is a *polyhedron* if there is a system of finitely many inequalities $\mathbf{Hx} \leq \mathbf{h}$ such that

$$P = \left\{ \mathbf{x} \in R^n \mid \mathbf{Hx} \leq \mathbf{h} \right\} \tag{4.18}$$

A set $P \subseteq R^n$ is a *polytope* if there is a finite set $X \subseteq R^n$ such that $P = \mathrm{Co}(X)$. Then, we have the following theorem.

Theorem 4.3 ([57, Theorem 3.1.3]) *Let $P \subseteq R^n$. Then, P is a bounded polyhedron if only if P is a polytope.*

Therefore, if $P \subseteq R^n$ is a polytope, then it is a convex hull of some finite set X. By the properties of the convex hull of a finite set X, P is a bounded, closed, convex set. Since P is a subset of the Euclidean space, P is a compact convex set. An extreme point is formally defined as follows.

Definition 4.1 (Extreme point) *Let $P \subseteq R^n$. An $\mathbf{x} \in P$ is an extreme point if*

there are no $\mathbf{y}, \mathbf{z} \in P \setminus \{\mathbf{x}\}$ *such that* $\mathbf{x} = \lambda\mathbf{y} + (1-\lambda)\mathbf{z}$ *for any* $\lambda \in (0,1)$. *Then,* $Ex(P)$ *is the set of all extreme points of* P.

Theorem 4.4 (Minkowski, 1910. [57, Theorem 2.4.5]) *Let* $P \subseteq R^n$ *be a compact convex set. Then,*

$$P = Co(Ex(P)). \tag{4.19}$$

Minkowski theorem plays an important role in this chapter, since it tells that, instead of studying the polytope P itself, for certain problems, e.g., achievability proofs, we can simply concentrate on all extreme points $\mathrm{Ex}(P)$. Finally, the following theorem helps us find all extreme points of a polytope P efficiently: We select any n linearly independent active/tight boundaries and check whether they give a point in the polytope P.

Theorem 4.5 ([82, Theorem 7.2(b)]) $\mathbf{x} \in R^n$ *is an extreme point of polyhedron* $P(\mathbf{H}, \mathbf{h})$ *if and only if* $\mathbf{Hx} \leq \mathbf{h}$ *and* $\mathbf{H'x} = \mathbf{h'}$ *for some* $n \times (n+1)$ *sub-matrix* $(\mathbf{H'}, \mathbf{h'})$ *of* $(\mathbf{H}, \mathbf{h})$ *with rank*$(\mathbf{H'}) = n$.

4.4 S.d.o.f. Region of K-User MAC Wiretap Channel

In this section, we study the K-user MAC wiretap channel defined in Section 4.2.1 and prove the s.d.o.f. region stated in Theorem 4.1. We first illustrate the regions for $K = 2$ and $K = 3$ cases as examples. We then provide the converse in Section 4.4.1, investigate the s.d.o.f. region in terms of its extreme points in Section 4.4.2, and show the achievability of each extreme point in Section 4.4.3.

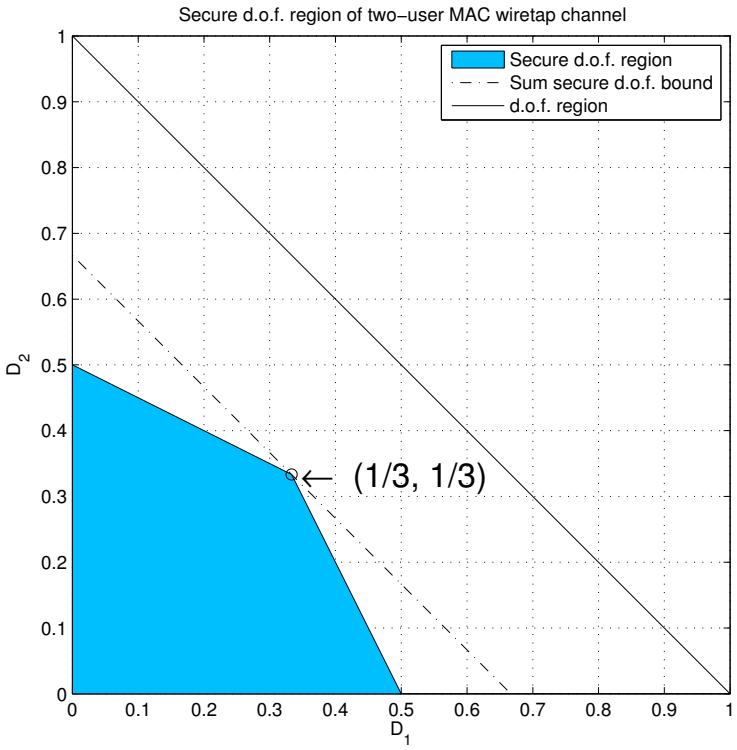


Figure 4.1: The s.d.o.f. region of the $K = 2$-user MAC wiretap channel.

For $K = 2$, the s.d.o.f. region in Theorem 4.1 becomes

$$D = \Big\{ \mathbf{d} : \; 2d_1 + d_2 \leq 1, \\ d_1 + 2d_2 \leq 1, \\ d_1, d_2 \geq 0 \Big\} \tag{4.20}$$

and is shown in Figure 4.1. The extreme points of this region are: $(0,0), (\frac{1}{2},0), (0,\frac{1}{2})$, and $(\frac{1}{3},\frac{1}{3})$. In order to provide the achievability of the region, it suffices to provide the achievability of these extreme points. In fact, the achievabilities of $(\frac{1}{2},0), (0,\frac{1}{2})$ were proved in Chapter 2, Section 2.4 in the helper setting and the achievability of $(\frac{1}{3},\frac{1}{3})$ was proved in Chapter 2, Section 2.9. Note that $(\frac{1}{3},\frac{1}{3})$ is the only sum

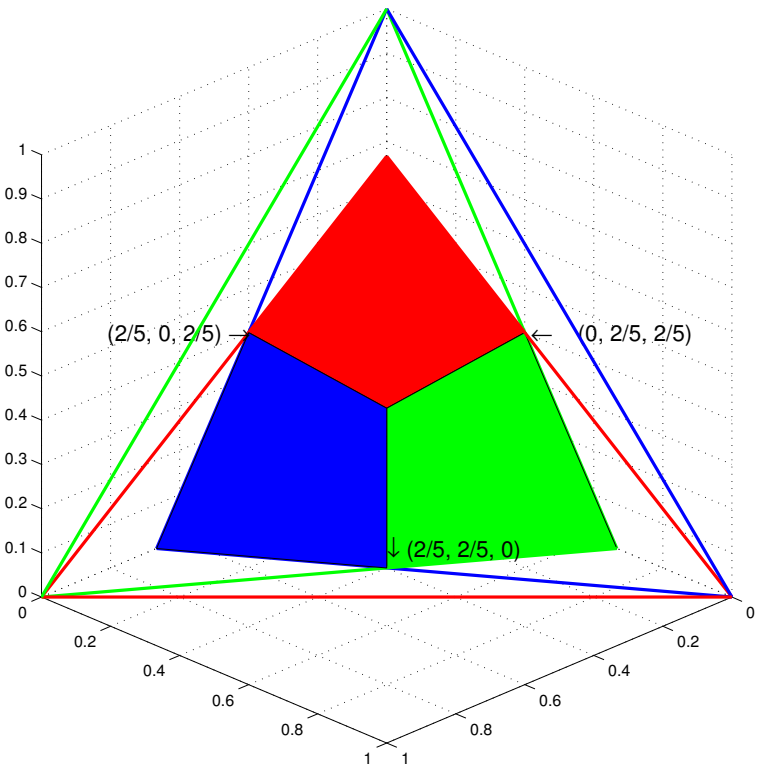


Figure 4.2: The s.d.o.f. region of the $K = 3$-user MAC wiretap channel.

s.d.o.f. optimum point.

For $K = 3$, the s.d.o.f. region in Theorem 4.1 becomes

$$D = \Big\{ \mathbf{d} : \; 3d_1 + 2d_2 + 2d_3 \leq 2, \\ 2d_1 + 3d_2 + 2d_3 \leq 2, \\ 2d_1 + 2d_2 + 3d_3 \leq 2, \\ d_1, d_2, d_3 \geq 0 \Big\} \tag{4.21}$$

and is shown in Figure 4.2. The extreme points of this region are:

$$(0,0,0)$$

$$(2/3,0,0),(0,2/3,0),(0,0,2/3)$$

$$(2/5,2/5,0),(2/5,0,2/5),(0,2/5,2/5)$$

$$(2/7,2/7,2/7)$$

which correspond to the maximum individual s.d.o.f. (see Gaussian wiretap channel with two helpers in Chapter 2, Section 2.5), the maximum sum of pair of s.d.o.f. (see two-user Gaussian MAC wiretap channel with one helper, proved in Section 4.4.3), and the maximum sum s.d.o.f. (see three-user Gaussian MAC wiretap channel in Chapter 2, Section 2.9). Note that $(\frac{2}{7},\frac{2}{7},\frac{2}{7})$ is the only sum s.d.o.f. optimum point.

4.4.1 Converse

The converse simply follows from a key inequality in the proof in Chapter 2, Section 2.9. We re-examine (2.232) in Chapter 2:

$$nR_i + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)h(\mathbf{Y}_1) + nc_i, \qquad i = 1,\ldots,K \tag{4.22}$$

where all $\{c_i\}$ in this chapter are constants independent of P.

Clearly, (4.22) is not symmetric. However, the lower bound derived in Section 2.9 was achieved by a symmetric scheme. Therefore, in Section 2.9, in order to

obtain a matching upper bound, we summed up (4.22) for all i to obtain:

$$[K(K-1)+1]\sum_{j=1}^{K} nR_j \leq K(K-1)h(\mathbf{Y}_1) + nc' \tag{4.23}$$

$$\leq K(K-1)\frac{n}{2}\log P + nc'' \tag{4.24}$$

which provided the desired upper bound for the sum s.d.o.f.

$$D_{s,\Sigma} \leq \frac{K(K-1)}{K(K-1)+1} \tag{4.25}$$

which is the converse for Theorem 2.6.

In fact, (4.22) provides more information than what is needed for the sum s.d.o.f. only. In this chapter, we start from (4.22)

$$nR_i + (K-1)\sum_{j=1}^{K} nR_j \leq (K-1)\left(\frac{n}{2}\log P\right) + nc_i, \qquad i = 1, \ldots, K \tag{4.26}$$

divide by $\frac{n}{2}\log P$ and take the limit $P \to \infty$ on both sides to obtain,

$$d_i + (K-1)\sum_{j=1}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{4.27}$$

that is,

$$Kd_i + (K-1)\sum_{j=1, j\neq i}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{4.28}$$

which concludes the converse proof of Theorem 4.1.

4.4.2 Polytope Structure and Extreme Points

To prove that the region D in Theorem 4.1 is tight (i.e., achievable), we first express it in terms of its *extreme points*, explicitly characterize all of its extreme points, and develop a scheme to achieve each of its extreme points.

The region in Theorem 4.1 is a polytope, which is a convex hull of some finite set X, as discussed in Section 4.3.1. By the properties of the convex hull of a finite set X, D is a bounded, closed, convex set. Since $D \subset R^K$, D is a compact convex set. From Minkowski theorem, the polytope D in Theorem 4.1 is a convex hull of its extreme points. Then, in order to prove that D is tight, it suffices to prove that each extreme point of D is achievable. Then, from convexification through time-sharing, all points in D are achievable.

In order to speak of the polytope, we re-write the constraints in (4.7) and (4.8) as

$$Kd_i + (K-1)\sum_{j=1, j\neq i}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{4.29}$$

$$-d_i \leq 0 \qquad i = 1, \ldots, K \tag{4.30}$$

Then, we write all the left hand sides of (4.29) and (4.30) as an $N \times K$ matrix $\mathbf{H}$ with corresponding right hand sides forming an N-length column vector $\mathbf{h}$, i.e., all points $\mathbf{d}$ in D satisfy

$$\mathbf{Hd} \leq \mathbf{h} \tag{4.31}$$

where $N \stackrel{\triangle}{=} 2K$. By Theorem 4.5, exploring all extreme points of D is equivalent to

finding all sub-matrices $(\mathbf{H}_J, \mathbf{h}_J)$ of $(\mathbf{H}, \mathbf{h})$, such that

$$\text{rank}(\mathbf{H}_J) = K \tag{4.32}$$

and

$$\mathbf{H}_J\mathbf{d} = \mathbf{h}_J, \quad \text{and} \quad \mathbf{H}\mathbf{d} \leq \mathbf{h} \tag{4.33}$$

where $\mathbf{H}_J$ is a sub-matrix of $\mathbf{H}$ with rows indexed by the index set J, and $\mathbf{h}_J$ is the sub-vector of $\mathbf{h}$ with rows indexed by J.

Let $\mathbf{d} \in D$ be a non-zero extreme point of D. Define a subset $S \subseteq \{1, \ldots, N\}$ as

$$S \stackrel{\triangle}{=} \left\{ s_i \stackrel{\triangle}{=} s(i) : \mathbf{H}_{s_i}\mathbf{d} = \mathbf{h}_{s_i} \text{ is } Kd_i + (K-1)\sum_{j=1, j\neq i}^{K} d_j = K-1, \quad i = 1, \ldots, K \right\} \tag{4.34}$$

where $s(i)$ is a function of the coordinate i with the value as the row index of $\mathbf{H}$ corresponding to the active boundaries in (4.29). Similarly, define the set $Z \subseteq \{1, \ldots, N\}$ as

$$Z \stackrel{\triangle}{=} \left\{ z_i \stackrel{\triangle}{=} z(i) : \mathbf{H}_{z_i}\mathbf{d} = \mathbf{h}_{z_i} \text{ is } d_i = 0, \quad i = 1, \ldots, K \right\} \tag{4.35}$$

where $z(i)$ is a function of the coordinate i with the value as the row index of $\mathbf{H}$

corresponding to the active boundaries in (4.30). Clearly, S and Z are disjoint, i.e.,

$$S \cap Z = \phi \tag{4.36}$$

For any row index set J, which corresponds to a set of active boundaries for $\mathbf{d}$, we have

$$J = S \cup Z \tag{4.37}$$

For example, for the three-user case, $K = 3$, according to (4.29) and (4.30), we have $\mathbf{H}$ and $\mathbf{h}$ as

$$\mathbf{H} = \begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \qquad \mathbf{h} = \begin{bmatrix} 2 \\ 2 \\ 2 \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{4.38}$$

If the equalities with $i = 1, 2$ hold in (4.29) and the equality with $i = 3$ holds in (4.30), then the corresponding sets S, Z, J are

$$S = \{s_1, s_2\} = \{1, 2\}, \quad Z = \{z_3\} = \{6\}, \quad J = S \cup Z = \{1, 2, 6\} \tag{4.39}$$

with the row-index functions

$$s_i = s(i) = i \tag{4.40}$$

$$z_i = z(i) = i + 3 \tag{4.41}$$

In this example, it is easy to check that

$$\text{rank}(\mathbf{H}_J) = \text{rank}\left(\left[\begin{array}{ccc} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 0 & 0 & -1 \end{array}\right]\right) = 3 = K \tag{4.42}$$

and the solution given by $\mathbf{H}_J\mathbf{d} = \mathbf{h}_J$ is

$$\mathbf{d} = \left(\frac{2}{5}, \frac{2}{5}, 0\right) \tag{4.43}$$

which satisfies (4.33). Therefore, this is an extreme point.

For the general case, we have the following theorem.

Theorem 4.6 *A point $\mathbf{d} \in D$ of Theorem 4.1 is an extreme point if and only if it is equal to, up to element reordering,*

$$\Big(\underbrace{\Delta, \ldots, \Delta}_{m \text{ items}}, \underbrace{0, \ldots, 0}_{(K-m) \text{ items}}\Big), \qquad 0 \leq m \leq K \tag{4.44}$$

where

$$\Delta = \frac{K-1}{m(K-1)+1} \tag{4.45}$$

Proof: First, for any m, $0 \leq m \leq K$, let the point $\mathbf{d}$ be as in (4.44). It is easy to check that the sub-matrix $(\mathbf{H}_J, \mathbf{h}_J)$, where

$$J = \Big\{ s_i : 1 \leq i \leq m \Big\} \cup \Big\{ z_j : m+1 \leq j \leq K \Big\} \tag{4.46}$$

satisfies all the conditions in Theorem 4.5, which means that $\mathbf{d}$ is an extreme point.

In order to show the other direction, we need to show that any extreme point $\mathbf{d}$ has the structure in (4.44) for some m, $0 \leq m \leq K$. To this end, we find the sub-matrix in Theorem 4.5.

If $|Z| = K$, due to (4.30), the sub-matrix $\mathbf{H}_Z$ is simply a diagnoal matrix with -1s on the diagonal, and consequently, $\text{rank}(\mathbf{H}_Z) = K$. Then, the solution of $\mathbf{H}_Z\mathbf{d} = \mathbf{h}_Z$ is $\mathbf{0}$, which satisfies (4.33). This extreme point corresponds to the case $m = 0$ in Theorem 4.6.

In the rest of the proof, we focus on non-zero extreme points, i.e., $|Z| < K$. Due to (4.29), it is easy to verify that $\mathbf{H}_S$ has $|S|$ rows with $\text{rank}(\mathbf{H}_S) = |S|$ where S is defined in (4.34). In order to make $\text{rank}(\mathbf{H}_J) = \text{rank}(\mathbf{H}_{S\cup Z}) = K$, we need at least $K - |S|$ more rows from $\mathbf{H}$, i.e., $|Z| \geq K - |S|$. If S is empty, then $|Z| \geq K$, which contradicts the assumption $|Z| < K$. Therefore, S is non-empty, i.e., $|S| \geq 1$.

First, we claim that

$$d_i = d_k, \quad \forall s_i, s_k \in S \tag{4.47}$$

If $|S| = 1$, there is nothing to prove, and we are done with the proof of (4.47). If

$|S| > 1$, consider any $s_i, s_k \in S$, $i \neq k$. By the definition of S, we have

$$(K-1)d_k + Kd_i + (K-1)\sum_{l \neq i,k} d_l = K-1 \tag{4.48}$$

$$(K-1)d_i + Kd_k + (K-1)\sum_{l \neq i,k} d_l = K-1 \tag{4.49}$$

which implies that $d_i = d_k$ for any $s_i, s_k \in S$, providing (4.47) for $|S| \geq 1$.

Next, we claim

$$d_i > 0, \quad \forall s_i \in S \tag{4.50}$$

If $|S| = K$, due to (4.47), (4.50) is trivially true since we are focusing on a non-zero extreme point. If $|S| < K$, then we observe that

$$d_i \geq d_j, \qquad \forall s_i \in S, s_j \notin S \tag{4.51}$$

which indicates that for any $s_i \in S$ the corresponding element in vector $\mathbf{d}$ is the largest one, i.e., $d_i = \max_k d_k$, which implies (4.50). Hence, it now suffices to show (4.51). We prove it by contradiction. Assume that there exists a coordinate j such that $s_j \notin S$ and d_j is strictly larger than d_i for any $s_i \in S$. By the definition of S in

(4.34), we have

$$K-1 = Kd_i + (K-1)d_j + (K-1)\sum_{l=1,l\neq i,j}^{K} d_l \tag{4.52}$$

$$< Kd_i + (K-1)d_j + (K-1)\sum_{l=1,l\neq i,j}^{K} d_l + (d_j - d_i) \tag{4.53}$$

$$= Kd_j + (K-1)d_i + (K-1)\sum_{l=1,l\neq i,j}^{K} d_l \tag{4.54}$$

which contradicts the constraint (4.29). Therefore, we must have (4.51) and consequently (4.50).

Finally, denote $m \stackrel{\triangle}{=} |S|$, and, without loss of generality, assume that $S = \{s_i : 1 \leq i \leq m\}$. By (4.50) and the definition of Z in (4.35), we note that $z_j \in Z$ only if $s_j \notin S$. Together with the constraint $|Z| \geq K - |S| = K - m$, we conclude that we must have $Z = \{z_j : m+1 \leq j \leq K\}$, i.e., $d_j = 0$ for $m+1 \leq j \leq K$. Thus, $\text{rank}(\mathbf{H}_{S\cup Z}) = K$, and, by (4.47), the solution given by the corresponding equations can be characterized as (4.44), which satisfies (4.33), completing the proof. □

4.4.3 Achievability

The previous section showed that the converse region is a polytope with extreme points which have m coordinates all equal to Δ given in (4.45), and the remaining $K-m$ coordinates all equal to zero. It is clear that zero vector is an extreme point in D and is trivially achievable. The rest of the achievability proof focuses on non-zero extreme points. In this section, we prove that each of these extreme points is

achievable. Without loss of generality, we prove that the s.d.o.f. point of

$$\mathbf{d} = \Big(\underbrace{\Delta, \ldots, \Delta}_{m \text{ items}}, \underbrace{0, \ldots, 0}_{(K-m) \text{ items}} \Big) \tag{4.55}$$

is achievable for all $1 < m < K$ with Δ in (4.45). By symmetry, this proves the achievability of all extreme points. Note that $m = K$ is shown in Chapter 2, Section 2.9, and $m = 1$ is shown in Chapter 2, Section 2.5.

Theorem 4.7 *The extreme point* $\mathbf{d} \in D$ *given in (4.55) is achieved by* m*-user Gaussian MAC wiretap channel with* $K - m$ *helpers for almost all channel gains.*

Proof: Consider the m-user Gaussian MAC wiretap channel with $K - m$ helpers where transmitter i, $i = 1, \ldots, m$, has confidential message W_i intended for the legitimate receiver and the remaining $K - m$ transmitters serve as independent helpers without messages of their own.

In order to achieve the extreme point $\mathbf{d}$ in (4.55), transmitter i, $i = 1, \ldots, m$, divides its message into $K-1$ mutually independent sub-messages. Each transmitter sends a linear combination of signals that carry the sub-messages. In addition to message carrying signals, all transmitters also send cooperative jamming signals U_i, $i = 1, \ldots, K$, respectively. The messages are sent in such a way that all of the cooperative jamming signals are aligned in a single dimension at the legitimate receiver, occupying the smallest possible space at the legitimate receiver, and hence allowing for the reliable decodability of the message carrying signals. In addition, each cooperative jamming signal is aligned with at most $K - 1$ message carrying

signals at the eavesdropper to limit the information leakage rate to the eavesdropper. An example of $K = 3$, $m = 2$, and $K - m = 1$ is given in Figure 4.3.

More specifically, we use a total of $m(K-1)+K$ mutually independent random variables

$$V_{ij}, \quad i \in \{1, \ldots, m\},\ j \in \{1, \cdots, K\} \setminus \{i\} \tag{4.56}$$

$$U_k, \quad k \in \{1, \cdots, K\} \tag{4.57}$$

where $\{V_{ij}\}_{j \neq i}$ denote the message carrying signals and U_i denotes the cooperative jamming signal sent from transmitter i. In particular, V_{ij} carries the jth sub-message of transmitter i. Each of these random variables is uniformly and independently drawn from the same discrete constellation $C(a, Q)$ given in (2.73), where a and Q will be specified later. We choose the input signals of the transmitters as

$$X_i = \sum_{j=1, j \neq i}^{K} \frac{g_j}{h_j g_i} V_{ij} + \frac{1}{h_i} U_i, \qquad i \in \{1, \ldots, m\} \tag{4.58}$$

$$X_j = \frac{1}{h_j} U_j, \qquad j \in \{m+1, \ldots, K\} \tag{4.59}$$

With these input selections, observations of the receivers are

$$Y_1 = \left[\sum_{i=1}^{m} \sum_{j=1, j \neq i}^{K} \left(\frac{g_j h_i}{h_j g_i} V_{ij} \right) \right] + \left(\sum_{k=1}^{K} U_k \right) + N_1 \tag{4.60}$$

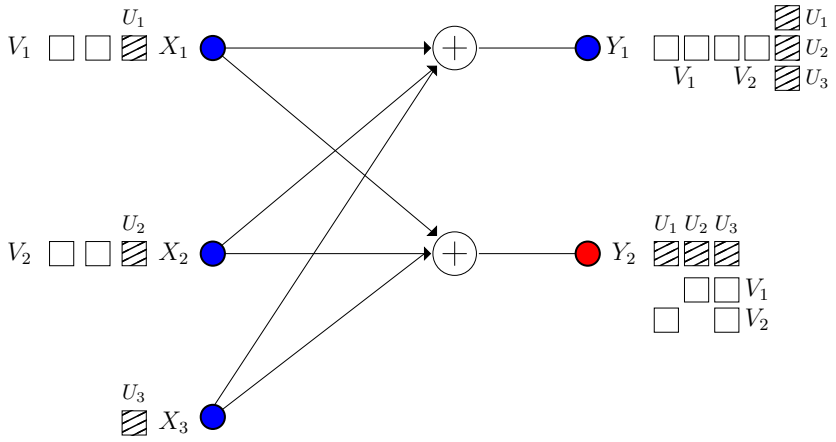


Figure 4.3: Illustration of secure interference alignment for the s.d.o.f. triple $(2/5, 2/5, 0)$ for the two-user MAC wiretap channel with one helper; $K = 3$ and $m = 2$. Here, we define $V_i \triangleq \{V_{ij} : j = 1, 2, 3, j \neq i\}$ for $i = 1, 2$.

and

$$Y_2 = \sum_{j=1}^{K} \frac{g_j}{h_j} \left(U_j + \sum_{i=1, i\neq j}^{m} V_{ij} \right) + N_2 \tag{4.61}$$

where the terms inside the parentheses in (4.60) and (4.61) are *aligned*.

By [34, Theorem 1], we can achieve the following sum secrecy rate for the m users

$$\sup \sum_{i=1}^{m} R_i \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{4.62}$$

where $\mathbf{V} \triangleq \{V_{ij} : i \in \{1, \ldots, m\},\ j \in \{1, \cdots, K\} \setminus \{i\}\}$.

By Lemma 2.3 in Chapter 2, for any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(m(K-1)+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P to meet the average power constraint, then

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\beta P^{\delta}\right) \tag{4.63}$$

for some constant $\beta > 0$ (independent of P), where $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y_1. This means that we can have $\Pr[\mathbf{V} \neq \hat{\mathbf{V}}] \to 0$ as $P \to \infty$.

By Fano's inequality and the Markov chain $\mathbf{V} \to Y_1 \to \hat{\mathbf{V}}$, we know that

$$H(\mathbf{V}|Y_1) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{4.64}$$

$$\leq 1 + \exp\left(-\beta P^{\delta}\right) \log(2Q+1)^{m(K-1)} \tag{4.65}$$

$$= o(\log P) \tag{4.66}$$

where $o(\cdot)$ is the little-o function. This means that

$$I(\mathbf{V}; Y_1) = H(\mathbf{V}) - H(\mathbf{V}|Y_1) \tag{4.67}$$

$$= \log(2Q+1)^{m(K-1)} - H(\mathbf{V}|Y_1) \tag{4.68}$$

$$\geq \log(2Q+1)^{m(K-1)} - o(\log P) \tag{4.69}$$

On the other hand, we can bound the second term in (4.62) as

$$I(\mathbf{V}; Y_2) \leq I\left(\mathbf{V}; Y_2 - N_2\right) \tag{4.70}$$

$$= \sum_{j=1}^{K} H\left(U_j + \sum_{i=1, i\neq j}^{m} V_{ij}\right) - H\left(U_1, \ldots, U_K\right) \tag{4.71}$$

$$\leq K \log \frac{2KQ+1}{2Q+1} \tag{4.72}$$

$$\leq K \log K \tag{4.73}$$

$$= o(\log P) \tag{4.74}$$

where (4.72) is due to the fact that entropy of each $U_j + \sum_{i=1,i\neq j}^{m} V_{ij}$ is maximized by the uniform distribution which takes values over a set of cardinality $2KQ+1$.

Combining (4.69) and (4.74), we obtain

$$\sup \sum_{i=1}^{m} R_i \geq I(\mathbf{V};Y_1) - I(\mathbf{V};Y_2) \tag{4.75}$$

$$\geq \log(2Q+1)^{m(K-1)} - o(\log P) \tag{4.76}$$

$$= \frac{m(K-1)(1-\delta)}{m(K-1)+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.77}$$

By choosing δ arbitrarily small, we can achieve the sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$ for almost all channel gains, which implies that the s.d.o.f. tuple of

$$\left(\underbrace{\frac{(K-1)}{m(K-1)+1},\ldots,\frac{(K-1)}{m(K-1)+1}}_{m \text{ item(s)}},\ \underbrace{0,\ldots,0}_{K-m \text{ item(s)}}\right) \tag{4.78}$$

is achievable by symmetry, which is (4.55). □

4.5 S.d.o.f. Region of K-User IC with Secrecy Constraints

In this section, we study the K-user IC with secrecy constraints defined in Section 4.2.2 and prove the s.d.o.f. region stated in Theorem 4.2. To this end, we consider both IC-CM and IC-EE and their combination IC-CM-EE in a unified framework. We first illustrate the regions for $K = 2, 3, 4$ cases as examples. The purpose of presenting $K = 4$ as an example is to show that, unlike the MAC case, starting with $K = 4$ interference constraints become effective and binding. We then provide

converses separately for IC-EE and IC-CM in Section 4.5.1 and Section 4.5.2, respectively, which imply a converse for IC-CM-EE. Finally, we show the achievability for IC-CM-EE, which implies the achievability for IC-EE and IC-CM. Specifically, we investigate the s.d.o.f. region in terms of its extreme points in Section 4.5.3 and show the general achievability in Section 4.5.4.

For $K = 2$, the s.d.o.f. region in Theorem 4.2 becomes

$$D = \Big\{ \mathbf{d} : \; 2d_1 + d_2 \leq 1, \\ d_1 + 2d_2 \leq 1, \\ d_1, d_2 \geq 0 \Big\} \tag{4.79}$$

which is as same as (4.20), and is shown in Figure 4.1. Note that (4.15) is not necessary for the two-user case, since summing the bounds $2d_1+d_2 \leq 1$ and $d_1+2d_2 \leq 1$ up gives a new bound

$$d_1 + d_2 \leq \frac{2}{3} \tag{4.80}$$

which is the result in Theorem 3.1 and makes the constraint in (4.15) strictly loose.

In order to provide the achievability, it suffices to check that the extreme points $(0,0)$, $(\frac{1}{2},0), (0,\frac{1}{2})$, and $(\frac{1}{3},\frac{1}{3})$ are achievable. In fact, the achievabilities of $(\frac{1}{2},0), (0,\frac{1}{2})$ are similar to Chapter 2, Section 2.4 and will be shown in Section 4.5.3. The achievability of $(\frac{1}{3},\frac{1}{3})$ was proved in Chapter 3. Note that $(\frac{1}{3},\frac{1}{3})$ is the only sum s.d.o.f. optimum point.

For $K = 3$, the s.d.o.f. region in Theorem 4.2 becomes

$$D = \Big\{ \mathbf{d} : \; 3d_1 + d_2 + d_3 \leq 2, \\ d_1 + 3d_2 + d_3 \leq 2, \\ d_1 + d_2 + 3d_3 \leq 2, \\ d_1, d_2, d_3 \geq 0 \Big\} \tag{4.81}$$

and (4.15) is not necessary for the three-user case, either. This is because, due to the positiveness of each element in $\mathbf{d}$, from the first two inequalities in (4.81), we have

$$3d_1 + d_2 \leq 3d_1 + d_2 + d_3 \leq 2 \tag{4.82}$$

$$d_1 + 3d_2 \leq d_1 + 3d_2 + d_3 \leq 2 \tag{4.83}$$

Summing the left hand sides up of (4.82) and (4.83) gives us

$$d_1 + d_2 \leq 1 \tag{4.84}$$

which is (4.15) with $V = \{1, 2\}$, and we have (4.15) for free from (4.81).

The extreme points of this region are:

$$(0,0,0)$$

$$(2/3,0,0),(0,2/3,0),(0,0,2/3)$$

$$(1/2,1/2,0),(1/2,0,1/2),(0,1/2,1/2)$$

$$(2/5,2/5,2/5)$$

which correspond to the maximum individual s.d.o.f. (see Gaussian wiretap channel with two helpers in Chapter 2, Section 2.5 and Section 4.5.3), the maximum sum of pair of s.d.o.f. (proved in Section 4.5.3), and the maximum sum s.d.o.f. (see three-user Gaussian IC-CM-EE in Chapter 3). Note that, $(\frac{1}{2},\frac{1}{2})$ is the maximum sum d.o.f. for a two-user IC *without* secrecy constraints, and $(\frac{2}{5},\frac{2}{5},\frac{2}{5})$ is the only sum s.d.o.f. optimum point.

For $K = 4$, the s.d.o.f. region in Theorem 4.2 becomes

$$\begin{aligned} D = \Big\{ \mathbf{d} : \; & 4d_1 + d_2 + d_3 + d_4 \leq 3, \\ & d_1 + 4d_2 + d_3 + d_4 \leq 3, \\ & d_1 + d_2 + 4d_3 + d_4 \leq 3, \\ & d_1 + d_2 + d_3 + 4d_4 \leq 3, \\ & d_1 + d_2 \leq 1, \\ & d_1 + d_3 \leq 1, \\ & d_1 + d_4 \leq 1, \\ & d_2 + d_3 \leq 1, \\ & d_2 + d_4 \leq 1, \\ & d_3 + d_4 \leq 1, \\ & d_1, d_2, d_3, d_4 \geq 0 \Big\} \end{aligned} \tag{4.85}$$

The extreme points of this region are:

$(0, 0, 0)$

$(3/4, 0, 0, 0), (0, 3/4, 0, 0), (0, 0, 3/4, 0), (0, 0, 0, 3/4)$

$(2/3, 1/3, 0, 0)$ up to element reordering

$(1/2, 1/2, 1/2, 0), (1/2, 1/2, 0, 1/2), (1/2, 0, 1/2, 1/2), (0, 1/2, 1/2, 1/2)$

$(3/7, 3/7, 3/7, 3/7)$

Here, in contrast to the two-user and three-user cases, (4.15) is absolutely necessary. For example, the point $(\frac{3}{5}, \frac{3}{5}, 0, 0)$ satisfies (4.14), but not (4.15). In fact, it cannot be achieved, and (4.15) is strictly needed to enforce that fact.

Regarding the region in Theorem 4.2, as illustrated in the examples above, we provide a few general comments here:

1) Although (4.15) only states the constraints for all pairs of rates, due to the same argument in [55], it can equivalently be stated as $\sum_{i\in V} d_i \leq \frac{|V|}{2}$ for all $|V| \geq 2$. We note that, when $|V| = K$, the corresponding upper bound is strictly loose due to Theorem 3.1 in Chapter 3, and that is why such bounds were not needed in Chapter 3, where sum s.d.o.f. was characterized.

2) As shown in the examples, when $K = 2$ or 3, (4.15) is not necessary. When $K \geq 4$, we need both (4.14) and (4.15) to completely characterize the region D. Neither of them can be removed from the theorem. For example, the all $\frac{1}{2}$ vector, $(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$, satisfies (4.15), but not (4.14). On the other hand, the point $(\frac{K-1}{K+1}, \frac{K-1}{K+1}, 0, 0, \ldots, 0)$, which has only two non-zero elements, satisfies (4.14), but not (4.15) for any $K \geq 4$. Therefore, (4.15) emerges only when $K \geq 4$. To the best of our knowledge, this is the first time that $K = 2$ or $K = 3$ do not represent the most generality of a multi-user problem, and we need to go up to $K = 4$ for this phenomenon to appear.

3) Different portions of the region D are governed by different upper bounds. To see this, we can study the structure of the extreme points of D, since D is the convex hull of them. The sum s.d.o.f. tuple, which is symmetric and has no zero

elements, is governed by the upper bounds in (4.14) due to secrecy constraints. However, as will be shown in Theorem 4.8 in Section 4.5.3, all other extreme points have zeros as some elements, and therefore are governed by the upper bounds in (4.15) due to interference constraints in [54, 55]. An explanation can be provided as follows: When some transmitters do not have messages to transmit, we may employ them as "helpers". Even though secrecy constraint is considered in our problem, with the help of the "helpers", the effect due to the existence of the eavesdropper in the network can be *eliminated*. Hence, the s.d.o.f. region is dominated by interference in this case.

4.5.1 Converse for K-User IC-EE

The constraint in (4.15) follows from the non-secrecy constraints on the K-user IC in [54, 55]. We note that this same constraint is valid for the converse proof of IC-CM in the next section as well.

In order to prove (4.14) in Theorem 4.2, we re-examine (3.31) in Chapter 3. Originally, we applied Lemma 3.1 in Chapter 3 by treating the signal from transmitter j as the unintended noise to its neighboring transmitter-receiver pair $j-1$, i.e., for any $i = 1, \ldots, K$,

$$n\sum_{j=1}^{K} R_j \leq \sum_{j=1, j\neq i}^{K} h(\tilde{\mathbf{X}}_j) + nc_{53} \tag{4.86}$$

$$\leq [h(\mathbf{Y}_K) - nR_K] + [h(\mathbf{Y}_1) - nR_1] + \cdots + [h(\mathbf{Y}_{i-2}) - nR_{i-2}]$$

$$+ [h(\mathbf{Y}_i) - nR_i] + \cdots + [h(\mathbf{Y}_{K-1}) - nR_{K-1}] + nc_{54} \tag{4.87}$$

By noting that $h(\mathbf{Y}_j) \leq \frac{n}{2}\log P + nc'_j$ for each j, we have

$$2n\sum_{j=1}^{K} R_j \leq (K-1)\frac{n}{2}\log P + nR_i + nc_{55} \tag{4.88}$$

Therefore, we have a total of K bounds for $i = 1, \ldots, K$. Summing these K bounds, we obtained:

$$(2K-1)n\sum_{j=1}^{K} R_j \leq K(K-1)\frac{n}{2}\log P + nc_{56} \tag{4.89}$$

which gave

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \tag{4.90}$$

completing the converse proof for the sum s.d.o.f. of IC-EE in Theorem 3.1 in Chapter 3.

Here, we continue from (3.31) and re-interpret it as:

$$n\sum_{j=1}^{K} R_j \leq \sum_{j=1, j\neq i}^{K} h(\tilde{\mathbf{X}}_j) + nc_{57} \tag{4.91}$$

$$\leq \underbrace{[h(\mathbf{Y}_i) - nR_i] + \cdots + [h(\mathbf{Y}_i) - nR_i]}_{K-1 \text{ items}} + nc_{58} \tag{4.92}$$

$$= (K-1)h(\mathbf{Y}_i) - (K-1)nR_i + nc_{58} \tag{4.93}$$

$$\leq (K-1)\left(\frac{n}{2}\log P\right) - (K-1)nR_i + nc_{59} \tag{4.94}$$

where $i \in \{1, \ldots, K\}$ is arbitrary. Here, the second inequality means that we apply

Lemma 3.1 in Chapter 3 by treating the signal from all transmitters $j \neq i$ as the unintended noise to the transmitter-receiver pair i.

Rearranging the terms in (4.94), dividing both sides by $\frac{n}{2}\log P$, and taking the limit $P \to \infty$ on both sides, we obtain

$$Kd_i + \sum_{j=1, j\neq i}^{K} d_j \leq K-1, \qquad i = 1, \ldots, K \tag{4.95}$$

which is (4.14) in Theorem 4.2, completing the converse proof for IC-EE.

4.5.2 Converse for K-User IC-CM

When we studied the sum s.d.o.f. of IC-CM, we applied Lemma 3.1 in Chapter 3 to (3.53) by treating the signal from transmitter j as the unintended noise to its neighbor transmitter-receiver pair $j+1$, i.e., for any $i = 1, \ldots, K$

$$\begin{aligned} n\sum_{j=1, j\neq i}^{K} R_j &\leq \sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) - h(\mathbf{Y}_i) + nc_{60} && (4.96)\\ &\leq \left[\sum_{j=1}^{K-1}\left[h(\mathbf{Y}_{j+1}) - nR_{j+1}\right]\right] + \left[h(\mathbf{Y}_1) - nR_1\right] - h(\mathbf{Y}_i) + nc_{61} && (4.97)\\ &= \sum_{j=1}^{K}\left[h(\mathbf{Y}_j) - nR_j\right] - h(\mathbf{Y}_i) + nc_{61} && (4.98) \end{aligned}$$

By noting that $h(\mathbf{Y}_j) \leq \frac{n}{2}\log P + nc'_j$ for each j, we have

$$\begin{aligned} nR_i + 2n\sum_{j=1, j\neq i}^{K} R_j &\leq \sum_{j=1, j\neq i}^{K} h(\mathbf{Y}_j) + nc_{61} && (4.99)\\ &\leq (K-1)\frac{n}{2}\log P + nc_{62} && (4.100) \end{aligned}$$

Therefore, we have a total of K bounds for $i = 1, \ldots, K$. Summing these K bounds, we obtained

$$(2K-1)n \sum_{j=1}^{K} R_j \leq K(K-1)\frac{n}{2} \log P + nc_{63} \tag{4.101}$$

which gave

$$D_{s,\Sigma} \leq \frac{K(K-1)}{2K-1} \tag{4.102}$$

completing the converse proof for the sum s.d.o.f. of IC-CM in Theorem 3.1 in Chapter 3.

Here, we continue from (3.53) and re-interpret it as follows: For any $i \in \{1, \ldots, K\}$, we select

$$k \stackrel{\triangle}{=} \begin{cases} i-1, & \text{if } i \geq 2 \\ K, & \text{if } i = 1 \end{cases} \tag{4.103}$$

and then have

$$n \sum_{j=1, j\neq i}^{K} R_j \leq \left[\sum_{j=1}^{K} h(\tilde{\mathbf{X}}_j) \right] - h(\mathbf{Y}_i) + nc_{64} \tag{4.104}$$

$$\leq h(\tilde{\mathbf{X}}_k) + \left[\sum_{j=1, j\neq k}^{K} h(\tilde{\mathbf{X}}_j) \right] - h(\mathbf{Y}_i) + nc_{65} \tag{4.105}$$

$$\leq h(\mathbf{Y}_i) - nR_i + \left[\sum_{j=1, j\neq k}^{K} h(\tilde{\mathbf{X}}_j) \right] - h(\mathbf{Y}_i) + nc_{66} \tag{4.106}$$

$$= \left[\sum_{j=1, j\neq k}^{K} h(\tilde{\mathbf{X}}_j) \right] - nR_i + nc_{66} \tag{4.107}$$

$$\leq \underbrace{[h(\mathbf{Y}_k) - nR_k] + \cdots + [h(\mathbf{Y}_k) - nR_k]}_{K-1 \text{ items}} - nR_i + nc_{67} \tag{4.108}$$

$$= (K-1)h(\mathbf{Y}_k) - (K-1)nR_k - nR_i + nc_{67} \tag{4.109}$$

$$\leq (K-1)\left(\frac{n}{2}\log P\right) - (K-1)nR_k - nR_i + nc_{67} \tag{4.110}$$

which is

$$(K-1)nR_k + n\sum_{j=1}^{K} R_j \leq (K-1)\left(\frac{n}{2}\log P\right) + nc_{67} \tag{4.111}$$

Here, inequality (4.106) means that we apply Lemma 3.1 in Chapter 3 by treating the signal from transmitter k as the unintended noise to the transmitter-receiver pair i. Similarly, inequality (4.108) means that we apply Lemma 3.1 by treating the signal from transmitter $j \neq k$ as the unintended noise to the transmitter-receiver pair k.

Rearranging the terms in (4.111), dividing both sides by $\frac{n}{2}\log P$, and taking

the limit $P \to \infty$ on both sides, we obtain

$$Kd_k + \sum_{j=1, j\neq k}^{K} d_j \leq K - 1, \qquad k = 1, \ldots, K \tag{4.112}$$

which is (4.14) in Theorem 4.2, completing the converse proof for IC-CM.

4.5.3 Polytope Structure and Extreme Points

Similar to the discussion and approach in the MAC problem in Section 4.4.2, it is easy to see that the region D characterized by Theorem 4.2 is a polytope, which is equal to the convex combinations of all extreme points of D due to Theorem 4.4. Therefore, in order to show the tightness of region D, it suffices to prove that all extreme points of D are achievable.

We first assume that $K \geq 3$, and determine the structure of all extreme points of D in the following theorem.

Theorem 4.8 *For the K-dimensional region D, $K \geq 3$, in Theorem 4.2, any ex-*

treme point must be a point with one of the following structures:

$$(0, 0, \ldots, 0), \tag{4.113}$$

$$\Big(\frac{K-1-p}{K-p}, \underbrace{\frac{1}{K-p}, \ldots, \frac{1}{K-p}}_{p \text{ items}}, \underbrace{0, \ldots, 0}_{m \text{ items}}\Big), \quad K-2 \geq p \geq 0, m = K-1-p \geq 1 \tag{4.114}$$

$$\Big(\underbrace{\frac{1}{2}, \ldots, \frac{1}{2}}_{p' \text{ items}}, \underbrace{0, \ldots, 0}_{m' \text{ items}}\Big), \qquad K-2 \geq p' \geq 3, m' \geq 1, p'+m' = K \geq 5 \tag{4.115}$$

$$\Big(\frac{K-1}{2K-1}, \frac{K-1}{2K-1}, \ldots, \frac{K-1}{2K-1}\Big) \tag{4.116}$$

up to element reordering.

The proof of Theorem 4.8 is provided in Appendix 4.7.1.

Now, in order to show the tightness of region D, it suffices to show the achievability for each structure in Theorem 4.8. Clearly, the zero vector in (4.113) is trivially achievable. The symmetric tuple in (4.116) is achievable due to Chapter 3. Therefore, it remains to show the achievability of the structures in (4.114) and (4.115).

In order to address the achievabilities of (4.114) and (4.115), we formulate a new channel model as a $(p+1)$-user IC-CM-EE channel with m independent helpers and N independent external eavesdroppers. The formal definition of this channel model is given in Section 4.5.4. Then, we have the following theorem.

Theorem 4.9 *For the $(p+1)$-user IC-CM-EE channel with m independent helpers and N independent external eavesdroppers, as far as $p \geq 0$, $m \geq 1$, and N is finite,*

the following s.d.o.f. tuple is achievable:

$$\Big(\frac{m}{m+1}, \underbrace{\frac{1}{m+1}, \frac{1}{m+1}, \ldots, \frac{1}{m+1}}_{p \text{ items}}\Big) \tag{4.117}$$

for almost all channel gains.

The proof of Theorem 4.9 is provided in Section 4.5.4.

Here, we provide a few comments about Theorem 4.9. Theorem 4.9 provides quite general results, and subsumes some other known cases:

1) The result in Chapter 2, Section 2.5 is a special case of Theorem 4.9 with $p = 0, m \geq 1, N = 1$.

2) (4.114) is a special case of Theorem 4.9 with $p \geq 0, m = K - 1 - p \geq 1, N = m + 1$.

3) (4.115) is a byproduct of Theorem 4.9: By choosing $p = p' - 1, m = 1, N = m' + 1$, we know that with just one helper, the following s.d.o.f. tuple is achievable:

$$\Big(\underbrace{\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}}_{p' \text{ items}}, 0\Big) \tag{4.118}$$

Now, if we add $m' - 1$ more independent helpers into the network, (4.115) can be achieved trivially.

Therefore, with the help of Theorem 4.9, each structure in Theorem 4.8 can be achieved, which provides the achievability proof for Theorem 4.2 for $K \geq 3$.

Finally, we address the $K = 2$ case. In this case, the region D characterized by (4.14)-(4.16) in Theorem 4.2 is given by (4.79). In order to provide the achievability, it suffices to prove that the extreme points $(\frac{1}{2}, 0), (0, \frac{1}{2})$, and $(\frac{1}{3}, \frac{1}{3})$ are achievable. The achievability of $(\frac{1}{3}, \frac{1}{3})$ was proved in Chapter 3. The achievabilities of $(\frac{1}{2}, 0), (0, \frac{1}{2})$ are the special cases of Theorem 4.9 with $p = 0, m = 1, N = 2$.

4.5.4 Achievability

The $(p+1)$-user IC-CM-EE channel with m independent helpers and N independent external eavesdroppers is

$$Y_i = \sum_{j=1}^{p+1+m} h_{ji} X_j + N_i, \qquad i = 1, \ldots, p+1 \tag{4.119}$$

$$Z_k = \sum_{j=1}^{p+1+m} g_{jk} X_j + N_{z_k}, \qquad k = 1, \ldots, N \tag{4.120}$$

where Y_i is the channel output of receiver i, Z_k is the channel output of external eavesdropper k, X_j is the channel input of transmitter j, h_{ji} is the channel gain of the jth transmitter to the ith receiver, g_{jk} is the channel gain of the jth transmitter to the kth eavesdropper, and $\{N_1, \ldots, N_{p+1}, N_{z_1}, \ldots, N_{z_N}\}$ are mutually independent zero-mean unit-variance Gaussian random variables. All channel gains are independently drawn from continuous distributions, and are time-invariant throughout the communication session. We further assume that all h_{ji} and g_{jk} are non-zero. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_j^2\right] \leq P$, for $j = 1, \ldots, p+1+m$.

Transmitter j, $j = p+2, \ldots, p+1+m$, is an independent helper in the network. On the other hand, each transmitter i, $i = 1, \ldots, p+1$, has a message W_i intended for the receiver Y_i. A rate tuple $(R_1, \ldots, R_{p+1})$ is said to be achievable if for any $\epsilon > 0$, there exist joint n-length codes such that each receiver i can decode the corresponding message reliably, i.e., the probability of decoding error is less than ϵ for all messages,

$$\max_i \Pr\left[W_i \neq \hat{W}_i\right] \leq \epsilon \tag{4.121}$$

where $\hat{W}_i$ is the estimation based on its observation $\mathbf{Y}_i$. The secrecy constraints are defined as follows:

$$\frac{1}{n} H(W_{-i}^{p+1} | \mathbf{Y}_i) \geq \frac{1}{n} H(W_{-i}^{p+1}) - \epsilon, \qquad i = 1, \ldots, p+1 \tag{4.122}$$

$$\frac{1}{n} H(W_1, \ldots, W_{p+1} | \mathbf{Z}_k) \geq \frac{1}{n} H(W_1, \ldots, W_{p+1}) - \epsilon, \qquad k = 1, \ldots, N \tag{4.123}$$

where $W_{-i}^{p+1} \triangleq \{W_1, \ldots, W_{p+1}\} \backslash \{W_i\}$. A s.d.o.f. tuple $(d_1, \ldots, d_{p+1})$ is achievable if there exists an achievable rate tuple $(R_1, \ldots, R_{p+1})$ such that

$$d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2} \log P} \tag{4.124}$$

for $i = 1, \ldots, p+1$.

Now, we prove Theorem 4.9, i.e., for $p \geq 0$, $m \geq 1$, and N is finite, the

following s.d.o.f. tuple is achievable:

$$\Big(\frac{m}{m+1}, \underbrace{\frac{1}{m+1}, \frac{1}{m+1}, \ldots, \frac{1}{m+1}}_{p \text{ items}}\Big) \tag{4.125}$$

for almost all channel gains.

The purpose of Theorem 4.9 is to prove the achievability of the structure (4.114) in Theorem 4.8. As shown in (4.114), we partition the transmitters into three groups: 1) the first group consists of only one transmitter with the largest s.d.o.f., $\frac{K-1-p}{K-p}$, which is no smaller than $\frac{1}{2}$, 2) the second group consists of $p \geq 0$ transmitters with the same s.d.o.f., $\frac{1}{K-p}$, which is no larger than $\frac{1}{2}$, and 3) the third group consists of $m \geq 1$ transmitters serving as independent helpers. Therefore, in (4.125), we consider the $p+1$-user IC with m helpers where $K = p + 1 + m$. Therefore, (4.125) and Theorem 4.9 show the achievability of (4.114). We know from remark 2) above that the achievability of (4.115) is a byproduct of Theorem 4.9. Also, (4.113) is trivially achieved, and the achievability of (4.116) is shown in Chapter 3. Therefore, we focus on Theorem 4.9, from this point on.

The technique we use in the proof of Theorem 4.9 is asymptotical interference alignment and cooperative jamming. The alignment scheme is illustrated in Figure 4.4 with $m = 3, p = 2, N = 1$. In Figure 4.4, we partition the transmitters into three groups, which are $\{X_1\}$ as the first group, $p = 2$ other transmitters $\{X_2, X_3\}$ as the second group, and $m = 3$ helpers as the third group. From the perspective of Y_1 and the eavesdropper Z, due to the existence of independent helpers, the alignment signaling design is similar to that in wiretap channel with helpers in Chapter

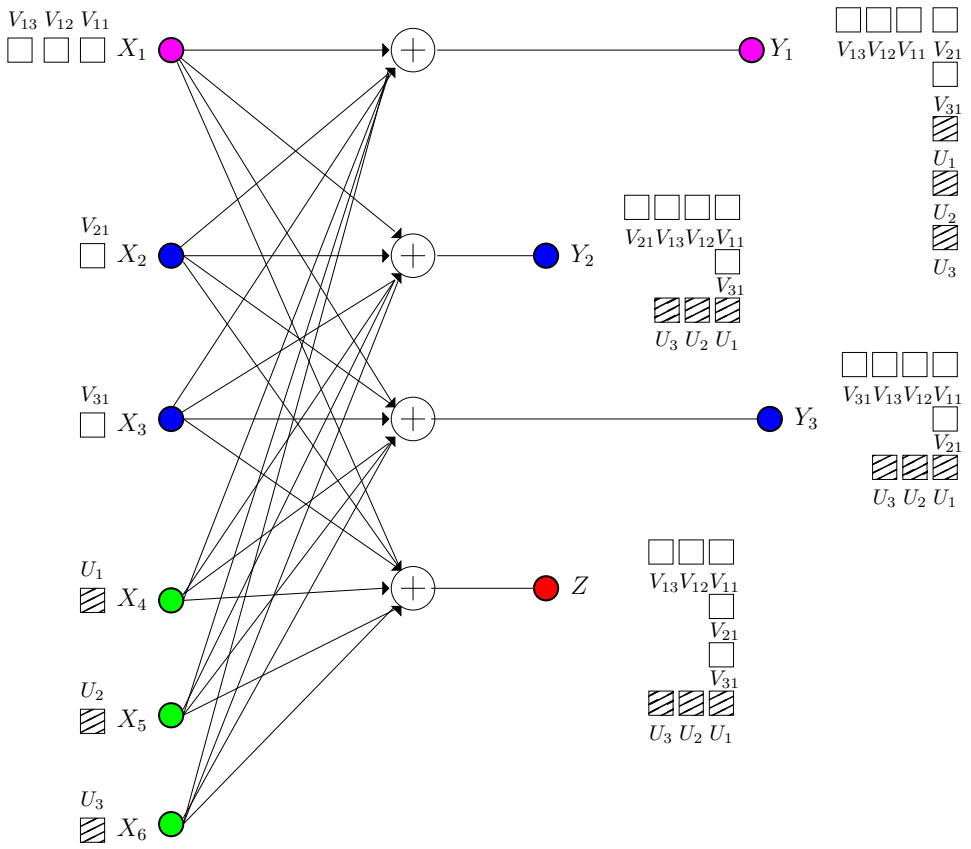


Figure 4.4: Illustration of secure interference alignment of Theorem 4.9 with $m = 3, p = 2, N = 1$.

2, Figure 2.2. However, from the perspective of Y_2, Y_3, and the eavesdropper Z, the alignment signaling design is similar to that in the IC in Chapter 3, Figure 3.1. This suggests that the signalling scheme that achieves on arbitrary extreme point of the s.d.o.f. region is in between the signalling scheme that achieves the sum s.d.o.f. of IC-CM-EE in Chapter 3 and the signalling scheme used in the helper network in Chapter 2, Section 2.5. Furthermore, if we let $p = 0$, the signaling scheme in Figure 4.4 would be almost identical to Figure 2.2. However, we cannot let $m \to 0$. As far as the number of independent helper(s) in Figure 4.4, m, is non-zero, in contrast to the scheme in Figure 3.1, the legitimate transmitters in the first and second

groups do not use use superposition code to send cooperative jamming signals by themselves, however, in Chapter 3 for IC-CM-EE without helpers, each legitimate transmitter needed to send both message signals and a cooperative signal. Note that in Figure 4.4 here, legitimate transmitters $\{X_1, X_2, X_3\}$ do not send any cooperative jamming signals (shaded boxes).

Here, we give the general achievable scheme. Let l be a large constant. Let us define a set T_1 which will represent *dimensions* as follows:

$$T_1 \triangleq \left\{ \left(\prod_{(j,k)\in L} h_{jk}^{r_{jk}} \right) \left(\prod_{k=1}^{N} \prod_{j=1}^{p+1+m} g_{jk}^{s_{jk}} \right) : \ r_{jk}, s_{jk} \in \{1, \ldots, l\} \right\} \tag{4.126}$$

where L contains almost all pairs corresponding to the cross-link channel gains

$$\begin{aligned} L = &\Big\{(j,k) : j \in \{2, \ldots, p+2\}, k = 1\Big\} \\ &\cup \Big\{(j,k) : j \in \{1, \ldots, p+1+m\}, k \in \{2, \ldots, p+1\}, j \neq k\Big\} \end{aligned} \tag{4.127}$$

Clearly, starting from the second helper X_{p+3}, if there exists any, the cross-link channel gains to the first legitimate receiver Y_1 are not in the set L. Therefore, we define the sets $\{T_j\}_{j=2}^{m}$

$$T_j = \frac{1}{h_{p+1+j,1}} T_1, \qquad j = 2, \ldots, m \tag{4.128}$$

Let M_i be the cardinality of T_i, $i = 1, \ldots, m$. Note that all M_i are the same, thus

we denote them as M,

$$M \stackrel{\triangle}{=} l^{|L|+N(p+1+m)} = l^{\theta} \tag{4.129}$$

where $\theta \stackrel{\triangle}{=} (p+1+m)p + p + N(p+1+m) + 1$.

Let $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ be the vector containing all the elements in the set T_j for any possible i. Therefore, $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ are M-dimensional vectors containing M rationally independent real numbers in T_j. The sets $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ will represent the *dimensions* along which message signals are transmitted. In particular, as illustrated in Figure 4.4, for each legitimate transmitter i, $i = 1, \ldots, p+1$, the message signal V_{i1} is transmitted in dimensions $\mathbf{t}_{i1}$. In order to asymptotically align U_1 from the first helper X_{p+2} with all V_{i1}s, the cooperative jamming signal U_1 is transmitted in dimensions $\mathbf{t}_{(1)}$. Similarly, for the first transmitter X_1, the message signal V_{1j}, $j = 2, \ldots, m$, is transmitted in dimensions $\mathbf{t}_{1j}$. Since we want to align the cooperative jamming signal U_j from the helper X_{p+1+j} with V_{1j} one by one, the jamming signal U_j is transmitted in dimensions $\mathbf{t}_{(j)}$.

Let us define an mM dimensional vector $\mathbf{b}_1$ by stacking $\mathbf{t}_{i1}$s as

$$\mathbf{b}_1^T = \left[\mathbf{t}_{11}^T, \mathbf{t}_{12}^T, \ldots, \mathbf{t}_{1m}^T\right] \tag{4.130}$$

Then, transmitter 1 generates a vector $\mathbf{a}_1$, which contains a total of mM discrete signals each identically and independently drawn from $C(a, Q)$ given in (2.73). For

convenience, we partition this transmitted signal as

$$\mathbf{a}_1^T = \left[\mathbf{v}_{11}^T, \mathbf{v}_{12}^T, \ldots, \mathbf{v}_{1m}^T\right] \tag{4.131}$$

where $\mathbf{v}_{1j}$ represents the information symbols in V_{1j}. Each of these vectors has length M, and therefore, the total length of $\mathbf{a}_1$ is mM. The channel input of transmitter 1 is

$$x_1 = \mathbf{a}_1^T \mathbf{b}_1 \tag{4.132}$$

Similarly, for the second group transmitters X_i, $i = 2, \ldots, p+1$, let $\mathbf{b}_i$ be $\mathbf{b}_i = \mathbf{t}_{i1}$. Then, transmitter i generates a vector $\mathbf{a}_i = \mathbf{v}_{i1}$, which contains a total of M discrete signals each identically and independently drawn from $C(a, Q)$ given in (2.73). The channel input of transmitter i is

$$x_i = \mathbf{a}_i^T \mathbf{b}_i = \mathbf{v}_{i1}^T \mathbf{t}_{i1}, \qquad i = 2, \ldots, p+1 \tag{4.133}$$

Finally, for the third group transmitters X_k, $k = p+2, \ldots, p+1+m$, serving as the helpers, let $\mathbf{b}_k$ be $\mathbf{b}_k = \mathbf{t}_{(k-p-1)}$. Then, helper k generates a vector $\mathbf{u}_{k-p-1}$ representing the cooperative jamming signal in U_{k-p-1}, which contains a total of M discrete signals each identically and independently drawn from $C(a, Q)$ given in (2.73). The channel input of transmitter k is

$$x_k = \mathbf{u}_{k-p-1}^T \mathbf{b}_k = \mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)}, \qquad k = p+2, \ldots, p+1+m \tag{4.134}$$

Before we investigate the performance of this signalling scheme, we analyze the structure of the received signals at the receivers. To see the detailed dimension structure of the received signals at the receivers, let us define $\tilde{T}_i$ as a superset of T_i, as follows

$$\tilde{T}_1 \triangleq \left\{ \left(\prod_{(j,k)\in L} h_{jk}^{r_{jk}} \right) \left(\prod_{k=1}^{N} \prod_{j=1}^{p+1+m} g_{jk}^{s_{jk}} \right) : \ r_{jk}, s_{jk} \in \{1, \ldots, l+1\} \right\} \tag{4.135}$$

$$\tilde{T}_j = \frac{1}{h_{p+1+j,1}} \tilde{T}_1, \qquad j = 2, 3, \ldots, m \tag{4.136}$$

where L is defined in (4.127) and the cardinalities of all T_i sets are the same and are denoted as $\tilde{M} = (l+1)^\theta$. Also, it is easy to check that since pair $(p+1+j, 1) \notin L$ for $j \geq 2$, we must have

$$\tilde{T}_i \cap \tilde{T}_j = \phi \tag{4.137}$$

for all $i \neq j$.

We first focus on receiver 1, which has the channel output

$$y_1 = \sum_{i=1}^{p+1+m} h_{i1} x_1 + n_1 \tag{4.138}$$

Substituting (4.132), (4.133) and (4.134) into (4.138), we get

$$y_1 = h_{11}x_1 + \sum_{j=2}^{p+1} h_{j1}x_j + \sum_{k=p+2}^{p+1+m} h_{k1}x_k + n_1 \tag{4.139}$$

$$= h_{11}\left(\sum_{i=1}^{m} \mathbf{v}_{1i}^T \mathbf{t}_{1i}\right) + \left(\sum_{j=2}^{p+1} h_{j1}\mathbf{v}_{j1}^T \mathbf{t}_{j1}\right) + \left(\sum_{k=p+2}^{p+1+m} h_{k1}\mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)}\right) + n_1 \tag{4.140}$$

$$= \left(\mathbf{v}_{11}^T h_{11}\mathbf{t}_{11}\right) + \left(\mathbf{v}_{12}^T h_{11}\mathbf{t}_{12}\right) + \ldots + \left(\mathbf{v}_{1m}^T h_{11}\mathbf{t}_{1m}\right) + \left(\sum_{j=2}^{p+1} h_{j1}\mathbf{v}_{j1}^T \mathbf{t}_{j1} + \sum_{k=p+2}^{p+1+m} h_{k1}\mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)}\right) + n_1 \tag{4.141}$$

Since $\mathbf{v}_{ij}$ and $\mathbf{u}_{k-p-1}$ are integer signals in $C(a, Q)$, it suffices to study their dimensions. In addition, note that $\mathbf{t}_{ij}$ and $\mathbf{t}_{(j)}$ represent the same dimensions in T_j defined in (4.126) and (4.128). It is easy to verify that

$$h_{j1}T_1 \subseteq \tilde{T}_1, \qquad j = 2, \ldots, p+1 \tag{4.142}$$

$$h_{k1}T_{k-p-1} \subseteq \tilde{T}_1, \qquad k = p+2, \ldots, p+1+m \tag{4.143}$$

which implies that except the intended message signals $\mathbf{v}_{1i}$, $i = 1, \ldots, m$, all unintended signals including message signals and cooperative jamming signals are all transmitted in the dimensions belonging to $\tilde{T}_1$. On the other hand, for intended signals,

$$h_{11}T_1 \subset h_{11}\tilde{T}_1 \tag{4.144}$$

$$h_{11}T_i \subseteq h_{11}\tilde{T}_i = \frac{h_{11}}{h_{p+1+i,1}}\tilde{T}_1, \qquad i = 2, \ldots, m \tag{4.145}$$

Note that the pair $(p+1+i,1) \notin L$ for $i \geq 2$ which implies that

$$h_{11}\tilde{T}_i \cap h_{11}\tilde{T}_j = \phi \tag{4.146}$$

for all $i, j \in \{1, \ldots, m\}$, $i \neq j$. Furthermore, $(1,1) \notin L$ either, which implies that

$$h_{11}\tilde{T}_i \cap \tilde{T}_1 = \phi, \qquad i \in \{1, \ldots, m\} \tag{4.147}$$

Together with (4.146), this indicates that the dimensions are separable as suggested by the parentheses in (4.141) and also the Y_1 side of Figure 4.4, which further implies that all the elements in the set

$$R_1 \triangleq \left(\bigcup_{j=1}^{m} h_{11}\tilde{T}_j \right) \cup \tilde{T}_1 \tag{4.148}$$

are rationally independent, and thereby the cardinality of R_1 is

$$M_R \triangleq |R_1| = (m+1)\tilde{M} = (m+1)(l+1)^{\theta} \tag{4.149}$$

For the legitimate receivers Y_i, $i = 2, \ldots, p+1$, without loss of generality, we focus on receiver 2; by symmetry, a similar structure will exist at all other receivers.

We observe that

$$y_2 = h_{12}x_1 + \sum_{j=2}^{p+1} h_{j2}x_j + \sum_{k=p+2}^{p+1+m} h_{k2}x_k + n_2 \tag{4.150}$$

$$= h_{12}\left(\sum_{i=1}^{m} \mathbf{v}_{1i}^T \mathbf{t}_{1i}\right) + \left(\sum_{j=2}^{p+1} h_{j2}\mathbf{v}_{j1}^T \mathbf{t}_{j1}\right) + \left(\sum_{k=p+2}^{p+1+m} h_{k2}\mathbf{u}_{k-p-1}^T \mathbf{t}_{(k-p-1)}\right) + n_2 \tag{4.151}$$

$$= \left(h_{22}\mathbf{v}_{21}^T \mathbf{t}_{21}\right) + \left(\mathbf{v}_{11}^T h_{12}\mathbf{t}_{11} + \sum_{j=3}^{p+1} \mathbf{v}_{j1}^T h_{j2}\mathbf{t}_{j1} + \mathbf{u}_1^T h_{p+2,2}\mathbf{t}_{(1)}\right)$$
$$+ \left(\mathbf{v}_{12}^T h_{12}\mathbf{t}_{12} + \mathbf{u}_2^T h_{p+3,2}\mathbf{t}_{(2)}\right) + \ldots + \left(\mathbf{v}_{1m}^T h_{12}\mathbf{t}_{1m} + \mathbf{u}_m^T h_{p+1+m,2}\mathbf{t}_{(m)}\right) + n_2 \tag{4.152}$$

Similarly, we observe that in the second set of parentheses of (4.152), since $\mathbf{t}_{i1}$ and $\mathbf{t}_{(1)}$ represent the same dimensions in T_1 for all i, we have

$$h_{i2}T_1 \subseteq \tilde{T}_1, \qquad i \in \{1, \ldots, p+2\}, i \neq 2 \tag{4.153}$$

Starting from the third set of parentheses of (4.152), we have

$$h_{12}T_j \subseteq \tilde{T}_j \tag{4.154}$$

$$h_{p+1+j,2}T_j \subseteq \tilde{T}_j \tag{4.155}$$

for all $j = 2, \ldots, m$. In addition, since the pair $(2, 2) \notin L$, we can infer that

$$h_{22}T_1 \subseteq h_{22}\tilde{T}_1 \tag{4.156}$$

and

$$h_{22}\tilde{T}_1 \cap \tilde{T}_j \tag{4.157}$$

for $j = 1, \ldots, m$. Together with (4.137), this indicates that the dimensions are separable as suggested by the parentheses in (4.152) and also the Y_2 side of Figure 4.4, which further implies that all the elements in the set

$$R_2 \triangleq \left(\bigcup_{j=1}^{m} \tilde{T}_j \right) \cup h_{22}\tilde{T}_1 \tag{4.158}$$

are rationally independent, and thereby the cardinality of R_2 is M_R in (4.149).

For the external eavesdropper Z_k, we note that

$$z_k = g_{1k}x_1 + \sum_{j=2}^{p+1} g_{jk}x_j + \sum_{i=p+2}^{p+1+m} g_{ik}x_i + n_{z_k} \tag{4.159}$$

$$= g_{1k}\left(\sum_{i=1}^{m} \mathbf{v}_{1i}^T \mathbf{t}_{1i} \right) + \left(\sum_{j=2}^{p+1} g_{jk}\mathbf{v}_{j1}^T \mathbf{t}_{j1} \right) + \left(\sum_{i=p+2}^{p+1+m} g_{ik}\mathbf{u}_{i-p-1}^T \mathbf{t}_{(i-p-1)} \right) + n_{z_k} \tag{4.160}$$

$$= \left(\mathbf{v}_{11}^T g_{1k}\mathbf{t}_{11} + \sum_{j=2}^{p+1} \mathbf{v}_{j1}^T g_{jk}\mathbf{t}_{j1} + \mathbf{u}_1^T g_{p+2,k}\mathbf{t}_{(1)} \right) + \left(\mathbf{v}_{12}^T g_{1k}\mathbf{t}_{12} + \mathbf{u}_2^T g_{p+3,k}\mathbf{t}_{(2)} \right) + \ldots + \left(\mathbf{v}_{1m}^T g_{1k}\mathbf{t}_{1m} + \mathbf{u}_m^T g_{p+1+m,k}\mathbf{t}_{(m)} \right) + n_{z_k} \tag{4.161}$$

In the first set of parentheses of (4.161), since $\mathbf{t}_{i1}$ and $\mathbf{t}_{(1)}$ represent the same dimensions in T_1 for all i, we have

$$g_{ik}T_1 \subseteq \tilde{T}_1, \qquad i \in \{1, \ldots, p+2\} \tag{4.162}$$

Starting from the second set of parentheses of (4.161), we have

$$g_{1k}T_j \subseteq \tilde{T}_j \tag{4.163}$$

$$g_{p+1+j,k}T_j \subseteq \tilde{T}_j \tag{4.164}$$

for all $j = 2, \ldots, m$. Due to (4.137), this indicates that the dimensions are separable as suggested by the parentheses in (4.161) and also the Z side of Figure 4.4, which further implies that all the elements in the set

$$R_Z \triangleq \left(\bigcup_{j=1}^{m} \tilde{T}_j \right) \tag{4.165}$$

are rationally independent, and thereby the cardinality of R_Z is M_{R_Z}

$$M_{R_Z} \triangleq |R_Z| = m\tilde{M} = m(l+1)^{\theta} \tag{4.166}$$

We will compute the secrecy rates achievable with the asymptotic alignment based scheme proposed above by using the following theorem.

Theorem 4.10 (Chapter 3, Theorem 3.1) *For K'-user interference channels with confidential messages, the following rate region is achievable*

$$R_i \geq I(V_i; Y_i) - \max_{j \in \mathcal{K}'_{-i}} I(V_i; Y'_j | V_{-i}^{K'}), \qquad i = 1, \ldots, K' \tag{4.167}$$

where $V_{-i}^{K'} \triangleq \{V_j\}_{j=1, j\neq i}^{K'}$ and $\mathcal{K}'_{-i} = \{1, \ldots, i-1, i+1, \ldots, K'\}$. The auxiliary random variables $\{V_i\}_{i=1}^{K'}$ are mutually independent, and for each i, we have the

following Markov chain $V_i \to X_i' \to (Y_1', \ldots, Y_{K'}')$.

We can reinterpret Theorem 4.10 as follows: For the $(p+1)$-user IC-CM-EE with m helpers and N external eavesdroppers, since each independent helper's contribution is the same as noise to both items in (4.167), which depend only on marginal distributions, we can treat the $(p+1)$-user IC-CM-EE channel as a $(p+1+N)$-user IC-CM with N new transmitters which keep silent, i.e., V_i and X_i', $i = p+2, \ldots, p+1+N$, are equal to zero, and

$$p(y_1', \ldots, y_{p+1+N}' | x_1', \ldots, x_{p+1+N}') = p(y_1, \ldots, y_{p+1}, z_1, \ldots, z_N | x_1, \ldots, x_{p+1}) \quad (4.168)$$

where x' and y' are the transmitter and receiver of the $(p+1+N)$-user IC-CM and x, y, z are the entities of the original $(p+1)$-user IC-CM-EE with m helpers and N external eavesdropper.

We thereby first select V_i as

$$V_1 \stackrel{\triangle}{=} \mathbf{a}_1 \quad (4.169)$$

$$V_i \stackrel{\triangle}{=} \mathbf{v}_{i1} \qquad i = 2, \ldots, p+1 \quad (4.170)$$

where $\mathbf{a}_1$ is defined in (4.131). Then, we evaluate the (4.167) for $i = 1, \ldots, p+1$.

For $i = 1$, by Lemma 2.3 in Chapter 2, for any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(M_R+\delta)}}$ and $a = \frac{\gamma_1 P^{\frac{1}{2}}}{Q}$, the probability of error of estimating V_1 as $\tilde{V}_1$ based on Y_1 can be upper bounded by

$$\Pr(e_1) \leq \exp\left(-\eta_{\gamma_1} P^{\delta}\right) \quad (4.171)$$

Furthermore, by Fano's inequality, we can conclude that

$$I(V_1;Y_1) \leq I(V_1;\tilde{V}_1) \tag{4.172}$$

$$= H(V_1) - H(V_1|\tilde{V}_1) \tag{4.173}$$

$$\geq \frac{mM(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.174}$$

$$= \frac{m(1-\delta)}{(m+1)\left(1+\frac{1}{l}\right)^{\theta}+\frac{\delta}{l^{\theta}}}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.175}$$

where $o(\cdot)$ is the little-o function. This provides a lower bound for the first term in (4.167) with $i = 1$.

Next, we need to derive an upper bound for the second item in (4.167), i.e, the secrecy penalty, for $i = 1$. For and $j \in \{2, \ldots, p+1\}$, by the Markov chain,

$$V_1 \rightarrow \left(\sum_{k=1}^{p+1} h_{kj}X_{kj}, V_2^{p+1}\right) \rightarrow Y_j \tag{4.176}$$

we have

$$I(V_1;Y_j|V_2^{p+1}) \leq I\left(V_1;\sum_{k=1}^{p+1} h_{kj}X_k\Big|V_2^{p+1}\right) \tag{4.177}$$

$$= H\left(\sum_{k=1}^{p+1} h_{kj}X_k\Big|V_2^{p+1}\right) - H\left(\sum_{k=1}^{p+1} h_{kj}X_k\Big|V_1^{p+1}\right) \tag{4.178}$$

The first term in (4.178) can be rewritten as

$$H\left(\sum_{k=1}^{p+1} h_{kj}X_k\Big|V_2^{p+1}\right) = H\left[\sum_{i=k}^{m}\left(\mathbf{v}_{1k}^T h_{1j}\mathbf{t}_{1k} + \mathbf{u}_k^T h_{p+1+k,j}\mathbf{t}_{(k)}\right)\right] \tag{4.179}$$

Note that there are in total mM_R rational dimensions each taking value from $C(a, 2Q)$. Regardless of the distribution in each rational dimension, the entropy is maximized by uniform distribution, i.e.,

$$H\left(\sum_{k=1}^{p+1} h_{kj}X_k \Big| V_2^{p+1}\right) \leq \log\left[(2Q+1)^{m\tilde{M}}\right] = \frac{m\tilde{M}(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.180}$$

The second term in (4.178) is

$$H\left(\sum_{k=1}^{p+1} h_{kj}X_k \Big| V_1^{p+1}\right) = H\left[\sum_{i=k}^{m}\left(\mathbf{u}_k^T h_{p+1+k,j}\mathbf{t}_{(k)}\right)\right] = \log\left[(2Q+1)^{mM}\right] \tag{4.181}$$

$$= \frac{mM(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.182}$$

Substituting (4.180) and (4.182) into (4.178), we get

$$I(V_1; Y_j|V_2^{p+1}) \leq \frac{m(\tilde{M}-M)(1-\delta)}{M_R+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.183}$$

We note that

$$\xi \triangleq \frac{m(\tilde{M}-M)(1-\delta)}{M_R+\delta} = \frac{m(\tilde{M}-M)(1-\delta)}{(m+1)\tilde{M}+\delta} \tag{4.184}$$

$$= \frac{m\left[(l+1)^\theta - l^\theta\right](1-\delta)}{(m+1)(l+1)^\theta+\delta} \tag{4.185}$$

$$= \frac{m\left[\sum_{k=0}^{\theta-1}\binom{\theta}{k}l^k\right](1-\delta)}{(m+1)(l+1)^\theta+\delta} \tag{4.186}$$

The maximum power of l in the numerator is $\theta-1$ and is less than the power θ of l

in the denominator. This implies that when m and δ are fixed, by choosing l large enough, the factor before the $\frac{1}{2}\log P$ term in (4.183), ξ, can be made arbitrarily small. Due to the non-perfect (i.e., only asymptotical) alignment, the upper bound for the information leakage rate is not a constant as in Chapter 2, but a function which can be made to approach zero d.o.f.

Similarly, we can derive the following

$$I(V_1; Z_k|V_2^{p+1}) \leq \xi \left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.187}$$

where Z_k, $k = 1, \ldots, N$, is the external eavesdropper. Substituting (4.175), (4.183) and (4.187) into (4.167), we obtain a lower bound for the achievable secrecy rate R_1 as

$$R_1 \geq \left[\frac{m(1-\delta)}{(m+1)\left(1+\frac{1}{l}\right)^{\theta} + \frac{\delta}{l^{\theta}}} - \xi\right] \left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.188}$$

Similarly, it is easy to derive that

$$R_i \geq \left[\frac{(1-\delta)}{(m+1)\left(1+\frac{1}{l}\right)^{\theta} + \frac{\delta}{l^{\theta}}} - \xi'\right] \left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.189}$$

for $i = 2, \ldots, p+1$ and ξ' can be made arbitrarily small. By choosing $l \to \infty$ and $\delta \to 0$, we can achieve a s.d.o.f. tuple arbitrarily close to

$$\Big(\frac{m}{m+1}, \underbrace{\frac{1}{m+1}, \ldots, \frac{1}{m+1}}_{p \text{ items}}, \Big) \tag{4.190}$$

which is (4.117), completing the proof of Theorem 4.9.

4.6 Conclusions

In this chapter, we determined the *entire s.d.o.f. regions* of the K-user MAC wiretap channel, K-user IC-EE, K-user IC-CM, and K-user IC-CM-EE. The converse for the MAC directly followed from the results in Chapter 2, Section 2.9. The converse for the IC was shown to be dominated by secrecy constraints and interference constraints in different parts. To show the tightness and achieve the regions characterized by the converses, we provided a general method to investigate this class of channels, whose s.d.o.f. regions have a polytope structure. We provided the equivalence between the extreme points in the polytope structure and the rank of sub-matrices containing all active upper bounds associated with each extreme point. Then, we achieved each extreme point by relating it to a specific channel model. More specifically, each extreme point of the MAC region can be achieved by an m-user MAC wiretap channel with $K-m$ helpers, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers. On the other hand, each asymmetric extreme point of the IC region can be achieved by a $(p+1)$-user IC-CM with m helpers, and N external eavesdroppers.

4.7 Appendix

4.7.1 Proof of Theorem 4.8

Regarding Theorem 4.8, first, we have few comments:

1) (4.115) will not be possible until $K \geq 5$ due to the constraint $K-2 \geq p' \geq 3$.

2) The point in (4.115) with $p' = K-1$, i.e., $(1/2, 1/2, \ldots, 1/2, 0)$, is actually an extreme point, but since (4.114) with $p = K-2$ also includes it, we classify it as (4.114) here.

3) Assume that we allow $p' = 2$ in (4.115) with $K \geq 5$. Then, the point becomes

$$\mathbf{d}_1 = \left(\frac{1}{2}, \frac{1}{2}, 0, 0, \ldots, 0\right) \tag{4.191}$$

However, this is just the middle point of two points in (4.114). More specifically, by choosing $p = 1$ in (4.114), we have $\mathbf{d}'_1 = (\frac{K-2}{K-1}, \frac{1}{K-1}, 0, 0, \ldots, 0)$ and $\mathbf{d}''_1 = (\frac{1}{K-1}, \frac{K-2}{K-1}, 0, 0, \ldots, 0)$ (by swapping the first two elements in $\mathbf{d}'_1$). Here $\mathbf{d}'_1 \neq \mathbf{d}''_1$ due to $K \geq 5$, and also it is easy to check that $\mathbf{d}_1 = \frac{1}{2}(\mathbf{d}'_1 + \mathbf{d}''_1)$, which means that $\mathbf{d}_1$ is not an extreme point.

Now, we start the proof of Theorem 4.8. In order to speak of a polytope, we re-write (4.16) as

$$-d_i \leq 0, \qquad i = 1, \ldots, K \tag{4.192}$$

Then, we can write all the left hand sides of (4.14), (4.15), (4.192) as an $N \times K$ matrix $\mathbf{H}$ with corresponding right hand sides forming an N-length column vector $\mathbf{h}$, i.e., all points $\mathbf{d}$ in D satisfy

$$\mathbf{Hd} \leq \mathbf{h} \tag{4.193}$$

where $N \triangleq 2K + \binom{K}{2} = 2K + \frac{K(K-1)}{2}$. For any extreme point $\mathbf{d} \in D$, let $J(\mathbf{d})$ be a set such that

$$J(\mathbf{d}) = \left\{ l : \mathbf{H}_l \mathbf{d} = \mathbf{h}_l, \quad l \in \{1, \ldots, N\} \right\} \tag{4.194}$$

where $\mathbf{H}_l$ is the lth row of $\mathbf{H}$ and $\mathbf{h}_l$ is the lth element of $\mathbf{h}$. Therefore, $J(\mathbf{d})$ represents all active boundaries. The remaining rows satisfy

$$\mathbf{H}_l \mathbf{d} < \mathbf{h}_l \tag{4.195}$$

for $l \notin J$.

For convenience, denote by $\mathbf{H}_J$ the sub-matrix of $\mathbf{H}$ with rows indexed by $J \triangleq J(\mathbf{d})$. Similarly denote by $\mathbf{h}_J$ the sub-vector of $\mathbf{h}$ with rows indexed by J. In order to find all extreme points in D, by Theorem 4.5 in Section 4.3.1, we need to find all $K \times (K+1)$ sub-matrices $(\mathbf{H}', \mathbf{h}')$ of $(\mathbf{H}, \mathbf{h})$ with $\text{rank}(\mathbf{H}') = K$ such that $\mathbf{H}\mathbf{d} \leq \mathbf{h}$ and $\mathbf{H}'\mathbf{d} = \mathbf{h}'$, which is also equivalent to finding all index sets J representing the active boundaries such that $\mathbf{H}\mathbf{d} \leq \mathbf{h}$, $\mathbf{H}_J\mathbf{d} = \mathbf{h}_J$, and $\text{rank}(\mathbf{H}_J) = K$.

For convenience of presentation, we always partition the set J as a union of mutually exclusive sets S, P and Z, i.e.,

$$J = S \cup P \cup Z \tag{4.196}$$

We denote by S the row indices representing the active boundaries in (4.14)

$$S \triangleq \left\{ s_i \triangleq s(i) : \mathbf{H}_{s_i}\mathbf{d} = h_{s_i} \text{ is } (K-1)d_i + \sum_{j=1}^{K} d_j = K-1, \quad i = 1, \ldots, K \right\} \tag{4.197}$$

where s_i stands for the function $s(i)$ of the coordinate i with the value as the row index of $\mathbf{H}$ corresponding to the active boundaries $(K-1)d_i + \sum_{j=1}^{K} d_j = K-1$. Thus, we have a one-to-one mapping between the row index and the function $s_i \triangleq s(i)$, i.e., if the row index $s_i \in J$, we know exactly the ith upper bound in (4.14) is active; on the other hand, if we know the coordinate i, we can determine the unique corresponding row index in $\mathbf{H}$ by the mapping $s : i \mapsto s_i$.

Similarly, we denote by P the row indices representing the active boundaries in (4.15)

$$P \triangleq \left\{ p_V \triangleq p(V) : \mathbf{H}_{p_V}\mathbf{d} = h_{p_V} \text{ is } \sum_{i \in V} d_i = 1, \quad V \subseteq \{1, \ldots, K\}, |V| = 2 \right\} \tag{4.198}$$

where the value of p_V is the corresponding row index of $\mathbf{H}$.

Finally, denote by Z the row indices representing the active boundaries in (4.192)

$$Z \triangleq \left\{ z_i \triangleq z(i) : \mathbf{H}_{z_i}\mathbf{d} = h_{z_i} \text{ is } d_i = 0, \quad i = 1, \ldots, K \right\} \tag{4.199}$$

where the value of z_i is the corresponding row index of $\mathbf{H}$.

There are approximately in total

$$\binom{N}{K} \approx \frac{\left(\frac{K+2}{2}\right)^K e^K}{\sqrt{2\pi K}} \tag{4.200}$$

possible selections of K equations in (4.193) for large K. In order for this search to have a reasonable complexity, we need to investigate the structure of D more carefully. We identify the following simple properties for the extreme points in the following lemmas.

Lemma 4.1 *Let* $\mathbf{d}$ *be a non-zero extreme point in* D*. Then, it must satisfy the following properties:*

1) $\max_k d_k \leq \frac{K-1}{K}$.

2) At most one element, if there is any, in $\mathbf{d}$ *is strictly larger than* $\frac{1}{2}$.

3) If there exists an element, say d_i*, which is equal to* $\frac{1}{2}$*, then,* $d_j \leq d_i = \frac{1}{2}$ *for all* j.

4) If $|S| \geq 2$ *and* $\forall s_i, s_j \in S$*, where* $i \neq j$*, then* $0 < d_i = d_j \leq \frac{1}{2}$.

5) If $s_i \in S$*, then* $d_j \leq d_i$ *for all* j*. Or, equivalently, if* $|S| \geq 1$ *and* $s_i \in S$*, then* $d_i = \max_{j=1,\ldots,K} d_j$*. Or, equivalently, if* $|S| \geq 1$ *and* $d_i = \max_{j=1,\ldots,K} d_j$*, then* $s_i \in S$.

6) If $\max_i d_i > \frac{1}{2}$*, then* $|S| \leq 1$.

The proof of Lemma 4.1 is provided in Appendix 4.7.2. In addition to the properties of the elements of the extreme points, we also need some results regarding the rank of the sub-matrices. It is easy to verify that a trivial necessary condition for $\text{rank}(\mathbf{H}_J) = K$ is $|S| + |P| + |Z| \geq K$. More formally, we have the following lemma.

Lemma 4.2 *For an extreme point* $\mathbf{d}$*,* $rank(\mathbf{H}_J) = K$ *only if*

$$rank(\mathbf{H}_{S\cup P}) + |Z| \geq K \tag{4.201}$$

Lemma 4.3 *Let* $\mathbf{d}$ *be a non-zero extreme point of* D*. If* $|P| \geq 1$ *and* $\max_k d_k > \frac{1}{2}$*, then there exists a coordinate* i_* *such that*

$$\frac{K-1}{K} \geq d_{i_*} = \max_k d_k > \frac{1}{2} \tag{4.202}$$

and a non-empty set

$$U' \triangleq \Big\{ j : d_j = 1 - d_{i_*} > 0 \Big\} \tag{4.203}$$

with cardinality $m' \triangleq |U'| = |P|$ *and*

$$P = P' \triangleq \Big\{ p_V : V = \{i_*, j\}, j \in U' \Big\} \tag{4.204}$$

In addition, S *is either empty or*

$$S = \{s_{i_*}\} \tag{4.205}$$

Futhermore,

$$rank(\mathbf{H}_{S\cup P}) = |P| + \mathbb{1}_{\{|S|\geq 1\}} \tag{4.206}$$

where $\mathbb{1}_{\{\cdot\}}$ *is the indicator function.*

Lemma 4.4 *Let* $\mathbf{d}$ *be a non-zero extreme point of* D*. If* $|P| \geq 1$ *and* $\max_k d_k \leq \frac{1}{2}$*,*

then there exists a non-empty set

$$U'' = \left\{ i : d_i = \frac{1}{2} \right\} \tag{4.207}$$

with cardinality $m'' \stackrel{\triangle}{=} |U''| \geq 2$*, and*

$$P = P'' \stackrel{\triangle}{=} \left\{ p_V : V = \{k, j\},\ k \neq j,\ \textit{and}\ k, j \in U'' \right\} \tag{4.208}$$

with rank

$$\textit{rank}(\mathbf{H}_P) = \begin{cases} m'', & |P| > 1 \\ 1, & |P| = 1 \end{cases} \tag{4.209}$$

In addition, S *is either empty or*

$$S = \left\{ s_i : i \in U'' \right\} \tag{4.210}$$

Futhermore,

$$\textit{rank}(\mathbf{H}_{S \cup P}) = \begin{cases} 1, & |P| = 1\ \&\ |S| = 0 \\ m'' + \mathbb{1}_{\{|S| \geq 1\}}, & \textit{otherwise} \end{cases} \tag{4.211}$$

The proofs of Lemmas 4.2, 4.3, and 4.4 are provided in Appendix 4.7.2.

Now, we are ready to prove Theorem 4.8.

Case: $|Z| = K$. Clearly, $\text{rank}(\mathbf{H}_Z) = K$ and only the zero vector satisfies

$$\mathbf{H0} \leq \mathbf{h} \tag{4.212}$$

$$\mathbf{H}_Z\mathbf{0} = \mathbf{h}_Z \tag{4.213}$$

Thus, $\mathbf{0}$ is an extreme point of D, which is (4.113). Therefore, in the remaining discussion we focus on non-zero points and $|Z| < K$.

Case: $|P| = 0$. Since $|Z| < K$, by Lemma 4.2, $|S| \geq 1$.

If $|S| = 1$, then again by Lemma 4.2, $|Z| = K - 1$. By property 5) of Lemma 4.1, $S = \{s_i\}$ for some i and $Z = \{z_j : j \neq i\}$. The extreme point $\mathbf{d}$ has the structure (4.114) with $p = 0$.

If $|S| = K$, then by property 4) of Lemma 4.1, $Z = \phi$, and the corresponding extreme point is (4.116).

If $2 \leq |S| < K$, due the positiveness implied by property 4) of Lemma 4.1 and the cardinality constraint by Lemma 4.2, the only consistent Z, which gives a solution for $\mathbf{H}_J\mathbf{d} = \mathbf{h}_J$, is

$$Z = \Big\{z_j : s_j \notin S\Big\} \tag{4.214}$$

Denote by x any d_i for $s_i \in S$. Then, we have

$$Kx + (|S| - 1)x = K - 1 \tag{4.215}$$

which implies that

$$x = \frac{K-1}{K-1+|S|} \tag{4.216}$$

Since P is empty, x must satisfy $x < \frac{1}{2}$ due to $|S| \geq 2$ and property 4) of Lemma 4.1. Substituting (4.216) into $x < \frac{1}{2}$ gives $|S| > K-1$, which contradicts the assumption $|S| < K$. Therefore, the solution given by $\mathbf{H}_J\mathbf{d} = \mathbf{h}_J$, where $J = S \cup Z$, violates (4.195).

Case: $|P| \geq 1$ **and** $\max_k d_k > \frac{1}{2}$. First of all, due to the positiveness implied by (4.202) and (4.203), the consistent set Z must satisfy

$$Z \subseteq \left\{ z_k : k \notin \{i_*\} \cup U' \right\} \tag{4.217}$$

which implies $|Z| \leq K - |U'| - 1 = K - |P| - 1$.

If S is empty, by Lemma 4.3, $\text{rank}(\mathbf{H}_{S\cup P}) = |P|$, which implies

$$\text{rank}(\mathbf{H}_{S\cup P}) + |Z| < K \tag{4.218}$$

which implies that $\text{rank}(\mathbf{H}_J) < K$, which does not give any extreme point, by Lemma 4.2.

Therefore, S is non-empty and determined by (4.205). In addition, Lemma 4.3 gives

$$\text{rank}(\mathbf{H}_{S\cup P}) = |P| + 1 \tag{4.219}$$

If $|P| = K - 1$, due to (4.203) and (4.205), we have the equality in (4.14) hold for i_*, i.e.,

$$Kd_{i_*} + (K-1)(1-d_{i_*}) = K - 1 \tag{4.220}$$

which leads to $d_{i_*} = 0$ contradicting (4.202).

Therefore, $|P| < K - 1$. Then, the consistent set Z satisfying Lemma 4.2 is

$$Z = \left\{ z_k : k \notin \{i_*\} \cup U' \right\} \tag{4.221}$$

In addition, due to (4.203) and (4.205), we have the equality in (4.14) hold for i_*, i.e.,

$$Kd_{i_*} + |P|(1-d_{i_*}) = K - 1 \tag{4.222}$$

which implies that

$$d_{i_*} = \frac{K - 1 - |P|}{K - |P|} \tag{4.223}$$

Since $d_{i_*} = \max_k d_k > \frac{1}{2}$, we have

$$|P| < K - 2 \tag{4.224}$$

The solution of this choice is exactly (4.114) with $1 \leq p < K-2$, and it satisfies (4.193).

Case: $|P| \geq 1$ **and** $\max_k d_k \leq \frac{1}{2}$. If S is empty, then by Lemma 4.4,

$$\text{rank}(\mathbf{H}_{S\cup P}) = \begin{cases} m'', & |P| > 1 \\ 1, & |P| = 1 \end{cases} \tag{4.225}$$

where m'' is the cardinality of the U'' defined in (4.207). Since $m'' \geq 2$, for both cases, $\text{rank}(\mathbf{H}_{S\cup P}) \leq m''$. Due to the positiveness of the element in U'', $|Z| \leq K - m''$. Therefore, by Lemma 4.2, the cardinality of Z can only take the value $|Z| = K - m''$, i.e.,

$$d_j = 0, \qquad \forall j \notin U'' \tag{4.226}$$

Also, Lemma 4.2 implies that $|P| > 1$ and $m'' > 2$; otherwise, $\text{rank}(\mathbf{H}_{S\cup P}) + |Z| = 1 + |Z| \leq 1 + K - m'' \leq K - 1 < K$.

Therefore, the elements in $\mathbf{d}$ are either $\frac{1}{2}$ or 0, and the number of $\frac{1}{2}$s is m''. Note that S is empty. Therefore, for any $i \in U''$, we must have the equality in (4.14) not hold, i.e.,

$$\frac{K}{2} + (m'' - 1)\frac{1}{2} < K - 1 \tag{4.227}$$

which indicates that

$$m'' < K - 1 \tag{4.228}$$

Combining with the condition $m'' > 2$ gives an extreme point that has the structure (4.115).

It remains to discuss the case where S is non-empty. By Lemma 4.4, S is determined by (4.210) and

$$\text{rank}(\mathbf{H}_{S\cup P}) = m'' + 1 \tag{4.229}$$

If $m'' = K - 1$, then the only solution is given by choosing $Z = \{z_j : j \notin U''\}$ with $|Z| = 1$, which is the structure in (4.114) with $p = K - 2$.

If $m'' < K - 1$, then $\text{rank}(\mathbf{H}_{S\cup P}) < K$. By Lemma 4.2 and the positiveness implied by U'' with cardinality m'', Z must satisfy

$$K - m'' \geq |Z| \geq K - \text{rank}(\mathbf{H}_{S\cup P}) = K - m'' - 1 > 0 \tag{4.230}$$

i.e., Z is not empty and the extreme point $\mathbf{d}$ has either $K - m'' - 1$ or $K - m''$ zero(s). On the other hand, $\mathbf{d}$ also has in total m'' $\frac{1}{2}$s due to the definition of U'' in (4.207). If $|Z| = K - m''$, then the extreme point $\mathbf{d}$ has the following form

$$d_i = \begin{cases} \frac{1}{2}, & i \in U'' \\ 0, & i \notin U'' \end{cases} \tag{4.231}$$

and we must have the equality in (4.14) hold for some $i \in U''$, i.e.,

$$\frac{K}{2} + (m'' - 1)\frac{1}{2} = K - 1 \tag{4.232}$$

which is not valid since $m'' < K-1$. Therefore, the equations corresponding to the selection of J are inconsistent. On the other hand, if $|Z| = K - m'' - 1$, then the extreme point $\mathbf{d}$ has the following form

$$d_i = \begin{cases} \frac{1}{2}, & i \in U'' \\ 0, & z_i \in Z \\ x, & otherwise \end{cases} \tag{4.233}$$

where $0 < x < \frac{1}{2}$. Again, we must have the equality in (4.14) hold for some $i \in U''$, i.e.,

$$\frac{K}{2} + (m'' - 1)\frac{1}{2} + x = K - 1 \tag{4.234}$$

which implies that

$$x = \frac{K - 1 - m''}{2} \tag{4.235}$$

Substituting this formula into $0 < x < \frac{1}{2}$ leads to

$$K - 2 < m'' < K - 1 \tag{4.236}$$

which is not possible since m'' is an integer, which completes the proof of Theorem 4.8.

4.7.2 Proofs of Lemma 4.1 through 4.4

4.7.2.1 Proof of Lemma 4.1

We prove all the properties one by one.

1) The constraint (4.14) and the positiveness constraint in (4.16) imply that for any coordinate i, we have

$$Kd_i \leq Kd_i + \sum_{j \neq i} d_j = K - 1 \tag{4.237}$$

i.e., $d_i \leq \frac{K-1}{K}$ for any i. Therefore, $\max_k d_k \leq \frac{K-1}{K}$.

2) We prove by contradiction. Assume that we have distinct coordinates, i, j, such that $d_i, d_j > \frac{1}{2}$ in $\mathbf{d}$. Then, the set $V \stackrel{\triangle}{=} \{i, j\}$ with $|V| = 2$ violates the constraint in (4.15). Therefore, this contraction implies that at most one element, if any, in $\mathbf{d}$ is strictly larger than $\frac{1}{2}$.

3) Similarly, assume that there exists a j such that $d_j > \frac{1}{2}$. Since $d_i = \frac{1}{2}$ by assumption, $d_i + d_j > 1$, which violates constraint (4.15). This implies that $d_j \leq d_i = \frac{1}{2}$ for all j.

4) Let $i, j \in S$ and $i \neq j$. Due to the definition of S, $s_i, s_j \in S$, i.e., from (4.197)

$$Kd_i + d_j + \sum_{k=1, k \neq i,j}^{K} d_k = K - 1 \tag{4.238}$$

$$Kd_j + d_i + \sum_{k=1, k \neq i,j}^{K} d_k = K - 1 \tag{4.239}$$

which implies $(K-1)d_i = (K-1)d_j$. Since $K - 1 > 0$, $d_i = d_j$. Furthermore, due to

property 2), both are no larger than $\frac{1}{2}$, and due to property 3), for any k, $d_k \leq d_i$. If $d_i = 0$, then the point $\mathbf{d}$ is the zero vector, which contradicts the assumption that $\mathbf{d}$ is a non-zero extreme point in D. Therefore, $d_i = d_j > 0$.

5) The three equivalent statements in this property are simply from three different perspectives addressing the same fact that the coordinates of $\mathbf{d}$, which are associated with the elements in S, are the most significant coordinates. We will prove the first statement and then prove the equivalence of them.

We prove the first statement of property 5) by contraction. Assume that there exists a j such that $d_j > d_i$. Then, consider the following expression (for $K \geq 3$)

$$Kd_j + d_i + \sum_{k=1,k\neq i,j}^{K} d_k = d_j + d_i + (K-1)d_j + \sum_{k=1,k\neq i,j}^{K} d_k \tag{4.240}$$

$$> d_j + d_i + (K-1)d_i + \sum_{k=1,k\neq i,j}^{K} d_k \tag{4.241}$$

$$= Kd_i + \sum_{k=1,k\neq i}^{K} d_k \tag{4.242}$$

$$= K - 1 \tag{4.243}$$

where the last equality is due to the assumption $s_i \in S$. This result violates the constraint (4.14). Therefore, for all j, $d_j \leq d_i$.

Next, we prove the second statement of property 5) using the first statement. This is trivially true because the assumption $|S| \geq 1$ and $s_i \in S$ implies that, by the first statement, $d_i \geq d_j$ for all j, i.e., $d_i = \max_j d_j$.

Then, we prove the third statement of property 5) using the second statement. By assumption, let $d_i = \max_k d_k$. However, assume that $s_i \notin S$. This implies that

there exists another coordinate j, $j \neq i$ such that $s_j \in S$ (since $|S| \geq 1$) and thereby by the second statement $d_j = \max_k d_k = d_i$. Then, consider

$$Kd_i + d_j + \sum_{k=1,k\neq i,j}^{K} d_k = Kd_j + d_i + \sum_{k=1,k\neq i,j}^{K} d_k = K - 1 \tag{4.244}$$

where the last equality is due to $s_j \in S$. This implies that s_i must belong to S by definition in (4.197), i.e., $s_i \in S$, which contradicts the assumption that $s_i \notin S$.

Finally, we prove the first statement of property 5) using the third statement. We prove this by contradiction as well. As stated in the condition of the first statement, $s_i \in S$, this means $|S| \geq 1$. Assume that there exists at least one element which is strictly larger than d_i. Pick the largest one among them and denote it by d_j. Clearly, $j \neq i$ and $d_j = \max_k d_k > d_i$. By the third statement, $s_j \in S$. Then, $|S| \geq 2$ and by property 4) $d_i = d_j$, which contradicts the assumption $d_j > d_i$.

6) We prove $|S| \leq 1$ by contraction. Assume that $|S| \geq 2$. Due to property 4) and the second statement of property 5), we have two distinct $j, k \in S$ such that $\frac{1}{2} \geq d_j = d_k = \max_i d_i > \frac{1}{2}$, which leads to a contradiction. Thus, $|S| \leq 1$.

4.7.2.2 Proof of Lemma 4.2

It is straightforward that

$$\text{rank}(\mathbf{H}_Z) = |Z| \tag{4.245}$$

since there are in total $|Z|$ 1s in the sub-matrix $\mathbf{H}_Z$ and the row index and column index of any two 1s are different. Since $(S \cup P) \cap Z = \phi$, we have

$$K = \text{rank}(\mathbf{H}_J) = \text{rank}(\mathbf{H}_{S \cup P \cup Z}) \leq \text{rank}(\mathbf{H}_{S \cup P}) + \text{rank}(\mathbf{H}_Z) \tag{4.246}$$

4.7.2.3 Proof of Lemma 4.3

If $|P| = 1$, then $P = \{p_V\}$ for a unique $V = \{i, j\}$ with $|V| = 2$. If $d_i = d_j$, then $d_i = d_j = \frac{1}{2}$ and $\max_k d_k \leq \frac{1}{2}$ due to property 3) of Lemma 4.1, which contradicts the condition $\max_k d_k > \frac{1}{2}$. Therefore, $d_i \neq d_j$. Without loss of generality, let $d_i > d_j$, then $d_i > \frac{1}{2}$ and i is the i_* required in Lemma 4.3 due to property 2) of Lemma 4.1. By property 1) of Lemma 4.1, $d_j = 1 - d_{i_*} > 0$, thus $j \in U'$. If there exists any k, $k \neq j$, such that $d_k = 1 - d_{i_*}$, then clearly $V' \stackrel{\triangle}{=} \{i_*, k\} \neq V$, but $p_{V'} \in P$, which contradicts the condition $|P| = 1$. Hence, $U' = \{j\}$ and P satisfies (4.204).

If $|P| \geq 2$, assume that $V_1 = \{i, j\}$, $V_2 = \{x, y\}$, $V_1 \neq V_2$, and $p_{V_1}, p_{V_2} \in P$. Without loss of generality, let $d_i = \max_{k \in \{i,j,x,y\}} d_k$. If $d_i < \frac{1}{2}$, then $d_j + d_i < 1$, which contradicts $p_{V_1} \in P$. If $d_i = \frac{1}{2}$, then due to property 3) of Lemma 4.1, $\max_k d_k \leq \frac{1}{2}$, which contradicts the condition $\max_k d_k > \frac{1}{2}$. Therefore, $d_i = \max_{k \in \{i,j,x,y\}} d_k > \frac{1}{2}$ and i is the i_* required in Lemma 4.3. For any $p_V \in P$, let $V = \{a, b\}$ and assume $d_a \geq d_b$. If $d_a = \frac{1}{2}$, this leads to a contradiction of $d_{i_*} > \frac{1}{2}$ due to property 3) of Lemma 4.1. Thus, $d_a > \frac{1}{2}$. Due to property 2) of Lemma 4.1, the coordinate a must be i_*, i.e., $a = i_*$. Then, $d_b = 1 - d_{i_*} > 0$ and that is true for any p_V. Hence,

$|P| = |U'|$ and (4.204) are trivially true.

If S is empty, we have a sub-matrix which has the form (by removing all columns containing all zeros and rearranging the columns)

$$\mathbf{H}_{S\cup P} = \mathbf{H}_P \doteq \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 1 \end{bmatrix} \tag{4.247}$$

where the number of rows is $|P| = |U'|$, the number of columns is $|P| + 1$, and the index of the first column corresponds to i_* and the indices of other columns correspond to U' defined in (4.203). Therefore, $\text{rank}(\mathbf{H}_{S\cup P}) = |P|$ and we are done.

If S is not empty, due to (4.202) and property 6) of Lemma 4.1, $|S| = 1$. Furthermore, due to property 5) of Lemma 4.1, $s_{i_*} \in S$, which is (4.205). Note that $\mathbf{H}_S$ is a K-length row vector containing no zeros. If $|P|+1 < K$, then $\mathbf{H}_S$ has more columns than the sub-matrix on the right hand side of (4.247). $\mathbf{H}_{S\cup P} = |P| + 1$ is true. If $|P| + 1 = K$, then

$$\mathbf{H}_{P\cup S} = \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 1 \\ K & 1 & 1 & 1 & \dots & 1 \end{bmatrix} \stackrel{\triangle}{=} M(K) \tag{4.248}$$

where $M(n)$ is $n \times n$ square matrix as in (4.248), where $n \geq 2$. Therefore, $\mathbf{H}_{P \cup S} = M(K)$. If we denote $f(n) \stackrel{\triangle}{=} \det[M(n)]$, then it is easy to write the recursive formula as

$$f(n) = (-1)^n - f(n-1), \qquad K \geq 3 \tag{4.249}$$

$$f(2) = 1 - K \tag{4.250}$$

which gives that $f(n) = (-1)^n(n-K-1)$, i.e., $\det \mathbf{H}_{P \cup S} = \det M(K) = (-1)^{K+1} \neq 0$ and $\text{rank}(\mathbf{H}_{P \cup S}) = |P| + 1 = K$, which completes the proof.

4.7.2.4 Proof of Lemma 4.4

If $\max_k d_K < \frac{1}{2}$, then $|P| = 0$, which contradicts the assumption $|P| \geq 1$. Therefore, $\max_k d_K = \frac{1}{2}$, which implies $|U''| \geq 1$. Assume that $i_* \in U''$. Due to property 3) of Lemma 4.1, $d_j \leq d_{i_*} = \frac{1}{2}$ for all j. If $\max_{k \neq i_*} d_k < \frac{1}{2}$, then we cannot find a set V such that $|V| = 2$ and $\sum_{k \in V} d_k = 1$, i.e., $|P| = 0$, which contradicts the assumption $|P| \geq 1$. Thus, $|U''| \geq 2$. Then, P'' defined in (4.208) satisfies $P'' \subseteq P$. On the other hand, for any coordinate pair (k', j') such that $k' \neq j'$ and $p_{\{k',j'\}} \in P$, since $d_{k'}, d_{j'} \leq \frac{1}{2}$, we must have $d_{k'} = d_{j'} = \frac{1}{2}$, and by definition of U'', $k', j' \in U''$, which implies $p_{\{k',j'\}} \in P''$. Therefore, $P = P''$.

If S is empty, then $\mathbf{H}_P = 1$ if $|P| = 1$ and we are. If S is empty but $|P| > 1$, the index set of the columns of $\mathbf{H}_P$, which contains nonzero elements, is U'' due to (4.208). Therefore, $\text{rank}(\mathbf{H}_P) \leq |U''| = m''$. In order to study the rank, we remove

the columns containing all zeros and rearrange the columns. Assume that

$$U'' = \left\{ i_1, i_2, \ldots, i_{m''} \right\} \tag{4.251}$$

where $i_1 = i_*$. Then, consider a $m'' \times m''$ sub-matrix of $\mathbf{H}_P$

$$\mathbf{H}_{J''} \doteq \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & 0 & \ldots & 1 \\ 0 & 1 & 1 & 0 & 0 & \ldots & 0 \end{bmatrix} \tag{4.252}$$

where

$$J'' \stackrel{\triangle}{=} \{p_V : V = \{i_*, i_j\}, j = 2, 3, \ldots, m''\} \cup \{p_{\{i_2, i_3\}}\} \subseteq P \tag{4.253}$$

It is easy to verify that $\det \mathbf{H}_{J''} = (-1)^{m''} \times 2 \neq 0$, therefore $\text{rank}(\mathbf{H}_{J''}) = m''$, i.e., $\text{rank}(\mathbf{H}_P) = m''$. This completes the proof of the case where S is empty.

Assume that $|S| \geq 1$, by property 5) of Lemma 4.1, S must have the form of (4.210). If $|P| = 1$, $m'' = |U''| = 2$. Then, the $3 \times K$ matrix $\mathbf{H}_{P \cup S}$ must have the

structure

$$\mathbf{H}_{P\cup S}=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & \dots & 0 \\ K & 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & K & 1 & 1 & 1 & \dots & 1 \end{bmatrix} \tag{4.254}$$

where the indices of the first two columns belong to U''. Clearly, $\mathbf{H}_{P\cup S} = 3 = m''+1$ since $m'' = 2$.

If $|P| > 1$, by using the J'' in (4.253), we have

$$\mathbf{H}_{J''\cup S} = \left[\begin{array}{cccccc|cccc} 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \hline K & 1 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ 1 & K & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \dots & K & 1 & 1 & \dots & 1 \end{array}\right] \tag{4.255}$$

Due to [83, Section 2.2, Problem 7],

$$\operatorname{rank}(\mathbf{H}_{P\cup S}) = \operatorname{rank}(\mathbf{H}_{J''\cup S}) = \operatorname{rank}(\mathbf{H}_{J''}) + 1 = m'' + 1 \tag{4.256}$$

which completes the proof.

Chapter 5

Sum Secure Degrees of Freedom of Two-Unicast Layered Wireless Networks

5.1 Introduction

In this chapter, we examine a class of multiple-hop wireless networks, which have two source nodes, two destination nodes, and a layered network between them. Therefore, we extend the one-hop results in Chapter 2 to the case of multi-hop networks. We determine the sum s.d.o.f. of two-unicast layered wireless networks. Without any secrecy constraints, the sum d.o.f. of this class of networks was studied by [64] and shown to take only one of three possible values: $1, \frac{3}{2}$ and 2, for all network configurations. We consider the setting where, in addition to being reliably transmitted, each message is required to be kept information-theoretically secure from the unintended receiver. We show that the sum s.d.o.f. can only take one of five possible values: $0, \frac{2}{3}, 1, \frac{3}{2}, 2$, for all network configurations. To determine the sum s.d.o.f., we divide the class of two-unicast layered networks into several sub-classes, and propose an achievable scheme based on the specific structure of the networks in each sub-class. Our achievable schemes are based on real interference alignment, cooperative jamming, interference neutralization and cooperative jamming neutralization techniques.

5.2 Definitions and Notations

Let V be the node set and $E \subset V \times V$ be the edge set. A two-unicast layered network $N = (G, L_2)$ is a directed graph $G = (V, E)$ with two source-destination pairs $L_2 = \{(s_1, d_1), (s_2, d_2)\} \subset V \times V$. The network has a layered structure which means that the node set V can be partitioned into r mutually disjoint subsets $V_1, V_2, \cdots, V_r$, denoting the nodes in each layer, such that $V_1 = \{s_1, s_2\}, V_r = \{d_1, d_2\}$ and

$$E \subset \bigcup_{i=1}^{r-1} V_i \times V_{i+1} \tag{5.1}$$

Since each node only belongs to one layer and each layer has an index, we define the index function $l(v)$ as the index of the layer containing the node v, i.e., $v \in V_{l(v)}$. Next, we give several definitions on graphs.

Definition 5.1 (Path) *A path P_{v_1,v_k} is an ordered set of nodes $\{v_1, v_2, \cdots, v_k\}$ provided that $(v_i, v_{i+1}) \in E$ for $i = 1, 2, \cdots, k-1$. Further, we denote $u \rightsquigarrow v$ if there exists at least one path $P_{u,v}$ from u to v.*

Two paths are disjoint provided that the two sets of nodes are disjoint. To avoid the trivial cases, we always assume that $s_1 \rightsquigarrow d_1$ and $s_2 \rightsquigarrow d_2$. In contrast to the assumption in [64], we cannot remove nodes v which do not belong to any path, since we may employ them to perform cooperative jamming.

Definition 5.2 *For a subset of nodes $S \subset V$, we denote by $G[S]$ the graph induced by S on G provided that $G[S] = (S, E_s)$ where $E_s = \{(v, u) \in E : v, u \in S\}$.*

Reference [64] defines interference and manageable interference as follows:

Definition 5.3 (Interference) *For $i = 1$ or 2, a node $v \notin P_{s_i,d_i}$ causes interference on P_{s_i,d_i} and we write $v \overset{I}{\rightsquigarrow} P_{s_i,d_i}$ if there exist a node $u \in P_{s_i,d_i}$ such that $(v,u) \in E$ and a path $P_{s_j,v}$ such that P_{s_i,d_i} and $P_{s_j,v}$ are disjoint.*

In Definition 5.3 and in the sequel, we use the notation $j = \bar{i}$ to denote the index of the other transmitter-receiver pair, i.e., $i = 1, j = 2$ or $i = 2, j = 1$. In order to characterize the interference from another pair, the number of nodes causing interference is defined as follows:

$$n_i(G[S], P_{s_i,d_i}) \overset{\triangle}{=} n_i(G[S]) \overset{\triangle}{=} \Big| \{ v \in S : v \overset{I}{\rightsquigarrow} P_{s_i,d_i}, \exists P_{s_j,v} \subset S \text{ and } P_{s_i,d_i} \cap P_{s_j,v} = \phi \} \Big| \tag{5.2}$$

for some subset $S \subset V$ and $(P_{s_1,d_1} \cup P_{s_2,d_2}) \subset S$.

Definition 5.4 (Manageable interference) *Two disjoint paths P_{s_1,d_1} and P_{s_2,d_2} have* **manageable interference** *if we can find $S \subset V$, such that $(P_{s_1,d_1} \cup P_{s_2,d_2}) \subset S$, $n_1(G[S]) \neq 1$ and $n_2(G[S]) \neq 1$.*

An example two-unicast layered network is shown in Figure 1.9. This network has $r = 5$ layers and two disjoint paths $P_{s_1,d_1} = \{s_1, u_1, u_2, u_3, d_1\}$ and $P_{s_2,d_2} = \{s_2, w_1, w_2, w_3, d_2\}$. Node t_1 causes interference on P_{s_2,d_2}, since we can find $w_2 \in P_{s_2,d_2}$ such that $(t_1, w_2) \in E$ and a path $P_{s_1,t_1} = \{s_1, t_1\}$ such that P_{s_1,t_1} and P_{s_2,d_2} are disjoint. This implies that $n_2(G[V]) = 1$. It is also easy to see that $n_1(G[V]) = 1$ due to node t_2. However, if we choose $S = V \backslash \{t_1, t_2\}$, then, for the graph $G[S]$ induced by S, $n_1(G[S]) = n_2(G[S]) = 0$. By definition, P_{s_1,d_1} and P_{s_2,d_2} have manageable

interference.

Regarding the channel model, each node v observes the signals through a memoryless additive Gaussian channel, i.e.,

$$Y_v = \sum_{u:(u,v)\in E} h_{v,u} X_u + N_v \tag{5.3}$$

where N_v is an additive zero-mean unit-variance Gaussian noise and X_u is the input signal sent from node u provided that the edge (u, v) exists. All the channel gains $h_{v,u}$ in the network are fixed during the communication session and known at all nodes. Channel gains are independently drawn from continuous distributions. The input signal of each node u, X_u, satisfies an average power constraint P, i.e., $\mathrm{E}[X_u^2] \leq P$.

The source node s_1 has a message W_1 uniformly chosen from set $\mathcal{W}_1$ for destination d_1. The rate of the message is $R_1 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_1|$. The source node s_1 uses a stochastic function $f_1 : \mathcal{W}_1 \to X_{s_1}^n$ to encode the message, where n is the number of channel uses. Similarly, source node s_2 has message W_2 (independent of W_1) uniformly chosen from set $\mathcal{W}_2$ for destination d_2. The rate of the message is $R_2 \stackrel{\triangle}{=} \frac{1}{n}\log|\mathcal{W}_2|$. Source node s_2 uses a stochastic function $f_2 : \mathcal{W}_2 \to X_{s_2}^n$ to encode the message. The messages are said to be transmitted reliably and securely if only the intended destination node can decode each message, i.e., each destination node is an eavesdropper for the other. Formally, for $i = 1$ or 2, a secrecy rate R_i is said to be achievable if for any $\epsilon > 0$ there exists an n-length code such that destination node d_i can decode the message as $\hat{W}_i$ reliably based on its observation $Y_{d_i}^n$, i.e., the

probability of decoding error is less than ϵ,

$$\Pr\left[W_i \neq \hat{W}_i\right] \leq \epsilon \tag{5.4}$$

and the message is kept information-theoretically secure against the other receiver,

$$\frac{1}{n}H(W_i|Y_{d_j}^n) \geq \frac{1}{n}H(W_i) - \epsilon \tag{5.5}$$

This definition implicitly implies that the source nodes trust all the intermediate relay nodes, but the unintended destination node. The sum s.d.o.f. is defined as:

$$D_{s,\Sigma} = \lim_{P\to\infty} \sup \frac{R_1 + R_2}{\frac{1}{2}\log P} \tag{5.6}$$

where the supremum is over all achievable secrecy rate pairs (R_1, R_2). The sum d.o.f. of two-unicast layered networks was found in [64] as:

Theorem 5.1 (Sum d.o.f. of two-unicast networks [64]) *For a two-unicast layered Gaussian network $N = (G = (V, E), L_2 = \{(s_1, d_1), (s_2, d_2)\})$ where the channel gains are chosen according to independent continuous distributions, with probability 1, D_Σ is given by*

A) 1, *if N contains a node v whose removal disconnects d_i from $\{s_i, s_j\}$ and s_j from $\{d_i, d_j\}$, for $i = 1$ or 2, $j = \bar{i}$,*

A′) 1, *if N contains an edge (v_2, v_1) such that the removal of v_1 disconnects d_i from $\{s_i, s_j\}$ and the removal of v_2 disconnects s_j from $\{d_i, d_j\}$, for $i = 1$ or 2, $j = \bar{i}$,*

B) 2, *if N contains two disjoint paths P_{s_1,d_1} and P_{s_2,d_2} with manageable interference,*

B′) 2, if N or any sub-network does not contain two disjoint paths P_{s_1,d_1} and P_{s_2,d_2}, but is not in case (A),

C) 3/2, in all other cases.

By considering secrecy for the end-to-end users in addition to reliability, the main result of this chapter is the characterization of the sum s.d.o.f. of two-unicast layered networks as stated in the following theorem.

Theorem 5.2 (Sum s.d.o.f. of two-unicast networks) *For a two-unicast layered Gaussian network $N = (G = (V, E), L_2 = \{(s_1, d_1), (s_2, d_2)\})$ where the channel gains are chosen according to independent continuous distributions, with probability 1, $D_{s,\Sigma}$ can take one of the following five possible values: $0, \frac{2}{3}, 1, \frac{3}{2}, 2$.*

We will prove Theorem 5.2 in the following three sections. In particular, in Section 5.3, we will show that for two-unicast layered networks in cases A and A', the sum s.d.o.f. can take one of three values: $0, \frac{2}{3}, 1$. Next, in Section 5.4, we will show that for two-unicast layered networks in cases B and B', the sum s.d.o.f. is 2. Finally, in Section 5.5, we will show that for two-unicast layered networks in case C, the sum s.d.o.f. is $\frac{3}{2}$.

In order to prove Theorem 5.2, we characterize the penultimate layer V_{r-1}, i.e., the last layer of the network before the layer of destinations, as:

$$V_{r-1} = G_1 \cup G_2 \cup G_3 \cup G_4 \tag{5.7}$$

where G_is are mutually disjoint sets defined as follows:

$$G_1 = \{u \in V_{r-1} : (u, d_1) \in E \text{ and } (u, d_2) \in E\} \tag{5.8}$$

$$G_2 = \{u \in V_{r-1} : (u, d_1) \in E \text{ and } (u, d_2) \notin E\} \tag{5.9}$$

$$G_3 = \{u \in V_{r-1} : (u, d_1) \notin E \text{ and } (u, d_2) \in E\} \tag{5.10}$$

$$G_4 = \{u \in V_{r-1} : (u, d_1) \notin E \text{ and } (u, d_2) \notin E\} \tag{5.11}$$

That is, we group the nodes in the penultimate layer V_{r-1} into four disjoint sets: G_1 through G_4. These are the sets of nodes that may or may not be connected to the destinations: G_1 is the set of all nodes in this layer which are connected to both destinations, G_2 is the set of all nodes that are connected to the first destination (d_1) but not to the second destination (d_2), G_3 is the set of all nodes which are connected to the second destination (d_2) but not to the first destination (d_1), and G_4 is the set of nodes that are not connected to d_1 or d_2. Since the last layer V_r only contains d_1, d_2, it is safe to remove the nodes belonging to G_4 from the network. For the rest of this chapter, we assume that the cardinality of set G_4 is zero, i.e., $|G_4| = 0$.

5.3 Sum Secure d.o.f. for Cases A and A'

In this section, we consider two-unicast layered networks in cases A and A', i.e., each network N contains an edge (v_2, v_1) such that removal of v_1 disconnects d_i from $\{s_i, s_j\}$ and removal of v_2 disconnects s_j from $\{d_i, d_j\}$, for $i = 1$ or 2, $j = \bar{i}$. If

$v_1 = v_2$, then the "*edge*" downgrades to a node, and this is case A; otherwise, this is case A'.

The sum d.o.f. capacity is $D_\Sigma = 1$ for this case, which is an upper bound for the sum s.d.o.f., $D_{s,\Sigma}$. We present our results by dividing all the networks in cases A and A' into 5 sub-cases, A_1 through A_5. We implicitly mean that, for each i, the sub-case A_i does not include the setting in A_j for any $j < i$, i.e., the sub-case A_2 does not include the setting in A_1, the sub-case A_3 does not include the settings in A_1 or A_2, etc. We start with a sub-case (sub-case A_1) where there exists at least one node in G_2 or G_3, i.e., $|G_2| \geq 1$ or $|G_3| \geq 1$. In this case, cooperative jamming is sufficient to achieve 1 secure d.o.f. if there exists a helper in the set $G_2 \cup G_3$. If the union of G_2 and G_3 is empty, then all the nodes in layer V_{r-1} are connected to both destinations, i.e., $V_{r-1} = G_1$. Since the signals from any node in G_1 are received by both destination nodes, we investigate the structure of the network and the set G_1 to find the exact sum s.d.o.f. based on interference neutralization and real interference alignment in sub-cases A_2 through A_5. Our result for cases A and A' is stated in the following theorem.

Theorem 5.3 *With probability 1, the sum s.d.o.f. of layered networks in cases A and A' is*

$$D_{s,\Sigma} = \begin{cases} 0 & \text{if } |G_1| = 1 \text{ and } |G_2 \cup G_3| = 0 \\ \frac{2}{3} & (*) \\ 1 & o.w. \end{cases} \tag{5.12}$$

where the condition $(*)$ is either of the following two conditions:

1. (**C1**) $r = 2$ *and* $|G_2 \cup G_3| = 0$,

2. (**C2**) $r \geq 3, |G_1| = 2$, $|G_2 \cup G_3| = 0$, *for each* w *there exists at most one* $u_w \in G_1$ *such that* $w \rightsquigarrow u_w$, *and the layered network is not in case A.*

We can interpret Theorem 5.3 in the following way. The first condition $|G_1| = 1$ and $|G_2 \cup G_3| = 0$ means that $V_{r-1} = G_1 = \{u\}$ has only one node u which is connected to both d_1 and d_2. Both destinations receive almost the same signals at high SNR, which implies that $D_{s,\Sigma} = 0$. This case is considered in detail in Section 5.3.2. Next, condition (**C1**), i.e., $r = 2$ and $|G_2 \cup G_3| = 0$, implies that $|G_1| = 2$ due to the assumption $V_1 = \{s_1, s_2\}$. Therefore, this layered network is a fully-connected two-user Gaussian IC with confidential messages, for which the sum s.d.o.f. is $\frac{2}{3}$ due to Chapter 2. Such networks belong to case A'. Since this result follows from Chapter 2, we will not consider it further in the following sub-sections. Next, condition (**C2**) is a variant of condition (**C1**), thereby the corresponding $D_{s,\Sigma}$ is also $\frac{2}{3}$. We will show this in Section 5.3.5. For all other network configurations, $D_{s,\Sigma}$ is 1. We will give the corresponding achievable schemes in Sections 5.3.1, 5.3.3, 5.3.4, and 5.3.5.

5.3.1 Sub-case A_1: $D_{s,\Sigma} = 1$ if $|G_2| \geq 1$ or $|G_3| \geq 1$.

Without loss of generality, we prove $D_{s,\Sigma} = 1$ for the setting $|G_3| \geq 1$. The same argument can be applied to $|G_2| \geq 1$. The cardinality of set G_3 is nonzero which means that there exists at least one node $u \in G_3$. There are two possibilities. The first possibility is that we can find some node $u \in G_3$ and u belongs to the path

P_{s_2,d_2}. Since by definition the edge (u, d_1) does not exist, if the message signal of the transmitter-receiver pair 2 is going through the path P_{s_2,d_2}, by keeping other nodes in the network silent, there is no information leakage to d_1, i.e., this message (message W_2) is secure and $D_{s,\Sigma} = 1$.

If we cannot find such node u (which is the second possibility), then we can utilize node u to perform cooperative jamming. Transmitter 1 transmits a message carrying 1 d.o.f. along the existing path P_{s_1,d_1}. All nodes on this path, except the node $\tilde{s} \in V_{r-1}$, simply relay the signal. Node u, which is connected to d_2 only, sends i.i.d. Gaussian cooperative jamming signal [14, 15] with average power P, which is independent of message W_1, to ensure the secrecy of the message from transmitter-receiver pair 1. The final hop becomes a Gaussian wiretap channel with an independent helper which is only connected to the eavesdropper. Due to the fact that the signal from node u is an artificial i.i.d. Gaussian noise, the source-destination pair $(\tilde{s}, d_1)$ can achieve the (maximum) secrecy rate, which is known [4]

$$\frac{1}{2}\log\left(1 + h_{d_1,\tilde{s}}^2 P\right) - \frac{1}{2}\log\left(1 + \frac{h_{d_2,\tilde{s}}^2 P}{1 + h_{d_2,u}^2 P}\right) \tag{5.13}$$

and from (5.6) the s.d.o.f. is $D_{s,\Sigma} = 1$.

5.3.2 Sub-case A_2: $D_{s,\Sigma} = 0$ if $|G_1| = 1$.

In this section, we consider the sub-case A_2 and prove that $D_{s,\Sigma} = 0$. After ruling out the setting in sub-case A_1, the setting of layered networks in A_2 is $|G_1| = 1$ and $|G_2| = |G_3| = 0$. First, note that $|G_2| = |G_3| = 0$ implies $|G_1| \geq 1$ due to

the existence of P_{s_i,d_i} for some i. Furthermore, if $|G_1| = 1$ and $|G_2| = |G_3| = 0$, this indicates that $V_{r-1} = G_1 = \{u\}$ has only one node u which is connected to both d_1 and d_2. The last hop of the layered network in this sub-case is a Gaussian BC with confidential messages, in which the transmitter is node u, and d_1, d_2 are the two receivers. The sum s.d.o.f. is 0: due to the degradedness of the underlying Gaussian BC, one of the users (stronger) has the secrecy capacity which is the secrecy capacity of the Gaussian wiretap channel, and the other user (weaker) has zero secrecy capacity. It is well-known that the secrecy capacity of the Gaussian wiretap channel does not scale with $\log P$, therefore, for both users, the s.d.o.f. is zero, implying that the sum s.d.o.f. is zero. This concludes that $D_{s,\Sigma} = 0$ if $|G_1| = 1$ and $|G_2| = |G_3| = 0$.

5.3.3 Sub-case A_3: $D_{s,\Sigma} = 1$ if there exist two distinct nodes $u_1, u_2 \in G_1$ and a source node s such that $s \rightsquigarrow u_1$ and $s \rightsquigarrow u_2$.

In this section, we consider the sub-case A_3 in which layer V_{r-1} contains several nodes, which are connected to both destinations. In addition, by excluding the settings in A_1 and A_2, we note that the layered networks in A_3 must have $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$. Since the condition (**C1**), i.e., $r = 2$ and $|G_2 \cup G_3| = 0$, has already been discussed and excluded in the present discussion, we know that the networks with $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$ must have at least three layeres, i.e., $r \geq 3$.

We propose an achievable scheme for this sub-case based on interference neu-

tralization [65]. The source node s, say s_i, which connects to u_1 and u_2, sends the message signal carrying 1 d.o.f. to its destination. All the nodes on the two paths P_{s_i,u_1} and P_{s_i,u_2} just relay the signal. The two nodes u_1 and u_2 perform amplify-and-forward with factors α_1 and α_2, respectively. The values of α_1 and α_2 will be specified later. All other nodes, including s_j, do not send/relay signals.

To show the achievable sum s.d.o.f. for this scheme, we construct the condensed network [64] with three key layers as shown in Figure 5.1. Then, the end-to-end transfer matrix $\mathbf{T} = [T_i, T_j]^T$ from s_i to d_i, d_j satisfies

$$\begin{aligned}\begin{pmatrix} Y_{d_i} \\ Y_{d_j} \end{pmatrix} &= \mathbf{T} X_{s_i} + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_i \tilde{h}_i h_{i,i} + \alpha_j \tilde{h}_j h_{i,j} \\ \alpha_i \tilde{h}_i h_{j,i} + \alpha_j \tilde{h}_j h_{j,j} \end{pmatrix} X_{s_i} + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix} \end{aligned} \tag{5.14}$$

where $\tilde{N}_1$ and $\tilde{N}_2$ are effective dependent noises with finite variances. However, they are independent of the message signal due to the linear construction.

If we choose $\alpha_i = 1$ and $\alpha_j = -(\tilde{h}_i h_{j,i})/(\tilde{h}_j h_{j,j})$, then the signal X_{s_i} from the source node s_i is perfectly canceled at the destination node d_j due to the fact $T_j = 0$, which also makes the observation $Y_{d_j}^n$ at d_j and W_i independent, i.e., $I(W_i; Y_{d_j}^n) = 0$. This indicates that message W_i is secure. On the other hand, for reliability, the probability that d_i can decode W_i with arbitrarily small probability of decoding

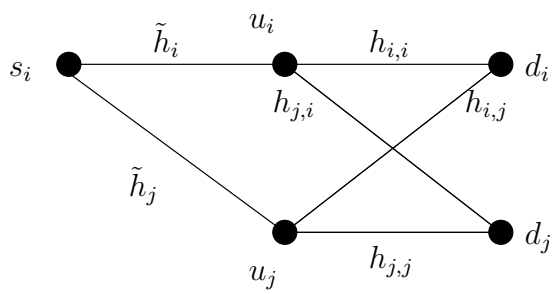


Figure 5.1: The condensed network for $s_i \rightsquigarrow u_1$ and $s_i \rightsquigarrow u_2$.

error is

$$P\left(T_i \neq 0\right) = P\left(\tilde{h}_i h_{i,i} - \tilde{h}_j h_{i,j} \frac{\tilde{h}_i h_{j,i}}{\tilde{h}_j h_{j,j}} \neq 0\right)$$
$$= P\left(h_{j,j} h_{i,i} - h_{i,j} h_{j,i} \neq 0\right) = 1 \tag{5.15}$$

which means that $D_{s,\Sigma} = 1$ with probability one.

5.3.4 Sub-case A_4: $D_{s,\Sigma} = 1$ if there exist two distinct nodes $u_1, u_2 \in G_1$ and a node w such that $w \rightsquigarrow u_1$ and $w \rightsquigarrow u_2$.

In this section, we show that, if there is a node which is connected to at least two nodes in G_1, even though it is not a source node, we still can achieve 1 sum s.d.o.f. After excluding all previous sub-cases, in addition to the definition of A_4, the layered networks in this sub-case must have the following properties: $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$, $r \geq 3$, and, for each source node s_i $(i = 1, 2)$, there exists one and only one $\tilde{u}_i \in G_1$ such that $s_i \rightsquigarrow \tilde{u}_i$.

For sub-case A_4, we propose the following achievable scheme. For any source node, say s_i, and a path $P_{s_i,u}$, where $u \in G_1$, the source node s_i sends the message

signal carrying 1 d.o.f. to node u. All the nodes on path $P_{s_i,u}$ just relay the signal. Node u encodes the message according to a secrecy capacity achieving code, which will be specified later, and sends the codeword to d_i. The special node w sends artificial i.i.d. Gaussian random noise with average power aP to jam the unintended destination d_j through the two nodes u_1 and u_2. The linear factor a is a constant to coordinate with the nodes in the network such that all the channel inputs satisfy the power constraint. The value of a depends on the network topology, but not on power P. All the nodes on two paths P_{w,u_1}, P_{w,u_2} relay the signals. Nodes u_1 and u_2 perform amplify-and-forward with factors α_1 and α_2, respectively. All other nodes, including s_j, do not send/relay signals.

The intuition behind this achievable scheme is similar to the previous sub-case. However, we carefully choose the factors α_1 and α_2 to neutralize the artificial noise at the legitimate destination d_i, and thereby utilize node w to perform cooperative jamming. After removing all unnecessary nodes, there are only two possibilities for sub-case A_4 as shown in Figure 5.2. If $u_i = \tilde{u}_i$ as shown in Figure 5.2(a), then this node u_i has to relay the message carrying signal and also the jamming signal. After scaling all signals in the network with a constant factor to satisfy the average power constraint, u_i sends a superposition of the two signals. Under this setting, we disregard the difference between the two possibilities and thereby focus on the cooperative jamming signal. In both condensed networks in Figure 5.2, if we consider the source node s_i as the transmitter, d_i as the legitimate receiver, and d_j as the eavesdropper, the networks are equivalent to Gaussian wiretap channels with dependent noises. Due to the fact that the secrecy capacity depends only on

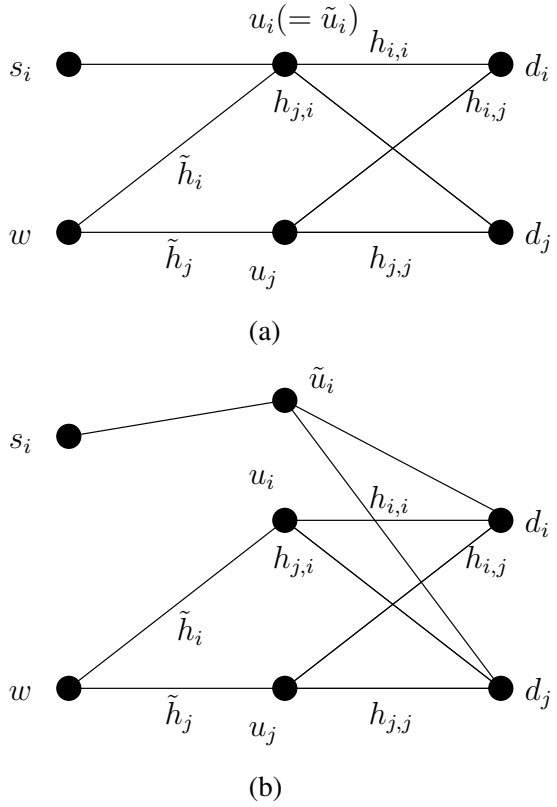


Figure 5.2: The two possible condensed networks for the sub-case A_4: $w \rightsquigarrow u_1$ and $w \rightsquigarrow u_2$.

the marginal distributions (but not on the joint), to show that 1 sum s.d.o.f. is achievable, it suffices to prove that with proper design of α_i and α_j, the jamming noise with average power aP from node w can be perfectly canceled at the legitimate receiver d_i, but not at the eavesdropper d_j.

Consider the end-to-end transfer matrix $\mathbf{T} = [T_i, T_j]^T$ from w to d_i, d_j:

$$\begin{aligned}\begin{pmatrix} Y_{d_i}^w \\ Y_{d_j}^w \end{pmatrix} &= \mathbf{T}N_w + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_i \tilde{h}_i h_{i,i} + \alpha_j \tilde{h}_j h_{i,j} \\ \alpha_i \tilde{h}_i h_{j,i} + \alpha_j \tilde{h}_j h_{j,j} \end{pmatrix} N_w + \begin{pmatrix} \tilde{N}_1 \\ \tilde{N}_2 \end{pmatrix} \end{aligned} \tag{5.16}$$

If we choose $\alpha_i = 1$ and $\alpha_j = -(\tilde{h}_i h_{i,i})/(\tilde{h}_j h_{i,j})$, then $T_i = 0$ and receiver d_i will have a clean view of the signal from s_i. Meanwhile, the probability that T_j is non-zero is

$$P\left(T_j \neq 0\right) = P\left(h_{j,j}h_{i,i} - h_{i,j}h_{j,i} \neq 0\right) = 1 \tag{5.17}$$

which concludes that $D_{s,\Sigma} = 1$ with probability one for sub-case A_4.

5.3.5 Sub-case A_5: All other settings in cases A and A'.

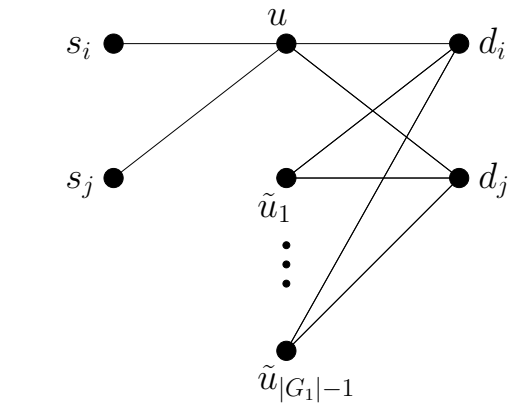
In this section, we consider the layered networks in cases A and A', which are not in any of the previous sub-cases. In this sub-case, by excluding the settings of all previous sub-cases, we know that $|G_1| \geq 2$ and $|G_2| = |G_3| = 0$, the number of layers $r \geq 3$, and there is an independence structure in layer V_{r-1}. By an independence structure, we mean that all the channel inputs from nodes belonging to $G_1 = V_{r-1}$ in the last hop must be mutually independent. This is because, for each node w in the network before V_{r-1}, there exists at most one $u_w \in G_1$ such that $w \rightsquigarrow u_w$.

Since we can precisely characterize the structure of the layered network in this sub-case, we claim that $D_{s,\Sigma} = \frac{2}{3}$ if condition (**C2**) is satisfied and is 1 otherwise. The proof is developed in three steps. The first step is to explore the structure of the network. The second step is to reduce the network to an equivalent Gaussian BC with confidential messages and $M \geq 1$ helper(s) or a two-user Gaussian IC with confidential messages and $M \geq 0$ helper(s). The final step is to use the s.d.o.f. results in Chapter 2.

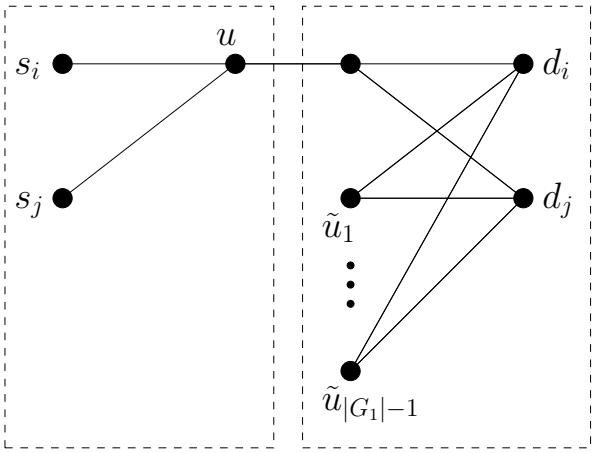
First, we show that $D_{s,\Sigma} = 1$ if the network belongs to case A. Let $s_i \rightsquigarrow u_i$

and $s_j \rightsquigarrow u_j$ for some $u_i, u_j \in V_{r-1}$. We prove $u_i = u_j$ by contradiction. Assuming $u_i \neq u_j$. Since, by the definition of case A, removal of v disconnects d_i from s_1, s_2, we must have $s_i \rightsquigarrow v$. Again, since the removal of v disconnects s_j from d_1, d_2, it must be that $s_j \rightsquigarrow v \rightsquigarrow u_j$, which implies $s_i \rightsquigarrow v \rightsquigarrow u_j$, i.e., $s_i \rightsquigarrow u_j$ and $s_i \rightsquigarrow u_i$, which is sub-case A_3. This leads to a contradiction. Denote $u \stackrel{\triangle}{=} u_i = u_j$. Then, for each other node $\tilde{u} \in G_1, \tilde{u} \neq u$, we must have $s_i \not\rightsquigarrow \tilde{u}$, $s_j \not\rightsquigarrow \tilde{u}$. The condensed network is shown in Figure 5.3(a), which is equivalent to the channel model in Figure 5.3(b). Due to the Markov chain $W_i, W_j \rightarrow Y_u^n \rightarrow Y_{d_i}^n, Y_{d_j}^n$, node u can decode messages W_i and W_j with arbitrarily small probability of error, which implies that $D_\Sigma = 1$ in the first dashed box of Figure 5.3(b). The bottleneck for the sum s.d.o.f. is the second box, which is a Gaussian BC with confidential messages and M independent helpers. Here $M = |G_1| - 1 \geq 1$. Finally, by utilizing real interference alignment based scheme in Chapter 2, we know that the sum s.d.o.f. of a Gaussian BC with confidential messages and $M \geq 1$ helper(s) is 1 with probability one. Hence, for the networks belonging to the intersection of case A_5 and case A, $D_{s,\Sigma}$ is 1 with probability one.

Second, we consider the networks in which s_i and s_j connect to different nodes in layer V_{r-1}. We show that these networks belong to case A'. We again prove this by contradiction. Let $s_i \rightsquigarrow u_i$ and $s_j \rightsquigarrow u_j$ for some $u_i, u_j \in V_{r-1}$. If $u_i = u_j \stackrel{\triangle}{=} u$, then due to the independence structure, these networks are equivalent to the network shown in Figure 5.3. Clearly, the removal of u disconnects d_1 from $\{s_1, s_2\}$ and s_2 from $\{d_1, d_2\}$. By definition, this is case A. This leads to a contradiction, and s_i and s_j connect to different nodes in layer V_{r-1}. The condensed network of this



(a)



(b)

Figure 5.3: The condensed network for the equivalent Gaussian BC of the sub-case A_5.

setting as shown in Figure 5.4 also becomes two concatenated networks, in which the sum s.d.o.f is dominated by the last hop due to the independence structure in layer V_{r-1}. The last hop is a two-user Gaussian IC with confidential messages and M independent helpers. Here $M = |G_1| - 2 \geq 0$. Finally, due to Chapter 2, we know the sum s.d.o.f. of this hop:

$$D_{s,\Sigma} = \begin{cases} \frac{2}{3} & \text{if } M = 0 \\ 1 & \text{if } M \geq 1 \end{cases} \tag{5.18}$$

where $M = 0$ corresponds to condition (**C2**) which gives a two-user Gaussian IC with confidential messages, and $M \geq 1$ corresponds to the same channel model with $M \geq 1$ independent helpers.

5.4 Sum Secure d.o.f. for Cases B and B'

In this section, we consider the layered networks in cases B and B'. As proven in [64], for all network configurations belonging to cases B and B', two achievable schemes are sufficient to achieve 2 sum d.o.f., where we either use a simple amplify-and-forward scheme to make the end-to-end transfer matrix diagonal with non-zero diagonal entries, i.e.,

$$\begin{bmatrix} Y_{d_1} \\ Y_{d_2} \end{bmatrix} = \begin{bmatrix} \beta_1 & 0 \\ 0 & \beta_2 \end{bmatrix} \begin{bmatrix} X_{s_1} \\ X_{s_2} \end{bmatrix} + \begin{bmatrix} N_1^{eff} \\ N_2^{eff} \end{bmatrix} \tag{5.19}$$

or find a $2\times2\times2$ condensed interference sub-network in the original layered network. In this section, we will show that the sum s.d.o.f is the same as the sum d.o.f., i.e., $D_{s,\Sigma} = 2$.

For the diagonal end-to-end transfer matrix, the operations of the nodes in the middle layers are either to perform amplify-and-forward or be silent, therefore, the effective noises are independent of the input signals. Moreover, due to the fact that the end-to-end transfer matrix is diagonal, for each $i = 1$ or 2, we have $I(W_i; Y_{d_j}^n) = 0$, i.e., there is no information leakage from the source node to the unintended destination node even when the effective noises at the destination nodes

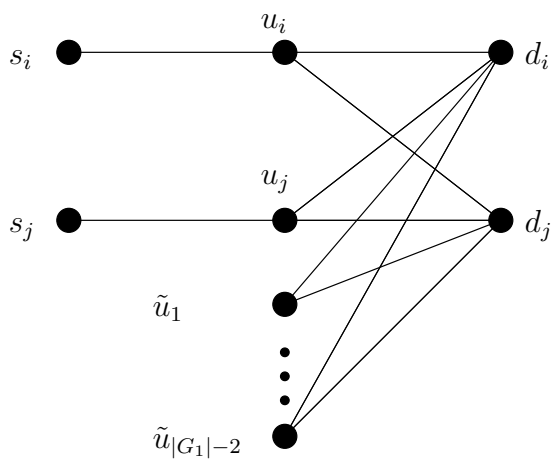


Figure 5.4: The condensed network for the equivalent Gaussian IC of the sub-case A_5.

are dependent. By interference neutralization, for this class of networks, the sum s.d.o.f. is exactly equal to the sum d.o.f., which is 2.

For the $2 \times 2 \times 2$ IC, which is a cascade of two fully connected one-hop ICs, [66] employed interference neutralization and real interference alignment to achieve 2 sum d.o.f. Here, we use this idea to design the auxiliary random variables for the $2 \times 2 \times 2$ interference channel, construct the channel inputs, and show that it can asymptotically achieve 2 sum s.d.o.f.

Theorem 5.4 *For $2 \times 2 \times 2$ Gaussian interference channels with confidential messages, the sum s.d.o.f. is 2, with probability one.*

The proof of this theorem is given in Appendix. Based on this result, for the $2 \times 2 \times 2$ condensed interference sub-network in the original layered network, we simply treat all nodes except the nodes belonging to this sub-network as silent nodes and utilize this achievable scheme. Note that although the equivalent interference sub-network has dependent noises at each node, due to the fact that the noises are independent

of the message and have finite variances, the difference between these two models will not affect the performance in terms of reliability or security. Therefore, in both cases, the upper bound of 2 sum s.d.o.f. is achievable, i.e., $D_{s,\Sigma} = 2$.

5.5 Sum Secure d.o.f. for Case C

In this section, we consider the layered networks in case C. The converse for this case is $D_{s,\Sigma} \leq D_{\Sigma} \leq \frac{3}{2}$ from [64]. The achievability scheme proposed in [64] operates in two modes: First, a temporary node d' is chosen. In both modes, we could find a sub-network which has two disjoint paths with manageable interference to transmit 2 sum d.o.f. Node d' is one of the destinations of the first mode, which stores the information and serves as the source node in the second mode.

An example of case C is shown in Figure 5.5. The network in both modes are the same. In each mode, the solid lines show the links over which information is transmitted, and dashed lines show the edges that are not used. In this example, node d'_1 is the temporary node, which is the last node on path P_{s_1,d_1} before the interference. In the first mode, source s_1 sends message W_1 to node d'_1 and s_2 sends message W_2 to destination d_2. Since the two paths P_{s_1,d'_1} and P_{s_2,d_2} are disjoint and interference free, 2 sum d.o.f. worth of information can be sent reliably and node d'_1 stores message W_1. In the second mode, d'_1 forwards message W_1 to d_1 and s_2 sends a new message $\tilde{W}_2$ to d_2. Since the sub-network in solid lines between source nodes (d'_1, s_2) and destination nodes (d_1, d_2) form a layered network in case B, the sum d.o.f. is 2. Finally, by choosing the number of channel uses in both modes to

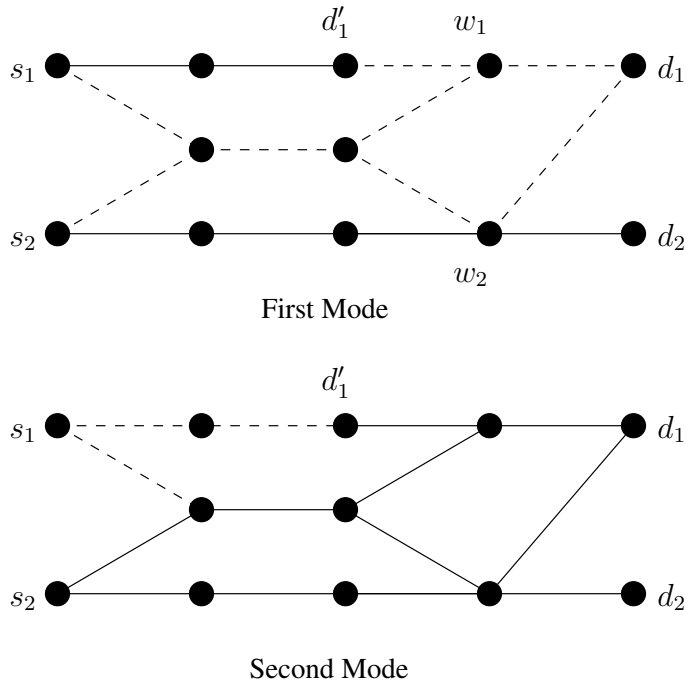


Figure 5.5: The condensed network for an example of case C. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

be the same, the achieved overall sum d.o.f. is $\frac{3}{2}$.

Reference [64] concluded that all network configurations in case C can be classified into two sub-cases C_1 and C_2. Further, in each sub-case, there are up to two different settings for the layered networks, which are given in Figures 5.5 and 5.6 for sub-case C_1, and Figures 5.7 and 5.8 for sub-case C_2. All other networks in case C have the same structure, and the same achievable scheme can be applied. In this section, we provide modified schemes for each setting of each sub-case to incorporate security in addition to reliability. In each case, we will achieve a sum s.d.o.f that is the same as the sum d.o.f., i.e., $D_{s,\Sigma} = D_{\Sigma} = \frac{3}{2}$.

5.5.1 Modified Scheme for Figure 5.5

We modify the achievable scheme described above to meet the secrecy constraint. The only issue of the original scheme is that the signal sent by w_2 in the first mode could be captured by the destination node d_1 if d_1 is in the next layer after w_2. To solve this problem, we use node w_1 on the path P_{s_1,d_1} and in the same layer as w_2 to jam the destination node d_1. Then, this hop simply becomes a Gaussian wiretap channel with a cooperative jammer, where the cooperative jammer is connected to the unintended receiver, but not to the intended receiver. This network has 1 s.d.o.f., i.e., node w_2 decodes the message it received and transmits the message based on a wiretap codebook to keep the message secure against the unintended destination d_1.

5.5.2 Modified Scheme for Figure 5.6

The other setting for layered networks in sub-case C_1 is shown in Figure 5.6. In the first mode, the source pair (s_1, s_2) transmits (W_1, W_2) to the destination pair (d_1, d_2'), where d_2' is the temporary node to store message W_2. Clearly, P_{s_1,d_1} and $P_{s_2,d_2'}$ are disjoint paths with manageable interference, i.e., case B. We can transmit W_1 to d_1 and W_2 to d_2' reliably and achieve 2 sum d.o.f. In the second mode, s_1 transmits a new message $\tilde{W}_1$ to d_1 and d_2' forwards message W_2 it received in the first mode to d_2. This scheme can achieve $\frac{3}{2}$ sum d.o.f., but the messages are not securely transmitted. The reason is that, in the first mode, if the destination node d_2 is in the next layer of w, it can receive a mixed signal from w, which contains

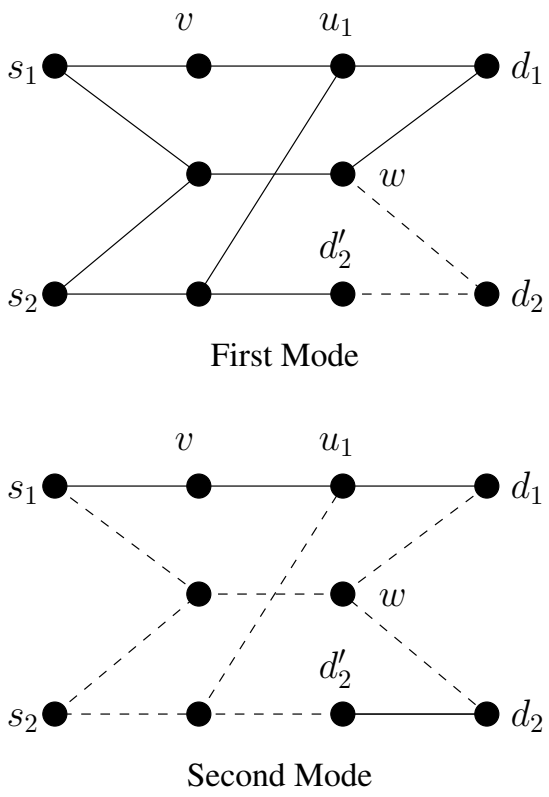


Figure 5.6: The condensed network for an example of case C. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

both W_1 and W_2.

To ensure the secrecy of both messages, we need to modify the achievable scheme and form an effective Gaussian wiretap channel with finite-variance noises. To this end, node d_2' sends pure Gaussian noise with average power P to jam the unintended receiver d_2. Signals from s_2 through different paths are canceled at d_1 due to the amplify-and-forward scheme used in case B. Since d_2 can decode W_2 after the second mode, it is safe to assume that in the first mode the signal relayed by node w does not contain the channel input of s_2. Therefore, the source-destination pair (s_1, d_1) forms a wiretap channel, where d_2 is the eavesdropper. Since the secrecy capacity depends only on the marginal distribution of $X_{s_1}, Y_{d_1}, Y_{d_2}$, but not the joint

distribution, with the help of cooperative jamming from d_2', we can always achieve 1 s.d.o.f. for the condensed wiretap channel even when the effective Gaussian additive noises at d_1 and d_2 are dependent.

5.5.3 Modified Scheme for Figure 5.7

The first setting of sub-case C_2 is shown in Figure 5.7. For the disjoint paths P_{s_1,d_1} and P_{s_2,d_2} in layered networks of sub-case C_2, there always exists a direct interference, i.e., two nodes v_1 and v_2 satisfy $v_1 \in P_{s_1,d_1}, v_2 \in P_{s_2,d_2}$ and $(v_2, v_1) \in E$ which implies $v_2 \overset{I}{\rightsquigarrow} P_{s_1,d_1}$. Meanwhile, as proven in [64], for this sub-case, there also exists a path Q_{s_1,d_1} such that $Q_{s_1,d_1} \cap P_{s_2,d_2} = \phi$ and $v_1 \notin Q_{s_1,d_1}$. This implies $v_1 \neq d_1$, and the $d_2' \neq d_2$, where d_2' is the temporary node on the path P_{s_2,d_2} and in the same layer with v_1.

To achieve $\frac{3}{2}$ sum s.d.o.f., we use the following modified achievable scheme. In the first mode, s_1 transmits message W_1 along the path Q_{s_1,d_1} to d_1, and s_2 transmits message W_2 along the path $P_{s_2,d_2'}$. If $d_2 = v_4$ which may receive the signal from v_3, we can always find a node on the path P_{s_2,d_2} to cooperatively jam d_2 due to the fact $d_2' \neq d_2$. In the second mode, s_1 transmits a new message $\tilde{W}_1$ along the path P_{s_1,d_1} to d_1, and d_2' relays message W_2 stored in the first mode along the path P_{d_2',d_2}. The two paths P_{s_1,d_1} and P_{d_2',d_2} are interference free, and therefore, the transmission is reliable and secure.

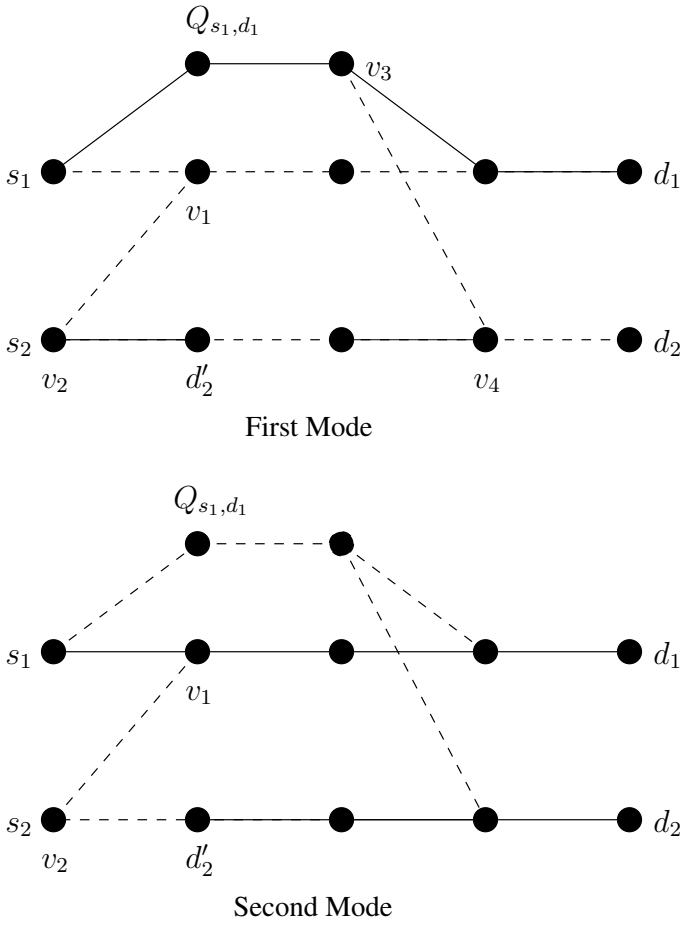


Figure 5.7: The condensed network for one of two cases in C_2. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

5.5.4 Modified Scheme for Figure 5.8

The second setting of sub-case C_2 is shown in Figure 5.8. The temporary node d_2' is chosen to be v_1. In this configuration, we also have $v_1 = d_2' \neq d_1$ and $l(d_2) > l(v_2)+1$. In the first mode, s_1 transmits message W_1 along the path Q_{s_1,d_1} to d_1, and s_2 transmits message W_2 along the path $P_{s_2,d_2'}$. This sub-network belongs to case B, which has 2 sum d.o.f. Since $d_2' \neq d_1$ and d_2 is not in the next layer of v_2, by keeping v_1 silent, messages W_1 and W_2 are secure. In the second mode, s_1 transmits a new message $\tilde{W}_1$ along the path P_{s_1,d_1} to d_1, and s_2 transmits message W_2 along the path

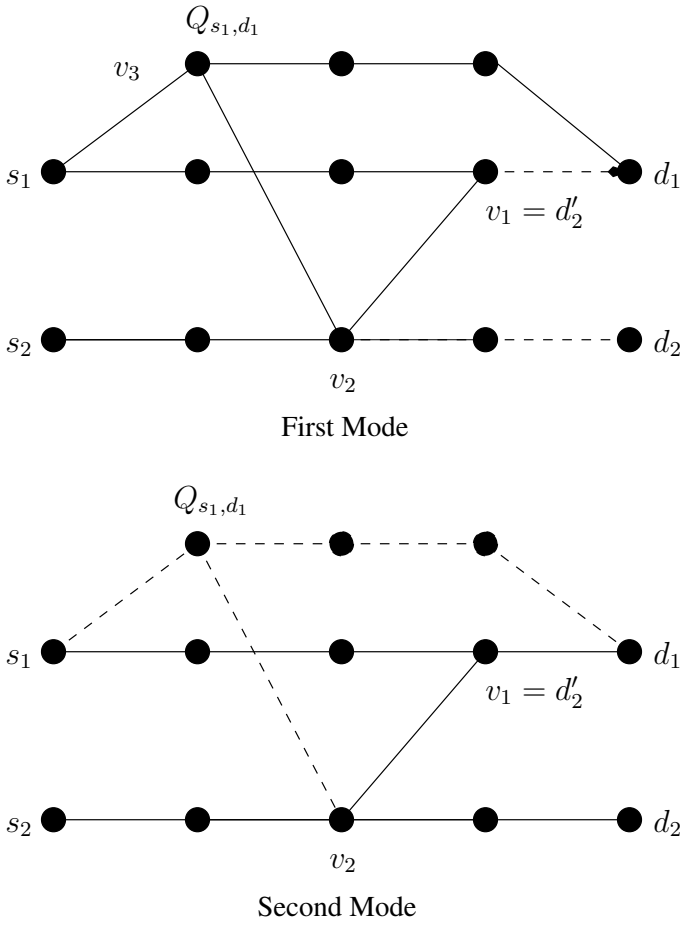


Figure 5.8: The condensed network for one of two cases in C_2. Solid lines show the edges over which signals are transmitted. Dashed lines show the edges that are not used in that mode.

P_{s_2,d_2}. Since d_2' has message W_2, it can decode message W_1 and only relay W_1 to d_1, which implies that $D_{s,\Sigma} = \frac{3}{2}$.

5.6 Conclusions

In this chapter, we considered the sum s.d.o.f. of two-unicast layered wireless networks. We used the setting in [64] and studied the cases in A, A', B, B' and C separately to incorporate security in addition to reliability. The major challenge was in cases A and A', where the sum d.o.f. is 1, due to the fact that both destination

nodes can decode the message signals. While this is inconsequential for the reliability problem in [64], it is a major problem when security is considered. To overcome this problem, we classified layered wireless networks into more detailed sub-cases, and in all sub-cases proposed modified achievable schemes that guarantee both reliability and security. In almost all sub-cases, we utilized the cooperative jamming and interference neutralization techniques to design an appropriate achievable scheme. A remaining challenge was a special configuration, where all of the nodes in the last layer before the destination layer were allowed to send only independent signals. We reduced the layered networks in this category into equivalent channel models and determined their s.d.o.f. As a result, we showed that all networks in cases A and A' have sum s.d.o.f. of $0, \frac{2}{3}$, or 1. We proposed modified schemes to achieve 2 sum s.d.o.f. for cases B and B' (which included the achievable scheme for the $2 \times 2 \times 2$ interference networks), and $\frac{3}{2}$ sum s.d.o.f. for case C.

5.7 Appendix

5.7.1 Sum Secure d.o.f. of $2 \times 2 \times 2$ Interference Network

In this section, we will show that sum s.d.o.f. of 2 can be achieved in the $2 \times 2 \times 2$ interference network with constant channel gains. The $2 \times 2 \times 2$ interference network is a concatenation of two fully connected two-user Gaussian ICs. The main idea is to design a wiretap channel with proper auxiliary random variables, and to show that with such a choice of random variables, the achievable secrecy rate can asymptotically approach 1 s.d.o.f. for each user. Our achievability is mainly

based on the real interference alignment [52] based scheme in [66]. There are two differences: 1) In [66], M signals are employed for transmitter 1 and $M-1$ signals are employed for transmitter 2. The integer M is chosen sufficiently large such that 1 d.o.f. can be achieved asymptotically for each user. Due to the fact that the last signal of transmitter 1, $x_{1,M}$, can be decoded by transmitter 2, this scheme is insecure. Here, we use only $M-1$ signals in the transmission by choosing $x_{1,M}=0$. 2) To achieve 2 sum d.o.f. in the $2\times 2\times 2$ interference network, in addition to scaling the signals with proper coefficients based on real interference alignment, the nodes in the middle layer of the $2\times 2\times 2$ interference network perform hard decisions to decode the original channel inputs from the previous layer and resend the signals again with well-designed coefficients. If these hard decisions have no error, then due to the special construction of the channel inputs based on interference neutralization and interference alignment, the messages are secure. However, if errors occur during decoding in the middle layer, then the mixed signals containing both messages observed by both destination nodes may leak information. To show the optimality of the proposed achievable scheme, we observe that the message rate scales with $\log P$, but the probability of hard decision error decreases exponentially fast with P, which makes the information leakage rate negligible in the high SNR regime. We provide a precise performance analysis in terms of both reliability and secrecy.

We use the notation in [66] for the channel model. In the first hop, the received

signal at relay $R_k, k \in \{1, 2\}$ is

$$Y_{R_k} = F_{k1}X_1 + F_{k2}X_2 + Z_k \tag{5.20}$$

where F_{kj} is the channel gain from source S_j to relay R_k, X_j is the input signal from S_j, Y_{R_k} is the received signal at relay R_k, and Z_k is an additive zero-mean unit-variance Gaussian noise. In the second hop, the received signal at destination $D_k, k \in \{1, 2\}$ is given by

$$Y_k = G_{k1}X_{R_1} + G_{k2}X_{R_2} + N_k \tag{5.21}$$

where G_{kj} is the channel gain from relay R_j to destination D_k, X_{R_j} is the input signal from relay R_j, Y_k is the received signal at D_k and N_k is an additive zero-mean unit-variance Gaussian noise. All the channel gains in the network are fixed during the communication session and known at all nodes.

In contrast to separating the message W_i into M independent sub-messages $W_{i,k_i}(k_i \in \{1, 2, \cdots, M\})$ in [66], we need to construct a virtual wiretap channel to achieve the sum s.d.o.f. For each user i, we separate the channel input signal x_i into M independent sub-signals $\{x_{i,k_i}\}_{k_i=1}^{M}$. The constellation of each sub-signal x_{i,k_i} is defined as follows

$$C(Q) = \{-Q, -Q+1, \cdots, Q-1, Q\} \tag{5.22}$$

If x_{i,k_i}'s are independent and uniform, each of them carries $\log(2Q+1)$ bits. The real channel input x_i is set to be the linear combination of $\{x_{i,k_i}\}$ with the rationally

independent coefficients[1] $\{t_{i,k_i}\}$, i.e.,

$$x_i = a \sum_{k_i=1}^{M} t_{i,k_i} x_{i,k_i} \tag{5.23}$$

where a is a constant to normalize the input signal power, and $t_{2,M} = 0$ since we only need $M-1$ data signals for x_2. The average power of this channel input is

$$\mathrm{E}[x_i^2] \le a^2 \left(\sum_{k_i=1}^{M} |t_{i,k_i} x_{i,k_i}| \right)^2 \le \left(\sum_{k_i=1}^{M} |t_{i,k_i}| \right)^2 a^2 Q^2 \tag{5.24}$$

When M is fixed, which will be specified later, we denote $\xi = \max_{i=1,2} \left(\sum_{k_i=1}^{M} |t_{i,k_i}| \right)^2$, and, for any $\epsilon > 0$, we choose

$$Q = P^{\frac{1-\epsilon}{2(M+\epsilon)}}, \quad a = \frac{1}{\sqrt{\xi}} P^{\frac{M-1+2\epsilon}{2(M+\epsilon)}} \tag{5.25}$$

Then, the signals x_1 and x_2 both satisfy the average power constraint, i.e.,

$$\mathrm{E}[x_i^2] \le P, \quad \text{for } i = 1, 2 \tag{5.26}$$

Furthermore, from [52], the minimum distance d_{min} between the points in the combined constellation can be lower bounded as follows:

$$d_{min} \ge \frac{k_\epsilon a}{(2Q)^{M-1+\epsilon}} = \frac{k_\epsilon}{2^{M-1+\epsilon}\sqrt{\xi}} P^{\frac{\epsilon}{2}} \tag{5.27}$$

[1] $a_1, a_2, \ldots, a_L$ are rationally independent if whenever $q_1, q_2, \ldots, q_L$ are integer numbers then $\sum_{i=1}^{L} q_i a_i = 0$ implies $q_i = 0$ for all i.

for some constant k_ϵ, which depends on ϵ, but not on P. This result implies that the error probability of hard decisions to recover the PAM signals decreases exponentially with the power P^ϵ.

We use the scheme in [66] to design the coefficients t_{i,k_i}s. At the relay node R_1, the received signal is as follows

$$Y_{R_1} = F_{1,1}t_{1,1}x_{1,1} + \sum_{i=1}^{M-1} F_{1,1}t_{1,i+1}(x_{1,i+1} + x_{2,i}) + Z_1 \tag{5.28}$$

We denote

$$x_{R_1,1} = x_{1,1} \tag{5.29}$$

$$x_{R_1,i+1} = x_{1,i+1} + x_{2,i}, \quad \text{for } i = 1, \cdots, M-1 \tag{5.30}$$

It is easy to see that $x_{R_1,1} \in C(Q)$ and $x_{R_1,i+1} \in C(2Q)$ for $i = 1, \cdots, M-1$.

Relay node R_1 performs hard decision to get $\hat{x}_{R_1,i}$ for $i = 1, \cdots, M$. The probability of decoding error $\Pr(R_1)$ decreases exponentially with power P^ϵ and the channel input of the relay node R_1 is:

$$x_{R_1} = b \sum_{k_1=1}^{M} t_{R_1,k_1}\hat{x}_{R_1,k_1} \tag{5.31}$$

where b is again a constant to normalize the input signal power. Similarly, relay

node R_2 makes the hard decision $\hat{x}_{R_2,i}$ of the signals $x_{R_2,i}$,

$$x_{R_2,i} = x_{1,i} + x_{2,i}, \quad \text{for } i = 1, \cdots, M-1 \tag{5.32}$$

$$x_{R_2,M} = x_{1,M} \tag{5.33}$$

and the probability of error $\Pr(R_2)$ exponentially decreases with power P^{ϵ}. The channel input of the relay node R_2 is:

$$x_{R_2} = b \sum_{k_2=1}^{M-1} t_{R_2,k_2} \hat{x}_{R_2,k_2} \tag{5.34}$$

The selection of $\{t_{R_1,k_1}\}$ and $\{t_{R_2,k_2}\}$ can be found in [66].

The observations of the two receivers in the final layer are

$$Y_1 = b \sum_{i=1}^{M} G_{1,1} t_{R_1,i} x_{D_1,i} + N_1 \tag{5.35}$$

$$Y_2 = b G_{2,1} t_{R_1,M} x_{D_2,M} + b \sum_{i=1}^{M-1} G_{2,2} t_{R_2,i} x_{D_2,i} + N_2 \tag{5.36}$$

where

$$x_{D_1,1} = \hat{x}_{R_1,1} \tag{5.37}$$

$$x_{D_1,i+1} = \hat{x}_{R_1,i+1} - \hat{x}_{R_2,i}, \quad \text{for } i = 1, \cdots, M-1 \tag{5.38}$$

$$x_{D_2,i} = \hat{x}_{R_2,i} - \hat{x}_{R_1,i}, \quad \text{for } i = 1, \cdots, M-1 \tag{5.39}$$

$$x_{D_2,M} = \hat{x}_{R_1,M} \tag{5.40}$$

Denote by A the event that the hard decisions at relay nodes 1 and 2 are both correct. Then, the probability of the complement event $\bar{A}$ decreases exponentially with power P^{ϵ} due to the following inequality

$$\begin{aligned} 1 - \Pr(A) &= \Pr(\bar{A}) && (5.41)\\ &= \Pr(\text{hard decision error occurs at } R_1 \text{ and/or } R_2) && (5.42)\\ &\leq \Pr(R_1) + \Pr(R_2) && (5.43)\\ &\leq 2\exp(-c_0 P^{\epsilon}) && (5.44) \end{aligned}$$

for some constant c_0 independent of P. If event A happens, which indicates that the hard decisions at both relay nodes are correct, then it is clear that

$$\begin{aligned} x_{D_1,1} &= \hat{x}_{R_1,1} = x_{1,1} && (5.45)\\ x_{D_1,i+1} &= \hat{x}_{R_1,i+1} - \hat{x}_{R_2,i} \\ &= x_{1,i+1} + x_{2,i} - x_{1,i} - x_{2,i} \\ &= x_{1,i+1} - x_{1,i}, \qquad \text{for } i = 1, \cdots, M-1 && (5.46) \end{aligned}$$

and

$$\begin{aligned} x_{D_2,1} &= \hat{x}_{R_2,1} - \hat{x}_{R_1,1} \\ &= x_{1,1} + x_{2,1} - x_{1,1} \\ &= x_{2,1} \end{aligned} \tag{5.47}$$

$$\begin{aligned} x_{D_2,i} &= \hat{x}_{R_2,i} - \hat{x}_{R_1,i} \\ &= x_{1,i} + x_{2,i} - x_{1,i} - x_{2,i-1} \\ &= x_{2,i} - x_{2,i-1}, \qquad \text{for } i = 2, \cdots, M-1 \end{aligned} \tag{5.48}$$

$$\begin{aligned} x_{D_2,M} &= \hat{x}_{R_1,M} \\ &= x_{1,M} + x_{2,M-1} \end{aligned} \tag{5.49}$$

which means that the observation Y_1 and $\{x_{2,i}\}_{i=1}^{M-1}$ are independent and, except the item $x_{1,M}$, the observation Y_2 and $\{x_{1,i}\}_{i=1}^{M-1}$ are independent[2].

To design the wiretap code, we choose the auxiliary random variables $v_{1,i}$ and $v_{2,i}$ as

$$v_{1,i} = x_{1,i} \text{ and } v_{2,i} = x_{2,i}, \quad \text{for } i = 1, \cdots, M-1 \tag{5.50}$$

with uniform distribution in $C(Q)$ and choose $x_{1,M} = 0$. Since for different channel uses the signals are i.i.d., and W_1, W_2 are independent, the following secrecy rate

[2]Note that $\{x_{1,i}\}_{i=1}^{M}$ are i.i.d.

pair is achievable [5, Theorem 2]:

$$I(\bar{v}_i; Y_i) - I(\bar{v}_i; Y_j|\bar{v}_j) \tag{5.51}$$

where $\bar{v}_i \triangleq (v_{i,1}, v_{i,2}, \cdots, v_{i,M-1})$ and $\bar{v}_j \triangleq (v_{j,1}, v_{j,2}, \cdots, v_{j,M-1})$ for $i = 1, 2$, and $j = \bar{i}$. By [66], information rate part, i.e., the first item in (5.51), is given by

$$I(\bar{v}_i; Y_i) \geq \frac{(M-1)(1-\epsilon)}{2(M+\epsilon)} \log P + o(\log P) \tag{5.52}$$

To upper bound the second item in (5.51), we define the binary random variable Z_A as

$$Z_A = \mathbb{1}_{\{A\}} \tag{5.53}$$

where $\mathbb{1}_{\{.\}}$ is the indicator function. As shown above, when event A happens,

$$\bar{v}_i \to \bar{v}_j \to Y_j \tag{5.54}$$

forms a Markov chain for $i = 1, 2$ and $j = \bar{i}$, i.e.,

$$I(\bar{v}_i; Y_j|\bar{v}_j, Z_A = 1) = 0 \tag{5.55}$$

The difficulty to analyze the achievable secrecy rate is that when the hard decisions at relay nodes are in error, the mixed signals at the unintended receiver will not be aligned in the *perfect* way, which will introduce dependence between the

Y_j and $v_{i,1\ldots M-1}$. However, we can upper bound the mutual information for each i as follows:

$$I(\bar{v}_i; Y_j|\bar{v}_j) = H(\bar{v}_i) - H(\bar{v}_i|Y_j, \bar{v}_j) \tag{5.56}$$

$$\leq H(\bar{v}_i) - H(\bar{v}_i|Y_j, Z_A, \bar{v}_j) \tag{5.57}$$

where the latter item can be rewriten as

$$H(\bar{v}_i|Y_j, Z_A, \bar{v}_j) = \sum_{z\in\{0,1\}} P(Z_A = z)H(\bar{v}_i|Y_j, Z_A = z, \bar{v}_j) \tag{5.58}$$

$$\geq P(Z_A = 1)H(\bar{v}_i|Y_j, Z_A = 1, \bar{v}_j) \tag{5.59}$$

$$= P(Z_A = 1)H(\bar{v}_i|Z_A = 1, \bar{v}_j) \tag{5.60}$$

(5.60) is due to (5.55). The former item in (5.57) can be upper bounded by

$$H(\bar{v}_i) = H(\bar{v}_i|Z_A, \bar{v}_j) + H(Z_A, \bar{v}_j) - H(Z_A, \bar{v}_j|\bar{v}_i) \tag{5.61}$$

$$= H(\bar{v}_i|Z_A, \bar{v}_j) + H(\bar{v}_j) + H(Z_A|\bar{v}_j) - H(\bar{v}_j|\bar{v}_i) - H(Z_A|\bar{v}_j, \bar{v}_i) \tag{5.62}$$

$$= H(\bar{v}_i|Z_A, \bar{v}_j) + H(Z_A|\bar{v}_j) - H(Z_A|\bar{v}_j, \bar{v}_i) \tag{5.63}$$

$$\leq H(\bar{v}_i|Z_A, \bar{v}_j) + 1 \tag{5.64}$$

$$= \sum_{z\in\{0,1\}} P(Z_A = z)H(\bar{v}_i|Z_A = z, \bar{v}_j) + 1 \tag{5.65}$$

Substituting (5.60) and (5.65) in (5.57), we have

$$I(\bar{v}_i; Y_j|\bar{v}_j) \leq \sum_{z\in\{0,1\}} P(Z_A = z)H(\bar{v}_i|Z_A = z, \bar{v}_j) + 1$$

$$- P(Z_A = 1)H(\bar{v}_i|Z_A = 1, \bar{v}_j) \tag{5.66}$$

$$\leq P(Z_A = 0)H(\bar{v}_i|Z_A = 0, \bar{v}_j) + 1 \tag{5.67}$$

$$\leq P(\bar{A})H(\bar{v}_i|Z_A = 0, \bar{v}_j) + 1 \tag{5.68}$$

$$\leq o(\log P) \tag{5.69}$$

The last inequality is due to (5.44) and the finite alphabet of the vector $\bar{v}_i = (v_{i,1}, v_{i,2}, \cdots, v_{i,M-1})$, which is maximized by uniform distribution, i.e.,

$$H(\bar{v}_i|Z_A = 0, \bar{v}_j) \leq \log |C|^{M-1} \tag{5.70}$$

$$= \frac{(M-1)(1-\epsilon)}{2(M+\epsilon)} \log P + o(\log P) \tag{5.71}$$

which means that the achievable rate (5.51) is lower bounded by

$$\frac{(M-1)(1-\epsilon)}{2(M+\epsilon)} \log P + o(\log P) \tag{5.72}$$

If we choose M large enough, then the sum s.d.o.f. will approach 2 arbitrarily close, completing the proof.

Chapter 6

Secure Degrees of Freedom of the Gaussian Wiretap Channel with Helpers and No Eavesdropper CSI: Blind Cooperative Jamming

6.1 Introduction

In this chapter, we revisit the Gaussian wiretap channel with M helpers considered in Chapter 2. The exact s.d.o.f. of the Gaussian wiretap channel with M helpers with perfect CSI at the transmitters is shown to be $\frac{M}{M+1}$. One of the main ingredients of our optimal achievable scheme with perfect CSI is to align cooperative jamming signals with the information symbols at the eavesdropper to limit the information leakage rate. This requires *perfect* eavesdropper CSI at the transmitters.

From a practical point of view, generally, it is difficult or impossible to obtain the eavesdropper's CSI. In this chapter, we consider the Gaussian wiretap channel with M helpers, where no eavesdropper CSI is available at the legitimate entities. Motivated by the result in [67], we propose a new achievable scheme in which cooperative jamming signals span the *entire space* of the eavesdropper, but are not exactly aligned with the information symbols. We show that this scheme achieves the same s.d.o.f. of $\frac{M}{M+1}$ but does not require any eavesdropper CSI; the transmitters *blindly* cooperative jam the eavesdropper.

6.2 System Model and Definitions

The Gaussian wiretap channel with M helpers, see Figure 1.2, is defined by

$$Y_1 = h_1 X_1 + \sum_{j=2}^{M+1} h_j X_j + N_1 \tag{6.1}$$

$$Y_2 = g_1 X_1 + \sum_{j=2}^{M+1} g_j X_j + N_2 \tag{6.2}$$

where Y_1 is the channel output of the legitimate receiver, Y_2 is the channel output of the eavesdropper, X_1 is the channel input of the legitimate transmitter, X_i, for $i = 2, \ldots, M+1$, are the channel inputs of the M helpers, h_i is the channel gain of the ith transmitter to the legitimate receiver, g_i is the channel gain of the ith transmitter to the eavesdropper, and N_1 and N_2 are two independent zero-mean unit-variance Gaussian random variables. All channel inputs satisfy average power constraints, $\mathrm{E}\left[X_i^2\right] \leq P$, for $i = 1, \ldots, M+1$.

Transmitter 1 intends to send a message W, uniformly chosen from a set $\mathcal{W}$, to the legitimate receiver (receiver 1). The rate of the message is $R \triangleq \frac{1}{n} \log |\mathcal{W}|$, where n is the number of channel uses. Transmitter 1 uses a stochastic function $f : \mathcal{W} \to \mathbf{X}_1$ to encode the message, where $\mathbf{X}_1 \triangleq X_1^n$ is the n-length channel input. We use boldface letters to denote n-length vector signals, e.g., $\mathbf{X}_1 \triangleq X_1^n$, $\mathbf{Y}_1 \triangleq Y_1^n$, $\mathbf{Y}_2 \triangleq Y_2^n$, etc. The legitimate receiver decodes the message as $\hat{W}$ based on its observation $\mathbf{Y}_1$. A secrecy rate R is said to be achievable if for any $\epsilon > 0$ there exists an n-length code such that receiver 1 can decode this message reliably, i.e.,

the probability of decoding error is less than ϵ,

$$\Pr\left[W \neq \hat{W}\right] \leq \epsilon \tag{6.3}$$

and the message is kept information-theoretically secure against the eavesdropper,

$$\frac{1}{n}H(W|\mathbf{Y}_2) \geq \frac{1}{n}H(W) - \epsilon \tag{6.4}$$

i.e., that the uncertainty of the message W, given the observation $\mathbf{Y}_2$ of the eavesdropper, is almost equal to the entropy of the message. The supremum of all achievable secrecy rates is the secrecy capacity C_s, and the s.d.o.f., D_s, is defined as

$$D_s \triangleq \lim_{P\to\infty} \frac{C_s}{\frac{1}{2}\log P} \tag{6.5}$$

Note that $D_s \leq 1$ is an upper bound. To avoid trivial cases, we assume that $h_1 \neq 0$ and $g_1 \neq 0$. Without the independent helpers, i.e., $M = 0$, and with full knowledge of all channel gains, the secrecy capacity of the Gaussian wiretap channel is known [4]

$$C_s = \frac{1}{2}\log\left(1 + h_1^2 P\right) - \frac{1}{2}\log\left(1 + g_1^2 P\right) \tag{6.6}$$

and from (6.5) the s.d.o.f. is zero. Therefore, we assume $M \geq 1$. If there exists a j ($j = 2, \ldots, M+1$) such that $h_j = 0$ and $g_j \neq 0$, then a lower bound of 1 s.d.o.f. can be obtained for this channel by letting this helper jam the eavesdropper by i.i.d. Gaussian noise of power P and keeping all other helpers silent. This lower

bound matches the upper bound, giving the s.d.o.f. On the other hand, if there exists a j ($j = 2, \ldots, M+1$) such that $h_j \neq 0$ and $g_j = 0$, then this helper can be removed from the channel model without affecting the s.d.o.f. Therefore, in the rest of the chapter, we assume that $M \geq 1$ and $h_j \neq 0$ and $g_j \neq 0$ for all $j = 1, \cdots, M+1$.

6.3 Achievable Scheme with no Eavesdropper CSI

In this section, we propose an achievable scheme to achieve the s.d.o.f. of $\frac{M}{M+1}$ with no eavesdropper CSI at any of the transmitters. The only assumption we make is that the legitimate transmitter knows an upper bound of $\sum_{k=1}^{M+1} g_k^2 \leq \bar{c}$ on the eavesdropper channel gains.

Let $\{V_2, V_3, \cdots, V_{M+1}, U_1, U_2, U_3, \cdots, U_{M+1}\}$ be mutually independent discrete random variables, each of which uniformly drawn from the same PAM constellation $C(a, Q)$ in (2.73), where Q is a positive integer and a is a real number used to normalize the transmission power, and is also the minimum distance between the points belonging to $C(a, Q)$. Exact values of a and Q will be specified later. We choose the input signal of the legitimate transmitter as

$$X_1 = \frac{1}{h_1} U_1 + \sum_{k=2}^{M+1} \alpha_k V_k \tag{6.7}$$

where $\{\alpha_k\}_{k=2}^{M+1}$ are rationally independent among themselves and also rationally independent of all channel gains. The input signal of the jth helper, $j = 2, \cdots, M+$

1, is chosen as

$$X_j = \frac{1}{h_j} U_j \tag{6.8}$$

Note that, neither the legitimate transmitter signal in (6.7) nor the helper signals in (6.8) depend on the eavesdropper CSI $\{g_k\}_{k=1}^{M+1}$. With these selections, observations of the receivers are given by,

$$Y_1 = \sum_{k=2}^{M+1} h_1 \alpha_k V_k + \left(\sum_{j=1}^{M+1} U_j \right) + N_1 \tag{6.9}$$

$$Y_2 = \sum_{k=2}^{M+1} g_1 \alpha_k V_k + \sum_{j=1}^{M+1} \frac{g_j}{h_j} U_j + N_2 \tag{6.10}$$

The intuition here is as follows: We use M independent sub-signals V_k, $k = 2, \cdots, M+1$, to represent the original message W. The input signal X_1 is a linear combination of V_ks and a jamming signal U_1. At the legitimate receiver, all of the cooperative jamming signals, U_ks, are aligned such that they occupy a small portion of the signal space. Since $\{1, h_1\alpha_2, h_1\alpha_3, \cdots, h_1\alpha_{M+1}\}$ are rationally independent for all channel gains, except for a set of Lebesgue measure zero, the signals $\left\{V_2, V_3, \cdots, V_{M+1}, \sum_{j=1}^{M+1} U_j\right\}$ can be distinguished by the legitimate receiver. In addition, we observe that $\left\{\frac{g_1}{h_1}, \cdots, \frac{g_{M+1}}{h_{M+1}}\right\}$ are rationally independent, and therefore, $\{U_1, U_2, \cdots, U_{M+1}\}$ *span* the *entire space* at the eavesdropper; see Figure 6.1 (with perfect CSI, see Figure 2.2 in Chapter 2). Here, by the *entire space*, we mean the maximum number of *dimensions* that the eavesdropper is capable of decoding, which is $M+1$ in this case. Since the *entire space* at the eavesdropper is occupied by the cooperative jamming signals, the message signals $\{V_2, V_3, \cdots, V_{M+1}\}$ are secure,

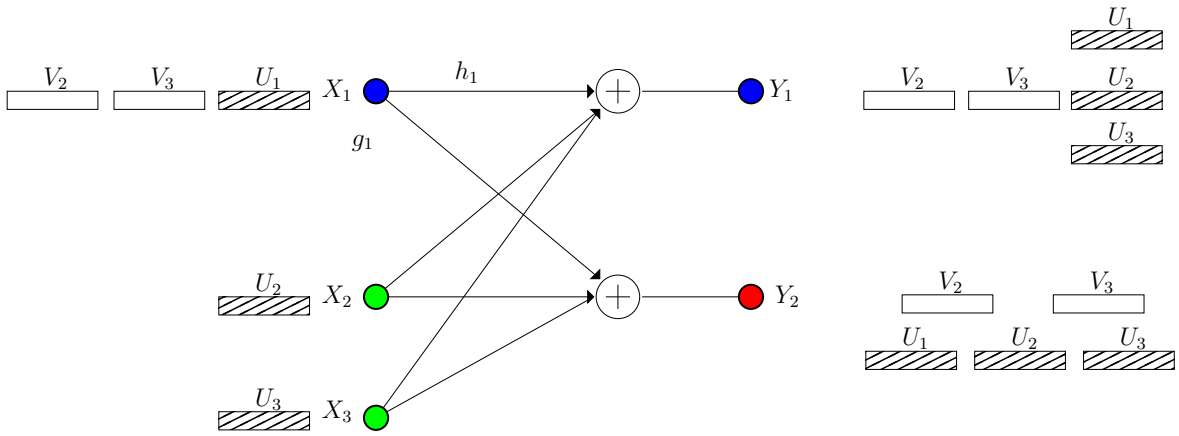


Figure 6.1: Illustration of the alignment scheme for the Gaussian wiretap channel with M helpers with no eavesdropper CSI.

as we will mathematically prove in the sequel.

Since, for $j \neq 1$, $\mathbf{X}_j$ is an i.i.d. sequence and is independent of $\mathbf{X}_1$, the following secrecy rate is achievable [3]

$$C_s \geq I(\mathbf{V}; Y_1) - I(\mathbf{V}; Y_2) \tag{6.11}$$

where $\mathbf{V} \stackrel{\triangle}{=} \{V_2, V_3, \cdots, V_{M+1}\}$.

First, we use Fano's inequality to bound the first term in (6.11). By Lemma 2.3, for any small enough $\delta > 0$ and almost surely all $\{1, h_1\alpha_2, h_1\alpha_3, \cdots, h_1\alpha_{M+1}\}$, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(M+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, then the average power constraint is satisfied and the probability of error is bounded by

$$\Pr\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \leq \exp\left(-\eta_\gamma P^\delta\right) \tag{6.12}$$

where η_γ is a positive constant which is independent of P and $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y_1.

By Fano's inequality and the Markov chain $\mathbf{V} \to Y_1 \to \hat{\mathbf{V}}$, we know that

$$H(\mathbf{V}|Y_1) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{6.13}$$

$$\leq 1 + \exp\left(-\eta_\gamma P^\delta\right) \log(2Q+1)^M \tag{6.14}$$

$$= o(\log P) \tag{6.15}$$

where δ and γ are fixed, and $o(\cdot)$ is the little-o function. This means that

$$I(\mathbf{V}; Y_1) = H(\mathbf{V}) - H(\mathbf{V}|Y_1) \tag{6.16}$$

$$\geq H(\mathbf{V}) - o(\log P) \tag{6.17}$$

$$= \log(2Q+1)^M - o(\log P) \tag{6.18}$$

$$\geq \log P^{\frac{M(1-\delta)}{2(M+1+\delta)}} - o(\log P) \tag{6.19}$$

$$= \frac{M(1-\delta)}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) \tag{6.20}$$

Next, we need to bound the second term in (6.11),

$$I(\mathbf{V};Y_2) = I(\mathbf{V},\mathbf{U};Y_2) - I(\mathbf{U};Y_2|\mathbf{V}) \tag{6.21}$$

$$= I(\mathbf{V},\mathbf{U};Y_2) - H(\mathbf{U}|\mathbf{V}) + H(\mathbf{U}|Y_2,\mathbf{V}) \tag{6.22}$$

$$= I(\mathbf{V},\mathbf{U};Y_2) - H(\mathbf{U}) + H(\mathbf{U}|Y_2,\mathbf{V}) \tag{6.23}$$

$$= h(Y_2) - h(Y_2|\mathbf{V},\mathbf{U}) - H(\mathbf{U}) + H(\mathbf{U}|Y_2,\mathbf{V}) \tag{6.24}$$

$$= h(Y_2) - h(N_2) - H(\mathbf{U}) + H(\mathbf{U}|Y_2,\mathbf{V}) \tag{6.25}$$

$$\leq h(Y_2) - h(N_2) - H(\mathbf{U}) + o(\log P) \tag{6.26}$$

$$\leq \frac{1}{2}\log 2\pi e(1+\bar{c}P) - \frac{1}{2}\log 2\pi e - \log(2Q+1)^{M+1} + o(\log P) \tag{6.27}$$

$$\leq \frac{1}{2}\log P - \frac{(M+1)(1-\delta)}{2(M+1+\delta)}\log P + o(\log P) \tag{6.28}$$

$$= \frac{(M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{6.29}$$

where $\mathbf{U} \triangleq \{U_1, U_2, \cdots, U_{M+1}\}$ and $\bar{c}$ is the upper bound on $\sum_{k=1}^{M+1} g_k^2$ defined at the beginning of this section, and (6.26) is due to the fact that given $\mathbf{V}$ and Y_2, the eavesdropper can decode $\mathbf{U}$ with probability of error approaching zero since $\left\{\frac{g_1}{h_1}, \cdots, \frac{g_{M+1}}{h_{M+1}}\right\}$ are rationally independent for all channel gains, except for a set of Lebesgue measure zero. Then, by Fano's inequality, $H(\mathbf{U}|Y_2,\mathbf{V}) \leq o(\log P)$ similar to the step in (6.15).

Combining (6.20) and (6.29), we have

$$C_s \geq I(\mathbf{V};Y_1) - I(\mathbf{V};Y_2) \tag{6.30}$$

$$\geq \frac{M(1-\delta)}{M+1+\delta}\left(\frac{1}{2}\log P\right) - \frac{(M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) \tag{6.31}$$

$$= \frac{M-(2M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) \tag{6.32}$$

where again $o(\cdot)$ is the little-o function. If we choose δ arbitrarily small, then we can achieve $\frac{M}{M+1}$ s.d.o.f. for this model where there is no eavesdropper CSI at the transmitters.

6.4 Conclusions

In this chapter, we studied the Gaussian wiretap channel with M helpers without any eavesdropper CSI at the transmitters. We proposed an achievable scheme that achieves a s.d.o.f. of $\frac{M}{M+1}$, which is the same as the s.d.o.f. found in Chapter 2 when the transmitters had perfect eavesdropper CSI. The new achievability scheme is based on real interference alignment and *blind* cooperative jamming. While in Chapter 2 we aligned cooperative jamming signals with the information symbols at the eavesdropper to protect the information symbols, which required eavesdropper CSI, here we used one more cooperative jamming signal to span the *entire space* at the eavesdropper to protect the information symbols. As in Chapter 2, here also, we aligned all of the cooperative jamming signals in the same dimension at the legitimate receiver, in order to occupy the smallest space at the legitimate receiver

to allow for the decodability of the information symbols. Therefore, we aligned the cooperative jamming signals carefully only at the legitimate receiver, which required only the legitimate receiver's CSI at the transmitters.

Chapter 7

Inseparability of the Multiple Access Wiretap Channel

7.1 Introduction

In this chapter, we investigate the separability of the parallel MAC wiretap channel. Separability, when exists, is useful as it enables us to code separately over parallel channels, and still achieve the optimum overall performance. It is well-known that the parallel single-user channel, parallel MAC and parallel BC are all separable, however, the parallel IC is not separable in general. In this chapter, we show that, while MAC is separable MAC wiretap channel is not separable in general. We prove this via a specific linear deterministic MAC wiretap channel. We then show that even the Gaussian MAC wiretap channel is inseparable in general. Finally, we show that, when the channel gains are drawn from continuous distributions, and when the s.d.o.f. region is considered, then the Gaussian MAC wiretap channel is almost surely separable.

7.2 System Model and Definitions

In a two-user MAC wiretap channel $p(y_1, y_2|x_1, x_2)$, each transmitter i, $i = 1, 2$, has a message W_i intended for the legitimate receiver whose channel output is Y_1. For each i, message W_i is uniformly and independently chosen from set $\mathcal{W}_i$. The rate of

message i is $R_i \triangleq \frac{1}{n}\log|\mathcal{W}_i|$. Transmitter i uses a stochastic function $f_i : \mathcal{W}_i \to X_i^n$, where the n-length vector X_i^n denotes the ith user's channel input in n channel uses. All messages are needed to be kept secret from the eavesdropper whose channel output is Y_2.

A secrecy rate pair (R_1, R_2) is said to be achievable if for any $\epsilon > 0$ there exist n-length codes such that the legitimate receiver can decode the messages reliably, i.e., the probability of decoding error is less than ϵ

$$\Pr\left[(W_1, W_2) \neq (\hat{W}_1, \hat{W}_2)\right] \leq \epsilon \tag{7.1}$$

and the messages are kept information-theoretically secure against the eavesdropper

$$\frac{1}{n}H(W_1, W_2|Y_2^n) \geq \frac{1}{n}H(W_1, W_2) - \epsilon \tag{7.2}$$

where $\hat{W}_1, \hat{W}_2$ are the estimates of the messages based on the legitimate receiver's observation Y_1^n.

The secrecy capacity region $\mathcal{C}$ is the closure of the set containing all achievable secrecy rate pairs. The sum secrecy capacity is $C_\Sigma = \sup(R_1 + R_2)$, where the supremum is over all achievable secrecy rate pairs $(R_1, R_2) \in \mathcal{C}$. For Gaussian MAC wiretap channel with average power constraint P for both transmitters, the s.d.o.f. region is defined as:

$$D_s = \left\{(d_1, d_2) : (R_1, R_2) \in \mathcal{C},\ d_i \triangleq \lim_{P\to\infty} \frac{R_i}{\frac{1}{2}\log P}\right\} \tag{7.3}$$

and the sum s.d.o.f. is defined as:

$$D_{s,\Sigma} \triangleq \lim_{P\to\infty} \frac{C_\Sigma}{\frac{1}{2}\log P} \tag{7.4}$$

Let $p(y_{1a}, y_{2a}|x_{1a}, x_{2a})$ and $p(y_{1b}, y_{2b}|x_{1b}, x_{2b})$ be two two-user MAC wiretap channels. The *parallel* two-user MAC wiretap channel is a two-user MAC wiretap channel in which the channel inputs of transmitter 1 and 2 are (x_{1a}, x_{1b}) and (x_{2a}, x_{2b}), respectively, and the channel inputs are sent simultaneously in parallel. The channel outputs of the legitimate receiver and the eavesdropper are (y_{1a}, y_{1b}) and (y_{2a}, y_{2b}), respectively, and are distributed according to

$$p\left(y_{1a}, y_{2a}, y_{1b}, y_{2b}|x_{1a}, x_{2a}, x_{1b}, x_{2b}\right) = p(y_{1a}, y_{2a}|x_{1a}, x_{2a})p(y_{1b}, y_{2b}|x_{1b}, x_{2b}) \tag{7.5}$$

We refer to each MAC wiretap channel, $p(y_{1a}, y_{2a}|x_{1a}, x_{2a})$ and $p(y_{1b}, y_{2b}|x_{1b}, x_{2b})$, as a *component* channel of the overall *parallel* MAC wiretap channel.

7.3 Inseparability of the MAC Wiretap Channel

In this section, we show that the parallel MAC wiretap channel is not separable in general. To this end, we provide a specific counter example.

Consider the linear deterministic parallel discrete memoryless MAC wiretap channel shown in Figure 7.1, which has three component channels: (a), (b) and (c). In the first component channel, (a), transmitter 1 has two sub-channel inputs, i.e., (X_{11}, X_{12}), and transmitter 2 has only one sub-channel input X_2. The legitimate

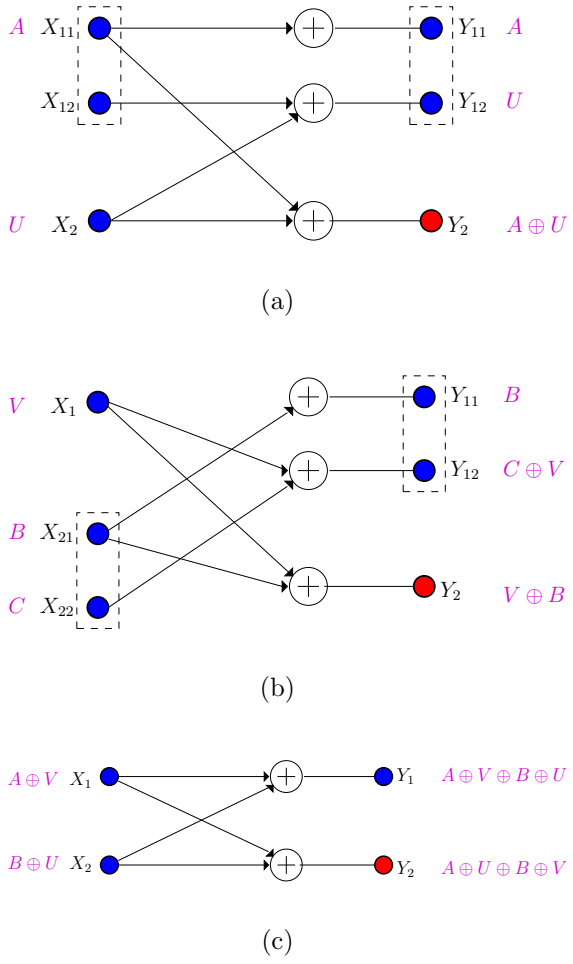


Figure 7.1: An inseparable linear deterministic parallel MAC wiretap channel. There are three component channels: (a), (b) and (c). An achievable scheme that codes across the parallel channels is shown in color magenta.

receiver observes (Y_{11}, Y_{12}) and the eavesdropper observes Y_2. In the second component channel, (b), the roles of the two transmitters are swapped. In the third component channel, (c), the legitimate receiver and the eavesdropper have identical observations. Specifically, the input/output relationships for sub-channel (a) are:

$$Y_{11} = X_{11}, \quad Y_{12} = X_{12} \oplus X_2, \quad Y_2 = X_{11} \oplus X_2 \tag{7.6}$$

where all symbols are binary, and addition is modulo-2.

While transmitters send independent data, they can each code their data jointly across their parallel channels. In the following two sub-sections, we show that the optimum separable (i.e., independent) coding yields 2 bits/channel-use for the sum secrecy rate, while through coding jointly across the component channels a sum secrecy rate of 3 bits/channel-use is achievable, and hence separation is strictly sub-optimal.

7.3.1 Optimum Sum Secrecy Rate with Separable Encoding

Due to independent coding across the component channels:

$$C_{\Sigma,\text{indep}} = C_{\Sigma,(a)} + C_{\Sigma,(b)} + C_{\Sigma,(c)} = 2C_{\Sigma,(a)} \tag{7.7}$$

where $C_{\Sigma,(a)} = C_{\Sigma,(b)}$ is due to symmetry, and $C_{\Sigma,(c)} = 0$ is due to the fact that the legitimate receiver and the eavesdropper have identical observations. Therefore, we only need to show $C_{\Sigma,(a)} = 1$ in order to show $C_{\Sigma,\text{indep}} = 2$. The achievability of this follows by the following signalling: The first user sends a 1 bit (uniform) information signal in X_{12}, and sends no signal in the other sub-channel which leaks to the eavesdropper, i.e., $X_{11} = 0$, and the second user does not send any information, i.e., $X_2 = 0$. This gives 1 bit secure rate for the first user, and hence 1 bit sum secrecy rate for the system, i.e., $C_{\Sigma,(a)} \geq 1$.

Next, we need to prove that the sum secrecy rate in the component channel (a) is upper bounded by 1, i.e., $C_{\Sigma,(a)} \leq 1$.

For convenience, let us denote $nR_\Sigma \stackrel{\triangle}{=} n(R_1+R_2)-n\epsilon$ in order not to carry $+n\epsilon$ throughout the derivation. Then, by definition, and Fano's inequality, we have

$$nR_\Sigma = nH(W_1,W_2) - n\epsilon \tag{7.8}$$

$$\leq I(W_1,W_2;Y_{11}^n,Y_{12}^n) - I(W_1,W_2;Y_2^n) \tag{7.9}$$

Using the chain rule on both terms on the right hand side,

$$nR_\Sigma \leq I(W_1,W_2;Y_{11}^n) + I(W_1,W_2;Y_{12}^n|Y_{11}^n) - I(W_1;Y_2^n) - I(W_2;Y_2^n|W_1) \tag{7.10}$$

$$= I(W_1;Y_{11}^n) + I(W_2;Y_{11}^n|W_1) - I(W_1;Y_2^n)$$

$$+ I(W_1,W_2;Y_{12}^n|Y_{11}^n) - I(W_2;Y_2^n|W_1) \tag{7.11}$$

$$= I(W_1;Y_{11}^n) + I(W_2;Y_{11}^n,W_1) - I(W_1;Y_2^n)$$

$$+ I(W_1,W_2;Y_{12}^n|Y_{11}^n) - I(W_2;Y_2^n|W_1) \tag{7.12}$$

$$= I(W_1;Y_{11}^n) - I(W_1;Y_2^n) + I(W_1,W_2;Y_{12}^n|Y_{11}^n) - I(W_2;Y_2^n|W_1) \tag{7.13}$$

$$= \big[I(W_1;Y_{11}^n) - I(W_1;Y_2^n)\big] + \big[I(W_1,W_2;Y_{12}^n|Y_{11}^n) - I(W_2;Y_2^n,W_1)\big] \tag{7.14}$$

where (7.12) and (7.14) come from the independence of W_2 and W_1, and (7.13) comes from the independence of W_2 and (W_1,Y_{11}^n). For the first part in (7.14), we

have

$$I(W_1; Y_{11}^n) - I(W_1; Y_2^n) \leq I(W_1; Y_{11}^n, Y_2^n) - I(W_1; Y_2^n) \tag{7.15}$$

$$= I(W_1; Y_{11}^n | Y_2^n) \tag{7.16}$$

$$= I(W_1; X_{11}^n | Y_2^n) \tag{7.17}$$

$$= H(X_{11}^n | Y_2^n) - H(X_{11}^n | Y_2^n, W_1) \tag{7.18}$$

where we refer to (7.6). For the second part in (7.14), we have

$$I(W_1, W_2; Y_{12}^n | Y_{11}^n) - I(W_2; Y_2^n, W_1)$$

$$= I(W_1; Y_{12}^n | Y_{11}^n) + I(W_2; Y_{12}^n | Y_{11}^n, W_1) - I(W_2; Y_2^n, W_1) \tag{7.19}$$

$$= I(W_1; Y_{12}^n | Y_{11}^n) + I(W_2; Y_{12}^n, Y_{11}^n, W_1) - I(W_2; Y_2^n, W_1) \tag{7.20}$$

$$\leq I(W_1; Y_{12}^n | Y_{11}^n) + I(W_2; Y_{12}^n, Y_{11}^n, Y_2^n, W_1) - I(W_2; Y_2^n, W_1) \tag{7.21}$$

$$= I(W_1; Y_{12}^n | Y_{11}^n) + I(W_2; Y_{12}^n, Y_{11}^n | Y_2^n, W_1) \tag{7.22}$$

$$\leq I(X_{11}^n, X_{12}^n; Y_{12}^n | Y_{11}^n) + I(X_2^n; Y_{12}^n, Y_{11}^n | Y_2^n, W_1) \tag{7.23}$$

$$= I(X_{12}^n; Y_{12}^n | X_{11}^n) + H(X_2^n | Y_2^n, W_1) \tag{7.24}$$

$$= I(X_{12}^n; Y_{12}^n | X_{11}^n) + H(X_{11}^n | Y_2^n, W_1) \tag{7.25}$$

where (7.20) follows from the independence of W_2 and (W_1, Y_{11}^n), (7.23) follows from

the Markov chains

$$W_1 \rightarrow (Y_{11}^n, X_{11}^n, X_{12}^n) \rightarrow Y_{12}^n$$

$$W_2 \rightarrow (X_2^n, Y_2^n, W_1) \rightarrow (Y_{12}^n, Y_{11}^n),$$

we obtain (7.24) by using the channel model in (7.6) and the fact that by knowing $(Y_{11}^n, Y_2^n) = (X_{11}^n, Y_2^n)$, X_2^n can be determined, and finally, we reach (7.25) by using the channel model in (7.6) and through the following derivation

$$H(X_2^n|Y_2^n, W_1) = H(X_2^n, Y_2^n, W_1) - H(Y_2^n, W_1) \tag{7.26}$$

$$= H(X_2^n, X_{11}^n, W_1) - H(Y_2^n, W_1) \tag{7.27}$$

$$= H(X_{11}^n, Y_2^n, W_1) - H(Y_2^n, W_1) \tag{7.28}$$

$$= H(X_{11}^n|Y_2^n, W_1) \tag{7.29}$$

Substituting (7.18) and (7.25) into (7.14), we obtain

$$nR_\Sigma \leq H(X_{11}^n|Y_2^n) + I(X_{12}^n; Y_{12}^n|X_{11}^n) \tag{7.30}$$

$$= H(X_{11}^n|X_{11}^n \oplus X_2^n) + I(X_{12}^n; X_{12}^n \oplus X_2^n|X_{11}^n) \tag{7.31}$$

where $\oplus$ means bitwise modulo plus. Now, intuitively, as shown in (7.31), if transmitter 1 intends to transmit n-bit message via X_{11}^n, then to protect it, transmitter 2 must send Bernoulli $(\frac{1}{2})$ i.i.d random noise; however, by performing that, the sub-channel capacity between X_{12}^n and Y_{12}^n is constrained and reduced to zero. To

confirm this, we continue from (7.31)

$$nR_\Sigma \le H(X_{11}^n|X_{11}^n \oplus X_2^n) + I(X_{12}^n; X_{12}^n \oplus X_2^n|X_{11}^n) \tag{7.32}$$

$$= H(X_2^n, X_{11}^n) - H(X_{11}^n \oplus X_2^n) + H(X_{12}^n \oplus X_2^n|X_{11}^n)$$

$$\quad - H(X_2^n|X_{12}^n, X_{11}^n) \tag{7.33}$$

$$= H(X_2^n) + H(X_{11}^n) - H(X_{11}^n \oplus X_2^n) + H(X_{12}^n \oplus X_2^n|X_{11}^n) - H(X_2^n) \tag{7.34}$$

$$= H(X_{11}^n) - H(X_{11}^n \oplus X_2^n) + H(X_{12}^n \oplus X_2^n|X_{11}^n) \tag{7.35}$$

$$= H(X_{11}^n|X_2^n) - H(X_{11}^n \oplus X_2^n) + H(X_{12}^n \oplus X_2^n|X_{11}^n) \tag{7.36}$$

$$= H(X_{11}^n \oplus X_2^n|X_2^n) - H(X_{11}^n \oplus X_2^n) + H(X_{12}^n \oplus X_2^n|X_{11}^n) \tag{7.37}$$

$$= H(X_{12}^n \oplus X_2^n|X_{11}^n) - I(X_2^n; X_{11}^n \oplus X_2^n) \tag{7.38}$$

$$\le H(X_{12}^n \oplus X_2^n|X_{11}^n) = H(Y_{12}^n|X_{11}^n) \le H(Y_{12}^n) \tag{7.39}$$

$$\le n \tag{7.40}$$

where we repeatedly use the independence of X_2^n and X_{11}^n, and also the independence of X_2^n and (X_{11}^n, X_{12}^n).

Finally, (7.40) implies $C_{\Sigma,(a)} \le 1$, concluding, together with the achievability, that $C_{\Sigma,(a)} = 1$, and hence $C_{\Sigma,\text{indep}} = 2$.

7.3.2 Joint Encoding Based Achievable Scheme

Here, we provide an achievable scheme to transmit 3 bits securely by coding across the component channels, i.e., by introducing correlation between the channel inputs of component channels. Let $\{A, B, C, U, V\}$ be mutually independent Bernoulli

($\frac{1}{2}$) random variables. Here, $\{A, B, C\}$ represent the message carrying signals, and $\{U, V\}$ represent the jamming noises. The joint encoding based achievable scheme is shown in color magenta in Figure 7.1, where transmitter 1 sends A, V and $A \oplus V$ in three component channels, respectively (note that we choose $X_{12} = 0$), and transmitter 2 sends U, (B, C) and $B \oplus U$ in three component channels, respectively.

With this scheme, the legitimate receiver observes $A, U, B, C \oplus V, A \oplus V \oplus B \oplus U$ from three component channels, which means that the legitimate receiver can decode message A from transmitter 1 and messages B, C from transmitter 2 with zero probability of error, i.e., the legitimate receiver can decode 3 bits reliably. On the other hand, the eavesdropper observes $A \oplus U$, $B \oplus V$ and $A \oplus U \oplus B \oplus V$, which implies

$$
\begin{aligned}
& I(A, B, C; A \oplus U, B \oplus V, A \oplus U \oplus B \oplus V) \\
&= I(A, B, C; A \oplus U, B \oplus V) && (7.41) \\
&= H(A \oplus U, B \oplus V) - H(A \oplus U, B \oplus V | A, B, C) && (7.42) \\
&= H(A \oplus U, B \oplus V) - H(U, V) && (7.43) \\
&= 2 - 2 = 0 && (7.44)
\end{aligned}
$$

where we use the independence of $\{A, B, C, U, V\}$ and also that they are all Bernoulli ($\frac{1}{2}$). This derivation implies that the eavesdropper learns nothing about the messages, and therefore, 3 bits are sent to the legitimate receiver reliably and securely.

7.4 Gaussian MAC Wiretap Channel

7.4.1 General Inseparability

In this section, we show that even the parallel Gaussian MAC wiretap channel is not separable in general. We prove this by providing a specific example. Also note that, it suffices to show the inseparability from the s.d.o.f. point of view, since it implies the inseparability of the secrecy capacity.

Consider the special two-user parallel Gaussian MAC wiretap channel shown in Figure 7.2, in which each component channel is a two-user Gaussian MAC wiretap channel defined by,

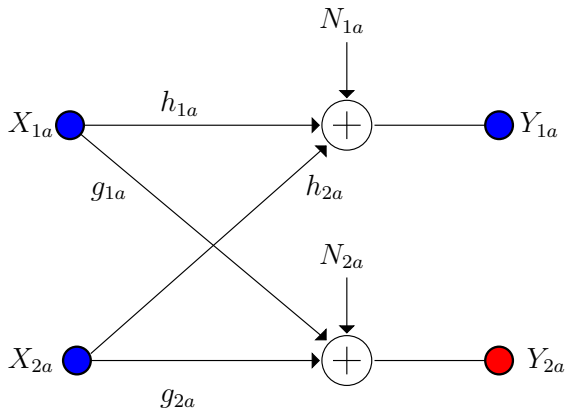
$$Y_{1k} = h_{1k}X_{1k} + h_{2k}X_{2k} + N_{1k} \tag{7.45}$$

$$Y_{2k} = g_{1k}X_{1k} + g_{2k}X_{2k} + N_{2k} \tag{7.46}$$

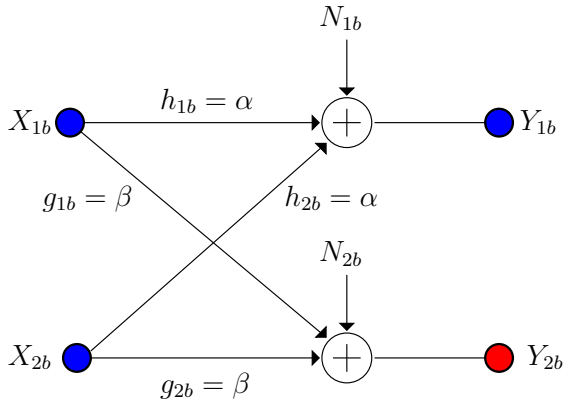
where $k = a, b$, and (h_{ia}, h_{ib}) and (g_{ia}, g_{ib}) are the time-invariant channel gains of user i to the legitimate receiver and the eavesdropper, respectively. We let

$$h_{1b} = h_{2b} = \alpha, \quad \text{and} \quad g_{1b} = g_{2b} = \beta \tag{7.47}$$

Then, the six random variables $\{h_{1a}, h_{2a}, g_{1a}, g_{2a}, \alpha, \beta\}$ are mutually independently distributed according to the same continuous distribution, and N_{1a}, N_{2a}, N_{1b}, N_{2b} are mutually independent Gaussian random variables with zero-mean and unit-variance. The channel inputs of each user satisfy average power constraints, $\mathrm{E}\left[X_{ia}^2 + X_{ib}^2\right] \leq P$,



(a)



(b)

Figure 7.2: An example two-user parallel Gaussian MAC wiretap channel.

for $i = 1, 2$.

From Chapter 2, for almost all channel gains $\{h_{1a}, h_{2a}, g_{1a}, g_{2a}\}$, the sum s.d.o.f. for component channel (a) is $\frac{2}{3}$. From [14], component channel (b) is degraded, and its sum s.d.o.f. is zero. This implies that, by independent encoding across the component channels, the optimum sum s.d.o.f. is $\frac{2}{3}$.

On the other hand, by selecting

$$X_{1a} = \frac{1}{g_{1a}} V,\ X_{2a} = \frac{1}{g_{2a}} U,\ X_{1b} = \frac{1}{\beta} V,\ X_{2b} = \frac{1}{\beta} U \tag{7.48}$$

where V and U are independent random variable drawn from the discrete PAM constellation in (2.73). Here, V represents the message-carrying signal and U represents the jamming signal. Let us define $\hat{Y}$ as

$$\hat{Y} = \frac{g_{2a}}{h_{2a}} Y_{1a} - \frac{\beta}{\alpha} Y_{1b} \tag{7.49}$$

$$= \left[\frac{g_{2a} h_{1a}}{g_{1a} h_{2a}} - 1 \right] V + \frac{g_{2a}}{h_{2a}} N_{1a} - \frac{\beta}{\alpha} N_{1b} \tag{7.50}$$

The factor in front of V is non-zero for almost all channel gains. Let us define $\hat{V}$ as the estimate of V obtained by selecting the closest point in $C(a, Q)$ based on the observation $\hat{Y}$. For any small enough $\delta > 0$, let us choose $Q = P^{\frac{1-\delta}{2}}$ and $a = \gamma P^{\frac{\delta}{2}}$, where γ is a constant independent of P to meet the average power constraint. Then, due to the Markov chain $V \to (Y_{1a}, Y_{1b}) \to \hat{Y} \to \hat{V}$, we have

$$I(V; Y_{1a}, Y_{1b}) \geq I(V; \hat{Y}) \geq I(V; \hat{V}) \tag{7.51}$$

$$= H(V) - H(V|\hat{V}) \tag{7.52}$$

$$= \log(2Q+1) - H(V|\hat{V}) \tag{7.53}$$

$$\geq \log(2Q+1) - 1 - \mathrm{P}\left[V \neq \hat{V}\right] \log(2Q+1) \tag{7.54}$$

$$\geq \left\{ 1 - \mathrm{P}\left[V \neq \hat{V}\right] \right\} \frac{1-\delta}{2} \log P - 1 \tag{7.55}$$

Now, due to the PAM structure, probability of error is

$$\mathrm{P}\left[V \neq \hat{V}\right] \leq \exp\left(-\gamma' a^2\right) \leq \exp\left(-\gamma'' P^{\delta}\right) \tag{7.56}$$

where γ', γ'' are constants independent of P. Then, from (7.55) and (7.56), at high SNR (large enough P), we have

$$I(V; Y_{1a}, Y_{1b}) \geq \frac{1-\delta}{2} \log P + o(\log P) \tag{7.57}$$

where $o(\cdot)$ is the little-o function.

On the other hand, for the information leakage rate,

$$I(V; Y_{2a}, Y_{2b}) \leq I(V; V+U) \tag{7.58}$$

$$\leq H(V+U) - H(V) \tag{7.59}$$

$$\leq \log \frac{4Q+1}{2Q+1} \leq 1 \tag{7.60}$$

By [34, Theorem 1], we can achieve the sum secrecy rate of

$$\sup\left(R_1 + R_2\right) \geq I(V; Y_{1a}, Y_{1b}) - I(V; Y_{2a}, Y_{2b}) \tag{7.61}$$

$$\geq \frac{1-\delta}{2} \log P + o(\log P) \tag{7.62}$$

for any $\delta \geq 0$, which implies that we can achieve 1 sum s.d.o.f. This means that by joint encoding across component channels, we achieve 1 sum s.d.o.f. outperforming optimum independent encoding, which can at most achieve $\frac{2}{3}$ sum s.d.o.f.

7.4.2 Separability in s.d.o.f. for Almost All Channel Gains

Although the Gaussian MAC wiretap channel is not always separable, the special construction provided in the last subsection is not "general", i.e., for almost all channel gains, the constraints in (7.47) are never met. Based on this observation, we show that the s.d.o.f. region of the parallel Gaussian MAC wiretap channel is separable for almost all channel gains.

From Chapter 4, the s.d.o.f. regions of the component Gaussian MAC wiretap channels are identical, i.e., $D_{s,(a)} = D_{s,(b)}$, and

$$D_{s,(a)} = \{(d_1, d_2) : \ 2d_1 + d_2 \leq 1, \ d_1 + 2d_2 \leq 1\} \tag{7.63}$$

Therefore, it suffices to show that for the overall parallel Gaussian MAC channel the s.d.o.f. region is

$$D_s = \{(d_1, d_2) : \ 2d_1 + d_2 \leq 2, \ d_1 + 2d_2 \leq 2\} \tag{7.64}$$

The achievability follows from Chapter 4 for almost all channel gains. In the achievability, we scale the power in each component channel, to meet the overall power constraint; however, this does not affect the s.d.o.f. calculations.

For the converse, we first *flatten* the parallel channel by concatenating the channel inputs and outputs of component channels into $2n$-length vectors. Instead of studying the parallel channel in n channel uses, we study the *flat channel* in $2n$ channel uses. The power constraint remains the same over $2n$ channel uses. In

addition, since introducing correlation in time and in component channels has the same effect, the flat channel must have the same converse as the original one.

Then, similar to the steps in Chapter 2, (2.202)-(2.211), we have

$$n(R_1 + R_2) \leq h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \mathbf{Y}_1, \mathbf{Y}_2) - h(\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2 | \mathbf{Y}_1, \mathbf{Y}_2) - h(\mathbf{Y}_2) + nc_{67} \tag{7.65}$$

where vectors in bold-face are $2n$-length vectors. The components of $2n$-vectors $\tilde{\mathbf{X}}_j$, for $j = 1, 2$, are $\tilde{X}_{ji} = X_{ji} + \tilde{N}_{ji}$, for $i = 1, \ldots, 2n$. Here, the sequence $\tilde{N}_j^{2n}$ is i.i.d. over time, is independent of all other random variables, and $\tilde{N}_{ji}$ is a Gaussian random variable with zero-mean and variance σ_{ji}^2, such that

$$\sigma_{ji}^2 < \min \left\{ \frac{1}{h_{ja}^2}, \frac{1}{g_{ja}^2}, \frac{1}{h_{jb}^2}, \frac{1}{g_{jb}^2} \right\} \tag{7.66}$$

Then, all the remaining steps in Chapter 2 follow, and we have

$$nR_i + nR_1 + nR_2 \leq h(Y_1^{2n}) + nc_{68} \leq \left(\frac{2n}{2} \log P \right) + nc_{69} \tag{7.67}$$

for $i = 1, 2$. This implies

$$2d_1 + d_2 \leq 2, \quad \text{and} \quad d_1 + 2d_2 \leq 2 \tag{7.68}$$

which completes the proof of the converse for this case.

7.5 Conclusions

In this chapter, we showed that the parallel MAC wiretap channel is not always separable by providing a specific example in which the sum secrecy rate by joint encoding over parallel channels outperforms the best rate achievable by individually optimal encoding for each component channel. Then, we showed that the parallel Gaussian MAC wiretap channel is inseparable in general as well. Finally, we showed, from a s.d.o.f. point of view, that the parallel Gaussian MAC wiretap channel is separable almost surely, however, separability in s.d.o.f. is weaker than separability in secrecy capacity.

Chapter 8

Secrecy Games on the One-Sided Interference Channel

8.1 Introduction

An interesting observation made in Chapter 2 is that in the case of two-user Gaussian IC with confidential messages, in order to achieve the optimum sum s.d.o.f., each transmitter jams its own receiver to protect the message of the other transmitter. This phenomenon has also appeared in other multi-transmitter scenarios, such as the K-user MAC wiretap channel and the K-user IC with secrecy constraints. In order to investigate this behavior in depth, in this chapter, we focus on the two-user one-sided IC with confidential messages. In this IC, in addition to the usual selfishness of the users, the relationship between the two pairs of users is further adversarial in the sense of both receivers' desires to eavesdrop on the communication of the other pair. We develop a game-theoretic model to study the information-theoretic secure communications in this setting. We first start with a game-theoretic model where each pair's payoff is their own secrecy rate. The analysis of the binary deterministic IC with this payoff function shows that self-jamming of a transmitter, which injures the eavesdropping ability of its own receiver, is not excluded by the Nash equilibria. We propose a refinement for the payoff function by explicitly accounting for the desire of the receiver to eavesdrop on the other party's communication. This payoff function captures the adversarial relationship between the two pairs of users better.

We determine the Nash equilibria for the binary deterministic channel for both payoff functions.

8.2 Problem Formulation

We consider a two-user one-sided IC, where each transmitter is free to choose a transmission strategy, which is defined as follows.

Definition 8.1 (Strategy s_i) *is the encoding method at transmitter i, such that:*

- *the number of information bits of equiprobable messages W_i is $\log(M_i)$, and the block length of codewords is n;*
- *the stochastic encoding function $f_i : \{1, 2, \cdots, M_i\} \to C_i$ maps the message w_i to an n-length codeword x_i^n which belongs to the codebook C_i;*
- *the corresponding rate of this encoder is $R_i = \frac{\log(M_i)}{n}$.*

We assume that the receiver i performs maximum-likelihood decoding on the received signal to get an estimate of the message $\hat{w}_i$. We denote the resulting probability of error as $P_{e,i} = P[W_i \neq \hat{W}_i]$. The decoding error probability $P_{e,i}$ is jointly determined by both strategies s_1 and s_2 due to interference. To characterize information-theoretic secrecy, we define the measure of information leakage of transmitter i as

$$L_i = \frac{1}{n} I(W_i; Y_j^n) \tag{8.1}$$

where $j = \bar{i}$, i.e., $i = 1, j = 2$ or $i = 2, j = 1$, and Y_j^n is the n-length symbol observed at receiver j.

Then, for any fixed threshold $\epsilon > 0$, which is small enough, given s_1 and s_2, we define the payoff of each transmitter as

$$\pi_i(s_1, s_2) = \begin{cases} R_i, & P_{e,i} \leq \epsilon \text{ and } L_i \leq \epsilon \\ 0, & \text{otherwise} \end{cases} \tag{8.2}$$

for $i = 1, 2$. It is important to emphasize that, as defined above, s_1 and s_2 jointly determine the payoff π_i of transmitter i. In order to improve π_i, transmitter i can deviate from s_i to any other strategy s_i', and the only criteria for this improvement are $P_{e,i}$ and L_i, not $P_{e,j}$ or L_j. This implies that such a deviation may affect the performance of the other transmitter j. To model the behavior of transmitters, who have the freedom to choose their strategies, it is reasonable to assume that each transmitter is selfish. Furthermore, each transmitter i is rational and intelligent, i.e., its objective is to find the best strategy s_i to maximize corresponding payoff π_i (given the other transmitter's strategy s_j), and each transmitter understands the situation, including the fact that another transmitter is also an intelligent rational decision maker.

Based on the above consideration and assumptions, the definition of the Nash equilibrium secrecy rate region $C_{s,NE}$ is given as follows:

Definition 8.2 (Nash equilibrium secrecy rate region) *Nash equilibrium secrecy rate region $C_{s,NE}$ is the closure of all rate pairs (R_{s1}, R_{s2}) such that, there exists a $\bar{\epsilon} > 0$ such that for all $\epsilon \in (0, \bar{\epsilon})$, there exists a strategy pair (s_1^*, s_2^*) which achieves the payoffs $\pi_i(s_1^*, s_2^*) = R_{si}$ for $i = 1, 2$ and s_i^* is the best response to s_j^* in*

the sense that

$$\pi_i(s_i^*, s_j^*) \geq \pi_i(s_i', s_j^*), \quad \forall s_i' \tag{8.3}$$

By this definition, if any transmitter i unilaterally attempts to deviate from the equilibrium strategy while the other transmitter j's strategy remains the same, the corresponding payoff π_i of transmitter-receiver pair i will not be improved, i.e., there is no incentive for each transmitter to deviate from the equilibrium strategy. Such a secrecy rate pair achieved by the best response strategy pair is an equilibrium in the secrecy rate region.

8.3 Binary Deterministic Channels with Confidential Messages

In this section, we consider the binary deterministic one-sided IC with confidential messages to analyze the Nash equilibrium secrecy rate region with the payoff function defined above. The channel model shown in Figure 8.1 is:

$$Y_{1a} = X_{1a}, \qquad Y_{1b} = X_{1b} \tag{8.4}$$

$$Y_{2a} = X_{1b} \oplus X_{2a}, \quad Y_{2b} = X_{2b} \tag{8.5}$$

where $\oplus$ is modulo-2 addition. This is a simple example to analyze the equilibrium. However, it is not difficult to see that it can be easily extended to general one-sided binary deterministic channels which are used in [84].

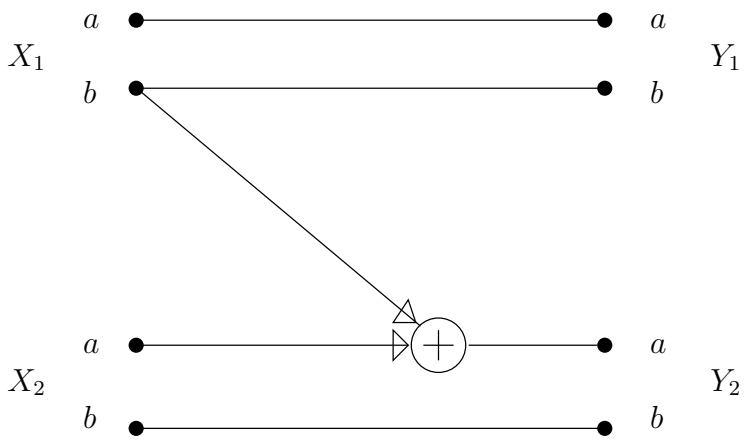


Figure 8.1: Binary deterministic one-sided IC with confidential messages.

The capacity region of this channel is [58]

$$C = \{(R_1, R_2) | R_1 \leq 2, R_2 \leq 2, R_1 + R_2 \leq 3\} \tag{8.6}$$

In fact, it is easy to check that each corner point of this pentagon is an achievable *secrecy* rate pair also, and therefore, the unconstrained capacity region in (8.6) is equal to the secrecy capacity region. In addition, if we do not consider the secrecy constraint L_i in the payoff function, then [76] already found the unique Nash equilibrium rate pair (R_1^*, R_2^*) to be $R_1^* = 2$ and $R_2^* = 1$. The explanation for this is as follows: Since there is no secrecy constraint, transmitter 1 can always transmit unencoded messages on both sub-channels with maximum rate 2 bits, and due to the interference, transmitter 2 can only achieve 1 bit as the maximum rate. It can be shown that neither user will have any incentive to deviate from this point, and there exists no other such point. The capacity region is shown in Figure 8.2. The unique Nash equilibrium with no secrecy constraints is shown with a filled circle.

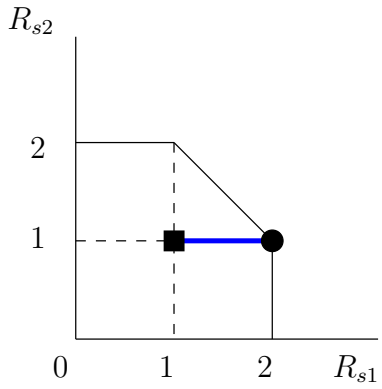


Figure 8.2: The (secrecy) capacity region. Unique Nash equilibrium point (filled circle) and Nash equilibrium secrecy rate region (blue wide line including the two end points) with the first payoff function, and the unique Nash equilibrium secrecy rate point (filled square) for the second payoff function.

With secrecy constraints, we will show that the Nash equilibrium secrecy rate region is not a unique point. We give the precise form of the Nash equilibrium secrecy rate region of this channel with the following theorem.

Theorem 8.1 (Nash equilibrium secrecy rate region $C_{s,NE}$)

$$C_{s,NE} = \{(R_{s1}, R_{s2}) | R_{s1} \in [1, 2], R_{s2} = 1\} \tag{8.7}$$

Proof: First, note that $R_{s1} \geq 1$ and $R_{s2} \geq 1$. This is because, given any strategy s_2, transmitter 1 can at least employ independent encoding on two sub-channels and transmit unencoded information on sub-channel a with zero decoding error probability and without any information leakage. The same argument can be applied to sub-channel b of transmitter 2. Next, note that $R_{s1} \leq 2$ is trivial. To prove $R_{s2} = 1$, it suffices to prove that $R_{s2} \leq 1$.

Assume that (s_1, s_2) is an equilibrium strategy, which is the best response to

each other and public to both transmitter-receiver pairs. The reliable transmission rate for transmitter 2 is upper bounded by

$$nR_{s2} = nR_2 \tag{8.8}$$

$$\leq \max_{P(X_2^n)} I(X_2^n; Y_2^n) \tag{8.9}$$

$$\leq \max_{P(X_2^n)} [I(X_{2a}^n; Y_{2a}^n) + H(X_{2b}^n)] \tag{8.10}$$

where the inequality in (8.10) is proved in Appendix 8.6.1 with $X_{2b} = Y_{2b}$. This could always (but not limited to) be achieved by independently encoding on both sub-channels. The necessary condition for the equality in (8.10) is

$$I(Y_{2a}^n; X_{2b}^n) = 0 \tag{8.11}$$

Considering s_1, the channel $X_1 \to Y_1, Y_2$ is a degraded wiretap channel with the following upper bound for the secrecy rate:

$$nR_{s1} \leq \max_{P(X_1^n)} I(X_1^n; Y_1^n) - I(X_1^n; Y_2^n) \tag{8.12}$$

The difference can be maximized by

$$
\begin{aligned}
& I(X_1^n; Y_1^n) - I(X_1^n; Y_2^n) \\
& \quad \leq H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_1^n; Y_2^n) && (8.13) \\
& \quad = H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_{1a}^n, X_{1b}^n; Y_2^n) && (8.14) \\
& \quad = H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_{1b}^n; Y_2^n) - I(X_{1a}^n; Y_2^n | X_{1b}^n) && (8.15) \\
& \quad = H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_{1b}^n; Y_2^n) && (8.16) \\
& \quad = H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_{1b}^n; Y_{2a}^n) - I(X_{1b}^n; Y_{2b}^n | Y_{2a}^n) && (8.17)
\end{aligned}
$$

where (8.13) is proven in Appendix with $X_{1a} = Y_{1a}$, (8.16) is due to the Markov chain $X_{1a}^n \to X_{1b}^n \to Y_2^n$. The fourth item in (8.17) is equal to

$$
\begin{aligned}
I(X_{1b}^n; Y_{2b}^n | Y_{2a}^n) &= H(Y_{2b}^n | Y_{2a}^n) - H(Y_{2b}^n | X_{1b}^n, Y_{2a}^n) && (8.18) \\
&= H(X_{2b}^n | Y_{2a}^n) - H(X_{2b}^n | X_{1b}^n, Y_{2a}^n) && (8.19) \\
&= H(X_{2b}^n) - H(X_{2b}^n | X_{1b}^n, Y_{2a}^n) && (8.20) \\
&= H(X_{2b}^n) - H(X_{2b}^n | X_{2a}^n, Y_{2a}^n) && (8.21) \\
&= H(X_{2b}^n) - H(X_{2b}^n | X_{2a}^n) && (8.22) \\
&= I(X_{2a}^n; X_{2b}^n) && (8.23)
\end{aligned}
$$

where (8.20) is due to (8.11) and (8.22) is due to the Markov chain $X_{2b}^n \to X_{2a}^n \to Y_{2a}^n$.

Substituting (8.23) in (8.17), we get

$$
\begin{aligned}
& I(X_1^n; Y_1^n) - I(X_1^n; Y_2^n) \\
& \quad \leq H(X_{1a}^n) + I(X_{1b}^n; Y_{1b}^n) - I(X_{1b}^n; Y_{2a}^n) - I(X_{2a}^n; X_{2b}^n) && (8.24) \\
& \quad = H(X_{1a}^n) + H(X_{1b}^n) - H(Y_{2a}^n) + H(Y_{2a}^n | X_{1b}^n) - I(X_{2a}^n; X_{2b}^n) && (8.25) \\
& \quad = H(X_{1a}^n) + H(X_{1b}^n) - H(Y_{2a}^n) + H(X_{2a}^n) - I(X_{2a}^n; X_{2b}^n) && (8.26) \\
& \quad = H(X_{1a}^n) + H(X_{1b}^n | X_{2a}^n) - H(Y_{2a}^n) + H(X_{2a}^n | X_{2b}^n) && (8.27) \\
& \quad = H(X_{1a}^n) + H(Y_{2a}^n | X_{2a}^n) - H(Y_{2a}^n) + H(X_{2a}^n | X_{2b}^n) && (8.28) \\
& \quad = H(X_{1a}^n) - I(X_{2a}^n; Y_{2a}^n) + H(X_{2a}^n | X_{2b}^n) && (8.29) \\
& \quad \leq H(X_{1a}^n) + H(X_{2a}^n | X_{2b}^n) && (8.30) \\
& \quad \leq n + H(X_{2a}^n | X_{2b}^n) && (8.31)
\end{aligned}
$$

where (8.26) is due to $H(Y_{2a}^n|X_{1b}^n) = H(X_{2a}^n|X_{1b}^n) = H(X_{2a}^n)$ and (8.30) is due to $I(X_{2a}^n; Y_{2a}^n) \geq 0$. When s_2 is given, $H(X_{2a}^n|X_{2b}^n)$ is a fixed item for transmitter 1. (8.31) could always (but not limited to) be achieved by a wiretap code with independent and uniform distributions for X_{1a}^n and X_{1b}^n. The necessary condition is

$$I(X_{2a}^n; Y_{2a}^n) = 0 \tag{8.32}$$

which means that, under the condition that transmitter 1 achieves the maximum secrecy rate, the upper bound for the reliable transmission rate (8.10) for transmitter

2 is only

$$nR_{s2} \leq \max_{P(X_2^n)} [I(X_{2a}^n; Y_{2a}^n) + H(X_{2b}^n)] \tag{8.33}$$

$$\leq \max_{P(X_2^n)} H(X_{2b}^n) \tag{8.34}$$

$$\leq n \tag{8.35}$$

which is achievable. Therefore, the reliable secrecy rate R_{s2} is upper bounded by 1.

Finally, we prove the achievability here. Assume that s_2 is the following: transmit unencoded information on sub-channel b, but pure noise with input distribution $P(X_{2a} = 0) = 1 - P(X_{2a} = 1) = p$, for some $0 \leq p \leq 1/2$ on sub-channel a. Then, $R_{s2} = 1$.

Given s_2, the channel $X_1 \to Y_1 \to Y_2$ is a degraded wiretap channel with the optimal encoder s_1^* which independently encodes the signals on two sub-channels. On sub-channel a, unencoded message is transmitted, and on sub-channel b, encoder transmits the secure message via a wiretap code with the optimal distribution $P^*(X_{1b} = 0) = 1/2$. It is straightforward to see that s_1^* and s_2 jointly determine the achievable secrecy rate for transmitter 1 as $R_{s1a} + R_{s1b} = 1 + I(X_{1b}; Y_{1b}) - I(X_{1b}; Y_{2a}) = 1 + \{1 - [1 - h_2(p)]\} = 1 + h_2(p)$, where h_2 is the binary entropy function.

It is easy to check that, to maximize the payoff π_2, s_2 is also the best response s_2^* to s_1^*, i.e., (s_1^*, s_2^*) are best responses to each other, and therefore form an equilibrium,

by definition. Then, the corresponding payoffs are

$$R_{s1} = 1 + h_2(p), \quad R_{s2} = 1 \tag{8.36}$$

where $0 \leq p \leq 1/2$, which means $R_{s1} \in [1, 2]$ and $R_{s2} = 1$. The Nash equilibrium line is shown as the blue line going from $[1, 1]$ to $[2, 1]$ in Figure 8.2. $\square$

8.4 Refinement of the Equilibrium

Achieving the Nash equilibrium pairs in the previous section required transmitter 2 to transmit artificial noise on sub-channel a to self-jam its own receiver. Since all of the equilibrium points yield the same payoff for pair 2, a rational transmitter 2 would rather help its receiver eavesdrop on the other pair than self-jam its own receiver. However, the self-jamming scheme is not excluded by the Nash equilibrium in Section 8.3.

We now modify the payoff function of the game in order for the resulting Nash equilibrium to reflect the adversarial relationship between the two pairs of users better in this IC with confidential messages. Here we explicitly account for the desire of the receiver to eavesdrop on the other party's communication by including the leakage of the other user's message in the payoff function of a user together with its own secrecy rate.

Definition 8.3 (Refinement of the game and equilibria) *The equilibrium secrecy rate region $\tilde{C}_{s,NE}$ is the closure of all rate pairs (R_{s1}, R_{s2}) such that there exists*

a $\bar{\epsilon} > 0$ such that for all $\epsilon \in (0, \bar{\epsilon})$, there exists a strategy pair (s_1^*, s_2^*) which achieves the payoffs $\pi_i(s_1^*, s_2^*) = R_{si}$ for $i = 1, 2$, and s_i^* is the best response to s_j^* in the sense that

$$\pi_i(s_i^*, s_j^*) \geq \pi_i(s_i', s_j^*), \quad \forall s_i' \tag{8.37}$$

In addition, (s_1^*, s_2^*) is also the best responses with respect to the following payoff

$$\tilde{\pi}_i(s_i, s_j) = \begin{cases} R_i + \beta \cdot L_j, & P_{e,i} \leq \epsilon \text{ and } L_i \leq \epsilon \\ 0, & \text{otherwise} \end{cases} \tag{8.38}$$

for any $\beta > 0$ and for all $i = 1, 2$ with $j = \bar{i}$.

We emphasize a few points here. First, any rate pair in $\tilde{C}_{s,NE}$ must also belong to $C_{s,NE}$. Secondly, we include the information leakage L_j defined in (8.1) into the definition of $\tilde{\pi}_i$ in addition to the R_i to further limit the rational behavior of the selfish transmitters and receivers, i.e., eavesdropping is at least not bad for the receiver. Lastly, for any rate pair $(R_{s1}, R_{s2}) \in \tilde{C}_{s,NE}$, by the definition of payoff π, there must exist a strategy pair which does not violate the secrecy constraint even though it is also an equilibrium with respect to the payoff $\tilde{\pi}$, which includes the information leakage in the definition.

We again examine the channel in Section 8.3 to illustrate the idea of the refined payoff function and the resulting equilibrium. With the new definition, the equilibrium rate pairs in the secrecy rate region are modified as stated in the following theorem.

Theorem 8.2 (Nash equilibrium secrecy rate region $\tilde{C}_{s,NE}$)

$$\tilde{C}_{s,NE} = \{(1,1)\} \tag{8.39}$$

Proof: $(1,1) \in \tilde{C}_{s,NE}$. This is because each transmitter transmits unencoded information on the private sub-channel, e.g., sub-channel a of transmitter 1 and sub-channel b of transmitter 2. Transmitter 1 sends pure noise with uniform distribution on sub-channel b. Transmitter 2 keeps silent. Here by silence, we mean that transmitter 2 sends a constant symbol which is known to everyone in this network, i.e., the corresponding rate is zero. Since no information is transmitted on the interfered sub-channel, there is no information leakage which implies that $(1,1) \in \tilde{C}_{s,NE}$.

$(2,1) \notin \tilde{C}_{s,NE}$. The only scheme to achieve this rate pair is that transmitter 1 transmits unencoded information on both sub-channels as s_1. And, for s_2 transmitter 2 transmits unencoded information on sub-channel b but sends pure noise (uniform distribution) on sub-channel a. Obviously, if transmitter 2 deviates from s_2 to one special strategy s_2' which keeps silent on sub-channel a, then the payoff $\tilde{\pi}_2$ will increase due to the information leakage L_1.

$(R_{s1},1) \notin \tilde{C}_{s,NE}$ for any $R_{s1} > 1$. We prove this by contradiction. Assume that this rate pair is in the set $\tilde{C}_{s,NE}$ and is achieved by some strategy pair (s_1, s_2). $R_{s1} > 1$ means that $H(W_1) \geq n(1+\triangle)$ for a positive constant value $\triangle > 0$. It is not difficult to see that transmitter 2 could always deviate to s_2', i.e., keeping silent on sub-channel a, then the secrecy rate R_{s2} remains the same but the information

leakage increases:

$$nL_1 = I(W_1; Y_2^n) = I(W_1; Y_{2a}^n) \tag{8.40}$$

$$= I(W_1; X_{1b}^n) \tag{8.41}$$

$$= I(W_1; Y_{1b}^n) \tag{8.42}$$

$$= I(W_1; Y_{1a}^n, Y_{1b}^n) - I(W_1; Y_{1a}^n | Y_{1b}^n) \tag{8.43}$$

$$= H(W_1) - H(W_1 | Y_{1a}^n, Y_{1b}^n) - I(W_1; Y_{1a}^n | Y_{1b}^n) \tag{8.44}$$

$$\geq H(W_1) - I(W_1; Y_{1a}^n | Y_{1b}^n) - n\epsilon' \tag{8.45}$$

$$\geq n(1 + \triangle) - H(Y_{1a}^n) - n\epsilon' \tag{8.46}$$

$$\geq n(\triangle - \epsilon') \tag{8.47}$$

where by Fano's inequality, $H(W_1|Y_{1a}^n, Y_{1b}^n) \leq n\epsilon'$ for some negligible ϵ'. Hence, the payoff $\tilde{\pi}_2(s_1, s_2') = R_{s2} + \beta L_1 > R_{s2} = \tilde{\pi}_2(s_1, s_2)$ which means that s_2 is not the best response to s_1 with respect to $\tilde{\pi}$, which implies that $(R_{s1}, 1) \notin \tilde{C}_{s,NE}$.

Therefore, we conclude that the Nash equilibrium contains only a single rate pair: $\tilde{C}_{s,NE} = \{(1, 1)\}$, which is shown with the filled square in Figure 8.2. □

This theorem shows that all the secrecy rate pairs in the set $C_{s,NE}$ but not in the set $\tilde{C}_{s,NE}$ are only achieved by the strategies employing self-jamming. The modified definition for the payoff and the resulting equilibrium are essential to rule out such rate pairs.

8.5 Conclusions

In this chapter, we studied the one-sided IC with confidential messages. To model the adversarial relationship between two transmitter-receiver pairs, we considered a scenario where each transmitter has the freedom to choose any strategy, and the only objective is to maximize a certain given payoff. To this end, we formally developed a game theory model and studied its equilibria. When we defined the payoff function to be only the secrecy rate of each user, the resulting Nash equilibria did not reject the behavior of self-jamming, in which a transmitter jams its own receiver. To improve the modeling of the adversarial relationship between the two pairs better, we defined a refined payoff function to explicitly incorporate the receiver's desire to eavesdrop on the other user. The equilibrium achieved with this payoff function excluded the possibility of self-jamming, for the deterministic binary channel considered here.

8.6 Appendix

8.6.1 Upper Bound for Independent Parallel Channel

For independent parallel channel $P(Y_\alpha, Y_\beta|X_\alpha, X_\beta) = P(Y_\alpha|X_\alpha)P(Y_\beta|X_\beta)$ with $Y_\beta = X_\beta$, the upper bound of the mutually information $I(X;Y)$ is the following:

$$
\begin{aligned}
I(X;Y) &= I(X_\alpha, X_\beta; Y_\alpha, Y_\beta) && (8.48)\\
&= I(X_\beta; Y_\alpha, Y_\beta) + I(X_\alpha; Y_\alpha, Y_\beta|X_\beta) && (8.49)\\
&= H(X_\beta) + I(X_\alpha; Y_\alpha|X_\beta) && (8.50)\\
&= H(X_\beta) + H(Y_\alpha|X_\beta) - H(Y_\alpha|X_\alpha, X_\beta) && (8.51)\\
&\leq H(X_\beta) + H(Y_\alpha) - H(Y_\alpha|X_\alpha, X_\beta) && (8.52)\\
&= H(X_\beta) + H(Y_\alpha) - H(Y_\alpha|X_\alpha) && (8.53)\\
&= H(X_\beta) + I(X_\alpha; Y_\alpha) && (8.54)
\end{aligned}
$$

where the (8.53) is due to the Markov chain $X_\beta \to X_\alpha \to Y_\alpha$. The equality holds iff $I(Y_a; X_\beta) = 0$.

Chapter 9

Conclusions

In this dissertation, we determined the s.d.o.f. of several different wireless communication channel models, and provided the corresponding optimal signalling schemes at high SNR.

In Chapter 2, we determined the s.d.o.f. of several fundamental channel models in one-hop wireless networks. We first considered the Gaussian wiretap channel with one helper. While the helper needs to create interference at the eavesdropper, it should not create too much interference at the legitimate receiver. Our approach is based on understanding this trade-off that the helper needs to strike. To that purpose, we developed an upper bound that relates the entropy of the cooperative jamming signal from the helper and the message rate. In addition, we developed an achievable scheme based on real interference alignment which aligns the cooperative jamming signal from the helper in the same *dimension* as the message signal. This ensures that the information leakage rate is upper bounded by a constant which does not scale with the power. In addition, to help the legitimate user decode the message, our achievable scheme renders the message signal and the cooperative jamming signal distinguishable at the legitimate receiver. This essentially implies that the message signal can *occupy* only half of the available space in terms of the d.o.f. We showed that the exact s.d.o.f. of the Gaussian wiretap channel with one

helper is $\frac{1}{2}$ by these matching achievability and converse proofs. We then generalized our achievability and converse techniques to the Gaussian wiretap channel with M helpers, Gaussian BC with confidential messages and helpers, two-user Gaussian IC with confidential messages and helpers, and K-user Gaussian MAC wiretap channel in this chapter. In the multiple-message settings, transmitters needed to send a mix of their own messages and cooperative jamming signals, which can be interpreted as applying *channel prefixing*. We determined the exact sum s.d.o.f. of all of these system models. In particular, we showed that the s.d.o.f. of a Gaussian wiretap channel with M helpers is $\frac{M}{M+1}$, and the sum s.d.o.f. of a K-user Gaussian MAC wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$.

In Chapter 3, we studied secure communications in K-user Gaussian interference networks, and addressed three important channel models: IC-EE, IC-CM and their combination IC-CM-EE in a unified framework. We showed that, for all three models, the sum s.d.o.f. is exactly $\frac{K(K-1)}{2K-1}$. Our achievability is based on structured signalling, structured cooperative jamming, channel prefixing and asymptotic real interference alignment. The key insight of the achievability is to carefully design the structure of all of the signals at the transmitters so that the signals are received at both legitimate receivers and eavesdroppers in the most desirable manner from a secure communication point of view. In particular, cooperative jamming signals protect information carrying signals via alignment, and the information carrying signals are further aligned to maximize s.d.o.f.

In Chapter 4, we determined the *entire s.d.o.f. regions* of the K-user MAC wiretap channel, K-user IC-EE, K-user IC-CM, and K-user IC-CM-EE. The con-

verse for the MAC directly followed from the results in Chapter 2. The converse for the IC was shown to be dominated by secrecy constraints and interference constraints in different parts. To show the tightness and achieve the regions characterized by the converses, we provided a general method to investigate this class of channels, whose s.d.o.f. regions have a polytope structure. We provided the equivalence between the extreme points in the polytope structure and the rank of sub-matrices containing all active upper bounds associated with each extreme point. Then, we achieved each extreme point by relating it to a specific channel model. More specifically, each extreme point of the MAC region can be achieved by an m-user MAC wiretap channel with $K-m$ helpers, i.e., by setting $K-m$ users' secure rates to zero and utilizing them as pure (structured) cooperative jammers. On the other hand, each asymmetric extreme point of the IC region can be achieved by a $(p+1)$-user IC-CM with m helpers, and N external eavesdroppers.

In Chapter 5, we considered the sum s.d.o.f. of two-unicast layered wireless networks. We used the setting in [64] and studied the cases in A, A', B, B' and C separately to incorporate security in addition to reliability. The major challenge was in cases A and A', where the sum d.o.f. is 1, due to the fact that both destination nodes can decode the message signals. While this is inconsequential for the reliability problem in [64], it is a major problem when security is considered. To overcome this problem, we classified layered wireless networks into more detailed sub-cases, and in all sub-cases proposed modified achievable schemes that guarantee both reliability and security. In almost all sub-cases, we utilized the cooperative jamming and interference neutralization techniques to design an appropriate achievable scheme.

A remaining challenge was a special configuration, where all of the nodes in the last layer before the destination layer were allowed to send only independent signals. We reduced the layered networks in this category into equivalent channel models and determined their s.d.o.f. using the results in previous chapters. As a result, we showed that all networks in cases A and A' have sum s.d.o.f. of $0, \frac{2}{3}$, or 1. We proposed modified schemes to achieve 2 sum s.d.o.f. for cases B and B' (which included the achievable scheme for the $2 \times 2 \times 2$ interference networks), and $\frac{3}{2}$ sum s.d.o.f. for case C.

In Chapter 6, we studied the Gaussian wiretap channel with M helpers without any eavesdropper CSI at the transmitters. We proposed an achievable scheme that achieves a s.d.o.f. of $\frac{M}{M+1}$, which is the same as the s.d.o.f. achieved when the transmitters had perfect eavesdropper CSI. The new achievability scheme is based on real interference alignment and *blind* cooperative jamming. While in Chapter 2 we aligned cooperative jamming signals with the information symbols at the eavesdropper to protect the information symbols, which required eavesdropper CSI, in Chapter 6 we used one more cooperative jamming signal to span the *entire space* at the eavesdropper to protect the information symbols. In addition, we aligned all of the cooperative jamming signals in the same dimension at the legitimate receiver, in order to occupy the smallest space at the legitimate receiver to allow for the decodability of the information symbols. Therefore, we aligned the cooperative jamming signals carefully only at the legitimate receiver, which required only the legitimate receiver's CSI at the transmitters.

In Chapter 7, we showed that the parallel MAC wiretap channel is not always

separable by providing a specific example in which the sum secrecy rate by joint encoding over parallel channels outperforms the best rate achievable by individually optimal encoding for each component channel. Then, we showed that the parallel Gaussian MAC wiretap channel is inseparable in general as well. Finally, we showed, from a s.d.o.f. point of view, that the parallel Gaussian MAC wiretap channel is separable almost surely, however, separability in s.d.o.f. is weaker than separability in secrecy capacity.

In Chapter 8, we studied the one-sided IC with confidential messages. To model the adversarial relationship between two transmitter-receiver pairs, we considered a scenario where each transmitter has the freedom to choose any strategy, and the only objective is to maximize a certain given payoff. To this end, we formally developed a game theory model and studied its equilibria. When we defined the payoff function to be only the secrecy rate of each user, the resulting Nash equilibria did not reject the behavior of self-jamming, in which a transmitter jams its own receiver. To improve the modeling of the adversarial relationship between the two pairs better, we defined a refined payoff function to explicitly incorporate the receiver's desire to eavesdrop on the other user. The equilibrium achieved with this payoff function excluded the possibility of self-jamming, for the deterministic binary channel considered here.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, October 1949.

[2] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, January 1975.

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

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[5] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[6] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, October 2009.

[7] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[8] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP Journal on Wireless Communications and*

Networking, Special Issue on Wireless Physical Layer Security, vol. 2009, no. 824235, March 2009.

[9] ——, "On secure broadcasting," in *42nd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, October 2008.

[10] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secure broadcasting: The secrecy rate region," in *46th Annual Allerton Conference on Communications, Control and Computing*, Monticello, IL, September 2008.

[11] E. Ekrem and S. Ulukus, "Secure broadcasting using multiple antennas," *Journal of Communications and Networks*, vol. 12, no. 5, pp. 411–432, October 2010.

[12] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *43rd Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2009.

[13] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5681–5694, September 2011.

[14] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, December 2008.

[15] ——, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[16] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

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

[18] E. Ekrem and S. Ulukus, "Cooperative secrecy in wireless communications," *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds., Springer-Verlag, 2009.

[19] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. Inf. Theory, Special issue on Information Theoretic Security*, submitted Nov 2006. Also available at [arXiv:cs/0611125v7].

[20] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.

[21] M. Yuksel and E. Erkip, "The relay channel with a wiretapper," in *41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2007.

[22] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[23] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, August 2010.

[24] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, January 2011.

[25] Y. Liang, G. Kramer, H. V. Poor, and S. S. (Shitz), "Compound wiretap channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, vol. 2009, no. 142374, March 2009.

[26] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5681–5698, September 2012.

[27] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, June 2011.

[28] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *IEEE Information Theory Workshop on Networking and Information Theory*, Volos, Greece, June 2009.

[29] J. Xie and S. Ulukus, "Real interference alignment for the K-user Gaussian interference compound wiretap channel," in *48th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2010.

[30] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, April 2014.

[31] X. He, "Cooperation and information theoretic security in wireless networks," Ph.D. Dissertation, Pennsylvania State University, 2010.

[32] M. Nafea and A. Yener, "How many antennas does a cooperative jammer need for achieving the degrees of freedom of multiple antenna Gaussian channels in the presence of an eavesdropper?" in *51st Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 2013.

[33] ——, "Degrees of freedom of the single antenna gaussian wiretap channel with a helper irrespective of the number of antennas at the eavesdropper," in *IEEE GlobalSIP Symposium on Cyber-Security and Privacy, GlobalSIP'13*, Austin, TX, December 2013.

[34] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," *IEEE Trans. Inf. Theory*, submitted March 2010. Also available at [arXiv:1003.0729].

[35] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, March 2012.

[36] T. Gou and S. A. Jafar, "On the secure Degrees of Freedom of wireless X networks," in *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

[37] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "The Gaussian wiretap channel with a helping interferer," in *IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008.

[38] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap

channel with helpers," in *50th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 2012.

[39] ——, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," in *IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013.

[40] ——, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. on Information Theory*, to appear. Also available at [arXiv:1209.5370].

[41] ——, "Unified secure DoF analysis of K-user Gaussian interference channels," in *IEEE International Symposium on Information Theory*, Istanbul, Turkey, July 2013.

[42] ——, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," submitted to *IEEE Trans. on Information Theory*, May 2013. Also available at [arXiv:1305.7214].

[43] ——, "Secure degrees of freedom region of the Gaussian multiple access wiretap channel," in *47th Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, November 2013.

[44] ——, "Secure degrees of freedom region of wireless networks: The polytope structure," submitted to *IEEE Trans. on Information Theory*, April 2014.

[45] ——, "On the sum secure degrees of freedom of two-unicast layered wireless networks," in *IEEE International Symposium on Information Theory*, Cambridge, MA, July 2012.

[46] ——, "Sum secure degrees of freedom of two unicast layered wireless networks," *IEEE Jour. on Selected Areas in Comm.*, vol. 31, no. 9, pp. 1931–1943, September 2013.

[47] ——, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Conference on Information Sciences and Systems*, Baltimore, MD, March 2013.

[48] ——, "Inseparability of the multiple access wiretap channel," in *IEEE International Symposium on Information Theory*, Honolulu, HI, June 2014.

[49] ——, "Secrecy games on the one-sided interference channel," in *IEEE International Symposium on Information Theory*, St. Petersburg, Russia, July 2011.

[50] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," in *IEEE Globe Telecommunications Conference*, Honolulu, Hawaii, December 2009.

[51] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani, "Real interference alignment with real numbers," *IEEE Trans. Inf. Theory*, submitted August 2009. Also available at [arXiv:0908.1208].

[52] A. S. Motahari, S. Oveis-Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Trans. Inf. Theory*, submitted November 2009. Also available at [arXiv:0908.2282].

[53] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[54] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wireless networks," in *IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[55] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, August 2008.

[56] D. Tse and S. V. Hanly, "Multiaccess fading channels-Part I: Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, November 1998.

[57] B. Grunbaum, *Convex Polytopes*, 2nd ed. Springer, 2003.

[58] A. El Gamal and M. Costa, "The capacity region of a class of deterministic interference channels," *IEEE Trans. Inf. Theory*, vol. 28, no. 2, pp. 343–346, March 1982.

[59] A. B. Carleial, "A case where interference does not reduce capacity," *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 569–570, September 1975.

[60] H. Sato, "On the capacity region of a discrete two-user channel for strong interference," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 377–379, March 1978.

[61] ——, "The capacity of the Gaussian interference channel under strong interference," *IEEE Trans. Inf. Theory*, vol. 27, no. 6, pp. 786–788, November 1981.

[62] N. Liu and S. Ulukus, "The capacity region of a class of discrete degraded interference channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4372–4378, September 2008.

[63] M. A. Maddah-Ali, A. S. Motahari, and A. K. 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.

[64] I. Shomorony and A. S. Avestimehr, "Two-unicast wireless networks: Characterizing the degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 353–383, January 2013.

[65] S. Mohajer, S. N. Diggavi, C. Fragouli, and D. Tse, "Transmission techniques for relay-interference networks," in *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

[66] T. Gou, S. A. Jafar, C. Wang, S. Jeon, and S. Chung, "Aligned interference neutralization and the degrees of freedom of the $2 \times 2 \times 2$ interference channel," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4381–4395, July 2012.

[67] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1568–1571, August 2013.

[68] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.

[69] D. Tse, "Optimal power allocation over parallel Gaussian broadcast channels," in *IEEE International Symposium on Information Theory*, Ulm, Germany, June 1997.

[70] L. Sankar, X. Shang, E. Erkip, and H. V. Poor, "Ergodic two-user interference channels: Is separability optimal?" in *46th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, September 2008.

[71] V. R. Cadambe and S. A. Jafar, "Parallel Gaussian interference channels are not always separable," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3983–3990, September 2009.

[72] H. Sun, C. Geng, and S. A. Jafar, "Topological interference management with alternating connectivity," available at [arXiv:1302.4020].

[73] P. Mukherjee, R. Tandon, and S. Ulukus, "Even symmetric parallel linear deterministic interference channels are inseparable," in *51th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, October 2013.

[74] N. Liu and W. Kang, "The secrecy capacity region of a special class of multiple access channels," in *IEEE International Symposium on Information Theory*, St. Petersburg, Russia, July 2011.

[75] M. Wiese and H. Boche, "An achievable region for the wiretap multiple-access channel with common message," in *IEEE International Symposium on Information Theory*, Cambridge, MA, July 2012.

[76] R. A. Berry and D. Tse, "Shannon meets Nash on the interference channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2821–2836, May 2011.

[77] R. D. Yates, D. Tse, and Z. Li, "Secret communication on interference channels," in *IEEE International Symposium on Information Theory*, Toronto, ON, July 2008.

[78] R. H. Etkin and E. Ordentlich, "The degrees-of-freedom of the K-user Gaussian interference channel is discontinuous at rational channel coefficients," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4932–4946, November 2009.

[79] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[80] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," submitted to *IEEE Trans. Inf. Theory*, Jul. 2010. Also available at [arXiv:1007.4801].

[81] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, August 2013.

[82] M. Padberg, *Linear Optimization and Extensions*, 2nd ed. Springer, 1999.

[83] F. Zhang, *Matrix Theory: Basic Results and Techniques*, 2nd ed. Springer, 2011.

[84] Z. Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *IEEE International Symposium on Information Theory*, Toronto, ON, July 2008.