ABSTRACT

Title of dissertation: SECURITY UNDER IMPERFECT CHANNEL KNOWLEDGE IN WIRELESS NETWORKS

Pritam Mukherjee, Doctor of Philosophy, 2016

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

This dissertation studies physical layer security in wireless networks using an information theoretic framework. The central theme of this work is exploring the effect of delayed or no channel state information (CSI) on physical layer security in various wireless channel models.

We begin with the fast Rayleigh fading wiretap channel, over which a legitimate transmitter wishes to have secure communication with a legitimate receiver in the presence of an eavesdropper. Subject to an average power constraint on the input, and with no CSI at any user, we show that the input distribution that achieves the secrecy capacity for this wiretap channel is discrete with a finite number of mass points. This enables us to evaluate the exact secrecy capacity of this channel numerically.

Next, we consider multi-user models, specifically, the wiretap channel with M helpers, the K-user multiple access wiretap channel, and the K-user interference channel with an external eavesdropper, when no eavesdropper's CSI is available

at the transmitters. In each case, we establish the optimal sum secure degrees of freedom (s.d.o.f.) by providing achievable schemes and matching converses. We show that the unavailability of the eavesdropper's CSI at the transmitter (CSIT) does not reduce the s.d.o.f. of the wiretap channel with helpers. However, there is loss in s.d.o.f. for both the multiple access wiretap channel and the interference channel with an external eavesdropper. In particular, we show that in the absence of eavesdropper's CSIT, the K-user multiple access wiretap channel reduces to a wiretap channel with $(K-1)$ helpers from a sum s.d.o.f. perspective, and the optimal sum s.d.o.f. reduces from $\frac{K(K-1)}{K(K-1)+1}$ to $\frac{K-1}{K}$. For the interference channel with an external eavesdropper, the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{2K-1}$ to $\frac{K-1}{2}$ in the absence of the eavesdropper's CSIT. Our results show that the lack of eavesdropper's CSIT does not have a significant impact on the optimal s.d.o.f. for any of the three channel models, especially when the number of users is large.

We, then, study multiple-input multiple-output (MIMO) multi-user channels. We begin with the case when full CSIT is available. We consider a two-user MIMO multiple access wiretap channel with N antennas at each transmitter, N antennas at the legitimate receiver, and K antennas at the eavesdropper. We determine the optimal sum s.d.o.f. for this model for all values of N and K. We subdivide our problem into several regimes based on the values of N and K, and provide achievable schemes based on real and vector space alignment techniques for fixed and fading channel gains, respectively. To prove the optimality of the achievable schemes, we provide matching converses for each regime. Our results show how the number of eavesdropper antennas affects the optimal sum s.d.o.f. of the multiple access wiretap channel.

In line with the theme of this dissertation, we next consider the MIMO wiretap channel with one helper and the two-user MIMO multiple access channel when no eavesdropper CSIT is available. In each case, the eavesdropper has K antennas while the remaining terminals have N antennas. We determine the optimal sum s.d.o.f. for each channel model for the regime $K \leq N$, and we show that in this regime, the multiple access wiretap channel reduces to the wiretap channel with a helper in the absence of eavesdropper CSIT. For the regime $N \leq K \leq 2N$, we obtain the optimal *linear* s.d.o.f., and show that the multiple access wiretap channel and the wiretap channel with a helper have the same optimal s.d.o.f. when restricted to linear encoding strategies. In the absence of any such restrictions, we provide an upper bound for the sum s.d.o.f. of the multiple access wiretap channel in the regime $N \leq K \leq 2N$. Our results show that unlike in the single-input single-output (SISO) case, there is loss of s.d.o.f. for even the wiretap channel with a helper due to lack of eavesdropper CSIT, when $K \geq N$.

Finally, we explore the effect of delayed CSIT on physical layer security. In particular, we consider the two user multiple-input single-output (MISO) broadcast channel with confidential messages, in which the nature of CSIT from each user can be of the form I_i, $i = 1, 2$ where $I_1, I_2 \in \{\mathsf{P}, \mathsf{D}, \mathsf{N}\}$, and the forms P, D and N correspond to perfect and instantaneous, completely delayed, and no CSIT, respectively. Thus, the overall CSIT can be any of nine possible states corresponding to all possible values of $I_1 I_2$. While the optimal sum s.d.o.f. in the homogeneous settings corresponding to $I_1 = I_2$ are already known in the literature, we focus on the heterogeneous settings where $I_1 \neq I_2$ and establish the optimal s.d.o.f. region in each case. We further consider the case where the CSIT state varies with time. Each state I_1I_2 can then occur for $\lambda_{I_1I_2}$ fraction of the total duration. We determine the s.d.o.f. region of the MISO broadcast channel with confidential messages under such an alternating CSIT setting, with a mild symmetry assumption, where $\lambda_{I_1I_2} = \lambda_{I_2I_1}$.

SECURITY UNDER IMPERFECT CHANNEL KNOWLEDGE IN WIRELESS NETWORKS

by

Pritam Mukherjee

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
2016

Advisory Committee:
Professor Şennur Ulukuş, Chair/Advisor
Professor Prakash Narayan
Professor Alexander Barg
Professor Charalampos Papamanthou
Professor Lawrence C. Washington

Dedication

To my wife, Sayantika.

Acknowledgments

First and foremost I would like to express my deepest gratitude for my advisor, Professor Sennur Ulukus for giving me the invaluable opportunity to work on challenging and interesting problems over the past six years. She has been extremely patient with me, allowing me free rein to choose my problems, guiding and supporting me when I faltered, and always being available to me for help and advice on both professional and personal problems. Even besides academics, I have learned much from her including the importance of hard work, perseverance, mindfulness and time management. It has been a pleasure to work with and learn from such an extraordinary individual.

I would also like to thank Prof. Prakash Narayan, Prof. Alexander Barg, Prof. Babis Papamanthou and Prof. Lawrence Washington for sparing their invaluable time and energy to be in my dissertation committee, and also for their valuable comments. I am also very grateful to Prof. Narayan for the numerous enlightening discussions we have had, and his continuous support and encouragement. I have also enjoyed and benefited greatly from the weekly Communication, Control and Signal Processing seminar, which is organized by Prof. Narayan and Prof. Barg; special thanks to both of them.

My friends at the Communication and Signal Processing Laboratory have been great company. I am especially grateful to Raef Bassily and Himanshu Tyagi for the many insightful discussions and also for being such good friends. Ravi Tandon and Jianwei Xie have been my collaborators and I have learnt a lot from both of them - my sincerest thanks to both of them. My daily interactions with Praneeth Boda, Berk Gurakan, Yi-Peng Wei, Omur Ozel, Ersen Ekrem, Ahmed Arafa , Karim Banawan and Abdulrahman Baknina have made this long journey enjoyable and fun - my thanks to all of them.

My housemates at my place of residence have been a great support. I would like to express my gratitude to Biswadip Dey, Shawon Sarkar, Upamanyu Ray and Risov Goswami for being a family outside of family to me.

My deepest gratitude goes to my family - my parents, who have always supported me through my career, especially my sister, brother-in-law and my sweet niece, whose house has been my refuge on many a lonely day in the last six years - without them, my life in the U.S. would have been far more onerous. Finally, I would like to thank my long-time girlfriend and now wife, Sayantika, who has patiently supported and encouraged me all throughout this journey. Her love and support has been a great source of strength for me.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

The focus of this dissertation is on physical layer security in wireless communication networks. Wireless communication networks are ubiquitous in the modern world; common examples include cellular networks, Wi-Fi and Bluetooth. Yet the wireless medium is inherently open to eavesdropping, and securing the information being transmitted through wireless networks against potential eavesdroppers presents a significant challenge. This dissertation explores the paradigm of physical layer security, which seeks to exploit inherent physical layer channel properties such as noise, fading, and multiple antennas at the terminals to guarantee security. The derived security guarantees are based on an information theoretic framework, and are not vulnerable to potential advances in the computational abilities of an eavesdropper.

The main thrust of this dissertation is on investigating how the availability of channel state information (CSI) at the terminals affects physical layer security in wireless networks. Wireless channels exhibit *fading*, that is, the channel gain for each receiver varies with time. To ensure reliable communication, in practical systems, the receivers measure the channel gains periodically and feed them back to the transmitters. These channel measurements available at a terminal constitute the CSI at the terminal. In this dissertation, we explore the role of CSI in securing

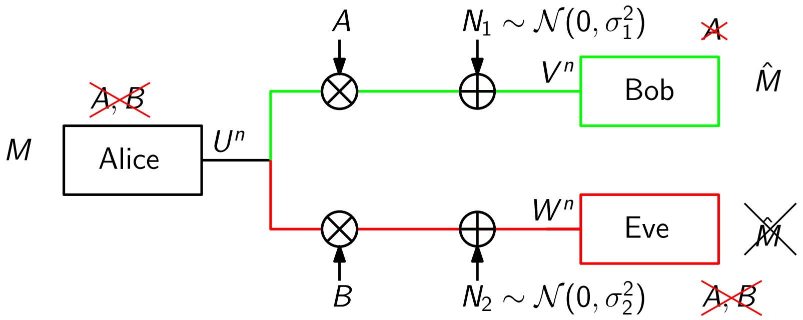


Figure 1.1: Fading wiretap channel with no CSI anywhere.

wireless communication for various channel models, such as the wiretap channel, the wiretap channel with helpers, the multiple access wiretap channel, the broadcast channel with confidential messages and the interference channel with an external eavesdropper.

We begin, in Chapter 2, with a fast fading Rayleigh wiretap channel where each terminal is equipped with only one antenna, as shown in Fig. 1.1. We consider a fast Rayleigh fading scenario, where the channel gains of both the legitimate link and the eavesdropper link fade in an independent identically distributed (i.i.d.) fashion from one symbol to the next with a Rayleigh distribution. This models a fast fading wireless communication channel with coherence time of one symbol duration. Under such a fast fading condition, the channel may change too quickly for receivers to estimate it. In addition, the eavesdropper will not feed her CSI estimate back even if she measures it. Thus, we assume no CSI is available at any terminal before the communication begins. For this system model, we determine the exact secrecy capacity.

We first show that this channel is equivalent to a degraded wiretap channel. This implies that no channel prefixing is needed [1]. We then consider the secrecy rate, which is the difference of mutual informations, as the objective function, which is concave, and determine the optimal input distribution as the result of a functional optimization problem. To analyze the Karush-Kuhn-Tucker (KKT) optimality conditions, we use a proof technique originally developed by Smith [2] to evaluate the channel capacity of an amplitude constrained Gaussian channel and later extended by Abou-Faycal et al. [3] to determine the channel capacity of a fast fading Rayleigh channel under an average power constraint. We extend the KKT conditions to the complex plane and use the identity theorem to prove that the optimum input distribution cannot have an infinite support over any finite interval. We then show that the optimal distribution has a finite support. Though we do not have a closed form expression for the secrecy capacity, it can be computed numerically by solving a finite dimensional optimization problem.

In Chapter 3, we extend our investigation of the impact of no CSI to several multi-terminal channel models. In particular, we consider three channel models: the wiretap channel with M helpers, the K-user multiple access wiretap channel, and the K-user interference channel with an external eavesdropper, when no eavesdropper CSI is available at the transmitters. For each of these channel models, the secrecy capacity regions remain unknown, even with full eavesdropper CSIT. In the absence of exact capacity regions, we study the secure degrees of freedom (s.d.o.f.) of each channel model in the high signal-to-noise (SNR) regime. For the wiretap channel with M helpers and full eavesdropper CSIT, reference [4] determines the optimal s.d.o.f. to be $\frac{M}{M+1}$. Further, reference [5] determines the optimal sum s.d.o.f. for the K-user multiple access wiretap channel with full eavesdropper

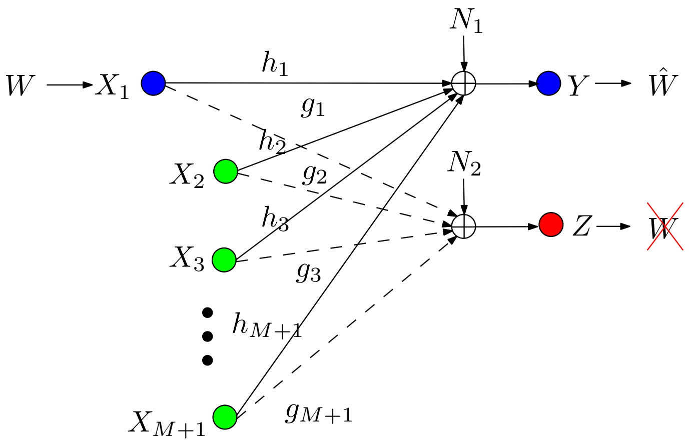


Figure 1.2: Wiretap channel with M helpers.

CSIT to be $\frac{K(K-1)}{K(K-1)+1}$. For the interference channel with an external eavesdropper, the optimal sum s.d.o.f. is shown to be $\frac{K(K-1)}{2K-1}$ in reference [6], with full eavesdropper CSIT. Here, we focus on the case when no eavesdropper CSIT is available. We show that for the wiretap channel with M helpers, an s.d.o.f. of $\frac{M}{M+1}$ is achievable even without eavesdropper's CSIT; thus, there is no loss of s.d.o.f. due to the unavailability of eavesdropper CSIT in this case. For the multiple access wiretap channel and the interference channel with an external eavesdropper, however, the optimal s.d.o.f. decreases when there is no eavesdropper CSIT. In particular, without eavesdropper CSIT, the K-user multiple access wiretap channel reduces to a wiretap channel with $(K-1)$ helpers and the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{K(K-1)+1}$ to $\frac{K-1}{K}$. For the interference channel with an external eavesdropper, the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{2K-1}$ to $\frac{K-1}{2}$ with no eavesdropper CSIT.

In order to establish the optimal sum s.d.o.f., we propose achievable schemes and provide matching converse proofs for each of these channel models. First, we consider the wiretap channel with M helpers shown in Fig. 1.2, and the K-user

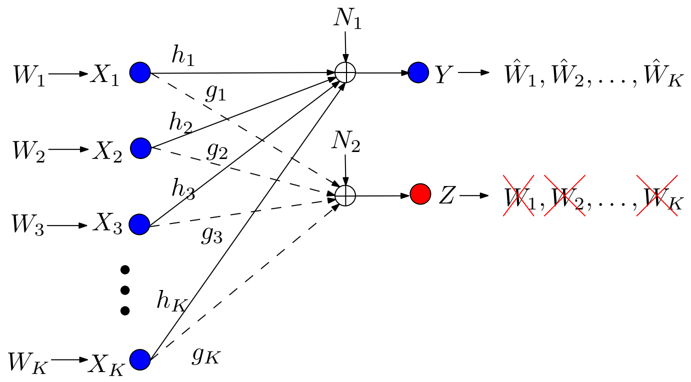


Figure 1.3: K-user multiple access wiretap channel.

multiple access wiretap channel, shown in Fig. 1.3. We note that any achievable scheme for the wiretap channel with $(K-1)$ helpers is also an achievable scheme for the K-user multiple access wiretap channel. Further, a converse for the K-user multiple access wiretap channel is an upper bound for the wiretap channel with $(K-1)$ helpers as well. Thus, we provide achievable schemes for the wiretap channel with helpe2rs and a converse for the multiple access wiretap channel. We consider both fixed and fading channel gains. For the wiretap channel with helpers and the multiple access wiretap channel, we present schemes based on real interference alignment [7] and vector space alignment [8] for fixed and fading channel gains, respectively.

For the interference channel, see Fig. 1.4, our achievable schemes are based on asymptotic real alignment [7,9] and asymptotic vector space alignment [8] for fixed and fading channel gains, respectively. As in [6], every transmitter sacrifices a part of its message space to transmit cooperative jamming signals in the form of artificial noise. However, instead of one artificial noise block as in [6], our scheme requires two noise blocks from each transmitter. The $2K$ noise blocks from the K transmitters

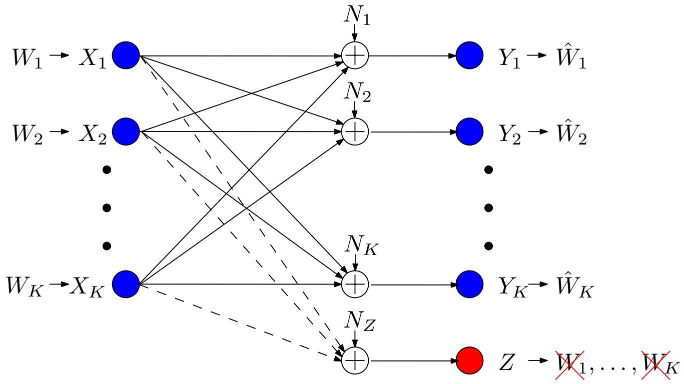

$W_1 \rightarrow X_1$
$W_2 \rightarrow X_2$
$W_K \rightarrow X_K$
N_1
N_2
N_K
N_Z
$Y_1 \rightarrow \hat{W}_1$
$Y_2 \rightarrow \hat{W}_2$
$Y_K \rightarrow \hat{W}_K$
$Z \rightarrow \cancel{W_1}, \ldots, \cancel{W_K}$

Figure 1.4: K-user interference channel with an external eavesdropper.

are then aligned at each legitimate receiver to occupy only $(K+1)$ *block dimensions* out of the full space of $2K$ dimensions, thus, achieving $\frac{K-1}{2K}$ s.d.o.f. per receiver. At the eavesdropper, however, the noise blocks do not align, and therefore, occupy the full space of $2K$ block dimensions, ensuring security of the message blocks. An interesting aspect of our proposed schemes for the interference channel is that they provide confidentiality of the messages not only from the external eavesdropper but also from the unintended legitimate receivers. Thus, our schemes for both fixed and fading channel gains achieve the optimal sum s.d.o.f. for the K-user interference channel with both *confidential messages* and an external eavesdropper, with no eavesdropper CSIT.

To prove the converses, we combine techniques from [4,6] and [10]. We exploit a key result in [10] that the output entropy at a receiver whose CSIT is not available is at least as large as the output entropy at a receiver whose CSIT is available, even when the transmitters cooperate and transmit correlated signals. This result is similar in spirit to the *least alignment lemma* in [11], where only *linear* transmission strategies are considered. Intuitively, no alignment of signals is possible at the receiver whose CSIT is unavailable; therefore, the signals occupy the maximum possible space at that receiver. We combine this insight with the techniques of [4,6]. Specifically, we use discretized versions of the *secrecy penalty lemma*, which quantifies the loss of rate due to the presence of an eavesdropper, and the *role of a helper lemma*, which captures the trade-off, arising out of decodability constraints, between the message rate and the entropy of an independent helper signal. Together, these techniques enable us to establish the optimal sum s.d.o.f. for the multiple access wiretap channel with no eavesdropper CSIT to be $\frac{K-1}{K}$ and the optimal sum s.d.o.f. for the interference channel with no CSIT from the external eavesdropper to be $\frac{K-1}{2}$.

In Chapter 4, we consider a multiple-input multiple-output (MIMO) version of the multiple access wiretap channel. However, the optimal sum s.d.o.f. of the MIMO multiple access wiretap channel is unknown even with two users and under full CSIT assumptions. Thus, we deviate from our theme of no CSIT in this dissertation and consider the two-user MIMO multiple access wiretap channel with full CSIT, where each transmitter has N antennas, the legitimate receiver has N antennas and the eavesdropper has K antennas; see Fig. 1.5. We study the case when the channel gains are fixed throughout the duration of the communication, as well as the case when the channel is fast fading and the channel gains vary in an i.i.d. fashion across time. Our goal is to characterize how the optimal sum s.d.o.f. of the MIMO multiple access wiretap channel varies with the number of antennas at the legitimate users and the eavesdropper.

To that end, we partition the range of K into various regimes, and propose

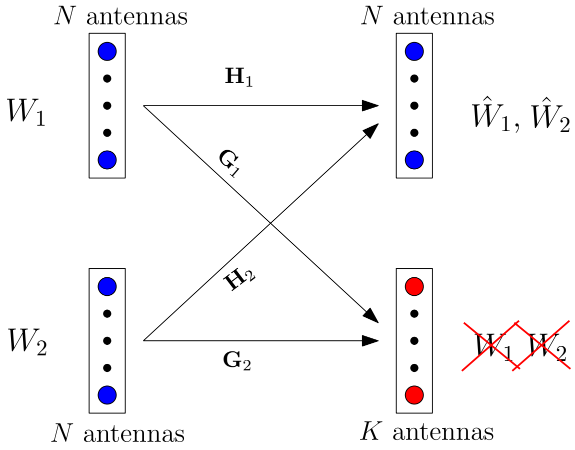


Figure 1.5: The MIMO multiple access wiretap channel.

achievable schemes for each regime. Our schemes are based on a combination of zero-forcing beamforming and vector space interference alignment techniques. When the number of antennas at the eavesdropper is less than the number of antennas at the transmitters, the nullspace of the eavesdropper channel can be exploited to send secure signals to the legitimate transmitter. This strategy is, in fact, optimal when the number of eavesdropper antennas is sufficiently small ($K \leq \frac{N}{2}$) and the optimal sum s.d.o.f. is limited by the decoding capability of the legitimate receiver. We note that the optimal scheme requires a single channel use and thus, can be used for both fixed and fading channel gains.

However, zero-forcing beamforming does not suffice when $K \geq \frac{N}{2}$. In the regime $\frac{N}{2} \leq K \leq \frac{4N}{3}$, the optimal sum s.d.o.f. is of the form $2\left(d+\frac{l}{3}\right)$, $l = 0, 1, 2$, where d is an integer. For the case of fading channel gains, we use vector space interference alignment [8] over three time slots to achieve the optimal sum s.d.o.f. The structure of the optimal signaling scheme is inspired by ideas from the optimal real alignment scheme presented in [4] for the single-input single-output (SISO) multiple access wiretap channel. Unlike the previous regime, this scheme for fading channel gains cannot be directly extended to the fixed channel gains case, except for the case $l = 0$, for which the sum s.d.o.f. is an integer and carefully precoded Gaussian signaling suffices. When $l \neq 0$, the s.d.o.f. has a fractional part, and Gaussian signaling alone is not optimal.

In order to handle the fractional s.d.o.f., we decompose the channel input at each transmitter into two parts: a Gaussian signaling part carrying d (the integer part) d.o.f. of information securely, and a structured signaling part carrying $\frac{l}{3}$ (the fractional part) d.o.f. of information securely. The structure of the Gaussian signals carrying the integer s.d.o.f. resembles that of the schemes for the fading channel gains. When $l = 1$, we design the structured signals carrying $\frac{2}{3}$ sum s.d.o.f. according to the real interference alignment based SISO scheme of [4]. However, when $l = 2$, a new scheme is required to achieve $\frac{4}{3}$ sum s.d.o.f. on the MIMO multiple access wiretap channel with two antennas at every terminal. To that end, we provide a novel optimal scheme for the canonical $2 \times 2 \times 2 \times 2$ MIMO multiple access wiretap channel. Interestingly, the scheme relies on asymptotic real interference alignment [9] at each antenna of the legitimate receiver.

When the number of eavesdropper antennas K is large enough $K \geq \frac{4N}{3}$, the optimal sum s.d.o.f. is given by $(2N - K)$, which is always an integer. In this regime Gaussian signaling along with vector space alignment techniques suffices. In fact, the scheme uses only one time slot and can be used with both fixed and fading channel gains. When the number of antennas at the eavesdropper is very large ($K \geq \frac{3N}{2}$), the two-user multiple access wiretap channel reduces to a wiretap channel with one helper, and, thus, the scheme for the MIMO wiretap channel with one helper in [12] is optimal.

To establish the optimality of our achievable schemes, we present matching converses in each regime. A simple upper bound is obtained by allowing cooperation between the two transmitters. This enhances the two-user multiple access wiretap channel to a MIMO wiretap channel with $2N$ antennas at the transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper. The optimal s.d.o.f. of this MIMO wiretap channel is well known to be $\min((2N-K)^+, N)$ [13,14], and this serves as an upper bound for the sum s.d.o.f. of the two-user multiple access wiretap channel. This bound is optimal when the number of eavesdropper antennas K is either quite small ($K \leq \frac{N}{2}$), or quite large ($K \geq \frac{4N}{3}$). When K is small, the sum s.d.o.f. is limited by the decoding capability of the legitimate receiver, and the optimal sum s.d.o.f. is N which is optimal even without any secrecy constraints. When K is large, the s.d.o.f. is limited by the requirement of secrecy from a very strong eavesdropper. For intermediate values of K, the distributed nature of the transmitters dominates, and we employ a generalization of the SISO converse techniques of [4] for the converse proof in the MIMO case, similar to [12].

In Chapter 5, we return to our theme of no eavesdropper CSIT, and study two channel models: the MIMO wiretap channel with one helper where the transmitter, the helper and the legitimate receiver each have N antennas, and the eavesdropper has K antennas; see Fig. 1.6, and the MIMO multiple access wiretap channel, where both transmitters and the legitimate receiver have N antennas and the eavesdropper has K antennas; see Fig. 1.7. In both cases, the channel is fast fading and the

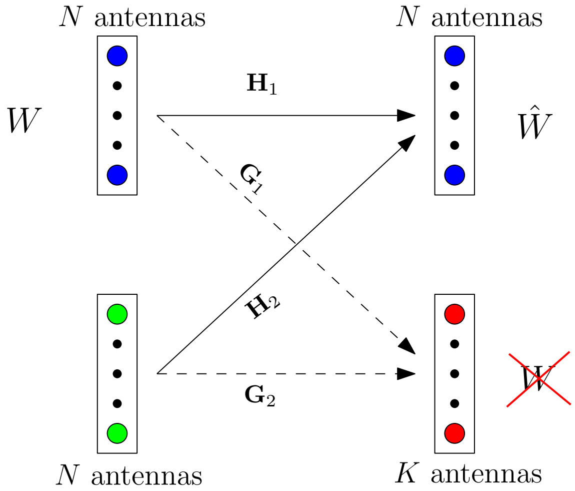


Figure 1.6: The MIMO wiretap channel with one helper and no Eve CSIT.

channel gains vary in an i.i.d. fashion across the links and time. We consider the case when the eavesdropper's CSI is not available at the transmitters. Our goal is to investigate the optimal sum s.d.o.f. of the MIMO wiretap channel with one helper and the MIMO multiple access wiretap channel as a function of N and K.

To that end, we provide an achievable scheme based on vector space alignment [8], that attains $\frac{1}{2}(2N-K)$ s.d.o.f. for the wiretap channel with one helper for all values of $0 \leq K \leq 2N$. When $K \leq N$, this value coincides with the optimal s.d.o.f. for the wiretap channel with one helper in the case where full eavesdropper CSIT is available. Therefore, for the regime $K \leq N$, there is no loss of s.d.o.f. for the wiretap channel with one helper due to the lack of eavesdropper CSIT. Further, the proposed scheme which does not require eavesdropper CSIT, is optimal. The achievable scheme for the wiretap channel with one helper also suffices as an achievable scheme for the multiple access wiretap channel, since we can treat one of the transmitters as a helper and use time-sharing among the two transmitters.

To prove the optimality of the proposed scheme for the multiple access wiretap

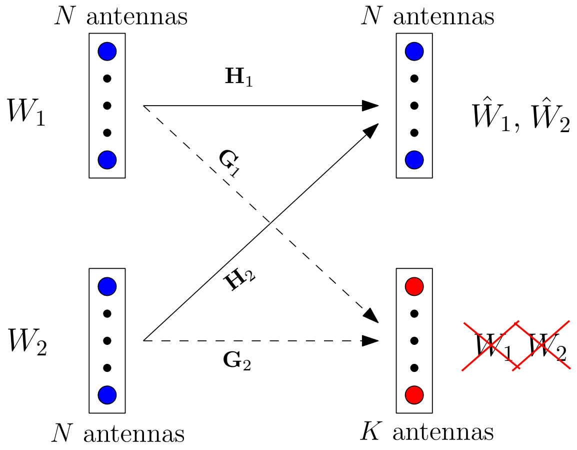


Figure 1.7: The MIMO multiple access wiretap channel with no Eve CSIT.

channel in the regime $K \leq N$, we provide a matching converse for this regime. For the converse proof, we use MIMO versions of the *secrecy penalty lemma* and the *role of a helper lemma* [4], and exploit channel symmetry at the eavesdropper. Since the transmitters do not have the eavesdropper's CSIT, the output at the K antennas of the eavesdropper are *entropy symmetric* [15], i.e., any two subsets of the antenna outputs have the same differential entropy, if the subsets are of equal size. Finally, we use a MIMO version of the result in [10, 16], which states that the differential entropy at the output of the terminal which does not provide CSIT is the greatest among terminals having equal number of antennas. The converse in the regime $K \leq N$ shows that the sum s.d.o.f. cannot exceed $\frac{1}{2}(2N - K)$ for the multiple access wiretap channel. Since a converse for the multiple access wiretap channel is valid for the wiretap channel with one helper as well, together with the achievable scheme, this shows that the optimal s.d.o.f. for both the wiretap channel with one helper and the multiple access wiretap channel in this regime is $\frac{1}{2}(2N - K)$; therefore, as in the SISO case, which is a subset of this regime with $N = K = 1$, the multiple access wiretap channel reduces to the wiretap channel with one helper when the eavesdropper's CSIT is not available. Recalling that with full eavesdropper CSIT, the optimal sum s.d.o.f. of the multiple access wiretap channel in this regime is $\min(N, \frac{2}{3}(2N-K))$; this also illustrates the loss of s.d.o.f. for the multiple access wiretap channel due to the lack of eavesdropper's CSIT.

Next, we consider the regime $N \leq K \leq 2N$. In this regime, we provide a loose upper bound which shows that the sum s.d.o.f. of the multiple access wiretap channel cannot be larger than $\frac{2N(2N-K)}{4N-K}$. This bound is clearly loose; at the point $N = K$, it equals $\frac{2N}{3}$, which is achievable with full eavesdropper CSIT, but *not* without eavesdropper CSIT. However, noting that $\frac{2N(2N-K)}{4N-K} < (2N-K)$, we can conclude that there will be loss of s.d.o.f. due to lack of eavesdropper CSIT, even for the wiretap channel with one helper, in the regime $\frac{3N}{2} \leq K \leq 2N$, where $(2N-K)$ s.d.o.f. is achievable with full eavesdropper CSIT [12].

In order to further investigate the optimality of $\frac{1}{2}(2N-K)$ as the sum s.d.o.f. for the multiple access wiretap channel in the regime $N \leq K \leq 2N$, we then restrict ourselves to *linear* encoding strategies [11, 17], where the channel input of each antenna in every time slot is restricted to be a linear combination of some information symbols intended for the legitimate receiver and some artificial noise symbols to provide secrecy at the eavesdropper. We show that under this restriction to linear encoding schemes, the *linear* sum s.d.o.f. can be no larger than $\frac{1}{2}(2N-K)$. The key idea of the proof is that since no alignment is possible at the eavesdropper, the artificial noise symbols should asymptotically occupy the maximum number of dimensions available at the eavesdropper; consequently, the dimension of the linear

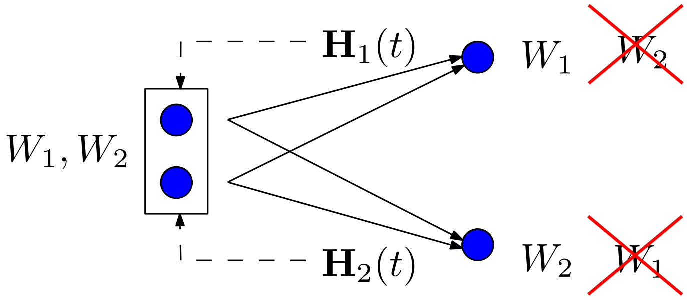


Figure 1.8: The MISO broadcast channel with confidential messages.

signal space at the eavesdropper should be $Kn + o(n)$ in n channel uses. Thus, $\frac{1}{2}(2N - K)$ is the optimal s.d.o.f. for the multiple access channel in the regime $N \leq K \leq 2N$, at least when restricted to linear encoding strategies.

In Chapter 6, we explore the delay aspect of CSI in the context of physical layer security. In practice, the delay occurs due to the time required for the acquisition of the channel measurements at the receivers as well as the transmission of those measurements to the transmitters. We adopt a simple modeling of the delay whereby the CSIT from a user can be one of three possible states: *perfect* or instantaneous (P), *delayed* (D) [18] or *none* (N). In state P, the transmitter has precise channel knowledge before the start of the communication. In state D, the transmitter does not have the CSI at the beginning of the communication. In slot t, the receiver may send any function of all the channel coefficients upto and including time t as CSI to the transmitter. However, the CSIT becomes available only after a delay such that the CSI is completely outdated, that is, independent of the current channel realization. In state N, no CSIT is available from the user.

We focus on the fading two-user multiple-input single-output (MISO) broadcast channel with confidential messages, in which the transmitter with two antennas has two confidential messages, one for each of the single antenna users; see Fig. 1.8. The CSIT state of each of the two receivers may be either P, D or N. The optimal sum s.d.o.f. of the two-user MISO broadcast channel with confidential messages is well known in the existing literature under the homogeneous CSIT settings: PP, DD and NN. In state PP, i.e., when both receivers provide perfect or instantaneous CSIT, the sum s.d.o.f. is 2, which is achievable by beamforming. In state NN, i.e., when there is no CSIT from either receiver, the sum s.d.o.f. is zero as the two users are statistically equivalent and hence no secrecy is possible. On the other hand, in state DD, with completely outdated CSIT from both users, [15] showed that the sum s.d.o.f. increases to 1.

In practice, however, the nature of CSIT can vary across users. This observation naturally leads to the setting of heterogeneous (or hybrid) CSIT which models the variability in the quality/delay of channel knowledge supplied by different users. In contrast to homogeneous CSIT, the setting of heterogeneous CSIT is much less understood. To the best of our knowledge, the complete characterization of the d.o.f. of all fixed heterogeneous CSIT configurations is only known for the two-user MISO broadcast channel: see [19,20] for state PD for which the optimal sum d.o.f. is shown to be 3/2; and [10] which recently settled the states PN and DN through a novel converse proof and showed that the optimal sum d.o.f. is given by 1. Beyond these results, partial results are available for the three-user MISO broadcast channel with hybrid CSIT in [21, 22] but by and large the problem of heterogeneous CSIT even without secrecy constraints remains open. In this chapter, we determine the optimal s.d.o.f. region of the MISO broadcast channel with confidential messages in all three heterogeneous CSIT scenarios: PD, PN and DN. We show that the optimal sum s.d.o.f. is 1 for both PD and PN states, while it is $\frac{1}{2}$ for state DN.

Besides exhibiting heterogeneity across users, the nature of channel knowledge may also vary over time/frequency. Such variability can arise either naturally (due to the time variation in tolerable feedback overhead from a user) or it can be artificially induced (by deliberately altering the channel feedback mechanism over time/frequency). For example, instead of requiring perfect CSIT from one user and delayed CSIT from the other user throughout the duration of communication, one may require that for half of the time, the first user provide perfect CSIT while the second user provide delayed CSIT (state PD), and the roles of the users are reversed for the remaining half of the time (state DP), the total network feedback overhead being the same in both cases. This leads naturally to the setting of alternating CSIT in which multiple CSIT states, for instance, PD and DP in the above example, arise over time. The alternating CSIT framework was introduced in [23] where the d.o.f. region was characterized for the two-user MISO broadcast channel. It was shown that synergistic gains in d.o.f. are possible by jointly coding across these states. We show that similar synergistic gains are possible even with security constraints for the MISO broadcast channel with confidential messages.

Our main contribution in this problem is the characterization of the optimal s.d.o.f. region for the general model with all nine possible CSIT states: PP, PD, PN, DP, NP, DD, DN, ND, and NN, where we assume that these states occur for arbitrary fractions of time, except for a mild condition of symmetry, which is that states I_1I_2 and I_2I_1 occur for equal fractions of the time if $I_1 \neq I_2$. With 9 states, each occurring for arbitrary fractions of the time, it is not immediately clear how to optimally code across the states and the achievability of the s.d.o.f. region is highly non-trivial. To this end, we first develop several key constituent schemes, where each scheme uses a subset of the 9 states to achieve a particular s.d.o.f. value. Now given an arbitrary[1] probability mass function (pmf) on the 9 CSIT states, we judiciously time share between the constituent schemes to achieve the optimal s.d.o.f. region.This is achieved by considering different sub-cases based on the relative proportions of the various states and explicitly characterizing how the constituent schemes should be time shared to obtain the optimal s.d.o.f. region in each sub-case.

Next, we provide a matching converse for the full region. The idea behind the converse is to first enhance the channel by providing more CSIT to obtain a new channel with fewer number of states but at least as large secrecy capacity as the original channel. We introduce the *local statistical equivalence* property, which states that if we consider the outputs of a receiver for such states in which it supplies delayed or no CSIT, the entropy of the channel outputs conditioned on the past outputs is the same as that of another artificial receiver whose channel is distributed identically as the original receiver. Outer bounds on the s.d.o.f. region for the enhanced channel are then derived using the local statistical equivalence property and combining the obtained outer bounds give us the desired outer bounds for the original channel.

[1] Arbitrary subject to mild symmetry, i.e., $\lambda_{I_1 I_2} = \lambda_{I_2 I_1}$

1.1 Related Work

The study of security under an information theoretic framework was pioneered by Shannon in his seminal paper [24], where two legitimate parties wish to communicate in the presence of an eavesdropper through noiseless channels. It was shown that secret keys shared among the legitimate parties and one-time-pad encryption was necessary for secure communications in this case. The noisy wiretap channel was introduced by Wyner, who determined the capacity equivocation region for the degraded case [1]. It was shown that secure communication is possible using stochastic encoding even without any pre-shared secret keys, if the eavesdropper's channel observation is degraded with respect to the legitimate user's channel. Csiszár and Körner generalized his result to arbitrary, not necessarily degraded, wiretap channels [25]. Leung-Yan-Cheong and Hellman determined the capacity-equivocation region of the Gaussian wiretap channel [26], and showed that the optimal channel input was Gaussian and the secrecy capacity is the difference between the capacities of the legitimate users' channel and the eavesdropping links in this case.

Recently, the study of information theoretic security in the physical layer has been extended to a variety of channel models ranging from fading channels [27–29], MIMO wiretap channels [13, 14, 30, 31], multiple access channels [5, 32–35], broadcast channels with confidential messages (BCCM) [36–38], wiretap channels with helpers [4, 39], and interference channels with confidential messages and external eavesdroppers [40–43]. In this dissertation, we will mostly discuss the fading wiretap channel, the wiretap channel with helpers, the multiple access wiretap channel, the interference channel with external eavesdroppers and the broadcast channel with confidential messages.

References [27, 28, 44, 45] consider the fading wiretap channel where all parties had complete and perfect CSI of both links. Modeling the fading wiretap under full CSI as a bank of independent parallel channels, these references show that the capacity achieving channel inputs are independent Gaussian random variables in all parallel channels, and the variances of these random variables are found via water-filling. Reference [29] considers the case where the transmitter has the legitimate channel's CSI but no eavesdropper CSI under the assumption of infinite coherence times for channel fading, where the channel state of the eavesdropper, although unknown at the transmitter, remains constant for an infinite duration, and shows the optimality of Gaussian channel inputs in this model. Reference [46] considers the same model under a fast fading condition, i.e., when the eavesdropper channel gain is unknown at the transmitter and also varies at the order of symbol duration, and shows that MQAM signaling or Gaussian signaling with added Gaussian artificial noise, may outperform plain Gaussian signaling. The s.d.o.f. in each case is, however, zero, irrespective of the availability or quality of CSI at the terminals.

In multi-user scenarios, however, positive s.d.o.f. values can be achieved, as in multiple access wiretap channels introduced in [32, 33] and wiretap channels with helpers introduced in [39, 47]. The multiple access wiretap channel was introduced by [32, 33], where the technique of cooperative jamming was introduced to improve the rates achievable with Gaussian signaling. Reference [34] provides outer bounds and identified cases where these outer bounds are within 0.5 bits per channel use of the rates achievable by Gaussian signaling. While the exact secrecy capacity remains unknown, the achievable rates in [32–34] all yield zero s.d.o.f. Reference [35] proposed scaling-based and ergodic alignment techniques to achieve a sum s.d.o.f. of $\frac{K-1}{K}$ for the K-user MAC-WT; thus, showing that an alignment based scheme strictly outperforms i.i.d. Gaussian signaling with or without cooperative jamming at high SNR. Finally, references [4,48] establish the optimal sum s.d.o.f. to be $\frac{K(K-1)}{K(K-1)+1}$ and the full s.d.o.f. region, respectively, for the SISO multiple access wiretap channel.

The K-user interference channel with an external eavesdropper is studied in [40]. When the eavesdropper's CSIT is available, [40] proposes a scheme that achieves sum s.d.o.f. of $\frac{K-1}{2}$. The optimal s.d.o.f. in this case, however, is established in [6] to be $\frac{K(K-1)}{2K-1}$, using cooperative jamming signals along with interference alignment techniques. When the eavesdropper's CSIT is not available, reference [40] proposes a scheme that achieves a sum s.d.o.f. of $\frac{K-2}{2}$.

The broadcast channel with confidential messages is studied in [36–38]. Reference [36] provided inner and outer bounds for the discrete memoryless broadcast channel with confidential messages. References [37,38] establish the secrecy capacity region of the MIMO broadcast channel with confidential messages when precise and instantaneous CSIT is available. Using these results, it follows that for the two-user MISO BCCM, the sum s.d.o.f. is 2 with perfect (P) CSIT. Even without any secrecy constraints, the sum d.o.f. of the MISO broadcast channel is 2 with perfect CSIT. With no CSIT (N) however, reference [49] showed that the sum d.o.f. collapses to 1. With delayed CSIT (D), it is shown in [18] that the sum d.o.f. for the two-user MISO broadcast channel increases to $\frac{4}{3}$; with confidential messages, the optimal sum s.d.o.f. is 1 [15]. Reference [18] also presents novel results for the more general setting of K-user MISO broadcast channel, for $K \geq 2$. With delayed CSI, [50] established the d.o.f. region for the two-user MIMO broadcast channel. References [19, 20] consider the two-user MISO broadcast channel in state PD and determine the optimal d.o.f. to be $\frac{3}{2}$ in this case. The optimal d.o.f. in states PN and DN are shown to be 1 in reference [10]. Partial results are also available for the three-user MISO BC with hybrid CSIT in [21, 22]. Other channel models where the effect of delayed CSIT has been investigated include the MIMO interference channel with delayed CSIT and output feedback [51], the X-channel [17, 52–55], the X-channel with global feedback [56], and the two-user SISO X-channel with confidential messages and global output feedback, [57].

A line of research closely related to imperfect or unavailable CSIT investigates the wiretap channel, the multiple access wiretap channel, and the broadcast channel with an *arbitrarily varying* eavesdropper [58–60], when the eavesdropper CSIT is not available. The eavesdropper's channel is assumed to be arbitrary, without any assumptions on its distribution, and security is guaranteed for *every* realization of the eavesdropper's channel. This models an exceptionally strong eavesdropper, which may control its own channel in an adversarial manner. Hence, the optimal sum s.d.o.f. is zero in each case with single antenna terminals, since the eavesdropper's channel realizations may be exactly equal to the legitimate user's channel realizations. On the other hand, in our model, the eavesdropper's channel gains are drawn from a known distribution, though the realizations are not known at the transmitters. We show that, with this mild assumption, strictly positive s.d.o.f. can be achieved even with single antennas at each transmitter and receiver for *almost all* channel realizations for helper, multiple access, and interference networks.

Chapter 2: The Wiretap Channel with No CSI

2.1 Introduction

In this chapter, we consider the Gaussian wiretap channel under Rayleigh fading, where the channel gains of both the legitimate link and the eavesdropper link fade in an independent identically distributed (i.i.d.) fashion from one symbol to the next with a Rayleigh distribution, see Fig. 2.1. This models a fast fading wireless communication channel with coherence time of one symbol duration. Under such a fast fading condition, the channel may change too quickly for receivers to estimate it. In addition, the eavesdropper will not feed her CSI estimate back even if she measures it. Thus, we assume no channel state information (CSI) is available at any terminal at the start of communication. The goal is to characterize the exact secrecy capacity for this channel model.

To that end, we use the proof technique that was originally developed by Smith [2] to evaluate the channel capacity of an amplitude constrained Gaussian channel. This technique was further used and extended by Abou-Faycal et al. [3] to determine the channel capacity of a fast fading Rayleigh channel under an average power constraint. Our work may be viewed as a wiretap version of Abou-Faycal et al.'s paper, which considered only reliable communication between two terminals,

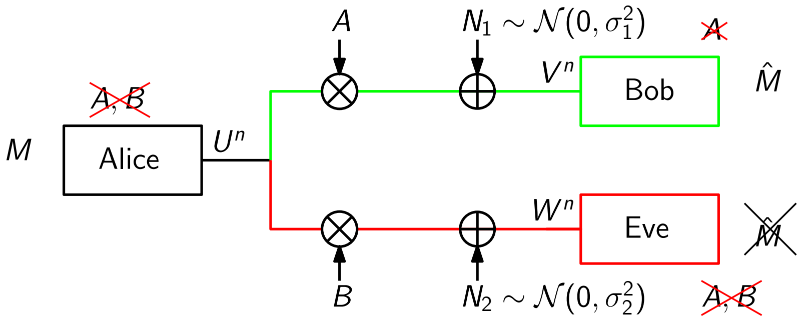

A
$N_1 \sim \mathcal{N}(0,\sigma_1^2)$
A
V^n
Bob
$\hat{M}$
A, B
M
Alice
U^n
W^n
Eve
$\hat{M}$
B
$N_2 \sim \mathcal{N}(0,\sigma_2^2)$
A, B

Figure 2.1: Fading wiretap channel with no CSI anywhere.

whereas we consider both reliability and secrecy. Our work is also closely related to [61] which considers secret key generation for a similar channel model.

We first show that this channel is equivalent to a degraded wiretap channel; thus, no channel prefixing is needed [1]. We then consider the secrecy rate, which is the difference of mutual informations, as the objective function, which is concave, and determine the optimal input distribution as the result of a functional optimization problem. We obtain the KKT optimality conditions, and extend these conditions to the complex plane and reach a contradiction using the identity theorem to conclude that the optimum input distribution cannot have an infinite support over any finite interval. We then show that the optimal distribution has a finite support. The secrecy capacity can then be evaluated numerically.

2.2 System Model, Definitions and Preliminaries

The fast Rayleigh fading wiretap channel, see Fig. 2.1 is given by:

$$V_i = A_i U_i + N_{1i} \tag{2.1}$$

$$W_i = B_i U_i + N_{2i} \tag{2.2}$$

where U_i is the channel input, V_i and W_i are the channel outputs of the legitimate receiver and the eavesdropper, respectively, and A_i and B_i are identically distributed complex circular Gaussian random variables with zero-mean and variance σ_h^2, representing fading. The realizations of A_i and B_i are unknown to all users, though their statistics are known. The noise terms N_{1i} and N_{2i} are zero-mean complex circular Gaussian random variables with variances σ_1^2 and σ_2^2, respectively, with $\sigma_2^2 > \sigma_1^2$. The random variables A_i, B_i, N_{1i}, N_{2i} are i.i.d. in time. The channel input is average power constrained: $\mathbb{E}\left[|U_i|^2\right] \leq P$.

As in [3], since the channel is stationary and memoryless, we can drop the time index i without any loss of generality. Also, since the phases of the fading parameters A and B are uniform, $|V|^2$ and $|W|^2$ are sufficient statistics to characterize the conditional distributions of V and W respectively, given the input U. Conditioned on $|U|$, $|V|^2$ and $|W|^2$ are exponentially distributed with parameters $\frac{1}{\sigma_h^2|u|^2+\sigma_1^2}$ and $\frac{1}{\sigma_h^2|u|^2+\sigma_2^2}$. We let $Y = |V|^2$, $Z = |W|^2$ and $X = |U|$, then

$$p_{Y|X}(y|x) = \frac{1}{\sigma_h^2 x^2 + \sigma_1^2} \exp\left[-\frac{y}{\sigma_h^2 x^2 + \sigma_1^2}\right] \tag{2.3}$$

$$p_{Z|X}(z|x) = \frac{1}{\sigma_h^2 x^2 + \sigma_2^2} \exp\left[-\frac{z}{\sigma_h^2 x^2 + \sigma_2^2}\right] \tag{2.4}$$

The transmitter sends a message M, uniformly chosen from $\mathcal{M}$, by encoding it to an n-length codeword $U^n = \varphi(M)$ using a stochastic encoding function φ. The legitimate receiver detects the message $\hat{M} = \psi(V^n)$ using a decoding function ψ. The rate of communication is $R = \frac{1}{n}\log|\mathcal{M}|$, and the probability of error is $P_e = \mathbb{P}[\hat{M} \neq M]$. The secrecy is measured by the equivocation of the message at the eavesdropper $\frac{1}{n}H(M|W^n)$. The secrecy capacity is defined as the supremum of all rates R where $P_e \leq \epsilon$, and the message is transmitted information-theoretically securely, i.e., $\frac{1}{n}H(M|W^n) \geq \frac{1}{n}H(M) - \epsilon$, in the limit as $\epsilon \to 0$.

We note that encoding and decoding depend only on the input distribution and the conditional marginals of the legitimate and eavesdropper channels. Thus, the secrecy capacity of the channel given in (2.1)-(2.2) is equal to the secrecy capacity of the following channel:

$$V_i = A_i U_i + N_{1i} \tag{2.5}$$

$$W_i = A_i U_i + N_{1i} + \tilde{N}_i \tag{2.6}$$

where $\tilde{N}_i \sim \mathcal{CN}(0, \sigma_2^2 - \sigma_1^2)$ and $\tilde{N}_i$ is independent of N_{1i}. It is clear that in the channel model of (2.5)-(2.6) the eavesdropper's output is a degraded version of the legitimate receiver's output, and $U \to V \to W$. In addition, since $I(U;V) = I(X;Y)$ and $I(U;W) = I(X;Z)$, the secrecy capacity is [1]

$$C_s = \sup_{F \in \mathcal{F}} I(U;V) - I(U;W) \tag{2.7}$$

$$= \sup_{F \in \mathcal{F}} I(X;Y) - I(X;Z) \tag{2.8}$$

where F denotes the input distribution drawn from the class of distributions $\mathcal{F}$ which satisfy the given power constraint. Furthermore, the Markov chain $X \to Y \to Z$ holds, because Z is independent of X given V, which follows from the Markov chain $U \to V \to W$, and that the phase of V is independent of X given Y, since the phase of the fading parameter A is uniform and independent of X. As shown by van Dijk [62] for the discrete case, for this continuous case also, we can show that $I(X;Y)-I(X;Z)$ is a concave function of the input distribution, when $X \to Y \to Z$. Thus, to find the secrecy capacity of the channel in (2.5)-(2.6), it suffices to solve the convex optimization problem in (2.8).

Before we determine the secrecy capacity, we note an upper bound on it as:

$$C_s \leq \log\left(1+\frac{\sigma_h^2 P}{\sigma_1^2}\right) - \log\left(1+\frac{\sigma_h^2 P}{\sigma_2^2}\right) \tag{2.9}$$

This upper bound can be derived as follows:

$$I(U;V) - I(U;W) = (h(V) - h(W)) - (h(V|U) - h(W|U)) \tag{2.10}$$

The first term on the right side of (2.10) can be upper bounded by using the entropy power inequality:

$$h(V) - h(W) \leq \log\left(\frac{\sigma_h^2 P + \sigma_2^2}{\sigma_h^2 P + \sigma_1^2}\right) \tag{2.11}$$

and the second term can be lower bounded by noting

$$h(V|U) - h(W|U) \geq h(V|A,U) - h(W|A,U) = \log\frac{\sigma_1^2}{\sigma_2^2} \tag{2.12}$$

giving the desired upper bound in (2.9). The inequality in (2.12) can be derived by noting that $I(V;A|U) \geq I(W;A|U)$. The significance of the upper bound in (2.9) is that it shows that the secrecy capacity is always finite, even when the power goes to infinity, and also that the secure degrees of freedom of this system is zero as in the cases of non-fading Gaussian wiretap channel and fading Gaussian wiretap channel with perfect CSI.

2.3 KKT Optimality Conditions

For a channel with continuous alphabet, the supremum in (2.8) need not be achievable. A sufficient condition for the achievability of the supremum is that there exists a topology on which mutual information is continuous in the input distribution, implying that the difference of two mutual information quantities induced by the same input distribution is also continuous, and the set of allowable input distributions $\mathcal{F}$ is compact. Both of these criteria hold in our case, as was shown in [3, Appendix I]. We solve the maximization in (2.8) using convex optimization techniques following Smith [2] and Abou-Faycal et al. [3]. The channel input X^* with distribution F^* that achieves the secrecy capacity must satisfy the KKT optimality condition:

$$\begin{aligned}\gamma(x^2-P)+C_s-\int p_{Y|X}(y|x)\ln\left[\frac{p_{Y|X}(y|x)}{p_Y(y;F^*)}\right]dy\\ +\int p_{Z|X}(z|x)\ln\left[\frac{p_{Z|X}(z|x)}{p_Z(z;F^*)}\right]dz\geq 0,\quad \forall x\in\mathbb{R}\end{aligned}\tag{2.13}$$

for some $\gamma \geq 0$, which is the Lagrange multiplier due to the average power constraint on the channel input. Furthermore, (2.13) is satisfied with equality if x lies in the support of X^*. Note that, in (2.13), $p_Y(y;F)$ and $p_Z(z;F)$ are the probability distributions of Y and Z, respectively, which are induced by the probability distribution F, of X, i.e.,

$$p_Y(y;F) = \int p_{Y|X}(y|x)\, dF(x) \tag{2.14}$$

$$p_Z(z;F) = \int p_{Z|X}(z|x)\, dF(x) \tag{2.15}$$

In the next section, we will examine the implications of the KKT conditions in (2.13) on the optimum probability distribution for the channel input X.

2.4 Characterization of X^*

Theorem 1 *The optimal X^* is discrete with only a finite number of points in any bounded interval.*

Proof: To prove the theorem, we need to rule out the following two cases:

1. The support of X^* contains an interval.
2. X^* is discrete but there exists a bounded interval containing infinitely many points belonging to the support of X^*.

We proceed by contradiction. Therefore, let us assume that either of the two cases 1) or 2) holds. Let E be the support set of X^*. Noting that

$$\int p_{Y|X}(y|x) \ln p_{Y|X}(y|x)\, dy = \ln\left(\frac{1}{\sigma_h^2 x^2 + \sigma_1^2}\right) - 1 \tag{2.16}$$

one can simplify (2.13) as:

$$f(x) \geq 0, \quad \forall x \in \mathbb{R} \tag{2.17}$$

with equality if $x \in E$, where $f(x)$ is given by

$$\begin{aligned} f(x) =& \gamma(x^2 - P) + C_s + \ln\left(\frac{\sigma_h^2 x^2 + \sigma_1^2}{\sigma_h^2 x^2 + \sigma_2^2}\right) + \int p_{Y|X}(y|x) \ln\left(p_Y(y; F^*)\right) dy \\ & - \int p_{Z|X}(z|x) \ln\left(p_Z(z; F^*)\right) dz \end{aligned} \tag{2.18}$$

Now, E contains a bounded set S with an infinite number of distinct points. Let S_c be a compact neighbourhood containing S. By the Bolzano-Weierstrass theorem, the set S must have an accumulation point in S_c. We extend $f(x)$ to the complex domain, and by letting $\ln x$ be the principal branch of the logarithm, f is well defined and analytic on the complex plane. The KKT conditions in (2.17) tell us that, f which is an analytic function on a domain D, is identically zero on a set with an accumulation point in D. The identity theorem tells us that f must be identically zero everywhere on D. More specifically, f must be zero on the entire real line. Thus, the equality in (2.17) holds, i.e., $f(x) = 0$, for all $x \in \mathbb{R}$. Since $X \rightarrow Y \rightarrow Z$,

$$p_{Z|X}(z|x) = \int p_{Y,Z|X}(y, z|x) dy \tag{2.19}$$

$$= \int p_{Y|X}(y|x) p_{Z|Y}(z|y) dy \tag{2.20}$$

We use (2.20) in (2.18) and exchange the order of integrals using Fubini's theorem, which is permissible since $|\ln p_Z(z; F^*)|$ is bounded by $\alpha + \beta z$ for some constants α and β, as will be shown in (2.31) and (2.43). This enables us to rewrite the equation $f(x) = 0$, for all $x \in \mathbb{R}$, equivalently as

$$\int p_{Y|X}(y|x) g(y)\, dy = \gamma(P - x^2) - C_s - \ln\left(\frac{\sigma_h^2 x^2 + \sigma_1^2}{\sigma_h^2 x^2 + \sigma_2^2}\right), \quad \forall x \in \mathbb{R} \tag{2.21}$$

where

$$g(y) = \ln p_Y(y; F^*) - \int p_{Z|Y}(z|y) \ln(p_Z(z; F^*))\, dz \tag{2.22}$$

Next, we define

$$s = \frac{1}{\sigma_h^2 x^2 + \sigma_1^2} \quad \text{and} \quad \Delta = \frac{1}{\sigma_2^2 - \sigma_1^2} \tag{2.23}$$

and get, after some simplification,

$$\int e^{-sy} g(y)\, dy = -\frac{1}{s}\frac{\gamma}{\sigma_h^2}\left(\frac{1}{s} - \sigma_1^2 - \sigma_h^2 P\right) - \frac{1}{s} C_s - \frac{1}{s}\ln\Delta + \frac{1}{s}\ln(s + \Delta) \tag{2.24}$$

Now, we recognize the left hand side of (2.24) as the Laplace transform of $g(y)$, and by taking an inverse Laplace transform of both sides, we get

$$g(y) = -\frac{\gamma}{\sigma_h^2} y - e^{-\Delta y}\ln y - \Delta \int_0^y e^{-\Delta t} \ln t\, dt - K \tag{2.25}$$

where $K = -\gamma\frac{\sigma_1^2}{\sigma_h^2} - \gamma P + C_s + \ln\Delta + C_E$ is a constant, and C_E is Euler's constant.

Thus, we have

$$\ln p_Y(y; F^*) = \int p_{Z|Y}(z|y) \ln p_Z(z; F^*)\, dz - \frac{\gamma}{\sigma_h^2} y \\ - e^{-\Delta y} \ln y - \Delta \int_0^y e^{-\Delta t} \ln t\, dt - K \tag{2.26}$$

Now, we bound each term on the right hand side of (2.26) to obtain a lower bound on $p_Y(y)$. First, we note

$$\Delta \int_0^y e^{-\Delta t} \ln t\, dt \leq \Delta \int_0^y e^{-\Delta t} \ln y\, dt = (1 - e^{-\Delta y}) \ln y \tag{2.27}$$

and thus,

$$e^{-\Delta y} \ln y + \Delta \int_0^y e^{-\Delta t} \ln t\, dt \leq \ln y \tag{2.28}$$

To bound the first term on the right hand side of (2.26), we first bound $p_Z(z)$ as,

$$\begin{aligned} p_Z(z) &= \int \frac{1}{\sigma_h^2 x^2 + \sigma_2^2} e^{-\frac{z}{\sigma_h^2 x^2 + \sigma_2^2}}\, dF(x) && (2.29) \\ &\geq \int \frac{1}{\sigma_h^2 x^2 + \sigma_2^2} e^{-\frac{z}{\sigma_2^2}}\, dF(x) && (2.30) \\ &\geq \frac{1}{\sigma_h^2 P + \sigma_2^2} e^{-\frac{z}{\sigma_2^2}} && (2.31) \end{aligned}$$

where we used the fact that $\frac{1}{\sigma_h^2 x^2 + \sigma_2^2}$ is convex in x^2, Jensen's inequality and the power constraint. Thus, the first term on the right hand side of (2.26) can be bounded as:

$$\int p_{Z|Y}(z|y) \ln p_Z(z; F^*) \, dz \geq \ln K_1 - K_2 \mathbb{E}[Z|Y=y] \tag{2.32}$$

where $K_1 = \frac{1}{\sigma_h^2 P + \sigma_2^2}$ and $K_2 = \frac{1}{\sigma_2^2}$.

From (2.6), $W = V + \tilde{N}$. Denoting the real and imaginary parts of a complex number by subscripts R and I, respectively, we note that,

$$Z = |W|^2 = Y + |\tilde{N}|^2 + 2V_R\tilde{N}_R + 2V_I\tilde{N}_I \tag{2.33}$$

and therefore,

$$\mathbb{E}[Z|Y=y] = y + (\sigma_2^2 - \sigma_1^2) \tag{2.34}$$

Using (2.32), (2.34) and (2.28) along with (2.26), we get,

$$\ln p_Y(y; F^*) \geq \ln K_1 - K_2 y - K_2(\sigma_2^2 - \sigma_1^2) - \frac{\gamma}{\sigma_h^2} y - \ln y - K \tag{2.35}$$

which implies that

$$p_Y(y) \geq \frac{c_1}{y} e^{-c_2 y}, \quad y \geq 0 \tag{2.36}$$

for some constants c_1 and c_2. We note that

$$\int_0^1 \frac{c_1}{y} e^{-c_2 y} dy = \infty \tag{2.37}$$

for any value of c_1 and c_2, and hence $p_Y(y)$ cannot be a valid probability density function and thus we have reached a contradiction. This contradiction implies that the two cases stated at the beginning cannot occur, i.e., the optimum probability distribution cannot contain a continuous interval, or an infinite number of discrete points in a finite interval. Therefore, the optimum probability distribution contains at most a finite number of discrete points in any given finite interval. ■

In the following theorem, we show that, in fact, X^* has a finite number of mass points.

Theorem 2 *The support of X^* has a finite number of points.*

Proof: Again, we proceed by contradiction. Assume that the support of X^* has infinitely many points. Let us denote the mass points by the increasing sequence $\{x_i\}_{i=1}^{\infty}$ and their corresponding probabilities by the sequence $\{p_i\}_{i=1}^{\infty}$. Since, by Theorem 1, there are only finitely many points in any bounded interval, we must have $\lim_{i\to\infty} x_i = \infty$. Then, the output probability is bounded as

$$p_Y(y) = \sum_{i=1}^{\infty} p_i p_{Y|X}(y|x_i) \tag{2.38}$$

$$\geq p_i p_{Y|X}(y|x_i) \tag{2.39}$$

$$= \frac{p_i}{\sigma_h^2 x_i^2 + \sigma_1^2} e^{-\frac{y}{\sigma_h^2 x_i^2 + \sigma_1^2}} \tag{2.40}$$

A similar bound clearly holds for $p_Z(z)$ as well. Also, $p_Y(y)$ can be upper-bounded as,

$$p_Y(y) = \int \frac{1}{\sigma_h^2 x^2 + \sigma_1^2} e^{-\frac{y}{\sigma_h^2 x^2 + \sigma_1^2}} \, dF(x) \tag{2.41}$$

$$\leq \int \frac{1}{\sigma_1^2} e^{-\frac{y}{\sigma_h^2 x^2 + \sigma_1^2}} \, dF(x) \tag{2.42}$$

$$\leq \frac{1}{\sigma_1^2} e^{-\frac{y}{\sigma_h^2 P + \sigma_1^2}} \tag{2.43}$$

where we have used the fact that $e^{-\frac{y}{\sigma_h^2 x^2 + \sigma_1^2}}$ is concave in x^2, Jensen's inequality and the power constraint.

Now we observe that $f(x)$ in (2.18) is a continuously differentiable function in x. Also, KKT conditions in (2.17) imply that $f(x_i) = 0, \forall i \in \mathbb{N}$ and $f(x) \geq 0, \forall x \in \mathbb{R}$. Denoting the derivative of $f(x)$ by $f'(x)$, we must have $f'(x_i) = 0, \forall i$. If not, $f(x)$ will change sign in the neighbourhood of x_i, which is not possible. To compute the derivative of $f(x)$, we note

$$\frac{dp_{Y|X}(y|x)}{dx} = \frac{2\sigma_h^2 x}{(\sigma_h^2 x^2 + \sigma_1^2)^2} \left[y - (\sigma_h^2 x^2 + \sigma_1^2) \right] p_{Y|X}(y|x) \tag{2.44}$$

and obtain,

$$\begin{aligned} f'(x) =& 2\gamma x + \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_1^2} - \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_2^2} \\ &+ \frac{2\sigma_h^2 x}{(\sigma_h^2 x^2 + \sigma_1^2)^2} \int y p_{Y|X}(y|x) \ln\left(p_Y(y)\right) dy \\ &- \frac{2\sigma_h^2 x}{(\sigma_h^2 x^2 + \sigma_1^2)} \int p_{Y|X}(y|x) \ln\left(p_Y(y)\right) dy \end{aligned}$$

$$
\begin{aligned}
&- \frac{2\sigma_h^2 x}{(\sigma_h^2 x^2 + \sigma_2^2)^2} \int z p_{Z|X}(z|x) \ln\left(p_Z(z)\right) dz \\
&+ \frac{2\sigma_h^2 x}{(\sigma_h^2 x^2 + \sigma_2^2)} \int p_{Z|X}(z|x) \ln\left(p_Z(z)\right) dz
\end{aligned} \tag{2.45}
$$

Using the bounds in (2.40) and (2.43) to bound the different terms in (2.45), we obtain

$$
\begin{aligned}
f'(x) \geq & 2\gamma x + \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_1^2} - \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_2^2} - \frac{2\sigma_h^2 x}{\sigma_h^2 x_i^2 + \sigma_2^2} \\
& + \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_1^2} \ln\left(\frac{p_i}{\sigma_h^2 x_i^2 + \sigma_1^2}\right) - \frac{4\sigma_h^2 x}{\sigma_h^2 x_i^2 + \sigma_1^2} \\
& - \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_1^2} \ln\frac{1}{\sigma_1^2} + \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_2^2} \ln\left(\frac{1}{\sigma_h^2 x_i^2 + \sigma_2^2}\right) \\
& - \frac{2\sigma_h^2 x}{\sigma_h^2 x^2 + \sigma_2^2} \ln\frac{1}{\sigma_2^2} + \frac{2\sigma_h^2 x}{\sigma_h^2 P + \sigma_1^2} + \frac{4\sigma_h^2 x}{\sigma_h^2 P + \sigma_2^2}
\end{aligned} \tag{2.46}
$$

Therefore, we have

$$
f'(x_i) \geq \left(2\gamma + \frac{2\sigma_h^2}{\sigma_h^2 P + \sigma_1^2} + \frac{4\sigma_h^2}{\sigma_h^2 P + \sigma_2^2}\right) x_i + o(x_i) \tag{2.47}
$$

where $o(x)$ denotes a function such that $o(x) \to 0$ as $x \to \infty$. By our assumption, $x_i \to \infty$ as $i \to \infty$. Thus, (2.47) implies that $f'(x_i) \to \infty$ as $i \to \infty$ which is a contradiction, since, $f'(x_i) = 0$, for every i. We conclude, therefore, that the support of the optimal input distribution has a finite number of points. ■

2.5 Numerical Results

In this section, we present simple numerical examples to verify and illustrate the results of this chapter. Fig. 2.2 shows an example of how the KKT conditions are satisfied for a particular value of power P. The plot shows that there are two mass points, one at 0 and the other at 1.7348, with probabilities 0.9668 and 0.0332, respectively. The secrecy capacity for this case is 0.03 bits per channel use.

Fig. 2.3 shows how the positions of the optimum probability mass points change with power. Note that there is always a mass point at zero. As the power increases, the optimum probability distribution has more and more mass points. At the transitions, where a new mass point is introduced, the numerical algorithm becomes unstable, nevertheless, it seems that the mass points originate far from the origin with very low probabilities (as seen in Fig. 2.4), then come closer towards the origin before receding away again with increasing power. Fig. 2.4 shows the probabilities of the corresponding mass points. As expected, at very low power, the probability of the point at zero is high, and it decreases as power is increased. The probabilities stabilize asymptotically.

2.6 Conclusions

In this chapter, we considered the fast Rayleigh fading wiretap channel with coherence time of one symbol duration. We proved that the optimal input distribution that achieves the secrecy capacity is discrete with finite number of mass points.

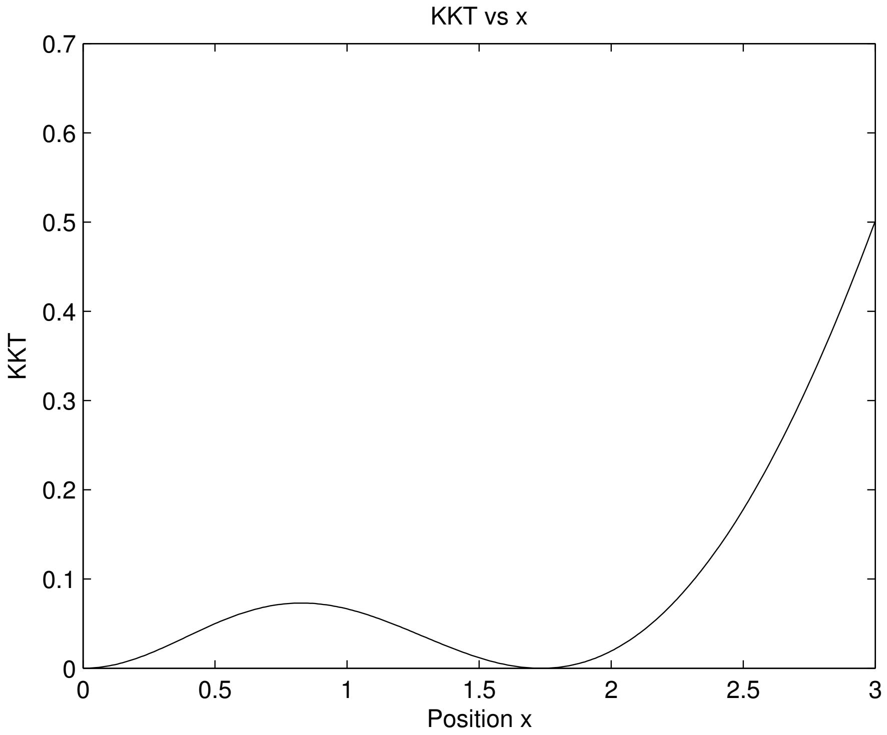


Figure 2.2: An optimal distribution satisfying the KKT conditions with $P = 0.1$, $\sigma_h = \sigma_1 = 1$, $\sigma_2 = 2$, $\gamma = 0.2461$, $C_s = 0.03$ and $F(x) = 0.9668\delta(x) + 0.0332\delta(x - 1.7348)$.

The secrecy capacity does not scale with power and the secure degrees of freedom (s.d.o.f.) is zero.

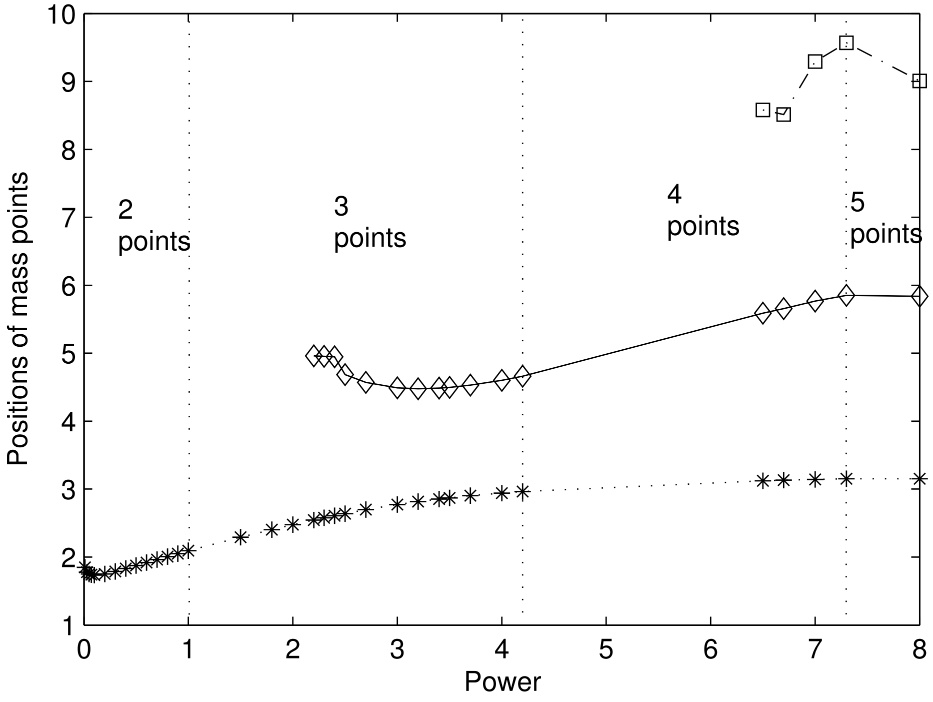


Figure 2.3: The position of the mass points versus power.

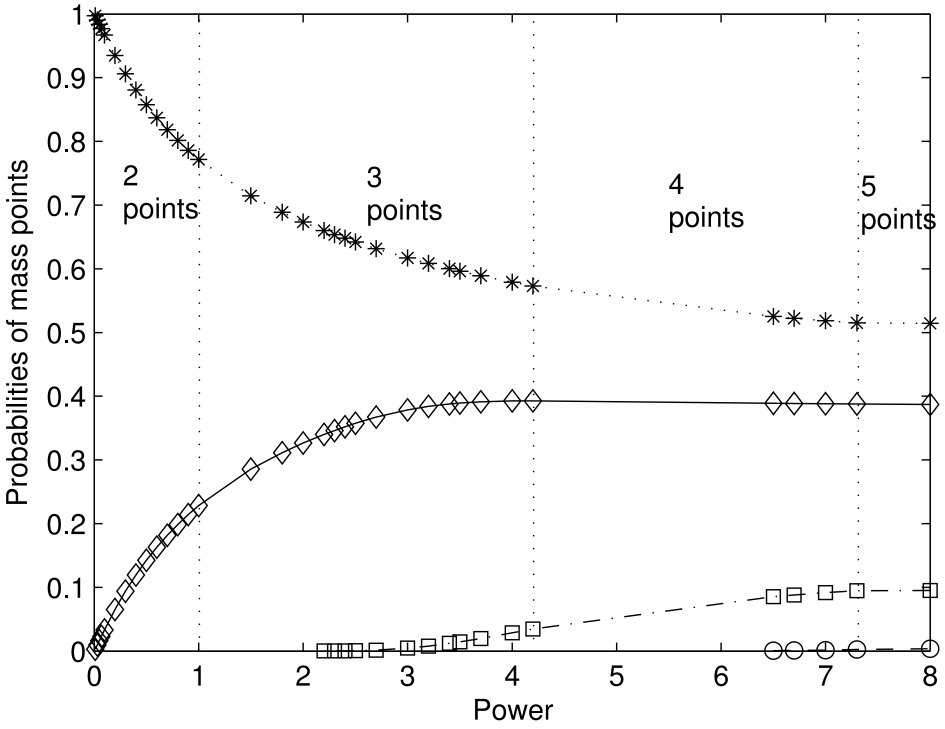


Figure 2.4: The probabilities of the mass points versus power.

Chapter 3: Secure Degrees of Freedom of One-hop Wireless Networks with No Eavesdropper CSIT

3.1 Introduction

In this chapter, we investigate how the unavailability of the eavesdropper's channel state information at the transmitter (CSIT) affects the optimal secure rates for three important channel models: the wiretap channel with helpers, the multiple access wiretap channel, and the interference channel with an external eavesdropper. With full eavesdropper CSIT, references [4, 63] determine the optimal s.d.o.f. of the wiretap channel with M helpers to be $\frac{M}{M+1}$. Further, references [5, 64] determine the optimal sum s.d.o.f. for the K-user multiple access wiretap channel with full eavesdropper CSIT to be $\frac{K(K-1)}{K(K-1)+1}$, while for the interference channel with an external eavesdropper, the optimal sum s.d.o.f. is shown to be $\frac{K(K-1)}{2K-1}$ in references [6, 43].

In this chapter, we show that for the wiretap channel with M helpers, an s.d.o.f. of $\frac{M}{M+1}$ is achievable even without eavesdropper's CSIT; thus, there is no loss of s.d.o.f. due to the unavailability of eavesdropper CSIT in this case. For the multiple access wiretap channel and the interference channel with an external eavesdropper, however, the optimal s.d.o.f. decreases when there is no eavesdropper CSIT. In particular, without eavesdropper CSIT, the K-user multiple access wiretap channel reduces to a wiretap channel with $(K-1)$ helpers and the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{K(K-1)+1}$ to $\frac{K-1}{K}$. For the interference channel with an external eavesdropper, the optimal sum s.d.o.f. decreases from $\frac{K(K-1)}{2K-1}$ to $\frac{K-1}{2}$ in the absence of eavesdropper CSIT.

In order to establish the optimal sum s.d.o.f., we propose achievable schemes and provide matching converse proofs for each of these channel models. Our achievable schemes are based on real interference alignment [7] and vector space alignment [8] for fixed and fading channel gains, respectively. To prove the converse, we combine techniques from [4, 6] and [10]. We exploit a key result in [10] that the output entropy at a receiver whose CSIT is not available is at least as large as the output entropy at a receiver whose CSIT is available, even when the transmitters cooperate and transmit correlated signals. Intuitively, no alignment of signals is possible at the receiver whose CSIT is unavailable; therefore, the signals occupy the maximum possible space at that receiver. We combine this insight with the techniques of [4, 6] to establish the optimal sum s.d.o.f. for the multiple access wiretap channel with no eavesdropper CSIT to be $\frac{K-1}{K}$ and the optimal sum s.d.o.f. for the interference channel with an external eavesdropper and no eavesdropper CSIT to be $\frac{K-1}{2}$.

3.2 System Model and Definitions

In this chapter, we consider three fundamental channel models: the wiretap channel with helpers, the multiple access wiretap channel, and the interference channel with an external eavesdropper. For each channel model, we consider two scenarios of channel variation: a) fixed channel gains, and b) fading channel gains. For the case of fixed channel gains, we assume that the channel gains are non-zero and have been drawn independently from a continuous distribution with bounded support and remain fixed for the duration of the communication. On the other hand, in the fading scenario, we assume a fast fading model, where the channel gains vary in an i.i.d. fashion from one symbol period to another. In each symbol period, the channel gains are non-zero and are drawn from a common continuous distribution with bounded support. The common continuous distribution is known at all the terminals in the system. While we consider only real channel gains in this chapter, we believe our results can be extended for complex channel gains; for further discussion, see [4, Section X].

Let Ω denote the collection of all channel gains in n channel uses. We assume full CSI at the receivers, that is, both the legitimates receivers and the eavesdropper know Ω. In the following subsections we describe each channel model and provide the relevant definitions.

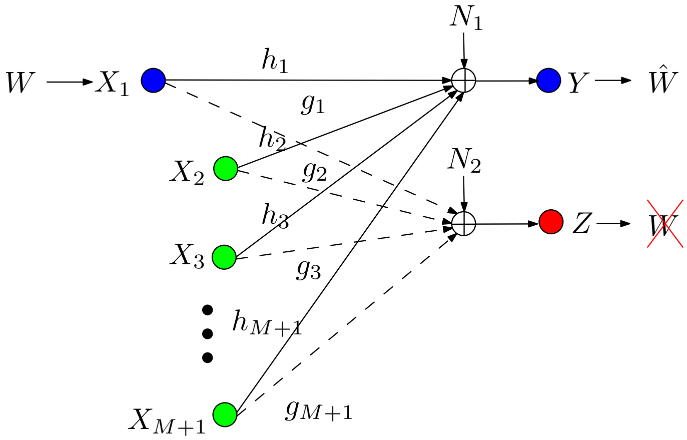


Figure 3.1: Wiretap channel with M helpers.

3.2.1 Wiretap Channel with Helpers

The wiretap channel with M helpers, see Fig. 3.1, is described by,

$$Y(t) = h_1(t)X_1(t) + \sum_{i=2}^{M+1} h_i(t)X_i(t) + N_1(t) \tag{3.1}$$

$$Z(t) = g_1(t)X_1(t) + \sum_{i=2}^{M+1} g_i(t)X_i(t) + N_2(t) \tag{3.2}$$

where $X_1(t)$ denotes the channel input of the legitimate transmitter, and $Y(t)$ denotes the channel output at the legitimate receiver, at time t. $X(i), i = 2, \dots, M+1$, are the channel inputs of the M helpers, and $Z(t)$ denotes the channel output at the eavesdropper, at time t. In addition, $N_1(t)$ and $N_2(t)$ are white Gaussian noise variables with zero-mean and unit-variance. Here, $h_i(t)$, $g_i(t)$ are the channel gains of the users to the legitimate receiver and the eavesdropper, respectively, and $g_i(t)$s are not known at any of the transmitters. All channel inputs are subject to the average power constraint $\mathbb{E}[X_i(t)^2] \leq P$, $i = 1, \dots, M+1$.

The legitimate transmitter wishes to transmit a message W which is uniformly distributed in $\mathcal{W}$. A secure rate R, with $R = \frac{\log|\mathcal{W}|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W \neq \hat{W}] \leq \epsilon_n$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W; Z^n, \Omega) \leq \epsilon_n \tag{3.3}$$

where $\epsilon_n \to 0$ as $n \to \infty$. The supremum of all achievable secure rates R is the secrecy capacity C_s and the s.d.o.f., d_s, is defined as

$$d_s = \lim_{P \to \infty} \frac{C_s}{\frac{1}{2} \log P} \tag{3.4}$$

3.2.2 Multiple Access Wiretap Channel

The K-user multiple access wiretap channel, see Fig. 3.2, is described by,

$$Y(t) = \sum_{i=1}^{K} h_i(t) X_i(t) + N_1(t) \tag{3.5}$$

$$Z(t) = \sum_{i=1}^{K} g_i(t) X_i(t) + N_2(t) \tag{3.6}$$

where $X_i(t)$ denotes the ith user's channel input, $Y(t)$ denotes the legitimate receiver's channel output, and $Z(t)$ denotes the eavesdropper's channel output, at time t. In addition, $N_1(t)$ and $N_2(t)$ are white Gaussian noise variables with zero-mean and unit-variance. Here, $h_i(t)$, $g_i(t)$ are the channel gains of the users to the legitimate receiver and the eavesdropper, respectively, and $g_i(t)$s are not known at any of the transmitters. All channel inputs are subject to the average power

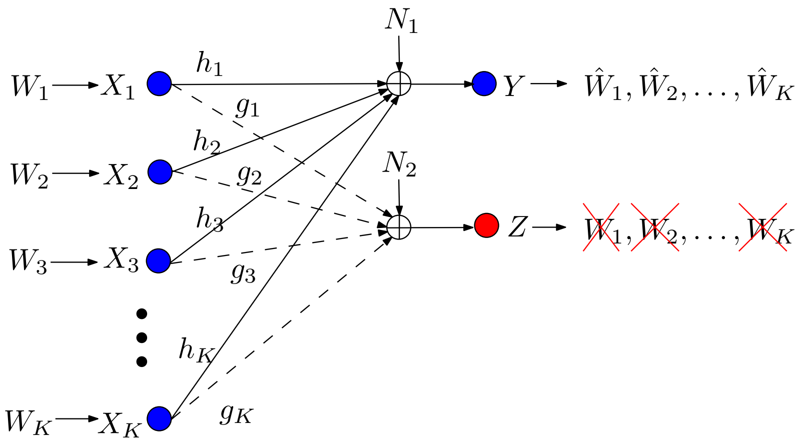


Figure 3.2: K-user multiple access wiretap channel.

constraint $\mathbb{E}[X_i(t)^2] \leq P$, $i = 1, \ldots, K$.

The ith user transmits message W_i which is uniformly distributed in $\mathcal{W}_i$. A secure rate tuple $(R_1, \ldots, R_K)$, with $R_i = \frac{\log |\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W_i \neq \hat{W}_i] \leq \epsilon_n$, for $i = 1, \ldots, K$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W^K; Z^n, \Omega) \leq \epsilon_n \tag{3.7}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Here, W^K denotes the set of all the messages, i.e., $\{W_1, \ldots, W_K\}$. An s.d.o.f. tuple $(d_1, \ldots, d_K)$ is said to be achievable if a rate tuple $(R_1, \ldots, R_K)$ is achievable with $d_i = \lim\limits_{P \to \infty} \frac{R_i}{\frac{1}{2}\log P}$. The sum s.d.o.f., d_s, is the largest achievable $\sum_{i=1}^K d_i$.

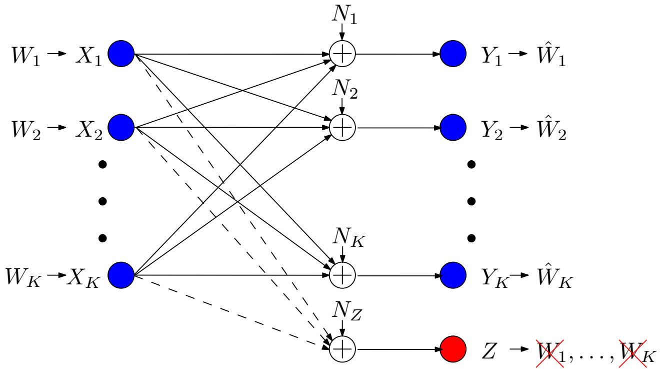

N_1
$W_1 \rightarrow X_1$
$Y_1 \rightarrow \hat{W}_1$
N_2
$W_2 \rightarrow X_2$
$Y_2 \rightarrow \hat{W}_2$
N_K
$W_K \rightarrow X_K$
$Y_K \rightarrow \hat{W}_K$
N_Z
$Z \rightarrow \cancel{W_1}, \ldots, \cancel{W_K}$

Figure 3.3: K-user interference channel with an external eavesdropper.

3.2.3 Interference Channel with External Eavesdropper

The K-user interference channel with an external eavesdropper, see Fig. 3.3, is described by

$$Y_i(t) = \sum_{j=1}^{K} h_{ji}(t)X_j(t) + N_i(t), \quad i = 1, \ldots, K \tag{3.8}$$

$$Z(t) = \sum_{j=1}^{K} g_j(t)X_j(t) + N_Z(t) \tag{3.9}$$

where $Y_i(t)$ is the channel output of receiver i, $Z(t)$ is the channel output at the eavesdropper, $X_j(t)$ is the channel input of transmitter j, $h_{ji}(t)$ is the channel gain from transmitter j to receiver i, $g_j(t)$ is the channel gain from transmitter j to the eavesdropper, and $\{N_1(t), \ldots, N_K(t), N_Z(t)\}$ are mutually independent zero-mean unit-variance white Gaussian noise random variables, at time t. The channel gains to the eavesdropper, $g_i(t)$s are not known at any of the transmitters. All channel inputs are subject to the average power constraint $\mathbb{E}[X_i(t)^2] \leq P$, $i = 1, \ldots, K$.

Transmitter i wishes to send a message W_i, chosen uniformly from a set $\mathcal{W}_i$, to receiver i. The messages $W_1, \ldots, W_K$ are mutually independent. A secure rate tuple $(R_1, \ldots, R_K)$, with $R_i = \frac{\log|\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at all the legitimate receivers, namely, $\Pr[W_i \neq \hat{W}_i] \leq \epsilon_n$, for $i = 1, \ldots, K$, and the security condition

$$\frac{1}{n} I(W^K; Z^n, \Omega) \leq \epsilon_n \tag{3.10}$$

where $\epsilon_n \to 0$, as $n \to \infty$. An s.d.o.f. tuple $(d_1, \ldots, d_K)$ is said to be achievable if a rate tuple $(R_1, \ldots, R_K)$ is achievable with $d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2}\log P}$. The sum s.d.o.f., d_s, is the largest achievable $\sum_{i=1}^{K} d_i$.

3.3 Main Results and Discussion

In this section, we state the main results of this chapter. We have the following theorems:

Theorem 3 *For the wiretap channel with M helpers and no eavesdropper CSIT, the optimal sum s.d.o.f., d_s, is given by,*

$$d_s = \frac{M}{M+1} \tag{3.11}$$

for fading channel gains and almost surely, for fixed channel gains.

Theorem 4 *For the K-user multiple access wiretap channel with no eavesdropper*

CSIT, the optimal sum s.d.o.f., d_s, is given by,

$$d_s = \frac{K-1}{K} \tag{3.12}$$

for fading channel gains and almost surely, for fixed channel gains.

Theorem 5 *For the K-user interference channel with an external eavesdropper with no eavesdropper CSIT, the optimal sum s.d.o.f., d_s, is given by,*

$$d_s = \frac{K-1}{2} \tag{3.13}$$

for fading channel gains and almost surely, for fixed channel gains.

We present the proofs of Theorems 3 and 4 in Section 3.4 and the proof of Theorem 5 in Section 3.5. Let us first state a corollary obtained from Theorems 3 and 4, which establishes the entire s.d.o.f. region of the K-user multiple access wiretap channel with no eavesdropper CSIT.

Corollary 1 *The s.d.o.f. region of the K-user multiple access wiretap channel with no eavesdropper CSIT is given by,*

$$d_i \geq 0, \; i = 1, \dots, K, \quad \textit{and} \quad \sum_{i=1}^{K} d_i \leq \frac{K-1}{K} \tag{3.14}$$

The proof of Corollary 1 follows directly from Theorems 3 and 4. In particular, we can treat the K-user multiple access wiretap channel as a $(K-1)$ helper wiretap channel with transmitter i as the legitimate transmitter, and the remaining

Channel model	**With Eve CSIT**	**Without Eve CSIT**
Wiretap channel with M helpers	$\frac{M}{M+1}$	$\frac{M}{M+1}$
K-user multiple access wiretap channel	$\frac{K(K-1)}{K(K-1)+1}$	$\frac{K-1}{K}$
K-user interference channel with an external eavesdropper	$\frac{K(K-1)}{2K-1}$	$\frac{K-1}{2}$

Table 3.1: Summary of s.d.o.f. values with and without eavesdropper CSIT.

transmitters as helpers. This achieves the corner points $d_i = \frac{K-1}{K}$ and $d_j = 0$ for $j \neq i$ from Theorem 3. Therefore, given the sum s.d.o.f. upper bound in Theorem 4, and that each corner point with s.d.o.f. of $\frac{K-1}{K}$ for a single user is achievable, the region in Corollary 1 follows.

It is useful, at this point, to compare our results to the cases when the eavesdropper's CSI is available at the transmitter. Table 3.1 shows a comparison of the optimal s.d.o.f. values with and without eavesdropper CSIT. Interestingly, there is no loss in s.d.o.f. for the wiretap channel with helpers due to the absence of eavesdropper's CSIT.

However, for the multiple access wiretap channel and the interference channel with an external eavesdropper, the optimal s.d.o.f. decreases due to the unavailability of eavesdropper CSIT. For the multiple access wiretap channel, as the number of users, K increases, the optimal sum s.d.o.f. approaches 1 as $\sim \frac{1}{K^2}$ with eavesdropper's CSIT but only as $\sim \frac{1}{K}$ without eavesdropper's CSIT. Therefore, the loss of s.d.o.f. as a fraction of the optimal sum s.d.o.f. with eavesdropper CSIT is $\sim \frac{1}{K}$ for large K.

For the interference channel with an external eavesdropper too, there is a loss in s.d.o.f. due to the unavailability of the eavesdropper's CSIT. However, in this case, the optimal s.d.o.f. without eavesdropper CSIT closely tracks the s.d.o.f. with eavesdropper CSIT. In fact, it can be verified that the s.d.o.f. loss is bounded by $\frac{1}{4}$, which implies that the loss of s.d.o.f. as a fraction of the optimal s.d.o.f. with eavesdropper CSIT is $\sim \frac{1}{K}$ for large K, in this case also.

For the multiple access wiretap channel, we also consider the case where some of the transmitters have the eavesdropper's CSI. We state our achievable s.d.o.f. in this case in the following theorem.

Theorem 6 *In the K-user MAC-WT, where $1 \leq m \leq K$ transmitters have eavesdropper CSI, and the remaining $K-m$ transmitters have no eavesdropper CSI, the following sum s.d.o.f. is achievable,*

$$d_s = \frac{m(K-1)}{m(K-1)+1} \tag{3.15}$$

for fading channel gains and almost surely, for fixed channel gains.

We present the proof of Theorem 6 in Section 3.6. In this case, we note that when only one user has eavesdropper CSIT, i.e., $m = 1$, our achievable rate is the same as when no user has eavesdropper CSIT as in Theorem 4. On the other hand, when all users have eavesdropper CSIT, i.e., $m = K$, our achievable rate is the same as the optimal sum s.d.o.f. in [4]. We note that our achievable sum s.d.o.f. varies from the no eavesdropper CSIT result in Theorem 4 to the full eavesdropper CSIT sum s.d.o.f. in [4] as m increases from 1 to K.

3.4 Proofs of Theorems 3 and 4

First, we note that an achievable scheme for Theorem 3 implies an achievable scheme for Theorem 4, since the K-user multiple access wiretap channel may be treated as a wiretap channel with $(K-1)$ helpers. Further, we note that a converse for Theorem 4 suffices as a converse for Theorem 3. Thus, we will only provide achievable schemes for Theorem 3 and a converse proof for Theorem 4. An alternate converse for Theorem 3 also follows from the converse presented in [4] for the wiretap channel with M helpers and with eavesdropper CSIT, as the converse for the case of known eavesdropper CSIT serves as a converse for the case of unknown eavesdropper CSIT.

Next, we note that under our fixed and fading channel models, it suffices to provide an achievable scheme for the case of fixed channel gains and prove a converse for the case of fading channel gains. In general, the optimal sum s.d.o.f. d_s for fixed channel gains may depend on the channel realization, and we denote by $d_s^{fixed}(\boldsymbol{\omega})$, the optimal sum s.d.o.f. for the fixed channel realization $\boldsymbol{\omega} \overset{\Delta}{=} (\boldsymbol{h}, \boldsymbol{g})$, where $\boldsymbol{h}$ and $\boldsymbol{g}$ denote the channel realizations of the legitimate receivers' channels and the eavesdropper's channel, respectively. We provide, in Section 3.4.1, a real alignment based achievable scheme for the wiretap channel with M helpers, and thus, show that the optimal sum s.d.o.f. $d_s^{fixed}(\boldsymbol{\omega}) \geq \frac{K-1}{K}$ for almost all channel gains $\boldsymbol{\omega}$. Now, we show that

$$d_s^{var} \geq \mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})] \tag{3.16}$$

where d_s^{var} is the optimal sum s.d.o.f. in the fading channel gains case, by showing that a sum s.d.o.f. of $\mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})]$ is achievable on the fading channel. To that end, we argue along the lines of [65]. Essentially, we quantize the (finite) range of each legitimate user's channel gain h_i, $i = 1, \dots, K$ into m equal intervals $[h_i^k, h_i^{k+1})$, $k = 1, \dots, m$. This results in the quantization of $\boldsymbol{h}$ into m^K rectangles $\mathcal{R}_j$, $j = 1, \dots, m^K$. Let n_j be the number of channel uses when the channel realization $\boldsymbol{h} \in \mathcal{R}_j$. Due to the i.i.d. nature of channel variation, $\frac{n_j}{n} \to \mathbb{P}(\boldsymbol{h} \in \mathcal{R}_j)$, as $n \to \infty$. When the channel realization $\boldsymbol{h} \in \mathcal{R}_j$, one can achieve the s.d.o.f. given by $\operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g})$, almost surely, over n_j channel uses as $n_j \to \infty$, where $\operatorname{ess\,inf}$ denotes the essential infimum. Therefore, over n channel uses, one can achieve an s.d.o.f. of at least $\sum_{j=1}^{m^K} \operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g}) \mathbb{P}(\boldsymbol{h} \in \mathcal{R}_j)$ which converges to $\mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})]$ as $m \to \infty$, using the fact that $\sum_{j=1}^{m^K} \operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g}) \mathbb{I}(\boldsymbol{h} \in \mathcal{R}_j)$ converges pointwise almost everywhere to $d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g})$, and noting that for each m, $\sum_{j=1}^{m^K} \operatorname{ess\,inf}_{\boldsymbol{h} \in \mathcal{R}_j} d_s^{fixed}(\boldsymbol{h}, \boldsymbol{g}) \mathbb{I}(\boldsymbol{h} \in \mathcal{R}_j)$ is bounded by 1 for the multiple access wiretap channel.

Next, we prove the converse for the multiple access wiretap channel with fading channel gains in Section 3.4.2, and show that

$$d_s^{var} \leq \frac{K-1}{K} \tag{3.17}$$

Combining (3.16), (3.17) and the fact that $d_s^{fixed}(\boldsymbol{\omega}) \geq \frac{K-1}{K}$ for almost all $\boldsymbol{\omega}$, we have

$$d_s^{var} = \frac{K-1}{K} \tag{3.18}$$

In order to determine the optimal sum s.d.o.f. in the fixed channel gains case, we first note using (3.16) and (3.18) that

$$\mathbb{E}_{\boldsymbol{\omega}}[d_s^{fixed}(\boldsymbol{\omega})] \leq d_s^{var} = \frac{K-1}{K} \tag{3.19}$$

Combined with the fact that $d_s^{fixed}(\boldsymbol{\omega}) \geq \frac{K-1}{K}$ for almost all channel gains $\boldsymbol{\omega}$, which follows from the achievable scheme we provide in Section 3.4.1, we have that

$$d_s^{fixed}(\boldsymbol{\omega}) = \frac{K-1}{K} \tag{3.20}$$

for almost all channel gains $\boldsymbol{\omega}$.

Thus, the achievable scheme for the wiretap channel with M helpers and fixed channel gains in Section 3.4.1, and the converse for the multiple access wiretap channel with fading channel gains in Section 3.4.2 suffice for the proofs of Theorems 3 and 4.

3.4.1 Achievability for the Wiretap Channel with Helpers

We now present achievable schemes for the wiretap channel with M helpers for fixed channel gains. We provide an achievable scheme for the case of fading channel gains in Appendix 3.8.1. Although one can utilize the achievable scheme developed for the fixed channel gains case on a symbol-by-symbol basis in the fading channel gains case, the alternative scheme provided in Appendix 3.8.1 is worth examining as it is designed to reveal similarities in the achievable schemes for the fixed and fading channel gains cases.

For fixed channels, we use the technique of real interference alignment [7, 9]. 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 $C(a, Q)$

$$C(a, Q) = a\{-Q, -Q+1, \ldots, Q-1, Q\} \tag{3.21}$$

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

$$X_1 = \frac{1}{h_1}U_1 + \sum_{k=2}^{M+1} \alpha_k V_k \tag{3.22}$$

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

$$X_j = \frac{1}{h_j} U_j \tag{3.23}$$

Note that, neither the legitimate transmitter signal in (3.22) nor the helper signals in (3.23) depend on the eavesdropper CSI $\{g_k\}_{k=1}^{M+1}$. With these selections, observations of the receivers are given by,

$$Y = \sum_{k=2}^{M+1} h_1 \alpha_k V_k + \left(\sum_{j=1}^{M+1} U_j \right) + N_1 \tag{3.24}$$

$$Z = \sum_{k=2}^{M+1} g_1 \alpha_k V_k + \sum_{j=1}^{M+1} \frac{g_j}{h_j} U_j + N_2 \tag{3.25}$$

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. This is similar to the case when there is full eavesdropper CSIT [4]. However, unlike the scheme in [4], we can no longer align signals at the eavesdropper due to lack of eavesdropper CSIT. Instead, 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

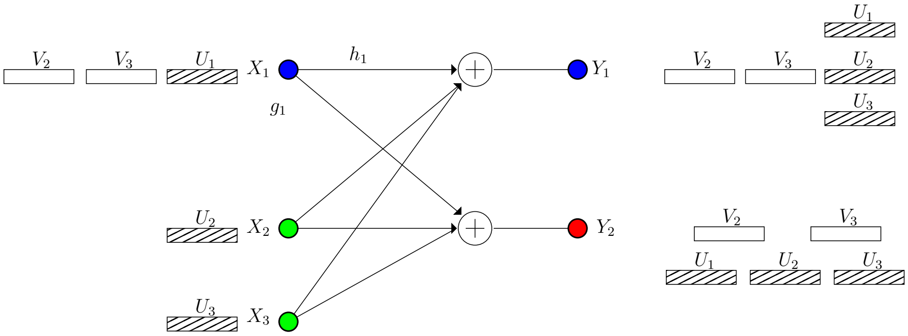


Figure 3.4: Illustration of the alignment scheme for the Gaussian wiretap channel with M helpers with no eavesdropper CSI.

Fig. 3.4. 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, as we will mathematically prove in the sequel.

The following secrecy rate is achievable [25]

$$C_s \geq I(\mathbf{V}; Y) - I(\mathbf{V}; Z) \tag{3.26}$$

where $\mathbf{V} \overset{\Delta}{=} \{V_2, V_3, \cdots, V_{M+1}\}$. Note that since Ω is known at both the legitimate receiver and the eavesdropper, it can be considered to be an additional output at both the legitimate receiver and the eavesdropper. Further, since $\mathbf{V}$ is chosen to be independent of Ω, Ω should appear in the conditioning of each of the mutual information quantities in (3.26). We keep this in mind, but drop it for the sake of notational simplicity.

First, we use Fano's inequality to bound the first term in (3.26). Note that the space observed at receiver 1 consists of $(2Q+1)^M(2MQ+2Q+1)$ points in $(M+1)$ dimensions, and the sub-signal in each dimension is drawn from a constellation of $C(a,(M+1)Q)$. Here, we use the property that $C(a,Q) \subset C(a,(M+1)Q)$. By using the Khintchine-Groshev theorem of Diophantine approximation in number theory [7,9], we can bound the minimum distance d_{min} between the points in receiver 1's space as follows: For any $\delta > 0$, there exists a constant k_δ such that

$$d_{min} \geq \frac{k_\delta a}{((M+1)Q)^{M+\delta}} \tag{3.27}$$

for almost all rationally independent $\{1, h_1\alpha_2, h_1\alpha_3, \cdots, h_1\alpha_{M+1}\}$, except for a set of Lebesgue measure zero. Then, we can upper bound the probability of decoding error of such a PAM scheme by considering the additive Gaussian noise at receiver 1,

$$\begin{aligned} \mathbb{P}\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] &\leq \exp\left(-\frac{d_{min}^2}{8}\right) && (3.28) \\ &\leq \exp\left(-\frac{a^2k_\delta^2}{8((M+1)Q)^{2(M+\delta)}}\right) && (3.29) \end{aligned}$$

where $\hat{\mathbf{V}}$ is the estimate of $\mathbf{V}$ by choosing the closest point in the constellation based on observation Y. For any $\delta > 0$, if we choose $Q = P^{\frac{1-\delta}{2(M+1+\delta)}}$ and $a = \gamma P^{\frac{1}{2}}/Q$, where γ is a constant independent of P, then

$$\begin{aligned} \mathbb{P}\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] &\leq \exp\left(-\frac{k_\delta^2\gamma^2(M+1)^2P}{8((M+1)Q)^{2(M+\delta)+2}}\right) && (3.30) \\ &= \exp\left(-\frac{k_\delta^2\gamma^2(M+1)^2P^\delta}{8(M+1)^{2(M+1+\delta)}}\right) && (3.31) \end{aligned}$$

and we can have $\mathbb{P}\left[\mathbf{V} \neq \hat{\mathbf{V}}\right] \to 0$ as $P \to \infty$. To satisfy the power constraint at the transmitters, we can simply choose

$$\gamma \leq \min\left\{\left[\frac{1}{|h_1|} + \sum_{k=2}^{M+1} |\alpha_k|\right]^{-1}, |h_2|, |h_3|, \cdots, |h_{M+1}|\right\} \tag{3.32}$$

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

$$H(\mathbf{V}|Y) \leq H(\mathbf{V}|\hat{\mathbf{V}}) \tag{3.33}$$

$$\leq 1 + \exp\left(-\frac{k_\delta^2 \gamma^2 (M+1)^2 P^\delta}{8(M+1)^{2(M+1+\delta)}}\right) \log(2Q+1)^M \tag{3.34}$$

$$= o(\log P) \tag{3.35}$$

where δ and γ are fixed, and $o(\cdot)$ is the little-o function. This means that

$$I(\mathbf{V}; Y) = H(\mathbf{V}) - H(\mathbf{V}|Y) \tag{3.36}$$

$$\geq H(\mathbf{V}) - o(\log P) \tag{3.37}$$

$$= \log(2Q+1)^M - o(\log P) \tag{3.38}$$

$$\geq \log P^{\frac{M(1-\delta)}{2(M+1+\delta)}} - o(\log P) \tag{3.39}$$

$$= \frac{M(1-\delta)}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) \tag{3.40}$$

Next, we need to bound the second term in (3.26),

$$I(\mathbf{V}; Z) = I(\mathbf{V}, \mathbf{U}; Z) - I(\mathbf{U}; Z|\mathbf{V}) \tag{3.41}$$

$$= I(\mathbf{V}, \mathbf{U}; Z) - H(\mathbf{U}|\mathbf{V}) + H(\mathbf{U}|Z, \mathbf{V}) \tag{3.42}$$

$$
\begin{aligned}
&= I(\mathbf{V}, \mathbf{U}; Z) - H(\mathbf{U}) + H(\mathbf{U}|Z, \mathbf{V}) && (3.43)\\
&= h(Z) - h(Z|\mathbf{V}, \mathbf{U}) - H(\mathbf{U}) + H(\mathbf{U}|Z, \mathbf{V}) && (3.44)\\
&= h(Z) - h(N_2) - H(\mathbf{U}) + H(\mathbf{U}|Z, \mathbf{V}) && (3.45)\\
&\leq h(Z) - h(N_2) - H(\mathbf{U}) + o(\log P) && (3.46)\\
&\leq \frac{1}{2}\log P - \frac{1}{2}\log 2\pi e - \log(2Q+1)^{M+1} + o(\log P) && (3.47)\\
&\leq \frac{1}{2}\log P - \frac{(M+1)(1-\delta)}{2(M+1+\delta)}\log P + o(\log P) && (3.48)\\
&= \frac{(M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (3.49)
\end{aligned}
$$

where $\mathbf{U} \triangleq \{U_1, U_2, \cdots, U_{M+1}\}$, and (3.46) is due to the fact that given $\mathbf{V}$ and Z, 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, $H(\mathbf{U}|Z, \mathbf{V}) \leq o(\log P)$ similar to the step in (3.35). In addition, $h(Z) \leq \frac{1}{2}\log P + o(\log P)$ in (3.47), since all the channel gains are drawn from a known distribution with bounded support.

Combining (3.40) and (3.49), we have

$$
\begin{aligned}
C_s &\geq I(\mathbf{V}; Y) - I(\mathbf{V}; Z) && (3.50)\\
&\geq \frac{M(1-\delta)}{M+1+\delta}\left(\frac{1}{2}\log P\right) - \frac{(M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) && (3.51)\\
&= \frac{M-(2M+2)\delta}{M+1+\delta}\left(\frac{1}{2}\log P\right) - o(\log P) && (3.52)
\end{aligned}
$$

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.

3.4.2 Converse for the Fading Multiple Access Wiretap Channel

We combine techniques from [4] and [10] to prove the converse. Here, we use $\mathbf{X}_i$ to denote the collection of all channel inputs $\{X_i(t),\ t = 1, \dots, n\}$ of transmitter i. Similarly, we use $\mathbf{Y}$ and $\mathbf{Z}$ to denote the channel outputs at the legitimate receiver and the eavesdropper, respectively, over n channel uses. We further define $\mathbf{X}_1^K$ as the collection of all channel inputs from all of the transmitters, i.e., $\{\mathbf{X}_i,\ i = 1 \dots, K\}$. Finally, for a fixed j, we use $\mathbf{X}_{-j}$ to denote all channel inputs from all transmitters except transmitter j, i.e., $\{\mathbf{X}_i,\ i \neq j,\ i = 1 \dots, K\}$. Since all receivers know Ω, it appears in the conditioning in every entropy and mutual information term below. We keep this in mind, but drop it for the sake of notational simplicity. We divide the proof into three steps.

3.4.2.1 Deterministic Channel Model

We will show that there is no loss of s.d.o.f. in considering the following integer-input integer-output deterministic channel in (3.53)-(3.54) instead of the one in (3.5)-(3.6)

$$Y(t) = \sum_{i=1}^{K} \lfloor h_i(t) X_i(t) \rfloor \tag{3.53}$$

$$Z(t) = \sum_{i=1}^{K} \lfloor g_i(t) X_i(t) \rfloor \tag{3.54}$$

with the constraint that

$$X_i \in \left\{0, 1, \dots, \left\lfloor \sqrt{P} \right\rfloor \right\} \tag{3.55}$$

To that end, we will show that given any codeword tuple $(\mathbf{X}_1^G, \dots, \mathbf{X}_K^G)$ for the original channel of (3.5)-(3.6), we can construct a codeword tuple $(\mathbf{X}_1^D, \dots, \mathbf{X}_K^D)$ with $X_i^D(t) = \left\lfloor X_i^G(t) \right\rfloor \mod \lfloor \sqrt{P} \rfloor$, for the deterministic channel of (3.53)-(3.54), that achieves an s.d.o.f. no smaller than the s.d.o.f. achieved by $(\mathbf{X}_1^G, \dots, \mathbf{X}_K^G)$ on the original channel. Let us denote by $\mathbf{Y}^G$ and $\mathbf{Z}^G$, the outputs of the original channel of (3.5)-(3.6), when $(\mathbf{X}_1^G, \dots, \mathbf{X}_K^G)$ is the input, that is,

$$Y^G(t) \triangleq \sum_{i=1}^{K} h_i(t) X_i^G(t) + N_1(t) \tag{3.56}$$

$$Z^G(t) \triangleq \sum_{i=1}^{K} g_i(t) X_i^G(t) + N_2(t) \tag{3.57}$$

Similarly, define

$$Y^D(t) \triangleq \sum_{i=1}^{K} \left\lfloor h_i(t) X_i^D(t) \right\rfloor \tag{3.58}$$

$$Z^D(t) \triangleq \sum_{i=1}^{K} \left\lfloor g_i(t) X_i^D(t) \right\rfloor \tag{3.59}$$

It suffices to show that

$$I(W_i; \mathbf{Y}^G) \leq I(W_i; \mathbf{Y}^D) + no(\log P) \tag{3.60}$$

$$I(W^K; \mathbf{Z}^D) \leq I(W^K; \mathbf{Z}^G) + no(\log P) \tag{3.61}$$

for every $i = 1, \ldots, K$. Here, (3.60) states that the information rate to the legitimate receiver in the discretized channel is at least as large as the information rate in the original Gaussian channel, and (3.61) states that the information leakage to the eavesdropper in the discretized channel is at most at the level of the information leakage in the original Gaussian channel, both of which quantified within a $o(\log P)$.

The proof of (3.60) follows along similar lines as the proof presented in [10, 66]; we include a sketch here for completeness. First, note that there is no loss of d.o.f. due to integer inputs and outputs. To see this, let us define $\bar{Y}^D(t) = \sum_{i=1}^{K} \lfloor h_i(t) \lfloor X_i^G(t) \rfloor \rfloor$, and $E(t) = Y^G(t) - \bar{Y}^D(t)$. We have

$$
\begin{aligned}
I(W_i; \boldsymbol{Y}^G|\Omega) =& I(W_i; \bar{\boldsymbol{Y}}^D + \boldsymbol{E}|\Omega) && (3.62)\\
\leq& I(W_i; \bar{\boldsymbol{Y}}^D, \boldsymbol{E}|\Omega) && (3.63)\\
=& I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) + I(W_i; \boldsymbol{E}|\bar{\boldsymbol{Y}}^D, \Omega) && (3.64)\\
\leq& I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) + h(\boldsymbol{E}|\Omega) - h(\boldsymbol{E}|\bar{\boldsymbol{Y}}^D, W_i, \boldsymbol{X}_1^K, \Omega) && (3.65)\\
\leq& I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) + \sum_{t=1}^{n} \mathbb{E}_\Omega \left[\frac{1}{2} \log \left(\sum_{i=1}^{K} (h_i(t) + 1)^2 + 1 \right) \right] - h(\boldsymbol{N}_1) \\
& && (3.66)\\
\leq& I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) + no(\log P) && (3.67)
\end{aligned}
$$

Next, we show that imposing per-symbol power constraints as in (3.55) does not incur any additional loss of d.o.f. It suffices to prove:

$$
I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) - I(W_i; \boldsymbol{Y}^D|\Omega) \leq no(\log P) \tag{3.68}
$$

We define $\hat{X}_i(t) = \lfloor X_i^G(t) \rfloor - X_i^D(t)$ and $\hat{Y} = \bar{Y}^D - Y^D$, and

$$I(W_i; \bar{\boldsymbol{Y}}^D|\Omega) \leq I(W_i; \boldsymbol{Y}^D, \hat{\boldsymbol{Y}}|\Omega) \tag{3.69}$$

$$\leq I(W_i; \boldsymbol{Y}^D|\Omega) + H(\hat{\boldsymbol{Y}}|\Omega) \tag{3.70}$$

$$\leq I(W_i; \boldsymbol{Y}^D|\Omega) + \sum_{t=1}^{n} H(\hat{Y}(t)|\Omega) \tag{3.71}$$

$$\leq I(W_i; \boldsymbol{Y}^D|\Omega) + \sum_{t=1}^{n} \sum_{i=1}^{K} H(\hat{X}_i(t)) + no(\log P) \tag{3.72}$$

Now, it can be shown that $H((\hat{X}_i(t)) \leq o(\log P)$ using the steps in [10][eqns. (138)-(158)]. Thus, (3.68) is proved. This concludes the sketch of proof of (3.60).

To prove (3.61), we first define

$$\bar{Z}(t) \overset{\Delta}{=} \sum_{i=1}^{K} \left\lfloor g_i(t) \left\lfloor X_i^G(t) \right\rfloor \right\rfloor \tag{3.73}$$

$$\hat{Z}(t) \overset{\Delta}{=} \bar{Z}(t) - Z^D(t) \tag{3.74}$$

$$\tilde{Z}(t) \overset{\Delta}{=} \left\lfloor Z^G(t) \right\rfloor - \bar{Z}(t) - \lfloor N_2(t) \rfloor \tag{3.75}$$

Then, we have,

$$I(W^K; \mathbf{Z}^D) \leq I(W^K; \mathbf{Z}^D, \mathbf{Z}^G, \bar{\mathbf{Z}}) \tag{3.76}$$

$$= I(W^K; \mathbf{Z}^G) + I(W^K; \bar{\mathbf{Z}}|\mathbf{Z}^G) + I(W^K; \mathbf{Z}^D|\bar{\mathbf{Z}}, \mathbf{Z}^G) \tag{3.77}$$

$$\leq I(W^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\mathbf{Z}^G) + H(\mathbf{Z}^D|\bar{\mathbf{Z}}, \mathbf{Z}^G) \tag{3.78}$$

$$\leq I(W^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\lfloor \mathbf{Z}^G \rfloor) + H(\mathbf{Z}^D|\bar{\mathbf{Z}}) \tag{3.79}$$

$$\leq I(W^K; \mathbf{Z}^G) + H(\bar{\mathbf{Z}}|\bar{\mathbf{Z}} + \tilde{\mathbf{Z}} + \lfloor \mathbf{N}_2 \rfloor) + H(\hat{\mathbf{Z}}) \tag{3.80}$$

$$\leq I(W^K;\mathbf{Z}^G)+\sum_{t=1}^{n}H(\bar{Z}(t)|\bar{Z}(t)+\tilde{Z}(t)+\lfloor N_2(t)\rfloor)+\sum_{t=1}^{n}H(\hat{Z}(t)) \tag{3.81}$$

$$\leq I(W^K;\mathbf{Z}^G)+no(\log P) \tag{3.82}$$

where $\lfloor \mathbf{Z}^G \rfloor = \big(\lfloor Z^G(1)\rfloor,\ldots,\lfloor Z^G(n)\rfloor\big)$. Here, (3.82) follows since $H(\hat{Z}(t)) \leq o(\log P)$ following the steps of the proof in [10, Appendix A.2]. In addition, recalling that Ω appears in the conditioning of each term in (3.81), note that $H(\bar{Z}(t)|\bar{Z}(t)+\tilde{Z}(t)+\lfloor N_2(t)\rfloor,\Omega) \leq \mathbb{E}\left[H(\bar{Z}(t)|\bar{Z}(t)+\tilde{Z}(t)+\lfloor N_2(t)\rfloor, g_1^K=\tilde{g}_1^K)\right]$. To bound this term, in going from (3.81) to (3.82), we have used the following lemma [67, Lemma E.1, Appendix E]

Lemma 1 *Consider integer valued random variables x, r and s such that*

$$x \perp r \tag{3.83}$$

$$s \in \{-L,\ldots,0,\ldots,L\} \tag{3.84}$$

$$\mathbb{P}(|r|\geq k)\leq e^{-f(k)} \tag{3.85}$$

for all positive k, for some integer L and a function $f(.)$. Let

$$y = x+r+s \tag{3.86}$$

Then,

$$H(x|y) \leq \log(2L+1) + 2\log_2 e \left(\sum_{k=1}^{\infty} f(k) e^{-f(k)} \right) + \frac{2L+1}{2} + N_f \tag{3.87}$$

where

$$N_f = \left| \left\{ n \in \mathbb{Z}^+ | e^{-f(n)} > \frac{1}{2} \right\} \right| \tag{3.88}$$

Note that, in our case, $\tilde{Z}(t)$ is integer valued and is bounded by $\sum_{i=1}^{K} \tilde{g}_i(t) + K + 1$ for each realization $\tilde{g}_i(t)$ of $g_i(t)$, and we have

$$\begin{aligned}
\mathbb{P}(| \lfloor N_2(t) \rfloor | > k) =& \mathbb{P}(|N_2(t) - \{N_2(t)\} | > k) && (3.89)\\
\leq& \mathbb{P}(|N_2(t)| + | \{N_2(t)\} | > k) && (3.90)\\
\leq& \mathbb{P}(|N_2(t)| + 1 > k) && (3.91)\\
\leq& e^{\frac{(k-1)^2}{2}} && (3.92)
\end{aligned}$$

Thus, using the choice $f(k) = \frac{(k-1)^2}{2}$, N_f is clearly bounded and thus, $H(\bar{Z}(t)|\bar{Z}(t) + \tilde{Z}(t) + \lfloor N_2(t) \rfloor, \Omega) \leq o(\log P)$, which is the step going from (3.81) to (3.82).

Therefore, the s.d.o.f. of the deterministic channel in (3.53)-(3.54) with integer channel inputs as described in (3.55) is no smaller than the s.d.o.f. of the original channel in (3.5)-(3.6). Consequently, any upper bound (e.g., converse) developed for the s.d.o.f. of (3.53)-(3.54) will serve as an upper bound for the s.d.o.f. of (3.5)-(3.6). Thus, we will consider this deterministic channel in the remaining part of the converse.

3.4.2.2 An Upper Bound on the Sum Rate

We begin as in the *secrecy penalty lemma* in [4], i.e., [4, Lemma 1]. Note that, unlike [4, Lemma 1], channel inputs are integer here and satisfy (3.55):

$$n\sum_{i=1}^{K} R_i \leq I(W^K;\mathbf{Y}) - I(W^K;\mathbf{Z}) + n\epsilon \tag{3.93}$$

$$\leq I(W^K;\mathbf{Y}|\mathbf{Z}) + n\epsilon \tag{3.94}$$

$$\leq I(\mathbf{X}_1^K;\mathbf{Y}|\mathbf{Z}) + n\epsilon \tag{3.95}$$

$$\leq H(\mathbf{Y}|\mathbf{Z}) + n\epsilon \tag{3.96}$$

$$= H(\mathbf{Y},\mathbf{Z}) - H(\mathbf{Z}) + n\epsilon \tag{3.97}$$

$$\leq H(\mathbf{X}_1^K,\mathbf{Y},\mathbf{Z}) - H(\mathbf{Z}) + n\epsilon \tag{3.98}$$

$$= H(\mathbf{X}_1^K) - H(\mathbf{Z}) + n\epsilon \tag{3.99}$$

$$\leq \sum_{k=1}^{K} H(\mathbf{X}_k) - H(\mathbf{Z}) + n\epsilon \tag{3.100}$$

where (3.99) follows since $H(\mathbf{Y},\mathbf{Z}|\mathbf{X}_1^K) = 0$ for the channel in (3.53)-(3.54). Also, to ensure decodability at the legitimate receiver, we use the *role of a helper lemma* in [4], i.e., [4, Lemma 2],

$$n\sum_{i\neq j} R_i \leq I(W_{-j};\mathbf{Y}) + n\epsilon' \tag{3.101}$$

$$\leq I(\mathbf{X}_{-j};\mathbf{Y}) + n\epsilon' \tag{3.102}$$

$$=H(\mathbf{Y})-H(\mathbf{Y}|\mathbf{X}_{-j})+n\epsilon' \tag{3.103}$$

$$=H(\mathbf{Y})-H\left(\sum_{i=1}^{K}\lfloor\mathbf{h}_i\mathbf{X}_i\rfloor|\mathbf{X}_{-j}\right)+n\epsilon' \tag{3.104}$$

$$=H(\mathbf{Y})-H(\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor)+n\epsilon' \tag{3.105}$$

$$=H(\mathbf{Y})-H(\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor,\mathbf{X}_j)+H(\mathbf{X}_j|\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor)+n\epsilon' \tag{3.106}$$

$$\leq H(\mathbf{Y})-H(\mathbf{X}_j)+H(\mathbf{X}_j|\lfloor\mathbf{h}_j\mathbf{X}_j\rfloor)+n\epsilon' \tag{3.107}$$

$$\leq H(\mathbf{Y})-H(\mathbf{X}_j)+\sum_{t=1}^{n}H(X_j(t)|\lfloor h_j(t)X_j(t)\rfloor)+n\epsilon' \tag{3.108}$$

$$\leq H(\mathbf{Y})-H(\mathbf{X}_j)+n\epsilon'+nc \tag{3.109}$$

where $\mathbf{h}_j\mathbf{X}_j \triangleq \{h_j(t)X_j(t), t=1,\ldots,n\}$, and recalling that Ω appears in the conditioning of each term in (3.108), (3.109) follows using the following lemma.

Lemma 2 *Let X be an integer valued random variable satisfying* (3.55)*, and h be drawn from a distribution $F(h)$ satisfying $\int_{-\infty}^{\infty}\log\left(1+\frac{1}{|h|}\right)dF(h)\leq c$ for some $c\in\mathbb{R}$. Then,*

$$H(X|\lfloor hX\rfloor,h)\leq c \tag{3.110}$$

The proof of this lemma is presented in Appendix 3.8.3. The constraint imposed in Lemma 2 is a mild technical condition. A sufficient condition for satisfying the constraint is that there exists an $\epsilon>0$ such that the probability density function (pdf) is bounded in the interval $(-\epsilon,\epsilon)$. This is due to the fact that $\log\left(1+\frac{1}{|h|}\right)\leq$

$\log\left(1+\frac{1}{|\epsilon|}\right)$, when $|h| > \epsilon$ and following:

$$\begin{aligned}\int_{-\epsilon}^{\epsilon} f(h)\log\left(1+\frac{1}{|h|}\right)dh \leq & M\int_{-\epsilon}^{\epsilon}\log\left(1+\frac{1}{|h|}\right)dh && (3.111)\\ \leq & 2M\left[\int_{0}^{\epsilon}\log\left(1+h\right)dh + \int_{0}^{\epsilon}|\log h| dh\right] && (3.112)\\ \leq & c && (3.113)\end{aligned}$$

where $f(h) \leq M$ on $(-\epsilon, \epsilon)$, and the last step follows since both integrals in (3.112) are bounded. Most common distributions such as Gaussian, exponential and Laplace satisfy this condition.

Eliminating $H(\mathbf{X}_j)$s using (3.100) and (3.109), we get,

$$\begin{aligned}Kn\sum_{i=1}^{K} R_i \leq & KH(\mathbf{Y}) - H(\mathbf{Z}) + nK(\epsilon' + c) + n\epsilon && (3.114)\\ \leq & (K-1)\frac{n}{2}\log P + (H(\mathbf{Y}) - H(\mathbf{Z})) + n\epsilon'' && (3.115)\end{aligned}$$

where $\epsilon'' = o(\log P)$. Dividing by n and letting $n \to \infty$,

$$K\sum_{i=1}^{K} R_i \leq (K-1)\frac{1}{2}\log P + \epsilon'' + \lim_{n\to\infty}\frac{1}{n}\left(H(\mathbf{Y}) - H(\mathbf{Z})\right) \qquad (3.116)$$

Now dividing by $\frac{1}{2}\log P$ and taking $P \to \infty$,

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{K} + \frac{1}{K}\lim_{P\to\infty}\lim_{n\to\infty}\frac{H(\mathbf{Y}) - H(\mathbf{Z})}{\frac{n}{2}\log P} \qquad (3.117)$$

3.4.2.3 Bounding the Difference of Entropies

We now upper bound the difference of entropies $H(\mathbf{Y}) - H(\mathbf{Z})$ in (3.117) as:

$$H(\mathbf{Y}) - H(\mathbf{Z}) \leq \sup_{\{\mathbf{X}_i\}:\mathbf{X}_i \perp\!\!\!\perp \mathbf{X}_j} H(\mathbf{Y}) - H(\mathbf{Z}) \tag{3.118}$$

$$\leq \sup_{\{\mathbf{X}_i\}} H(\mathbf{Y}) - H(\mathbf{Z}) \tag{3.119}$$

where $X \perp\!\!\!\perp Y$ is used to denote that X and Y are statistically independent and (3.119) follows from (3.118) by relaxing the condition of independence in (3.118). Since the $\mathbf{X}_i$s in (3.119) may be arbitrarily correlated, we can think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y}) - H(\mathbf{Z})$, where $\mathbf{Y}$ and $\mathbf{Z}$ are two single antenna receiver outputs, under the constraint that the channel gains to $\mathbf{Z}$ are unknown at the transmitter. This brings us to the K-user MISO broadcast channel setting of [10], where it is shown that the difference of entropies, $H(\mathbf{Y}) - H(\mathbf{Z})$ cannot be larger than $no(\log P)$, if the channel gains to the second receiver are unknown, even without security constraints. Indeed, we have the following lemma.

Lemma 3 *For the deterministic channel model stated in* (3.53)-(3.55)*, with the channel gains to* $\mathbf{Z}$ *unknown at the transmitter, we have*

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \leq no(\log P) \tag{3.120}$$

The proof of Lemma 3 follows along the lines of [10, eqns. (75)-(103)]; in order to make our proof self-contained[1], we provide a sketch of the relevant steps in Appendix 3.8.4.

Using (3.120) in (3.117), we have

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{K} \tag{3.121}$$

This completes the converse proof of Theorem 4.

3.5 Proof of Theorem 5

In this section, we present the proof of Theorem 5. We first present separate achievable schemes for fixed and fading channel gains and then present the converse. For the interference channel, we require asymptotic schemes with both real [9], and vector space alignment [8] techniques. The converse combines techniques from [43] and [10].

3.5.1 Achievability for the Interference Channel

An achievable scheme for the interference channel with an external eavesdropper and no eavesdropper CSIT is presented in [40, Theorem 3]. That scheme achieves sum s.d.o.f. of $\frac{K-2}{2}$. Here, we present the optimal schemes which achieve $\frac{K-1}{2}$ sum s.d.o.f for fixed channel gains. In this section, we focus on the case when $K = 3$, which highlights the main ideas of the general K-user scheme for fixed channel gains. We present a corresponding vector space alignment scheme for fading channel gains in

[1] Based on the suggestion of an anonymous reviewer.

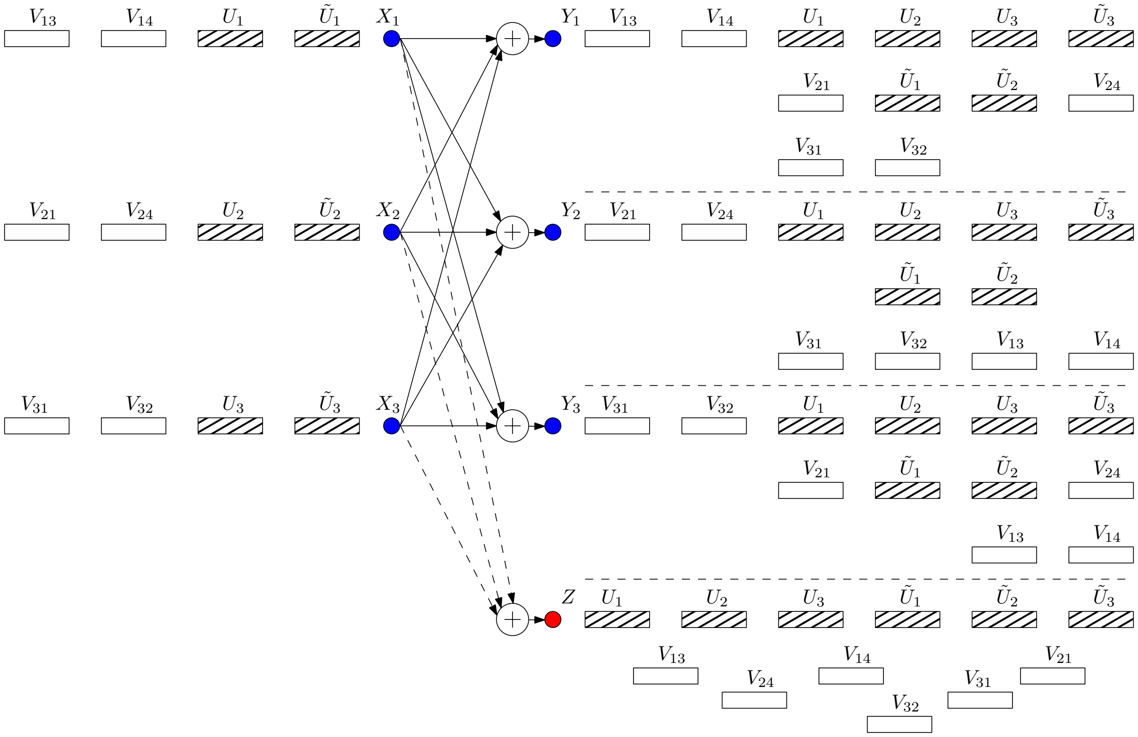

V_{13} V_{14} U_1 $\tilde{U}_1$ X_1
Y_1 V_{13} V_{14} U_1 U_2 U_3 $\tilde{U}_3$
V_{21} $\tilde{U}_1$ $\tilde{U}_2$ V_{24}
V_{31} V_{32}
V_{21} V_{24} U_2 $\tilde{U}_2$ X_2
Y_2 V_{21} V_{24} U_1 U_2 U_3 $\tilde{U}_3$
$\tilde{U}_1$ $\tilde{U}_2$
V_{31} V_{32} V_{13} V_{14}
V_{31} V_{32} U_3 $\tilde{U}_3$ X_3
Y_3 V_{31} V_{32} U_1 U_2 U_3 $\tilde{U}_3$
V_{21} $\tilde{U}_1$ $\tilde{U}_2$ V_{24}
V_{13} V_{14}
Z U_1 U_2 U_3 $\tilde{U}_1$ $\tilde{U}_2$ $\tilde{U}_3$
V_{13} V_{24} V_{14} V_{32} V_{31} V_{21}

Figure 3.5: Alignment for the interference channel with $K = 3$.

Appendix 3.8.5. We present the general K-user schemes for both fixed and fading channel gains in Appendix 3.8.6. As in the achievability for the wiretap channel with helpers, we use real interference alignment techniques for fixed channel gains. However, unlike the case of wiretap channel with helpers, we need to use asymptotic alignment in each case.

We use the technique of asymptotic real interference alignment introduced in [9]. Fig. 3.5 shows the desired signal alignment at the receivers and the eavesdropper. In the figure, the boxes labeled by V denote the message symbols, while the hatched boxes labeled with U denote artificial noise symbols. We observe from Fig. 3.5 that 4 out of 6 *signal dimensions* are buried in the artificial noise. Thus, heuristically, the s.d.o.f. for each legitimate user pair is $\frac{2}{6} = \frac{1}{3}$, and the sum s.d.o.f. is, therefore,

$3 \times \frac{1}{3} = 1$, as expected from our optimal sum s.d.o.f. expression $\frac{K-1}{2} = \frac{3-1}{2} = 1$.

In the K-user case, we have a similar alignment scheme. Each transmitter sends two artificial noise blocks along with $(K-1)$ message blocks. At each legitimate receiver, the $2K$ noise blocks from the K transmitters align such that they occupy only $(K+1)$ *block dimensions*. This is done by aligning $\tilde{U}_k$ with U_{k+1} for $k = 1, \ldots, (K-1)$, at each legitimate receiver. The unintended messages at each legitimate receiver are aligned underneath the $(K+1)$ artificial noise dimensions. To do so, we use two main ideas. First, two blocks from the same transmitter cannot be aligned at *any* receiver. This is because if two blocks from the same transmitter align at any receiver, they align at every other receiver as well, which is clearly not desirable. Secondly, each message block aligns with the same artificial noise block at every unintended receiver. Thus, in Fig. 3.5, V_{21} and V_{24} appear in different columns at each receiver. Further, V_{21} appears underneath U_1 at both of the unintended legitimate receivers 1 and 2. It can be verified that these properties hold for every message block. As an interesting by-product, this alignment scheme provides confidentiality of the unintended messages at the legitimate transmitters for free. The $(K-1)$ intended message blocks at a legitimate receiver occupy distinct block dimensions; thus, achieving a d.o.f. of $\frac{K-1}{2K}$ for each transmitter-receiver pair. At the eavesdropper, no alignment is possible since its CSIT is unavailable. Thus, the $2K$ artificial noise blocks occupy the full space of $2K$ block dimensions. This ensures security of the messages at the eavesdropper.

Note that we require two artificial noise blocks to be transmitted from each transmitter. When the eavesdropper CSIT is available, the optimal achievable scheme, presented in [6], requires one artificial noise block from each transmitter; the K noise blocks from the K transmitters are aligned with the messages at the eavesdropper in order to ensure security. In our case, however, the eavesdropper's CSIT is not available. Thus, in order to guarantee security, we need a total of $2K$ noise blocks to occupy the full space of $2K$ block dimensions at the eavesdropper. This is achieved by sending two artificial noise blocks from each transmitter. Further, to achieve an s.d.o.f. of $\frac{K-1}{2K}$ per user pair, we need to create $(K-1)$ noise-free message block dimensions at each legitimate receiver. We ensure this by systematically aligning the $2K$ noise symbols to occupy only $(K+1)$ block dimensions at each legitimate receiver. To the best of our knowledge, this is the first achievable scheme in the literature that uses two artificial noise blocks from each transmitter and then aligns them to maximize the noise-free message dimensions at each legitimate receiver.

Let us now present the 3-user scheme in more detail. Let m be a large integer. Also, let c_1, c_2, c_3 and c_4 be real constants drawn from a fixed continuous distribution with bounded support independently of each other and of all the channel gains. This ensures that the c_is are *rationally independent* of each other and of the channel gains. Now, we define four sets T_i, $i = 1, \ldots, 4$, as follows:

$$T_1 \overset{\Delta}{=} \{h_{11}^{r_{11}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{21}^{r_{21}} h_{31}^{r_{31}} h_{32}^{r_{32}} h_{23}^{r_{32}} c_1^s :\ r_{jk}, s \in \{1, \ldots, m\}\} \tag{3.122}$$

$$T_2 \overset{\Delta}{=} \left\{ h_{21}^{r_{21}} h_{22}^{r_{22}} h_{23}^{r_{23}} \left(\frac{h_{12}}{h_{11}}\right)^{r_{12}} \left(\frac{h_{13}}{h_{11}}\right)^{r_{13}} h_{31}^{r_{31}} h_{32}^{r_{32}} c_2^s :\ r_{jk}, s \in \{1, \ldots, m\} \right\} \tag{3.123}$$

$$T_3 \overset{\Delta}{=} \left\{ h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} \left(\frac{h_{21}}{h_{22}}\right)^{r_{21}} \left(\frac{h_{23}}{h_{22}}\right)^{r_{23}} h_{12}^{r_{12}} h_{13}^{r_{13}} c_3^s :\ r_{jk}, s \in \{1, \ldots, m\} \right\} \tag{3.124}$$

$$T_4 \triangleq \{h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} h_{21}^{r_{21}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{23}^{r_{23}} c_4^s : \ r_{jk}, s \in \{1, \dots, m\}\} \tag{3.125}$$

Let M_i be the cardinality of the set T_i. Note that all the M_is are the same, which we denote by M, which is given as,

$$M \triangleq m^8 \tag{3.126}$$

We subdivide each message W_i into 2 independent sub-messages $V_{ij}, j = 1, \dots, 4, j \neq i, i+1$. For each transmitter i, let $\mathbf{p}_{ij}$ be the vector containing all the elements of T_j, for $j \neq i, i+1$. For any given (i,j) with $j \neq i, i+1$, $\mathbf{p}_{ij}$ represents the dimension along which message V_{ij} is sent. Further, at each transmitter i, let $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ be vectors containing all the elements in sets T_i and $\beta_i T_{i+1}$, respectively, where

$$\beta_i = \begin{cases} \frac{1}{h_{ii}}, & \text{if } i = 1, 2 \\ 1, & \text{if } i = 3 \end{cases} \tag{3.127}$$

The vectors $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ represent dimensions along which artificial noise symbols U_i and $\tilde{U}_i$, respectively, are sent. We define a $4M$ dimensional vector $\mathbf{b}_i$ by stacking the $\mathbf{p}_{ij}$s, $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ as

$$\mathbf{b}_i^T = \begin{bmatrix} \mathbf{p}_{i1}^T \dots \mathbf{p}_{i(i-1)}^T & \mathbf{p}_{i(i+2)}^T \dots \mathbf{p}_{i4} & \mathbf{q}_i & \tilde{\mathbf{q}}_i \end{bmatrix} \tag{3.128}$$

The transmitter encodes V_{ij} using an M dimensional vector $\mathbf{v}_{ij}$, and the cooperative jamming signals U_i and $\tilde{U}_i$ using M dimensional vectors $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. Each element of $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$ are drawn in an i.i.d. fashion from $C(a, Q)$ in (3.21). Let

$$\mathbf{a}_i^T = \begin{bmatrix}\mathbf{v}_{i1}^T \dots \mathbf{v}_{i(i-1)}^T & \mathbf{v}_{i(i+2)}^T \dots \mathbf{v}_{i4} & \mathbf{u}_i & \tilde{\mathbf{u}}_i\end{bmatrix} \tag{3.129}$$

The channel input of transmitter i is then given by

$$x_i = \mathbf{a}_i^T \mathbf{b}_i \tag{3.130}$$

Let us now analyze the structure of the received signals at the receivers. For example, consider receiver 1. The desired signals at receiver 1, $\mathbf{v}_{13}$ and $\mathbf{v}_{14}$ arrive along dimensions $h_{11}T_3$ and $h_{11}T_4$, respectively. Since only T_i (and not $T_j, j \neq i$) contains c_i, these dimensions are rationally independent. Thus, they appear along different columns in Fig. 3.5. The artificial noise symbols $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ and $\tilde{\mathbf{u}}_3$ arrive along dimensions $h_{11}T_1$, $h_{21}T_2$, $h_{31}T_3$ and $h_{31}T_4$, respectively. Again they are all rationally separate and thus, appear along different columns in Fig. 3.5. Further, they are all separate from the dimensions of the desired signals, because T_3 and T_4 do not contain h_{11}, while T_1 and T_2 do not contain either c_3 or c_4. On the other hand, the unintended signals $\mathbf{v}_{21}$ and $\mathbf{v}_{31}$ arrive along $h_{21}T_1$ and $h_{31}T_1$, and since T_1 contains powers of h_{21} and h_{31}, they align with the artificial noise $\mathbf{u}_1$ in $\tilde{T}_1$, where,

$$\tilde{T}_1 \overset{\Delta}{=} \{h_{11}^{r_{11}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{21}^{r_{21}} h_{31}^{r_{31}} h_{32}^{r_{32}} h_{23}^{r_{32}} c_1^s : \; r_{jk}, s \in \{1, \dots, m+1\}\} \tag{3.131}$$

Similarly, we define

$$\tilde{T}_2 \triangleq \left\{ h_{21}^{r_{21}} h_{22}^{r_{22}} h_{23}^{r_{23}} \left(\frac{h_{12}}{h_{11}}\right)^{r_{12}} \left(\frac{h_{13}}{h_{11}}\right)^{r_{13}} h_{31}^{r_{31}} h_{32}^{r_{32}} c_2^s : \; r_{jk}, s \in \{1, \ldots, m+1\} \right\} \tag{3.132}$$

$$\tilde{T}_3 \triangleq \left\{ h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} \left(\frac{h_{21}}{h_{22}}\right)^{r_{21}} \left(\frac{h_{23}}{h_{22}}\right)^{r_{23}} h_{12}^{r_{12}} h_{13}^{r_{13}} c_3^s : \; r_{jk}, s \in \{1, \ldots, m+1\} \right\} \tag{3.133}$$

$$\tilde{T}_4 \triangleq \{ h_{31}^{r_{31}} h_{32}^{r_{32}} h_{33}^{r_{33}} h_{21}^{r_{21}} h_{12}^{r_{12}} h_{13}^{r_{13}} h_{23}^{r_{23}} c_4^s : \; r_{jk}, s \in \{1, \ldots, m+1\} \} \tag{3.134}$$

We note that the unintended signals $\mathbf{v}_{32}$ and $\mathbf{v}_{24}$ arrive along $h_{31}T_2$ and $h_{21}T_4$ and thus, align with $\mathbf{u}_2$ and $\tilde{\mathbf{u}}_3$, respectively, in $\tilde{T}_2$ and $\tilde{T}_4$. Thus, they appear in the same column in Fig.3.5. Finally, the artificial noise symbols $\tilde{\mathbf{u}}_1$ and $\tilde{\mathbf{u}}_2$ align with $\mathbf{u}_2$ and $\mathbf{u}_3$, respectively.

At receiver 2, the desired signals $\mathbf{v}_{21}$ and $\mathbf{v}_{24}$ arrive along rationally independent dimensions $h_{22}T_1$ and $h_{22}T_4$, respectively. The artificial noise symbols $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ and $\tilde{\mathbf{u}}_3$ arrive along dimensions $h_{12}T_1$, $h_{22}T_2$, $h_{32}T_3$ and $h_{32}T_4$, respectively. Thus, they lie in dimensions $\tilde{T}_1$, $\tilde{T}_2$, $\tilde{T}_3$ and $\tilde{T}_4$, respectively. They are all separate from the dimensions of the desired signals, because $\tilde{T}_1$ and $\tilde{T}_4$ do not contain h_{22}, while $\tilde{T}_2$ and $\tilde{T}_3$ do not contain either c_1 or c_4. The artificial noise symbols $\tilde{\mathbf{u}}_1$ and $\tilde{\mathbf{u}}_2$ arrive along dimensions $\left(\frac{h_{12}}{h_{11}}\right) T_2$ and T_3, respectively; thus, they align with $\mathbf{u}_2$ and $\mathbf{u}_3$ in $\tilde{T}_2$ and $\tilde{T}_3$, respectively. The unintended signals $\mathbf{v}_{13}$ and $\mathbf{v}_{14}$ arrive along $h_{12}T_3$ and $h_{12}T_4$, respectively, and lie in $\tilde{T}_3$ and $\tilde{T}_4$, respectively. Similarly, $\mathbf{v}_{31}$ and $\mathbf{v}_{32}$ lie in $\tilde{T}_1$ and $\tilde{T}_2$, respectively. A similar analysis is true for receiver 3 as well.

At the eavesdropper, there is no alignment, since the channel gains of the eavesdropper are not known at the transmitters. In fact, the artificial noise symbols all arrive along different dimensions at the receiver. Thus, heuristically, they exhaust the decoding capability of the eavesdropper almost completely.

We note that the interference at each receiver is confined to the dimensions $\tilde{T}_1$, $\tilde{T}_2$, $\tilde{T}_3$ and $\tilde{T}_4$. Further, these dimensions are separate from the dimensions occupied by the desired signals at each receiver. Specifically, at receiver i, the desired signals occupy dimensions $h_{ii}T_j, j \neq i, i+1$. These dimensions are separate from $\tilde{T}_i$ and $\tilde{T}_{i+1}$, since only T_j contains powers of c_j. Further, $\tilde{T}_j, j \neq i, i+1$ do not contain powers of h_{ii}. Thus, the set

$$S = \left(\bigcup_{j \neq i, i+1} h_{ii} T_j \right) \bigcup \left(\bigcup_{j=1}^{4} \tilde{T}_j \right) \tag{3.135}$$

has cardinality

$$M_S = 2m^8 + 4(m+1)^8 \tag{3.136}$$

Intuitively, out of these M_S dimensions, $2m^8$ dimensions carry the desired signals. Thus, the s.d.o.f. of each legitimate user pair is $\frac{2m^8}{2m^8+4(m+1)^8}$ which approaches $\frac{1}{3}$ as $m \to \infty$. Thus, the sum s.d.o.f. is 1. We omit the formal calculation of the achievable rate here and instead present it in Appendix 3.8.7 for the general K-user case. Further, note that the unintended messages at each receiver are buried in artificial noise, see Fig. 3.5. Thus, our scheme provides confidentiality of messages from unintended legitimate receivers as well.

3.5.2 Converse for the Interference Channel

The steps of the converse are similar to that of the proof in Section 3.4.2. The notation here is also the same as in Section 3.4.2. Again, we divide the proof into three steps.

3.5.2.1 Deterministic Channel Model

We consider the deterministic channel given as,

$$Y_k(t) = \sum_{i=1}^{K} \lfloor h_{ik}(t) X_i(t) \rfloor \tag{3.137}$$

$$Z(t) = \sum_{i=1}^{K} \lfloor g_i(t) X_i(t) \rfloor \tag{3.138}$$

for $k = 1, \ldots, K$, with the constraint that

$$X_i(t) \in \left\{0, 1, \ldots, \left\lfloor \sqrt{P} \right\rfloor \right\} \tag{3.139}$$

We can show that there is no loss of s.d.o.f. in considering the channel in (3.137)-(3.138) instead of the one in (3.8)-(3.9), as in Section 3.4.2.1. Thus, we will consider this deterministic channel in the remaining part of the converse. Since all receivers know Ω, it appears in the conditioning in every entropy and mutual information term below. We keep this in mind, but drop it for the sake of notational simplicity.

3.5.2.2 An Upper Bound on the Sum Rate

We begin as in the *secrecy penalty lemma* in [4], i.e., [4, Lemma 1]. Note that, unlike [4, Lemma 1], channel inputs are integer here:

$$n\sum_{i=1}^{K} R_i \leq I(W^K;\mathbf{Y}_1^K) - I(W^K;\mathbf{Z}) + n\epsilon \tag{3.140}$$

$$\leq I(W^K;\mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon \tag{3.141}$$

$$\leq I(\mathbf{X}_1^K;\mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon \tag{3.142}$$

$$\leq H(\mathbf{Y}_1^K|\mathbf{Z}) + n\epsilon \tag{3.143}$$

$$= H(\mathbf{Y}_1^K,\mathbf{Z}) - H(\mathbf{Z}) + n\epsilon \tag{3.144}$$

$$\leq H(\mathbf{X}_1^K,\mathbf{Y}_1^K,\mathbf{Z}) - H(\mathbf{Z}) + n\epsilon \tag{3.145}$$

$$= H(\mathbf{X}_1^K) - H(\mathbf{Z}) + n\epsilon \tag{3.146}$$

$$\leq \sum_{k=1}^{K} H(\mathbf{X}_k) - H(\mathbf{Z}) + n\epsilon \tag{3.147}$$

where (3.146) follows since $H(\mathbf{Y}_1^K,\mathbf{Z}|\mathbf{X}_1^K)=0$ for the channel in (3.137)-(3.138).

Also, to ensure decodability at the legitimate receiver, we use the *role of a helper lemma* in [4], i.e., [4, Lemma 2],

$$nR_i \leq I(W_i;\mathbf{Y}_i) + n\epsilon' \tag{3.148}$$

$$\leq I(\mathbf{X}_i;\mathbf{Y}_i) + n\epsilon' \tag{3.149}$$

$$= H(\mathbf{Y}_i) - H(\mathbf{Y}_i|\mathbf{X}_i) + n\epsilon' \tag{3.150}$$

$$= H(\mathbf{Y}_i) - H(\lfloor \mathbf{h}_j\mathbf{X}_j \rfloor) + n\epsilon' \tag{3.151}$$

$$=H(\mathbf{Y}_i) - H(\lfloor \mathbf{h}_j \mathbf{X}_j \rfloor, \mathbf{X}_j) + H(\mathbf{X}_j | \lfloor \mathbf{h}_j \mathbf{X}_j \rfloor) + n\epsilon' \tag{3.152}$$

$$\leq H(\mathbf{Y}_i) - H(\mathbf{X}_j) + H(\mathbf{X}_j | \lfloor \mathbf{h}_j \mathbf{X}_j \rfloor) + n\epsilon' \tag{3.153}$$

$$\leq H(\mathbf{Y}_i) - H(\mathbf{X}_j) + \sum_{t=1}^{n} H(X_j(t) | \lfloor h_j(t) X_j(t) \rfloor) + n\epsilon' \tag{3.154}$$

$$\leq H(\mathbf{Y}_i) - H(\mathbf{X}_j) + n\epsilon' + nc \tag{3.155}$$

for every $i \neq j$, where (3.155) follows using Lemma 2.

Let Π be any derangement of $(1, \ldots, n)$, and let $j = \Pi(i)$. Then, using (3.155), we obtain,

$$\sum_{k=1}^{K} H(\mathbf{X}_k) \leq \sum_{k=1}^{K} H(\mathbf{Y}_k) - n \sum_{k=1}^{K} R_k + nK(\epsilon' + c) \tag{3.156}$$

Using (3.156) in (3.147), we get,

$$2n \sum_{i=1}^{K} R_i \leq \sum_{k=1}^{K} H(\mathbf{Y}_k) - H(\mathbf{Z}) + nK(\epsilon' + c) + n\epsilon \tag{3.157}$$

$$\leq (K-1)\frac{n}{2} \log P + (H(\mathbf{Y}_K) - H(\mathbf{Z})) + n\epsilon'' \tag{3.158}$$

where $\epsilon'' = o(\log P)$. Dividing by n and letting $n \to \infty$,

$$2 \sum_{i=1}^{K} R_i \leq (K-1)\frac{1}{2} \log P + \lim_{n \to \infty} \frac{1}{n} (H(\mathbf{Y}_K) - H(\mathbf{Z})) + \epsilon'' \tag{3.159}$$

Now dividing by $\frac{1}{2}\log P$ and taking $P \to \infty$,

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{2} + \frac{1}{2} \lim_{P\to\infty} \lim_{n\to\infty} \frac{H(\mathbf{Y}_K) - H(\mathbf{Z})}{\frac{n}{2}\log P} \tag{3.160}$$

3.5.2.3 Bounding the Difference of Entropies

As we did in Section 3.4.2.3, we enhance the system by relaxing the condition that channel inputs from different transmitters are mutually independent, and think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y}_K) - H(\mathbf{Z})$, where $\mathbf{Y}_K$ and $\mathbf{Z}$ are two single antenna receiver outputs, under the constraint that the channel gains to $\mathbf{Z}$ are unknown at the transmitter. Using Lemma 3, the difference of entropies, $H(\mathbf{Y}_K) - H(\mathbf{Z})$ cannot be larger than $no(\log P)$, if the channel gains to the second receiver is unknown. Thus,

$$H(\mathbf{Y}_K) - H(\mathbf{Z}) \leq no(\log P) \tag{3.161}$$

Using (3.161) in (3.160), we have

$$\sum_{i=1}^{K} d_i \leq \frac{K-1}{2} \tag{3.162}$$

This completes the converse proof of Theorem 5.

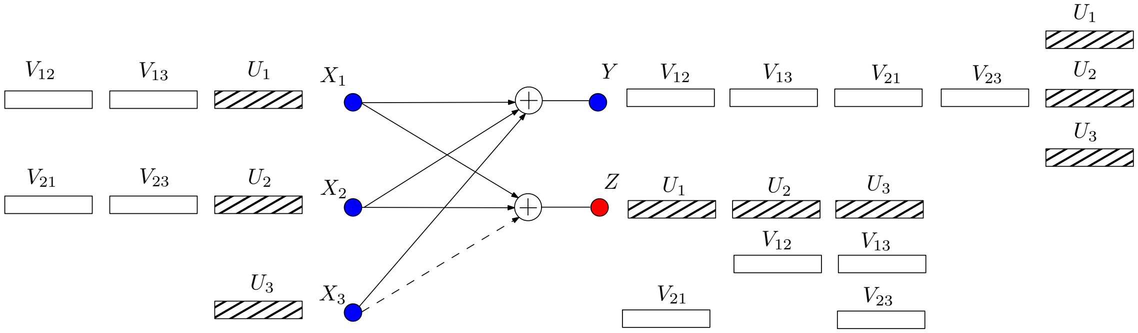


Figure 3.6: Alignment of signals when $K = 3$ and $m = 2$.

3.6 Proof of Theorem 6

As in the previous section, we focus on the fixed channel gains case and defer the achievable scheme for the fading channel gains to Appendix 3.8.9. Our scheme achieves a sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$, when m of the K transmitters have eavesdropper's CSI for almost all fixed channel gains. In particular, it achieves the s.d.o.f. tuple $(d_1, \ldots, d_m, d_{m+1}, \ldots, d_K) = \left(\frac{K-1}{m(K-1)+1}, \ldots, \frac{K-1}{m(K-1)+1}, 0, \ldots, 0\right)$. We employ $m(K-1) + K$ mutually independent random variables:

$$V_{ij}, \quad i = 1, \ldots, m, j = 1, \ldots, K, j \neq i$$

$$U_j, \quad j = 1, \ldots, K$$

uniformly drawn from the same PAM constellation $C(a, Q)$ in (3.21). Transmitter i, $i = 1, \ldots, m$ transmits:

$$X_i = \sum_{j=1, j\neq i}^{K} \frac{g_j}{h_j g_i} V_{ij} + \frac{1}{h_i} U_i, \quad i = 1, \ldots, m \tag{3.163}$$

while transmitters $(m+1)$ to K transmit

$$X_i = \frac{1}{h_i} U_i, \quad i = m+1, \dots, K \tag{3.164}$$

The channel outputs are given by,

$$Y = \sum_{i=1}^{m} \sum_{j \neq i} \frac{h_i g_j}{h_j g_i} V_{ij} + \sum_{i=1}^{K} U_i + N_1 \tag{3.165}$$

$$Z = \sum_{i=1}^{K} \frac{g_i}{h_i} \left(U_i + \sum_{j=1, j \neq i}^{m} V_{ji} \right) + N_2 \tag{3.166}$$

Intuitively, every V_{ij} gets superimposed with U_j at the eavesdropper, thus securing it. This is shown in Fig. 3.6. The proof of decodability and security guarantee follows exactly the proof in [4, Section IX-B] and is omitted here.

3.7 Conclusions

In this chapter, we established the optimal sum s.d.o.f. for three channel models: the wiretap channel with M helpers, the K-user multiple access wiretap channel, and the K-user interference channel with an external eavesdropper, in the absence of eavesdropper's CSIT. While there is no loss in the s.d.o.f. for the wiretap channel with helpers in the absence of the eavesdropper's CSIT, the s.d.o.f. decreases in the cases of the multiple access wiretap channel and the interference channel with an external eavesdropper. We show that in the absence of eavesdropper's CSIT, the K-user multiple access wiretap channel is equivalent to a wiretap channel with

$(K-1)$ helpers from a sum s.d.o.f. perspective. The question of optimality of the sum s.d.o.f. when some but not all of the transmitters have the eavesdropper's CSIT remains a subject of future work.

3.8 Appendix

3.8.1 Achievable Scheme for the Fading Wiretap Channel with Helpers

We present an achievable scheme for the wiretap channel with helpers for the case of fading channel gains, i.e., when the channel gains vary in an i.i.d. fashion from one time slot to another. In this scheme, the legitimate transmitter sends M independent Gaussian symbols, $\mathbf{V} = \{V_2, \dots, V_{M+1}\}$ securely to the legitimate receiver in $(M+1)$ time slots. This is done as follows:

At time $t = 1, \dots, M+1$, the legitimate transmitter sends a scaled artificial noise, i.e., cooperative jamming, symbol U_1 along with information symbols as,

$$X_1(t) = \frac{1}{h_1(t)} U_1 + \sum_{k=2}^{M+1} \alpha_k(t) V_k \tag{3.167}$$

where the $\alpha_k(t)$s are chosen such that the $(M+1) \times (M+1)$ matrix T, with entries $T_{ij} = \alpha_i(j) h_1(j)$, where $\alpha_1(j) = \frac{1}{h_1(j)}$, is full rank. The jth helper, $j = 2, \dots, M+1$, transmits:

$$X_j(t) = \frac{1}{h_j(t)} U_j \tag{3.168}$$

The channel outputs at time t are,

$$Y(t) = \sum_{k=2}^{M+1} h_1(t)\alpha_k(t)V_k + \left(\sum_{j=1}^{M+1} U_j\right) + N_1(t) \tag{3.169}$$

$$Z(t) = \sum_{k=2}^{M+1} g_1(t)\alpha_k(t)V_k + \sum_{j=1}^{M+1} \frac{g_j(t)}{h_j(t)}U_j + N_2(t) \tag{3.170}$$

Note the similarity of the scheme with that of the real interference scheme for fixed channel gains, i.e., the similarity between (3.169)-(3.170) and (3.24)-(3.25). Indeed the alignment structure after $(M+1)$ channel uses is exactly as in Fig. 3.4. Note also how the artificial noise symbols align at the legitimate receiver over $(M+1)$ time slots. At high SNR, at the end of the $(M+1)$ slots, the legitimate receiver recovers $(M+1)$ linearly independent equations with $(M+1)$ variables: $V_2, \dots, V_{M+1}, \sum_{j=1}^{M+1} U_j$. Thus, the legitimate receiver can recover $\mathbf{V} \triangleq (V_2, \dots, V_{M+1})$ within noise variance.

Formally, let us define $\mathbf{U} \triangleq (U_1, \dots, U_{M+1})$, $\mathbf{Y} \triangleq (Y(1), \dots, Y(M+1))$, and $\mathbf{Z} \triangleq (Z(1), \dots, Z(M+1))$. The observations at the legitimate receiver and the eavesdropper can then be compactly written as

$$\mathbf{Y} = (\mathbf{A}_V, \mathbf{A}_U)\begin{pmatrix} \mathbf{V}^T \\ \mathbf{U}^T \end{pmatrix} + \mathbf{N}_1 \tag{3.171}$$

$$\mathbf{Z} = (\mathbf{B}_V, \mathbf{B}_U)\begin{pmatrix} \mathbf{V}^T \\ \mathbf{U}^T \end{pmatrix} + \mathbf{N}_2 \tag{3.172}$$

where $\mathbf{A}_V$ is a $(M+1) \times M$ matrix with $(\mathbf{A}_V)_{ij} = h_1(i)\alpha_{j+1}(i)$, $\mathbf{A}_U$ is a $(M+1) \times$

$(M+1)$ matrix with all ones, $\mathbf{B}_V$ is a $(M+1)\times M$ matrix with $(\mathbf{B}_V)_{ij} = g_1(i)\alpha_{j+1}(i)$, and $\mathbf{B}_U$ is a $(M+1)\times(M+1)$ matrix with $(\mathbf{B}_U)_{ij} = \frac{g_j(i)}{h_j(i)}$. $\mathbf{N}_1$ and $\mathbf{N}_2$ are $(M+1)$ dimensional vectors containing the noise variables $N_1(t)$ and $N_2(t)$, respectively, for $t = 1, \ldots, M+1$. To calculate differential entropies, we use the following lemma.

Lemma 4 *Let* $\mathbf{A}$ *be an* $M \times N$ *dimensional matrix and let* $\mathbf{X} = (X_1, \ldots, X_N)^T$ *be a jointly Gaussian random vector with zero-mean and variance* $P\mathbf{I}$*. Also, let* $\mathbf{N} = (N_1, \ldots, N_M)^T$ *be a jointly Gaussian random vector with zero-mean and variance* $\sigma^2\mathbf{I}$*, independent of* $\mathbf{X}$*. If* $r = \mathit{rank}(\mathbf{A})$*, then,*

$$h(\mathbf{AX}+\mathbf{N}) = r\left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.173}$$

We present the proof of Lemma 4 in Appendix 3.8.2.

Using Lemma 4, we compute

$$\begin{aligned}
I(\mathbf{V};\mathbf{Y}) =& h(\mathbf{Y}) - h(\mathbf{Y}|\mathbf{V}) && (3.174)\\
=& (M+1)\frac{1}{2}\log P - h(\mathbf{A}_U\mathbf{U}^T + \mathbf{N}_1) + o(\log P) && (3.175)\\
=& (M+1)\left(\frac{1}{2}\log P\right) - \frac{1}{2}\log P + o(\log P) && (3.176)\\
=& M\left(\frac{1}{2}\log P\right) + o(\log P) && (3.177)
\end{aligned}$$

where (3.175) follows since $\mathbf{U}$ and $\mathbf{N}_1$ are independent of $\mathbf{V}$ and since $(\mathbf{A}_V, \mathbf{A}_U)$ has rank $(M+1)$ due to the choice of $\alpha_i(t)$s, and (3.176) follows since $\mathbf{A}_U$ clearly has rank 1. We also have,

$$
\begin{aligned}
I(\mathbf{V};\mathbf{Z}) =& h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{V}) && (3.178)\\
=&(M+1)\frac{1}{2}\log P - h(\mathbf{B}_U\mathbf{U}^T + \mathbf{N}_2) + o(\log P) && (3.179)\\
=&(M+1)\frac{1}{2}\log P - (M+1)\frac{1}{2}\log P + o(\log P) && (3.180)\\
=&o(\log P) && (3.181)
\end{aligned}
$$

where we have used the fact that both $(\mathbf{B}_V, \mathbf{B}_U)$ and $\mathbf{B}_U$ have rank $(M+1)$, almost surely, since the $\alpha_i(t)$s do not depend on the $g_i(t)$s and since both the $g_i(t)$s and $h_i(t)$s come from a continuous distribution. Note that, in both calculations above, we have implicitly used the fact that Ω is known to both the legitimate receiver and the eavesdropper, and that it appears in the conditioning of each mutual information and differential entropy term. Equation (3.181) means that the leakage to the eavesdropper does not scale with $\log P$.

Now, consider the vector wiretap channel from $\mathbf{V}$ to $\mathbf{Y}$ and $\mathbf{Z}$, by treating the $M+1$ slots in the scheme above as one channel use. Similar to (3.26), the following secrecy rate is achievable

$$
\begin{aligned}
C_s^{vec} \geq& I(\mathbf{V};\mathbf{Y}) - I(\mathbf{V};\mathbf{Z}) && (3.182)\\
=& M\left(\frac{1}{2}\log P\right) + o(\log P) && (3.183)
\end{aligned}
$$

Since each channel use of this vector channel uses $(M+1)$ actual channel uses, the achievable rate for the actual channel is,

$$C_s \geq \frac{M}{M+1}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.184}$$

Thus, the achievable s.d.o.f. of this scheme is $\frac{M}{M+1}$. The results in (3.52) and (3.184) complete the achievability of Theorem 3, for fixed and fading channel gains, respectively.

3.8.2 Proof of Lemma 4

Since $\mathbf{AX}+\mathbf{N}$ is a jointly Gaussian random vector with zero-mean and covariance $P\mathbf{AA}^T + \sigma^2\mathbf{I}$, we have [68],

$$\begin{aligned} h(\mathbf{AX}+\mathbf{N}) =& \frac{1}{2}\log(2\pi e)^M \left|P\mathbf{AA}^T + \sigma^2\mathbf{I}\right| && (3.185)\\ =& \frac{1}{2}\log(2\pi e)^M \left|P\mathbf{W\Sigma W}^T + \sigma^2\mathbf{I}\right| && (3.186)\\ =& \frac{1}{2}\sum_{i=1}^{r}\log\left(\lambda_i P + \sigma^2\right) + o(\log P) && (3.187)\\ =& r\left(\frac{1}{2}\log P\right) + o(\log P) && (3.188) \end{aligned}$$

where we note that $\mathbf{AA}^T$ is positive semi-definite, with an eigenvalue decomposition $\mathbf{W\Sigma W}^T$, where $\mathbf{\Sigma}$ is a diagonal matrix with r non-zero entries $\lambda_1, \ldots, \lambda_r$.

3.8.3 Proof of Lemma 2

First, note that

$$H(X|\left\lfloor hX \right\rfloor, h) = \mathbb{E}_h\left[H(X|\left\lfloor hX \right\rfloor, h = \tilde{h})\right] \tag{3.189}$$

Now, for a fixed h, let us define $S_h(\nu)$ as the set of all realizations of X such that $\lfloor hX \rfloor = \nu$, i.e., $S_h(\nu) \triangleq \left\{i \in \left\{1, \ldots, \lfloor\sqrt{P}\rfloor\right\} : \lfloor ih \rfloor = \nu\right\}$. Then,

$$H\left(X|\left\lfloor hX \right\rfloor, h = \tilde{h}\right) \leq \log|S_{\tilde{h}}(\lfloor \tilde{h}X \rfloor)| \tag{3.190}$$

For any ν, we can upper-bound $|S_{\tilde{h}}(\nu)|$ as follows: Let, i_1 and i_2 be the minimum and maximum elements of $S_{\tilde{h}}(\nu)$. Then, $\lfloor i_1\tilde{h} \rfloor = \lfloor i_2\tilde{h} \rfloor$ implies that $(i_2 - i_1)|\tilde{h}| < 1$, which means $(i_2 - i_1) < \frac{1}{|\tilde{h}|}$. Hence,

$$\begin{aligned} |S_{\tilde{h}}(\nu)| \leq & i_2 - i_1 + 1 & (3.191)\\ < & 1 + \frac{1}{|\tilde{h}|} & (3.192) \end{aligned}$$

Thus, using (3.189) and (3.190), we have,

$$H\left(X|\left\lfloor hX \right\rfloor, h\right) \leq \mathbb{E}_h\left[\log\left(1 + \frac{1}{|h|}\right)\right] \leq c \tag{3.193}$$

where c is a constant independent of P.

3.8.4 Proof of Lemma 3

Recall that we wish to prove that for the deterministic channel model stated in (3.53)-(3.55), with the channel gains to $\mathbf{Z}$ unknown at the transmitter, we have

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \leq no(\log P) \tag{3.194}$$

We first note that we can bound $H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega)$ as:

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \leq \sup_{\{\mathbf{X}_i\}:\mathbf{X}_i \perp\!\!\!\perp \mathbf{X}_j} H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \tag{3.195}$$

$$\leq \sup_{\{\mathbf{X}_i\}} H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \tag{3.196}$$

where $X \perp\!\!\!\perp Y$ is used to denote that X and Y are statistically independent and (3.196) follows from (3.195) by relaxing the condition of independence in (3.195). Since the $\mathbf{X}_i$s in (3.196) may be arbitrarily correlated, we can think of the K single antenna terminals as a single transmitter with K antennas. Thus, we wish to maximize $H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega)$, where $\mathbf{Y}$ and $\mathbf{Z}$ are two single antenna receiver outputs, under the constraint that the channel gains to $\mathbf{Z}$ are unknown at the transmitter. This brings us to the K-user MISO broadcast channel setting of [10]. The proof then follows by following the steps of [10, eqns. (75)-(103)]; however, we present it here for completeness. The proof has the following steps:

Functional Dependence: For a given channel realization of $\boldsymbol{H} \overset{\Delta}{=} \{h_i^n, i = 1, \ldots, K\}$, there may be multiple vectors $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K)$ that cast the same image at

$\boldsymbol{Y}$. Thus, the mapping from $\boldsymbol{Y}, \boldsymbol{H}$ to one of these vectors $(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K)$ is random. We denote this map as $\mathcal{L}$, i.e.,

$$(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K) = \mathcal{L}(\boldsymbol{Y}, \boldsymbol{H}) \tag{3.197}$$

Now, we note that

$$\begin{aligned} H(\boldsymbol{Z}|\Omega) \geq & H(\boldsymbol{Z}|\Omega, \mathcal{L}) && (3.198) \\ & \geq \min_{L \in \{\mathcal{L}\}} H(\boldsymbol{Z}|\Omega, \mathcal{L} = L) && (3.199) \end{aligned}$$

Let the minimizing mapping be L_0. We choose this to be the deterministic mapping

$$(\boldsymbol{X}_1, \ldots, \boldsymbol{X}_K) = L_0(\boldsymbol{Y}, \boldsymbol{H}) \tag{3.200}$$

Essentially, for a given $\boldsymbol{Y}$ and $\boldsymbol{H}$, we choose the mapping that minimizes the entropy at $\boldsymbol{Z}$. Note that this mapping makes $\boldsymbol{Z}$ a deterministic function of $(\boldsymbol{Y}, \Omega)$, which we denote by $\boldsymbol{Z}(\boldsymbol{Y}, \Omega)$, and that while $H(\boldsymbol{Y}|\Omega)$ is not affected, this choice of $\boldsymbol{Z}$ minimizes $H(\boldsymbol{Z}|\Omega)$, i.e.,

$$H(\boldsymbol{Y}|\Omega) - H(\boldsymbol{Z}|\Omega) \leq H(\boldsymbol{Y}|\Omega) - H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) \tag{3.201}$$

Further, note that this selection can be done irrespective of any security or decodability constraints.

Aligned Image Sets: For a given channel realization Ω, define the aligned image set $\mathcal{A}(\Omega)$ as the set of all $\boldsymbol{Y}$ that have the same image in $\boldsymbol{Z}$:

$$\mathcal{A}_{\boldsymbol{\nu}}(\Omega) = \{\boldsymbol{y} : \boldsymbol{Z}(\boldsymbol{y}, \Omega) = \boldsymbol{Z}(\boldsymbol{\nu}, \Omega)\} \tag{3.202}$$

Bounding Difference of Entropies via Size of Aligned Sets: We have

$$\begin{aligned} H(\boldsymbol{Y}|\Omega) =& H(\boldsymbol{Y}, \boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) && (3.203)\\ =& H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + H(\boldsymbol{Y}|\boldsymbol{Z}(\boldsymbol{Y}, \Omega), \Omega) && (3.204)\\ =& H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + H(\mathcal{A}_{\boldsymbol{Y}}(\Omega)|\Omega) && (3.205)\\ \leq& H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + \mathbb{E}[\log|\mathcal{A}_{\boldsymbol{Y}}(\Omega)|] && (3.206)\\ \leq& H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) + \log\mathbb{E}[|\mathcal{A}_{\boldsymbol{Y}}(\Omega)|] && (3.207) \end{aligned}$$

Therefore, we have,

$$H(\boldsymbol{Y}|\Omega) - H(\boldsymbol{Z}(\boldsymbol{Y}, \Omega)|\Omega) \leq \mathbb{E}[|\mathcal{A}_{\boldsymbol{Y}}(\Omega)|] \tag{3.208}$$

Bounding the Probability of Alignment: Given the channel $\boldsymbol{H}$ and two realizations $\boldsymbol{y}$ and $\boldsymbol{y}'$ of $\boldsymbol{Y}$, such that $\boldsymbol{X}_j(\boldsymbol{y}, \boldsymbol{H}) = \boldsymbol{x}_j$, and $\boldsymbol{X}_j'(\boldsymbol{y}', \boldsymbol{H}) = \boldsymbol{x}_j'$, we bound the probability of image alignment at $\boldsymbol{Z}$. Note that for alignment, we must have for all $t = 1, \ldots, n$,

$$\sum_{i=1}^{K} \lfloor g_i(t) x_i(t) \rfloor = \sum_{i=1}^{K} \lfloor g_i(t) x_i'(t) \rfloor \tag{3.209}$$

$$\Rightarrow g_{i^*(t)}(t)(x'_{i^*}(t) - x_{i^*}(t)) \in \sum_{i=1, i\neq i^*(t)}^{K} \lfloor g_i(t)x_i(t)\rfloor - \lfloor g_i(t)x'_i(t)\rfloor + \Delta \tag{3.210}$$

where $\Delta \in (-1, 1)$, and

$$i^*(t) = \arg\max_i |(x'_i(t) - x_i(t)| \tag{3.211}$$

Therefore, for any t such that $x'_{i^*}(t) \neq x_{i^*}(t)$, $g_{i^*}(t)(t)$ must lie within an interval of length $\frac{2}{|x'_{i^*}(t) - x_{i^*}(t)|}$. If $f_{\max}$ is the maximum of 1 and an upper bound on the probability density function of $g_i(t)$ (note that the probability density is assumed to be bounded), we have,

$$\mathbb{P}\left(\boldsymbol{y}' \in \mathcal{A}_{\boldsymbol{y}}(\Omega)\right) \leq f_{\max}^n \prod_{t: x'_{i^*(t)}(t)\neq x_{i^*(t)}(t)} \frac{2}{|x'_{i^*(t)}(t) - x_{i^*(t)}(t)|} \tag{3.212}$$

We now express this probability in terms of $y(t)$ and $y'(t)$ as follows: We note

$$\begin{aligned} y'(t) - y(t) =& \sum_{i=1}^{K} \left(\lfloor h_i(t)x_i(t)\rfloor - \lfloor h_i(t)x'_i(t)\rfloor\right) && (3.213)\\ \leq& \sum_{i=1}^{K} \lfloor h_i(t)(x_i(t) - x'(t))\rfloor + (-K, K) && (3.214) \end{aligned}$$

Therefore, we have

$$\begin{aligned} |y'(t) - y(t)| \leq& |x'_{i^*(t)}(t) - x_{i^*(t)}(t)| \sum_{i=1}^{K} |h_i(t)| + K && (3.215)\\ \Rightarrow \frac{1}{|x'_{i^*(t)}(t) - x_{i^*(t)}(t)|} \leq& \frac{\sum_{i=1}^{K} |h_i(t)|}{|y'(t) - y(t)| - K} && (3.216) \end{aligned}$$

whenever $|y'(t) - y(t)| > K$. Thus, we have

$$\mathbb{P}\left(\boldsymbol{y}' \in \mathcal{A}_{\boldsymbol{y}}(\Omega)\right) \leq \bar{h}^n f_{\max}^n \prod_{t:|y'(t)-y(t)|>K} \frac{1}{|y'(t) - y(t)| - K} \tag{3.217}$$

where

$$\bar{h}^n = \max\left(1, \prod_{t:x'_{i^*(t)}(t)\neq x_{i^*(t)}(t)} 2\sum_{i=1}^{K} |h_i(t)|\right) \tag{3.218}$$

Bounding the Size of the Aligned Image Set:

$$\begin{align}
\mathbb{E}[|\mathcal{A}_{\boldsymbol{y}}(\Omega)|] =& \sum_{\boldsymbol{y}'} \mathbb{P}\left(\boldsymbol{y}' \in \mathcal{A}_{\boldsymbol{y}}(\Omega)\right) \tag{3.219}\\
\leq& \bar{h}^n f_{\max}^n \prod_{t=1}^{n} \left(\sum_{y'(t):|y'(t)-y(t)|\leq K} 1 + \sum_{y'(t):K<|y'(t)-y(t)|\leq Q_y(t)} \frac{1}{|y'(t) - y(t)| - K} \right) \tag{3.220}\\
\leq& \bar{h}^n f_{\max}^n \left(\log\sqrt{P} + o(\log P)\right)^n \tag{3.221}
\end{align}$$

where $Q_y(t) \leq \sqrt{P}\sum_{i=1}^{K} |h_i(t)| + K$. Therefore, taking logarithms, we have

$$\log \mathbb{E}[|\mathcal{A}_{\boldsymbol{y}}(\Omega)|] \leq n o(\log P) \tag{3.222}$$

Now, combining (3.201), (3.208) and (3.222), we have the desired result, i.e.,

$$H(\mathbf{Y}|\Omega) - H(\mathbf{Z}|\Omega) \leq n o(\log P) \tag{3.223}$$

which completes the proof of Lemma 3.

3.8.5 Achievability for $K = 3$ with Fading Channel Gains

Our scheme uses asymptotic vector space alignment introduced in [8]. Let $\Gamma = (K-1)^2 = (3-1)^2 = 4$. We use $M_n = 2n^\Gamma + 4(n+1)^\Gamma$ channel uses to transmit $6n^\Gamma$ message symbols securely to the legitimate receivers in the presence of the eavesdropper. Thus, we achieve a sum s.d.o.f. of $\frac{6n^\Gamma}{2n^\Gamma+4(n+1)^\Gamma}$, which approaches 1 as $n \rightarrow \infty$.

First, at transmitter i, we divide its message W_i into 2 sub-messages $V_{ij}, j = 1, \ldots, 4, j \neq i, i+1$. Each V_{ij} is encoded into n^Γ independent streams $v_{ij}(1), \ldots, v_{ij}(n^\Gamma)$, which we denote as $\mathbf{v}_{ij} \triangleq \left(v_{ij}(1), \ldots, v_{ij}(n^\Gamma)\right)^T$. We also require artificial noise symbols U_i and $\tilde{U}_i$ at each transmitter i. We encode the artificial noise symbols U_i and $\tilde{U}_i$ as

$$\mathbf{u}_i \triangleq \left(u_i(1), \ldots, u_i((n+1)^\Gamma)\right)^T, i = 1, 2, 3 \tag{3.224}$$

$$\tilde{\mathbf{u}}_i \triangleq \left(\tilde{u}_i(1), \ldots, \tilde{u}_i(n^\Gamma)\right)^T, i = 1, 2 \tag{3.225}$$

$$\tilde{\mathbf{u}}_3 \triangleq \left(\tilde{u}_i(1), \ldots, \tilde{u}_i((n+1)^\Gamma)\right)^T \tag{3.226}$$

In each channel use $t \leq M_n$, we choose precoding column vectors $\mathbf{p}_{ij}(t)$, $\mathbf{q}_i(t)$ and $\tilde{\mathbf{q}}_i(t)$ with the same number of elements as $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. In channel use t, transmitter i sends

$$X_i(t) = \sum_{j \neq i, i+1} \mathbf{p}_{ij}(t)^T \mathbf{v}_{ij} + \mathbf{q}_i(t)^T \mathbf{u}_i + \tilde{\mathbf{q}}_i(t)^T \tilde{\mathbf{u}}_i \tag{3.227}$$

where we have dropped the limits on j in the summation for notational simplicity. By stacking the precoding vectors for all M_n channel uses, we let,

$$\mathbf{P}_{ij} = \begin{pmatrix} \mathbf{p}_{ij}(1)^T \\ \vdots \\ \mathbf{p}_{ij}^T(M_n) \end{pmatrix}, \qquad \mathbf{Q}_i = \begin{pmatrix} \mathbf{q}_i(1)^T \\ \vdots \\ \mathbf{q}_i(M_n)^T \end{pmatrix}, \qquad \tilde{\mathbf{Q}}_i = \begin{pmatrix} \tilde{\mathbf{q}}_i(1)^T \\ \vdots \\ \tilde{\mathbf{q}}_i(M_n)^T \end{pmatrix} \tag{3.228}$$

Now, letting $\mathbf{X}_i = (X_i(1), \dots, X_i(M_n))^T$, the channel input for transmitter i over M_n channel uses can be compactly represented as

$$\mathbf{X}_i = \sum_j \mathbf{P}_{ij} \mathbf{v}_{ij} + \mathbf{Q}_i \mathbf{u}_i + \tilde{\mathbf{Q}}_i \tilde{\mathbf{u}}_i \tag{3.229}$$

Recall that, channel use t, the channel output at receiver l and the eavesdropper are, respectively, given by

$$Y_l(t) = \sum_{k=1}^{3} h_{kl}(t) X_k(t) + N_l(t) \tag{3.230}$$

$$Z(t) = \sum_{k=1}^{3} g_k(t) X_k(t) + N_Z(t) \tag{3.231}$$

where we have dropped the Gaussian noise at high SNR.

Let $\mathbf{H}_{kl} \overset{\Delta}{=} \operatorname{diag}(h_{kl}(1), \dots, h_{kl}(M_n))$. Similarly, define $\mathbf{G}_k = \operatorname{diag}(g_k(1), \dots,$

$g_k(M_n))$. The channel outputs at receiver l and the eavesdropper over all M_n channel uses, $\mathbf{Y}_l = (Y_l(1), \ldots, Y_l(M_n))^T$ and $\mathbf{Z} = (Z(1), \ldots, Z(M_n))^T$, respectively, can be represented by

$$\begin{aligned}
\mathbf{Y}_l &= \sum_{k=1}^{3} \mathbf{H}_{kl} \mathbf{X}_k + \mathbf{N}_l && (3.232)\\
&= \sum_{k=1}^{3} \mathbf{H}_{kl} \left(\sum_{\substack{j=1\\ j\neq k,k+1}}^{4} \mathbf{P}_{kj} \mathbf{v}_{kj} + \mathbf{Q}_k \mathbf{u}_k + \tilde{\mathbf{Q}}_k \tilde{\mathbf{u}}_k \right) + \mathbf{N}_l && (3.233)\\
&= \sum_{\substack{j=1\\ j\neq l,l+1}}^{4} \mathbf{H}_{ll} \mathbf{P}_{lj} \mathbf{v}_{lj} + \sum_{\substack{k=1\\ k\neq l}}^{3} \sum_{\substack{j=1\\ j\neq k,k+1}}^{4} \mathbf{H}_{kl} \mathbf{P}_{kj} \mathbf{v}_{kj} + \sum_{k=1}^{3} \mathbf{H}_{kl} \left(\mathbf{Q}_k \mathbf{u}_k + \tilde{\mathbf{Q}}_k \tilde{\mathbf{u}}_k \right) + \mathbf{N}_l \\
& && (3.234)
\end{aligned}$$

and,

$$\begin{aligned}
\mathbf{Z} &= \sum_{k=1}^{3} \mathbf{G}_k \mathbf{X}_k + \mathbf{N}_Z && (3.235)\\
&= \sum_{k=1}^{3} \sum_{\substack{j=1\\ j\neq k,k+1}}^{4} \mathbf{G}_k \mathbf{P}_{kj} \mathbf{v}_{kj} + \sum_{k=1}^{3} \mathbf{G}_k \left(\mathbf{Q}_k \mathbf{u}_k + \tilde{\mathbf{Q}}_k \tilde{\mathbf{u}}_k \right) + \mathbf{N}_Z && (3.236)
\end{aligned}$$

Now, receiver l wants to decode $\mathbf{v}_{lj}, j = 1, \ldots, 4, j \neq l, l+1$. Thus, the remaining terms in (3.234) constitute interference at the lth receiver. Let $CS(\mathbf{X})$ denote the column space of matrix $\mathbf{X}$. Then, I_l denoting the space spanned by this interference is given by

$$I_l = \left(\bigcup_{k \neq l, j \neq k, k+1} CS\left(\mathbf{H}_{kl}\mathbf{P}_{kj}\right) \right) \bigcup \left(\bigcup_{k=1}^{3} CS\left(\mathbf{H}_{kl}\mathbf{Q}_k\right) \right) \bigcup \left(\bigcup_{k=1}^{3} CS\left(\mathbf{H}_{kl}\tilde{\mathbf{Q}}_k\right) \right) \tag{3.237}$$

Note that there are $2n^\Gamma$ symbols to be decoded by each legitimate receiver in $2n^\Gamma + 4(n+1)^\Gamma$ channel uses. Thus, for decodability, the interference can occupy a subspace of rank at most $4(n+1)^\Gamma$, that is,

$$\text{rank}(I_l) \leq 4(n+1)^\Gamma \tag{3.238}$$

To that end, we align the noise and message subspaces at each legitimate receiver appropriately. Note that no such alignment is possible at the external eavesdropper since the transmitters do not have its CSI. In addition, note that we have a total of $2n^\Gamma + 4(n+1)^\Gamma$ artificial noise symbols which will span the full received signal space at the eavesdropper and secure all the messages.

Fig. 3.5 shows the alignment we desire. We remark that the same figure represents the alignment of signals both for real interference alignment and the vector space alignment schemes. Now, let us enumerate the conditions for the desired signal alignment at each receiver. From Fig. 3.5, it is clear that there are 6 alignment equations at each legitimate receiver, corresponding to four unintended messages and two artificial noise symbols $\tilde{U}_1$ and $\tilde{U}_2$. Table 3.2 shows the alignment equations for each legitimate receiver.

	$\mathbf{Q}_1$	$\mathbf{Q}_2$	$\mathbf{Q}_3$	$\tilde{\mathbf{Q}}_3$
Receiver 1	$\mathbf{H}_{21}\mathbf{P}_{21} \preceq \mathbf{H}_{11}\mathbf{Q}_1$ $\mathbf{H}_{31}\mathbf{P}_{31} \preceq \mathbf{H}_{11}\mathbf{Q}_1$	$\mathbf{H}_{11}\tilde{\mathbf{Q}}_1 \preceq \mathbf{H}_{21}\mathbf{Q}_2$ $\mathbf{H}_{31}\mathbf{P}_{32} \preceq \mathbf{H}_{21}\mathbf{Q}_2$	$\mathbf{H}_{21}\tilde{\mathbf{Q}}_2 \preceq \mathbf{H}_{31}\mathbf{Q}_3$	$\mathbf{H}_{21}\mathbf{P}_{24} \preceq \mathbf{H}_{31}\tilde{\mathbf{Q}}_3$
Receiver 2	$\mathbf{H}_{32}\mathbf{P}_{31} \preceq \mathbf{H}_{12}\mathbf{Q}_1$	$\mathbf{H}_{12}\tilde{\mathbf{Q}}_1 \preceq \mathbf{H}_{22}\mathbf{Q}_2$ $\mathbf{H}_{32}\mathbf{P}_{32} \preceq \mathbf{H}_{22}\mathbf{Q}_2$	$\mathbf{H}_{22}\tilde{\mathbf{Q}}_2 \preceq \mathbf{H}_{32}\mathbf{Q}_3$ $\mathbf{H}_{12}\mathbf{P}_{13} \preceq \mathbf{H}_{32}\mathbf{Q}_3$	$\mathbf{H}_{12}\mathbf{P}_{14} \preceq \mathbf{H}_{32}\tilde{\mathbf{Q}}_3$
Receiver 3	$\mathbf{H}_{23}\mathbf{P}_{21} \preceq \mathbf{H}_{13}\mathbf{Q}_1$	$\mathbf{H}_{13}\tilde{\mathbf{Q}}_1 \preceq \mathbf{H}_{23}\mathbf{Q}_2$	$\mathbf{H}_{23}\tilde{\mathbf{Q}}_2 \preceq \mathbf{H}_{33}\mathbf{Q}_3$ $\mathbf{H}_{13}\mathbf{P}_{13} \preceq \mathbf{H}_{33}\mathbf{Q}_3$	$\mathbf{H}_{23}\mathbf{P}_{24} \preceq \mathbf{H}_{33}\tilde{\mathbf{Q}}_3$ $\mathbf{H}_{13}\mathbf{P}_{14} \preceq \mathbf{H}_{33}\tilde{\mathbf{Q}}_3$

Table 3.2: Summary of alignment equations.

Now, me make the following selections:

$$\mathbf{P}_{21} = \mathbf{P}_{31} \overset{\Delta}{=} \tilde{\mathbf{P}}_1 \tag{3.239}$$

$$\mathbf{P}_{32} \overset{\Delta}{=} \tilde{\mathbf{P}}_2 \tag{3.240}$$

$$\mathbf{P}_{13} \overset{\Delta}{=} \tilde{\mathbf{P}}_3 \tag{3.241}$$

$$\mathbf{P}_{14} = \mathbf{P}_{24} \overset{\Delta}{=} \tilde{\mathbf{P}}_4 \tag{3.242}$$

$$\tilde{\mathbf{Q}}_1 = \mathbf{H}_{11}^{-1}\mathbf{H}_{31}\tilde{\mathbf{P}}_2 \tag{3.243}$$

$$\tilde{\mathbf{Q}}_2 = \mathbf{H}_{22}^{-1}\mathbf{H}_{12}\tilde{\mathbf{P}}_3 \tag{3.244}$$

Note that (3.243) and (3.244) imply that the artificial noises $\tilde{\mathbf{u}}_1$ and $\tilde{\mathbf{u}}_2$ align exactly with unintended message symbols $\mathbf{v}_{32}$ and $\mathbf{v}_{13}$ at receivers 1 and 2, respectively. With these selections, it suffices to find matrices $\tilde{\mathbf{P}}_i, i = 1, \ldots, 4$, $\mathbf{Q}_i, i = 1, 2, 3$, and $\tilde{\mathbf{Q}}_3$. The alignment equations may now be written as

$$\mathbf{T}_{ij}\tilde{\mathbf{P}}_i \preceq \mathbf{Q}_i, \quad i = 1, 2, 3, \quad j = 1, \ldots, 4 \tag{3.245}$$

	T_{1j}	T_{2j}	T_{3j}	T_{4j}
$j=1$	$\mathbf{H}_{11}^{-1}\mathbf{H}_{21}$	$\mathbf{H}_{21}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{31}^{-1}\mathbf{H}_{21}\mathbf{H}_{22}^{-1}\mathbf{H}_{12}$	$\mathbf{H}_{31}^{-1}\mathbf{H}_{21}$
$j=2$	$\mathbf{H}_{11}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{22}^{-1}\mathbf{H}_{12}\mathbf{H}_{11}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{32}^{-1}\mathbf{H}_{12}$	$\mathbf{H}_{32}^{-1}\mathbf{H}_{12}$
$j=3$	$\mathbf{H}_{12}^{-1}\mathbf{H}_{32}$	$\mathbf{H}_{22}^{-1}\mathbf{H}_{32}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{23}\mathbf{H}_{22}^{-1}\mathbf{H}_{12}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{23}$
$j=4$	$\mathbf{H}_{13}^{-1}\mathbf{H}_{23}$	$\mathbf{H}_{23}^{-1}\mathbf{H}_{13}\mathbf{H}_{11}^{-1}\mathbf{H}_{31}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{13}$	$\mathbf{H}_{33}^{-1}\mathbf{H}_{13}$

Table 3.3: Values of T_{ij}.

$$\mathbf{T}_{4j}\tilde{\mathbf{P}}_4 \preceq \tilde{\mathbf{Q}}_3, \quad j = 1, \ldots, 4 \tag{3.246}$$

where the T_{ij}s are tabulated in Table 3.3, and the notation $\mathbf{A} \preceq \mathbf{B}$ is used to denote that $CS(\mathbf{A}) \subseteq CS(\mathbf{B})$ for matrices $\mathbf{A}$ and $\mathbf{B}$ where $CS(\mathbf{X})$ refers to the column space of the matrix $\mathbf{X}$.

We can now construct the matrices $\tilde{\mathbf{P}}_i, i = 1, \ldots, 4$, $\mathbf{Q}_i, i = 1, \ldots, 3$ and $\tilde{\mathbf{Q}}_3$ as in [8]

$$\tilde{\mathbf{P}}_i = \left\{ \left(\prod_{j=1}^{4} \mathbf{T}_{ij}^{\alpha_j} \right) \mathbf{w}_i : \alpha_j \in \{1, \ldots, n\} \right\} \tag{3.247}$$

$$\mathbf{Q}_i = \left\{ \left(\prod_{j=1}^{4} \mathbf{T}_{ij}^{\alpha_j} \right) \mathbf{w}_i : \alpha_j \in \{1, \ldots, n+1\} \right\} \tag{3.248}$$

$$\tilde{\mathbf{Q}}_3 = \left\{ \left(\prod_{j=1}^{4} \mathbf{T}_{ij}^{\alpha_j} \right) \mathbf{w}_4 : \alpha_j \in \{1, \ldots, n+1\} \right\} \tag{3.249}$$

where each $\mathbf{w}_i$ is the $M_n \times 1$ column vector containing elements drawn independently from a continuous distribution with bounded support. Note that an element in $\mathbf{P}_i$ is the product of powers of some channel coefficients and an extra random variable, just like an element in the sets T_i defined for the real interference scheme. Further, the set of channel coefficients appearing in $\mathbf{P}_i$ is the same as those contained in set T_i. Thus, there is a loose correspondence between the real and vector space alignment techniques.

Now, consider the decodability of the desired signals at the receivers. For example, consider receiver 1. Due to the alignment conditions in Table 3.2, the interference subspace at receiver 1 is given by

$$\mathbf{I}_1 = \begin{bmatrix}\mathbf{H}_{11}\mathbf{Q}_1 & \mathbf{H}_{21}\mathbf{Q}_2 & \mathbf{H}_{31}\mathbf{Q}_3 & \mathbf{H}_{\mathbf{31}}\tilde{\mathbf{Q}}_3\end{bmatrix} \tag{3.250}$$

The desired signal subspace, on the other hand, is

$$\mathbf{D}_1 = \begin{bmatrix}\mathbf{H}_{11}\tilde{\mathbf{P}}_3 & \mathbf{H}_{11}\tilde{\mathbf{P}}_4\end{bmatrix} \tag{3.251}$$

For decodability, it suffices to show that

$$\mathbf{\Lambda}_1 = [\mathbf{D}_1 \quad \mathbf{I}_1] \tag{3.252}$$

is full rank. To do so, we use [69, Lemmas 1, 2]. Consider any row m of the matrix $\mathbf{\Lambda}_1$. Note that the mth row of $\mathbf{H}_{i1}\mathbf{Q}_i$ contains the term w_{mi} with exponent 1, but no w_{mj} for $i \neq j$, where w_{mi} denotes the element in the mth row of $\mathbf{w}_i$. In fact, for $i = 1, \dots, 4$, the term w_{mi} occurs nowhere else in the matrix $\mathbf{\Lambda}_l$ except in $\mathbf{H}_{i1}\mathbf{Q}_i$ ($\mathbf{H}_{31}\tilde{\mathbf{Q}}_3$, when $i = 4$) and $\mathbf{H}_{11}\tilde{\mathbf{P}}_i$. This shows that $\mathbf{D}_1$ and $\mathbf{I}_1$ have full column ranks individually. Further, the matrix $\begin{bmatrix}\mathbf{H}_{11}\tilde{\mathbf{P}}_3 & \mathbf{H}_{31}\mathbf{Q}_3\end{bmatrix}$ has full column rank because

$\mathbf{Q}_3$ does not contain any elements of $\mathbf{H}_{11}$. Similarly, $\left[\mathbf{H}_{11}\tilde{\mathbf{P}}_4 \quad \mathbf{H}_{31}\tilde{\mathbf{Q}}_3\right]$ is full column rank for the same reason. Thus, $\mathbf{\Lambda}_1$, which is a $M_n \times M_n$ matrix, is full column rank, and hence full rank. This ensures decodability of the desired signals at receiver 1. a similar analysis holds for the other receivers as well.

The security of the message signals at the eavesdropper is ensured by the fact that the artificial noises $\mathbf{Q}_i$ and $\tilde{\mathbf{Q}}_i$, $i = 1, 2, 3$, do not align at the eavesdropper, and instead span the full received signal space at the eavesdropper. Indeed, the $M_n \times M_n$ matrix

$$\mathbf{I}_E = \left[\mathbf{G}_1\mathbf{Q}_1 \quad \mathbf{G}_2\mathbf{Q}_2 \quad \mathbf{G}_3\mathbf{Q}_3 \quad \mathbf{G}_1\tilde{\mathbf{Q}}_1 \quad \mathbf{G}_2\tilde{\mathbf{Q}}_2 \quad \mathbf{G}_3\tilde{\mathbf{Q}}_3\right] \tag{3.253}$$

is full rank. Thus, if $\mathbf{V}_i = \{\mathbf{v}_{ij}, j \neq i, i+1\}$ denotes the collection of all messages of transmitter i, and $\mathbf{u}^T = \left[\mathbf{u}_1^T, \mathbf{u}_2^T, \mathbf{u}_2^T, \tilde{\mathbf{u}}_1^T, \tilde{\mathbf{u}}_2^T, \tilde{\mathbf{u}}_3^T\right]$,

$$I(\mathbf{V}_1^3; \mathbf{Z}) = h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{V}_1^3) \tag{3.254}$$

$$= h(\mathbf{Z}) - h(\mathbf{I}_E\mathbf{u}) \tag{3.255}$$

$$\leq \frac{M_n}{2}\log P - \frac{M_n}{2}\log P + o(\log P) \tag{3.256}$$

$$= o(\log P) \tag{3.257}$$

In the above calculation, we have dropped the conditioning on Ω for notational simplicity. Now, by treating all M_n channel uses as 1 vector channel use, and using [43, Theorem 2], an achievable rate for the vector channel is

$$R_i^{M_n} = I(\mathbf{V}_i; \mathbf{Y}_i) - I(\mathbf{V}_i; \mathbf{Z}|\mathbf{V}_{-i}) \tag{3.258}$$

$$= 2n^\Gamma \log P - o(\log P) \tag{3.259}$$

where (3.259) follows since the $2n^\Gamma$ symbols are decodable within noise variance, and since $I(\mathbf{V}_i; \mathbf{Z}|\mathbf{V}_{-i}) \leq I(\mathbf{V}_1^3; \mathbf{Z}) \leq o(\log P)$. Thus, the rate $\frac{2n^\Gamma}{M_n}$ is achievable per user pair per channel use, which gives a sum s.d.o.f. of $\frac{6n^\Gamma}{2n^\Gamma + 4(n+1)^\Gamma}$, which approaches 1, as $n \to \infty$.

3.8.6 Achievability for the K-user Interference Channel with an External Eavesdropper

Here, we present the general achievable schemes for the K-user interference channel with an external eavesdropper.

3.8.7 Fixed Channel Gains

Let m be a large constant. We pick $(K+1)$ points $c_1, \ldots, c_{K+1}$ in an i.i.d. fashion from a continuous distribution with bounded support. Then, $c_1, \ldots, c_{K+1}$ are rationally independent almost surely. Let us define sets T_i, for $i = 1, \ldots, K+1$, which will represent *dimensions* as follows:

$$T_1 \triangleq \left\{ \left(\prod_{k=1}^{K} h_{1k}^{r_{1k}} \right) \left(\prod_{j,k=1, j\neq 1,k}^{K} h_{jk}^{r_{jk}} \right) c_1^s : \ r_{jk}, s \in \{1, \ldots, m\} \right\} \tag{3.260}$$

$$T_i \triangleq \left\{ \left(\prod_{k=1}^{K} h_{ik}^{r_{ik}} \right) \left(\prod_{k=2}^{K} \left(\frac{h_{(i-1)k}}{h_{(i-1)1}} \right)^{r_{(i-1)k}} \right) \left(\prod_{\substack{j,k=1 \\ j \neq i, i-1, k}}^{K} h_{jk}^{r_{jk}} \right) c_i^s : \; r_{jk}, s \in \{1, \ldots, m\} \right\},$$

$$i = 2, \ldots, K-1 \tag{3.261}$$

$$T_K \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{k=1, k \neq 2}^{K} \left(\frac{h_{(K-1)k}}{h_{(K-1)2}} \right)^{r_{(K-1)k}} \right) \left(\prod_{\substack{j,k=1 \\ j \neq K, K-1, k}}^{K} h_{jk}^{r_{jk}} \right) c_K^s : \right.$$

$$\left. r_{jk}, s \in \{1, \ldots, m\} \right\} \tag{3.262}$$

$$T_{K+1} \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{j,k=1, j \neq K, k}^{K} h_{jk}^{r_{jk}} \right) c_{K+1}^s : \; r_{jk}, s \in \{1, \ldots, m\} \right\} \tag{3.263}$$

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

$$M \triangleq m^{2+K(K-1)} \tag{3.264}$$

First, we divide each message into many sub-messages; specifically, the message of the ith transmitter, W_i, is divided into $(K-1)$ sub-messages V_{ij}, $j = 1, \ldots, K+1, j \neq i, i+1$. For each transmitter i, let $\mathbf{p}_{ij}$ be the vector containing all the elements of T_j, for $j \neq i, i+1$. For any given (i, j) with $j \neq i, i+1$, $\mathbf{p}_{ij}$ represents the dimension along which message V_{ij} is sent. Further, at each transmitter i, let $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ be vectors containing all the elements in sets T_i and $\beta_i T_{i+1}$, respectively, where

$$\beta_i = \begin{cases} \frac{h_{(i+2)1}}{h_{i1}}, & \text{if } 1 \leq i \leq K-2 \\ \frac{h_{12}}{h_{i2}}, & \text{if } i = K-1 \\ 1, & \text{if } i = K \end{cases} \tag{3.265}$$

The vectors $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ represent dimensions along which artificial noise symbols U_i and $\tilde{U}_i$, respectively, are sent. We define a $(K+1)M$ dimensional vector $\mathbf{b}_i$ by stacking the $\mathbf{p}_{ij}$s, $\mathbf{q}_i$ and $\tilde{\mathbf{q}}_i$ as

$$\mathbf{b}_i^T = \begin{bmatrix}\mathbf{p}_{i1}^T \dots \mathbf{p}_{i(i-1)}^T & \mathbf{p}_{i(i+2)}^T \dots \mathbf{p}_{i(K+1)} & \mathbf{q}_i & \tilde{\mathbf{q}}_i\end{bmatrix} \tag{3.266}$$

The transmitter encodes V_{ij} using an M dimensional vector $\mathbf{v}_{ij}$, and the cooperative jamming signals U_i and $\tilde{U}_i$ using M dimensional vectors $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. Each element of $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$ are drawn in an i.i.d. fashion from $C(a, Q)$ in (3.21). Let

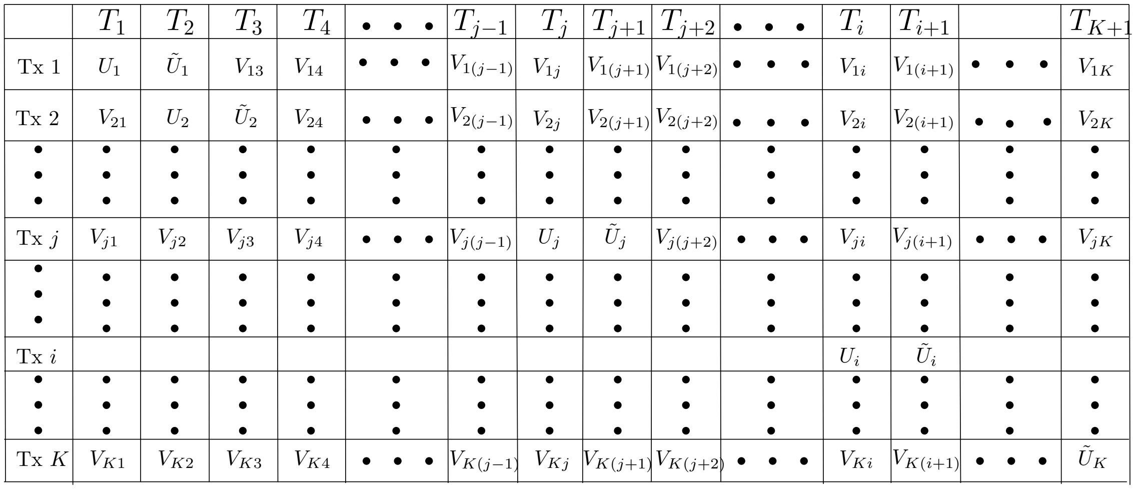
$$\mathbf{a}_i^T = \begin{bmatrix}\mathbf{v}_{i1}^T \dots \mathbf{v}_{i(i-1)}^T & \mathbf{v}_{i(i+2)}^T \dots \mathbf{v}_{i(K+1)} & \mathbf{u}_i & \tilde{\mathbf{u}}_i\end{bmatrix} \tag{3.267}$$

The channel input of transmitter i is then given by

$$x_i = \mathbf{a}_i^T \mathbf{b} \tag{3.268}$$

Let us now analyze the structure of the received signals at the legitimate receivers. The alignment of the interfering signal spaces at receiver i is shown in Fig. 3.7. The ith row depicts the signals originating from transmitter i. The signals in the same column align together at the receiver. For simplicity of exposition, let us consider receiver 1.

At the first receiver, the desired signals $\mathbf{v}_{13}, \dots, \mathbf{v}_{1(K+1)}$ come along dimensions $h_{11}T_3, \dots, h_{11}T_{K+1}$, respectively. These dimensions are *separate* almost surely, since T_i contains powers of c_i while $T_j, j \neq i$ does not. Thus, they correspond to



	T_1	T_2	T_3	T_4	• • •	T_{j-1}	T_j	T_{j+1}	T_{j+2}	• • •	T_i	T_{i+1}		T_{K+1}
Tx 1	U_1	$\tilde{U}_1$	V_{13}	V_{14}	• • •	$V_{1(j-1)}$	V_{1j}	$V_{1(j+1)}$	$V_{1(j+2)}$	• • •	V_{1i}	$V_{1(i+1)}$	• • •	V_{1K}
Tx 2	V_{21}	U_2	$\tilde{U}_2$	V_{24}	• • •	$V_{2(j-1)}$	V_{2j}	$V_{2(j+1)}$	$V_{2(j+2)}$	• • •	V_{2i}	$V_{2(i+1)}$	• • •	V_{2K}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Tx j	V_{j1}	V_{j2}	V_{j3}	V_{j4}	• • •	$V_{j(j-1)}$	U_j	$\tilde{U}_j$	$V_{j(j+2)}$	• • •	V_{ji}	$V_{j(i+1)}$	• • •	V_{jK}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Tx i											U_i	$\tilde{U}_i$		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Tx K	V_{K1}	V_{K2}	V_{K3}	V_{K4}	• • •	$V_{K(j-1)}$	V_{Kj}	$V_{K(j+1)}$	$V_{K(j+2)}$	• • •	V_{Ki}	$V_{K(i+1)}$	• • •	$\tilde{U}_K$

Figure 3.7: Alignment of interference signals at receiver i.

separate boxes in the Fig. 3.5 for $K = 3$. For the same reason, cooperative jamming signals $\mathbf{u}_1, \ldots, \mathbf{u}_K$, $\tilde{\mathbf{u}}_K$, which arrive along the dimensions $h_{11}T_1, \ldots, h_{K1}T_K$, $h_{K1}T_{K+1}$ occupy different dimensions almost surely. Further, the message signals $\mathbf{v}_{13}, \ldots, \mathbf{v}_{1(K+1)}$, and the cooperative jamming signals $\mathbf{u}_1, \ldots, \mathbf{u}_K, \tilde{\mathbf{u}}_K$ do not overlap, since none of $T_3 \ldots, T_{K+1}$ contain h_{11}. Thus, they appear as separate boxes in Fig. 3.5.

Now, let us consider the signals that are not desired at receiver 1. A signal $\mathbf{v}_{kl}, k \neq 1, K+1$ arrives at receiver 1 along $h_{k1}T_l$. If we define

$$\tilde{T}_1 \triangleq \left\{ \left(\prod_{k=1}^{K} h_{1k}^{r_{1k}} \right) \left(\prod_{j,k=1, j\neq 1,k}^{K} h_{jk}^{r_{jk}} \right) c_1^s : \ r_{jk}, s \in \{1, \ldots, m+1\} \right\} \tag{3.269}$$

$$\tilde{T}_i \triangleq \left\{ \left(\prod_{k=1}^{K} h_{ik}^{r_{ik}} \right) \left(\prod_{k=2}^{K} \left(\frac{h_{(i-1)k}}{h_{(i-1)1}} \right)^{r_{(i-1)k}} \right) \left(\prod_{\substack{j,k=1 \\ j \neq i, i-1, k}}^{K} h_{jk}^{r_{jk}} \right) c_i^s : \right.$$

$$\left. r_{jk}, s \in \{1, \ldots, m+1\} \right\}, \quad i = 2, \ldots, K-1 \tag{3.270}$$

$$\tilde{T}_K \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{\substack{k=1,k\neq 2\\ m=K-1}}^{K} \left(\frac{h_{mk}}{h_{m2}} \right)^{r_{mk}} \right) \left(\prod_{\substack{j,k=1\\ j\neq K,K-1,k}}^{K} h_{jk}^{r_{jk}} \right) c_K^s : \right.$$

$$\left. r_{jk}, s \in \{1, \ldots, m+1\} \right\} \tag{3.271}$$

$$\tilde{T}_{K+1} \triangleq \left\{ \left(\prod_{k=1}^{K} h_{Kk}^{r_{Kk}} \right) \left(\prod_{j,k=1,j\neq K,k}^{K} h_{jk}^{r_{jk}} \right) c_{K+1}^s : \; r_{jk}, s \in \{1, \ldots, m+1\} \right\} \tag{3.272}$$

we notice that the dimensions in $h_{k1}T_l$, $k \neq 1$ are subsets of $\tilde{T}_l$, as is $h_{l1}T_l$ for every $l = 1, \ldots, K$. Thus, each $\mathbf{v}_{kl}$ aligns with $\mathbf{u}_l$ in $\tilde{T}_l$, for $l = 1, \ldots, K$, as is shown in Fig. 3.7. Further, a signal $\mathbf{v}_{k(K+1)}$, $k \neq 1, K$, arrives along the dimensions $h_{k1}T_{K+1}$, $k \neq 1$ which is a subset of $\tilde{T}_{K+1}$, as is $h_{K1}T_{K+1}$, along which $\tilde{\mathbf{u}}_K$ arrives. Thus, each $\mathbf{v}_{k(K+1)}$, $k \neq 1, K$ aligns with $\tilde{\mathbf{u}}_K$, see Fig. 3.7. Finally, the cooperative jamming signals $\tilde{\mathbf{u}}_1, \ldots,$ $\tilde{\mathbf{u}}_{K-2}$, and $\tilde{\mathbf{u}}_{K-1}$ arrive at receiver 1 along dimensions $h_{31}T_2, \ldots,$ $h_{K1}T_{K-1}$, and $h_{12}\left(\frac{h_{(K-1)1}}{h_{(K-1)2}}\right)T_K$, respectively, which are all in $\tilde{T}_2 \ldots$, $\tilde{T}_{K-1}$ and $\tilde{T}_K$, respectively. Thus, the signal $\tilde{\mathbf{u}}_i, i = 1, \ldots, K-1$ align with $\mathbf{u}_{i+1}$ in $\tilde{T}_{i+1}$, which is seen in Fig. 3.5 for $K = 3$, and in Fig. 3.7 for general K.

We further note that the sets $h_{11}T_3, \ldots, h_{11}T_{K+1}, \tilde{T}_1, \ldots, \tilde{T}_{K+1}$ are all separable since only T_i and $\tilde{T}_i$ (and not T_j or $\tilde{T}_j$) contain powers of c_i, and none of $\tilde{T}_3, \ldots,$ $\tilde{T}_{K+1}$ contains h_{11}. A similar observation holds for the received signal at any of the remaining receivers. Thus, the set

$$S = \left(\bigcup_{i=3}^{K+1} h_{11}T_i \right) \bigcup \left(\bigcup_{i=1}^{K+1} \tilde{T}_i \right) \tag{3.273}$$

has cardinality given by

$$M_s = (K-1)m^{K(K-1)+2} + (K+1)(m+1)^{K(K-1)+2} \tag{3.274}$$

At the external eavesdropper, there is no alignment and the cooperative jamming signals occupy the full space, thereby exhausting the decoding capability of the eavesdropper. This secures all the messages at the external eavesdropper.

We next provide an analysis for the achievable sum rate. Since we have only one eavesdropper, we use [43, Theorem 2] and observe that the rate

$$R_i = I(V_i; Y_i) - I(V_i; Z|V_{-i}) \tag{3.275}$$

is achievable, where V_i ia an auxiliary random variable satisfying $V_i \rightarrow X_i \rightarrow Y, Z$, and V_{-i} denotes the collection $\{V_j, j \neq i\}$. Note that since Ω is known at all the legitimate receivers and the eavesdropper, and since $\mathbf{V}_i$s are chosen to be independent of Ω, Ω should appear in the conditioning of each of the mutual information quantities in (3.275). We keep this in mind, but drop it for the sake of notational simplicity.

First, we can upper bound the probability of error at each receiver. Let

$$V_i \triangleq \left(\mathbf{v}_{i1} \dots \mathbf{v}_{i(i-1)} \quad \mathbf{v}_{i(i+2)} \dots \mathbf{v}_{i(K+1)}\right) \tag{3.276}$$

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

$$\Pr(V_i \neq \hat{V}_i) \leq \exp\left(-\eta_{\gamma_i} P^{\delta}\right) \tag{3.277}$$

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

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

$$\begin{aligned}
I(V_i; Y_i) &\geq I(V_i; \hat{V}_i) && (3.278)\\
&= H(V_i) - H(V_i|\hat{V}_i) && (3.279)\\
&= \log(|\mathcal{V}_i|) - H(V_i|\hat{V}_i) && (3.280)\\
&\geq \log(|\mathcal{V}_i|) - 1 - \Pr(V_i \neq \hat{V}_i)\log(|\mathcal{V}_i|) && (3.281)\\
&= \left[1 - \Pr(V_i \neq \hat{V}_i)\right]\log(|\mathcal{V}_i|) - 1 && (3.282)\\
&= \log(|\mathcal{V}_i|) - o(\log P) && (3.283)\\
&= \frac{(K-1)M(1-\delta)}{M_S + \delta}\left(\frac{1}{2}\log P\right) + o(\log P) && (3.284)
\end{aligned}$$

where $o(\cdot)$ is the little-o function, $\mathcal{V}_i$ is the alphabet of V_i and, in this case, the cardinality of $\mathcal{V}_i$ is $(2Q+1)^{(K-1)M} = (2Q+1)^{(K-1)m^{K(K-1)+2}}$. Here, M is defined in (3.264).

Now, we bound the second term in (3.275). Let

$$U \triangleq \{\mathbf{u}_i, \tilde{\mathbf{u}}_i, i = 1, \ldots, K\} \tag{3.285}$$

We have,

$$\begin{aligned} I(V_i;Z|V_{-i}) =& I(V_i,U;Z|V_{-i}) - I(U;Z|V_1^K) && (3.286)\\ =& h(Z) - h(Z|U,V_1^K) - H(U|V_1^K) + H(U|Z,V_1^K) && (3.287)\\ \le& \frac{1}{2}\log P - h(N_Z) - H(U) + o(\log P) && (3.288)\\ =& \frac{1}{2}\log P - H(U) + o(\log P) && (3.289)\\ =& \frac{1}{2}\log P - \log(2Q+1)^{2KM} + o(\log P) && (3.290)\\ =& \frac{1}{2}\log P - \frac{(1-\delta)2KM}{2(M_S+\delta)}\log P + o(\log P) && (3.291) \end{aligned}$$

Now, combining (3.284) and (3.291), we have,

$$R_i \ge \frac{2Km^{K(K-1)+2} - (K+1)(m+1)^{K(K-1)+2} - M\delta(3K-1)}{(K-1)m^{K(K-1)} + (K+1)(m+1)^{K(K-1)+2}}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{3.292}$$

By choosing δ small enough and choosing m large enough, we can make R_i arbitrarily close to $\frac{K-1}{2K}$. Thus, the sum s.d.o.f. of $\frac{K-1}{2}$ is achievable with fixed channel gains.

3.8.8 Fading Channel Gains

Here, we present a scheme that achieves $\frac{K-1}{2}$ s.d.o.f. using asymptotic vector space alignment with channel extension. Let $\Gamma = (K-1)^2$. We use $M_n = (K-1)n^\Gamma + (K+1)(n+1)^\Gamma$ channel uses to transmit $K(K-1)n^\Gamma$ message symbols securely to the legitimate receivers in the presence of the eavesdropper. Thus, we achieve a sum s.d.o.f. of $\frac{K(K-1)n^\Gamma}{(K-1)n^\Gamma+(K+1)(n+1)^\Gamma}$, which gets arbitrarily close to $\frac{K-1}{2}$ as $n \to \infty$.

First, we divide each message into many sub-messages; specifically, the message of the ith transmitter, W_i, is divided into $(K-1)$ sub-messages $V_{ij}, j = 1, \ldots, K+1, j \neq i, i+1$. Each V_{ij} is encoded into n^Γ independent streams $v_{ij}(1), \ldots, v_{ij}(n^\Gamma)$, which we denote as $\mathbf{v}_{ij} \triangleq \left(v_{ij}(1), \ldots, v_{ij}(n^\Gamma)\right)^T$. We also require artificial noise symbols U_i and $\tilde{U}_i$ at each transmitter i. Again, we encode the artificial noise symbols U_i and $\tilde{U}_i$ as

$$\mathbf{u}_i \triangleq \left(u_i(1), \ldots, u_i((n+1)^\Gamma)\right)^T, i = 1, \ldots, K \tag{3.293}$$

$$\tilde{\mathbf{u}}_i \triangleq \left(\tilde{u}_i(1), \ldots, \tilde{u}_i(n^\Gamma)\right)^T, i = 1, \ldots, K-1 \tag{3.294}$$

$$\tilde{\mathbf{u}}_K \triangleq \left(\tilde{u}_i(1), \ldots, \tilde{u}_i((n+1)^\Gamma)\right)^T \tag{3.295}$$

In each channel use $t \leq M_n$, we choose precoding column vectors $\mathbf{p}_{ij}(t)$, $\mathbf{q}_i(t)$ and $\tilde{\mathbf{q}}_i(t)$ with the same number of elements as $\mathbf{v}_{ij}$, $\mathbf{u}_i$ and $\tilde{\mathbf{u}}_i$, respectively. In channel use t, transmitter i sends

$$X_i(t) = \sum_j \mathbf{p}_{ij}(t)^T \mathbf{v}_{ij} + \mathbf{q}_i(t)^T \mathbf{u}_i + \tilde{\mathbf{q}}_i(t)^T \tilde{\mathbf{u}}_i \tag{3.296}$$

where we have dropped the limits on j in the summation for notational simplicity. By stacking the precoding vectors for all M_n channel uses, we let,

$$\mathbf{P}_{ij} = \begin{pmatrix} \mathbf{p}_{ij}(1)^T \\ \vdots \\ \mathbf{p}_{ij}^T(M_n) \end{pmatrix}, \qquad \mathbf{Q}_i = \begin{pmatrix} \mathbf{q}_i(1)^T \\ \vdots \\ \mathbf{q}_i(M_n)^T \end{pmatrix}, \qquad \tilde{\mathbf{Q}}_i = \begin{pmatrix} \tilde{\mathbf{q}}_i(1)^T \\ \vdots \\ \tilde{\mathbf{q}}_i(M_n)^T \end{pmatrix} \tag{3.297}$$

Now, letting $\mathbf{X}_i = (X_i(1), \dots, X_i(M_n))^T$, the channel input for all transmitter i over M_n channel uses can be compactly represented as

$$\mathbf{X}_i = \sum_j \mathbf{P}_{ij}\mathbf{v}_{ij} + \mathbf{Q}_i\mathbf{u}_i + \tilde{\mathbf{Q}}_i\tilde{\mathbf{u}}_i \tag{3.298}$$

Recall that, channel use t, the channel output at receiver l and the eavesdropper are, respectively, given by

$$Y_l(t) = \sum_{k=1}^{K} h_{kl}(t)X_k(t) + N_l(t) \tag{3.299}$$

$$Z(t) = \sum_{k=1}^{K} g_k(t)X_k(t) + N_Z(t) \tag{3.300}$$

Let $\mathbf{H}_{kl} \overset{\Delta}{=} \text{diag}\left(h_{kl}(1), \dots, h_{kl}(M_n)\right)$. Similarly, define $\mathbf{G}_k = \text{diag}\left(g_k(1), \dots, g_k(M_n)\right)$. The channel outputs at receiver l and the eavesdropper over all M_n channel uses, $\mathbf{Y}_l = (Y_l(1), \dots,$

$Y_l(M_n))^T$ and $\mathbf{Z} = (Z(1), \dots, Z(M_n))^T$, respectively, can be represented by

$$\mathbf{Y}_l = \sum_{k=1}^{K} \mathbf{H}_{kl}\mathbf{X}_k + \mathbf{N}_l \tag{3.301}$$

$$= \sum_{k=1}^{K} \mathbf{H}_{kl} \left(\sum_{\substack{j=1 \\ j\neq k,k+1}}^{K+1} \mathbf{P}_{kj}\mathbf{v}_{kj} + \mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k \right) + \mathbf{N}_l \tag{3.302}$$

$$= \sum_{\substack{j=1 \\ j\neq l,l+1}}^{K+1} \mathbf{H}_{ll}\mathbf{P}_{lj}\mathbf{v}_{lj} + \sum_{\substack{k=1 \\ k\neq l}}^{K} \sum_{\substack{j=1 \\ j\neq k,k+1}}^{K+1} \mathbf{H}_{kl}\mathbf{P}_{kj}\mathbf{v}_{kj} + \sum_{k=1}^{K} \mathbf{H}_{kl}\left(\mathbf{Q}_k\mathbf{u}_k + \tilde{\mathbf{Q}}_k\tilde{\mathbf{u}}_k\right) + \mathbf{N}_l \tag{3.303}$$

and,

$$\begin{aligned}\mathbf{Z} =& \sum_{k=1}^{K} \mathbf{G}_k \mathbf{X}_k + \mathbf{N}_Z && (3.304)\\ =& \sum_{k=1}^{K} \sum_{\substack{j=1\\ j\neq k,k+1}}^{K+1} \mathbf{G}_k \mathbf{P}_{kj} \mathbf{v}_{kj} + \sum_{k=1}^{K} \mathbf{G}_k \left(\mathbf{Q}_k \mathbf{u}_k + \tilde{\mathbf{Q}}_k \tilde{\mathbf{u}}_k \right) + \mathbf{N}_Z && (3.305)\end{aligned}$$

Note that receiver l wants to decode $\mathbf{v}_{lj}, j = 1, \ldots, K+1, j \neq l, l+1$. Thus, the remaining terms in (3.303) constitute interference at the lth receiver. Recall that $CS(\mathbf{X})$ denotes the column space of the matrix $\mathbf{X}$. Then, I_l denoting the space spanned by this interference is

$$I_l = \left(\bigcup_{k\neq l, j\neq k,k+1} CS\left(\mathbf{H}_{kl}\mathbf{P}_{kj}\right) \right) \bigcup \left(\bigcup_{k=1}^{K} CS\left(\mathbf{H}_{kl}\mathbf{Q}_k\right) \right) \bigcup \left(\bigcup_{k=1}^{K} CS\left(\mathbf{H}_{kl}\tilde{\mathbf{Q}}_k\right) \right) \tag{3.306}$$

Note that there are $(K-1)n^{\Gamma}$ symbols to be decoded by each legitimate receiver in $(K-1)n^{\Gamma} + (K+1)(n+1)^{\Gamma}$ channel uses. Thus, for decodability, the interference can occupy a subspace of rank at most $(K+1)(n+1)^{\Gamma}$, that is,

$$\text{rank}(I_l) \leq (K+1)(n+1)^{\Gamma} \tag{3.307}$$

To that end, we align the noise and message subspaces at each legitimate receiver appropriately. Note that no such alignment is possible at the external eavesdropper since the transmitters do not have its CSI. However, note that we have a total of $(K-1)n^{\Gamma} + (K+1)(n+1)^{\Gamma}$ artificial noise symbols which will span the full received signal space at the eavesdropper and secures all the messages.

Fig. 3.5 shows the alignment for $K=3$ receivers. For the general K-user case, Fig. 3.7 shows the alignment in the interfering signal dimensions. At receiver l, it is as follows: First, the artificial noise symbols $\tilde{\mathbf{u}}_k$ is aligned with $\mathbf{u}_{k+1}$, for every $k=1,\dots,K-1$. Thus, we have,

$$\mathbf{H}_{kl}\tilde{\mathbf{Q}}_k \preceq \mathbf{H}_{(k+1)l}\mathbf{Q}_{(k+1)}, \quad k=1,\dots,K-1 \tag{3.308}$$

where $\mathbf{A} \preceq \mathbf{B}$ is used to denote that $CS(\mathbf{A}) \subseteq CS(\mathbf{B})$. Thus, the subspace spanned by the artificial noise symbols can have a rank of at most $(K+1)(n+1)^{\Gamma}$.

The unwanted message symbols $\mathbf{v}_{kj}$, $k \neq l$, are aligned with $\mathbf{u}_j$ if $j \leq K$, or $\tilde{\mathbf{u}}_K$ otherwise. Thus,

$$\mathbf{H}_{kl}\mathbf{P}_{kj} \preceq \mathbf{H}_{jl}\mathbf{Q}_j, \quad j \leq K \tag{3.309}$$

$$\mathbf{H}_{kl}\mathbf{P}_{k(K+1)} \preceq \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K \tag{3.310}$$

for each $k \neq l$. Since, the unwanted messages at each receiver are aligned under the artificial noise subspaces, they do not increase the rank of I_l any further.

We can group the alignment equations for the artificial noise $\mathbf{u}_k$, $k=1,\dots,K$, and $\tilde{\mathbf{u}}_K$ for all K legitimate receivers. For $\mathbf{u}_1$, we have,

$$\mathbf{H}_{kl}\mathbf{P}_{k1} \preceq \mathbf{H}_{1l}\mathbf{Q}_1, \quad k \in \{2,\dots,K\}, l \in \{1,\dots,K\}, l \neq k \tag{3.311}$$

Clearly, these are $(K-1)^2$ alignment equations. Similarly, we have $(K-1)^2$ alignment equations for $\tilde{\mathbf{u}}_K$, given by

$$\mathbf{H}_{kl}\mathbf{P}_{k(K+1)} \preceq \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K, \quad k \in \{1,\ldots,K-1\}, l \in \{1,\ldots,K\}, l \neq k \tag{3.312}$$

For the artificial noises $\mathbf{u}_k, k = 2,\ldots,K$, we have the following alignment equations:

$$\mathbf{H}_{(k-1)l}\tilde{\mathbf{Q}}_{k-1} \preceq \mathbf{H}_{kl}\mathbf{Q}_k \tag{3.313}$$

$$\mathbf{H}_{il}\mathbf{P}_{ik} \preceq \mathbf{H}_{kl}\mathbf{Q}_k, \quad i \neq k-1, k, \quad l \neq i \tag{3.314}$$

Thus, there are $(K-1)^2+1$ alignment equations for each $\mathbf{u}_k, k = 2,\ldots,K$. Now we make the following selections:

$$\mathbf{P}_{k1} =\tilde{\mathbf{P}}_1, \quad k = 2,\ldots,K \tag{3.315}$$

$$\mathbf{P}_{k(K+1)} =\tilde{\mathbf{P}}_{K+1}, \quad k = 1,\ldots,K-1 \tag{3.316}$$

$$\mathbf{P}_{ik} =\tilde{\mathbf{P}}_k, \quad i \neq k-1, k, \quad k = 2,\ldots,K \tag{3.317}$$

$$\mathbf{H}_{(k-1)1}\tilde{\mathbf{Q}}_{k-1} =\mathbf{H}_{(k+1)1}\tilde{\mathbf{P}}_k, \quad k = 2,\ldots,K-1 \tag{3.318}$$

$$\mathbf{H}_{(K-1)2}\tilde{\mathbf{Q}}_{K-1} =\mathbf{H}_{12}\tilde{\mathbf{P}}_K \tag{3.319}$$

Now, note that it suffices to choose the matrices $\tilde{\mathbf{P}}_k$, $k = 1,\ldots,K+1$ in order to specify all the precoding matrices. Using these selections in our alignment equations in (3.311), (3.312), (3.313) and (3.314), we have $(K-1)^2$ alignment equations for each $\mathbf{u}_k$, $k = 1, \ldots, K$ and $\tilde{\mathbf{u}}_K$, given by,

$$\mathbf{T}_k \tilde{\mathbf{P}}_k \preceq \mathbf{Q}_k, \quad \mathbf{T}_k \in \tau_k, \quad k = 1, \ldots, K \tag{3.320}$$

$$\mathbf{T}_{K+1} \tilde{\mathbf{P}}_{K+1} \preceq \tilde{\mathbf{Q}}_K, \quad \mathbf{T}_{K+1} \in \tau_{K+1} \tag{3.321}$$

where the sets τ_k, $k = 1, \ldots, K+1$ are given by

$$\tau_1 = \left\{ \mathbf{H}_{1l}^{-1} \mathbf{H}_{kl}, k \in \{2, \ldots, K\}, l \in \{1, \ldots, K\}, l \neq k \right\} \tag{3.322}$$

$$\tau_{K+1} = \left\{ \mathbf{H}_{Kl}^{-1} \mathbf{H}_{kl}, k \in \{1, \ldots, K-1\}, l \in \{1, \ldots, K\}, l \neq k \right\} \tag{3.323}$$

$$\tau_k = \tau_k^P \bigcup \tau_k^Q \tag{3.324}$$

where,

$$\tau_k^P = \left\{ \mathbf{H}_{kl}^{-1} \mathbf{H}_{il}, i \notin \{k-1, k\}, l \neq i, l \in \{1, \ldots, K\} \right\} \tag{3.325}$$

$$\tau_k^Q = \begin{cases} \left\{ \mathbf{H}_{kl}^{-1} \mathbf{H}_{(k-1)l} \mathbf{H}_{(k-1)1}^{-1} \mathbf{H}_{(k+1)1}, l \in \{1, \ldots, K\} \right\}, & \text{if } k \in \{2, \ldots, K-1\} \\ \left\{ \mathbf{H}_{Kl}^{-1} \mathbf{H}_{(K-1)l} \mathbf{H}_{(K-1)2}^{-1} \mathbf{H}_{12}, l \in \{1, \ldots, K\} \right\}, & \text{if } k = K \end{cases} \tag{3.326}$$

We can now construct the matrices $\tilde{\mathbf{P}}_k, k = 1, \ldots, K+1$, $\mathbf{Q}_k, k = 1, \ldots, K$ and $\tilde{\mathbf{Q}}_K$ as in [8]

$$\tilde{\mathbf{P}}_k = \left\{ \left(\prod_{\mathbf{T} \in \tau_k} \mathbf{T}^{\alpha_T} \right) \mathbf{w}_k : \alpha_T \in \{1, \ldots, n\} \right\} \tag{3.327}$$

$$\mathbf{Q}_k = \left\{ \left(\prod_{\mathbf{T} \in \tau_k} \mathbf{T}^{\alpha_T} \right) \mathbf{w}_k : \alpha_T \in \{1, \dots, n+1\} \right\} \tag{3.328}$$

$$\tilde{\mathbf{Q}}_K = \left\{ \left(\prod_{\mathbf{T} \in \tau_{K+1}} \mathbf{T}^{\alpha_T} \right) \mathbf{w}_{K+1} : \alpha_T \in \{1, \dots, n+1\} \right\} \tag{3.329}$$

where each $\mathbf{w}_k$ is the $M_n \times 1$ column vector containing elements drawn independently from a continuous distribution with bounded support. This completes the description of our scheme.

Decodability: By our construction, the interference space at legitimate receiver l is given by,

$$I_l = \left(\bigcup_{k=1}^{K} CS(\mathbf{H}_{kl}\mathbf{Q}_k) \right) \bigcup \left(CS(\mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K) \right) \tag{3.330}$$

and clearly,

$$\text{rank}(I_l) \leq (K+1)(n+1)^{\Gamma} \tag{3.331}$$

We only need to show that desired signals $\mathbf{v}_{lj}, j \neq l, l+1$ fall outside I_l. The desired signal space at receiver l is given by

$$\mathbf{D}_l = \left[\mathbf{H}_{ll}\tilde{\mathbf{P}}_1 \dots \mathbf{H}_{ll}\tilde{\mathbf{P}}_{l-1} \quad \mathbf{H}_{ll}\tilde{\mathbf{P}}_{l+2} \dots, \mathbf{H}_{ll}\tilde{\mathbf{P}}_K \right] \tag{3.332}$$

We want to show that the matrix

$$\mathbf{\Lambda}_l = \left[\mathbf{D}_l \quad \tilde{\mathbf{I}}_l \right] \tag{3.333}$$

where,

$$\tilde{\mathbf{I}}_l = \begin{bmatrix} \mathbf{H}_{1l}\mathbf{Q}_1 \dots \mathbf{H}_{Kl}\mathbf{Q}_K & \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K \end{bmatrix} \tag{3.334}$$

is full rank almost surely. To do so, we will use [69, Lemmas 1, 2]. Note that the mth row of $\mathbf{H}_{kl}\mathbf{Q}_k$ contains the term w_{mk} with exponent 1, but no $w_{mk'}$ for $k \neq k'$, where w_{mk} denotes the element in the mth row of $\mathbf{w}_k$. In fact, the term w_{mk} occurs nowhere else in the matrix $\mathbf{\Lambda}_l$ except in $\mathbf{H}_{kl}\mathbf{Q}_k$ and $\mathbf{H}_{ll}\tilde{\mathbf{P}}_k$. This shows, using [69, Lemmas 1, 2], that $\mathbf{D}_l$ and $\tilde{\mathbf{I}}_l$ are full rank almost surely. Further, it suffices to show that the matrices $\begin{bmatrix} \mathbf{H}_{ll}\tilde{\mathbf{P}}_k & \mathbf{H}_{kl}\mathbf{Q}_k \end{bmatrix}, k = 1, \dots, K$, and $\begin{bmatrix} \mathbf{H}_{ll}\tilde{\mathbf{P}}_{K+1} & \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_K \end{bmatrix}$ are all full column rank. First, $\begin{bmatrix} \mathbf{H}_{ll}\tilde{\mathbf{P}}_1 & \mathbf{H}_{kl}\mathbf{Q}_1 \end{bmatrix}$ is full column rank since $\mathbf{H}_{kl}\mathbf{Q}_1$ misses the term $\mathbf{H}_{ll}$. Similarly, $\begin{bmatrix} \mathbf{H}_{ll}\tilde{\mathbf{P}}_{K+1} & \mathbf{H}_{Kl}\tilde{\mathbf{Q}}_1 \end{bmatrix}$ is full column rank. Further, if $k \neq l, l+1$, $\mathbf{H}_{kl}\mathbf{Q}_k$ does not contain $\mathbf{H}_{ll}$ and hence $\begin{bmatrix} \mathbf{H}_{ll}\tilde{\mathbf{P}}_k & \mathbf{H}_{kl}\mathbf{Q}_k \end{bmatrix}$ is full column rank. Finally, note that the lth transmitter does not transmit any message signals along $\tilde{\mathbf{P}}_k$, when $k = l, l+1$. Thus, the matrix $\mathbf{\Lambda}_l$ is full rank almost surely. This ensures decodability of the desired signals at each receiver.

Security guarantee: Let $\mathbf{v} = \{\mathbf{v}_{ij}, i, j \in \{1, \dots, K\}, j \neq i, i+1\}$, that is, $\mathbf{v}$ is the collection of all legitimate messages to be secured from the eavesdropper. Also, let $\mathbf{u} = \{\mathbf{u}_k, \tilde{\mathbf{u}}_k, k = 1, \dots, K\}$, that is $\mathbf{u}$ is the collection of all the artificial noise symbols. We note that

$$I(\mathbf{v};\mathbf{Z}) = h(\mathbf{Z}) - h(\mathbf{Z}|\mathbf{v}) \tag{3.335}$$

$$\leq \frac{M_n}{2}\log P - h(\mathbf{A}\mathbf{u}) + o(\log P) \tag{3.336}$$

$$=\frac{M_n}{2}\log P - \frac{M_n}{2}\log P + o(\log P) \tag{3.337}$$

$$=o(\log P) \tag{3.338}$$

where $\mathbf{A}$ is a $M_n \times M_n$ full rank matrix, and we have used Lemma 4 in (3.337). Also, we have implicitly used the fact that Ω appears in the conditioning of each mutual information and differential entropy term in the above calculation. Now, as before, by treating the vector channel with M_n slots as one channel use, and using wiretap channel codes, we get,

$$R_i \geq \frac{(K-1)n^\Gamma}{M_n}\log P + o(\log P) \tag{3.339}$$

for each $i = 1, \ldots, K$, which gives us the required sum s.d.o.f. of $\frac{K(K-1)n^\Gamma}{(K-1)n^\Gamma+(K+1)(n+1)^\Gamma}$, which approaches $\frac{K-1}{2}$ as $n \to \infty$.

3.8.9 Achievable Scheme for the Multiple Access Wiretap Channel with Partial CSIT and Fading Channel Gains

We construct a scheme that achieves the desired sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$ with fading channel gains. Without loss of generality, assume that the first m transmitters have eavesdropper CSI, while the remaining transmitters have no eavesdropper CSI. We provide a scheme to achieve the rate tuple $(d_1, \ldots, d_m, d_{m+1}, \ldots, d_K) = \left(\frac{K-1}{m(K-1)+1}, \ldots, \frac{K-1}{m(K-1)+1}, 0, \ldots, 0\right)$, thus, achieving the sum s.d.o.f. of $\frac{m(K-1)}{m(K-1)+1}$. For each $i = 1, \ldots, m$, transmitter i sends $\mathbf{V}_i = \{V_{ij}, , j \neq i, j = 1, \ldots, K\}$ symbols in

$m(K-1)+1$ time slots. Let $\mathbf{V}=\{\mathbf{V}_i, i=1,\dots,K\}$. Fig. 3.6 illustrates the alignment of the signals at the end of the scheme when $K=3$ and $m=2$. The scheme is as follows:

At time $t\in\{1,\dots,m(K-1)+1\}$, the ith transmitter, $i=1,\dots,K$, sends,

$$X_i(t)=\begin{cases}\sum_{j=1,j\neq i}^{K}\frac{g_j(t)}{h_j(t)g_i(t)}V_{ij}+\frac{1}{h_i(t)}U_i, & 1\leq i\leq m\\ \\ \frac{1}{h_i(t)}U_i, & m+1\leq i\leq K\end{cases} \tag{3.340}$$

where U_i is an artificial noise symbol. This ensures that the noise symbols U_i all align at the legitimate receiver. On the other hand, the artificial noise symbol from the jth transmitter U_j protects all the messages V_{ij} for every i, at the eavesdropper. The channel outputs are given by,

$$Y(t)=\sum_{i=1}^{m}\sum_{j\neq i}\frac{h_i(t)g_j(t)}{h_j(t)g_i(t)}V_{ij}+\sum_{i=1}^{K}U_i+N_1(t) \tag{3.341}$$

$$Z(t)=\sum_{i=1}^{K}\frac{g_i(t)}{h_i(t)}\left(U_i+\sum_{j=1,j\neq i}^{m}V_{ji}\right)+N_2(t) \tag{3.342}$$

After the $m(K-1)+1$ time slots, the legitimate receiver ends up with $m(K-1)+1$ linearly independent equations with $m(K-1)+1$ variables: $\sum_{i=1}^{K}U_i$ and the $m(K-1)$ variables $\{V_{ij}\}$. Thus, it can decode all the $m(K-1)$ message symbols V_{ij}. Defining $\mathbf{Y}=\{Y(t),\ t=1,\dots,m(K-1)+1\}$ and $\mathbf{Z}$ similarly as $\mathbf{Y}$, this means that $I(\mathbf{V};\mathbf{Y})=m(K-1)\frac{1}{2}\log P+o(\log P)$, and also $I(\mathbf{V};\mathbf{Z})\leq o(\log P)$, concluding the achievability proof.

Chapter 4: Secure Degrees of Freedom of the Multiple Access Wiretap Channel with Multiple Antennas

4.1 Introduction

We consider the two-user multiple-input multiple-output (MIMO) multiple access wiretap channel where each transmitter has N antennas, the legitimate receiver has N antennas and the eavesdropper has K antennas; see Fig. 4.1. We consider the case when the channel gains are fixed throughout the duration of the communication, as well as the case when the channel is fast fading and the channel gains vary in an i.i.d. fashion across time. Our goal in this chapter is to characterize how the optimal sum secure degrees of freedom (s.d.o.f.) of the MIMO multiple access wiretap channel varies with the number of antennas at the legitimate users and the eavesdropper.

To that end, we partition the range of K into various regimes, and propose achievable schemes for each regime. With fading channel gains, our schemes are based on a combination of zero-forcing beamforming and vector space interference alignment techniques. In order to achieve the optimal sum s.d.o.f., which is in the form $2\left(d+\frac{l}{3}\right)$, $l = 0, 1, 2$, where d is an integer, with fixed real channel gains,

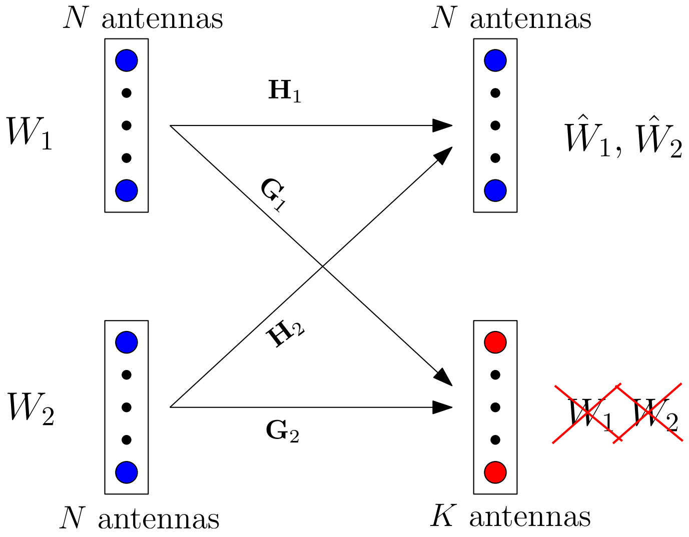


Figure 4.1: The MIMO multiple access wiretap channel.

we decompose the channel input at each transmitter into two parts: a Gaussian signaling part carrying d (the integer part) d.o.f. of information securely, and a structured signaling part carrying $\frac{l}{3}$ (the fractional part) d.o.f. of information securely. The structure of the Gaussian signals carrying the integer s.d.o.f. resembles that of the schemes for the fading channel gains. The structured signals carrying $\frac{2l}{3}$ sum s.d.o.f. are designed using the real interference alignment technique [9].

We also establish the optimality of our achievable schemes with matching converses in each regime. A simple upper bound, given by $\min((2N-K)^+, N)$, is obtained by allowing cooperation between the two transmitters, which enhances the two-user multiple access wiretap channel to a MIMO wiretap channel with $2N$ antennas at the transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper [13,14]. This bound is optimal when the number of eavesdropper antennas K is either quite small ($K \leq \frac{N}{2}$), or quite large ($K \geq \frac{4N}{3}$). When K is small, the sum s.d.o.f. is limited by the decoding capability of the legitimate receiver, and the optimal sum s.d.o.f. is N which is optimal even without any secrecy constraints. When K is large, the s.d.o.f. is limited by the requirement of secrecy from a very strong eavesdropper. For intermediate values of K, the distributed nature of the transmitters dominates, and we employ a generalization of the SISO converse techniques of [4] for the converse proof in the MIMO case.

4.2 System Model

The two-user multiple access wiretap channel, see Fig. 4.1, is described by,

$$\mathbf{Y}(t) = \mathbf{H}_1(t)\mathbf{X}_1(t) + \mathbf{H}_2(t)\mathbf{X}_2(t) + \mathbf{N}_1(t) \tag{4.1}$$

$$\mathbf{Z}(t) = \mathbf{G}_1(t)\mathbf{X}_1(t) + \mathbf{G}_2(t)\mathbf{X}_2(t) + \mathbf{N}_2(t) \tag{4.2}$$

where $\mathbf{X}_i(t)$ is an N dimensional column vector denoting the ith user's channel input, $\mathbf{Y}(t)$ is an N dimensional vector denoting the legitimate receiver's channel output, and $\mathbf{Z}(t)$ is a K dimensional vector denoting the eavesdropper's channel output, at time t. In addition, $\mathbf{N}_1(t)$ and $\mathbf{N}_2(t)$ are N and K dimensional white Gaussian noise vectors, respectively, with $\mathbf{N}_1 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$ and $\mathbf{N}_2 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_K)$, where $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. Here, $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are the $N \times N$ and $K \times N$ channel matrices from transmitter i to the legitimate receiver and the eavesdropper, respectively, at time t. When the channel gains are fixed, the entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are drawn from an arbitrary but fixed continuous distribution with bounded support in an i.i.d. fashion prior to the start of the communication, and remain fixed throughout the duration of the communication, i.e., for $1 \leq t \leq n$.

When the channel gains are fading, the entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are drawn from the fixed continuous distribution with bounded support in an i.i.d. fashion at every time slot t. We assume that the channel matrices $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are known with full precision at all terminals, at time t. All channel inputs satisfy the average power constraint $E[\|\mathbf{X}_i(t)\|^2] \leq P$, $i = 1, 2$, where $\|\mathbf{X}\|$ denotes the Euclidean (or the spectral norm) of the vector (or matrix) $\mathbf{X}$.

Transmitter i wishes to send a message W_i, uniformly distributed in $\mathcal{W}_i$, securely to the legitimate receiver in the presence of the eavesdropper. A secure rate pair (R_1, R_2), with $R_i = \frac{\log|\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W_i \neq \hat{W}_i] \leq \epsilon_n$, for $i = 1, 2$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \leq \epsilon_n \tag{4.3}$$

where $\epsilon_n \to 0$ as $n \to \infty$. An s.d.o.f. pair (d_1, d_2) is said to be achievable if a rate pair (R_1, R_2) is achievable with

$$d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2}\log P} \tag{4.4}$$

The sum s.d.o.f. d_s is the largest achievable $d_1 + d_2$.

4.3 Main Result

The main result of this chapter is the determination of the optimal sum s.d.o.f. of the MIMO multiple access wiretap channel. We have the following theorem.

Theorem 7 *The optimal sum s.d.o.f. of the MIMO multiple access wiretap channel with N antennas at the transmitters, N antennas at the legitimate receiver and K antennas at the eavesdropper is given by*

$$d_s = \begin{cases} N, & \text{if } K \leq \frac{1}{2}N \\ \frac{2}{3}(2N-K), & \text{if } \frac{1}{2}N \leq K \leq N \\ \frac{2}{3}N, & \text{if } N \leq K \leq \frac{4}{3}N \\ 2N-K, & \text{if } \frac{4}{3}N \leq K \leq 2N \\ 0, & \text{if } K \geq 2N. \end{cases} \tag{4.5}$$

for almost all channel gains.

We present the converse proof for this theorem in Section 4.4. The achievable schemes for the case of fading channel gains are presented in Section 4.5, while the achievable schemes for the case of fixed channel gains are presented in Section 4.6.

Fig. 4.2 shows the variation of the optimal sum s.d.o.f. with the number of eavesdropper antennas K. Note that as in the SISO case, the optimal sum s.d.o.f. is higher for the multiple access wiretap channel than for the wiretap channel with one helper [12], when $K < 3N/2$. However, when the number of eavesdropper antennas

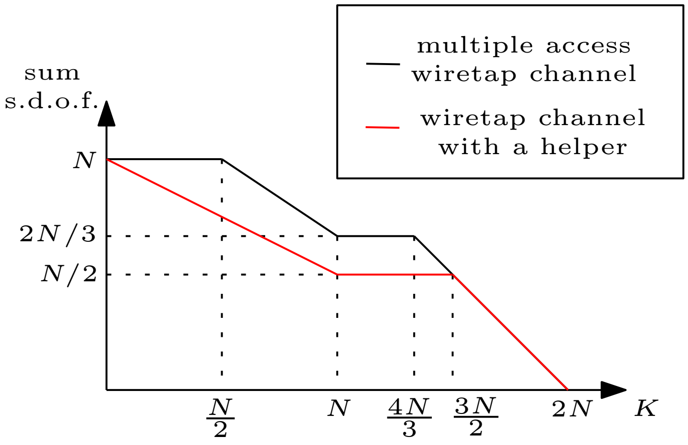


Figure 4.2: d_s versus K.

K is large enough, i.e., when $K \geq 3N/2$, the optimal sum s.d.o.f. of the multiple access wiretap channel is the same as the optimal s.d.o.f. of the wiretap channel with a helper.

Further, note that when the number of eavesdropper antennas K is small enough ($K \leq \frac{N}{2}$), the optimal sum s.d.o.f. is N, which is the optimal d.o.f. of the multiple access channel without any secrecy constraints. Thus, there is no penalty for imposing the secrecy constraints in this regime. Also note that allowing cooperation beteen the transmitters does not increase the sum s.d.o.f. in this regime. Heuristically, the eavesdropper is quite weak in this regime, and the optimal sum s.d.o.f. is limited by the decoding capabilities of the legitimate receiver.

On the other hand, when the number of antennas K is quite large ($K \geq \frac{4N}{3}$), the optimal sum s.d.o.f. is $(2N - K)$, which is the optimal s.d.o.f. obtained by allowing cooperation between the transmitters. Intuitively, the eavesdropper is very strong in this regime and the sum s.d.o.f. is limited by the requirement of secrecy from this strong eavesdropper. In the intermediate regime, when $\frac{N}{2} \leq K \leq \frac{4N}{3}$, the distributed nature of the transmitters becomes a key factor and the upper bound obtained by allowing cooperation between the transmitters is no longer achievable; see Fig. 4.3.

4.4 Proof of the Converse

We prove the following upper bounds which are combined to give the converse for the full range of N and K,

$$d_1 + d_2 \leq \min((2N-K)^+, N) \tag{4.6}$$

$$d_1 + d_2 \leq \max\left(\frac{2}{3}(2N-K), \frac{2}{3}N\right) \tag{4.7}$$

where $(x)^+$ denotes $\max(x, 0)$.

It can be verified from Fig. 4.3 that the minimum of the two bounds in (4.6)-(4.7) gives the converse to the sum s.d.o.f. stated in (4.5) for all ranges of N and K. Thus, we next provide proofs of each of the bounds in (4.6) and (4.7).

4.4.1 Proof of $d_1 + d_2 \leq \min((2N-K)^+, N)$

This bound follows by allowing cooperation between the transmitters, which reduces the two-user multiple access wiretap channel to a single-user MIMO wiretap channel with $2N$ antennas at the transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper. The optimal s.d.o.f. for this MIMO wiretap channel is known to be $\min((2N-K)^+, N)$ [13, 14].

4.4.2 Proof of $d_1 + d_2 \leq \max\left(\frac{2}{3}(2N-K), \frac{2}{3}N\right)$

We only show that $d_1 + d_2 \leq \frac{2}{3}(2N-K)$, when $K \leq N$, and note that the bound $d_1 + d_2 \leq \frac{2}{3}N$ for $K > N$ follows from the fact that increasing the number of eavesdropper antennas cannot increase the sum s.d.o.f.; thus, the sum s.d.o.f. when $K > N$ is upper-bounded by the sum s.d.o.f. for the case of $K = N$, which is $\frac{2}{3}N$.

To prove $d_1 + d_2 \leq \frac{2}{3}(2N-K)$ when $K \leq N$, we follow [4,12]. We define noisy versions of $\mathbf{X}_i$ as $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$ where $\tilde{\mathbf{N}}_i \sim \mathcal{N}(\mathbf{0}, \rho_i^2 \mathbf{I}_N)$ with $\rho_i^2 < \min\left(\frac{1}{\|\mathbf{H}_i\|^2}, \frac{1}{\|\mathbf{G}_i\|^2}\right)$. The *secrecy penalty lemma* [4] can then be derived as

$$\begin{aligned} n(R_1 + R_2) \leq& I(W_1, W_2; \mathbf{Y}^n | \mathbf{Z}^n) + n\epsilon && (4.8)\\ \leq& h(\mathbf{Y}^n | \mathbf{Z}^n) + nc_1 && (4.9)\\ =& h(\mathbf{Y}^n, \mathbf{Z}^n) - h(\mathbf{Z}^n) + nc_1 && (4.10)\\ \leq& h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 && (4.11)\\ \leq& h(\tilde{\mathbf{X}}_1^n) + h(\tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 && (4.12) \end{aligned}$$

Now consider a stochastically equivalent version of $\mathbf{Z}$ given by $\tilde{\mathbf{Z}} = \mathbf{G}_1\tilde{\mathbf{X}}_1 + \mathbf{G}_2\mathbf{X}_2 + \mathbf{N}_Z$, where $\mathbf{N}_Z$ is an independent Gaussian noise vector, distributed as $\mathcal{N}(\mathbf{0}, \mathbf{I}_K - \rho_1^2 \mathbf{G}_1 \mathbf{G}_1^H)$. Further, let $\mathbf{G}_1 = [\tilde{\mathbf{G}}_1 \quad \hat{\mathbf{G}}_1]$ and $\tilde{\mathbf{X}}_1^T = [\tilde{\mathbf{X}}_{1a}^T \quad \tilde{\mathbf{X}}_{1b}^T]^T$, where $\tilde{\mathbf{G}}_1$ is the matrix with the first K columns of $\mathbf{G}_1$, $\hat{\mathbf{G}}_1$ has the last $N-K$ columns of $\mathbf{G}_1$, $\tilde{\mathbf{X}}_{1a}$ is a vector with the top K elements of $\tilde{\mathbf{X}}_1$, while $\tilde{\mathbf{X}}_{1b}$ has the remaining $N-K$ elements of $\tilde{\mathbf{X}}_1$. Then, we have

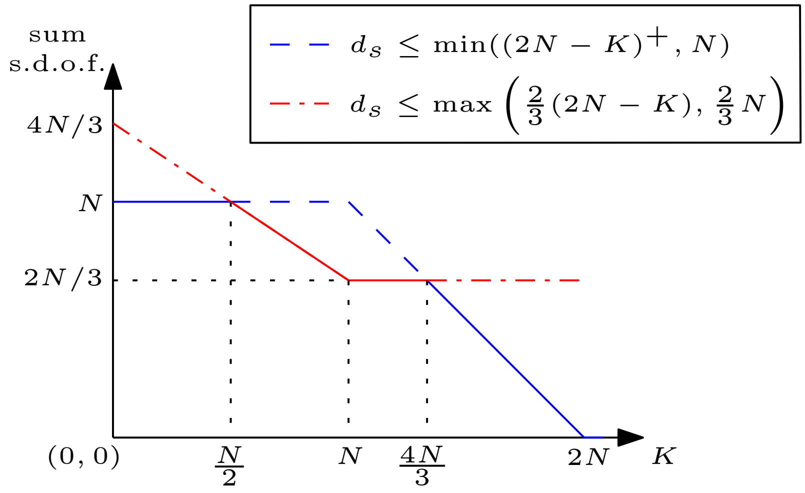


Figure 4.3: The two upper bounds.

$$h(\mathbf{Z}^n) = h(\tilde{\mathbf{Z}}^n) = h(\mathbf{G}_1^n\tilde{\mathbf{X}}_1^n + \mathbf{G}_2^n\mathbf{X}_2^n + \mathbf{N}_Z^n) \tag{4.13}$$

$$\geq h(\mathbf{G}_1^n\tilde{\mathbf{X}}_1^n) \tag{4.14}$$

$$= h(\tilde{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1a}^n + \hat{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1b}^n) \tag{4.15}$$

$$\geq h(\tilde{\mathbf{G}}_1^n\tilde{\mathbf{X}}_{1a}^n|\tilde{\mathbf{X}}_{1b}^n) \tag{4.16}$$

$$= h(\tilde{\mathbf{X}}_{1a}^n|\tilde{\mathbf{X}}_{1b}^n) + nc_3 \tag{4.17}$$

Using (4.17) in (4.12), we have

$$n(R_1 + R_2) \leq h(\tilde{\mathbf{X}}_{1b}^n) + h(\tilde{\mathbf{X}}_2^n) + nc_4 \tag{4.18}$$

The *role of a helper lemma* [4] also generalizes to the MIMO case as

$$nR_1 \leq I(\mathbf{X}_1^n; \mathbf{Y}^n) \tag{4.19}$$

$$= h(\mathbf{Y}^n) - h(\mathbf{H}_2^n\mathbf{X}_2^n + \mathbf{N}_1^n) \tag{4.20}$$

$$\leq h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_2^n) + nc_5 \tag{4.21}$$

Adding (4.18) and (4.21), we have

$$n(2R_1 + R_2) \leq h(\mathbf{Y}^n) + h(\tilde{\mathbf{X}}_{1b}^n) + nc_6 \tag{4.22}$$

$$\leq N\frac{n}{2}\log P + (N-K)\frac{n}{2}\log P + nc_7 \tag{4.23}$$

$$=(2N-K)\frac{n}{2}\log P + nc_7 \tag{4.24}$$

First dividing by n and letting $n \to \infty$, and then dividing by $\frac{1}{2}\log P$ and letting $P \to \infty$, we have

$$2d_1 + d_2 \leq 2N - K \tag{4.25}$$

By reversing the roles of the transmitters, we have

$$d_1 + 2d_2 \leq 2N - K \tag{4.26}$$

Combining (4.25) and (4.26), we have the required bound

$$d_1 + d_2 \leq \frac{2}{3}(2N - K) \tag{4.27}$$

This completes the proof of the converse of Theorem 7.

4.5 Achievable Schemes for Fading Channel Gains

We provide separate achievable schemes for each of the following regimes:

1. $K \leq N/2$

2. $N/2 \leq K \leq N$

3. $N \leq K \leq 4N/3$

4. $4N/3 \leq K \leq 3N/2$

5. $3N/2 \leq K \leq 2N$

Each scheme described in the following sections can be outlined as follows. We neglect the impact of noise at high SNR. Then, to achieve a certain sum s.d.o.f., d_s, we achieve the s.d.o.f. pair (d_1, d_2) with $d_s = d_1 + d_2$. We send n_1 symbols $\mathbf{v}_1 = (v_{11}, \ldots, v_{1n_1})$ and n_2 symbols $\mathbf{v}_2 = (v_{21}, \ldots, v_{2n_2})$ from the first and second transmitters, respectively, in n_B slots, such that $d_1 = n_1/n_B$ and $d_2 = n_2/n_B$. Finally, we show that the leakage of information symbols at the eavesdropper is $o(\log P)$. We however want a stronger guarantee of security, namely,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \to 0 \tag{4.28}$$

as $n \to \infty$. To achieve this, we view the n_B slots described in the scheme as a block and treat the equivalent channel from $\mathbf{v}_1$ and $\mathbf{v}_2$ to $\mathbf{Y}$ and $\mathbf{Z}$ as a memoryless multiple access wiretap channel with $\mathbf{Y}$ being the output at the legitimate receiver and $\mathbf{Z}$ being the output at the eavesdropper. The following sum secure rate is achievable [70]:

$$\sup(R_1 + R_2) \geq I(\mathbf{V}; \mathbf{Y}) - I(\mathbf{V}; \mathbf{Z}) \tag{4.29}$$

where $\mathbf{V} \triangleq \{\mathbf{v}_1, \mathbf{v}_2\}$. Using the proposed scheme, $\mathbf{v}_1$ and $\mathbf{v}_2$ can be reconstructed from $\mathbf{Y}$ to within noise distortion. Thus,

$$I(\mathbf{V}; \mathbf{Y}) =(n_1 + n_2)\frac{1}{2}\log P + o(\log P) \tag{4.30}$$

Also, for each scheme, by design

$$I(\mathbf{V}; \mathbf{Z}) =o(\log P) \tag{4.31}$$

Thus, from (4.29), the achievable sum secure rate in each block is $(n_1 + n_2)\frac{1}{2}\log P + o(\log P)$. Since our block contains n_B channel uses, the effective sum secure rate is

$$\sup(R_1 + R_2) \geq \left(\frac{n_1 + n_2}{n_B}\right)\frac{1}{2}\log P + o(\log P) \tag{4.32}$$

Thus, the achievable sum s.d.o.f. is $\frac{n_1+n_2}{n_B}$, with the stringent security requirement as well.

In the following subsections, we present the achievable scheme for each regime.

4.5.1 $K \leq N/2$

In this regime, the optimal sum s.d.o.f. is N. In our scheme, transmitter 1 sends $(N-K)$ independent Gaussian symbols $\mathbf{v}_1 \in \mathbb{R}^{N-K}$ while transmitter 2 sends K independent Gaussian symbols $\mathbf{v}_2 \in \mathbb{R}^{K}$, in one time slot. This can be done by beamforming the information streams at both transmitters to directions that are orthogonal to the eavesdropper's channel. To this end, the transmitted signals are:

$$\mathbf{X}_1 = \mathbf{P}_1 \mathbf{v}_1 \tag{4.33}$$

$$\mathbf{X}_2 = \mathbf{P}_2 \mathbf{v}_2 \tag{4.34}$$

where $\mathbf{P}_1 \in \mathbb{R}^{N \times (N-K)}$ is a matrix whose $(N-K)$ columns span the $(N-K)$ dimensional nullspace of $\mathbf{G}_1$, and $\mathbf{P}_2 \in \mathbb{R}^{N \times K}$ is a matrix with K linearly independent vectors drawn from the $(N-K)$ dimensional nullspace of $\mathbf{G}_2$. This can be done since $K \leq N-K$. The channel outputs are:

$$\mathbf{Y} =[\mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2] \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} + \mathbf{N}_1 \tag{4.35}$$

$$\mathbf{Z} =\mathbf{N}_2 \tag{4.36}$$

Note that $[\mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2]$ is an $N \times N$ matrix with full rank almost surely, and thus, both $\mathbf{v}_1$ and $\mathbf{v}_2$ can be decoded at the legitimate receiver to within noise variance. On the other hand, they do not appear in the eavesdropper's observation and thus their security is guaranteed.

4.5.2 $N/2 \leq K \leq N$

The optimal sum s.d.o.f. in this regime is $\frac{2}{3}(2N-K)$. Thus, transmitter i sends $(2N-K)$ Gaussian symbols $\left\{\mathbf{v}_i \in \mathbb{R}^{2K-N}, \tilde{\mathbf{v}}_i(t) \in \mathbb{R}^{N-K}, t=1,2,3\right\}$, each drawn independently from $\mathcal{N}(0,\bar{P})$, in 3 time slots for $i=1,2$, where $\bar{P}=\alpha P$ and α is chosen to satisfy the power constraint. Intuitively, transmitter i sends the $(N-K)$ symbols $\tilde{\mathbf{v}}_i(t)$ by beamforming orthogonal to the eavesdropper in each time slot $t=1,2,3$. The remaining $(2K-N)$ symbols are sent over 3 time slots using a scheme similar to the SISO scheme of [4]. Thus, the transmitted signals at time t are:

$$\mathbf{X}_1(t) = \mathbf{G}_1(t)^{\perp}\tilde{\mathbf{v}}_1(t) + \mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_1 \tag{4.37}$$

$$\mathbf{X}_2(t) = \mathbf{G}_2(t)^{\perp}\tilde{\mathbf{v}}_2(t) + \mathbf{P}_2(t)\mathbf{v}_2 + \mathbf{H}_2(t)^{-1}\mathbf{Q}(t)\mathbf{u}_2 \tag{4.38}$$

where $\mathbf{G}_i(t)^{\perp}$ is an $N \times (N-K)$ full rank matrix with $\mathbf{G}_i(t)\mathbf{G}_i(t)^{\perp} = \mathbf{0}_{N\times(N-K)}$, $\mathbf{u}_i$ is a $(2K-N)$ dimensional vector whose entries are drawn in an i.i.d. fashion from $\mathcal{N}(0,\bar{P})$, and $\mathbf{P}_i$ and $\mathbf{Q}$ are $N \times (2K-N)$ precoding matrices that will be fixed later. The channel outputs are:

$$\begin{aligned}\mathbf{Y}(t) =& \mathbf{H}_1(t)\mathbf{G}_1(t)^{\perp}\tilde{\mathbf{v}}_1(t) + \mathbf{H}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{H}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 \\ &+ \mathbf{H}_2(t)\mathbf{G}_2(t)^{\perp}\tilde{\mathbf{v}}_2(t) + \mathbf{Q}(t)(\mathbf{u}_1+\mathbf{u}_2) + \mathbf{N}_1(t) \end{aligned} \tag{4.39}$$

$$\mathbf{Z}(t) = \mathbf{G}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{G}_2(t)\mathbf{H}_2(t)^{-1}\mathbf{Q}(t)\mathbf{u}_2$$

$$+\mathbf{G}_2(t)\mathbf{P}_2(t)\mathbf{v}_2+\mathbf{G}_1(t)\mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_1+\mathbf{N}_2(t) \tag{4.40}$$

We now choose $\mathbf{Q}(t)$ to be any $N \times (2K-N)$ matrix with full column rank, and choose

$$\mathbf{P}_i(t)=\mathbf{G}_i(t)^T(\mathbf{G}_i(t)\mathbf{G}_i(t)^T)^{-1}(\mathbf{G}_j(t)\mathbf{H}_j(t)^{-1})\mathbf{Q}(t) \tag{4.41}$$

where $i,j \in \{1,2\}, i \neq j$. It can be verified that this selection aligns $\mathbf{v}_i$ with $\mathbf{u}_j$, $i \neq j$, at the eavesdropper, and this guarantees that the information leakage is $o(\log P)$. On the other hand, the legitimate receiver decodes the desired signals $\left\{\tilde{\mathbf{v}}_i(t) \in \mathbb{R}^{N-K}, t \in \{1,2,3\}\right\}$, $\left\{\mathbf{v}_i \in \mathbb{R}^{2K-N}, i=1,2\right\}$ and the aligned artificial noise symbols $\mathbf{u}_1+\mathbf{u}_2 \in \mathbb{R}^{2K-N}$, i.e., $6(N-K)+3(2N-K)=3N$ symbols using $3N$ observations in 3 time slots, to within noise variance. This completes the scheme for the regime $N/2 \leq K \leq N$.

4.5.3 $N \leq K \leq 4N/3$

In this regime, the optimal sum s.d.o.f. is $\frac{2}{3}N$. Therefore, transmitter i in our scheme sends N Gaussian symbols, $\mathbf{v}_i \in \mathbb{R}^N$, in 3 time slots. The transmitted signals in time slot t are given by

$$\mathbf{X}_1(t)=\mathbf{P}_1(t)\mathbf{v}_1+\mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_1 \tag{4.42}$$

$$\mathbf{X}_2(t)=\mathbf{P}_2(t)\mathbf{v}_2+\mathbf{H}_1(t)^{-1}\mathbf{Q}(t)\mathbf{u}_2 \tag{4.43}$$

where the $\mathbf{P}_1(t)$, $\mathbf{Q}(t)$, and $\mathbf{P}_2(t)$ are $N \times N$ precoding matrices to be designed. Let us define

$$\tilde{\mathbf{P}}_i \triangleq \begin{bmatrix} \mathbf{P}_i(1) \\ \mathbf{P}_i(2) \\ \mathbf{P}_i(3) \end{bmatrix}, \quad \tilde{\mathbf{Q}} \triangleq \begin{bmatrix} \mathbf{Q}(1) \\ \mathbf{Q}(2) \\ \mathbf{Q}(3) \end{bmatrix} \tag{4.44}$$

Further, if we define

$$\tilde{\mathbf{H}}_i \triangleq \begin{bmatrix} \mathbf{H}_i(1) & \mathbf{0}_{N\times N} & \mathbf{0}_{N\times N} \\ \mathbf{0}_{N\times N} & \mathbf{H}_i(2) & \mathbf{0}_{N\times N} \\ \mathbf{0}_{N\times N} & \mathbf{0}_{N\times N} & \mathbf{H}_i(3) \end{bmatrix} \tag{4.45}$$

and $\tilde{\mathbf{G}}_i$ similarly, we can compactly represent the channel outputs over all 3 time slots as

$$\tilde{\mathbf{Y}} = \tilde{\mathbf{H}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{H}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 + \tilde{\mathbf{Q}}(\mathbf{u}_1 + \mathbf{u}_2) + \tilde{\mathbf{N}}_1 \tag{4.46}$$

$$\tilde{\mathbf{Z}} = \tilde{\mathbf{G}}_1\tilde{\mathbf{P}}_1\mathbf{v}_1 + \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\tilde{\mathbf{Q}}\mathbf{u}_2 + \tilde{\mathbf{G}}_2\tilde{\mathbf{P}}_2\mathbf{v}_2 + \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\tilde{\mathbf{Q}}\mathbf{u}_1 + \tilde{\mathbf{N}}_2 \tag{4.47}$$

where $\tilde{\mathbf{N}}_i \triangleq [\mathbf{N}_i(1)^T \quad \mathbf{N}_i(2)^T \quad \mathbf{N}_i(3)^T]^T$, $\tilde{\mathbf{Y}} \triangleq [\mathbf{Y}(1)^T \quad \mathbf{Y}(2)^T \quad \mathbf{Y}(3)^T]^T$, and $\tilde{\mathbf{Z}}$ is defined similarly. To ensure secrecy, we impose the following conditions

$$\tilde{\mathbf{G}}_1\tilde{\mathbf{P}}_1 = \tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\tilde{\mathbf{Q}} \tag{4.48}$$

$$\tilde{\mathbf{G}}_2\tilde{\mathbf{P}}_2 = \tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\tilde{\mathbf{Q}} \tag{4.49}$$

We rewrite the conditions in (4.48)-(4.49) as

$$\mathbf{\Psi}\begin{bmatrix}\tilde{\mathbf{P}}_1\\ \tilde{\mathbf{P}}_2\\ \tilde{\mathbf{Q}}\end{bmatrix}=\mathbf{0}_{6K\times N} \tag{4.50}$$

where

$$\mathbf{\Psi}\triangleq\begin{bmatrix}\tilde{\mathbf{G}}_1 & \mathbf{0}_{3K\times 3N} & -\tilde{\mathbf{G}}_2\tilde{\mathbf{H}}_2^{-1}\\ \mathbf{0}_{3K\times 3N} & \tilde{\mathbf{G}}_2 & -\tilde{\mathbf{G}}_1\tilde{\mathbf{H}}_1^{-1}\end{bmatrix} \tag{4.51}$$

Note that $\mathbf{\Psi}$ has a nullity $9N-6K$. Since $9N-6K\geq N$ in this regime, we can choose N vectors of dimension $9N$ randomly such that they are linearly independent and lie in the nullspace of $\mathbf{\Psi}$. We can then assign to $\tilde{\mathbf{P}}_1$, $\tilde{\mathbf{P}}_2$ and $\tilde{\mathbf{Q}}$, the top, the middle and the bottom $3N$ rows of the matrix comprising the N chosen vectors. This guarantees secrecy of the message symbols at the eavesdropper.

To see the decodability, we rewrite the received signal at the legitimate receiver as

$$\tilde{\mathbf{Y}}=\mathbf{\Phi}\begin{bmatrix}\mathbf{v}_1\\ \mathbf{v}_2\\ \mathbf{u}_1+\mathbf{u}_2\end{bmatrix}+\tilde{\mathbf{N}}_1 \tag{4.52}$$

where $\mathbf{\Phi}\triangleq[\tilde{\mathbf{H}}_1\tilde{\mathbf{P}}_1 \quad \tilde{\mathbf{H}}_2\tilde{\mathbf{P}}_2 \quad \tilde{\mathbf{Q}}]$. We note that $\mathbf{\Phi}$ is $3N\times 3N$ and full rank almost surely; thus, the desired signals $\mathbf{v}_1$ and $\mathbf{v}_2$ can be decoded at the legitimate receiver within noise distortion at high SNR.

4.5.4 $4N/3 \leq K \leq 3N/2$

The optimal s.d.o.f. in this regime is $2N-K$. To achieve this s.d.o.f., the first transmitter sends $K-N$ Gaussian symbols $\left\{\mathbf{v}_1 \in \mathbb{R}^{3N-2K}, \tilde{\mathbf{v}} \in \mathbb{R}^{3K-4N}\right\}$, while the second transmitter sends $3N-2K$ Gaussian symbols $\left\{\mathbf{v}_2 \in \mathbb{R}^{3N-2K}\right\}$, in one time slot. The scheme is as follows. The transmitted signals are

$$\mathbf{X}_1 = \mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 \tag{4.53}$$

$$\mathbf{X}_2 = \mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 \tag{4.54}$$

where $\tilde{\mathbf{u}} \in \mathbb{R}^{3K-4N}$ and $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{R}^{3N-2K}$ are artificial noise vectors, whose entries are drawn in an i.i.d. fashion from $\mathcal{N}(0, \bar{P})$. The precoding matrices $\mathbf{R}_i \in \mathbb{R}^{N\times(3K-4N)}$, and $\mathbf{P}_i, \mathbf{Q}_i \in \mathbb{R}^{N\times(3N-2K)}$ will be chosen later. The channel outputs are

$$\mathbf{Y} =\mathbf{H}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2\mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1 \tag{4.55}$$

$$\mathbf{Z} =\mathbf{G}_1\mathbf{R}_1\tilde{\mathbf{v}} + \mathbf{G}_2\mathbf{R}_2\tilde{\mathbf{u}} + \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 + \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 + \mathbf{N}_2 \tag{4.56}$$

To ensure secrecy, we want to impose the following conditions:

$$\mathbf{G}_1\mathbf{R}_1 =\mathbf{G}_2\mathbf{R}_2 \tag{4.57}$$

$$\mathbf{G}_1\mathbf{P}_1 =\mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q} \tag{4.58}$$

$$\mathbf{G}_2\mathbf{P}_2 = \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q} \tag{4.59}$$

To satisfy (4.57), we choose $\mathbf{R}_1$ and $\mathbf{R}_2$ to be the first and the last N rows of a $2N \times 3K - 4N$ matrix whose columns consist of any $3K - 4N$ linearly independent vectors drawn randomly from the nullspace of $[\mathbf{G}_1 \quad -\mathbf{G}_2]$. This is possible since, $3K - 4N \leq 2N - K$ in this regime. To satisfy (4.58)-(4.59), we let $\mathbf{P}_1$, $\mathbf{P}_2$ and $\mathbf{Q}$ to be the first, the second and the last N rows of a $3N \times (3N - 2K)$ matrix whose columns are randomly chosen to span the $(3N - 2K)$ dimensional nullspace of the matrix $\mathbf{\Lambda}$ given by

$$\mathbf{\Lambda} \triangleq \begin{bmatrix} \mathbf{G}_1 & \mathbf{0}_{K\times N} & -\mathbf{G}_2\mathbf{H}_2^{-1} \\ \mathbf{0}_{K\times N} & \mathbf{G}_2 & -\mathbf{G}_1\mathbf{H}_1^{-1} \end{bmatrix} \tag{4.60}$$

To see the decodablity, we can rewrite the observation at the legitimate receiver as

$$\mathbf{Y} = \mathbf{\Phi} \begin{bmatrix} \tilde{\mathbf{v}} \\ \mathbf{v}_1 \\ \mathbf{v}_2 \\ \tilde{\mathbf{u}} \\ \mathbf{u}_1 + \mathbf{u}_2 \end{bmatrix} + \mathbf{N}_1 \tag{4.61}$$

where $\mathbf{\Phi}$ is the $N \times N$ matrix defined as

$$\mathbf{\Phi} = [\mathbf{H}_1\mathbf{R}_1 \quad \mathbf{H}_1\mathbf{P}_1 \quad \mathbf{H}_2\mathbf{P}_2 \quad \mathbf{H}_2\mathbf{R}_2 \quad \mathbf{Q}] \tag{4.62}$$

Since $\mathbf{\Phi}$ is full rank almost surely, the legitimate receiver can decode its desired symbols $\tilde{\mathbf{v}}, \mathbf{v}_1$, and $\mathbf{v}_2$.

4.5.5 $3N/2 \leq K \leq 2N$

In this regime, it is clear from Fig. 4.2 that the multiple access wiretap channel has the same optimal sum s.d.o.f. as the optimal s.d.o.f. of the wiretap channel with one helper. Thus, an optimal achievable scheme for the wiretap channel with one helper suffices as the scheme for the multiple access wiretap channel as well. Such an optimal scheme, based on real interference alignment, is provided in [12] for the wiretap channel with one helper with fixed channel gains. Here, we provide a scheme based on vector space alignment.

In order to achieve the optimal sum s.d.o.f. of $2N - K$ in this regime, the first transmitter sends $2N-K$ independent Gaussian symbols $\mathbf{v} \in \mathbb{R}^{2N-K}$ securely, in one time slot. The second transmitter just transmits artificial noise symbols $\mathbf{u} \in \mathbb{R}^{2N-K}$, whose entries are drawn in an i.i.d. fashion from $\mathcal{N}(0, \bar{P})$. The transmitted signals are

$$\mathbf{X}_1 = \mathbf{P}\mathbf{v} \tag{4.63}$$

$$\mathbf{X}_2 = \mathbf{Q}\mathbf{u} \tag{4.64}$$

where $\mathbf{P}$ and $\mathbf{Q}$ are $N \times (2N-K)$ precoding matrices to be fixed later. The received signals are

$$\mathbf{Y} = \mathbf{H}_1\mathbf{P}\mathbf{v} + \mathbf{H}_2\mathbf{Q}\mathbf{u} + \mathbf{N}_1 \tag{4.65}$$

$$\mathbf{Z} = \mathbf{G}_1\mathbf{P}\mathbf{v} + \mathbf{G}_2\mathbf{Q}\mathbf{u} + \mathbf{N}_2 \tag{4.66}$$

To ensure security, we wish to ensure that

$$\mathbf{G}_1\mathbf{P} = \mathbf{G}_2\mathbf{Q} \tag{4.67}$$

This can be done by choosing $\mathbf{P}$ and $\mathbf{Q}$ to be the top and the bottom N rows of a $2N \times (2N-K)$ matrix whose linearly independent columns are drawn randomly from the nullspace of $[\mathbf{G}_1 \quad -\mathbf{G}_2]$. The decodability is ensured by noting that the matrix $[\mathbf{H}_1\mathbf{P} \quad \mathbf{H}_2\mathbf{Q}]$ is full column rank and $2(2N-K) \leq N$ in this regime.

4.6 Achievable Schemes for Fixed Channel Gains

We note that the achievable schemes proposed for the fading channel gains in the regimes $K \leq \frac{N}{2}$ and $\frac{4N}{2} \leq K \leq 2N$ are single time-slot schemes and suffice for the fixed channel gains case. However, in the regime $\frac{N}{2} \leq K \leq \frac{4N}{3}$, the schemes for the fading channel gains exploit the diversity of channel gains over three time slots; thus, these schemes cannot be used in the fixed channel gains case. Therefore, we now propose new achievable schemes for this regime. In this regime, the optimal sum s.d.o.f. is of the form $2\left(d + \frac{l}{3}\right)$, $l = 0, 1, 2$, where d is an integer. When $l = 0$, the sum s.d.o.f. is an integer and carefully precoded Gaussian signaling suffices. However, when $l \neq 0$, the s.d.o.f. has a fractional part, and Gaussian signaling alone is not optimal, since Gaussian signals with full power cannot carry fractional d.o.f. of information.

The general structure of our schemes is as follows: We decompose the channel input at each transmitter into two parts: a Gaussian signaling part carrying d (the integer part) d.o.f. of information securely, and a structured signaling part carrying $\frac{l}{3}$ (the fractional part) d.o.f. of information securely. The structure of the Gaussian signals carrying the integer s.d.o.f. d are the same as that of the corresponding schemes for the fading channel gains. This ensures security at the eavesdropper as well as decodability at the legitimate receiver as long as the structured signals carrying the fractional s.d.o.f. $\frac{2l}{3}$ from both transmitters can be decoded at the legitimate receiver. The design of the structured signals is motivated from the SISO scheme of [4]. In fact, when $l = 1$, we use the signal structure of the scheme in [4], where real interference alignment is used to transmit $\frac{2}{3}$ sum s.d.o.f. on the SISO multiple access wiretap channel. However, when $l = 2$, a new scheme is required to achieve $\frac{4}{3}$ sum s.d.o.f. on the MIMO multiple access wiretap channel with two antennas at every terminal. To that end, we first provide a novel scheme, based on asymptotic real interference alignment [7,9], for the canonical $2 \times 2 \times 2 \times 2$ MIMO multiple access wiretap channel.

4.6.1 Scheme for the $2 \times 2 \times 2 \times 2$ System

The optimal sum s.d.o.f. is $\frac{4}{3}$. Since the legitimate receiver has 2 antennas, we achieve $\frac{2}{3}$ s.d.o.f. on each antenna. The scheme is as follows.

Let m be a large integer. Define $M \overset{\Delta}{=} m^{\Gamma}$, where Γ will be specified later. The channel inputs are given by

$$\mathbf{X}_1 = \mathbf{G}_1^{-1}\mathbf{G}_2\mathbf{H}_2^{-1} \begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{11} \\ \\ \mathbf{t}_2\mathbf{v}_{12} \end{pmatrix} + \mathbf{H}_1^{-1} \begin{pmatrix} \mathbf{t}_1^T\mathbf{u}_{11} \\ \\ \mathbf{t}_2\mathbf{u}_{12} \end{pmatrix} \tag{4.68}$$

$$\mathbf{X}_2 = \mathbf{G}_2^{-1}\mathbf{G}_1\mathbf{H}_1^{-1} \begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{21} \\ \\ \mathbf{t}_2\mathbf{v}_{22} \end{pmatrix} + \mathbf{H}_2^{-1} \begin{pmatrix} \mathbf{t}_1^T\mathbf{u}_{21} \\ \\ \mathbf{t}_2\mathbf{u}_{22} \end{pmatrix} \tag{4.69}$$

where $\mathbf{t}_i, i = 1, 2$ are M dimensional precoding vectors which will be fixed later, and $\mathbf{u}_{ij}, \mathbf{v}_{ij}$ are independent random variables drawn uniformly from the same PAM constellation $C(a, Q)$ given by

$$C(a, Q) = a\{-Q, -Q + 1, \ldots, Q - 1, Q\} \tag{4.70}$$

where Q is a positive integer and a is a real number used to normalize the transmission power. The exact values of a and Q will be specified later. The variables $\mathbf{v}_{ij}$ denote the information symbols of transmitter i, while $\mathbf{u}_{ij}$ are the cooperative jamming signals being transmitted from transmitter i.

The channel outputs are given by

$$\mathbf{Y} =\mathbf{A}\begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{11} \\ \\ \mathbf{t}_2\mathbf{v}_{12} \end{pmatrix} + \mathbf{B}\begin{pmatrix} \mathbf{t}_1^T\mathbf{v}_{21} \\ \\ \mathbf{t}_2\mathbf{v}_{22} \end{pmatrix} + \begin{pmatrix} \mathbf{t}_1^T(\mathbf{u}_{11}+\mathbf{u}_{21}) \\ \\ \mathbf{t}_2(\mathbf{u}_{12}+\mathbf{u}_{22}) \end{pmatrix} + \mathbf{N}_1 \tag{4.71}$$

$$\mathbf{Z} =\mathbf{G}_1\mathbf{H}_1^{-1}\begin{pmatrix} \mathbf{t}_1^T(\mathbf{u}_{11}+\mathbf{v}_{21}) \\ \\ \mathbf{t}_2(\mathbf{u}_{12}+\mathbf{v}_{22}) \end{pmatrix} + \mathbf{G}_2\mathbf{H}_2^{-1}\begin{pmatrix} \mathbf{t}_1^T(\mathbf{u}_{21}+\mathbf{v}_{11}) \\ \\ \mathbf{t}_2(\mathbf{u}_{22}+\mathbf{v}_{12}) \end{pmatrix} + \mathbf{N}_2 \tag{4.72}$$

where $\mathbf{A} = \mathbf{H}_1\mathbf{G}_1^{-1}\mathbf{G}_2\mathbf{H}_2^{-1}$ and $\mathbf{B} = \mathbf{H}_2\mathbf{G}_2^{-1}\mathbf{G}_1\mathbf{H}_1^{-1}$. Note that the information symbols $\mathbf{v}_{ij}$ are buried in the cooperative jamming signals $\mathbf{u}_{kj}$, where $k \neq i$, at the eavesdropper. Intuitively, this ensures security of the information symbols at the eavesdropper. At the legitimate receiver, we can express the received signal $\mathbf{Y}$ more explicitly as

$$\begin{pmatrix} \mathbf{t}_2^T(a_{12}\mathbf{v}_{12}+b_{12}\mathbf{v}_{22}) + \mathbf{t}_1^T(a_{11}\mathbf{v}_{11}+b_{11}\mathbf{v}_{21}+\mathbf{u}_{11}+\mathbf{u}_{21}) \\ \\ \mathbf{t}_1^T(a_{21}\mathbf{v}_{11}+b_{21}\mathbf{v}_{21}) + \mathbf{t}_2^T(a_{22}\mathbf{v}_{12}+b_{22}\mathbf{v}_{22}+\mathbf{u}_{12}+\mathbf{u}_{22}) \end{pmatrix} \tag{4.73}$$

We define

$$T_1 = \{a_{11}^{r_1}b_{11}^{r_2}, r_i \in \{0,\dots,m-1\}\} \tag{4.74}$$

$$T_2 = \{a_{22}^{r_1}b_{22}^{r_2}, r_i \in \{0,\dots,m-1\}\} \tag{4.75}$$

Letting $\Gamma = 2$, we note that

$$|T_1| = |T_2| = M \tag{4.76}$$

We choose $\mathbf{t}_i$ to be the M dimensional vector that has all the elements of T_i. We note that all elements in T_i are rationally independent, since the channel gains are drawn independently from a continuous distribution. Also, the elements of T_i can be verified to be rationally independent of the elements of T_j, if $i \neq j$. With the above selections, let us analyze the structure of the received signal at the legitimate receiver.

At the first antenna, $\mathbf{u}_{11}$ and $\mathbf{u}_{21}$ arrive along the dimensions of T_1. The signals $\mathbf{v}_{11}$ and $\mathbf{v}_{21}$ arrive along dimensions $a_{11}T_1$ and $b_{11}T_1$ and, thus, they align with $\mathbf{u}_{11}$ and $\mathbf{u}_{21}$ in $\tilde{T}_1$, where,

$$\tilde{T}_1 = \{a_{11}^{r_1} b_{11}^{r_2}, r_i \in \{0, \dots, m\}\} \tag{4.77}$$

Thus, $\mathbf{v}_{11}$ and $\mathbf{v}_{21}$ cannot be reliably decoded from the observation of the first antenna. However, the desired signals $\mathbf{v}_{12}$ and $\mathbf{v}_{22}$ arrive along dimensions $a_{12}T_2$ and $b_{12}T_2$, respectively. Note that the elements of $a_{12}T_2$ and $b_{12}T_2$ are rationally independent and thus, $\mathbf{v}_{12}$ and $\mathbf{v}_{22}$ occupy separate rational dimensions. Also they are separate from the interference space $\tilde{T}_1$. Therefore, $\mathbf{v}_{12}$ and $\mathbf{v}_{22}$ can be reliably decoded at high SNR. Heuristically, the s.d.o.f. achieved using the first antenna is $\frac{2|T_1|}{2|T_1|+|\tilde{T}_2|} = \frac{2m^2}{2m^2+(m+1)^2} \approx \frac{2}{3}$ for large enough m.

At the second antenna, a similar analysis holds. The signals $\mathbf{v}_{12}$, $\mathbf{v}_{22}$, $\mathbf{u}_{12}$ and $\mathbf{u}_{22}$ align with each other in the dimensions of $\tilde{T}_2$, which is defined as

$$\tilde{T}_2 = \{a_{22}^{r_1} b_{22}^{r_2}, r_i \in \{0, \dots, m\}\} \tag{4.78}$$

The signals $\mathbf{v}_{11}$ and $\mathbf{v}_{21}$ arrive along dimensions that are separate from each other as well as from the dimensions in $\tilde{T}_2$, and thus, can be decoded reliably. The s.d.o.f. achieved in the second antenna is also $\frac{2m^2}{2m^2+(m+1)^2} \approx \frac{2}{3}$ for large m. Therefore, the sum s.d.o.f. achieved using both antennas is $\frac{4}{3}$, as desired.

Formally, an achievable sum rate is given in equation (4.29), where $\mathbf{V} \triangleq \{\mathbf{v}_{ij}, i, j \in \{1,2\}\}$. In order to bound the term $I(\mathbf{V};\mathbf{Y})$, we first bound the probability of error. Let $M_S \triangleq 2m^2 + (m+1)^2$ be the number of rational dimensions at each receiver antenna. Also let $\mathbf{V}_i = \{\mathbf{v}_{kj}, k = 1,2; j \neq i\}$ be the desired symbols at the ith antenna of the receiver. In order to decode, the receiver makes an estimate $\hat{V}_i$ of $\mathbf{V}_i$ by choosing the closest point in the constellation based on the signal received at antenna i. For any $\delta > 0$, there exists a positive constant γ, which is independent of P, such that if we choose $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, then for almost all channel gains the average power constraint is satisfied and the probability of error, $\Pr(\mathbf{V}_i \neq \hat{\mathbf{V}}_i)$, is upper-bounded by $\exp\left(-\eta_\gamma P^\delta\right)$, where η_γ is a positive constant which is independent of P. Since $\mathbf{V} = \{\mathbf{V}_i, i = 1,2\}$,

$$\Pr(\mathbf{V} \neq \hat{\mathbf{V}}) \leq 2\exp\left(-\eta_\gamma P^\delta\right) \tag{4.79}$$

By Fano's inequality and the Markov chain $\mathbf{V} \to \mathbf{Y} \to \hat{\mathbf{V}}$,

$$\begin{aligned} I(\mathbf{V};\mathbf{Y}) &= H(\mathbf{V}) - H(\mathbf{V}|\hat{\mathbf{V}}) && (4.80)\\ &\geq \log(|\mathcal{V}|) - 1 - \Pr(\mathbf{V} \neq \hat{\mathbf{V}})\log(|\mathcal{V}|) && (4.81)\\ &= \log(|\mathcal{V}|) - o(\log P) && (4.82) \end{aligned}$$

$$=\frac{4M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right)+o(\log P) \tag{4.83}$$

where $\mathcal{V}$ is the alphabet of $\mathbf{V}$ with cardinality $(2Q+1)^{4M}=(2Q+1)^{4m^2}$. Next, we compute

$$\begin{aligned} I(\mathbf{V};\mathbf{Z}) \leq & I\left(\{\mathbf{v}_{ij}, i,j=1,2\}; \left\{\mathbf{v}_{ij}+\mathbf{u}_{\hat{i}j}, \begin{matrix} \hat{i}\neq i, \\ i,j=1,2 \end{matrix}\right\}\right) && (4.84) \\ \leq & \sum_{i,j=1,\hat{i}\neq i}^{2} H(\mathbf{v}_{ij}+\mathbf{u}_{\hat{i}j})-H(\mathbf{u}_{\hat{i}j}) && (4.85) \\ \leq & 4M\log(4Q+1)-4M\log(2Q+1) && (4.86) \\ \leq & 4M=o(\log P) && (4.87) \end{aligned}$$

Using (4.83) and (4.87) in (4.29), we have

$$\sup(R_1+R_2) \geq \frac{4M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right)+o(\log P) \tag{4.88}$$

By choosing δ small enough and m large enough, we can make the sum s.d.o.f. arbitrarily close to $\frac{4}{3}$.

4.6.2 Achievable Schemes for $\frac{N}{2}\leq K\leq N$

We use structured PAM signaling along with Gaussian signaling. Let $d=\lfloor\frac{2K-N}{3}\rfloor$, and $l=(2K-N)\text{mod } 3=(2N-K)\text{mod } 3$. Let $\mathbf{v}_i^{(1)}=\{v_{ij}, j=1,\ldots,d\}$, where each $v_{ij}, j=1,\ldots,d$ is drawn in an i.i.d. fashion $\sim\mathcal{N}(0,\alpha P)$, and $\mathbf{v}_i^{(2)}=$

$\left\{v_{i(d+1)}, \ldots, v_{i(d+l)}\right\}$ are structured PAM signals to be specified later. When $l = 0$, $\mathbf{v}_i^{(2)}$ is the empty set. Let $\mathbf{v}_i = \left(\mathbf{v}_i^{(1)}, \mathbf{v}_i^{(2)}\right)$. Also, let $\tilde{\mathbf{v}}_i = \{\tilde{v}_{ij}, j = 1, \ldots, N - K\}$ denote the symbols that can be transmitted securely by beamforming orthogonal to the eavesdropper channel. Transmitter i sends:

$$\mathbf{X}_i = \mathbf{G}_i^{\perp}\tilde{\mathbf{v}}_i + \mathbf{P}_i\mathbf{v}_i + \mathbf{H}_i^{-1}\mathbf{Q}\mathbf{u}_i \tag{4.89}$$

where $\mathbf{G}_i^{\perp}$ is an $N \times (N - K)$ full rank matrix with $\mathbf{G}_i\mathbf{G}_i^{\perp} = \mathbf{0}_{N\times(N-K)}$, $\mathbf{u}_i = \left(\mathbf{u}_i^{(1)}, \mathbf{u}_i^{(2)}\right)$ is a $(d+l)$ dimensional vector with the entries of $\mathbf{u}_i^{(1)} = \{u_{ij}, j = 1, \ldots, d\}$ being drawn independently of $\mathbf{v}$ and each other from $\mathcal{N}(0, \alpha P)$, and the structure of $\mathbf{u}_i^{(2)} = \left\{u_{i(d+1)}, \ldots, u_{i(d+l)}\right\}$ will be specified later. $\mathbf{P}_i$ and $\mathbf{Q}$ are $N \times (d + l)$ precoding matrices that will also be fixed later. The received signals are:

$$\mathbf{Y} = \mathbf{H}_1\mathbf{G}_1^{\perp}\tilde{\mathbf{v}}_1 + \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{H}_2\mathbf{G}_2^{\perp}\tilde{\mathbf{v}}_2 + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1 \tag{4.90}$$

$$\mathbf{Z} = \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 + \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 + \mathbf{N}_2 \tag{4.91}$$

We now choose $\mathbf{Q}$ to be any $N \times (d + l)$ matrix with full column rank, and choose $\mathbf{P}_i = \mathbf{G}_i^T(\mathbf{G}_i\mathbf{G}_i^T)^{-1}(\mathbf{G}_j\mathbf{H}_j^{-1})\mathbf{Q}$, where $i, j \in \{1, 2\}, i \neq j$. It can be verified that this selection aligns $\mathbf{v}_i$ with $\mathbf{u}_j$, $i \neq j$, at the eavesdropper, and this guarantees that the information leakage is $o(\log P)$. Next, let $\mathbf{P}_i^{(1)}$, $\mathbf{Q}^{(1)}$ be matrices containing the first d columns of $\mathbf{P}_i$ and $\mathbf{Q}$, respectively, while $\mathbf{P}_i^{(2)}$ and $\mathbf{Q}^{(2)}$ contain the last l columns of $\mathbf{P}_i$ and $\mathbf{Q}$, respectively. Let $\mathbf{B}$ be a matrix whose columns lie in the nullspace of the matrix $\mathbf{F}^T = [\mathbf{H}_1\mathbf{G}_1^{\perp} \quad \mathbf{H}_2\mathbf{G}_2^{\perp} \quad \mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{Q}^{(1)}]^T$. Note that $\mathbf{F}$ is a

$(N-l) \times N$ matrix and thus there exists a $N \times l$ matrix $\mathbf{B}$ such that $\mathbf{FB} = \mathbf{0}$. We consider the filtered output $[\tilde{\mathbf{Y}}, \hat{\mathbf{Y}}]^T = \mathbf{EY}$, where

$$\mathbf{E} = \begin{pmatrix} \mathbf{D}_{l \times N} \\ \mathbf{I}_{N-l} \quad \mathbf{0}_{(N-l) \times l} \end{pmatrix} \tag{4.92}$$

and $\mathbf{D} = (\mathbf{B}^T \mathbf{Q}^{(2)})^{-1} \mathbf{B}^T$ and let

$$\tilde{\mathbf{Y}} = \mathbf{D}\mathbf{H}_1 \mathbf{P}_1^{(2)} \mathbf{v}_1^{(2)} + \mathbf{D}\mathbf{H}_2 \mathbf{P}_2^{(2)} \mathbf{v}_2^{(2)} + (\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}) + \mathbf{D}\mathbf{N}_1 \tag{4.93}$$

Note that (4.93) represents the output at the receiver of a multiple access wiretap channel with l antennas at each terminal. If $l = 1$, we let $\mathbf{v}_i^{(2)} = v_{i(d+1)}$ be drawn uniformly and independently from the PAM constellation $C(a, Q)$, with $Q = P^{\frac{1-\delta}{2(3+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$. Also, $\mathbf{u}_i^{(2)} = u_{i(d+1)}$ is chosen uniformly from $C(a, Q)$ and independently from $\mathbf{v}_j, j = 1, 2$. The receiver can then decode $v_{1(d+1)}$, $v_{2(d+1)}$ and $(u_{1(d+1)} + u_{2(d+1)})$ with vanishing probability of error. On the other hand, if $l = 2$, we choose $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_i^{(2)}$ as in the $2 \times 2 \times 2 \times 2$ multiple access wiretap channel, i.e., $v_{i(d+k)} = \mathbf{t}_k^T \hat{\mathbf{v}}_{ik}, k = 1, 2$, where $\hat{\mathbf{v}}_{ik}$ is an M dimensional vector whose entries are drawn from the PAM constellation $C(a, Q)$ with $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, and $\mathbf{t}_i$ is chosen appropriately analogous to the selection for the $2 \times 2 \times 2 \times 2$ multiple access wiretap channel, noting the similarity of (4.93) with (4.71). The cooperative jamming signal $\mathbf{u}_i^{(2)}$ is chosen similarly. Then, the receiver can decode $\mathbf{v}_i^{(2)}$ and also $\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}$ with vanishing probability of error.

Thus, for $l = 1, 2$, $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}$ can be eliminated from $\hat{\mathbf{Y}}$. Noting that

$2(N-K)+3d \leq N-l$, $\tilde{\mathbf{v}}_i$ and $\mathbf{v}_i^{(1)}$ can also be decoded from $\tilde{\mathbf{Y}}$. We compute

$$I(\mathbf{v}_1, \mathbf{v}_2, \tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2; \mathbf{Y}) = I(\mathbf{v}_1^{(1)}, \mathbf{v}_2^{(1)}, \tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2; \mathbf{Y}|\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}) + I(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}; \mathbf{Y}) \tag{4.94}$$

The second term depends on the value of l. When $l=1$,

$$\begin{aligned} I(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}; \mathbf{Y}) =& \log(2Q+1)^2 + o(\log P) & (4.95)\\ =& 2\frac{1-\delta}{(3+\delta)}\left(\frac{1}{2}\log P\right) + o(\log P) & (4.96)\end{aligned}$$

On the other hand, when $l=2$, we have

$$I(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}; \mathbf{Y}) = \frac{4M(1-\delta)}{M_S+\delta}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.97}$$

Thus, in either case, by choosing δ sufficiently small and m large enough when $l=2$, we have

$$I(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}; \mathbf{Y}) = \frac{2l}{3}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.98}$$

Noting that $\mathbf{v}_1^{(1)}, \mathbf{v}_2^{(1)}, \tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2$ can be decoded to within noise variance from $\mathbf{Y}$, given $\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}$, the first term of (4.94) is

$$I(\mathbf{v}_1^{(1)}, \mathbf{v}_2^{(1)}, \tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2; \mathbf{Y}|\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}) \geq 2(d+N-K)\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.99}$$

Using (4.98) and (4.99) in (4.94), we have,

$$I(\mathbf{v}_1, \mathbf{v}_2, \tilde{\mathbf{v}}_1, \tilde{\mathbf{v}}_2; \mathbf{Y}) \geq 2\left(d + N - K + \frac{l}{3}\right)\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.100}$$

$$= \frac{2}{3}\left(2N - K\right)\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.101}$$

This completes the achievable schemes for the regime $\frac{N}{2} \leq K \leq N$.

4.6.3 Achievable Schemes for $N \leq K \leq \frac{4N}{3}$

As in the previous regime, we use structured PAM signaling along with Gaussian signaling. Let $d = \lfloor \frac{N}{3} \rfloor$ and $l = N \text{mod } 3$. Let $\mathbf{v}_i = \left(\mathbf{v}_i^{(1)}, \mathbf{v}_i^{(2)}\right)$ be the information symbols such that the entries of $\mathbf{v}_i^{(1)} = \{v_{ij}, j = 1, \ldots, d\}$ are drawn in an i.i.d. fashion $\sim \mathcal{N}(0, \alpha P)$, and the entries of $\mathbf{v}_i^{(2)} = \{v_{ij}, j = d+1, \ldots, d+l\}$ are structured PAM signals to be designed later. Let $\mathbf{u}_i = \left(\mathbf{u}_i^{(1)}, \mathbf{u}_i^{(2)}\right)$ denote the cooperative jamming symbols such that the entries of $\mathbf{u}_i^{(1)} = \{u_{ij}, j = 1, \ldots, d\}$ are drawn in an i.i.d. fashion $\sim \mathcal{N}(0, \alpha P)$, and the entries of $\mathbf{u}_i^{(2)} = \{u_{ij}, j = d+1, \ldots, d+l\}$ are structured PAM signals independent of $\mathbf{v}_j, j = 1, 2$ and $\mathbf{u}_j, j \neq i$. Transmitter i sends

$$\mathbf{X}_i = \mathbf{P}_i \mathbf{v}_i + \mathbf{H}_i^{-1}\mathbf{Q}\mathbf{u}_i \tag{4.102}$$

where the $\mathbf{P}_1$, $\mathbf{Q}$, and $\mathbf{P}_2$ are $N \times (d+l)$ precoding matrices to be designed. The channel outputs are given by

$$\mathbf{Y} = \mathbf{H}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{H}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{Q}(\mathbf{u}_1 + \mathbf{u}_2) + \mathbf{N}_1 \tag{4.103}$$

$$\mathbf{Z} = \mathbf{G}_1\mathbf{P}_1\mathbf{v}_1 + \mathbf{G}_2\mathbf{H}_2^{-1}\mathbf{Q}\mathbf{u}_2 + \mathbf{G}_2\mathbf{P}_2\mathbf{v}_2 + \mathbf{G}_1\mathbf{H}_1^{-1}\mathbf{Q}\mathbf{u}_1 + \mathbf{N}_2 \tag{4.104}$$

To ensure secrecy, we impose that for $i \neq j$

$$\mathbf{G}_i\mathbf{P}_i = \mathbf{G}_j\mathbf{H}_j^{-1}\mathbf{Q} \tag{4.105}$$

We rewrite the conditions in (4.105) as

$$\mathbf{\Psi}\begin{bmatrix} \mathbf{P}_1^T & \mathbf{P}_2^T & \mathbf{Q}^T \end{bmatrix}^T = \mathbf{0}_{2K\times(d+l)} \tag{4.106}$$

where

$$\mathbf{\Psi} \triangleq \begin{bmatrix} \mathbf{G}_1 & \mathbf{0}_{K\times N} & -\mathbf{G}_2\mathbf{H}_2^{-1} \\ \mathbf{0}_{K\times N} & \mathbf{G}_2 & -\mathbf{G}_1\mathbf{H}_1^{-1} \end{bmatrix} \tag{4.107}$$

Note that $\mathbf{\Psi}$ has a nullity $3N-2K$. This alignment is feasible if $3N-2K \geq d+l$, i.e., if $K \leq 4d+l$. This is satisfied since, in this regime, $K \leq 4d+l+\frac{1}{3}l$, which implies $K \leq 4d+1$ for integers N and K, since $0 \leq l \leq 2$. This guarantees security and the information leakage is $o(\log P)$. Next, let $\mathbf{P} = \left(\mathbf{P}_i^{(1)}, \mathbf{P}_i^{(2)}\right)$ such that $\mathbf{P}_i^{(1)}$, contains the first d columns of $\mathbf{P}_i$. We define $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ similarly. Let $\mathbf{B}$ be a matrix whose columns lie in the nullspace of the matrix $\mathbf{F}^T = [\mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{H}_1\mathbf{P}_1^{(1)} \quad \mathbf{Q}^{(1)}]^T$. Note that $\mathbf{F}$ is a $(N-l) \times N$ matrix and thus there exists a non-zero $N \times l$ matrix $\mathbf{B}$ such that $\mathbf{FB} = \mathbf{0}$. We consider the filtered output $[\tilde{\mathbf{Y}}, \hat{\mathbf{Y}}]^T = \mathbf{EY}$, where $\mathbf{E}$ is as in (4.92). We have

$$\tilde{\mathbf{Y}} = \mathbf{DH}_1\mathbf{P}_1^{(2)}\mathbf{v}_1^{(2)} + \mathbf{DH}_2\mathbf{P}_2^{(2)}\mathbf{v}_2^{(2)} + (\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}) + \mathbf{DN}_1 \tag{4.108}$$

When $l = 1$, we choose $\mathbf{v}_i^{(2)} = v_{i(d+1)}$ and $\mathbf{u}_i^{(2)} = u_{i(d+1)}$ to be PAM signals drawn independently from $C(a, Q)$ with $Q = P^{\frac{1-\delta}{2(3+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$. The receiver can then decode $v_{1(d+1)}$, $v_{2(d+1)}$ and $(u_{1(d+1)} + u_{2(d+1)})$ with vanishing probability of error. When $l = 2$, we choose $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_i^{(2)}$ analogous to the case of the $2 \times 2 \times 2 \times 2$ multiple access wiretap channel, i.e., $v_{i(d+k)} = \mathbf{t}_k^T\hat{\mathbf{v}}_{ik}, k = 1, 2$, where $\hat{\mathbf{v}}_{ik}$ is an M dimensional vector whose entries are drawn from the PAM constellation $C(a, Q)$ with $Q = P^{\frac{1-\delta}{2(M_S+\delta)}}$ and $a = \frac{\gamma P^{\frac{1}{2}}}{Q}$, and $\mathbf{t}_i$ is chosen appropriately, noting the similarity of (4.108) with (4.71). The cooperative jamming signals $\mathbf{u}_i^{(2)}, i = 1, 2$ are chosen similarly. Such a selection allows the receiver to decode $\mathbf{v}_i^{(2)}$ and also $\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}$ with vanishing probability of error. Thus, they can be eliminated from the received observation $\mathbf{Y}$.

Thus, we can eliminate $\mathbf{v}_i^{(2)}$ and $\mathbf{u}_1^{(2)} + \mathbf{u}_2^{(2)}$ from $\hat{\mathbf{Y}}$. Noting that $3d \leq N - l$, $\mathbf{v}_i^{(1)} = \{v_{ij}, j = 1, \ldots, d\}$ can also be decoded to within noise variance from $\mathbf{Y}$. As in (4.96)-(4.97),

$$I(\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}; \mathbf{Y}) = \frac{2l}{3}\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.109}$$

Also, as in (4.99), we have

$$I(\mathbf{v}_1^{(1)}, \mathbf{v}_2^{(1)}; \mathbf{Y}|\mathbf{v}_1^{(2)}, \mathbf{v}_2^{(2)}) \geq 2d\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.110}$$

Using (4.109) and (4.110), we have

$$I(\mathbf{v}_1, \mathbf{v}_2; \mathbf{Y}) \geq 2\left(d + \frac{l}{3}\right)\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.111}$$

$$= \frac{2}{3}N\left(\frac{1}{2}\log P\right) + o(\log P) \tag{4.112}$$

4.7 Conclusions

In this chapter, we determined the optimal sum s.d.o.f. of the two-user MIMO multiple access wiretap channel with N antennas at each transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper. For the case of fading channel gains, we provided vector space alignment based achievable schemes that exploit the channel variation over multiple time slots in general. When the channel gains are fixed, such channel diversity is not available, and we provided single time-slot schemes that use real interference alignment on structured signaling. We also provided matching converses to establish the optimality of the achievable schemes for both fixed and fading channel gains. Our results highlight the effect of the number of eavesdropper antennas on the s.d.o.f. of the multiple access wiretap channel.

Chapter 5: MIMO One Hop Networks with No Eve CSIT

5.1 Introduction

In this chapter, we study the MIMO wiretap channel with one helper and the MIMO multiple access wiretap channel without eavesdropper CSIT. In each case, the legitimate transmitters and the receiver have N antennas each, and the eavesdropper has K antennas; see Fig. 5.1 and Fig. 5.2. In both cases, the channel is fast fading and the channel gains vary in an i.i.d. fashion across the links and time. Our goal in this chapter is to investigate the optimal sum s.d.o.f. of the MIMO wiretap channel with one helper and the MIMO multiple access wiretap channel as a function of N and K.

To that end, we provide an achievable scheme based on vector space alignment [8], that attains $\frac{1}{2}(2N-K)$ s.d.o.f. for the wiretap channel with one helper for all values of $0 \leq K \leq 2N$. Note that when $K \leq N$, this value coincides with the optimal s.d.o.f. for the wiretap channel with one helper in the case where full eavesdropper CSIT is available, and is, therefore, optimal without eavesdropper CSIT as well. Further, the proposed scheme suffices as an achievable scheme for the multiple access wiretap channel as well.

To prove the optimality of the proposed scheme for the multiple access wiretap

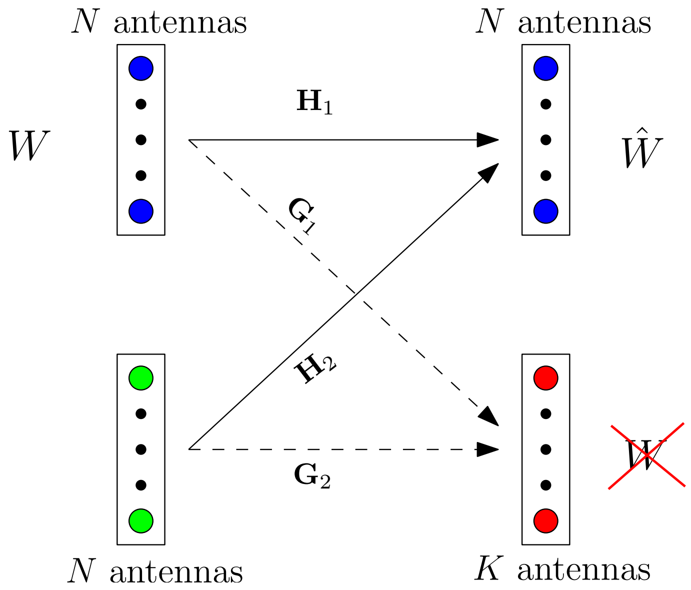


Figure 5.1: Wiretap channel with a helper.

channel, we next provide a matching converse for the regime $K \leq N$. We use the MIMO versions of the *secrecy penalty lemma* and the *role of a helper lemma* [4], and exploit channel symmetry at the eavesdropper. Since the transmitters do not have the eavesdropper's CSIT, the output at the K antennas of the eavesdropper are *entropy symmetric* [15], i.e., any two subsets of the antenna outputs have the same differential entropy, if the subsets are of equal size. Finally, we use a MIMO version of the *least alignment lemma* [10, 16] to complete the proof of the converse. As in the SISO case, when $K \leq N$ the multiple access wiretap channel reduces to the wiretap channel with one helper when the eavesdropper's CSIT is not available.

Next, for the regime $N \leq K \leq 2N$, we provide an upper bound which shows that the sum s.d.o.f. of the multiple access wiretap channel cannot be larger than $\frac{2N(2N-K)}{4N-K}$. Though loose, this bound suffices to show that, unlike the regime $K \leq N$, there is loss of s.d.o.f. due to lack of eavesdropper CSIT, even for the wiretap channel

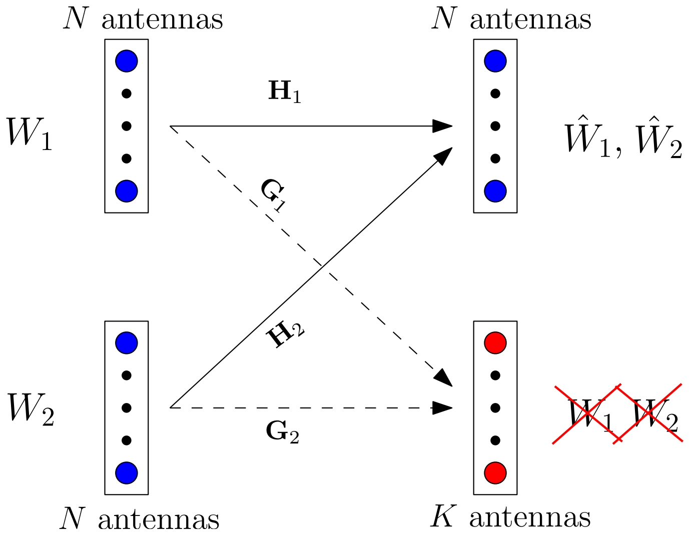


Figure 5.2: The multiple access wiretap channel.

with one helper, in the regime $\frac{3N}{2} \leq K \leq 2N$.

Finally, for the regime $N \leq K \leq 2N$, we restrict ourselves to *linear* encoding strategies [11, 17], where the channel input of each antenna in every time slot is restricted to be a linear combination of some information symbols intended for the legitimate receiver and some artificial noise symbols to provide secrecy at the eavesdropper, and show that under this restriction to linear encoding schemes, the *linear* sum s.d.o.f. can be no larger than $\frac{1}{2}(2N - K)$. The key idea of the proof is that since no alignment is possible at the eavesdropper, the artificial noise symbols should asymptotically occupy the maximum number of dimensions available at the eavesdropper; consequently, the dimension of the linear signal space at the eavesdropper should be $Kn + o(n)$ in n channel uses.

5.2 System Model

We consider two fundamental channel models: the wiretap channel with one helper and the multiple access wiretap channel. In each case, we assume that the channel gains are non-zero and are drawn from a common continuous distribution with bounded support in an i.i.d. fashion in each channel use. The common continuous distribution is known at all the terminals in the system. We assume no eavesdropper CSIT, that is, the channel gains to the eavesdropper are not available at any transmitter. In the following subsections we describe each channel model and provide the relevant definitions.

5.2.1 Wiretap Channel with Helpers

The MIMO wiretap channel with one helper, see Fig. 5.1, is described by,

$$\mathbf{Y}(t) =\mathbf{H}_1(t)\mathbf{X}_1(t) + \mathbf{H}_2(t)\mathbf{X}_2(t) + \mathbf{N}_1(t) \tag{5.1}$$

$$\mathbf{Z}(t) =\mathbf{G}_1(t)\mathbf{X}_1(t) + \mathbf{G}_2(t)\mathbf{X}_2(t) + \mathbf{N}_2(t) \tag{5.2}$$

where $\mathbf{X}_1(t)$ and $\mathbf{X}_2(t)$ are the N dimensional column vectors denoting the input of the legitimate transmitter and the helper, respectively, $\mathbf{Y}(t)$ is an N dimensional vector denoting the legitimate receiver's channel output, and $\mathbf{Z}(t)$ is a K dimensional vector denoting the eavesdropper's channel output, at time t. In addition, $\mathbf{N}_1(t)$ and $\mathbf{N}_2(t)$ are N and K dimensional white Gaussian noise vectors, respectively, with $\mathbf{N}_1 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$ and $\mathbf{N}_2 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_K)$, where $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. Here, $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are the $N \times N$ and $K \times N$ channel matrices from transmitter i to the legitimate receiver and the eavesdropper, respectively, at time t. The entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are drawn from a fixed continuous distribution with bounded support in an i.i.d. fashion at every time slot t. We assume that the channel matrices at the legitimate receiver, $\mathbf{H}_i(t)$, are known with full precision at all terminals, at time t. However, the channel matrices to the eavesdropper, $\mathbf{G}_i(t)$ are not known at any transmitter. All channel inputs satisfy the average power constraint $E[\|\mathbf{X}_i(t)\|^2] \leq P,\ i = 1, 2$, where $\|\mathbf{X}\|$ denotes the Euclidean (or the spectral) norm of the vector (or matrix) $\mathbf{X}$.

The transmitter wishes to send a message W, uniformly distributed in $\mathcal{W}_i$, securely to the legitimate receiver in the presence of the eavesdropper. A secure rate R, with $R = \frac{\log|\mathcal{W}|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W \neq \hat{W}] \leq \epsilon_n$, for $i = 1, 2$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W; \mathbf{Z}^n) \leq \epsilon_n \tag{5.3}$$

where $\epsilon_n \to 0$ as $n \to \infty$. An s.d.o.f. d is said to be achievable if a rate R is achievable with

$$d = \lim_{P \to \infty} \frac{R}{\frac{1}{2}\log P} \tag{5.4}$$

5.2.2 The Multiple Access Wiretap Channel

The two-user multiple access wiretap channel, see Fig. 5.2, is as follows:

$$\mathbf{Y}(t) = \mathbf{H}_1(t)\mathbf{X}_1(t) + \mathbf{H}_2(t)\mathbf{X}_2(t) + \mathbf{N}_1(t) \tag{5.5}$$

$$\mathbf{Z}(t) = \mathbf{G}_1(t)\mathbf{X}_1(t) + \mathbf{G}_2(t)\mathbf{X}_2(t) + \mathbf{N}_2(t) \tag{5.6}$$

where $\mathbf{X}_i(t)$ is an N dimensional column vector denoting the ith user's channel input, $\mathbf{Y}(t)$ is an N dimensional vector denoting the legitimate receiver's channel output, and $\mathbf{Z}(t)$ is a K dimensional vector denoting the eavesdropper's channel output, at time t. In addition, $\mathbf{N}_1(t)$ and $\mathbf{N}_2(t)$ are N and K dimensional white Gaussian noise vectors, respectively, with $\mathbf{N}_1 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$ and $\mathbf{N}_2 \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_K)$, where $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. Here, $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are the $N \times N$ and $K \times N$ channel matrices from transmitter i to the legitimate receiver and the eavesdropper, respectively, at time t. The entries of $\mathbf{H}_i(t)$ and $\mathbf{G}_i(t)$ are drawn from a fixed continuous distribution with bounded support in an i.i.d. fashion at every time slot t. We assume that the channel matrices to the legitimate receiver, $\mathbf{H}_i(t)$, are known with full precision at all terminals, at time t. However, the channel matrices to the eavesdropper, $\mathbf{G}_i(t)$, are not available at the transmitters. All channel inputs satisfy the average power constraint $E[\|\mathbf{X}_i(t)\|^2] \leq P,\ i = 1, 2$.

Transmitter i wishes to send a message W_i, uniformly distributed in $\mathcal{W}_i$, securely to the legitimate receiver in the presence of the eavesdropper. A secure rate pair (R_1, R_2), with $R_i = \frac{\log|\mathcal{W}_i|}{n}$ is achievable if there exists a sequence of codes which satisfy the reliability constraints at the legitimate receiver, namely, $\Pr[W_i \neq \hat{W}_i] \leq \epsilon_n$, for $i = 1, 2$, and the secrecy constraint, namely,

$$\frac{1}{n} I(W_1, W_2; \mathbf{Z}^n) \leq \epsilon_n \tag{5.7}$$

where $\epsilon_n \to 0$ as $n \to \infty$. An s.d.o.f. pair (d_1, d_2) is said to be achievable if a rate pair (R_1, R_2) is achievable with

$$d_i = \lim_{P \to \infty} \frac{R_i}{\frac{1}{2} \log P} \tag{5.8}$$

The sum s.d.o.f. d_s is the largest achievable $d_1 + d_2$.

5.2.3 A Linear Secure Degrees of Freedom Perspective

In this chapter, we will also consider *linear* coding strategies as defined in [17, 71]. In such cases, the degrees of freedom simply represents the dimension of the linear subspace of transmitted signals.

When we focus on linear coding schemes, we consider a communication scheme of blocklength n, where transmitter i wishes to send $m_i(n)$ *information* symbols $\mathbf{v}_i \in \mathbb{R}^{m_i(n)}$ to the legitimate receiver reliably and securely. In case of the wiretap channel with one helper, $m_2(n) = 0$. Each information symbol is a zero-mean Gaussian random variable with variance αP, where α is a constant chosen to ensure that the power constraints are satisfied at each transmitter. In addition to the information symbols, transmitter i can use $n_i(n)$ artificial noise symbols, $\mathbf{u}_i \in \mathbb{R}^{n_i(n)}$

each of which is a zero-mean Gaussian random variable with variance αP. These artificial noise symbols need not be decoded at the receiver; instead they help to drown out the information symbols at the eavesdropper, thus, providing security.

At each time t, the information symbols $\mathbf{v}_i$ at transmitter i are modulated by a precoding matrix $\mathbf{P}_i(t) \in \mathbb{R}^{N \times m_i(n)}$, while the artificial noise symbols $\mathbf{u}_i$ are modulated using a precoding matrix $\mathbf{Q}_i(t) \in \mathbb{R}^{N \times n_i(n)}$. Since the channel gains $\mathbf{H}_i(t)$, $i = 1, 2$ are known at both transmitters at time t, the precoding matrices $\mathbf{P}_i(t)$ and $\mathbf{Q}_i(t)$ can each depend on $\{\mathbf{H}_1(k), \mathbf{H}_2(k), k = 1, \dots, t\}$. However, since the channel gains $\mathbf{G}_i(t)$ are not available at any transmitter, $\mathbf{P}_i$ and $\mathbf{Q}_i$ are independent of $\{\mathbf{G}_i(t), t = 1, \dots, n\}$.

At time t, transmitter i sends a linear combination of the information and the artificial noise symbols:

$$\mathbf{X}_i(t) = \mathbf{P}_i(t)\mathbf{v}_i + \mathbf{Q}_i(t)\mathbf{u}_i \tag{5.9}$$

The channel outputs at time t are, therefore,

$$\begin{aligned}\mathbf{Y}(t) =& \mathbf{H}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{H}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 \\ &+ \mathbf{H}_1(t)\mathbf{Q}_1(t)\mathbf{u}_1 + \mathbf{H}_2(t)\mathbf{Q}_2(t)\mathbf{u}_2 + \mathbf{N}_1(t) \qquad (5.10)\\ \mathbf{Z}(t) =& \mathbf{G}_1(t)\mathbf{P}_1(t)\mathbf{v}_1 + \mathbf{G}_2(t)\mathbf{P}_2(t)\mathbf{v}_2 \\ &+ \mathbf{G}_1(t)\mathbf{Q}_1(t)\mathbf{u}_1 + \mathbf{G}_2(t)\mathbf{Q}_2(t)\mathbf{u}_2 + \mathbf{N}_2(t) \qquad (5.11)\end{aligned}$$

Now letting $\bar{\mathbf{P}}_i = [\mathbf{P}_i(1), \dots, \mathbf{P}_i(n)]^T$, $\bar{\mathbf{Q}}_i = [\mathbf{Q}_i(1), \dots, \mathbf{Q}_i(n)]$, we can compactly write the channel outputs as

$$\bar{\mathbf{Y}} = \bar{\mathbf{H}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2\mathbf{v}_2 + \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_1 \tag{5.12}$$

$$\bar{\mathbf{Z}} = \bar{\mathbf{G}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2\mathbf{v}_2 + \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_2 \tag{5.13}$$

where $\bar{\mathbf{H}}_i$ and $\bar{\mathbf{G}}_i$ are the $Nn \times Nn$ and $Kn \times Nn$ block diagonal matrices

$$\bar{\mathbf{H}}_i = \begin{bmatrix} \mathbf{H}_i(1) & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_i(2) & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_i(n) \end{bmatrix} \tag{5.14}$$

$$\bar{\mathbf{G}}_i = \begin{bmatrix} \mathbf{G}_i(1) & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_i(2) & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{G}_i(n) \end{bmatrix} \tag{5.15}$$

and $\bar{\mathbf{N}}_i = [\mathbf{N}_i(1), \dots, \mathbf{N}_i(n)]^T$ for $i = 1, 2$.

At the legitimate receiver, the interference subspace is

$$\mathcal{I}_B = \text{colspan}([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]) \tag{5.16}$$

Let $\mathcal{I}_B^c$ denote the orthogonal subspace of $\mathcal{I}_B$. If we ignore the additive Gaussian noise, i.e., in the high transmit power regime, the decodability of $\mathbf{v}_1$ and $\mathbf{v}_2$ at the legitimate receiver corresponds to the constraint that the projection of the subspace colspan($[\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2]$) onto $\mathcal{I}_B^c$ must have dimension $m_1(n) + m_2(n)$, i.e.,

$$\begin{aligned}\dim\Big(\mathrm{Proj}_{\mathcal{I}_B^c}\mathrm{colspan}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2]\right)\Big) &= \dim\left(\mathrm{colspan}\left(\bar{\mathbf{P}}_1\right)\right) + \dim\left(\mathrm{colspan}\left(\bar{\mathbf{P}}_2\right)\right) \\ &= m_1(n) + m_2(n) \qquad (5.17)\end{aligned}$$

This can be rewritten as requiring that

$$\mathrm{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) - \mathrm{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) = m_1(n) + m_2(n) \qquad (5.18)$$

On the other hand, at the eavesdropper, we require that

$$\lim_{n\to\infty}\frac{1}{n}\dim\Big(\mathrm{Proj}_{\mathcal{I}_E^c}\mathrm{colspan}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2]\right)\Big) = 0,\ a.s. \qquad (5.19)$$

where

$$\mathcal{I}_E = \mathrm{colspan}([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]) \qquad (5.20)$$

The security requirement in (5.19) can be reformulated as follows: Let $L(n)$ be the number of *leakage dimensions* defined as

$$L(n) = \mathrm{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) - \mathrm{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \qquad (5.21)$$

Then, we want

$$\lim_{n\to\infty} \frac{L(n)}{n} = 0, \ a.s. \tag{5.22}$$

In other words, we want the artificial noise symbols to occupy the full received signal space at the eavesdropper asymptotically. This secrecy requirement is a weaker version of the original constraint $\frac{1}{n}I(W_1, W_2; \mathbf{Z}^n) \to 0$. Indeed, it is analogous to requiring that $\lim_{n\to\infty} \lim_{P\to\infty} \frac{I(W_1,W_2;\mathbf{Z}^n)}{\log P} = 0$. However, this does not lead to any loss of generality in our case because the proposed achievable scheme which satisfies the weakened secrecy requirement may be modified using stochastic encoding techniques [1] to obtain a scheme that satisfies the stronger security constraint as well. Note that a converse with the weaker secrecy requirement suffices as a converse for the case of the stronger secrecy requirement.

For the wiretap channel with one helper, a *linear* s.d.o.f. d with $d = m_1(n)/n$ is said to be achievable if there exists a sequence of precoding matrices $\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}_1, \bar{\mathbf{Q}}_2$ such that both the reliability constraints in (5.17) and the security constraints in (5.19) are satisfied.

For the multiple access wiretap channel, a *linear* s.d.o.f. pair (d_1, d_2), with $d_i = m_i(n)/n$ is said to be achievable if there exists a sequence of precoding matrices $\bar{\mathbf{P}}_i, \bar{\mathbf{Q}}_i$ such that both the reliability constraints in (5.17) and the security constraints in (5.19) are satisfied. The *linear* sum s.d.o.f. d_s is the supremum of $d_1 + d_2$, such that the pair (d_1, d_2) is achievable.

5.3 Main Results

The main result of this chapter is the determination of the optimal linear sum s.d.o.f. for the MIMO wiretap channel with one helper and the MIMO multiple access channel. We have the following theorem.

Theorem 8 *For both the $N \times N \times N \times K$ wiretap channel with one helper and the multiple access wiretap channel with no eavesdropper CSIT, the optimal linear sum s.d.o.f. d_s is*

$$d_s = \max\left(\frac{1}{2}(2N-K), 0\right) \tag{5.23}$$

for almost all channel gains. Further, without any linearity constraints on the encoding schemes, the optimal sum s.d.o.f. d_s is

$$d_s \begin{cases} = \frac{1}{2}(2N-K), & 0 \leq K \leq N \\ \leq \frac{2N(2N-K)}{4N-K}, & N \leq K \leq 2N \\ = 0, & K \geq 2N \end{cases} \tag{5.24}$$

We also have the following corollary.

Corollary 2 *For the $N \times N \times N \times K$ multiple access wiretap channel with no eavesdropper CSIT, the linear s.d.o.f. region is given by the set of all nonnegative*

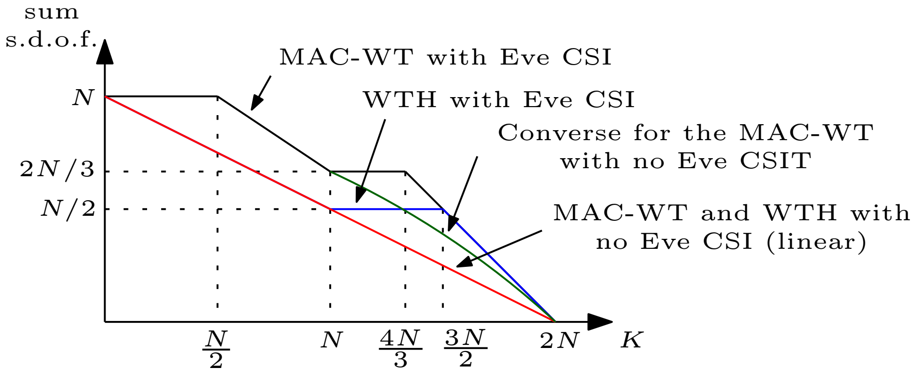


Figure 5.3: Sum s.d.o.f. with number of eavesdropper antennas.

pairs $(d_1, d_2$ *that satisfy:*

$$d_1 + d_2 = \frac{1}{2}(2N - K) \tag{5.25}$$

The proof of the corollary follows from the observation that every point in the given region can be achieved by time sharing between the points $\left(\frac{1}{2}(2N - K), 0\right)$ and $\left(0, \frac{1}{2}(2N - K)\right)$, which can themselves be attained by treating the multiple access wiretap channel as a wiretap channel with one helper. Also, no point outside the given region is achievable since the sum s.d.o.f. is bounded by $\frac{1}{2}(2N - K)$, from Theorem 8.

Fig. 5.3 shows the optimal linear sum s.d.o.f. for the wiretap channel with one helper and the multiple access wiretap channel with and without eavesdropper CSIT. Similar to the SISO case in Chapter 3, the MIMO multiple access wiretap channel reduces to the wiretap channel with one helper when the eavesdropper CSIT is not available for the regime $0 \leq K \leq N$, and at least from a linear s.d.o.f. perspective in the regime $N \leq K \leq 2N$. However, unlike in the SISO case, the linear s.d.o.f. for the wiretap channel with one helper decreases due to the lack of eavesdropper CSIT. Even without any linearity constraints, the optimal s.d.o.f. for the wiretap channel with one helper does decrease due to lack of eavesdropper CSIT, as can be seen from the general loose upper bound, especially in the regime $\frac{3N}{2} \leq K \leq 2N$.

5.4 Proof of Theorem 8

In this section, we will prove Theorem 8 by providing an achievable scheme and a converse. Since Theorem 8 implies that the wiretap channel with one helper and the multiple access wiretap channel have the same linear sum s.d.o.f., we first note that it suffices to provide a linear achievable scheme for the wiretap channel with one helper, since the multiple access wiretap channel can be treated as a wiretap channel with one helper with time sharing between the users. Also, since any rate achievable for the wiretap channel with one helper is achievable for the multiple access wiretap channel, a converse for the multiple access wiretap channel suffices as a converse for the wiretap channel with one helper as well. Thus, in the following subsections, we provide an achievable scheme for the wiretap channel with one helper and a converse for the multiple access wiretap channel.

5.4.1 Achievable Scheme for the Wiretap Channel with One Helper

In this scheme, the transmitter sends $(2N - K)$ information symbols reliably and securely to the legitimate receiver in two time slots, in order to achieve $\frac{1}{2}(2N - K)$ s.d.o.f. In the framework of linear coding strategies discussed in Section 5.2.3, we set the blocklength $n = 2$, $m_1 = 2N - K$, $m_2 = 0$. Also, we choose $n_1 = n_2 = K$, i.e., K artificial noise symbols are sent from each transmitter over the two time slots. At each time slot, transmitter i sends a linear combination of its information and artificial noise symbols as in (5.9). Note, however, that for the wiretap channel with one helper, transmitter 2 does not have any information symbols $\mathbf{v}_2$, and hence, there is no $\mathbf{P}_2$. The channel outputs can be written compactly as in (5.12)-(5.13) as:

$$\bar{\mathbf{Y}} = \bar{\mathbf{H}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_1 \tag{5.26}$$

$$\bar{\mathbf{Z}} = \bar{\mathbf{G}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1\mathbf{u}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2\mathbf{u}_2 + \bar{\mathbf{N}}_2 \tag{5.27}$$

It remains to choose the precoding matrices $\bar{\mathbf{P}}_1$, $\bar{\mathbf{Q}}_1$ and $\bar{\mathbf{Q}}_2$ appropriately. We make the following selection:

$$\bar{\mathbf{Q}}_i = \bar{\mathbf{H}}_i^{-1}\bar{\mathbf{Q}}, \quad i = 1, 2 \tag{5.28}$$

where $\bar{\mathbf{Q}}$ is a $2N \times K$ matrix with rank K. Also choose $\bar{\mathbf{P}}_1$ to be a $2N \times (2N - K)$ matrix with rank $2N - K$, such that the matrix $[\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}]$ has rank $2N$. Note that this condition will be satisfied almost surely if the elements of $\bar{\mathbf{P}}_1$ and $\bar{\mathbf{Q}}$ are chosen from any continuous distribution in an i.i.d. fashion. With this selection, the channel outputs are:

$$\bar{\mathbf{Y}} = \bar{\mathbf{H}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{Q}}_1(\mathbf{u}_1 + \mathbf{u}_2) + \bar{\mathbf{N}}_1 \tag{5.29}$$

$$\bar{\mathbf{Z}} = \bar{\mathbf{G}}_1\bar{\mathbf{P}}_1\mathbf{v}_1 + \bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}\mathbf{u}_1 + \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}\mathbf{u}_2 + \bar{\mathbf{N}}_2 \tag{5.30}$$

The decodability of $\mathbf{v}_1$ at the legitimate receiver in the high transmit power regime follows immediately since the matrix $[\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}]$ has rank $2N$ by our choice of $\bar{\mathbf{P}}_1$ and $\bar{\mathbf{Q}}$. On the other hand, the number of *leakage dimensions* L is

$$L = \text{rank}[\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}, \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}] - \text{rank}[\bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}, \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}] \tag{5.31}$$

$$\leq 2K - 2K \tag{5.32}$$

$$= 0 \tag{5.33}$$

where we have used the fact that for any full-rank $\bar{\mathbf{Q}}$ chosen independently of $\bar{\mathbf{G}}_1, \bar{\mathbf{G}}_2$, $\text{rank}[\bar{\mathbf{G}}_1\bar{\mathbf{H}}_1^{-1}\bar{\mathbf{Q}}, \bar{\mathbf{G}}_2\bar{\mathbf{H}}_2^{-1}\bar{\mathbf{Q}}] = 2K$ for almost all channel realizations of $(\bar{\mathbf{G}}_1, \bar{\mathbf{G}}_2)$. This follows from the following lemma by noting that each row and each column of $\bar{\mathbf{G}}_i$ has at least one entry drawn from a continuous distribution in an i.i.d. fashion and the matrices $\bar{\mathbf{H}}_i^{-1}\bar{\mathbf{Q}}$ for $i = 1, 2$ do not depend on the $\bar{\mathbf{G}}_i$s.

Lemma 5 *Let $\mathbf{P}_1 \in \mathbb{R}^{N\times m_1}$ and $\mathbf{P}_2 \in \mathbb{R}^{N\times m_2}$ fixed matrices with ranks p_1 and p_2, respectively. Let $\mathbf{G}_1$ and $\mathbf{G}_2$ be $K \times N$ matrices whose each row and each column has at least one entry that is drawn from some continuous distribution in an i.i.d. fashion, and the remaining elements are arbitrary but fixed. Then,*

$$K \geq \mathit{rank}[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2] \geq \min(p_1 + p_2, K) \tag{5.34}$$

almost surely.

The proof of this lemma is relegated to Appendix 5.6.1.

Therefore, the security requirement in (5.22) is satisfied as well. This completes the achievable scheme. We remark here that though the achievability has been shown for linear framework, it can be easily shown that the leakage $I(\mathbf{v}_1; \bar{\mathbf{Z}}) \leq o(\log P)$, as done in Chapter 4. Further by using stochastic encoding techniques, one can obtain an achievable scheme for which the leakage $\frac{1}{n}I(W; \mathbf{Z}^n) \to 0$ as $n \to \infty$.

5.4.2 Converse

In this section, we will prove the converse for the multiple access wiretap channel. To that end, we consider two regimes of K. When $0 \leq K \leq N$, we prove the converse for general transmission schemes without any restrictions of linearity. For the regime $N \leq K \leq 2N$, we prove the converse under the assumption of linear coding schemes only. We also provide a general upper bound in this regime which does not match the achievablity; nevertheless, it shows that there is loss in s.d.o.f. for the wiretap channel with one helper and the multiple access wiretap channel due to no eavesdropper CSIT.

5.4.2.1 $0 \leq K \leq N$: Converse with No Restrictions

We wish to show that:

$$d_1 + d_2 \leq \frac{1}{2}(2N - K) \tag{5.35}$$

Let us first state three lemmas which are useful for the proof.

Lemma 6 (Channel symmetry [15, Lemma 3]) *Let $Z^K = \{Z_1, \dots, Z_K\}$ be entropy symmetric, i.e., for any subsets A and B of $\{1, \dots, K\}$, with $|A| = |B| \leq K$,*

$$h(\{Z_i, i \in A\}) = h(\{Z_i, i \in B\}) \tag{5.36}$$

Then, for any $M \geq N$, the following holds:

$$\frac{1}{N} h(Z^N) \geq \frac{1}{M} h(Z^M) \tag{5.37}$$

Lemma 7 (Least alignment lemma [16, Lemma 3]) *Consider two receivers, each with L antennas. Suppose the channel gains to receiver 2 are not available at the transmitters. If $\mathbf{Y}$ and $\mathbf{Z}$ denote the channel outputs at receivers 1 and 2, respectively, we have*

$$h(\mathbf{Z}^n) \geq h(\mathbf{Y}^n) + no(\log P) \tag{5.38}$$

Combining the above two lemmas, we have the following lemma.

Lemma 8 *For the $N \times N \times N \times K$ MIMO multiple access wiretap channel with no eavesdropper CSIT, with $K \leq N$*

$$h(\mathbf{Z}^n) \geq \frac{K}{N} h(\mathbf{Y}^n) + no(\log P) \tag{5.39}$$

We relegate the proof of this lemma to Appendix 5.6.2.

Let us now proceed with the converse proof. As in [4, 12], we define noisy versions of $\mathbf{X}_i$ as $\tilde{\mathbf{X}}_i = \mathbf{X}_i + \tilde{\mathbf{N}}_i$ where $\tilde{\mathbf{N}}_i \sim \mathcal{N}(\mathbf{0}, \rho_i^2 \mathbf{I}_N)$ with $\rho_i^2 < \min\left(\frac{1}{\|\mathbf{H}_i\|^2}, \frac{1}{\|\mathbf{G}_i\|^2}\right)$. The *secrecy penalty lemma* [4] can then be derived as

$$\begin{aligned} n(R_1 + R_2) \leq & I(W_1, W_2; \mathbf{Y}^n | \mathbf{Z}^n) + n\epsilon & (5.40) \\ \leq & h(\mathbf{Y}^n | \mathbf{Z}^n) + nc_1 & (5.41) \\ = & h(\mathbf{Y}^n, \mathbf{Z}^n) - h(\mathbf{Z}^n) + nc_1 & (5.42) \\ \leq & h(\tilde{\mathbf{X}}_1^n, \tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 & (5.43) \\ \leq & h(\tilde{\mathbf{X}}_1^n) + h(\tilde{\mathbf{X}}_2^n) - h(\mathbf{Z}^n) + nc_2 & (5.44) \end{aligned}$$

The *role of a helper lemma* [4] also generalizes to the MIMO case as

$$\begin{aligned} nR_1 \leq & I(\mathbf{X}_1^n; \mathbf{Y}^n) & (5.45) \\ = & h(\mathbf{Y}^n) - h(\mathbf{H}_2^n \mathbf{X}_2^n + \mathbf{N}_1^n) & (5.46) \\ \leq & h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_2^n) + nc_5 & (5.47) \end{aligned}$$

By symmetry, we also have

$$nR_2 \leq h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_1^n) + nc_5 \quad (5.48)$$

Adding (5.44), (5.47) and (5.48), we have

$$\begin{aligned} 2n(R_1 + R_2) \leq & 2h(\mathbf{Y}^n) - h(\mathbf{Z}^n) + no(\log P) & (5.49) \\ \leq & 2h(\mathbf{Y}^n) - \frac{K}{N} h(\mathbf{Y}^n) + no(\log P) & (5.50) \end{aligned}$$

$$=\frac{2N-K}{N}h(\mathbf{Y}^n)+no(\log P) \tag{5.51}$$

$$\leq(2N-K)\left(\frac{n}{2}\log P\right)+no(\log P) \tag{5.52}$$

where (5.50) follows from Lemma 8 and we have used the fact that $h(\mathbf{Y}^n) \leq \frac{N}{2}\log P + no(\log P)$. Therefore, we have,

$$R_1+R_2 \leq \frac{1}{2}(2N-K)\left(\frac{1}{2}\log P\right)+o(\log P) \tag{5.53}$$

Dividing by $\frac{1}{2}\log P$ and taking the limit $P \to \infty$, we have

$$d_1+d_2 \leq \frac{1}{2}(2N-K) \tag{5.54}$$

which completes the proof of the converse for the regime $0 \leq K \leq N$.

5.4.2.2 $N \leq K \leq 2N$: Converse with Linear Coding Strategies

We begin with the following lemma.

Lemma 9 *For the $N \times N \times N \times K$ multiple access wiretap channel, and for any* linear *achievable scheme satisfying both the reliability and security constraints, and also $d_1 + d_2 > 0$,*

$$\lim_{n\to\infty}\frac{1}{n}rank\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1,\bar{\mathbf{G}}_2\bar{\mathbf{P}}_2,\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1,\bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)=\lim_{n\to\infty}\frac{1}{n}rank\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1,\bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)=K \tag{5.55}$$

We relegate the proof of this lemma to Appendix 5.6.3.

To proceed with the upper bound, first note that since strictly positive sum s.d.o.f. is achievable for the multiple access wiretap channel using linear schemes, we can safely discard the case $d_1 + d_2 = 0$ for the purpose of the converse. Therefore, from Lemma 9, the rank of the vector space spanned by the output at the eavesdropper is $Kn + o(n)$, i.e.,

$$\lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) = \lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) = K \tag{5.56}$$

We have,

$$m_1(n) + m_2(n) = \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) - \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) \tag{5.57}$$

$$\begin{aligned}
&\leq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) - \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) \\
&\quad - \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \\
&\quad + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) &\text{(5.58)} \\
&\leq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) - \frac{1}{2}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \\
&\quad - \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \\
&\quad + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) &\text{(5.59)} \\
&\leq \text{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) + \frac{1}{2}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \\
&\quad - \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) &\text{(5.60)}
\end{aligned}$$

$$\begin{aligned}
\leq & \operatorname{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) \\
& -\frac{1}{2}\operatorname{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) + o(n) && (5.61) \\
\leq & Nn - \frac{1}{2}Kn + o(n) && (5.62) \\
= & \frac{(2N-K)n}{2} + o(n) && (5.63)
\end{aligned}$$

where (5.57) follows from the decodability constraint, (5.58) follows from the secrecy constraint (5.22), and (5.59) follows from the following:

$$\begin{aligned}
2 \times \operatorname{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) & \geq \operatorname{rank}\left([\bar{\mathbf{H}}_1\bar{\mathbf{Q}}_1]\right) + \operatorname{rank}\left([\bar{\mathbf{H}}_2\bar{\mathbf{Q}}_2]\right) && (5.64) \\
& = \operatorname{rank}\left([\bar{\mathbf{Q}}_1]\right) + \operatorname{rank}\left([\bar{\mathbf{Q}}_2]\right) && (5.65) \\
& = \operatorname{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1]\right) + \operatorname{rank}\left([\bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) && (5.66) \\
& \geq \operatorname{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) && (5.67)
\end{aligned}$$

The above equalities all hold almost surely since $\bar{\mathbf{H}}_i$ and $\bar{\mathbf{G}}_i$ are both full column rank almost surely.

Now dividing by n and taking limit $n \to \infty$, we have

$$d_1 + d_2 \leq \frac{1}{2}(2N - K) \qquad (5.68)$$

5.4.2.3 $N \leq K \leq 2N$: Converse with No Restrictions

We have the following lemma.

Lemma 10 *For the $N \times N \times N \times K$ MIMO multiple access wiretap channel with* *no eavesdropper CSIT, with $K \leq 2N$*

$$h(\mathbf{Z}^n) \geq \frac{K}{2N} h(\mathbf{Y}^n, \mathbf{Z}^n) + no(\log P) \tag{5.69}$$

The proof of this lemma is relegated to the Appendix 5.6.4.

Now we proceed with the upper bound as in the case of $0 \leq K \leq N$:

$$\begin{aligned}
n(R_1 + R_2) \leq & I(W_1, W_2; \mathbf{Y}^n | \mathbf{Z}^n) + n\epsilon && (5.70)\\
\leq & h(\mathbf{Y}^n | \mathbf{Z}^n) + nc_1 && (5.71)\\
= & h(\mathbf{Y}^n, \mathbf{Z}^n) - h(\mathbf{Z}^n) + nc_1 && (5.72)\\
\leq & \left(1 - \frac{K}{2N}\right) h(\mathbf{Y}^n, \mathbf{Z}^n) + no(\log P) && (5.73)\\
\leq & \frac{2N - K}{2N} \left(h(\tilde{\mathbf{X}}_1^n) + h(\tilde{\mathbf{X}}_2^n)\right) + no(\log P) && (5.74)
\end{aligned}$$

The *role of the helper* lemmas yield:

$$\begin{aligned}
nR_1 \leq & h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_2^n) + no(\log P) && (5.75)\\
nR_2 \leq & h(\mathbf{Y}^n) - h(\tilde{\mathbf{X}}_1^n) + no(\log P) && (5.76)
\end{aligned}$$

Eliminating $h(\tilde{\mathbf{X}}_1^n)$ and $h(\tilde{\mathbf{X}}_2^n)$ from (5.74), (5.75) and (5.76), we have

$$\begin{aligned}
n(R_1 + R_2) \leq & \frac{2(2N - K)}{4N - K} h(\mathbf{Y}^n) + no(\log P) && (5.77)\\
\leq & \frac{2N(2N - K)}{4N - K} \left(\frac{n}{2} \log P\right) + no(\log P) && (5.78)
\end{aligned}$$

Dividing by n and letting $n \to \infty$, we have

$$R_1 + R_2 \leq \frac{2N(2N-K)}{4N-K} \left(\frac{1}{2} \log P \right) + o(\log P) \tag{5.79}$$

Now dividing by $\frac{1}{2} \log P$ and letting $P \to \infty$,

$$d_1 + d_2 \leq \frac{2N(2N-K)}{4N-K} \tag{5.80}$$

5.5 Conclusions

In this chapter, we considered two fundamental multi-user channel models: the MIMO wiretap channel with one helper and the MIMO multiple access wiretap channel. In each case, the eavesdropper has K antennas while the remaining terminals have N antennas. We assumed that the CSIT of the legitimate receiver is available but no eavesdropper CSIT is available. We determined the optimal sum s.d.o.f. for each channel model for the regime $K \leq N$, and showed that in this regime, the multiple access wiretap channel reduces to the wiretap channel with one helper in the absence of eavesdropper CSIT. For the regime $N \leq K \leq 2N$, we obtained the optimal *linear* s.d.o.f., and showed that the multiple access wiretap channel and the wiretap channel with one helper have the same optimal s.d.o.f. when restricted to linear encoding strategies. In the absence of any such restrictions, we provided a loose upper bound for the sum s.d.o.f. of the multiple access wiretap channel in the regime $N \leq K \leq 2N$. Our results showed that unlike in the SISO case, there is loss of s.d.o.f. for even the wiretap channel with one helper due to lack of eavesdropper

CSIT, especially when $K \geq N$.

5.6 Appendix

5.6.1 Proof of Lemma 5

First note when $N \leq K$, $\mathbf{G}_i$s have full column rank almost surely. Therefore,

$$\text{rank}[\mathbf{G}_i\mathbf{P}_i] = \text{rank}[\mathbf{P}_i] = p_i \tag{5.81}$$

almost surely. On the other hand, when $N \geq K$, we have

$$\text{rank}[\mathbf{G}_i\mathbf{P}_i] \geq \text{rank}[\mathbf{G}_i\hat{\mathbf{P}}_i] \tag{5.82}$$

where $\hat{\mathbf{P}}_i$ is a $N \times p_i$ submatrix of $\mathbf{P}_i$ with full column rank. Let $\bar{p}_i = \min(K, p_i)$. Now, the determinant of any $\bar{p}_i \times \bar{p}_i$ submatrix of $\mathbf{G}_i\hat{\mathbf{P}}_i$ is a multi-variate polynomial of the random entries of $\mathbf{G}_i$ and is zero for only finitely many realizations. Therefore, $\mathbf{G}_i\hat{\mathbf{P}}_i$ has rank $\bar{p}_i$. Note that when $N \leq K$, $\bar{p}_i = p_i$ is satisfied trivially.

Therefore, there exists a set $I_i \subseteq \{1, \ldots, m_i\}$ such that $|I_i| = \bar{p}_i$ and the collection of column vectors $\mathbf{C}_i = \{\mathbf{c}_{ij}, j \in I_i\}$ are linearly independent, where $\mathbf{c}_{ij}$ denotes the jth column of $\mathbf{G}_i\mathbf{P}_i$. Then,

$$\text{rank}[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2] \geq \text{rank}[\mathbf{C}_1, \mathbf{C}_2] \tag{5.83}$$

The matrix $[\mathbf{C}_1, \mathbf{C}_2]$ is a $K \times \bar{p}_1 + \bar{p}_2$ matrix. Now, if $K \leq \bar{p}_1 + \bar{p}_2$, consider any $K \times K$ submatrix of $[\mathbf{C}_1, \mathbf{C}_2]$. The determinant of this submatrix is a multivariate polynomial function of the random entries of $\mathbf{G}_1$ and $\mathbf{G}_2$, and therefore, the determinant can be zero for only finitely many realizations, corresponding to the roots of the multi-variate polynomial function. Note that this is true if each row and each column of $\bar{\mathbf{G}}_i$ has at least one random entry. Also, the polynomial function is not identically zero. Therefore, in this case,

$$\text{rank}[\mathbf{C}_1, \mathbf{C}_2] = K \tag{5.84}$$

On the other hand, if $K \geq \bar{p}_1 + \bar{p}_2$, we can consider a $(\bar{p}_1 + \bar{p}_2) \times (\bar{p}_1 + \bar{p}_2)$ submatrix of $[\mathbf{C}_1, \mathbf{C}_2]$, and using a similar argument, claim that

$$\text{rank}[\mathbf{C}_1, \mathbf{C}_2] = \bar{p}_1 + \bar{p}_2 \tag{5.85}$$

Combining (5.83), (5.84) and (5.85), we have that

$$\begin{aligned}
\text{rank}[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2] &\geq \min\left(\bar{p}_1 + \bar{p}_2, K\right) && (5.86)\\
&= \min\left(\min(p_1, K) + \min(p_2, K), K\right) && (5.87)\\
&= \min\left(\min(p_1 + p_2, K + p_1, K + p_2, 2K), K\right) && (5.88)\\
&= \min\left(p_1 + p_2, K\right) && (5.89)
\end{aligned}$$

Finally, it trivially holds that $K \geq \text{rank}[\mathbf{G}_1\mathbf{P}_1, \mathbf{G}_2\mathbf{P}_2]$. This completes the proof of the lemma.

5.6.2 Proof of Lemma 8

Note that $K \leq N$. Consider $N-K$ additional outputs $\hat{\mathbf{Z}}$ at the eavesdropper as:

$$\hat{\mathbf{Z}}(t) = \hat{\mathbf{G}}_1(t)\mathbf{X}_1(t) + \hat{\mathbf{G}}_2(t)\mathbf{X}_2(t) + \hat{\mathbf{N}}_2(t) \tag{5.90}$$

where each $\hat{\mathbf{G}}_i$ is a $(N-K) \times N$ matrix whose entries are drawn in an i.i.d. fashion from the same continuous distribution as the entries of $\mathbf{G}_i$, and the entries of $\hat{\mathbf{N}}_2$ are i.i.d. zero-mean unit-variance Gaussian noise. Assume that the $\hat{\mathbf{G}}_i$s are not available at the transmitters either. Then, the enhanced output $\bar{\mathbf{Z}}(t) = (\mathbf{Z}(t), \hat{\mathbf{Z}}(t))$ is entropy symmetric. Therefore, using Lemma 6, we have

$$h(\mathbf{Z}^n) \geq \frac{K}{N} h(\bar{\mathbf{Z}}^n) \tag{5.91}$$

Now, since the $\mathbf{G}_i$s and $\hat{\mathbf{G}}_i$s are not available at the transmitters, using Lemma 7, we have

$$h(\bar{\mathbf{Z}}^n) \geq h(\mathbf{Y}^n) + no(\log P) \tag{5.92}$$

Combining (5.91) and (5.92), we get the desired result that

$$h(\mathbf{Z}^n) \geq \frac{K}{N} h(\mathbf{Y}^n) + no(\log P) \tag{5.93}$$

5.6.3 Proof of Lemma 9

Since $d_1 + d_2 > 0$, w.l.o.g. assume $d_1 > 0$. We wish to prove that

$$\lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) = \lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) = K \tag{5.94}$$

For the sake of contradiction, suppose $\lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) < K$. We have

$$\begin{aligned}
&\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \\
&\qquad \geq \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) && (5.95)\\
&\qquad = \text{rank}\left([\bar{\mathbf{G}}_1[\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}_1], \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) && (5.96)\\
&\qquad \geq \min\left(\text{rank}\left([\bar{\mathbf{P}}_1, \bar{\mathbf{Q}}_1]\right) + \text{rank}\left([\bar{\mathbf{Q}}_2]\right), Kn\right) && (5.97)\\
&\qquad = \min\left(\text{rank}\left([\bar{\mathbf{P}}_1]\right) + \text{rank}\left([\bar{\mathbf{Q}}_1]\right) + \text{rank}\left([\bar{\mathbf{Q}}_2]\right), Kn\right) && (5.98)\\
&\qquad = \min\left(m_1(n) + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1]\right) + \text{rank}\left([\bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right), Kn\right) && (5.99)\\
&\qquad \geq \min\left(m_1(n) + \text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right), Kn\right) && (5.100)
\end{aligned}$$

where (5.97) follows from Lemma 5, (5.98) follows from the decodability requirement, and (5.99) follows almost surely since $\bar{\mathbf{G}}_i$ is full column rank almost surely as long as $K > N$. Therefore,

$$\lim_{n\to\infty} \frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{P}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{P}}_2, \bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right)$$

$$\geq \min\left(d_1 + \lim_{n\to\infty}\frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right), K\right) \tag{5.101}$$

$$> \lim_{n\to\infty}\frac{1}{n}\text{rank}\left([\bar{\mathbf{G}}_1\bar{\mathbf{Q}}_1, \bar{\mathbf{G}}_2\bar{\mathbf{Q}}_2]\right) \tag{5.102}$$

which contradicts the security requirement in (5.22).

5.6.4 Proof of Lemma 10

Consider $2N - K$ additional outputs $\hat{\mathbf{Z}}$ at the eavesdropper:

$$\hat{\mathbf{Z}}(t) = \hat{\mathbf{G}}_1(t)\mathbf{X}_1(t) + \hat{\mathbf{G}}_2(t)\mathbf{X}_2(t) + \hat{\mathbf{N}}_2(t) \tag{5.103}$$

where each $\hat{\mathbf{G}}_i$ is a $(2N-K)\times N$ matrix whose entries are drawn in an i.i.d. fashion from the same continuous distribution as the entries of $\mathbf{G}_i$, and the entries of $\hat{\mathbf{N}}_2$ are i.i.d. zero-mean unit-variance Gaussian noise. Assume that the $\hat{\mathbf{G}}_i$s are not available at the transmitters either. Then, the enhanced output $\bar{\mathbf{Z}}(t) = (\mathbf{Z}(t), \hat{\mathbf{Z}}(t))$ is entropy symmetric. Therefore, using Lemma 6, we have

$$h(\mathbf{Z}^n) \geq \frac{K}{2N}h(\bar{\mathbf{Z}}^n) \tag{5.104}$$

Now, given $\bar{\mathbf{Z}}^n$, we can decode both inputs $\mathbf{X}_1^n$ and $\mathbf{X}_2^n$ to within noise variance, and therefore also $\mathbf{Y}^n$ and $\mathbf{Z}^n$. Therefore,

$$h(\bar{\mathbf{Z}}^n) \geq h(\mathbf{Y}^n, \mathbf{Z}^n) + no(\log P) \tag{5.105}$$

Combining (5.104) and (5.105), we get the desired result that

$$h(\mathbf{Z}^n) \geq \frac{K}{2N} h(\mathbf{Y}^n, \mathbf{Z}^n) + no(\log P) \tag{5.106}$$

Chapter 6: Two-User MISO Broadcast Channel with Alternating CSIT

6.1 Introduction

In this chapter, we focus on the effect of delay and time variation of the availability of CSI. We consider the s.d.o.f. region of the fading two-user MISO broadcast channel with confidential messages, in which the transmitter with two antennas has two confidential messages, one for each of the single antenna users (see Fig. 6.1). The CSIT from each user can be of the form I_i, $i = 1, 2$ where $I_1, I_2 \in \{\mathsf{P}, \mathsf{D}, \mathsf{N}\}$, and the forms P, D and N correspond to perfect and instantaneous, completely delayed, and no CSIT, respectively. This gives rise to nine possible CSIT states: three *homogeneous* states PP, DD and NN, and six heterogeneous states PD, DP, PN, NP, DN and ND.

The optimal s.d.o.f. region is well known in the literature for each of the three homogeneous states; the optimal sum s.d.o.f. is 2 in state PP, 1 in state DD [15] and 0 in state NN, due to statistical equivalence of both receivers in the absence of any CSIT. Thus, in this chapter, we first focus on the heterogeneous CSIT settings, namely states PD, PN and DN. We determine the optimal s.d.o.f. region for each of the three states. We introduce the *local statistical equivalence* property, which states that if we consider the outputs of a receiver for such states in which it supplies delayed or no CSIT, the entropy of the channel outputs conditioned on the past outputs is the same as that of another artificial receiver whose channel is distributed identically as the original receiver, and provide new converse proofs based on it. We also provide a new achievable scheme for the DN state.

Next, we consider time variation of CSIT states. We assume that the CSIT state I_1I_2 occurs for an arbitrary fraction $\lambda_{I_1I_2}$ of the total duration of communication, subject to the mild constraint $\lambda_{I_1I_2} = \lambda_{I_2I_1}$, when $I_1 \neq I_2$. We determine the optimal s.d.o.f. region of the two-user MISO broadcast channel with confidential messages in this setting of *alternating* CSIT, which is first introduced in [23] without any secrecy requirements.

With nine states, each occurring for an arbitrary fraction of the time, it is not immediately clear how to optimally code across the states and the achievability of the s.d.o.f. region is highly non-trivial. To this end, we first develop several key constituent schemes, where each scheme uses a subset of the nine states to achieve a particular s.d.o.f. value. Now given an arbitrary probability mass function (pmf) on the nine CSIT states, we judiciously time share between the constituent schemes to achieve the optimal s.d.o.f. region. We consider different sub-cases based on the relative proportions of the various states and explicitly characterize how the constituent schemes should be time shared to obtain the optimal s.d.o.f. region in each sub-case.

Finally, we provide a matching converse for the full region. The idea behind

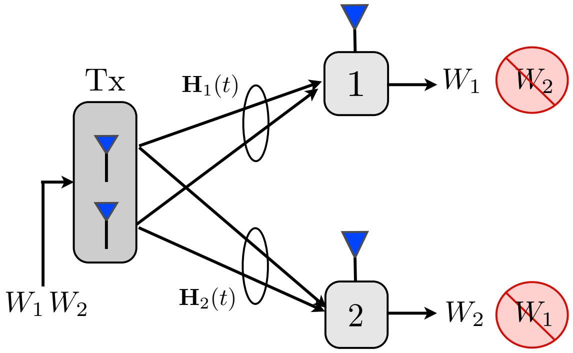


Figure 6.1: The MISO broadcast channel with confidential messages.

the converse is to first enhance the channel by providing more CSIT to obtain a new channel with fewer number of states but at least as large secrecy capacity as the original channel. Outer bounds on the s.d.o.f. region for the enhanced channel are then obtained by exploiting the *local statistical equivalence property*, yielding the desired outer bounds for the original channel.

6.2 System Model

We consider a two-user MISO broadcast channel, shown in Fig. 6.1, where the transmitter Tx, equipped with 2 antennas, wishes to send independent confidential messages to two single antenna receivers 1 and 2. The input-output relations at time t are given by,

$$Y(t) = \mathbf{H}_1(t)\mathbf{X}(t) + N_1(t) \tag{6.1}$$

$$Z(t) = \mathbf{H}_2(t)\mathbf{X}(t) + N_2(t), \tag{6.2}$$

where $Y(t)$ and $Z(t)$ are the channel outputs of receivers 1 and 2, respectively. The 2×1 channel input $\mathbf{X}(t)$ is power constrained as $\mathbb{E}[||\mathbf{X}(t)||^2] \leq P$, and $N_1(t)$ and $N_2(t)$ are circularly symmetric complex white Gaussian noises with zero-mean and unit-variance. The 1×2 channel vectors $\mathbf{H}_1(t)$ and $\mathbf{H}_2(t)$ of receivers 1 and 2, respectively, are independent and identically distributed (i.i.d.) with continuous distributions, and are also i.i.d. over time. We denote $\mathbf{H}(t) = \{\mathbf{H}_1(t), \mathbf{H}_2(t)\}$ as the collective channel vectors at time t and $\mathbf{H}^n = \{\mathbf{H}(1), \dots, \mathbf{H}(n)\}$ as the sequence of channel vectors up until and including time n.

In practice, the receivers estimate the channel coefficients and feed them back to the transmitter. In general, the receiver can choose to send not only the current measurements, but rather any function of all the channel measurements it has taken upto that time. The CSIT at time t can thus be any function of the measured channel coefficients upto time t. There are two key aspects to the CSIT: precision and delay. Precision captures the fact that the measurements made at the receivers and sent to the transmitter are imprecise (usually, quantized) and noisy. Delay is introduced since making measurements and feeding them back to the transmitter takes time. We will focus on the delay aspect of CSIT, and assume that the CSIT when available, has infinite precision.

In order to model the delay in CSIT, we assume that at each time t, there are 3 possible CSIT states for each user:

- *Perfect CSIT* (P): This denotes the availability of precise and instantaneous CSI of a user at the transmitter. In this state, the transmitter has precise channel knowledge before the start of the communication.

- *Delayed CSIT* (D): In this state, the transmitter does not have the CSI at the beginning of the communication. In slot t, the receiver may send any function of all the channel coefficients upto and including time t as CSI to the transmitter. However, the CSIT becomes available only after a delay such that the CSI is completely outdated, that is, independent of the current channel realization.

- *No CSIT* (N): In this state, there is no CSI of the user available at the transmitter.

Denote the CSIT of user 1 by I_1 and the CSIT of user 2 by I_2. Then,

$$I_1, I_2 \in \{\mathsf{P}, \mathsf{D}, \mathsf{N}\}. \tag{6.3}$$

Thus, for the two-user MISO broadcast channel, we have 9 CSIT states, namely PP, DD, NN, PD, DP, PN, NP, DN, and ND. Let $\lambda_{I_1 I_2}$ be the fraction of the time the state $I_1 I_2$ occurs. Then,

$$\sum_{I_1, I_2} \lambda_{I_1 I_2} = 1. \tag{6.4}$$

We also assume symmetry: $\lambda_{I_1 I_2} = \lambda_{I_2 I_1}$ for every $I_1 I_2$. Specifically,

$$\lambda_{PD} = \lambda_{DP} \tag{6.5}$$

$$\lambda_{DN} = \lambda_{ND} \tag{6.6}$$

$$\lambda_{PN} = \lambda_{NP}. \tag{6.7}$$

Further, we assume that perfect and global CSI is available at both receivers.

A secure rate pair (R_1, R_2) is achievable if there exists a sequence of codes which satisfy the reliability constraints at the receivers, namely, $\Pr\left[W_i \neq \hat{W}_i\right] \leq \epsilon_n$, for $i = 1, 2$, and the confidentiality constraints, namely,

$$\frac{1}{n} I(W_1; Z^n, \mathbf{H}^n) \leq \epsilon_n, \qquad \frac{1}{n} I(W_2; Y^n, \mathbf{H}^n) \leq \epsilon_n, \tag{6.8}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Informally, the constraints in (6.8) ensure that the information leakage, per channel use, of the first receiver's message at the second receiver should be arbitrarily small, and vice versa. A s.d.o.f. pair (d_1, d_2) is achievable, if there exists an achievable rate pair (R_1, R_2) such that

$$d_1 = \lim_{P \to \infty} \frac{R_1}{\log P}, \qquad d_2 = \lim_{P \to \infty} \frac{R_2}{\log P}. \tag{6.9}$$

Let us define the following:

$$\lambda_P \triangleq \lambda_{PP} + \lambda_{PD} + \lambda_{PN} \tag{6.10}$$

$$\lambda_D \triangleq \lambda_{PD} + \lambda_{DD} + \lambda_{DN} \tag{6.11}$$

$$\lambda_N \triangleq \lambda_{PN} + \lambda_{DN} + \lambda_{NN}. \tag{6.12}$$

Using these definitions, it is easy to verify that

$$\lambda_P + \lambda_D + \lambda_N = 1. \tag{6.13}$$

Here, we can interpret these three quantities as follows:

- λ_P: represents the total fraction of time the CSIT of a user is in the P state.
- λ_D: represents the total fraction of time the CSIT of a user is delayed, that is, the state D.
- λ_N: represents the total fraction of time a user supplies no CSIT.

Given the probability mass function (pmf), $\lambda_{I_1 I_2}$, our goal is to characterize the s.d.o.f. region of the two-user MISO broadcast channel with confidential messages.

6.3 Main Result and Discussion

Theorem 9 *The s.d.o.f. region for the two-user MISO broadcast channel with confidential messages with alternating CSIT, $\mathcal{D}(\lambda_{I_1 I_2})$, is the set of all non-negative pairs (d_1, d_2) satisfying,*

$$d_1 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right) \tag{6.14}$$

$$d_2 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right) \tag{6.15}$$

$$3d_1 + d_2 \leq 2 + 2\lambda_P \tag{6.16}$$

$$d_1 + 3d_2 \leq 2 + 2\lambda_P \tag{6.17}$$

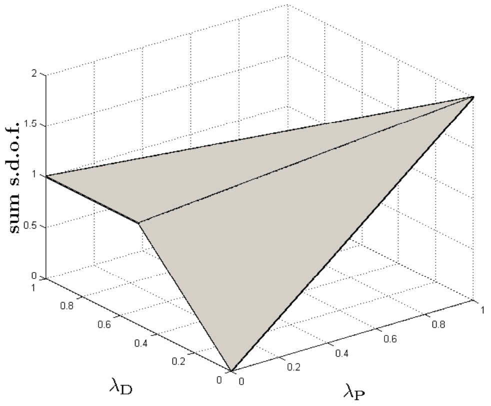


Figure 6.2: The sum s.d.o.f. as a function of λ_P and λ_D.

$$d_1 + d_2 \leq 2(\lambda_P + \lambda_D). \tag{6.18}$$

A proof for the achievability of this region will be provided in Section 6.5 using constituent schemes presented in Section 6.4. A converse is provided in Section 6.6.

We next make a series of remarks highlighting the consequences and interesting aspects of this theorem.

Remark 1. [Sum s.d.o.f.: $\max(d_1 + d_2)$]

From the region stated in (6.14)-(6.18), it is clear that the sum s.d.o.f. is given by,

$$\text{sum s.d.o.f.} = \min\left(2\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}\right), 2(1-\lambda_{NN}), 2(\lambda_P+\lambda_D), 1+\lambda_P\right). \tag{6.19}$$

The sum s.d.o.f. expression in (6.19) can be significantly simplified by noting that the first two terms in the minimum are inactive due to the inequalities $1 + \lambda_P \leq 2\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}\right)$, and $2(\lambda_P + \lambda_D) = 2(1-\lambda_N) \leq 2(1-\lambda_{NN})$. These inequalities follow directly from (6.10)-(6.13). Using these inequalities, the sum s.d.o.f. expression above is equivalent to

$$\text{sum s.d.o.f.} = \min\left(2(\lambda_P + \lambda_D), 1 + \lambda_P\right) \tag{6.20}$$

$$= \min\left(2(\lambda_P + \lambda_D), 2\lambda_P + \lambda_D + \lambda_N\right) \tag{6.21}$$

$$= 2\lambda_P + \lambda_D + \min(\lambda_D, \lambda_N). \tag{6.22}$$

Fig. 6.2 shows the sum s.d.o.f. as a function of λ_P and λ_D.

Remark 2. [Same marginals property]

From (6.22), we notice that the marginal probabilities λ_P, λ_D and λ_N are sufficient to determine the sum s.d.o.f. *Thus, for any given pmf $\lambda_{I_1I_2}$, satisfying the symmetry conditions* (6.5)-(6.7)*, there exists an* ***equivalent*** *alternating CSIT problem having only three states:* PP*,* DD *and* NN *occurring for λ_P, λ_D and λ_N fractions of the time, respectively, that has the same sum s.d.o.f.* This observation is similar to the case when there is no secrecy [23]. *However unlike in [23], the s.d.o.f. region* ***does not*** *have the same property in general* as we can see the explicit dependence of the s.d.o.f. region in (6.14)-(6.18) on λ_{PP} and λ_{NN}.

Remark 3. [Channel knowledge equivalence]

We next highlight an interesting property which shows that from the sum s.d.o.f. perspective, no CSIT is equivalent to delayed CSIT when $\lambda_D \geq \lambda_N$, and delayed CSIT is equivalent to perfect CSIT when $\lambda_D < \lambda_N$.

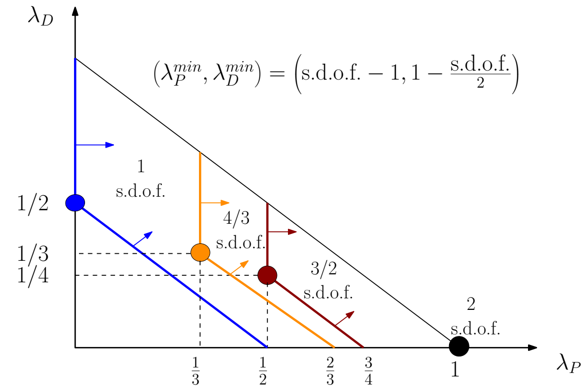


Figure 6.3: Trade-off between delayed and perfect CSIT.

Equivalence of delayed and no CSIT when $\lambda_D \geq \lambda_N$: From a sum s.d.o.f. perspective, we see that when $\lambda_D \geq \lambda_N$, the sum s.d.o.f. depends only on λ_P. Hence, as long as $\lambda_D \geq \lambda_N$ holds, the N states behave as D states in the sense that, if the N states were enhanced to D states, the sum s.d.o.f. would not increase. Essentially, the N states can be combined with various D states and we obtain the same sum s.d.o.f. as if every N state were replaced by a D state. Consider an example, where the states PD, DP and NN occur for $\frac{2}{5}$th, $\frac{2}{5}$th and $\frac{1}{5}$th fractions of the time, respectively. Note that $\lambda_D = \frac{2}{5} > \lambda_N = \frac{1}{5}$ in this case. The sum s.d.o.f., from (6.22), is $2\lambda_P + \lambda_D + \lambda_N = \frac{7}{5}$. Now, if we enhance the N states to D states, we get the states PD, DP and DD occur for $\frac{2}{5}$th, $\frac{2}{5}$th and $\frac{1}{5}$th of the time, respectively. The sum s.d.o.f. of this enhanced system is still $\frac{7}{5}$.

Equivalence of delayed and perfect CSIT when $\lambda_D \leq \lambda_N$: From a sum s.d.o.f. perspective, we see that when $\lambda_D \leq \lambda_N$, the sum s.d.o.f. depends only on λ_N. Hence, in this case, if $\lambda_D \leq \lambda_N$, the delayed CSIT is as good as perfect CSIT, that is, every D state can be enhanced to a P state without any increase in the sum s.d.o.f. For example, consider a system where the states PD, DP and NN occur for $\frac{1}{5}$th, $\frac{1}{5}$th and

$\frac{3}{5}$th fractions of the time, respectively. Note that $\lambda_D = \frac{1}{5} < \lambda_N = \frac{3}{5}$ in this case. The sum s.d.o.f. for this system is $\frac{4}{5}$, from (6.22). By enhancing the D states to P states, we get a system, where the states PP and NN occur for $\frac{2}{5}$th and $\frac{3}{5}$th fractions of the time, respectively. The sum s.d.o.f. in for this enhanced system is still $\frac{4}{5}$.

Remark 4. [Minimum CSIT required for a sum s.d.o.f. value]

Fig. 6.3 shows the trade-off between λ_P and λ_D for a given value of sum s.d.o.f. The highlighted corner point in each curve shows the most *efficient* point in terms of CSIT requirement. *Any other feasible point either involves redundant CSIT or unnecessary instantaneous CSIT where delayed CSIT would have sufficed.* For example, following are the minimum CSIT requirements for various sum s.d.o.f. values:

$$\text{sum s.d.o.f.} = 2 \ : (\lambda_P, \lambda_D)_{\min} = (1, 0) \tag{6.23}$$

$$\text{sum s.d.o.f.} = \frac{3}{2} : (\lambda_P, \lambda_D)_{\min} = \left(\frac{1}{2}, \frac{1}{4}\right) \tag{6.24}$$

$$\text{sum s.d.o.f.} = \frac{4}{3} : (\lambda_P, \lambda_D)_{\min} = \left(\frac{1}{3}, \frac{1}{3}\right) \tag{6.25}$$

$$\text{sum s.d.o.f.} = 1 \ : (\lambda_P, \lambda_D)_{\min} = \left(0, \frac{1}{2}\right). \tag{6.26}$$

In general, for a given value of sum s.d.o.f. $= s$, the minimum CSIT requirements are given by:

$$(\lambda_P, \lambda_D)_{\min} = \begin{cases} \left(s-1, 1-\frac{s}{2}\right), & \text{if } 1 \leq s \leq 2 \\ \left(0, \frac{s}{2}\right), & \text{if } 0 \leq s \leq 1. \end{cases} \tag{6.27}$$

Remark 5. [Cost of security]

We recall that in the case with no security [23], the sum d.o.f. is given by,

$$\text{sum d.o.f.} = 2 - \frac{2\lambda_N}{3} - \frac{\max(\lambda_N, 2\lambda_D)}{3}. \tag{6.28}$$

Comparing with (6.22), we see that the loss in d.o.f. that must be incurred to incorporate secrecy constraints is given by,

$$(\text{sum d.o.f.}) - (\text{sum s.d.o.f.}) \triangleq \text{loss} = \begin{cases} \lambda_N, & \text{if } \lambda_N \geq 2\lambda_D \\ \frac{2}{3}(2\lambda_N - \lambda_D), & \text{if } 2\lambda_D \geq \lambda_N \geq \lambda_D \\ \frac{1}{3}(\lambda_N + \lambda_D), & \text{if } \lambda_D \geq \lambda_N. \end{cases} \tag{6.29}$$

If we define $\alpha = \lambda_D/(\lambda_D + \lambda_N)$, we can rewrite (6.29) as follows,

$$\text{loss} = (\lambda_D + \lambda_N) \times \begin{cases} (1 - \alpha), & \text{if } \alpha \leq \frac{1}{3} \\ \left(\frac{4}{3} - 2\alpha\right), & \text{if } \frac{1}{2} \geq \alpha \geq \frac{1}{3} \\ \frac{1}{3}, & \text{if } \alpha \geq \frac{1}{2}. \end{cases} \tag{6.30}$$

We show this loss as a function of α in Fig. 6.4. Note that $\lambda_D + \lambda_N$ is the fraction of the time a user feeds back imperfect (delayed or none) CSIT. If this fraction is fixed, increasing the fraction of the delayed CSIT decreases the penalty due to the security constraints, but only to a certain extent. When $\lambda_N \geq \lambda_D$, increasing the fraction of delayed CSIT leads to a decrease in the penalty due to the security

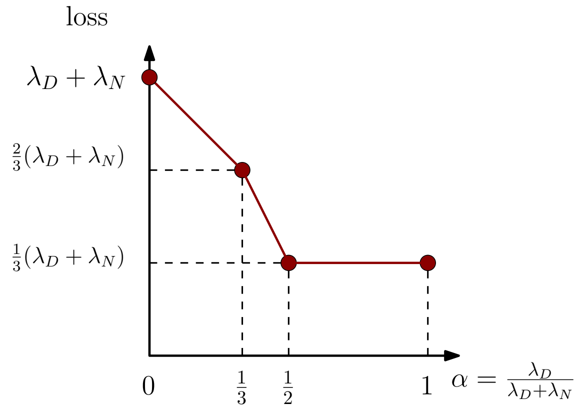


Figure 6.4: Cost of security.

constraints. However, once the fraction of the delayed CSIT (state D) matches that of no CSIT (N), that is, $\lambda_D \geq \lambda_N$, increasing the fraction of delayed CSIT further does not reduce the penalty any more.

Remark 6. [S.d.o.f. characterization of individual CSIT states]

As an additional relevant result, we also characterize the respective s.d.o.f. regions for the 6 individual CSIT states. To the best of our knowledge, the only CSIT states for which the s.d.o.f. regions were previously known are: PP (with sum s.d.o.f.= 2), DD (with sum s.d.o.f.= 1), PN (with s.d.o.f.= 1), and NN (with s.d.o.f.= 0). For the remaining two CSIT states, i.e., PD and DN, we establish the optimal s.d.o.f. regions. In particular, for the PD CSIT state, we show in Appendix 6.8.4 that the s.d.o.f. region is given by $d_1 + d_2 \leq 1$. For the DN state, we show in Appendix 6.8.5 that the s.d.o.f. region is given by $d_1 + d_2 \leq 1/2$. As the next remark shows, these complete set of results for the individual CSIT states confirm the synergistic benefits (or lack thereof) in various alternating CSIT scenarios.

Remark 7. [Synergistic benefits]

It was shown in [23] that by coding across different states one can achieve higher sum d.o.f. than by optimal encoding for each state separately and time sharing. A similar result holds true in our case as well. We illustrate this with the help of a few examples.

Example 1. Consider a special case where only states PD and DP occur, each for half of the time. We show that the optimal sum s.d.o.f. is $\frac{3}{2}$ in this case; see (6.22) here. The best achievable scheme for the PD (or DP) state alone was known to achieve a sum s.d.o.f. of 1. This was either by treating the PD state as a PN state and zero forcing, or by treating PD as a DD state. However a converse proof showing the optimality of 1 sum s.d.o.f. was not known. In Appendix 6.8.4, we present a converse proof to show that the sum s.d.o.f. of 1 is indeed optimal for the PD state alone. Thus, by encoding for each state separately and time sharing between the PD and DP states, we can achieve only 1 sum s.d.o.f., whereas joint encoding across the states achieves sum s.d.o.f. of $\frac{3}{2}$. Thus, we have synergistic benefit of 50% in this case.

Example 2. Consider another special case with three states: PD, DP and NN each occurring for one-third of the time. The optimal sum s.d.o.f. is $\frac{4}{3}$. If we encode for each state separately and time share between them, we can achieve a sum s.d.o.f. of $\frac{1}{3} \times 1 + \frac{1}{3} \times 1 + \frac{1}{3} \times 0 = \frac{2}{3}$, since the NN state does not provide any secrecy. If we encode across the PD and DP states optimally and then time share with the NN state, we can achieve $\frac{2}{3} \times \frac{3}{2} + \frac{1}{3} \times 0 = 1$ sum s.d.o.f. Thus, in this case too, we get synergistic benefit by coding across all the states together.

Example 3. Now, assume we have the following three states: PN, NP and DD each occurring for one-third of the time. The optimal sum s.d.o.f. for this case is $\frac{4}{3}$. On the other hand, the optimal sum s.d.o.f. of the PN state alone is 1, [10], and that of the DD state alone is also 1, [15]. Thus, by separately encoding for each state and time sharing, we can achieve $\frac{1}{3} \times 1 + \frac{1}{3} \times 1 + \frac{1}{3} \times 1 = 1$ sum s.d.o.f. Note that the optimal sum s.d.o.f. for PN and NP states, each occurring for half of the time, is also 1, using (6.22). Thus, by optimal encoding for PN and NP together and time sharing with the DD state also yields sum s.d.o.f. of 1. Therefore, there is synergistic benefit to be gained by coding across all the states together in this case too.

Example 4. Consider the case where the two states, DD and NN occur for equal fractions of time. The optimal sum s.d.o.f. of the DD state alone is 1 [15]. The NN state, by itself does not provide any secrecy and its s.d.o.f. $= 0$. Thus, by encoding for the individual states and time sharing, at most $1 \times \frac{1}{2} + 0 \times \frac{1}{2} = \frac{1}{2}$ sum s.d.o.f. is achievable. However, by jointly encoding across both the DD and NN states, the optimal sum s.d.o.f. of 1 is achievable. Thus, we have synergistic benefit of 100% in terms of sum s.d.o.f. in this case.

Example 5. Finally, consider the case where the two states, DN and ND occur for equal fractions of time. We show in Appendix 6.8.5 that the optimal sum s.d.o.f. for DN state is $\frac{1}{2}$. Thus, by separately encoding across the individual states, only $\frac{1}{2}$ sum s.d.o.f. is achievable. However, by jointly encoding across both the DN and DN states, the optimal sum s.d.o.f. of 1 is achievable. Thus, we have synergistic benefit of 100% in terms of sum s.d.o.f. in this case.

Remark 7. [Lack of synergistic benefits]

There are some situations where joint encoding across alternating states does not yield any benefit in terms of the s.d.o.f. region. For example, consider a case with only 2 states, PN and NP, each occurring for half of the time. The optimal sum s.d.o.f. for the PN state alone is 1, which is achieved by zero forcing. The optimal sum s.d.o.f. of both PN and NP states together is also 1; thus, encoding for each state separately is optimal in this case. Indeed separable encoding for each individual state suffices to achieve the full s.d.o.f. region as well. *This result is perhaps surprising, since in the case with no security, we do get synergistic benefits of joint encoding across the* PN *and* NP *states. The optimal sum s.d.o.f. with joint encoding is* $\frac{3}{2}$*, while that for each state alone is* 1*,* [23].

6.4 Constituent Schemes

Before we present the achievability of the s.d.o.f. region, we first present the key constituent schemes that will be instrumental in the proof. We combine these schemes carefully and time share between them to achieve the s.d.o.f. region. A summary of these constituent schemes is shown in Table 6.1. Before we discuss the individual schemes we make the following remark that applies to all the schemes presented here.

Summary of Constituent Schemes (CS)				
Sum s.d.o.f.	CS Notation	CSIT States	Fractions of States	(d_1, d_2)
2	S^2	PP	1	$(1, 1)$
3/2	$S_1^{3/2}$	PD, DP	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{3}{4}, \frac{3}{4}\right)$
	$S_2^{3/2}$	PD, DP, PN, NP	$\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right)$	$\left(\frac{3}{4}, \frac{3}{4}\right)$
4/3	$S_1^{4/3}$	PD, DP, NN	$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, \frac{2}{3}\right)$
	$S_2^{4/3}$	PN, NP, DD	$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, \frac{2}{3}\right)$
1	S_1^1	DD	1	$\left(\frac{1}{2}, \frac{1}{2}\right)$
	S_2^1	DD, NN	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{1}{2}, \frac{1}{2}\right)$
	S_3^1	DN, ND	$\left(\frac{1}{2}, \frac{1}{2}\right)$	$\left(\frac{1}{2}, \frac{1}{2}\right)$
2/3	$S_1^{2/3}$	DD	1	$\left(\frac{2}{3}, 0\right)$
	$S_2^{2/3}$	DD, NN	$\left(\frac{2}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, 0\right)$
	$S_3^{2/3}$	DN, ND, NN	$\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$	$\left(\frac{2}{3}, 0\right)$

Table 6.1: Constituent schemes.

6.4.1 A Note on the Achievable Security Guarantee

Each scheme described in the following sections can be outlined as follows. We neglect the impact of noise at high SNR. Then, to achieve a certain s.d.o.f. pair (d_1, d_2), we send n_1 symbols $\underline{\mathbf{u}} = (u_1, \ldots, u_{n_1})$ and n_2 symbols $\underline{\mathbf{v}} = (v_1, \ldots, v_{n_2})$ intended for the first and second receivers, respectively, in n_B slots, such that $d_1 = n_1/n_B$ and $d_2 = n_2/n_B$. Finally, we argue that the leakage of information symbols at the unintended receiver is $o(\log P)$. We however want a stronger guarantee of security, namely,

$$\frac{1}{n} I(W_1; Z^n, \mathbf{H}^n) \leq \epsilon_n, \qquad \frac{1}{n} I(W_2; Y^n, \mathbf{H}^n) \leq \epsilon_n. \tag{6.31}$$

To achieve this, we view the n_B slots described in the scheme as a block and treat the equivalent channel from $\underline{\mathbf{u}}$ to $(\mathbf{Y}, \mathbf{H})$ and $(\mathbf{Z}, \mathbf{H})$ as a memoryless wiretap channel (with $(\mathbf{Y}, \mathbf{H})$ being the legitimate receiver) by ignoring the CSI of the previous block. We do the same for the channel from $\underline{\mathbf{v}}$ to $(\mathbf{Z}, \mathbf{H})$ and $(\mathbf{Y}, \mathbf{H})$ (with $(\mathbf{Z}, \mathbf{H})$ as the legitimate receiver). Note also that no information about $\mathbf{H}$ is used to create the codebooks for $\underline{\mathbf{u}}$ and $\underline{\mathbf{v}}$ in any of the schemes. More formally, the following secrecy rate pair is achievable for receivers 1 and 2, respectively, from [1]:

$$R_1 = I(\underline{\mathbf{u}}; \mathbf{Y}, \mathbf{H}) - I(\underline{\mathbf{v}}; \mathbf{Z}, \mathbf{H}) = I(\underline{\mathbf{u}}; \mathbf{Y}|\mathbf{H}) - I(\underline{\mathbf{v}}; \mathbf{Z}|\mathbf{H}) \tag{6.32}$$

$$R_2 = I(\underline{\mathbf{v}}; \mathbf{Z}, \mathbf{H}) - I(\underline{\mathbf{u}}; \mathbf{Y}, \mathbf{H}) = I(\underline{\mathbf{v}}; \mathbf{Z}|\mathbf{H}) - I(\underline{\mathbf{u}}; \mathbf{Y}|\mathbf{H}), \tag{6.33}$$

where we noted that $\underline{\mathbf{u}}$ and $\underline{\mathbf{v}}$ are all independent of $\mathbf{H}$. Using the proposed scheme, $\underline{\mathbf{u}}$ (resp., $\underline{\mathbf{v}}$) can be reconstructed from $(\mathbf{Y}, \mathbf{H})$ (resp., $(\mathbf{Z}, \mathbf{H})$) to within a noise distortion. Thus,

$$I(\underline{\mathbf{u}}; \mathbf{Y}|\mathbf{H}) = n_1 \log P + o(\log P) \tag{6.34}$$

$$I(\underline{\mathbf{v}}; \mathbf{Z}|\mathbf{H}) = n_2 \log P + o(\log P). \tag{6.35}$$

Also, for each scheme,

$$I(\underline{\mathbf{v}}; \mathbf{Y}|\mathbf{H}) = o(\log P) \tag{6.36}$$

$$I(\underline{\mathbf{u}}; \mathbf{Z}|\mathbf{H}) = o(\log P). \tag{6.37}$$

Thus, from (6.32) and (6.33), the achievable secure rates in each block are,

$$R_1 = n_1 \log P + o(\log P) \tag{6.38}$$

$$R_2 = n_2 \log P + o(\log P). \tag{6.39}$$

Since our block contains n_B channel uses, the effective secure rates are

$$R_1 = \frac{n_1}{n_B} \log P + o(\log P) \tag{6.40}$$

$$R_2 = \frac{n_2}{n_B} \log P + o(\log P). \tag{6.41}$$

These rates clearly yield the required s.d.o.f. pair (d_1, d_2), while also conforming to our stringent security requirement.

In the following subsections, we now present the achievability of each scheme in detail.

Notation: A particular sum s.d.o.f. value can be achieved in various ways through alternation between different possible sets of CSIT states. To this end, we use the following notation: if there are r schemes achieving a particular s.d.o.f. value, we denote these schemes as: $S_1^{\text{sum s.d.o.f.}}, S_2^{\text{sum s.d.o.f.}}, \ldots, S_r^{\text{sum s.d.o.f.}}$. For example, in Table 6.1, for achieving the sum s.d.o.f. value of 1, we present $r = 3$ distinct schemes and these are denoted as S_1^1, S_2^1 and S_3^1.

Given a 1×2 channel vector $\mathbf{H}(t)$, we denote by $\mathbf{H}(t)^{\perp}$, a 2×1 beamforming vector that is orthogonal to the 1×2 channel vector $\mathbf{H}(t)$; in other words, $\mathbf{H}(t)\mathbf{H}(t)^{\perp} = 0$.

6.4.2 Scheme Achieving Sum s.d.o.f. of 2

A sum s.d.o.f. of 2 is achievable only in the state PP, that is, when the transmitter has perfect CSIT from both users. This is achievable using zero-forcing. The following scheme achieves a sum s.d.o.f. of 2.

6.4.2.1 Scheme S^2

The scheme S^2 uses the state PP and achieves the rate pair $(d_1, d_2) = (1, 1)$. The scheme is as follows. We wish to send confidential symbols u and v to receivers 1 and 2, respectively, in one time slot, thus achieving a sum s.d.o.f. of 2. Since the transmitter knows both channel coefficients $\mathbf{H}_1$ and $\mathbf{H}_2$, it sends,

$$\mathbf{X} = u\mathbf{H}_2^{\perp} + v\mathbf{H}_1^{\perp}, \tag{6.42}$$

where, $\mathbf{H}_i(t)^{\perp}$ is a 2×1 beamforming vector that is orthogonal to the 1×2 channel vector $\mathbf{H}_i(t)$ for $i = 1, 2$. This is to ensure that the symbols do not leak to unintended receivers. For s.d.o.f. calculations, we disregard the additive noise and the outputs at the receivers are:

$$Y = u\mathbf{H}_1\mathbf{H}_2^{\perp} \tag{6.43}$$

$$Z = v\mathbf{H}_2\mathbf{H}_1^{\perp}, \tag{6.44}$$

which allows both receivers to decode their respective messages. Also, since u does not appear at all in Z, the confidentiality of u is guaranteed. Similarly, the confidentiality of v too is satisfied.

6.4.3 Schemes Achieving Sum s.d.o.f. of 3/2

The following schemes achieve $\frac{3}{2}$ sum s.d.o.f.:

6.4.3.1 Scheme $S_1^{3/2}$

In this subsection, we present the scheme $S_1^{3/2}$ which uses the states $(\mathsf{PD}, \mathsf{DP})$ with fractions $(\frac{1}{2}, \frac{1}{2})$ to achieve rate pair $(d_1, d_2) = (\frac{3}{4}, \frac{3}{4})$.

We wish to send 3 confidential symbols from the transmitter to each of the receivers in 4 channel uses at high P (that is negligible noise). Let us denote by (u_1, u_2, u_3) and (v_1, v_2, v_3) the confidential symbols intended for receivers 1 and 2, respectively. Also, in 2 of the 4 channel uses, the channel is in state PD; in the remaining 2 uses, the channel is in state DP. The scheme is as follows:

1) At time $t = 1$, $S(1) = \mathsf{PD}$: As the transmitter knows $\mathbf{H}_1(1)$, it sends:

$$\mathbf{X}(1) = [u_1 \quad 0]^T + q\mathbf{H}_1(1)^{\perp}, \tag{6.45}$$

where $\mathbf{H}_1(1)\mathbf{H}_1(1)^{\perp} = 0$, and q denotes an artificial noise distributed as $\mathcal{CN}(0, P)$. Here $\mathbf{H}_1(1)^{\perp}$ is a 2×1 beamforming vector orthogonal to the 1×2 channel vector $\mathbf{H}_1(1)$ of receiver 1 that ensures that the artificial noise q does not create interference at receiver 1. The receivers' outputs are:

$$Y(1) = h_{11}(1)u_1 \tag{6.46}$$

$$Z(1) = h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp} \triangleq K. \tag{6.47}$$

Thus, receiver 1 has observed u_1 while receiver 2 gets a linear combination of u_1 and q, which we denote as K. Due to delayed CSIT from receiver 2, the transmitter can reconstruct K in the next channel use and use it for transmission.

2) At time $t = 2$, $S(2) = \mathsf{DP}$: The transmitter knows $\mathbf{H}_2(2)$ and K. It sends

$$\mathbf{X}(2) = [v_1 + K \quad v_2 + K]^T + u_2\mathbf{H}_2(2)^{\perp}. \tag{6.48}$$

The received signals are:

$$\begin{aligned} Y(2) &= h_{11}(2)v_1 + h_{12}(2)v_2 + (h_{11}(2) + h_{12}(2))K + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp} && (6.49)\\ &= L_1(v_1, v_2, K) + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp} && (6.50)\\ Z(2) &= h_{21}(2)v_1 + h_{22}(2)v_2 + (h_{21}(2) + h_{22}(2))K && (6.51)\\ &\triangleq L_2(v_1, v_2, K), && (6.52) \end{aligned}$$

where we have defined $L_1(v_1, v_2, K)$ and $L_2(v_1, v_2, K)$ as linear combinations of v_1, v_2 and K at receivers 1 and 2, respectively.

3) At time $t = 3$, $S(3) = \mathsf{DP}$: The transmitter knows $\mathbf{H}_2(3)$ and $L_1(v_1, v_2, K)$

(via delayed CSIT from $t = 2$). Using these, it transmits:

$$\mathbf{X}(3) = [L_1(v_1, v_2, K) \quad 0]^T + u_3\mathbf{H}_2(3)^{\perp}, \tag{6.53}$$

and the channel outputs are:

$$Y(3) = h_{11}(3)L_1(v_1, v_2, K) + u_3\mathbf{H}_1(3)\mathbf{H}_2(3)^{\perp} \tag{6.54}$$

$$Z(3) = h_{21}(3)L_1(v_1, v_2, K). \tag{6.55}$$

At the end of this step, note that, receiver 2 can decode v_1 and v_2 by first eliminating K using $Z(1)$ and $Z(3)$ to get a linear combination of v_1 and v_2, which it can then use with $Z(2)$ to solve for v_1 and v_2.

4) At time $t = 4$, $S(4) = \mathsf{PD}$: The transmitter knows $\mathbf{H}_1(4)$ and it sends

$$\mathbf{X}(4) = [L_1(v_1, v_2, K) \quad 0]^T + v_3\mathbf{H}_1(4)^{\perp}, \tag{6.56}$$

and the channel outputs are:

$$Y(4) = h_{11}(4)L_1(v_1, v_2, K) \tag{6.57}$$

$$Z(4) = h_{21}(4)L_1(v_1, v_2, K) + v_3\mathbf{H}_2(4)\mathbf{H}_1(4)^{\perp}. \tag{6.58}$$

Thus, at the end of these four steps the outputs at the two receivers can be

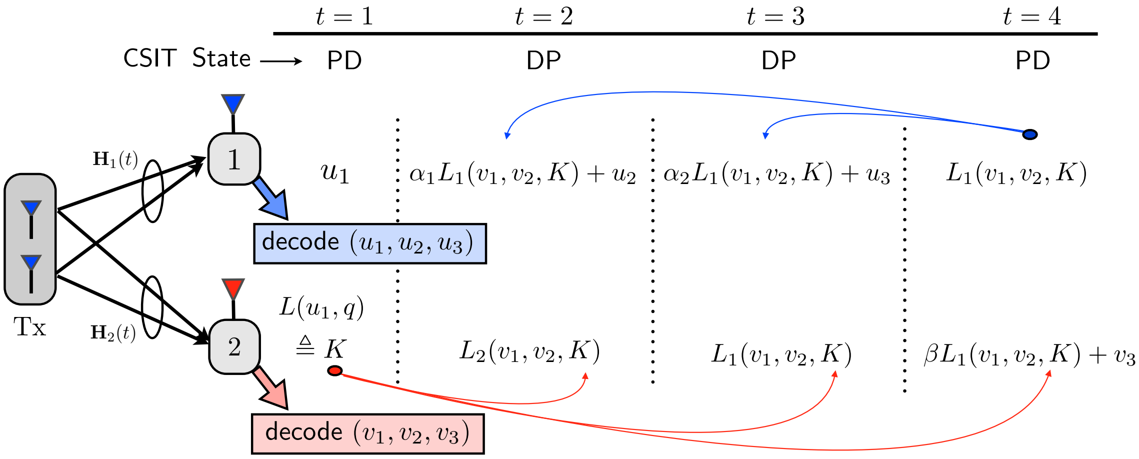


Figure 6.5: Achieving $\frac{3}{2}$ s.d.o.f. using scheme $S_1^{3/2}$.

summarized (see Fig. 6.5) as:

$$\mathbf{Y} = \begin{bmatrix} u_1 \\ \alpha_1 L_1(v_1, v_2, K) + u_2 \\ \alpha_2 L_1(v_1, v_2, K) + u_3 \\ L_1(v_1, v_2, K) \end{bmatrix}, \qquad \mathbf{Z} = \begin{bmatrix} K \\ L_2(v_1, v_2, K) \\ L_1(v_1, v_2, K) \\ \beta L_1(v_1, v_2, K) + v_3 \end{bmatrix}.$$

Using $\mathbf{Y}$, receiver 1 can decode all three symbols (u_1, u_2, u_3) and using $\mathbf{Z}$, receiver 2 can decode (v_1, v_2, v_3). Next we prove that the information leakage is only $o(\log P)$.

Security guarantees:

We consider the four slots as a single block and the equivalent channel from $\underline{\mathbf{u}} = (u_1, u_2, u_3)$ to $(\mathbf{Y}, \mathbf{H})$ and $(\mathbf{Z}, \mathbf{H})$ as a memoryless channel by ignoring the CSI of the previous block. We do the same for the channel from $\underline{\mathbf{v}} = (v_1, v_2, v_3)$ to $(\mathbf{Y}, \mathbf{H})$ and $(\mathbf{Z}, \mathbf{H})$. Recall that all the random variables $\{u_i, v_i, i = 1, 2, 3\}$ and q are independent and distributed as $\mathcal{CN}(0, P)$.

First, let us consider the confidentiality of the first user's symbols $\underline{\mathbf{u}}$. The information leakage at user 2 is:

$$I(\underline{\mathbf{u}};\mathbf{Z}|\mathbf{H}) = I(u_1,u_2,u_3;\mathbf{Z}|\mathbf{H}) \tag{6.59}$$

$$= I(u_1;\mathbf{Z}|\mathbf{H}) \tag{6.60}$$

$$\leq I(u_1;K|\mathbf{H}) \tag{6.61}$$

$$= I(u_1;h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp}|\mathbf{H}) \tag{6.62}$$

$$= h(h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp}|\mathbf{H}) - h(h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp}|u_1,\mathbf{H}) \tag{6.63}$$

$$= h(h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp}|\mathbf{H}) - h(q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp}|\mathbf{H}) \tag{6.64}$$

$$= (\log P + o(\log P)) - (\log P + o(\log P)) \tag{6.65}$$

$$= o(\log P), \tag{6.66}$$

where (6.60) follows from the fact that $\mathbf{Z}$ does not have any term involving (u_2, u_3), and (6.61) follows from the Markov chain $u_1 \to K \to \mathbf{Z}$.

For the second user's symbols, the information leakage at the first receiver is:

$$I(\underline{\mathbf{v}};\mathbf{Y}|\mathbf{H}) = I(v_1,v_2,v_3;\mathbf{Y}|\mathbf{H}) \tag{6.67}$$

$$= I(v_1,v_2;\mathbf{Y}|\mathbf{H}) \tag{6.68}$$

$$\leq I(v_1,v_2;L_1(v_1,v_2,K)|\mathbf{H}) \tag{6.69}$$

$$= h(L_1(v_1,v_2,K)|\mathbf{H}) - h(L_1(v_1,v_2,K)|v_1,v_2,\mathbf{H}) \tag{6.70}$$

$$\leq \log P - h(K|v_1,v_2,\mathbf{H}) + o(\log P) \tag{6.71}$$

$$= \log P - h(K|\mathbf{H}) + o(\log P) \tag{6.72}$$

$$= \log P - \log P + o(\log P) \tag{6.73}$$

$$= o(\log P), \tag{6.74}$$

where (6.68) follows since v_3 does not appear in $\mathbf{Y}$ and (6.69) follows from the Markov chain $(v_1, v_2) \to L_1(v_1, v_2, K) \to \mathbf{Y}$.

6.4.3.2 Scheme $S_2^{3/2}$

In this sub-section, we present the scheme $S_2^{3/2}$ which uses the states $(\mathsf{PD}, \mathsf{DP}, \mathsf{PN}, \mathsf{NP})$ with fractions $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ to achieve $(d_1, d_2) = (\frac{3}{4}, \frac{3}{4})$.

Let us consider the utilization of CSIT in the scheme $S_1^{3/2}$ stated above. In the first slot, delayed CSIT is required from the second user, since that knowledge allows the transmitter to reconstruct K and use it in the second slot. Similarly, in the second time slot, delayed CSIT from the first user is required so that the transmitter can reconstruct $L_1(v_1, v_2, K)$ to transmit in the third and fourth slots. However, in the third and fourth slots, the transmitter does not require any CSIT of the first and second users, respectively. Thus, the same scheme works with PN and NP states in the last two slots. Since it is essentially the same scheme interpreted in a different way, the security of the scheme follows from that of $S_1^{3/2}$.

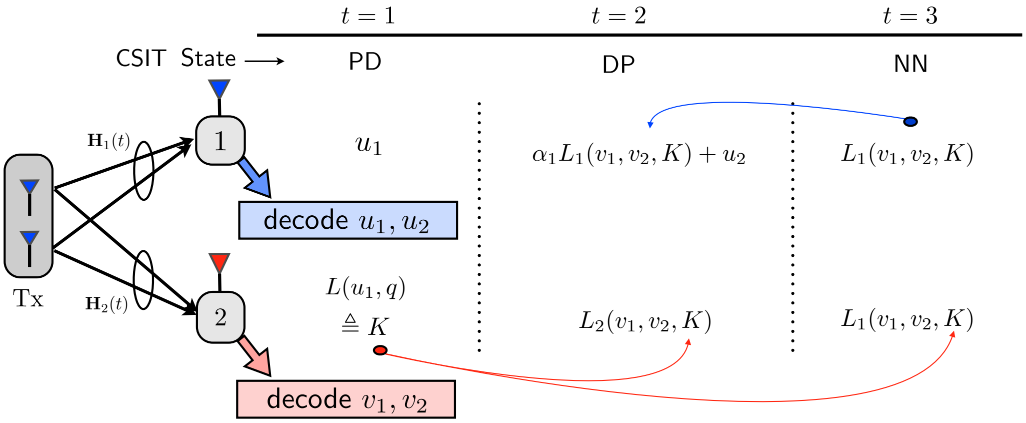


Figure 6.6: Achieving sum s.d.o.f. of $\frac{4}{3}$ using $S_1^{4/3}$.

6.4.4 Schemes Achieving Sum s.d.o.f. of 4/3

6.4.4.1 Scheme $S_1^{4/3}$

In this sub-section, we present the scheme $S_1^{4/3}$ which uses the states $(\mathsf{PD}, \mathsf{DP}, \mathsf{NN})$ for fractions $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ to achieve s.d.o.f. pair $(d_1, d_2) = (\frac{2}{3}, \frac{2}{3})$.

We wish to send 2 symbols to each user in 3 time slots. Let (u_1, u_2) and (v_1, v_2) be the symbols intended for the first and second users, respectively. Fig. 6.6 shows the scheme. It is as follows:

1) At time $t = 1$, $S(1) = \mathsf{PD}$: As the transmitter knows $\mathbf{H}_1(1)$, it sends:

$$\mathbf{X}(1) = [u_1 \quad 0]^T + q\mathbf{H}_1(1)^{\perp}, \tag{6.75}$$

where $\mathbf{H}_1(1)\mathbf{H}_1(1)^{\perp} = 0$, and q denotes an artificial noise distributed as $\mathcal{CN}(0, P)$. Here $\mathbf{H}_1(1)^{\perp}$ is a 2×1 beamforming vector that ensures that the artificial noise q

does not create interference at receiver 1. The receivers' outputs are:

$$Y(1) = h_{11}(1)u_1 \tag{6.76}$$

$$Z(1) = h_{21}(1)u_1 + q\mathbf{H}_2(1)\mathbf{H}_1(1)^{\perp} \triangleq K. \tag{6.77}$$

Thus, receiver 1 has observed u_1 while receiver 2 gets a linear combination of u_1 and q, which we denote as K. Due to delayed CSIT from receiver 2, the transmitter can reconstruct K in the next channel use and use it for transmission.

2) At time $t = 2$, $S(2) = \mathsf{DP}$: The transmitter knows $\mathbf{H}_2(2)$ and K. It sends

$$\mathbf{X}(2) = [v_1 + K \quad v_2 + K]^T + u_2\mathbf{H}_2(2)^{\perp}. \tag{6.78}$$

The received signals are:

$$\begin{aligned} Y(2) &= h_{11}(2)v_1 + h_{12}(2)v_2 + (h_{11}(2) + h_{12}(2))K + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp} && (6.79)\\ &= L_1(v_1, v_2, K) + u_2\mathbf{H}_1(2)\mathbf{H}_2(2)^{\perp} && (6.80)\\ Z(2) &= h_{21}(2)v_1 + h_{22}(2)v_2 + (h_{21}(2) + h_{22}(2))K \\ &\triangleq L_2(v_1, v_2, K), && (6.81) \end{aligned}$$

where we have defined $L_1(v_1, v_2, K)$ and $L_2(v_1, v_2, K)$ as independent linear combinations of v_1, v_2 and K at receivers 1 and 2, respectively.

3) At time $t = 3$, $S(3) = \mathsf{NN}$: The transmitter transmits:

$$\mathbf{X}(3) = [L_1(v_1, v_2, K) \quad 0]^T . \tag{6.82}$$

The receivers get:

$$Y(3) = h_{11}(3)L_1(v_1, v_2, K) \tag{6.83}$$

$$Z(3) = h_{21}(3)L_1(v_1, v_2, K). \tag{6.84}$$

At the end of three slots, therefore, the received outputs can be summarized as:

$$\mathbf{Y} = \begin{bmatrix} u_1 \\ \alpha_1 L_1(v_1, v_2, K) + u_2 \\ L_1(v_1, v_2, K) \end{bmatrix}, \qquad \mathbf{Z} = \begin{bmatrix} K \\ L_2(v_1, v_2, K) \\ L_1(v_1, v_2, K) \end{bmatrix}.$$

Using $\mathbf{Y}$, receiver 1 can decode (u_1, u_2), while receiver 2 can decode (v_1, v_2) using $\mathbf{Z}$. The information leakage is only $o(\log P)$ as we show next.

Security guarantees:

The equivocation calculation follows similar to that of the scheme $S_1^{3/2}$. For the first user's symbols $\underline{\mathbf{u}} = (u_1, u_2)$, we have,

$$I(\underline{\mathbf{u}}; \mathbf{Z}|\mathbf{H}) = I(u_1, u_2; \mathbf{Z}|\mathbf{H}) \tag{6.85}$$

$$= I(u_1; \mathbf{Z}|\mathbf{H}) \tag{6.86}$$

$$\leq I(u_1; K|\mathbf{H}) \tag{6.87}$$

$$= o(\log P), \tag{6.88}$$

where (6.86) follows from the fact that $\mathbf{Z}$ does not have any term involving u_2, and (6.87) follows from the Markov chain $u_1 \rightarrow K \rightarrow \mathbf{Z}$.

For the second user's symbols, the information leakage at the first receiver is:

$$I(\underline{\mathbf{v}}; \mathbf{Y}|\mathbf{H}) \leq I(v_1, v_2; L_1(v_1, v_2, K)|\mathbf{H}) \tag{6.89}$$

$$= h(L_1(v_1, v_2, K)|\mathbf{H}) - h(L_1(v_1, v_2, K)|v_1, v_2, \mathbf{H}) \tag{6.90}$$

$$\leq \log P - h(K|v_1, v_2, \mathbf{H}) + o(\log P) \tag{6.91}$$

$$= \log P - h(K|\mathbf{H}) + o(\log P) \tag{6.92}$$

$$= \log P - \log P + o(\log P) \tag{6.93}$$

$$= o(\log P), \tag{6.94}$$

where (6.89) follows from the Markov chain $(v_1, v_2) \rightarrow L_1(v_1, v_2, K) \rightarrow \mathbf{Y}$.

6.4.4.2 Scheme $S_2^{4/3}$

We now present the scheme $S_2^{4/3}$ which uses the states $\mathsf{PN}, \mathsf{NP}, \mathsf{DD}$ with fractions $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ to achieve $(d_1, d_2) = (\frac{2}{3}, \frac{2}{3})$.

In this case we will send 4 symbols to each user in 6 time slots. Let $\underline{\mathbf{u}} = (u_1, u_2, u_3, u_4)$ and $\underline{\mathbf{v}} = (v_1, v_2, v_3, v_4)$ be the symbols intended for the first and second users, respectively. Fig. 6.7 shows the scheme. It is as follows:

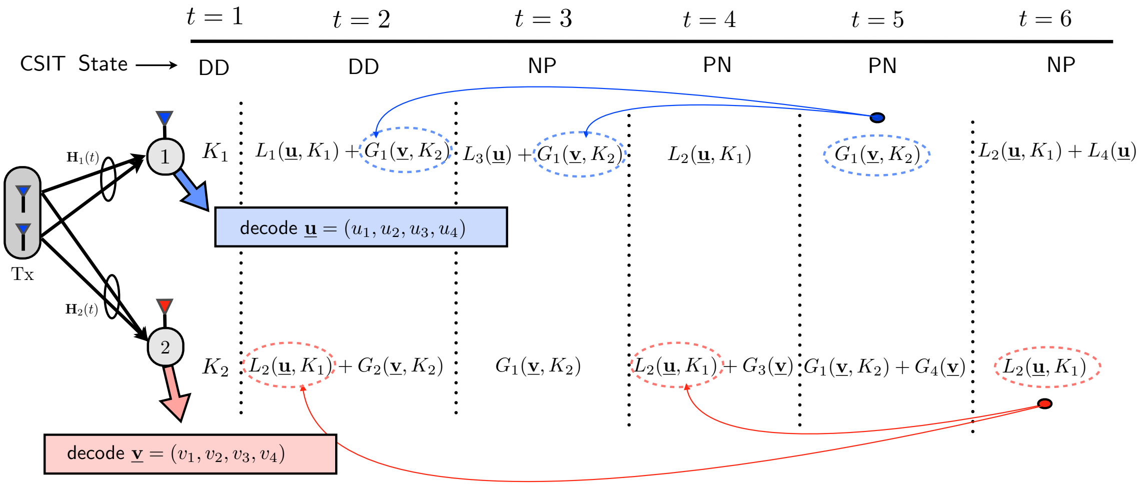

$t=1$
$t=2$
$t=3$
$t=4$
$t=5$
$t=6$
CSIT State
DD
DD
NP
PN
PN
NP
$\mathbf{H}_1(t)$
$\mathbf{H}_2(t)$
Tx
1
2
K_1
$L_1(\underline{\mathbf{u}}, K_1) + G_1(\underline{\mathbf{v}}, K_2)$
$L_3(\underline{\mathbf{u}}) + G_1(\underline{\mathbf{v}}, K_2)$
$L_2(\underline{\mathbf{u}}, K_1)$
$G_1(\underline{\mathbf{v}}, K_2)$
$L_2(\underline{\mathbf{u}}, K_1) + L_4(\underline{\mathbf{u}})$
decode $\underline{\mathbf{u}} = (u_1, u_2, u_3, u_4)$
K_2
$L_2(\underline{\mathbf{u}}, K_1) + G_2(\underline{\mathbf{v}}, K_2)$
$G_1(\underline{\mathbf{v}}, K_2)$
$L_2(\underline{\mathbf{u}}, K_1) + G_3(\underline{\mathbf{v}})$
$G_1(\underline{\mathbf{v}}, K_2) + G_4(\underline{\mathbf{v}})$
$L_2(\underline{\mathbf{u}}, K_1)$
decode $\underline{\mathbf{v}} = (v_1, v_2, v_3, v_4)$

Figure 6.7: Achieving sum s.d.o.f. $\frac{4}{3}$ using $S_2^{4/3}$.

1) At time $t = 1$, $S(1) = \mathsf{DD}$: In this slot, the transmitter sends artificial noise symbols to create keys that can be used in later slots. The channel input is

$$\mathbf{X}(1) = [q_1 \quad q_2]^T, \tag{6.95}$$

where q_1 and q_2 are i.i.d. as $\mathcal{CN}(0, P)$. The received signals are:

$$Y(1) = h_{11}(1)q_1 + h_{12}(1)q_2 \triangleq K_1 \tag{6.96}$$

$$Z(1) = h_{21}(1)q_1 + h_{22}(1)q_2 \triangleq K_2. \tag{6.97}$$

Due to delayed CSIT, the transmitter learns K_1 and K_2 and uses them in the next time slots.

2) At time $t = 2$, $S(2) = \mathsf{DD}$: In this slot, the transmitter sends:

$$\mathbf{X}(2) = [u_1 + u_2 + v_3 + v_4 + K_1 \quad v_1 + v_2 + u_3 + u_4 + K_2]^T. \tag{6.98}$$

The received signals are:

$$
\begin{aligned}
Y(2) &= h_{11}(2)(u_1+u_2+v_3+v_4+K_1)+h_{12}(2)(v_1+v_2+u_3+u_4+K_2) && (6.99)\\
&\triangleq L_1(\underline{\mathbf{u}},K_1)+G_1(\underline{\mathbf{v}},K_2) && (6.100)\\
Z(2) &= h_{21}(2)(u_1+u_2+v_3+v_4+K_1)+h_{22}(2)(v_1+v_2+u_3+u_4+K_2) && (6.101)\\
&\triangleq L_2(\underline{\mathbf{u}},K_1)+G_2(\underline{\mathbf{v}},K_2). && (6.102)
\end{aligned}
$$

Note that since K_1 (or K_2) is known at the first (or second) receiver, it can be removed. The unintended symbols remain buried in the artificial noise, ensuring security. Also, if G_1 (or L_2) could be sent to the second (or first) receiver, it would provide a linear combination of the intended symbols that is linearly independent of G_2 (or L_1). This is what we will do in the third and fourth time slots.

3) At time $t=3$, $S(3)=\mathsf{NP}$: In this state, the transmitter knows $\mathbf{H}_2$ perfectly. It sends,

$$
\mathbf{X}(3)=[G_1(\underline{\mathbf{v}},K_2) \quad 0]^T+L_3(\underline{\mathbf{u}})\mathbf{H}_2(3)^{\perp}, \qquad (6.103)
$$

where L_3 is linearly independent of both L_1 and L_2. The received signals are:

$$
\begin{aligned}
Y(3) =& h_{11}(3)G_1(\underline{\mathbf{v}},K_2)+L_3(\underline{\mathbf{u}})\mathbf{H}_1(3)\mathbf{H}_2(3)^{\perp} && (6.104)\\
Z(3) =& h_{21}(3)G_1(\underline{\mathbf{v}},K_2). && (6.105)
\end{aligned}
$$

4) At time $t=4$, $S(4)=\mathsf{PN}$: In this state, the transmitter knows $\mathbf{H}_1(4)$

perfectly. It sends,

$$\mathbf{X}(4) = [L_2(\underline{\mathbf{u}}, K_1) \quad 0]^T + G_3(\underline{\mathbf{v}})\mathbf{H}_1(4)^{\perp}, \tag{6.106}$$

where G_3 is linearly independent of both G_1 and G_2. The received signals are:

$$Y(4) = h_{11}(4)L_2(\underline{\mathbf{u}}, K_1) \tag{6.107}$$

$$Z(4) = h_{21}(4)L_2(\underline{\mathbf{u}}, K_1) + G_3(\underline{\mathbf{v}})\mathbf{H}_2(4)\mathbf{H}_1(4)^{\perp}. \tag{6.108}$$

Now note that if we could supply G_1 and L_2 to the first and second receivers, respectively, both receivers will end up with 3 linearly independent combinations of their intended symbols. Thus, in the next two slots, the transmitter will supply G_1 and L_2 to the first and second receivers, respectively, as well as send one more linearly independent combination of the intended information symbols to each receiver.

5) At time $t = 5$, $S(5) = \mathsf{PN}$: In this state, the transmitter knows $\mathbf{H}_1(5)$ perfectly. It sends,

$$\mathbf{X}(5) = [G_1(\underline{\mathbf{v}}, K_2) \quad 0]^T + G_4(\underline{\mathbf{v}})\mathbf{H}_1(5)^{\perp}. \tag{6.109}$$

The receivers receive:

$$Y(5) = h_{11}(5)G_1(\underline{\mathbf{v}}, K_2) \tag{6.110}$$

$$Z(5) = h_{21}(5)G_1(\underline{\mathbf{v}}, K_2) + G_4(\underline{\mathbf{v}})\mathbf{H}_2(5)\mathbf{H}_1(5)^{\perp}. \tag{6.111}$$

6) At time $t = 6$, $S(6) = \mathsf{NP}$: Now the transmitter knows $\mathbf{H}_2(6)$ perfectly, and it sends:

$$\mathbf{X}(6) = [L_2(\underline{\mathbf{u}}, K_1) \quad 0] + L_4(\underline{\mathbf{u}})\mathbf{H}_2(6)^{\perp}. \tag{6.112}$$

The received signals are:

$$Y(6) = h_{11}(6)L_2(\underline{\mathbf{u}}, K_1) + L_4(\underline{\mathbf{u}})\mathbf{H}_1(6)\mathbf{H}_2(6)^{\perp} \tag{6.113}$$

$$Z(6) = h_{21}(6)L_2(\underline{\mathbf{u}}, K_1). \tag{6.114}$$

Let us summarize the received signals at each receiver after these 6 time slots:

$$\mathbf{Y} = \begin{bmatrix} K_1 \\ L_1(\underline{\mathbf{u}}, K_1) + G_1(\underline{\mathbf{v}}, K_2) \\ \alpha_1 G_1(\underline{\mathbf{v}}, K_2) + L_3(\underline{\mathbf{u}}) \\ L_2(\underline{\mathbf{u}}, K_1) \\ G_1(\underline{\mathbf{v}}, K_2) \\ \alpha_2 L_2(\underline{\mathbf{u}}, K_1) + L_4(\underline{\mathbf{u}}) \end{bmatrix}, \qquad \mathbf{Z} = \begin{bmatrix} K_2 \\ L_2(\underline{\mathbf{u}}, K_1) + G_2(\underline{\mathbf{v}}, K_2) \\ G_1(\underline{\mathbf{v}}, K_2) \\ \beta_1 L_2(\underline{\mathbf{u}}, K_1) + G_3(\underline{\mathbf{v}}) \\ \beta_2 G_1(\underline{\mathbf{v}}, K_2) + G_4(\underline{\mathbf{v}}) \\ L_2(\underline{\mathbf{u}}, K_1) \end{bmatrix}.$$

The information symbols can now be decoded at the intended receivers from these observations. Also the leakage of information is only $o(\log P)$, as we prove next.

Security guarantees:

For the first user's symbols $\underline{\mathbf{u}} = (u_1, u_2, u_3, u_4)$, we have,

$$
\begin{aligned}
I(\underline{\mathbf{u}}; \mathbf{Z}|\mathbf{H}) \leq & I(\underline{\mathbf{u}}; L_2(\underline{\mathbf{u}}, K_1)|\mathbf{H}) && (6.115)\\
= & h(L_2(\underline{\mathbf{u}}, K_1)|\mathbf{H}) - h(L_2(\underline{\mathbf{u}}, K_1)|\underline{\mathbf{u}}, \mathbf{H}) && (6.116)\\
\leq & \log P - h(K_1|\underline{\mathbf{u}}, \mathbf{H}) + o(\log P) && (6.117)\\
= & \log P - h(K_1|\mathbf{H}) + o(\log P) && (6.118)\\
= & \log P - \log P + o(\log P) && (6.119)\\
= & o(\log P), && (6.120)
\end{aligned}
$$

where (6.115) follows from the Markov chain $U \rightarrow L_2(\underline{\mathbf{u}}, K_1) \rightarrow \mathbf{Z}$.

For the second user's symbols, the information leakage at the first receiver is:

$$
\begin{aligned}
I(\underline{\mathbf{v}}; \mathbf{Y}|\mathbf{H}) \leq & I(\underline{\mathbf{v}}; G_1(\underline{\mathbf{v}}, K_2)|\mathbf{H}) && (6.121)\\
= & h(G_1(\underline{\mathbf{v}}, K_2)|\mathbf{H}) - h(G_1(\underline{\mathbf{v}}, K_2)|\underline{\mathbf{v}}, \mathbf{H}) && (6.122)\\
\leq & \log P - h(K_2|\underline{\mathbf{v}}, \mathbf{H}) + o(\log P) && (6.123)\\
= & \log P - h(K_2|\mathbf{H}) + o(\log P) && (6.124)\\
= & \log P - \log P + o(\log P) && (6.125)\\
= & o(\log P), && (6.126)
\end{aligned}
$$

where (6.89) follows from the Markov chain $\underline{\mathbf{v}} \rightarrow G_1(\underline{\mathbf{v}}, K_2) \rightarrow \mathbf{Y}$.

6.4.5 Schemes Achieving Sum s.d.o.f. of 1

6.4.5.1 Scheme S_1^1

We first recap the scheme S_1^1 which uses the state DD to achieve $(d_1, d_2) = (\frac{1}{2}, \frac{1}{2})$. This scheme was presented in [15]. The scheme was used to transmit 2 information symbols to each receiver in 4 time slots. At $t = 1$, the transmitter sends artificial noise symbols using both antennas. The received signals act as keys K_1 and K_2 for the respective users 1 and 2. Since there is delayed CSIT, the transmitter can reconstruct these keys and use them in the next slots. At $t = 2$, the transmitter sends the two information symbols (u_1, u_2) intended for the first receiver linearly combined with the first user's key. Thus, the first user can retrieve a linear combination of just its intended symbols. However, the second user gets a linear combination $L(u_1, u_2, K_1)$. Due to delayed CSIT however, the transmitter can reconstruct L. In the third slot, the roles of the receivers are reversed and the transmitter sends the second user's symbols (v_1, v_2) linearly combined with the second user's key K_2. This allows the second user to retrieve a linear combination of just its information symbol, which however remain secure at the first user, which receives $G(v_1, v_2, K_2)$. In the fourth slot, the transmitter sends a linear combination of L and G. Essentially this provides the first user with L, from which it can eliminate K_1 to get another independent linear combination of (u_1, u_2). A similar situation takes place at the second user. Finally, each user has two linearly independent combinations of two symbols and thus can decode the information symbols intended for it. The information leakage is only $o(\log P)$, as shown in [15].

6.4.5.2 Scheme S_2^1

In this sub-section, we present the scheme S_2^1 which uses the states $(\mathsf{DD}, \mathsf{NN})$ with fractions $(\frac{1}{2}, \frac{1}{2})$ to achieve $(d_1, d_2) = (\frac{1}{2}, \frac{1}{2})$.

The scheme S_1^1 requires delayed CSIT from at least one user for the first 3 time slots. We need to modify this scheme to ensure that delayed CSIT is required only for 2 of the 4 time slots. Fig. 6.8 shows the new scheme. It is as follows:

1) At time $t = 1$, $S(1) = \mathsf{DD}$: The strategy in this slot is the same as in the scheme S_1^1. In this slot, the transmitter sends artificial noise symbols to create keys that can be used in later slots. The channel input is

$$\mathbf{X}(1) = [q_1 \quad q_2]^T, \tag{6.127}$$

where q_1 and q_2 are i.i.d. as $\mathcal{CN}(0, P)$. The received signals are:

$$Y(1) = h_{11}(1)q_1 + h_{12}(1)q_2 \triangleq K_1 \tag{6.128}$$

$$Z(1) = h_{21}(1)q_1 + h_{22}(1)q_2 \triangleq K_2. \tag{6.129}$$

Due to delayed CSIT, the transmitter learns K_1 and K_2 and uses them in the next time slots.

2) At time $t = 2$, $S(2) = \mathsf{DD}$: Instead of sending only the first user's symbols as in scheme S_1^1, the transmitter now sends linear combination of both users' symbols.

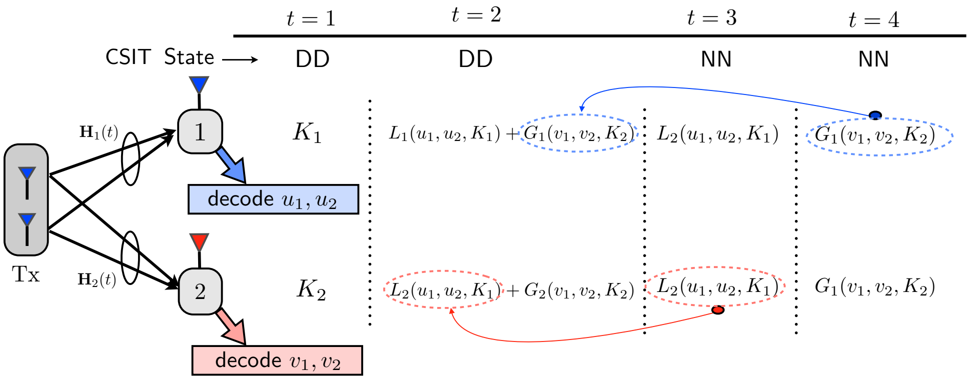


Figure 6.8: Achieving sum s.d.o.f. of 1 using S_2^1.

It sends:

$$\mathbf{X}(2) = [u_1 + v_1 + K_1 \quad u_2 + v_2 + K_2]^T . \tag{6.130}$$

The received signals are:

$$\begin{aligned} Y(2) =& h_{11}(u_1 + v_1 + K_1) + h_{12}(u_2 + v_2 + K_2) && (6.131) \\ \triangleq& L_1(u_1, u_2, K_1) + G_1(v_1, v_2, K_2) && (6.132) \\ Z(2) =& h_{21}(u_1 + v_1 + K_1) + h_{22}(u_2 + v_2 + K_2) && (6.133) \\ \triangleq& L_2(u_1, u_2, K_1) + G_2(v_1, v_2, K_2). && (6.134) \end{aligned}$$

We notice that if L_2 and G_1 could be provided to both users, each user can get 2 linear combinations of the symbols intended for it and hence decode both symbols. Hence, in the remaining two slots, we will transmit L_2 and G_1 to both users and this will not require any CSIT from any user.

3) At time $t = 3$, $S(3) = \mathsf{NN}$: The transmitter does not have any CSIT. It

sends:

$$\mathbf{X}(3) = \left[L_2(u_1, u_2, K_1) \quad 0\right]^T . \tag{6.135}$$

The received signals are:

$$Y(3) = h_{11}(3)L_2(u_1, u_2, K_1) \tag{6.136}$$

$$Z(3) = h_{21}(3)L_2(u_1, u_2, K_1). \tag{6.137}$$

4) At time $t = 4$, $S(4) = \mathsf{NN}$: The transmitter sends:

$$\mathbf{X}(4) = \left[G_1(v_1, v_2, K_2) \quad 0\right]^T . \tag{6.138}$$

The received signals are:

$$Y(4) = h_{11}(4)G_1(v_1, v_2, K_2) \tag{6.139}$$

$$Z(4) = h_{21}(4)G_1(v_1, v_2, K_2). \tag{6.140}$$

Thus, at the end of 4 slots the received signals may be summarized as:

$$\mathbf{Y} = \begin{bmatrix} K_1 \\ L_1(u_1, u_2, K_1) + G_1(v_1, v_2, K_2) \\ L_2(u_1, u_2, K_1) \\ G_1(v_1, v_2, K_2) \end{bmatrix}, \quad \mathbf{Z} = \begin{bmatrix} K_2 \\ L_2(u_1, u_2, K_1) + G_2(v_1, v_2, K_2) \\ L_2(u_1, u_2, K_1) \\ G_1(v_1, v_2, K_2) \end{bmatrix}$$

Clearly, user 1 can decode (u_1, u_2) and user 2 can get (v_1, v_2). The information leakage is at most $o(\log P)$ as we show below.

Security guarantees:

For the first user's symbols $\underline{\mathbf{u}} = (u_1, u_2)$, we have,

$$I(\underline{\mathbf{u}}; \mathbf{Z}|\mathbf{H}) \leq I(\underline{\mathbf{u}}; L_2(\underline{\mathbf{u}}, K_1)|\mathbf{H}) \tag{6.141}$$

$$= h(L_2(\underline{\mathbf{u}}, K_1)|\mathbf{H}) - h(L_2(\underline{\mathbf{u}}, K_1)|\underline{\mathbf{u}}, \mathbf{H}) \tag{6.142}$$

$$\leq \log P - h(K_1|\underline{\mathbf{u}}, \mathbf{H}) + o(\log P) \tag{6.143}$$

$$= \log P - h(K_1|\mathbf{H}) + o(\log P) \tag{6.144}$$

$$= \log P - \log P + o(\log P) \tag{6.145}$$

$$= o(\log P), \tag{6.146}$$

where (6.141) follows from the Markov chain $U \rightarrow L_2(\underline{\mathbf{u}}, K_1) \rightarrow \mathbf{Z}$.

For the second user's symbols $\underline{\mathbf{v}} = (v_1, v_2)$, the information leakage at the first receiver is:

$$I(\underline{\mathbf{v}}; \mathbf{Y}|\mathbf{H}) \leq I(\underline{\mathbf{v}}; G_1(\underline{\mathbf{v}}, K_2)|\mathbf{H}) \tag{6.147}$$

$$= h(G_1(\underline{\mathbf{v}}, K_2)|\mathbf{H}) - h(G_1(\underline{\mathbf{v}}, K_2)|\underline{\mathbf{v}}, \mathbf{H}) \tag{6.148}$$

$$\leq \log P - h(K_2|\underline{\mathbf{v}}, \mathbf{H}) + o(\log P) \tag{6.149}$$

$$= \log P - h(K_2|\mathbf{H}) + o(\log P) \tag{6.150}$$

$$= \log P - \log P + o(\log P) \tag{6.151}$$

$$= o(\log P), \tag{6.152}$$

where (6.147) follows from the Markov chain $\underline{\mathbf{v}} \rightarrow G_1(\underline{\mathbf{v}}, K_2) \rightarrow \mathbf{Y}$.

6.4.5.3 Scheme S_3^1

We next present a novel scheme S_3^1 which uses the states $(\mathsf{DN}, \mathsf{ND})$ with fractions $(\frac{1}{2}, \frac{1}{2})$ to achieve $(d_1, d_2) = (\frac{1}{2}, \frac{1}{2})$. In particular, we present a scheme which achieves the s.d.o.f. pair $(d_1, d_2) = \left(\frac{2n}{4n+1}, \frac{2n}{4n+1}\right)$ as a function of the block length n. Taking the limit $n \rightarrow \infty$ yields the s.d.o.f. pair $\left(\frac{1}{2}, \frac{1}{2}\right)$.

The scheme is shown in Fig. 6.9. Unlike all the other schemes in this chapter where the optimal sum s.d.o.f. can be achieved within a finite number of time slots, this scheme cannot achieve sum s.d.o.f. of 1 in a finite number of slots. Indeed, there does not exist a scheme that can achieve sum s.d.o.f. of 1 in finitely many slots. To see why, assume that there exists such a scheme with n slots. In this scheme, states DN and ND occur for equal fractions of time; thus, $\lambda_D = \lambda_N = \frac{1}{2}$. Now, note that the delayed CSIT in the last slot cannot be used; thus, the scheme would work equally well if the last slot were NN instead of DN or ND. However, changing the state in the last slot to NN would imply $\lambda_D < \frac{1}{2}$, which in turn implies that $d_1 + d_2 < 1$ from (6.18). Thus, no scheme that uses only a finite number of slots can achieve a sum s.d.o.f. of 1.

Here we provide an asymptotic scheme that achieves a sum s.d.o.f. of $\frac{4n}{4n+1}$ in n slots. As the number of slots $n \rightarrow \infty$, the sum s.d.o.f. approaches 1. We wish to send $2n$ symbols to each receiver in $4n + 1$ time slots. The scheme involves transmission in 4 blocks where the first 3 blocks, say A, B and C each have n time slots, while

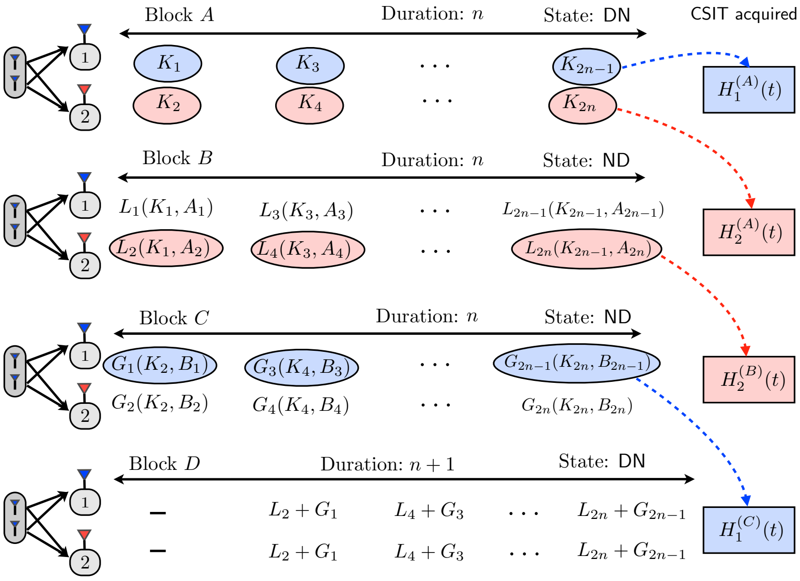


Figure 6.9: Achieving sum s.d.o.f. of $4n/(4n+1)$ using scheme S_3^1.

the last block D has $n+1$ slots; thus, a total of $4n+1$ time slots are required in the scheme. The scheme is as follows:

1) In block A, $S(t) = \mathsf{DN}$: In each time slot i in block A, the transmitter generates two artificial noise symbols and sends them using its two antennas. The receivers receive different linear combinations of the two artificial noise symbols K_{2i-1} and K_{2i} as shown in Fig. 6.9. Due to delayed CSIT from the first user, the transmitter can reconstruct each of $K_{2i-1}, i = 1, \ldots,$ by the end of block A. Thus, they can act as shared keys between the transmitter and the first receiver. However, since the second receiver does not feedback any CSIT (due to the fact that the state in the block is DN), the transmitter cannot reconstruct the observations of the second receiver at the end of block A.

2) In block B, $S(t) = \mathsf{ND}$: At the beginning of this slot, the transmitter has the keys $K_{2i-1}, i = 1, \ldots, n$ shared with the first user. It uses these keys to send information intended for the first user. It creates $2n$ linearly independent

combinations of the $2n$ symbols intended for the first receiver: $a_1, \ldots, a_{2n}$. In slot i, it transmits

$$\mathbf{X}^B(i) = \left[a_{2i-1} + K_{2i-1} \quad a_{2i} + K_{2i-1}\right]^T . \tag{6.153}$$

The first and second receivers receive linearly independent combinations given by $L_{2i-1}(A_{2i-1}, K_{2i-1})$ and $L_{2i}(A_{2i}, K_{2i-1})$ in slot i, where A_i denotes the ith linear combination of the first user's symbols, as shown in Fig. 6.9. Since the state is ND, the second user provides delayed CSIT to the transmitter. In the ith slot, the second user feeds back $\mathbf{H}_2^A(i)$, that is, the channel coefficients of the second user in slot i within block A. *Note that this is unlike any other achievable scheme we have encountered so far; in all other schemes, the receiver feeds back the channel coefficients of the current slot which appears as delayed CSIT at the beginning of the next slot.* Thus, at the end of slot B, the transmitter has all the channel coefficients of the second user from block A; thus, it can reconstruct the outputs of the second receiver in block A, $K_{2i}, i = 1, \ldots, n$, which now act as shared keys between the transmitter and the second receiver.

3) In block C, $S(t) = \mathsf{ND}$: At the beginning of this slot, the transmitter has the keys $K_{2i}, i = 1, \ldots, n$ shared with the second user. It uses these keys to send information securely to the second user. It creates $2n$ linearly independent combinations of the $2n$ symbols intended for the second receiver: $b_1, \ldots, a_{2n}$. In slot

i, it transmits

$$\mathbf{X}^C(i) = [b_{2i-1} + K_{2i-1} \quad b_{2i} + K_{2i-1}]^T \,. \tag{6.154}$$

The first and second receivers receive linearly independent combinations $G_{2i-1}(B_{2i-1}, K_{2i})$ and $G_{2i}(B_{2i}, K_{2i})$ in slot i, where B_i denotes the ith linear combination of the second user's symbols, as shown in Fig. 6.9. As CSIT, in the ith slot, the second user feeds back the channel coefficients $\mathbf{H}_2^B(i)$, which allows the transmitter to reconstruct $L_{2i}(A_{2i}, K_{2i-1})$. Note that now if $L_{2i}(A_{2i}, K_{2i-1})$ and $G_{2i-1}(B_{2i-1}, K_{2i})$ could be exchanged, each of the receivers would receive $2n$ linear combinations of the $2n$ symbols intended for it, thus, allowing both receivers to decode their own messages. However, $G_{2i-1}(B_{2i-1}, K_{2i})$ is not known to the transmitter yet, since the first user has not fed back its channel in block C. This CSIT will be obtained in the next block.

4) In block D, $S(t) = \mathsf{ND}$: The transmitter wishes to send the symbols $L_{2i}(A_{2i}, K_{2i-1}) + G_{2i-1}(B_{2i-1}, K_{2i}), i = 1, \ldots, n$, in this block. To do so, the transmitter does not transmit anything in the first slot in this block. It only acquires the channel coefficients $\mathbf{H}_1^C(i)$ from the first user who is supplying delayed CSIT in this block. In the ith slot, $i = 1, \ldots, n$, the transmitter acquires the channel coefficients $\mathbf{H}_1^C(i)$ and transmits:

$$\mathbf{X}^D(i) = [L_{2i-2}(A_{2i-2}, K_{2i-3}) + G_{2i-3}(B_{2i-3}, K_{2i-2}) \quad 0]^T \,, \quad i = 2, \ldots, n+1. \tag{6.155}$$

The first user can now obtain $L_{2i-1}(A_{2i-1}, K_{2i-1})$ and $L_{2i}(A_{2i}, K_{2i-1})$ for every $i = 1, \ldots, n$, while the second user obtains $G_{2i-1}(B_{2i-1}, K_{2i})$ and $G_{2i}(B_{2i}, K_{2i})$ for $i = 1, \ldots, n$. Now by eliminating the respective keys, each user can decode the $2n$ symbols intended for it from the $2n$ linearly independent combinations available to it. Also the keys ensure the confidentiality, and the information leakage is only $o(\log P)$, as we show next.

Security guarantees:

Let $\underline{\mathbf{u}} = (a_1, \ldots, a_{2n})$ and $\underline{\mathbf{v}} = (b_1, \ldots, b_{2n})$ be the symbols intended for users 1 and 2, respectively. The leakage of $\underline{\mathbf{u}}$ at user 2 is given by

$$I(\underline{\mathbf{u}}; \mathbf{Z}|\mathbf{H}) \leq I(\underline{\mathbf{u}}; \{L_{2i}(A_{2i}, K_{2i-1})\}_{i=1}^{n} |\mathbf{H}) \tag{6.156}$$

$$= h(\{L_{2i}(A_{2i}, K_{2i-1})\}_{i=1}^{n} |\mathbf{H}) - h(\{L_{2i}(A_{2i}, K_{2i-1})\}_{i=1}^{n} |\underline{\mathbf{u}}, \mathbf{H}) \tag{6.157}$$

$$\leq n \log P - h(\{K_{2i-1}\}_{i=1}^{n} |\mathbf{H}) + o(\log P) \tag{6.158}$$

$$= n \log P - n \log P + o(\log P) \tag{6.159}$$

$$= o(\log P), \tag{6.160}$$

where (6.156) follows due to the Markov chain $\underline{\mathbf{u}} \rightarrow \{L_{2i}(A_{2i}, K_{2i-1})\}_{i=1}^{n} \rightarrow \mathbf{Z}$, and (6.159) follows from the fact that $\{K_{2i-1}\}_{i=1}^{n}$ are mutually independent and each is distributed as $\mathcal{N}(0, P)$.

Similarly, for the second user's symbols, the leakage at the first user is given by,

$$I(\underline{\mathbf{v}}; \mathbf{Y}|\mathbf{H}) \leq I(\underline{\mathbf{v}}; \{G_{2i-1}(B_{2i-1}, K_{2i})\}_{i=1}^{n} |\mathbf{H}) \tag{6.161}$$

$$=h(\{G_{2i-1}(B_{2i-1},K_{2i})\}_{i=1}^{n}|\mathbf{H})-h(\{G_{2i-1}(B_{2i-1},K_{2i})\}_{i=1}^{n}|\underline{\mathbf{v}},\mathbf{H}) \tag{6.162}$$

$$\leq n\log P-h(\{K_{2i}\}_{i=1}^{n}|\mathbf{H})+o(\log P) \tag{6.163}$$

$$=n\log P-n\log P+o(\log P) \tag{6.164}$$

$$=o(\log P), \tag{6.165}$$

where (6.161) follows due to the Markov chain $\underline{\mathbf{v}}\rightarrow\{G_{2i-1}(B_{2i-1},K_{2i})\}_{i=1}^{n}\rightarrow\mathbf{Y}$, and (6.164) follows from the fact that $\{K_{2i}\}_{i=1}^{n}$ are mutually independent and each is distributed as $\mathcal{N}(0,P)$.

6.4.6 Schemes Achieving Sum s.d.o.f. of 2/3

6.4.6.1 Scheme $S_1^{2/3}$

The scheme $S_1^{2/3}$ uses the state DD to achieve $(d_1,d_2)=(\frac{2}{3},0)$. Such a scheme was presented in [15]. The scheme can be summarized as follows. At time $t=1$, the transmitter sends two artificial noise symbols using its two antennas. Each user receives a different linear combination of the noise symbols and they act as keys. Let K_1 and K_2 be the keys at receivers 1 and 2, respectively. Due to delayed CSIT, the transmitter can reconstruct K_1. At time $t=2$, the transmitter sends the two symbols intended for the first receiver (u_1,u_2), linearly combined with K_1. Receiver 1 can remove K_1 from its received signal and get one linear combination of (u_1,u_2) at the end of this slot. The second user receives a linear combination of u_1,u_2 and

K_1, say $L(u_1, u_2, K_1)$; however, not knowing K_1, it cannot decode the information symbols. Due to delayed CSIT, the transmitter learns L and transmits it in $t = 3$. The second receiver gets no new information but the first receiver can get a second linear combination of (u_1, u_2) by eliminating K_1 from L. This allows receiver 1 to decode (u_1, u_2), while the information leakage to receiver 2 is $o(\log P)$.

6.4.6.2 Scheme $S_2^{2/3}$

The scheme $S_2^{2/3}$ uses the states $(\mathsf{DD}, \mathsf{NN})$ with fractions $(\frac{2}{3}, \frac{1}{3})$ to achieve $(d_1, d_2) = (\frac{2}{3}, 0)$. We note that in scheme $S_1^{2/3}$, the delayed CSIT in slot $t = 3$ is not required. Thus, the scheme can work with the states $(\mathsf{DD}, \mathsf{NN})$ with fractions $(\frac{2}{3}, \frac{1}{3})$, and we call this $S_2^{2/3}$.

6.4.6.3 Scheme $S_3^{2/3}$

Finally, the scheme $S_3^{2/3}$ uses the states $(\mathsf{DN}, \mathsf{ND}, \mathsf{NN})$ with fractions $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ to achieve $(d_1, d_2) = (\frac{2}{3}, 0)$. We notice that instead of having DD state in the first two slots, it suffices to have DN in the first slot (since the transmitter does not need K_2) and ND in the second slot (since the transmitter only needs to reconstruct the second user's received signal L). Thus, it suffices to have the states $(\mathsf{DN}, \mathsf{ND}, \mathsf{NN})$ with fractions $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ for the scheme to work, and we call this $S_3^{2/3}$.

6.5 Achievability

Now that we have all the required constituent schemes summarized in Table 6.1, we proceed to show how these schemes can be combined to achieve the region stated in Theorem 1. We restate the region of Theorem 1 here for convenience:

$$d_1 \leq \min\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}, 1-\lambda_{NN}\right) \tag{6.166}$$

$$d_2 \leq \min\left(\frac{2+2\lambda_P-\lambda_{PP}}{3}, 1-\lambda_{NN}\right) \tag{6.167}$$

$$3d_1+d_2 \leq 2+2\lambda_P \tag{6.168}$$

$$d_1+3d_2 \leq 2+2\lambda_P \tag{6.169}$$

$$d_1+d_2 \leq 2(\lambda_P+\lambda_D). \tag{6.170}$$

We classify this region into two cases:

- Case A: in which d_1+d_2 bound of (6.170) is inactive. This corresponds to the condition

$$1+\lambda_P \leq 2\lambda_P+2\lambda_D, \tag{6.171}$$

which is equivalent to

$$\lambda_N \leq \lambda_D. \tag{6.172}$$

- Case B: in which $d_1 + d_2$ bound of (6.170) is active which corresponds to

$$\lambda_N > \lambda_D. \tag{6.173}$$

In the next two sub-sections, we present the achievability for each of these cases separately.

6.5.1 Achievability for Case A: $\lambda_D \geq \lambda_N$

For Case A, the s.d.o.f. region reduces to:

$$d_1 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right) \tag{6.174}$$

$$d_2 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right) \tag{6.175}$$

$$3d_1 + d_2 \leq 2 + 2\lambda_P \tag{6.176}$$

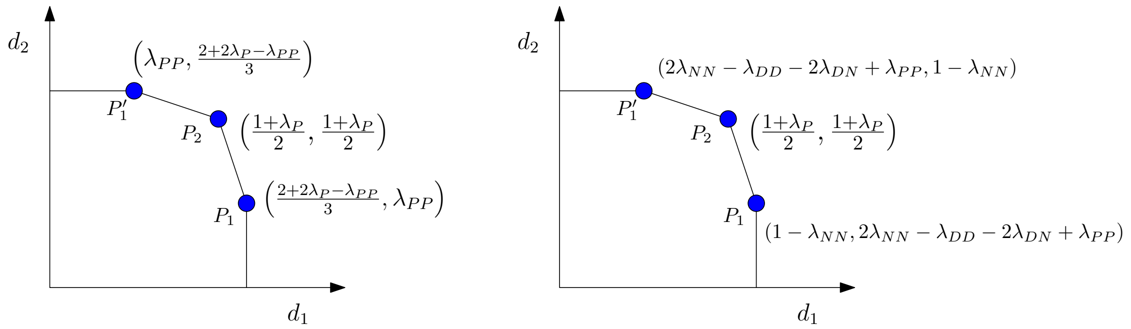
$$d_1 + 3d_2 \leq 2 + 2\lambda_P. \tag{6.177}$$

Depending on which single user bound is active, we consider two cases:

1. $\frac{2+2\lambda_P-\lambda_{PP}}{3} \leq 1 - \lambda_{NN}$, which is equivalent to the condition $\lambda_{DD} + 2\lambda_{DN} \geq 2\lambda_{NN}$,

2. $\frac{2+2\lambda_P-\lambda_{PP}}{3} \geq 1 - \lambda_{NN}$, which is equivalent to the condition $\lambda_{DD} + 2\lambda_{DN} \leq 2\lambda_{NN}$.

As shown in Fig. 6.10, due to symmetry, it suffices to achieve the points P_1 and P_2 in each case.



(a) $\lambda_{DD} + 2\lambda_{DN} \geq 2\lambda_{NN}$.

(b) $\lambda_{DD} + 2\lambda_{DN} \leq 2\lambda_{NN}$.

Figure 6.10: s.d.o.f. regions in case A.

6.5.1.1 Achievability of Point P_1

We first show the achievability of the point P_1 in both cases. To do so, let us consider the two cases one by one:

1. $\lambda_{DD} + 2\lambda_{DN} \geq 2\lambda_{NN}$: In this case, the single user bounds are:

$$d_1 \leq \frac{2 + 2\lambda_P - \lambda_{PP}}{3} \tag{6.178}$$

$$d_2 \leq \frac{2 + 2\lambda_P - \lambda_{PP}}{3}. \tag{6.179}$$

As seen in Fig. 6.10a, the point P_1 is $\left(\frac{2+2\lambda_{\mathsf{P}}-\lambda_{\mathsf{PP}}}{3}, \lambda_{\mathsf{PP}}\right)$. To achieve this point, using the state PP, we achieve $(1,1)$, with $\mathsf{PD}, \mathsf{DP}, \mathsf{PN}, \mathsf{NP}$, we achieve the pair $(1,0)$ either through zero-forcing, or by transmitting artificial noise in a direction orthogonal to the first user's channel. For the states $(\mathsf{DD}, \mathsf{NN}) \sim (\frac{2}{3}, \frac{1}{3})$, and $(\mathsf{DN}, \mathsf{ND}, \mathsf{NN}) \sim (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, we achieve the pair $(\frac{2}{3}, 0)$ by using the schemes $S_2^{2/3}$ and $S_3^{2/3}$, respectively. Essentially, the NN state can be fully alternated with the DD state and the DN and ND states to achieve $\frac{2}{3}$ s.d.o.f. for user 1.

Time sharing yields the following s.d.o.f. pair:

$$\begin{aligned} d_2 &= \lambda_{PP} && (6.180) \\ d_1 &= \lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN} + \underbrace{\frac{2}{3}}_{S_2^{2/3}} (\lambda_{DD} + 2\lambda_{DN} + \lambda_{NN}) && (6.181) \\ &= 2\lambda_P - \lambda_{PP} + \frac{2}{3}(\lambda_{DD} + \lambda_{NN}) && (6.182) \\ &= 2\lambda_P - \lambda_{PP} + \frac{2}{3}(1 - 2\lambda_P + \lambda_{PP}) && (6.183) \\ &= \frac{2 + 2\lambda_P - \lambda_{PP}}{3}. && (6.184) \end{aligned}$$

2. $\lambda_{DD} + 2\lambda_{DN} \leq 2\lambda_{NN}$: In this case the single user bounds are:

$$d_1 \leq 1 - \lambda_{NN} \quad (6.185)$$

$$d_2 \leq 1 - \lambda_{NN}. \quad (6.186)$$

Again, we wish to achieve the point P_1 in Fig. 6.10b. The point P_1 is given by:

$$P_1 : (d_1, d_2) = (1 - \lambda_{NN}, \lambda_{PP} + (2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD})). \quad (6.187)$$

Here we consider two further subcases

- $\lambda_{NN} \leq \lambda_{DD} + \lambda_{DN}$: In this case, to achieve the point P_1, we first use up the full DN and ND states with a part of the NN state using scheme $S_3^{2/3}$. We alternate the remaining $(\lambda_{NN} - \lambda_{DN})$ duration of NN state with the DD state using two schemes: $S_2^{2/3}$ and S_2^1. Note that in this subcase, $0 \leq 2(\lambda_{DD} + \lambda_{DN} - \lambda_{NN}) \leq \lambda_{DD}$. We use the state DD for duration $2(\lambda_{DD} + \lambda_{DN} - \lambda_{NN})$ and state NN for duration $(\lambda_{DD} + \lambda_{DN} - \lambda_{NN})$ together using scheme $S_2^{2/3}$ to achieve the s.d.o.f. pair $\left(\frac{2}{3}, 0\right)$. The remaining $(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD})$ duration of the state NN is alternated with the remaining $(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD})$ duration of state DD using the scheme S_2^1 to achieve the s.d.o.f. pair $\left(\frac{1}{2}, \frac{1}{2}\right)$. The state PP allows us to achieve the s.d.o.f. pair $(1, 1)$ while the remaining states PD, DP, PN, and NP each achieves $(1, 0)$. Thus, by using time sharing, the s.d.o.f. pair is:

$$\begin{aligned} d_1 =& \lambda_{PP} + 1 \times 2\lambda_{PD} + 1 \times 2\lambda_{PN} + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3\lambda_{DN} \\ &+ \underbrace{\frac{2}{3}}_{S_2^{2/3}} \times 3(\lambda_{DD} + \lambda_{DN} - \lambda_{NN}) + \underbrace{\frac{1}{2}}_{S_2^1} \times 2(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}) \end{aligned} \tag{6.188}$$

$$=1 - \lambda_{NN} \tag{6.189}$$

$$\begin{aligned} d_2 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times 2(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}) \\ =& \lambda_{PP} + (2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}), \end{aligned} \tag{6.190}$$

which is precisely the point P_1.

- $\lambda_{NN} \geq \lambda_{DD} + \lambda_{DN}$: In this case, the state NN cannot be completely used with the states DD, DN and ND. But we note that $\lambda_D \geq \lambda_N$ implies that $\lambda_D \geq \lambda_{NN}$. We first use up the DN and ND states by alternating with the NN state using scheme $S_3^{2/3}$. A portion λ_{DD} of the remaining $(\lambda_{NN} - \lambda_{DN})$ duration of the NN state uses up the DD state in scheme S_2^1 achieving the pair $\left(\frac{1}{2}, \frac{1}{2}\right)$. The remaining $(\lambda_{NN} - \lambda_{DN} - \lambda_{DD})$ portion of the NN state is used with the PD and DP states through the scheme $S_1^{4/3}$ to achieve the pair $\left(\frac{2}{3}, \frac{2}{3}\right)$. For the remainder of the state PD, DP and the states PN, NP, we can achieve the pair $(1, 0)$, while $(1, 1)$ is achieved in the PP state. By time sharing, we get

$$\begin{aligned} d_1 =& \lambda_{PP} + 2\lambda_{PN} + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3\lambda_{DN} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3(\lambda_{NN} - \lambda_{DN} - \lambda_{DD}) \\ & + 2(\lambda_{PD} - \lambda_{NN} + \lambda_{DN} + \lambda_{DD}) + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} \qquad (6.191) \\ =& 1 - \lambda_{NN} \qquad (6.192) \\ d_2 =& \lambda_{PP} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3(\lambda_{NN} - \lambda_{DN} - \lambda_{DD}) + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} \qquad (6.193) \\ =& \lambda_{PP} + 2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}, \qquad (6.194) \end{aligned}$$

which is again the point P_1.

6.5.1.2 Achieving the Sum s.d.o.f. Achieving Point P_2

The point P_2 corresponds to:

$$P_2 : (d_1, d_2) = \left(\frac{1 + \lambda_P}{2}, \frac{1 + \lambda_P}{2} \right). \tag{6.195}$$

We rewrite the condition $\lambda_D \geq \lambda_N$ corresponding to case A as:

$$\lambda_{PD} + \lambda_{DD} \geq \lambda_{PN} + \lambda_{NN}. \tag{6.196}$$

From this condition it is not immediately clear how the constituent schemes should be jointly utilized. Hence we break this condition into three mutually exclusive cases:

1. Sub-case $A1$: $\lambda_{PD} \geq \lambda_{PN}$ and $\lambda_{DD} \geq \lambda_{NN}$,
2. Sub-case $A2$: $\lambda_{PD} \geq \lambda_{PN}$ and $\lambda_{DD} \leq \lambda_{NN}$,
3. Sub-case $A3$: $\lambda_{PD} \leq \lambda_{PN}$ and $\lambda_{DD} \geq \lambda_{NN}$.

Now, we consider these three sub-cases one by one:

Sub-case $A1$: $\lambda_{PD} \geq \lambda_{PN}$ and $\lambda_{DD} \geq \lambda_{NN}$. In this sub-case, the original condition $\lambda_D \geq \lambda_N$ is automatically satisfied. For this sub-case, it is clear that the states PN and NP can be fully alternated along with the PD and DP using scheme $S_2^{3/2}$ to achieve $\frac{3}{2}$ s.d.o.f. The remaining fraction of time for PD (and DP) is hence: $\lambda_{PD} - \lambda_{PN}$. The state NN can be fully utilized along with DD to achieve 1 s.d.o.f. using the scheme S_2^1. The DN and ND states are alternated with each other to achieve 1 s.d.o.f. Thus, we achieve the following sum s.d.o.f.:

$$
\begin{aligned}
d_1 + d_2 &= \underbrace{2}_{S^2} \times \lambda_{PP} + \underbrace{\frac{3}{2}}_{S_2^{3/2}} \times (2\lambda_{PD} + 2\lambda_{PN}) + \underbrace{1}_{S_2^1} \times (\lambda_{DD} + \lambda_{NN}) + 2\lambda_{DN} \\
&= 2\lambda_{PP} + 3\lambda_{PD} + 3\lambda_{PN} + \lambda_{DD} + \lambda_{NN} + 2\lambda_{DN} && (6.197) \\
&= 1 + \lambda_P. && (6.198)
\end{aligned}
$$

Sub-case $A2$: $\lambda_{PD} \geq \lambda_{PN}$, $\lambda_{DD} \leq \lambda_{NN}$. As in sub-case $A1$, we can fully alternate the PN and NP states with the PD and DP states using the scheme $S_2^{3/2}$ to achieve the s.d.o.f. of $\frac{3}{2}$. Since $\lambda_{DD} \leq \lambda_{NN}$, we instead fully alternate the state DD along with NN using scheme S_2^1 to achieve a sum s.d.o.f. of 1. The remaining fraction of the NN state is $\lambda_{NN} - \lambda_{DD}$ which can be alternated with the remaining fraction of $(\mathsf{PD}, \mathsf{DP})$, which is $\lambda_{PD} - \lambda_{PN}$ as long as $\lambda_{PD} - \lambda_{PN} \geq \lambda_{NN} - \lambda_{DD}$. This achieves $\frac{4}{3}$ sum s.d.o.f. Indeed, this is feasible as this is precisely the condition $\lambda_D \geq \lambda_N$. The DN and ND states are alternated with each other to achieve 1 s.d.o.f.

$$
\begin{aligned}
d_1 + d_2 =& \underbrace{2}_{S^2} \times \lambda_{PP} + \underbrace{\frac{3}{2}}_{S_2^{3/2}} \times (4\lambda_{PN}) + \underbrace{1}_{S_2^1} \times (2\lambda_{DD}) + 2\lambda_{DN} \\
&+ \underbrace{\frac{4}{3}}_{S_1^{4/3}} \times (3(\lambda_{NN} - \lambda_{DD})) + \underbrace{\frac{3}{2}}_{S_1^{3/2}} \times 2(\lambda_{PD} - \lambda_{PN} - \lambda_{NN} + \lambda_{DD}) && (6.199) \\
=& 2\lambda_{PP} + 6\lambda_{PN} + 2\lambda_{DD} + 4\lambda_{NN} - 4\lambda_{DD} + 3\lambda_{PD} + 3\lambda_{DD} - 3\lambda_{PN} \\
&- 3\lambda_{NN} + 2\lambda_{DN} && (6.200)
\end{aligned}
$$

$$=2\lambda_{PP}+3\lambda_{PD}+3\lambda_{PN}+\lambda_{DD}+\lambda_{NN}+2\lambda_{DN} \tag{6.201}$$

$$=1+\lambda_P. \tag{6.202}$$

Sub-case $A3$: $\lambda_{PD} \leq \lambda_{PN}$, $\lambda_{DD} \geq \lambda_{NN}$. Unlike the previous two sub-cases, here, we cannot fully alternate the PN and NP states with the PD and DP states. Instead, we fully use up the PD and DP states with a part of the PN and NP states using scheme $S_2^{3/2}$ to achieve the sum s.d.o.f. of $\frac{3}{2}$. The remaining duration of PN (or the NP) state is $\lambda_{PN}-\lambda_{PD}$. Now, we can also fully alternate the NN state with DD since $\lambda_{DD} \geq \lambda_{NN}$ using the scheme S_2^1 to achieve the sum s.d.o.f. of 1; and thus, the remaining fraction of DD state is $\lambda_{DD}-\lambda_{NN}$. We now alternate the remaining PN and NP states with the remaining DD state using the scheme $S_2^{4/3}$ to achieve the sum s.d.o.f. of $\frac{4}{3}$. For this to be feasible, we require $\lambda_{DD}-\lambda_{NN} \geq \lambda_{PN}-\lambda_{PD}$ which is again precisely the condition $\lambda_D \geq \lambda_N$. The remaining DD state achieves sum s.d.o.f. of 1 using scheme S_1^1. The DN and ND states are alternated with each other to achieve 1 s.d.o.f.

$$\begin{aligned} d_1+d_2 =& \underbrace{2}_{S^2}\times\lambda_{PP}+\underbrace{\frac{3}{2}}_{S_2^{3/2}}\times(4\lambda_{PD})+\underbrace{1}_{S_2^1}\times(2\lambda_{NN}) \\ &+\underbrace{\frac{4}{3}}_{S_2^{4/3}}\times(3(\lambda_{PN}-\lambda_{PD}))+\underbrace{1}_{S_1^1}\times(\lambda_{DD}-\lambda_{NN}-\lambda_{PN}+\lambda_{PD})+2\lambda_{DN} \end{aligned} \tag{6.203}$$

$$=2\lambda_{PP}+6\lambda_{PD}+2\lambda_{NN}+4\lambda_{PN}-4\lambda_{PD}+\lambda_{PD}+\lambda_{DD}-\lambda_{PN}$$

$$-\lambda_{NN}+2\lambda_{DN} \tag{6.204}$$

$$=2\lambda_{PP}+3\lambda_{PD}+3\lambda_{PN}+\lambda_{DD}+\lambda_{NN}+2\lambda_{DN} \tag{6.205}$$

$$=1+\lambda_P. \tag{6.206}$$

Hence, for Case A, i.e., when $\lambda_D \geq \lambda_N$, we have the complete characterization of the s.d.o.f. region.

6.5.2 Achievability for Case B: $\lambda_N > \lambda_D$

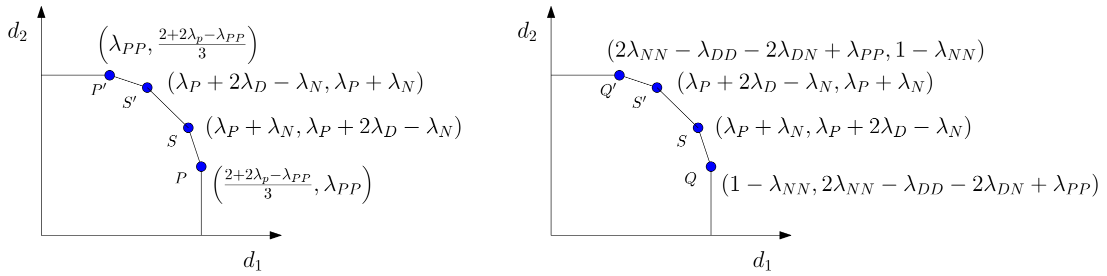
In this case, the $3d_1 + d_2/d_1 + 3d_2$ bounds are inactive at the symmetric sum rate point. However, these $3d_1 + d_2/d_1 + 3d_2$ bounds play a role at other points in the region, in particular, when one of the users requires full secure rate, the $3d_1 + d_2/d_1 + 3d_2$ bounds are relevant in some cases. Thus, these bounds are still partially relevant. Based on whether the $3d_1 + d_2/d_1 + 3d_2$ bounds are partially relevant or completely irrelevant, we divide our achievability into two broad cases:

1. $3d_1 + d_2$ bounds are partially relevant, at the point where one user requires full secret rate,
2. $3d_1 + d_2$ bounds are completely irrelevant to the region.

Now let us investigate each of these two cases individually.

6.5.2.1 When $3d_1 + d_2$ Bounds are Partially Relevant

This case happens when the intersection of the lines defined by the $3d_1 + d_2$ bound and the single user bound is inside the region defined by the lines $d_1 = 0$, $d_2 = 0$,


d_2
$\left(\lambda_{PP}, \frac{2+2\lambda_p-\lambda_{PP}}{3}\right)$
P'
S'
$(\lambda_P + 2\lambda_D - \lambda_N, \lambda_P + \lambda_N)$
S
$(\lambda_P + \lambda_N, \lambda_P + 2\lambda_D - \lambda_N)$
P
$\left(\frac{2+2\lambda_p-\lambda_{PP}}{3}, \lambda_{PP}\right)$
d_1
d_2
$(2\lambda_{NN} - \lambda_{DD} - 2\lambda_{DN} + \lambda_{PP}, 1 - \lambda_{NN})$
Q'
S'
$(\lambda_P + 2\lambda_D - \lambda_N, \lambda_P + \lambda_N)$
S
$(\lambda_P + \lambda_N, \lambda_P + 2\lambda_D - \lambda_N)$
Q
$(1 - \lambda_{NN}, 2\lambda_{NN} - \lambda_{DD} - 2\lambda_{DN} + \lambda_{PP})$
d_1

(a) $\lambda_{DD} + 2\lambda_{DN} \geq 2\lambda_{NN}$.

(b) $\lambda_{DD} + 2\lambda_{DN} \leq 2\lambda_{NN}$.

Figure 6.11: s.d.o.f. regions in case B when $3d_1+d_2$ and d_1+3d_2 bounds are partially active.

single user bounds and the $d_1 + d_2$ bound. We note that this depends on which of the single user bounds is active, giving rise to two cases, as shown in Fig. 6.11:

- $1 - \lambda_{NN} \geq \frac{2+2\lambda_P-\lambda_{PP}}{3}$, in which case, the $3d_1 + d_2$ bounds are always relevant, since $\lambda_{PP} \leq 2(\lambda_P + \lambda_D) - \frac{2+2\lambda_P-\lambda_{PP}}{3}$. In this case, when one user requires full rate, it suffices to achieve extremal point given by:

$$P : (d_1, d_2) = \left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, \lambda_{PP}\right), \tag{6.207}$$

- $1 - \lambda_{NN} \leq \frac{2+2\lambda_P-\lambda_{PP}}{3}$, in which case, the $3d_1 + d_2$ bounds are relevant as long as $\lambda_{NN} \leq \lambda_D$. We will need to show the achievability of one of the extremal points when one of the users requires full rate, given by:

$$Q : (d_1, d_2) = (1 - \lambda_{NN}, \lambda_{PP} + (2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD})). \tag{6.208}$$

However, we note that in both cases, the extremal points that achieve the sum rate are defined by the intersection of the lines $3d_1+d_2 = 2+2\lambda_P$ and $d_1+d_2 = 2(\lambda_P+\lambda_D)$. These points are symmetric with respect to the line $d_1 = d_2$ and it suffices to show the achievability of either one of them. As shown in the figures, it suffices to achieve the point

$$S : (d_1, d_2) = (\lambda_P + \lambda_N, \lambda_P + 2\lambda_D - \lambda_N). \tag{6.209}$$

Thus, to show the achievability of the full region, we need to show how the points P, Q and S are achieved in their relevant cases. We will begin with point S since it remains unaffected by which of the single user bounds is active.

The sum rate point S:

Now we are effectively operating under the constraint $\lambda_{NN} \leq \lambda_D \leq \lambda_N$, and wish to achieve the point $(\lambda_P + \lambda_N, \lambda_P + 2\lambda_D - \lambda_N)$. From this condition it is not immediately clear how the constituent schemes should be jointly utilized. Hence we focus on the second half of the inequality, which simplifies to $\lambda_{PD} + \lambda_{DD} \leq \lambda_{PN} + \lambda_{NN}$, and break this condition into three mutually exclusive cases:

- Sub-case $B1$: $\lambda_{PD} \leq \lambda_{PN}$ and $\lambda_{DD} \leq \lambda_{NN}$,
- Sub-case $B2$: $\lambda_{PD} \geq \lambda_{PN}$ and $\lambda_{DD} \leq \lambda_{NN}$,
- Sub-case $B3$: $\lambda_{PD} \leq \lambda_{PN}$ and $\lambda_{DD} \geq \lambda_{NN}$.

Now let us consider each case one by one:

Sub-case $B1$: $\lambda_{PD} \leq \lambda_{PN}$ and $\lambda_{DD} \leq \lambda_{NN}$: In this case, the full DD state will be used up with a part of the NN state using scheme S_2^1 to achieve the rate pair $\left(\frac{1}{2}, \frac{1}{2}\right)$. The duration of the remaining NN state is $(\lambda_{NN} - \lambda_{DD})$. Now if $\lambda_{NN} - \lambda_{DD} \leq \lambda_{DN}$, this remaining NN state can be fully used up with the DN and ND states using scheme $S_3^{2/3}$ achieving the pair $(\frac{2}{3}, 0)$. The remaining DN and ND states achieve the pair $(\frac{1}{2}, \frac{1}{2})$ using the scheme S_3^1. The PD and DP states are fully alternated with the PN and NP states using scheme $S_2^{3/2}$ to achieve the pair $\left(\frac{3}{4}, \frac{3}{4}\right)$. The remaining PN and NP states achieve the pair $(1, 0)$. The rate pair achieved then is

$$\begin{aligned}
d_1 =& \lambda_{PP} + \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times 4\lambda_{PD} + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} + 1 \times 2(\lambda_{PN} - \lambda_{PD}) + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3(\lambda_{NN} - \lambda_{DD}) \\
&+ \underbrace{\frac{1}{2}}_{S_3^1} \times 2(\lambda_{DN} - \lambda_{NN} + \lambda_{DD}) \\
=& \lambda_{PP} + \lambda_{PD} + \lambda_{DN} + \lambda_{NN} + 2\lambda_{PN} \\
=& \lambda_P + \lambda_N \qquad (6.210) \\
d_2 =& \lambda_{PP} + \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times 4\lambda_{PD} + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} + \underbrace{\frac{1}{2}}_{S_3^1} \times 2(\lambda_{DN} - \lambda_{NN} + \lambda_{DD}) \\
=& \lambda_{PP} + 3\lambda_{PD} + 2\lambda_{DD} + \lambda_{DN} - \lambda_{NN} \\
=& \lambda_P + 2\lambda_D - \lambda_N. \qquad (6.211)
\end{aligned}$$

If on the other hand, $\lambda_{NN} - \lambda_{DD} \geq \lambda_{DN}$, the remaining state NN cannot be fully alternated with the states DN and ND. However, $\lambda_{NN} \leq \lambda_{DN} + \lambda_{DD} + \lambda_{PD}$ from our original condition. Therefore, the full DN and ND states are alternated with a part of the NN state using scheme $S_3^{2/3}$ achieving the pair $(\frac{2}{3}, 0)$. The remaining duration of the NN state is $(\lambda_{NN} - \lambda_{DD} - \lambda_{DN})$, which can be fully alternated with the PD and DP states using the scheme $S_1^{4/3}$ achieving the pair $(\frac{2}{3}, \frac{2}{3})$. The remaining PD and DP states can be alternated with the PN and NP states using scheme $S_2^{3/2}$

achieving the point $(\frac{3}{4}, \frac{3}{4})$. The rest of the PN and NP states achieve the point $(1, 0)$. Thus, we have,

$$\begin{aligned}
d_1 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3\lambda_{DN} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3(\lambda_{NN} - \lambda_{DN} - \lambda_{DD}) \\
&+ \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times 4(\lambda_{PD} - (\lambda_{NN} - \lambda_{DN} - \lambda_{DD})) \\
&+ 1 \times 2(\lambda_{PN} - \lambda_{PD} + (\lambda_{NN} - \lambda_{DN} - \lambda_{DD})) \\
=& \lambda_P + \lambda_N \qquad (6.212) \\
d_2 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3(\lambda_{NN} - \lambda_{DN} - \lambda_{DD}) \\
&+ \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times 4(\lambda_{PD} - (\lambda_{NN} - \lambda_{DN} - \lambda_{DD})) \\
=& \lambda_P + 2\lambda_D - \lambda_N. \qquad (6.213)
\end{aligned}$$

Sub-case $B2$: $\lambda_{PD} \geq \lambda_{PN}$ and $\lambda_{DD} \leq \lambda_{NN}$: In this case, since $\lambda_{NN} \geq \lambda_{DD}$, the entire DD state is alternated with a portion of the NN state using scheme S_2^1 to achieve the s.d.o.f. pair $\left(\frac{1}{2}, \frac{1}{2}\right)$. The remaining duration of the NN state is $\lambda_{NN} - \lambda_{DD}$. Now if $\lambda_{NN} - \lambda_{DD} \leq \lambda_{PD}$, the remaining NN state is used with a part of the PD and DP states in scheme $S_1^{4/3}$ achieving the pair $\left(\frac{2}{3}, \frac{2}{3}\right)$. The remaining portion of the PD and DP states can then be utilized with the PN and NP states using scheme $S_2^{3/2}$ achieving the pair $\left(\frac{3}{4}, \frac{3}{4}\right)$. The remaining PN and NP states are utilized to just achieve the rate pair $(1, 0)$. The DN and ND states are used to achieve the pair

$(\frac{1}{2}, \frac{1}{2})$ using the scheme S_3^1. Thus, we have,

$$\begin{aligned}
d_1 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times (2\lambda_{DD}) + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times (3(\lambda_{NN} - \lambda_{DD})) \\
&+ \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times (4\,(\lambda_{PD} - (\lambda_{NN} - \lambda_{DD}))) + \frac{1}{2} \times 2\lambda_{DN} \\
&+ 1 \times (2\lambda_{PN} - 2\,(\lambda_{PD} - (\lambda_{NN} - \lambda_{DD}))) && (6.214) \\
=& \lambda_P + \lambda_N && (6.215) \\
d_2 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times (2\lambda_{DD}) + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times (3(\lambda_{NN} - \lambda_{DD})) \\
&+ \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times (4\,(\lambda_{PD} - (\lambda_{NN} - \lambda_{DD}))) + \frac{1}{2} \times 2\lambda_{DN} && (6.216) \\
=& \lambda_{PP} + 2\lambda_{DD} + 3\lambda_{PD} - \lambda_{NN} + \lambda_{DN} && (6.217) \\
=& \lambda_P + 2\lambda_D - \lambda_N. && (6.218)
\end{aligned}$$

If on the other hand, $\lambda_{NN} - \lambda_{DD} \geq \lambda_{PD}$, the full PD and DP states will be used up with a part of the remaining NN state using scheme $S_1^{4/3}$ achieving the pair $(\frac{2}{3}, \frac{2}{3})$. The remaining duration of the NN state is $\lambda_{NN} - \lambda_{DD} - \lambda_{PD}$, which is less than λ_{DN} from our original condition. Therefore, this remaining NN state can be fully utilized with the DN and ND states using scheme $S_3^{2/3}$ to achieve the pair $(\frac{2}{3}, 0)$. The remaining DN and ND states achieve the pair $(\frac{1}{2}, \frac{1}{2})$, while the PN and NP states achieve the pair $(1, 0)$. Thus, we have,

$$
\begin{aligned}
d_1 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3\lambda_{PD} + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3(\lambda_{NN} - \lambda_{DD} - \lambda_{PD}) \\
& + \underbrace{\frac{1}{2}}_{S_3^1} \times 2(\lambda_{DN} + \lambda_{DD} + \lambda_{PD} - \lambda_{NN}) + 1 \times 2\lambda_{PN} && (6.219) \\
=& \lambda_{PP} + \lambda_{PD} + 2\lambda_{PN} + \lambda_{DN} + \lambda_{NN} && (6.220) \\
=& \lambda_P + \lambda_N && (6.221) \\
d_2 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times 2\lambda_{DD} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3\lambda_{PD} + \underbrace{\frac{1}{2}}_{S_3^1} \times 2(\lambda_{DN} + \lambda_{DD} + \lambda_{PD} - \lambda_{NN}) \\
=& \lambda_{PP} + 2\lambda_{DD} + 3\lambda_{PD} + \lambda_{DN} - \lambda_{NN} && (6.222) \\
=& \lambda_P + 2\lambda_D - \lambda_N. && (6.223)
\end{aligned}
$$

Sub-case $B3$: $\lambda_{PD} \leq \lambda_{PN}$ and $\lambda_{DD} \geq \lambda_{NN}$: To achieve the sum rate point, we should alternate the entire PD and DP states with part of the PN and NP states using the scheme $S_2^{3/2}$. Also the entire NN state should be alternated with the DD state using the scheme S_2^1. The remaining DD state can then be fully utilized with a part of the remaining PN and NP states using scheme $S_2^{4/3}$, since, $\lambda_{DD} - \lambda_{NN} \leq \lambda_{PN} - \lambda_{PD}$. The remaining PN and NP states will be exploited to achieve the s.d.o.f. pair $(1, 0)$. The DN and ND states together achieve the pair $(\frac{1}{2}, \frac{1}{2})$. Thus, we have,

$$
d_1 = \lambda_{PP} + \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times (4\lambda_{PD}) + \underbrace{\frac{1}{2}}_{S_2^1} \times (2\lambda_{NN}) + \underbrace{\frac{2}{3}}_{S_2^{4/3}} \times (3(\lambda_{DD} - \lambda_{NN})) + \frac{1}{2} \times 2\lambda_{DN}
$$

$$+1 \times (2(\lambda_{PN} - \lambda_{PD}) - 2(\lambda_{DD} - \lambda_{NN})) \tag{6.224}$$

$$= \lambda_{PP} + \lambda_{PD} + 2\lambda_{PN} + \lambda_{NN} + \lambda_{DN} \tag{6.225}$$

$$= \lambda_P + \lambda_N \tag{6.226}$$

$$d_2 = \lambda_{PP} + \underbrace{\frac{3}{4}}_{S_2^{3/2}} \times (4\lambda_{PD}) + \underbrace{\frac{1}{2}}_{S_2^1} \times (2\lambda_{NN}) + \underbrace{\frac{2}{3}}_{S_2^{4/3}} \times \left(3(\lambda_{DD} - \lambda_{NN}) + \frac{1}{2} \times 2\lambda_{DN}\right) \tag{6.227}$$

$$= \lambda_{PP} + 3\lambda_{PD} + 2\lambda_{DD} - \lambda_{NN} + \lambda_{DN} \tag{6.228}$$

$$= \lambda_P + 2\lambda_D - \lambda_N. \tag{6.229}$$

The points P and Q:

- Point P: Recall that we need to achieve the point $P : \left(\frac{2+2\lambda_P - \lambda_{PP}}{3}, \lambda_{PP}\right)$ when $1 - \lambda_{NN} \geq \frac{2+2\lambda_P-\lambda_{PP}}{3}$, a condition that simplifies to $\lambda_{DD} + 2\lambda_{DN} \geq 2\lambda_{NN}$. To achieve this point, using the state PP, we achieve $(1,1)$, with $\mathsf{PD}, \mathsf{DP}, \mathsf{PN}, \mathsf{NP}$, we achieve the pair $(1,0)$. For the states $(\mathsf{DD}, \mathsf{NN}) \sim (\frac{2}{3}, \frac{1}{3})$, and $(\mathsf{DN}, \mathsf{ND}, \mathsf{NN}) \sim (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, we achieve the pair $(\frac{2}{3}, 0)$ by using the schemes $S_2^{2/3}$ and $S_3^{2/3}$, respectively. Essentially, the NN state is used up with the DD state and the DN and ND states to achieve $\frac{2}{3}$ s.d.o.f. for user 1.

  Time sharing yields the following s.d.o.f. pair:

$$d_2 = \lambda_{PP} \tag{6.230}$$

$$d_1 = \lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN} + \underbrace{\frac{2}{3}}_{S_2^{2/3}} (\lambda_{DD} + 2\lambda_{DN} + \lambda_{NN}) \tag{6.231}$$

$$= 2\lambda_P - \lambda_{PP} + \frac{2}{3}(\lambda_{DD} + 2\lambda_{DN} + \lambda_{NN}) \tag{6.232}$$

$$= 2\lambda_P - \lambda_{PP} + \frac{2}{3}(1 - 2\lambda_P + \lambda_{PP}) \tag{6.233}$$

$$= \frac{2 + 2\lambda_P - \lambda_{PP}}{3}. \tag{6.234}$$

- Point Q: We need to achieve the point $Q : (1 - \lambda_{NN}, \lambda_{PP} + (2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}))$ when $1 - \lambda_{NN} \leq \frac{2+2\lambda_P - \lambda_{PP}}{3}$, or equivalently, when $\lambda_{DD} + 2\lambda_{DN} \leq \lambda_{NN}$ and under the added constraint $\lambda_{NN} \leq \lambda_D$. Here, we consider two further subcases:

  – $\lambda_{NN} \leq \lambda_{DD} + \lambda_{DN}$: In this case, to achieve the point Q, we first use up the full DN and ND states with a part of the NN state using scheme $S_3^{2/3}$. We alternate the remaining $(\lambda_{NN} - \lambda_{DN})$ duration of NN state with the DD state using two schemes: $S_2^{2/3}$ and S_2^1. Note that in this case, $0 \leq 2(\lambda_{DD} + \lambda_{DN} - \lambda_{NN}) \leq \lambda_{DD}$. We use the state DD for duration $2(\lambda_{DD} + \lambda_{DN} - \lambda_{NN})$ and state NN for duration $(\lambda_{DD} + \lambda_{DN} - \lambda_{NN})$ together using scheme $S_2^{2/3}$ to achieve the s.d.o.f. pair $\left(\frac{2}{3}, 0\right)$. The remaining $(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD})$ duration of the state NN is alternated with the remaining $(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD})$ duration of state DD using the scheme S_2^1 to achieve the s.d.o.f. pair $\left(\frac{1}{2}, \frac{1}{2}\right)$. The state PP allows us to achieve the s.d.o.f. pair $(1, 1)$ while the remaining states PD, DP, PN, and NP each achieves $(1, 0)$.

Thus, by using time sharing, the s.d.o.f. pair is:

$$\begin{aligned} d_1 =& \lambda_{PP} + 1 \times 2\lambda_{PD} + 1 \times 2\lambda_{PN} + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3\lambda_{DN} \\ &+ \underbrace{\frac{2}{3}}_{S_2^{2/3}} \times 3(\lambda_{DD} + \lambda_{DN} - \lambda_{NN}) && (6.235) \\ &+ \underbrace{\frac{1}{2}}_{S_2^{1}} \times 2(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}) && (6.236) \\ =& 1 - \lambda_{NN} && (6.237) \\ d_2 =& \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^{1}} \times 2(2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}) \\ =& \lambda_{PP} + (2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}), && (6.238) \end{aligned}$$

which is precisely the point Q.

- $\lambda_{NN} \geq \lambda_{DD} + \lambda_{DN}$: In this case, the state NN cannot be completely used with the states DD, DN and ND. But we note that $\lambda_D \geq \lambda_{NN}$. We first use up the DN and ND states by alternating with the NN state using scheme $S_3^{2/3}$. A portion λ_{DD} of the remaining $(\lambda_{NN} - \lambda_{DN})$ duration of the NN state uses up the DD state in scheme S_2^1 achieving the pair $\left(\frac{1}{2}, \frac{1}{2}\right)$. The remaining $(\lambda_{NN} - \lambda_{DN} - \lambda_{DD})$ portion of the NN state is used with the PD and DP states through the scheme $S_1^{4/3}$ to achieve the pair $\left(\frac{2}{3}, \frac{2}{3}\right)$. For the remainder of the state PD, DP and the states PN, NP, we can achieve the pair $(1, 0)$, while $(1, 1)$ is achieved in the PP state. By time sharing, we get

$$d_1 = \lambda_{PP} + 2\lambda_{PN} + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3\lambda_{DN} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3(\lambda_{NN} - \lambda_{DN} - \lambda_{DD})$$

$$+ 2(\lambda_{PD} - \lambda_{NN} + \lambda_{DN} + \lambda_{DD}) + \underbrace{\frac{1}{2}}_{S_2^{1}} \times 2\lambda_{DD} \tag{6.239}$$

$$= 1 - \lambda_{NN} \tag{6.240}$$

$$d_2 = \lambda_{PP} + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times 3(\lambda_{NN} - \lambda_{DN} - \lambda_{DD}) + \underbrace{\frac{1}{2}}_{S_2^{1}} \times 2\lambda_{DD} \tag{6.241}$$

$$= \lambda_{PP} + 2\lambda_{NN} - 2\lambda_{DN} - \lambda_{DD}, \tag{6.242}$$

which is again the point Q.

Thus, we have achieved the point Q as well.

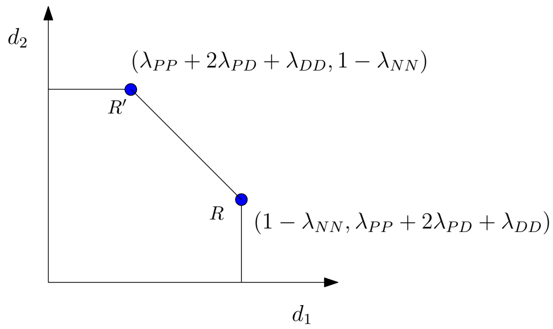
This completes the achievability of the full region when the $3d_1 + d_2$ bounds are relevant.

6.5.2.2 When $3d_1 + d_2$ Bounds are Irrelevant

This case occurs when $\lambda_{NN} \geq \lambda_D$. In this case, the single user bounds are

$$d_1 \leq 1 - \lambda_{NN} \tag{6.243}$$

$$d_2 \leq 1 - \lambda_{NN}, \tag{6.244}$$



(a) $\lambda_{DN}+\lambda_{PN} \neq 0$.

(b) $\lambda_{DN}=\lambda_{PN}=0$.

Figure 6.12: s.d.o.f. regions in case B, when $3d_1+d_2$ and d_1+3d_2 bounds are completely irrelevant.

and as shown in Fig. 6.12a the only point to achieve is given by:

$$R:(d_1,d_2)=(1-\lambda_{NN}, \lambda_{PP}+2\lambda_{PD}+\lambda_{DD}). \tag{6.245}$$

Note that $\lambda_{PP}+2\lambda_{PD}+\lambda_{DD} \leq 1-\lambda_{NN}$ with equality if and only if $\lambda_{PN}=\lambda_{DN}=0$. Thus, it suffices to achieve the point R which goes to the degenerate point $(1-\lambda_{NN}, 1-\lambda_{NN})$ when $\lambda_{PN}=\lambda_{DN}=0$, as shown in Fig. 6.12b.

To achieve this point, we alternate part of the NN state with the DD state using scheme S_2^1 to achieve the pair $\left(\frac{1}{2},\frac{1}{2}\right)$, and with the PD and DP states using the scheme $S_1^{4/3}$ to achieve the pair $\left(\frac{2}{3},\frac{2}{3}\right)$ and with the DN and ND states using the scheme $S_3^{2/3}$ to achieve the pair $(\frac{2}{3},0)$. The remaining NN state is left unused. The PN and NP states, if available, is used to achieve the s.d.o.f. pair $(1,0)$. Thus, we have,

$$d_1 = \lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times (2\lambda_{DD}) + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times (3\lambda_{PD}) + \underbrace{\frac{2}{3}}_{S_3^{2/3}} \times 3\lambda_{DN} + 1 \times 2\lambda_{PN}$$

$$=1-\lambda_{NN} \tag{6.246}$$

$$d_2 =\lambda_{PP} + \underbrace{\frac{1}{2}}_{S_2^1} \times (2\lambda_{DD}) + \underbrace{\frac{2}{3}}_{S_1^{4/3}} \times (3\lambda_{PD}) \tag{6.247}$$

$$=\lambda_{PP} + \lambda_{DD} + 2\lambda_{PD} \tag{6.248}$$

$$=1-\lambda_{NN} \text{ if } \lambda_{PN} = \lambda_{DN} = 0. \tag{6.249}$$

This completes the proof of the achievability.

6.6 Proof of the Converse

6.6.1 Local Statistical Equivalence Property and Associated Lemma

We introduce a property of the channel which we call *local statistical equivalence*. Let us focus on the channel output of receiver 2 corresponding to the state PD and DD at time t:

$$Z_{pd}(t) = \mathbf{H}_{2,pd}(t)\mathbf{X}_{pd}(t) + N_{2,pd}(t) \tag{6.250}$$

$$Z_{dd}(t) = \mathbf{H}_{2,dd}(t)\mathbf{X}_{dd}(t) + N_{2,dd}(t). \tag{6.251}$$

Now consider $(\tilde{\mathbf{H}}_{2,pd}(t), \tilde{\mathbf{H}}_{2,dd}(t))$, $(\tilde{N}_{2,pd}(t), \tilde{N}_{2,dd}(t))$, which are independent of and identically distributed as $(\mathbf{H}_{2,pd}(t), \mathbf{H}_{2,dd}(t))$ and $(N_{2,pd}(t), N_{2,dd}(t))$, respectively. Using these random variables, we define artificial channel outputs as:

$$\tilde{Z}_{pd}(t) = \tilde{\mathbf{H}}_{2,pd}(t)\mathbf{X}_{pd}(t) + \tilde{N}_{2,pd}(t) \tag{6.252}$$

$$\tilde{Z}_{dd}(t) = \tilde{\mathbf{H}}_{2,dd}(t)\mathbf{X}_{dd}(t) + \tilde{N}_{2,dd}(t). \tag{6.253}$$

Let $\Omega = (\mathbf{H}^n, \tilde{\mathbf{H}}^n)$. Now the *local statistical equivalence* property is the following:

$$h(Z_{pd}(t), Z_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) = h(\tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega). \tag{6.254}$$

This property shows that if we consider the outputs of a receiver for such states in which it supplies delayed CSIT, then the entropy of the channel outputs conditioned on the past outputs is the same as that of another artificial receiver whose channel is distributed identically as the original receiver. Note that in an alternating CSIT setting, we focus on only the states in which the receiver provides delayed CSIT; hence we call it *local*. The original and artificial receivers have *statistically equivalent* channels in the sense that the conditional differential entropies of the outputs at the real and the artificial receivers given the past outputs are equal. The proof of this property is given in Appendix 6.8.1. We next present the following lemma which together with the local statistical equivalence property is instrumental in the converse proofs.

Lemma 11 *For our channel model, with CSIT alternating among the states* DD*,* PD *and* DP *we have:*

$$h(Z^n|\Omega) \dot{\geq} h(Y_{pd}^n, Y_{dd}^n|Z^n, \Omega) \tag{6.255}$$

$$2h(Z^n|\Omega) \dot{\geq} h(Y_{pd}^n, Y_{dd}^n|\Omega) \tag{6.256}$$

$$h(Y^n|\Omega) \dot{\geq} h(Z_{dp}^n, Z_{dd}^n|Y^n, \Omega) \tag{6.257}$$

$$2h(Y^n|\Omega) \dot{\geq} h(Z_{dp}^n, Z_{dd}^n|\Omega), \tag{6.258}$$

where $a \dot{\geq} b$ *denotes* $\lim_{P\to\infty} \frac{a}{\log P} \geq \lim_{P\to\infty} \frac{b}{\log P}$.

This lemma is proved in Appendix 6.8.2.

In the following sections, we use the local statistical equivalence property along with Lemma 11 to prove the bounds on individual d.o.f. d_1 and d_2, the sum d.o.f. $(d_1 + d_2)$ and the weighted d.o.f. $3d_1 + d_2$ and $d_1 + 3d_2$.

6.6.2 The Single User Bounds

We recall the single user bounds in (6.14)-(6.15):

$$d_1 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right) \tag{6.259}$$

$$d_2 \leq \min\left(\frac{2 + 2\lambda_P - \lambda_{PP}}{3}, 1 - \lambda_{NN}\right). \tag{6.260}$$

6.6.2.1 Proof of $d_i \leq \frac{2+2\lambda_P-\lambda_{PP}}{3}$, $i = 1, 2$

In this section, we prove the following single-user bounds:

$$d_1 \leq \frac{2 + 2\lambda_P - \lambda_{PP}}{3} = \frac{2 + 2\lambda_P + 2\lambda_{PD} + 2\lambda_{PN}}{3} \tag{6.261}$$

$$d_2 \leq \frac{2 + 2\lambda_P - \lambda_{PP}}{3} = \frac{2 + 2\lambda_P + 2\lambda_{PD} + 2\lambda_{PN}}{3}. \tag{6.262}$$

To do so, we enhance the transmitter in the following way:

- First, if in any state, the transmitter has perfect CSIT from any of the users, we provide perfect CSI for the other user too, that is, the states PP, PD, DP, PN, NP are all enhanced to the state PP.
- Next, we enhance all the remaining states, (i.e., DD, DN, ND, NN) to DD.

The enhanced channel has two states: PP occurring for $\lambda_{pp} = \lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN}$ (using symmetry of the alternation), and DD occurring for the remaining fraction of the time. Now, we have the following lemma for such a channel with only PP and DD states.

Lemma 12 *Consider the two-user MISO broadcast channel with confidential messages with only two states:* PP *and* DD *occurring for λ_{pp} and λ_{dd} fractions of time, respectively, such that $\lambda_{pp} + \lambda_{dd} = 1$. Then,*

$$d_1 \leq \frac{2 + \lambda_{pp}}{3} \tag{6.263}$$

$$d_2 \leq \frac{2 + \lambda_{pp}}{3}. \tag{6.264}$$

The proof of this lemma is provided in Appendix 6.8.3.1.

Now using $\lambda_{pp} = \lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN}$ in Lemma 12, we get the bounds in (6.261)-(6.262).

6.6.2.2 Proof of $d_i \leq 1 - \lambda_{NN}$, $i = 1, 2$

In this section, we prove the following single user bounds:

$$d_1 \leq 1 - \lambda_{NN} \tag{6.265}$$

$$d_2 \leq 1 - \lambda_{NN}. \tag{6.266}$$

To prove these, we again enhance the transmitter, but in a different way. We provide the transmitter with perfect CSIT in every state except the NN state, that is, every state except the NN state is enhanced to the PP state. Thus, we end up with a system with two states: PP occurring for $1 - \lambda_{NN}$ fraction of the time and NN occurring for λ_{NN} fraction of the time. Note that since there is no delayed CSIT in the enhanced system, there is no feedback. For such a system we have the following lemma.

Lemma 13 *For the two-user MISO broadcast channel with confidential messages with only two states:* PP *and* NN *occurring for $1 - \lambda_{nn}$ and λ_{nn} fractions of time, respectively, and no feedback,*

$$d_1 \leq 1 - \lambda_{nn} \tag{6.267}$$

$$d_2 \leq 1 - \lambda_{nn}. \tag{6.268}$$

The proof of this lemma is provided in Appendix 6.8.3.2.

Using $\lambda_{nn} = \lambda_{NN}$ in Lemma 13, we get the bounds in (6.265)-(6.266).

Combining the bounds in (6.261)-(6.262) and (6.265)-(6.266), we have the bounds in (6.14)-(6.15).

6.6.3 Proof of $d_1 + d_2$ Bound

Recall the sum s.d.o.f. bound from (6.18):

$$d_1 + d_2 \leq 2(\lambda_P + \lambda_D). \tag{6.269}$$

The original system model has nine possible states, namely, PP, DD, NN, DP, PD, PN, NP, DN, and ND. We enhance the transmitter in the following way: whenever in any state, the transmitter receives delayed CSI of a channel, we provide perfect CSI of the channel to the transmitter; in other words, we convert each D state to a P state. This clearly does not decrease the secrecy capacity (and thus, the s.d.o.f. region). Also note that the enhanced system does not have any delayed CSIT, and hence no feedback. Now the enhanced system has only four states: PP, PN, NP, NN, occurring for $\lambda_{pp} = \lambda_{PP} + \lambda_{DD} + \lambda_{DP} + \lambda_{PD}$, $\lambda_{pn} = \lambda_{PN} + \lambda_{DN}$, $\lambda_{np} = \lambda_{NP} + \lambda_{ND}$ and $\lambda_{nn} = \lambda_{NN}$ fractions of time, respectively. For such a system with four states we have the following lemma:

Lemma 14 *Consider the two-user MISO broadcast channel with confidential messages with only four of the nine states:* PP*,* PN*,* NP *and* NN *occurring for λ_{pp}, λ_{pn}, λ_{np} and λ_{nn} fractions of the time, with $\lambda_{pp} + \lambda_{pn} + \lambda_{np} + \lambda_{nn} = 1$. Also, assume* *there is no feedback. Then,*

$$d_1 + d_2 \leq 2\lambda_{pp} + \lambda_{pn} + \lambda_{np}. \tag{6.270}$$

Proof of this lemma is presented in Appendix 6.8.3.3.

Thus, using $\lambda_{pp} = \lambda_{PP} + \lambda_{DD} + \lambda_{DP} + \lambda_{PD}$, $\lambda_{pn} = \lambda_{PN} + \lambda_{DN}$, $\lambda_{np} = \lambda_{NP} + \lambda_{ND}$ and $\lambda_{nn} = \lambda_{NN}$ in Lemma 14, we have,

$$d_1 + d_2 \leq 2(\lambda_{PP} + \lambda_{DP} + \lambda_{PD} + \lambda_{DD}) + \lambda_{PN} + \lambda_{DN} + \lambda_{NP} + \lambda_{ND} \tag{6.271}$$

$$= 2(\lambda_P + \lambda_D), \tag{6.272}$$

where (6.272) follows due to the assumed symmetry: $\lambda_{PD} = \lambda_{DP}$, and this completes the proof of the bound on $d_1 + d_2$.

6.6.4 Proof of $3d_1 + d_2$ and $d_1 + 3d_2$ Bounds

In this section, we prove the following bounds from (6.16)-(6.17):

$$3d_1 + d_2 \leq 2 + 2\lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN} \tag{6.273}$$

$$d_1 + 3d_2 \leq 2 + 2\lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN}. \tag{6.274}$$

To do so, we enhance the system in the following way: Whenever in any state, the transmitter has no CSIT from a user, we provide the transmitter delayed CSIT of that user's channel; in other words, we enhance each N state to a D state. After this enhancement, we are left with only four states, namely PP, PD, DP and DD occurring for $\lambda_{pp} = \lambda_{PP}$, $\lambda_{pd} = \lambda_{PD}+\lambda_{PN}$, $\lambda_{dp} = \lambda_{DP}+\lambda_{NP}$ and $\lambda_{dd} = \lambda_{DD}+\lambda_{DN}+\lambda_{ND}+\lambda_{NN}$ fractions of the time, respectively. We have the following lemma for such a system with four states:

Lemma 15 *Consider the two-user MISO broadcast channel with confidential messages with only four of the nine states:* PP*,* PD*,* DP *and* DD *occurring for* λ_{pp}*,* λ_{pd}*,* λ_{dp} *and* λ_{dd} *fractions of the time, with* $\lambda_{pd} = \lambda_{dp}$ *and* $\lambda_{pp} + \lambda_{pd} + \lambda_{dp} + \lambda_{dd} = 1$*. Then,*

$$3d_1 + d_2 \leq 2 + 2\lambda_{pp} + 2\lambda_{pd} \tag{6.275}$$

$$d_1 + 3d_2 \leq 2 + 2\lambda_{pp} + 2\lambda_{pd}. \tag{6.276}$$

We provide a proof for this lemma in Appendix 6.8.3.4.

Using $\lambda_{pp} = \lambda_{PP}$, $\lambda_{pd} = \lambda_{PD} + \lambda_{PN}$, $\lambda_{dp} = \lambda_{DP} + \lambda_{NP}$ and $\lambda_{dd} = \lambda_{DD} + \lambda_{DN} + \lambda_{ND} + \lambda_{NN}$ in Lemma 15, and symmetry of the alternating states, we have,

$$3d_1 + d_2 \leq 2 + 2\lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN} \tag{6.277}$$

$$= 2 + 2\lambda_P \tag{6.278}$$

$$d_1 + 3d_2 \leq 2 + 2\lambda_{PP} + 2\lambda_{PD} + 2\lambda_{PN} \tag{6.279}$$

$$= 2 + 2\lambda_P, \tag{6.280}$$

which completes the proofs for the bounds on $3d_1 + d_2$ and $d_1 + 3d_2$.

6.7 Conclusions

In this chapter, we studied the two-user MISO broadcast channel with confidential messages and characterized its s.d.o.f. region with alternating CSIT. The converse proofs for the s.d.o.f. region presented in the chapter are based on novel arguments such as local statistical equivalence property and enhancing the system model in different ways, where each carefully chosen enhancement strictly improves the quality of CSIT in a certain manner. For each such enhanced system, we invoke the local statistical equivalence property and incorporate the confidentiality constraints and obtain corresponding upper bounds on the individual (d_1, d_2), sum $(d_1 + d_2)$ and weighted $(3d_1 + d_2, d_1 + 3d_2)$ s.d.o.f.

To establish the achievability of the s.d.o.f. region, several constituent schemes are developed, where each scheme by itself only operates over a subset of 9 states. The achievability of the optimal s.d.o.f. region is then established by time-sharing between the core constituent schemes. The core constituent schemes not only serve the purpose of establishing the s.d.o.f. region but also highlight the synergies across multiple CSIT states which can be exploited to achieve higher s.d.o.f. in comparison to their individually optimal s.d.o.f. values. Besides highlighting the synergistic benefits of alternating CSIT for secrecy, the optimal s.d.o.f. region also quantifies the information theoretic minimal CSIT required from each user to attain a certain s.d.o.f. value. In addition, we also quantify the loss in d.o.f., as a function of the overall CSIT quality, which must be incurred for incorporating confidentiality constraints.

6.8 Appendix

6.8.1 Proof of Local Statistical Equivalence

In this subsection, we prove the *local statistical equivalence* property:

$$h(Z_{pd}(t), Z_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) = h(\tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega). \tag{6.281}$$

To this end, first denote by F, the common distribution of $(\mathbf{H}_{2,pd}(t), \mathbf{H}_{2,dd}(t))$, and $(\tilde{\mathbf{H}}_{2,pd}(t), \tilde{\mathbf{H}}_{2,dd}(t))$. Let $\Omega = \Big\{\mathbf{H}_1(t), \mathbf{H}_2(t), \tilde{\mathbf{H}}_1(t), \tilde{\mathbf{H}}_2(t), t = 1, \ldots, n\Big\}$ be the set of channel vectors upto time n. Also, let $\Omega_t = \Omega \backslash \Big\{\mathbf{H}_{2,pd}(t), \tilde{\mathbf{H}}_{2,pd}(t), \mathbf{H}_{2,dd}(t), \tilde{\mathbf{H}}_{2,dd}(t)\Big\}$. We have,

$$\begin{aligned}
& h(Z_{pd}(t), Z_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}\Omega) \\
=& \mathbb{E}_F\Big[h(Z_{pd}(t), Z_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega_t, \tilde{\mathbf{H}}_{2,pd}(t), \tilde{\mathbf{H}}_{2,dd}(t), \mathbf{H}_{2,pd}(t) = \mathbf{h}(t), \\
& \qquad \mathbf{H}_{2,dd}(t) = \mathbf{g}(t))] && (6.282) \\
=& \mathbb{E}_F\left[h(\mathbf{h}(t)\mathbf{X}_{pd}(t) + N_{2,pd}(t), \mathbf{g}(t)\mathbf{X}_{dd}(t) + N_{2,dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega_t)\right] && (6.283) \\
=& \mathbb{E}_F\Big[h(\mathbf{h}(t)\mathbf{X}_{pd}(t) + \tilde{N}_{2,pd}(t), \mathbf{g}(t)\mathbf{X}_{dd}(t) + \tilde{N}_{2,dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega_t)\Big] && (6.284) \\
=& \mathbb{E}_F\Big[h(\mathbf{h}(t)\mathbf{X}_{pd}(t) + \tilde{N}_{2,pd}(t), \mathbf{g}(t)\mathbf{X}_{dd}(t) + \tilde{N}_{2,dd}(t)|Z_{pd}^{t-1}, Z_{pd}^{t-1}, \Omega_t, \\
& \qquad \tilde{\mathbf{H}}_{2,pd}(t) = \mathbf{h}(t), \tilde{\mathbf{H}}_{2,dd}(t) = \mathbf{g}(t))\Big] && (6.285) \\
=& \mathbb{E}_F\Big[h(\tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega_t, \mathbf{H}_{2,pd}(t), \mathbf{H}_{2,dd}(t), \tilde{\mathbf{H}}_{2,pd}(t) = \mathbf{h}(t), \\
& \qquad \tilde{\mathbf{H}}_{2,dd}(t) = \mathbf{g}(t))\Big] && (6.286) \\
=& h(\tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega), && (6.287)
\end{aligned}$$

where (6.283) follows because $(\mathbf{X}_{pd}(t), \mathbf{X}_{dd}(t))$ does not depend on $\Big(\mathbf{H}_{2,pd}(t), \tilde{\mathbf{H}}_{2,pd}(t),$ $\mathbf{H}_{2,dd}(t), \tilde{\mathbf{H}}_{2,dd}(t)\Big)$, (6.284) follows since the additive noises $(N_{2,pd}(t), N_{2,dd}(t))$ and $(\tilde{N}_{2,pd}(t), \tilde{N}_{2,dd}(t))$ are i.i.d. and independent of all other random variables, (6.285)-(6.286) follow since $(\mathbf{H}_{2,pd}(t), \mathbf{H}_{2,dd}(t))$ and $(\tilde{\mathbf{H}}_{2,pd}(t), \tilde{\mathbf{H}}_{2,dd}(t))$ have the same distribution F and the fact that $(\mathbf{X}_{pd}(t), \mathbf{X}_{dd}(t))$ does not depend on $\Big(\mathbf{H}_{2,pd}(t), \tilde{\mathbf{H}}_{2,pd}(t),$ $\mathbf{H}_{2,pd}(t), \tilde{\mathbf{H}}_{2,dd}(t)\Big)$.

6.8.2 Proof of Lemma 11

We consider the scenario in which there are only three CSIT states, namely DD, PD and DP. For such a specific alternating CSIT model, we define the channel outputs as:

$$Z^n \triangleq \left(Z^n_{dd}, Z^n_{pd}, Z^n_{dp}\right)$$

$$Y^n \triangleq \left(Y^n_{dd}, Y^n_{pd}, Y^n_{dp}\right).$$

Also let Ω denote the set of all channel vectors upto and including time n, that is, in other words, $\Omega = \Big\{\mathbf{H}_1(t), \mathbf{H}_2(t), \tilde{\mathbf{H}}_1(t), \tilde{\mathbf{H}}_2(t), t = 1, \ldots, n\Big\}$. We wish to prove that with CSIT alternating among the states DD, PD and DP we have:

$$h(Z^n|\Omega) \dot{\geq} h(Y^n_{pd}, Y^n_{dd}|Z^n, \Omega) \tag{6.288}$$

$$2h(Z^n|\Omega) \dot{\geq} h(Y^n_{pd}, Y^n_{dd}|\Omega) \tag{6.289}$$

$$h(Y^n|\Omega) \dot{\geq} h(Z^n_{dp}, Z^n_{dd}|Y^n, \Omega) \tag{6.290}$$

$$2h(Y^n|\Omega) \dot{\geq} h(Z_{dp}^n, Z_{dd}^n|\Omega). \tag{6.291}$$

First we note that due to symmetry, it suffices to prove (6.288) and (6.289). We proceed as follows:

$$\begin{aligned}
h(Z^n|\Omega) =& h(Z_{pd}^n, Z_{dd}^n|\Omega) + h(Z_{dp}^n|Z_{pd}^n, Z_{dd}^n\Omega) & (6.292)\\
=& \sum_{t=1}^{n} h(Z_{pd}(t), Z_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) + h(Z_{dp}^n|Z_{pd}^n, Z_{dd}^n, \Omega). & (6.293)
\end{aligned}$$

Using the *local statistical equivalence* property, we get,

$$h(Z^n|\Omega) = \sum_{t=1}^{n} h(\tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) + h(Z_{dp}^n|Z_{pd}^n, Z_{dd}^n, \Omega). \tag{6.294}$$

Adding (6.293) and (6.294), and lower bounding, we get,

$$\begin{aligned}
2h(Z^n|\Omega) \geq& \sum_{t=1}^{n} h(Z_{pd}(t), Z_{dd}(t), \tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) + 2h(Z_{dp}^n|Z_{pd}^n, Z_{dd}^n\Omega) & \\
\geq& \sum_{t=1}^{n} h(Z_{pd}(t), Z_{dd}(t), \tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) + h(Z_{dp}^n|Z_{pd}^n, Z_{dd}^n, \Omega) & \\
& + no(\log P) & (6.295)\\
=& \sum_{t=1}^{n} h(Z_{pd}(t), Z_{dd}(t), \tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t), Y_{pd}(t), Y_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) & \\
& - \sum_{t=1}^{n} h(Y_{pd}(t), Y_{dd}(t)|Z_{pd}(t), Z_{dd}(t), \tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t), Z_{pd}^{t-1}, Z_{dd}^{t-1}\Omega) & \\
& + h(Z_{dp}^n|Z_{pd}^n, Z_{dd}^n, \Omega) + no(\log P) & (6.296)\\
\geq& \sum_{t=1}^{n} h(Z_{pd}(t), Z_{dd}(t), Y_{pd}(t), Y_{dd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, \Omega) + h(Z_{dp}^n|Z_{pd}^n, Z_{dd}^n, \Omega) &
\end{aligned}$$

$$
\begin{aligned}
&+ no(\log P) && (6.297)\\
\geq &\sum_{t=1}^{n} h(Z_{pd}(t), Z_{dd}(t), Y_{dd}(t)Y_{pd}(t)|Z_{pd}^{t-1}, Z_{dd}^{t-1}, Y_{pd}^{t-1}, Y_{dd}^{t-1}\Omega) && \\
&+ h(Z_{dp}^{n}|Z_{pd}^{n}, Y_{pd}^{n}, Y_{dd}^{n}, Z_{dd}^{n}, \Omega) + no(\log P) && (6.298)\\
=&h(Z_{pd}^{n}, Z_{dd}^{n}, Y_{pd}^{n}, Y_{dd}^{n}|\Omega) + h(Z_{dp}^{n}|Z_{pd}^{n}, Y_{pd}^{n}, Z_{dd}^{n}, Y_{dd}^{n}\Omega) + no(\log P) && (6.299)\\
=&h(Z^{n}, Y_{pd}^{n}, Y_{dd}^{n}|\Omega) + no(\log P), && (6.300)
\end{aligned}
$$

where (6.295) follows by noting that

$$h(Z_{dp}^{n}|Z_{pd}^{n}, Z_{dd}^{n}, \Omega) \geq h(Z_{dp}^{n}|Z_{pd}^{n}, Z_{dd}^{n}, \mathbf{X}^{n}, \Omega) = no(\log P) \tag{6.301}$$

and (6.296) follows since given $(Z_{pd}(t), \tilde{Z}_{pd}(t), Z_{dd}(t), \tilde{Z}_{dd}(t))$, one can reconstruct $(\mathbf{X}_{pd}(t), \mathbf{X}_{dd}(t))$ and hence $(Y_{pd}(t), Y_{dd}(t))$ within noise distortion, implying that

$$h(Y_{pd}(t), Y_{dd}(t)|Z_{pd}(t), Z_{dd}(t)\tilde{Z}_{pd}(t), \tilde{Z}_{dd}(t), Z_{pd}^{t-1}, \Omega) \leq no(\log P). \tag{6.302}$$

Now both (6.288) and (6.289) can be derived from (6.300). We simply expand the right hand side of (6.300) in two ways:

$$
\begin{aligned}
2h(Z^{n}|\Omega) \geq &h(Z^{n}, Y_{pd}^{n}, Y_{dd}^{n}|\Omega) + no(\log P) && (6.303)\\
=&h(Z^{n}|\Omega) + h(Y_{pd}^{n}, Y_{dd}^{n}|Z^{n}, \Omega) + no(\log P), && (6.304)
\end{aligned}
$$

which implies $h(Z^{n}|\Omega) \dot{\geq} h(Y_{pd}^{n}, Y_{dd}^{n}|Z^{n}, \Omega)$, which is exactly (6.288). Alternatively from (6.300), we also have

$$2h(Z^n|\Omega) \geq h(Y_{pd}^n, Y_{dd}^n|\Omega) + h(Z^n|Y_{pd}^n, Y_{dd}^n\Omega) + no(\log P) \tag{6.305}$$

$$\geq h(Y_{pd}^n, Y_{dd}^n|\Omega) + no(\log P), \tag{6.306}$$

which implies $2h(Z^n|\Omega) \dot{\geq} h(Y_{pd}^n, Y_{dd}^n|\Omega)$, thus proving the relation in (6.289). This completes the proof of Lemma 11.

6.8.3 Proofs of Lemmas 12-15

6.8.3.1 Proof of Lemma 12

Recall that we wish to prove that for the two-user MISO broadcast channel with only two states: PP and DD occurring for λ_{pp} and λ_{dd} fractions of time, respectively, such that $\lambda_{pp} + \lambda_{dd} = 1$,

$$d_1 \leq \frac{2+\lambda_{pp}}{3}, \quad d_2 \leq \frac{2+\lambda_{pp}}{3}. \tag{6.307}$$

To do so, we proceed as follows:

$$nR_1 \leq I(W_1; Y_{pp}^n, Y_{dd}^n|\Omega) + no(n) \tag{6.308}$$

$$= I(W_1; Y_{dd}^n|\Omega) + I(W_1; Y_{pp}^n|Y_{dd}^n, \Omega) + no(n) \tag{6.309}$$

$$\leq n\lambda_{pp}\log P + I(W_1; Y_{dd}^n|\Omega) + no(n) \tag{6.310}$$

$$\leq n\lambda_{pp}\log P + I(W_1; Y_{dd}^n, Z_{dd}^n|\Omega) + no(n) \tag{6.311}$$

$$\leq n\lambda_{pp} \log P + I(W_1; Y_{dd}^n | Z_{dd}^n, \Omega) + no(\log P) + no(n) \tag{6.312}$$

$$\leq n\lambda_{pp} \log P + h(Y_{dd}^n | Z_{dd}^n, \Omega) + no(\log P) + no(n) \tag{6.313}$$

$$\leq n\lambda_{pp} \log P + h(Z_{dd}^n | \Omega) + no(\log P) + no(n), \tag{6.314}$$

where (6.308) follows from decodability of W_1 at receiver 1 and Fano's inequality, (6.313) follows from confidentiality constraint of message W_1 at receiver 2, and (6.314) follows from application of Lemma 11.

Starting from (6.310), we also have

$$nR_1 \leq n\lambda_{pp} \log P + I(W_1; Y_{dd}^n | \Omega) + no(n) \tag{6.315}$$

$$\leq n\lambda_{pp} \log P + I(W_1; Y_{dd}^n | \Omega) - I(W_1; Z_{dd}^n | \Omega) + no(\log P) + no(n) \tag{6.316}$$

$$\begin{aligned}\leq\ & n\lambda_{pp} \log P + h(Y_{dd}^n | \Omega) - h(Y_{dd}^n | W_1, \Omega) - h(Z_{dd}^n | \Omega) + h(Z_{dd}^n | W_1, \Omega) \\ & + no(\log P) + no(n)\end{aligned} \tag{6.317}$$

$$\begin{aligned}\leq\ & n\lambda_{pp} \log P + h(Y_{dd}^n | \Omega) - \frac{1}{2} h(Z_{dd}^n | W_1, \Omega) - h(Z_{dd}^n | \Omega) + h(Z_{dd}^n | W_1, \Omega) \\ & + no(\log P) + no(n)\end{aligned} \tag{6.318}$$

$$\leq n\lambda_{pp} \log P + h(Y_{dd}^n | \Omega) + \frac{1}{2} h(Z_{dd}^n | W_1, \Omega) - h(Z_{dd}^n | \Omega) + no(\log P) + no(n) \tag{6.319}$$

$$\leq n\lambda_{pp} \log P + h(Y_{dd}^n | \Omega) + \frac{1}{2} h(Z_{dd}^n | \Omega) - h(Z_{dd}^n | \Omega) + no(\log P) + no(n) \tag{6.320}$$

$$= n\lambda_{pp} \log P + h(Y_{dd}^n | \Omega) - \frac{1}{2} h(Z_{dd}^n | \Omega) + no(\log P) + no(n) \tag{6.321}$$

$$\leq n\lambda_{pp} \log P + n\lambda_{dd} \log P - \frac{1}{2} h(Z_{dd}^n | \Omega) + no(\log P) + no(n), \tag{6.322}$$

where (6.316) follows from confidentiality constraint of message W_1 at receiver 2, (6.318) follows from application of Lemma 11, and (6.320) follows from the fact that conditioning reduces differential entropy.

Eliminating $h(Z_{dd}^n|\Omega)$ from the bounds (6.322) and (6.314), we have,

$$3nR_1 \leq (3n\lambda_{pp} + 2n\lambda_{dd}) \log P + no(\log P) + no(n) \tag{6.323}$$

$$= (2 + \lambda_{pp}) n \log P + no(\log P). \tag{6.324}$$

Now first dividing by n and letting $n \to \infty$, then dividing by $\log P$ and letting $P \to \infty$, we get,

$$d_1 \leq \frac{2 + \lambda_{pp}}{3}. \tag{6.325}$$

By symmetry, we get the same single user bound for user 2, completing the proof of Lemma 12.

6.8.3.2 Proof of Lemma 13

We want to show that for the two-user MISO broadcast channel with only two states: PP and NN occurring for $1 - \lambda_{nn}$ and λ_{nn} fractions of time, respectively,

$$d_1 \leq 1 - \lambda_{nn} \tag{6.326}$$

$$d_2 \leq 1 - \lambda_{nn}. \tag{6.327}$$

To prove this, we note that since there is no feedback, the secrecy capacity depends only on the marginal distributions of channel outputs given the input distribution; [25]. Since the transmitter does not have channel knowledge of any of the users in the state NN, our system with outputs

$$Y^n = (Y_{pp}^n, Y_{nn}^n) \tag{6.328}$$

$$Z^n = (Z_{pp}^n, Z_{nn}^n) \tag{6.329}$$

has the same secrecy capacity of a new system with outputs given by

$$Y^n = (Y_{pp}^n, Y_{nn}^n) \tag{6.330}$$

$$Z^n = (Z_{pp}^n, Y_{nn}^n). \tag{6.331}$$

Thus, from the secrecy requirement, we get,

$$I(W_1; Y_{nn}^n) = I(W_1; Z_{nn}^n) \leq I(W_1; Z^n) \leq no(\log P). \tag{6.332}$$

Then we have,

$$\begin{aligned} nR_1 \leq& I(W_1; Y_{pp}^n, Y_{nn}^n) + no(n) & (6.333)\\ =& I(W_1; Y_{nn}^n) + I(W_1; Y_{pp}^n | Y_{nn}^n) + no(n) & (6.334)\\ \leq& I(W_1; Y_{pp}^n | Y_{nn}^n) + no(\log P) + no(n) & (6.335)\\ \leq& h(Y_{pp}^n | Y_{nn}^n) + no(\log P) + no(n) & (6.336)\end{aligned}$$

$$\leq h(Y_{pp}^n) + no(\log P) + no(n) \tag{6.337}$$

$$\leq n(1-\lambda_{nn}) \log P + no(\log P) + no(n), \tag{6.338}$$

where, (6.335) follows from equation (6.332), (6.336) follows since $h(Y_{pp}^n|Y_{nn}^n, W_1) \geq h(Y_{pp}^n|Y_{nn}^n, W_1, \mathbf{X}^n) \geq o(\log P)$, and (6.337) follows since conditioning reduces differential entropy.

Dividing by n, and letting $n \to \infty$, we get,

$$R_1 \leq (1-\lambda_{nn}) \log P + o(\log P). \tag{6.339}$$

Dividing by $\log P$ and letting $P \to \infty$, we have,

$$d_1 \leq 1 - \lambda_{nn}. \tag{6.340}$$

By symmetry, we also have,

$$d_2 \leq 1 - \lambda_{nn}. \tag{6.341}$$

This completes the proof of Lemma 13.

6.8.3.3 Proof of Lemma 14

We wish to prove that for the two-user MISO broadcast channel with no feedback and only four of the nine states: PP, PN, NP and NN occurring for λ_{pp}, λ_{pn}, λ_{np} and

λ_{nn} fractions of the time, with $\lambda_{pp} + \lambda_{pn} + \lambda_{np} + \lambda_{nn} = 1$,

$$d_1 + d_2 \leq 2\lambda_{pp} + \lambda_{pn} + \lambda_{np}. \tag{6.342}$$

To that end, for each of the two receivers, we introduce another statistically equivalent receiver. At receiver 1, we introduce a virtual receiver $\tilde{1}$, with channel output denoted by $\tilde{Y}$, while the channel output at the virtual receiver $\tilde{2}$ at receiver 2 is denoted by $\tilde{Z}$. Since the secrecy capacity without feedback depends only on the marginals [25], without loss of generality, we can assume that the channels in the state NN are the same for all receivers. The outputs at each of the receivers are

$$Y^n =(Y^n_{pp}, Y^n_{pn}, Y^n_{np}, Y^n_{nn}) \tag{6.343}$$

$$Z^n =(Z^n_{pp}, Z^n_{pn}, Z^n_{np}, Y^n_{nn}) \tag{6.344}$$

$$\tilde{Y}^n =(Y^n_{pp}, Y^n_{pn}, \tilde{Y}^n_{np}, Y^n_{nn}) \tag{6.345}$$

$$\tilde{Z}^n =(Z^n_{pp}, \tilde{Z}^n_{pn}, Z^n_{np}, Y^n_{nn}), \tag{6.346}$$

where

$$\tilde{Y}_{np}(t) =\tilde{\mathbf{H}}_{1,np}(t)\mathbf{X}_{np}(t) + \tilde{N}_{1,np}(t) \tag{6.347}$$

$$\tilde{Z}_{pn}(t) =\tilde{\mathbf{H}}_{2,pn}(t)\mathbf{X}_{pn}(t) + \tilde{N}_{2,pn}(t), \tag{6.348}$$

such that $\tilde{\mathbf{H}}_{1,np}$, $\tilde{\mathbf{H}}_{2,pn}$ are i.i.d. with the same distribution as $\mathbf{H}_{1,np}$, $\mathbf{H}_{2,pn}$, respectively, and $\tilde{N}_{1,np}$, $\tilde{N}_{2,pn}$ are i.i.d. with same distribution as $N_{1,np}$, $N_{2,pn}$. We upper bound the first receiver's rate as

$$
\begin{aligned}
nR_1 \leq & I(W_1; Y_{pp}^n, Y_{pn}^n, Y_{np}^n, Y_{nn}^n|\Omega) + no(n) && (6.349)\\
= & I(W_1, Y_{pn}^n, Y_{np}^n, Y_{nn}^n|\Omega) + I(W_1, Y_{pp}^n|Y_{pn}^n, Y_{np}^n, Y_{nn}^n, \Omega) && (6.350)\\
\leq & n\lambda_{pp}\log P + I(W_1, Y_{pn}^n, Y_{np}^n, Y_{nn}^n|\Omega) && (6.351)\\
= & n\lambda_{pp}\log P + I(W_1; Y_{pn}^n Y_{nn}^n|\Omega) + I(W_1; Y_{np}^n|Y_{pn}^n Y_{nn}^n, \Omega) + no(n) && (6.352)\\
= & n\lambda_{pp}\log P + I(W_1; Y_{pn}^n, Y_{nn}^n|\Omega) + h(Y_{np}^n|Y_{pn}^n, Y_{nn}^n, \Omega)\\
& - h(Y_{np}^n|Y_{pn}^n, Y_{nn}^n, W_1, \Omega) + no(n) && (6.353)\\
\leq & n(\lambda_{pp} + \lambda_{np})\log P + I(W_1; Y_{pn}^n, Y_{nn}^n|\Omega)\\
& - h(Y_{np}^n|Y_{nn}^n, Y_{pn}^n, W_1, \Omega) + no(n) + no(\log P) && (6.354)\\
\leq & n(\lambda_{pp} + \lambda_{np})\log P + I(W_1; Y_{pn}^n, Y_{nn}^n, Z_{pn}^n, \tilde{Z}_{pn}^n, Z_{np}^n, W_2|\Omega)\\
& - h(Y_{np}^n|Y_{pn}^n, Y_{nn}^n, W_1, \Omega) + no(n) + no(\log P) && (6.355)\\
= & n(\lambda_{pp} + \lambda_{np})\log P + I(W_1; Y_{pn}^n, \tilde{Z}_{pn}^n|Y_{nn}^n, Z_{pn}^n, Z_{np}^n, W_2, \Omega)\\
& - h(Y_{np}^n|Y_{pn}^n, Y_{nn}^n, W_1, \Omega) + no(n) + no(\log P) && (6.356)\\
= & n(\lambda_{pp} + \lambda_{np})\log P + h(Y_{pn}^n, \tilde{Z}_{pn}^n|Y_{nn}^n, Z_{pn}^n, Z_{np}^n, W_2, \Omega)\\
& - h(Y_{pn}^n, \tilde{Z}_{pn}^n|Z_{pn}^n, Y_{nn}^n, Z_{np}^n, W_1, W_2, \Omega) - h(Y_{np}^n|Y_{pn}^n, Y_{nn}^n, W_1, \Omega)\\
& + no(n) + no(\log P) && (6.357)\\
\leq & n(\lambda_{pp} + \lambda_{np})\log P + h(Y_{pn}^n, \tilde{Z}_{pn}^n|Z_{pn}^n, Z_{np}^n, Y_{nn}^n, W_2, \Omega)\\
& - h(Y_{np}^n|Y_{pn}^n, Y_{nn}^n, W_1, \Omega) + no(n) + no(\log P) && (6.358)\\
= & n(\lambda_{pp} + \lambda_{np})\log P + h(\tilde{Z}_{pn}^n|Z_{pn}^n, Z_{np}^n, Y_{nn}^n, W_2, \Omega)\\
& + h(Y_{pn}^n|Z_{pn}^n, \tilde{Z}_{pn}^n, Z_{np}^n, Y_{nn}^n, W_2, \Omega) - h(Y_{np}^n|Y_{pn}^n, Y_{nn}^n, W_1, \Omega)
\end{aligned}
$$

$$
\begin{aligned}
&+ no(n) + no(\log P) && (6.359)\\
\leq& n(\lambda_{pp} + \lambda_{np}) \log P + h(\tilde{Z}_{pn}^n | Z_{np}^n, Y_{nn}^n, W_2, \Omega) - h(Y_{np}^n | Y_{pn}^n, Y_{nn}^n, W_1, \Omega)\\
&+ no(n) + no(\log P) && (6.360)\\
=& n(\lambda_{pp} + \lambda_{np}) \log P + h(Z_{pn}^n | Z_{np}^n, Y_{nn}^n, W_2, \Omega) - h(Y_{np}^n | Y_{pn}^n, Y_{nn}^n, W_1, \Omega)\\
&+ no(n) + no(\log P), && (6.361)
\end{aligned}
$$

where (6.356) follows since,

$$
\begin{aligned}
I(W_1; Z_{pn}^n, Z_{np}^n, Y_{nn}^n, W_2|\Omega) \leq& I(W_1; Z_{pp}^n, Z_{pn}^n, Z_{np}^n, Y_{nn}^n, W_2|\Omega) && (6.362)\\
=& I(W_1, Z_{pp}^n, Z_{pn}^n, Z_{np}^n, Y_{nn}^n|\Omega)\\
&+ I(W_1; W_2 | Z_{pp}^n, Z_{pn}^n, Z_{np}^n, Y_{nn}^n, \Omega) && (6.363)\\
=& no(\log P) + I(W_1; W_2 | Z_{pp}^n, Z_{pn}^n, Z_{np}^n, Y_{nn}^n, \Omega) && (6.364)\\
\leq& no(\log P) + H(W_2 | Z_{pp}^n, Z_{pn}^n, Z_{np}^n, Y_{nn}^n, \Omega) && (6.365)\\
\leq& no(\log P) + no(n), && (6.366)
\end{aligned}
$$

where, (6.364) and (6.366) follow from the secrecy and decodability requirements, respectively. In addition, (6.358) follows since $h(Y_{pn}^n, \tilde{Z}_{pn}^n | Z_{pn}^n, Z_{np}^n, Y_{nn}^n, W_1, W_2, \Omega) \geq o(\log P)$, (6.360) follows since given Z_{pn}^n and $\tilde{Z}_{pn}^n$, one can reconstruct $\mathbf{X}_{pn}^n$ and hence Y_{pn}^n to within noise distortion, and (6.361) follows due to the statistical equivalence of receivers 2 and $\tilde{2}$ in the state PN.

Similarly, by symmetry, we have,

$$\begin{aligned}nR_2 \leq & n(\lambda_{pp} + \lambda_{pn}) \log P + h(Y_{np}^n | Y_{pn}^n, Y_{nn}^n, W_1, \Omega) \\ & - h(Z_{pn}^n | Z_{np}^n, Y_{nn}^n, W_2, \Omega) + no(n) + no(\log P). \qquad (6.367)\end{aligned}$$

Adding (6.361) and (6.367), we have,

$$n(R_1 + R_2) \leq n(2\lambda_{pp} + \lambda_{pn} + \lambda_{np}) \log P + 2no(n) + o(\log P). \qquad (6.368)$$

First dividing by $n \log(P)$ and letting $n \to \infty$, and then letting $P \to \infty$, we obtain,

$$d_1 + d_2 \leq 2\lambda_{pp} + \lambda_{pn} + \lambda_{np}. \qquad (6.369)$$

This completes the proof of Lemma 14.

6.8.3.4 Proof of Lemma 15

We want to show that for the two-user MISO broadcast channel with only four of the nine states: PP, PD, DP and DD occurring for λ_{pp}, λ_{pd}, λ_{dp} and λ_{dd} fractions of the time, with $\lambda_{pd} = \lambda_{dp}$ and $\lambda_{pp} + \lambda_{pd} + \lambda_{dp} + \lambda_{dd} = 1$,

$$\begin{aligned}3d_1 + d_2 \leq & 2 + 2\lambda_{pp} + 2\lambda_{pd} \qquad (6.370) \\ d_1 + 3d_2 \leq & 2 + 2\lambda_{pp} + 2\lambda_{pd}. \qquad (6.371)\end{aligned}$$

To do so, for each of the two receivers, we introduce another statistically equivalent receiver. At receiver 1, we introduce a virtual receiver $\tilde{1}$, with channel output denoted by $\tilde{Y}$, while the channel output at the virtual receiver $\tilde{2}$ at receiver 2 is denoted by $\tilde{Z}$. Since the capacity depends on the marginals, without loss of generality, we can assume that the channels in the state NN are the same for all receivers. The outputs at each of the receivers can be written as

$$Y^n = (Y^n_{pp}, Y^n_{pd}, Y^n_{dp}, Y^n_{nn}) \tag{6.372}$$

$$Z^n = (Z^n_{pp}, Z^n_{pd}, Z^n_{dp}, Y^n_{nn}) \tag{6.373}$$

$$\tilde{Y}^n = (Y^n_{pp}, Y^n_{pd}, \tilde{Y}^n_{dp}, Y^n_{nn}) \tag{6.374}$$

$$\tilde{Z}^n = (Z^n_{pp}, \tilde{Z}^n_{pd}, Z^n_{dp}, Y^n_{nn}), \tag{6.375}$$

where

$$\tilde{Y}_{dp}(t) = \tilde{\mathbf{H}}_{1,dp}(t)\mathbf{X}_{dp}(t) + \tilde{N}_{1,dp}(t) \tag{6.376}$$

$$\tilde{Z}_{pd}(t) = \tilde{\mathbf{H}}_{2,pd}(t)\mathbf{X}_{pd}(t) + \tilde{N}_{2,pd}(t), \tag{6.377}$$

such that $\tilde{\mathbf{H}}_{1,dp}$, $\tilde{\mathbf{H}}_{2,pd}$ are i.i.d. with the same distribution as $\mathbf{H}_{1,dp}$, $\mathbf{H}_{2,pd}$, respectively, and $\tilde{N}_{1,dp}$, $\tilde{N}_{2,pd}$ are i.i.d. with same distribution as $N_{1,dp}$, $N_{2,pd}$. We consider a special case with only four states PP, PD, DP and DD. Aided by Lemma 11, we proceed to prove Lemma 15, as follows:

$$nR_1 \leq I(W_1; Y^n|\Omega) + no(n) \tag{6.378}$$

$$\leq I(W_1; Y^n|\Omega) - I(W_1; Z^n_{dp}Z^n_{dd}|\Omega) + no(\log P) + no(n) \tag{6.379}$$

$$\leq h(Y^n|\Omega) - \frac{1}{2}h(Z_{dp}^n, Z_{dd}^n|W_1, \Omega) - h(Z_{dp}^n, Z_{dd}^n|\Omega) + h(Z_{dp}^n, Z_{dd}^n|W_1, \Omega)$$

$$+ no(\log P) + no(n) \tag{6.380}$$

$$= h(Y^n|\Omega) + \frac{1}{2}h(Z_{dp}^n, Z_{dd}^n|W_1, \Omega) - h(Z_{dp}^n, Z_{dd}^n|\Omega) + no(\log P) + no(n) \tag{6.381}$$

$$\leq h(Y^n|\Omega) + \frac{1}{2}h(Z_{dp}^n, Z_{dd}^n|\Omega) - h(Z_{dp}^n, Z_{dd}^n|\Omega) + no(\log P) + no(n) \tag{6.382}$$

$$= h(Y^n|\Omega) - \frac{1}{2}h(Z_{dp}^n, Z_{dd}^n|\Omega) + no(\log P) + no(n) \tag{6.383}$$

$$\leq n\log P - \frac{1}{2}h(Z_{dp}^n, Z_{dd}^n|\Omega) + no(\log P) + no(n), \tag{6.384}$$

where (6.379) follows from the security constraints, (6.380) follows from a conditioned version of Lemma 11 (conditioned on W_1), and (6.382) follows, since conditioning reduces differential entropy.

We also have the following bounds for user 1:

$$nR_1 \leq I(W_1; Y^n|W_2, \Omega) + no(n) \tag{6.385}$$

$$\leq I(W_1; Y^n, Z^n|W_2, \Omega) + no(n) \tag{6.386}$$

$$= I(W_1; Y^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{6.387}$$

$$\leq h(Y^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{6.388}$$

$$= h(Y_{pd}^n, Y_{dp}^n, Y_{dd}^n|Z^n, W_2, \Omega) + h(Y_{pp}^n|Y_{pd}^n, Y_{dp}^n, Y_{dd}^n, Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{6.389}$$

$$\leq n\lambda_{pp}\log P + h(Y_{dp}^n|Z^n, W_2, \Omega) + h(Y_{pd}^n, Y_{dd}^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{6.390}$$

$$\leq n(\lambda_{pp} + \lambda_{dp})\log P + h(Y_{pd}^n, Y_{dd}^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{6.391}$$

$$\leq n(\lambda_{pp}+\lambda_{dp})\log P + h(Z^n|W_2,\Omega) + no(\log P) + no(n), \tag{6.392}$$

where (6.387) follows since,

$$\begin{aligned} I(W_1;Z^n|W_2,\Omega) \leq & I(W_1;Z^n,W_2|\Omega) && (6.393)\\ =& I(W_1;Z^n|\Omega) + I(W_1;W_2|Z^n,\Omega) && (6.394)\\ \leq & no(\log P) + H(W_2|Z^n,\Omega) && (6.395)\\ \leq & no(\log P) + no(n), && (6.396)\end{aligned}$$

using the security and reliability constraints. In addition, (6.392) follows from the conditional version of Lemma 11 (conditioned on W_2).

For receiver 2, we have

$$\begin{aligned} nR_2 \leq & I(W_2;Z^n|\Omega) + no(n) && (6.397)\\ =& h(Z^n|\Omega) - h(Z^n|W_2,\Omega) + no(n) && (6.398)\\ =& h(Z^n_{pp}|Z^n_{pd},Z^n_{dp},Z^n_{dd},\Omega) + h(Z^n_{pd},Z^n_{dp},Z^n_{dd}|\Omega) - h(Z^n|W_2,\Omega) + no(n) && (6.399)\\ \leq & n\lambda_{pp}\log P + h(Z^n_{pd}|\Omega) + h(Z^n_{dp},Z^n_{dd}|\Omega) - h(Z^n|W_2,\Omega) + no(n) && (6.400)\\ \leq & n(\lambda_{pp}+\lambda_{dp})\log P + h(Z^n_{dp},Z^n_{dd}|\Omega) - h(Z^n|W_2,\Omega) + no(n). && (6.401)\end{aligned}$$

In summary, from (6.384), (6.392) and (6.401), we have,

$$nR_1 \leq n\log P - \frac{1}{2}h(Z^n_{dp},Z^n_{dd}|\Omega) + no(\log P) + no(n), \tag{6.402}$$

$$nR_1 \leq n(\lambda_{pp} + \lambda_{dp}) \log P + h(Z^n | W_2, \Omega) + no(\log P) + no(n), \tag{6.403}$$

$$nR_2 \leq n(\lambda_{pp} + \lambda_{dp}) \log P + h(Z^n_{dp}, Z^n_{dd} | \Omega) - h(Z^n | W_2, \Omega) + no(n). \tag{6.404}$$

Eliminating $h(Z^n_{dp}, Z^n_{dd}|\Omega)$ and $h(Z^n|W_2, \Omega)$ from these inequalities and taking the limit $n \to \infty$, we arrive at

$$3R_1 + R_2 \leq (2 + 2\lambda_{pp} + 2\lambda_{dp}) \log P + o(\log P). \tag{6.405}$$

Dividing by $\log P$ and taking the limit $P \to \infty$, we get the required result

$$3d_1 + d_2 \leq 2 + 2\lambda_{pp} + 2\lambda_{dp}. \tag{6.406}$$

6.8.4 Proof of the s.d.o.f. Region for PD State

In this subsection, we present the proof for the s.d.o.f. region of the fixed PD state (perfect CSIT from user 1 and delayed CSIT from user 2). The s.d.o.f. region in this case is given by all non-negative pairs (d_1, d_2) satisfying,

$$d_1 + d_2 \leq 1. \tag{6.407}$$

To prove this claim, we first provide a proof of the converse and then two achievable schemes that are sufficient to achieve the full region.

6.8.4.1 Converse

To this end, we create a virtual receiver with output $\tilde{Z}^n$ with a channel that is statistically equivalent to user 2. The channel output $\tilde{Z}$ is given by

$$\tilde{Z}(t) = \tilde{\mathbf{H}}_2(t)\mathbf{X}(t) + \tilde{N}_2(t), \tag{6.408}$$

where $\tilde{\mathbf{H}}_2$ and $\tilde{N}_2$ are i.i.d. as $\mathbf{H}_2$ and N_2, respectively. Then, the local statistical equivalence property implies that

$$h(Z(t)|Z^{t-1}, W_2, \Omega) = h(\tilde{Z}(t)|Z^{t-1}, W_2, \Omega), \tag{6.409}$$

where Ω is the set of all channel coefficients upto and including time n. Let us now bound the rate of user 1:

$$\begin{aligned}
nR_1 \leq & I(W_1; Y^n|W_2, \Omega) + no(n) && (6.410)\\
\leq & I(W_1; Y^n, Z^n|W_2, \Omega) + no(n) && (6.411)\\
= & I(W_1; Y^n|Z^n, W_2, \Omega) + no(\log P) + no(n) && (6.412)\\
\leq & I(W_1; Y^n, \tilde{Z}^n|Z^n, W_2, \Omega) + no(\log P) + no(n) && (6.413)\\
= & h(Y^n, \tilde{Z}^n|Z^n, W_2, \Omega) - h(Y^n, \tilde{Z}^n|Z^n, W_1, W_2, \Omega) + no(\log P) + no(n) && \\
& && (6.414)\\
\leq & h(Y^n, \tilde{Z}^n|Z^n, W_2, \Omega) + no(\log P) + no(n) && (6.415)\\
= & h(\tilde{Z}^n|Z^n, W_2, \Omega) + h(Y^n|Z^n, \tilde{Z}^n, W_2, \Omega) + no(\log P) + no(n) && (6.416)
\end{aligned}$$

$$\leq h(\tilde{Z}^n|Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{6.417}$$

$$= \sum_{t=1}^{n} h(\tilde{Z}(t)|\tilde{Z}^{t-1}, Z^n, W_2, \Omega) + no(\log P) + no(n) \tag{6.418}$$

$$\leq \sum_{t=1}^{n} h(\tilde{Z}(t)|Z^{t-1}, W_2, \Omega) + no(\log P) + no(n) \tag{6.419}$$

$$= \sum_{t=1}^{n} h(Z(t)|Z^{t-1}, W_2, \Omega) + no(\log P) + no(n) \tag{6.420}$$

$$= h(Z^n|W_2, \Omega) + no(\log P) + no(n), \tag{6.421}$$

where (6.412) follows since $I(W_1; Z^n|W_2, \Omega) \leq no(\log P)$ from (6.393), (6.417) follows due to the fact that given Z^n and $\tilde{Z}^n$, it is possible to reconstruct $\mathbf{X}^n$ and hence Y^n to within noise distortion, and (6.420) follows from (6.409).

For the second user, we have,

$$nR_2 \leq I(W_2; Z^n|\Omega) + no(n) \tag{6.422}$$

$$= h(Z^n|\Omega) - h(Z^n|W_2, \Omega) + no(n) \tag{6.423}$$

$$\leq n \log P - h(Z^n|W_2, \Omega) + no(n). \tag{6.424}$$

Adding (6.421) and (6.424), we have,

$$n(R_1 + R_2) \leq n \log P + no(\log P) + no(n). \tag{6.425}$$

Dividing by n and letting $n \to \infty$,

$$R_1 + R_2 \leq \log P + o(\log P). \tag{6.426}$$

Now dividing by $\log P$ and letting $P \to \infty$,

$$d_1 + d_2 \leq 1. \tag{6.427}$$

This completes the proof of the converse for the case of PD state alone.

6.8.4.2 Achievable Schemes

Note that it is sufficient to achieve only two points: a) $(d_1, d_2) = (1, 0)$ and b) $(d_1, d_2) = (0, 1)$. The achievability of these corner points follow in straightforward manner from existing arguments as follows: sending message to user 1 by superimposing it with artificial noise in a direction orthogonal to user 1's channel to achieve the pair $(1, 0)$; and sending the message to user 2 in a direction orthogonal to user 1's channel to achieve the pair $(0, 1)$. This completes the proof of the achievability of the region in (6.407).

6.8.5 Proof of the s.d.o.f. Region for DN State

For the MISO broadcast channel with confidential messages with the fixed state DN (delayed CSIT from the first user and no CSIT from the second user), the s.d.o.f. region is given by the set of all non-negative pairs (d_1, d_2) satisfying,

$$d_1 + d_2 \leq \frac{1}{2}. \tag{6.428}$$

To prove this claim, we first provide a proof of the converse and then two achievable schemes that are sufficient to achieve the full region.

6.8.5.1 Converse

We first create a virtual receiver with output $\tilde{Y}^n$ with a statistically equivalent channel as user 1. The channel output $\tilde{Y}(t)$ is given by

$$\tilde{Y}(t) = \tilde{\mathbf{H}}_1(t)\mathbf{X}(t) + \tilde{N}_1(t), \tag{6.429}$$

where $\tilde{\mathbf{H}}_1$ and $\tilde{N}_1$ are i.i.d. as $\mathbf{H}_1$ and N_1, respectively. Then, the local statistical equivalence property implies that

$$h(Y(t)|Y^{t-1}, W_1, \Omega) = h(\tilde{Y}(t)|Y^{t-1}, W_1, \Omega), \tag{6.430}$$

where Ω is the set of all channel coefficients upto and including time n. Similar to the proof of Lemma 11, Appendix 6.8.2, it can be readily shown that,

$$2h(Y^n|W_1, \Omega) \geq h(Z^n|W_1, \Omega) + o(\log P). \tag{6.431}$$

Then, for the first user, we have,

$$\begin{aligned} nR_1 \leq & I(W_1; Y^n|\Omega) - I(W_1; Z^n|\Omega) + no(n) + no(\log P) && (6.432) \\ = & h(Y^n|\Omega) - h(Y^n|W_1, \Omega) - h(Z^n|\Omega) + h(Z^n|W_1, \Omega) && (6.433) \end{aligned}$$

$$\leq h(Y^n|\Omega) - \frac{1}{2}h(Z^n|W_1,\Omega) - h(Z^n|\Omega) + h(Z^n|W_1,\Omega) \tag{6.434}$$

$$= h(Y^n|\Omega) + \frac{1}{2}h(Z^n|W_1,\Omega) - h(Z^n|\Omega) \tag{6.435}$$

$$\leq h(Y^n|\Omega) + \frac{1}{2}h(Z^n|\Omega) - h(Z^n|\Omega) \tag{6.436}$$

$$= h(Y^n|\Omega) - \frac{1}{2}h(Z^n|\Omega), \tag{6.437}$$

where (6.434) follows from (6.431). For the second user,

$$nR_2 \leq I(W_2; Z^n|\Omega) - I(W_2; Y^n|\Omega) + no(n) + no(\log P) \tag{6.438}$$

$$= h(Z^n|\Omega) - h(Y^n|\Omega) + (h(Y^n|W_2,\Omega) - h(Z^n|W_2,\Omega)) + no(n) + no(\log P). \tag{6.439}$$

Adding (6.437) and (6.439), we obtain,

$$n(R_1 + R_2) \leq \frac{1}{2}h(Z^n|\Omega) + (h(Y^n|W_2,\Omega) - h(Z^n|W_2,\Omega)) + no(n) + no(\log P) \tag{6.440}$$

$$\leq \frac{n}{2}\log P + (h(Y^n|W_2,\Omega) - h(Z^n|W_2,\Omega)) + no(n) + no(\log P). \tag{6.441}$$

Thus, in order to obtain $d_1 + d_2 \leq 1/2$, it suffices to show that

$$h(Y^n|W_2,\Omega) - h(Z^n|W_2,\Omega) \leq no(\log P) \tag{6.442}$$

where the transmitter has delayed CSIT from user 1 and no CSIT from user 2. To this end, we invoke a recent result in [10, (39)-(66)], which showed that the maximum of $h(Y^n|W_2,\Omega)-h(Z^n|W_2,\Omega)$ is less than $no(\log P)$, under the assumption of perfect CSIT from user 1 and no CSIT from user 2. Hence, the same upper bound on the maximum value also holds under a weaker assumption of delayed CSIT from user 1. Thus, using the fact that

$$(h(Y^n|W_2,\Omega)-h(Z^n|W_2,\Omega)) \leq no(\log P), \tag{6.443}$$

and substituting in (6.441), we have,

$$n(R_1+R_2) \leq \frac{n}{2}\log P + no(n) + no(\log P). \tag{6.444}$$

Dividing by n and letting $n \to \infty$, we get,

$$R_1+R_2 \leq \frac{1}{2}\log P + o(\log P). \tag{6.445}$$

Dividing by $\log P$ and letting $P \to \infty$ yields

$$d_1+d_2 \leq \frac{1}{2}. \tag{6.446}$$

This completes the proof of the converse.

6.8.5.2 Achievable Schemes

To prove the achievability of the s.d.o.f. region in (6.428), it suffices to consider only the two points: a) $(d_1,d_2)=\left(\frac{1}{2},0\right)$ and b) $(d_1,d_2)=\left(0,\frac{1}{2}\right)$. Every other point in the region can be obtained by time-sharing. A scheme for achieving $(d_1, d_2) = \left(\frac{1}{2}, 0\right)$ was presented in [15]. We include it here for completeness.

Scheme Achieving $(d_1, d_2) = \left(\frac{1}{2}, 0\right)$*:* We wish to send 1 symbol u securely to the first user in 2 time slots. This can be done as follows:

1) At time $t = 1$: The transmitter does not have any channel knowledge. It sends:

$$\mathbf{X}(1) = [q_1 \quad q_2]^T, \tag{6.447}$$

where q_1 and q_2 denote independent artificial noise symbols distributed as $\mathcal{CN}(0, P)$. Both receivers receive linear combinations of the two symbols q_1 and q_2. The receivers' outputs are:

$$Y(1) = h_{11}(1)q_1 + h_{12}(1)q_2 \stackrel{\Delta}{=} L_1(q_1, q_2) \tag{6.448}$$

$$Z(1) = h_{21}(1)q_1 + h_{22}(1)q_2. \tag{6.449}$$

Due to delayed CSIT from receiver 1, the transmitter can reconstruct $L_1(q_1, q_2)$ in the next time slot and use it for transmission.

2) At time $t = 2$: The transmitter sends:

$$\mathbf{X}(2) = [u \quad L_1(q_1, q_2)]^T. \tag{6.450}$$

The received signals are:

$$Y(2) = h_{11}(2)u + h_{12}(2)L_1(q_1, q_2) \tag{6.451}$$

$$Z(2) = h_{21}(2)u + h_{22}(2)L_1(q_1, q_2). \tag{6.452}$$

Since the receivers have full channel knowledge, receiver 1 can recover u by eliminating $L_1(q_1, q_2)$ from Y(1) and Y(2). On the other hand, the information leakage to the second user is given by,

$$\begin{aligned}
I(u; Z(1), Z(2)|\Omega) =& h(Z(1), Z(2)|\Omega) - h(Z(1), Z(2)|u, \Omega) && (6.453)\\
\leq& 2\log P - h(h_{21}(1)q_1 + h_{22}(1)q_2, h_{11}(1)q_1 + h_{12}(1)q_2|\Omega) && (6.454)\\
=& 2\log P - 2\log P + o(\log P) && (6.455)\\
=& o(\log P). && (6.456)
\end{aligned}$$

Scheme Achieving $(d_1, d_2) = \left(0, \frac{1}{2}\right)$*:* In this scheme, we wish to send 1 symbol u securely to the second user in 2 time slots. This can be done as follows:

1) At time $t = 1$: The transmitter does not have any channel knowledge. It sends:

$$\mathbf{X}(1) = [u \quad q_1]^T, \tag{6.457}$$

where q denotes an independent artificial noise symbol distributed as $\mathcal{CN}(0, P)$. Both receivers receive linear combinations of the two symbols u and q. The receivers' outputs are:

$$Y(1) = h_{11}(1)u + h_{12}(1)q \triangleq L(u,q) \tag{6.458}$$

$$Z(1) = h_{21}(1)u + h_{22}(1)q \triangleq G(u,q). \tag{6.459}$$

Due to delayed CSIT from receiver 1, the transmitter can reconstruct $L(u,q)$ in the next times lot and use it for transmission.

2) At time $t = 2$: The transmitter sends:

$$\mathbf{X}(2) = [L(u,q) \quad 0]^T. \tag{6.460}$$

The received signals are:

$$Y(2) = h_{11}(2)L(u,q) \tag{6.461}$$

$$Z(2) = h_{21}(2)L(u,q). \tag{6.462}$$

Since the receivers have full channel knowledge, receiver 2 can recover u by eliminating q from $L(u,q)$ and $G(u,q)$. On the other hand, the information leakage to the first user is given by,

$$\begin{aligned} I(u;Y(1),Y(2)|\Omega) =& I(u;L(u,q)|\Omega) && (6.463)\\ =& h(L(u,q)|\Omega) - h(L(u,q)|u,\Omega) && (6.464)\\ \leq& \log P - \log P + o(\log P) && (6.465)\end{aligned}$$

$$=o(\log P). \tag{6.466}$$

This completes the proof of achievability.

Chapter 7: Conclusions

In this dissertation, we explored how imperfect CSI affects physical layer security in wireless networks. We determined the optimal secrecy capacity or the secure degrees of freedom (s.d.o.f.) region of various channel models under no or delayed channel state information at the transmitters (CSIT).

In Chapter 2, we considered the fast Rayleigh fading wiretap channel with coherence time of one symbol duration. We proved that the optimal input distribution that achieves the secrecy capacity is discrete with finite number of mass points. We evaluated the exact secrecy capacity numerically for various values of input power and channel parameters. We showed that the secrecy capacity does not scale with power and the s.d.o.f. is zero.

In Chapter 3, we established the optimal sum s.d.o.f. for three SISO channel models: the wiretap channel with M helpers, the K-user multiple access wiretap channel, and the K-user interference channel with an external eavesdropper, in the absence of eavesdropper's CSIT. While there is no loss in the s.d.o.f. for the wiretap channel with helpers in the absence of the eavesdropper's CSIT, the s.d.o.f. decreases in the cases of the multiple access wiretap channel and the interference channel with an external eavesdropper. We further showed that in the absence of eavesdropper's

CSIT, the K-user multiple access wiretap channel is equivalent to a wiretap channel with $(K-1)$ helpers from a sum s.d.o.f. perspective.

In Chapter 4, we determined the optimal sum s.d.o.f. of the two-user MIMO multiple access wiretap channel with N antennas at each transmitter, N antennas at the legitimate receiver and K antennas at the eavesdropper. We provided optimal achievable schemes based on interference alignment techniques. We also provided matching converses to establish the optimality of the achievable schemes. Our results highlight the effect of the number of eavesdropper antennas on the sum s.d.o.f. of the MIMO multiple access wiretap channel.

In Chapter 5, we considered the MIMO wiretap channel with one helper and the MIMO multiple access wiretap channel, with no eavesdropper CSIT. In each case, the eavesdropper has K antennas while the remaining terminals have N antennas. We determined the optimal sum s.d.o.f. for each channel model for the regime $K \leq N$, and showed that in this regime, the multiple access wiretap channel reduces to the wiretap channel with a helper in the absence of eavesdropper CSIT. For the regime $N \leq K \leq 2N$, we obtained the optimal *linear* s.d.o.f., and showed that the multiple access wiretap channel and the wiretap channel with one helper have the same optimal s.d.o.f. when restricted to linear encoding strategies. In the absence of any such restrictions, we provided a loose upper bound for the sum s.d.o.f. of the multiple access wiretap channel in the regime $N \leq K \leq 2N$. Our results showed that unlike in the SISO case, there is loss of s.d.o.f. for even the wiretap channel with one helper due to lack of eavesdropper CSIT, especially when $K \geq N$.

In Chapter 6, we studied the two-user MISO broadcast channel with confidential messages and characterized its s.d.o.f. region with heterogeneous and alternating CSIT. The converse proofs for the s.d.o.f. region presented in the chapter are based on novel arguments such as local statistical equivalence property and enhancing the system model in different ways, where each carefully chosen enhancement strictly improves the quality of CSIT in a certain manner. To establish the achievability of the s.d.o.f. region, several constituent schemes are developed, where each scheme by itself only operates over a subset of nine states. The achievability of the optimal s.d.o.f. region is then established by time-sharing between the core constituent schemes. The core constituent schemes not only serve the purpose of establishing the s.d.o.f. region but also highlight the synergies across multiple CSIT states which can be exploited to achieve higher s.d.o.f. in comparison to their individually optimal s.d.o.f. values.

The contents of Chapter 2 are published in [72], Chapter 3 in [73–75], Chapter 4 in [76–78], Chapter 5 in [79], and Chapter 6 in [80–83]. Additional results which are not included in this dissertation are published in [84–88].

Bibliography

[1] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct. 1975.

[2] J. G. Smith. The information capacity of amplitude and variance-constrained scalar Gaussian channels. *Information and Control*, 18(3):203–219, Apr. 1971.

[3] I. C. Abou-Faycal, M. D. Trott, and S. Shamai. The capacity of discrete-time memoryless Rayleigh-fading channels. *IEEE Transactions on Information Theory*, 47(4):1290–1301, May 2001.

[4] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. *IEEE Transactions on Information Theory*, 60(6):3359–3378, Jun. 2014.

[5] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian multiple access wiretap channel. In *IEEE ISIT*, Jul. 2013.

[6] J. Xie and S. Ulukus. Secure degrees of freedom of K-user Gaussian interference channels: A unified view. *IEEE Transactions on Information Theory*, 61(5):2647–2661, May 2015.

[7] A. S. Motahari, S. Oveis-Gharan, and A. K. Khandani. Real interference alignment with real numbers. *IEEE Transactions on Information Theory*, submitted Aug. 2009. Also available at [arXiv:0908.1208].

[8] V. R. Cadambe and S. A. Jafar. Interference alignment and degrees of freedom of the K-user interference channel. *IEEE Transactions on Information Theory*, 54(8):3425–3441, Aug. 2008.

[9] 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 Transactions on Information Theory*, 60(8):4799–4810, Aug. 2014.

[10] A. G. Davoodi and S. A. Jafar. Aligned image sets under channel uncertainty: Settling a conjecture by Lapidoth, Shamai and Wigger on the collapse of degrees of freedom under finite precision CSIT. Available at [arXiv:1403.1541].

[11] S. Lashgari and A. S. Avestimehr. Blind wiretap channel with delayed CSIT. In *IEEE ISIT*, Jun. 2014.

[12] M. Nafea and A. Yener. Secure degrees of freedom of $N \times N \times M$ wiretap channel with a K-antenna cooperative jammer. In *IEEE ICC*, Jun. 2015.

[13] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Transactions on Information Theory*, 57(8):4961–4972, Aug. 2011.

[14] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas - Part II: The MIMOME wiretap channel. *IEEE Transactions on Information Theory*, 56(11):5515–5532, Nov. 2010.

[15] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai. Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT. *IEEE Transactions on Information Theory*, 59(9):5244–5256, Sep. 2013.

[16] S. Lashgari and S. Avestimehr. Blind MIMOME wiretap channel with delayed CSIT. Available at [arXiv:1405.0521].

[17] S. Lashgari, S. Avestimehr, and C. Suh. Linear degrees of freedom of the X-channel with delayed CSIT. *IEEE Transactions on Information Theory*, 60(4):2180–2189, Apr. 2014.

[18] M. A. Maddah-Ali and D. Tse. Completely stale transmitter channel state information is still useful. *IEEE Transactions on Information Theory*, 58(7):4418–4431, Jul. 2012.

[19] H. Maleki, S. A. Jafar, and S. Shamai. Retrospective interference alignment over interference networks. *IEEE Journal of Selected Topics in Signal Processing*, 6(3):228–240, Jun. 2012.

[20] R. Tandon, M. A. Maddah-Ali, A. Tulino, H. V. Poor, and S. Shamai. On fading broadcast channels with partial channel state information at the transmitter. In *IEEE ISWCS*, Aug. 2012.

[21] S. Amuru, R. Tandon, and S. Shamai. On the degrees-of-freedom of the 3-user MISO broadcast channel with hybrid CSIT. In *IEEE ISIT*, Jun. 2014.

[22] K. Mohanty and M. K. Varanasi. On the DoF region of the K-user MISO broadcast channel with hybrid CSIT. Available at [arXiv:1311.6647].

[23] R. Tandon, S. A. Jafar, S. Shamai, and H. V. Poor. On the synergistic benefits of alternating CSIT for the MISO broadcast channel. *IEEE Transactions on Information Theory*, 59(7):4106–4128, Jul. 2013.

[24] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, Oct. 1949.

[25] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[26] S. Leung-Yan-Cheong and M. Hellman. The Gaussian wire-tap channel. *IEEE Transactions on Information Theory*, 24(4):451–456, Jul. 1978.

[27] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. *IEEE Transactions on Information Theory*, 54(6):2470–2492, Jun. 2008.

[28] Z. Li, R. D. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In R. Liu and W. Trappe, editors, *Securing Wireless Communications at the Physical Layer*, pages 1–18. Springer US, 2010.

[29] P. K. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory*, 54(10):4687–4698, Oct. 2008.

[30] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Transactions on Information Theory*, 55(9):4033–4039, Sep. 2009.

[31] T. Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Transactions on Information Theory*, 55(6):2547–2553, Jun. 2009.

[32] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Transactions on Information Theory*, 54(12):5747–5755, Dec. 2008.

[33] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, Jun. 2008.

[34] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *Allerton Conf.*, Sep. 2008.

[35] R. Bassily and S. Ulukus. Ergodic secret alignment. *IEEE Transactions on Information Theory*, 58(3):1594–1611, Mar. 2012.

[36] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Transactions on Information Theory*, 54(6):2493–2507, Jun. 2008.

[37] R. Liu and H. V. Poor. Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages. *IEEE Transactions on Information Theory*, 55(3):1235–1249, Mar. 2009.

[38] R. Liu, T. Liu, H. V. Poor, and S. Shamai. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 56(9):4215–4227, Sep. 2010.

[39] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference assisted secret communication. *IEEE Transactions on Information Theory*, 57(5):3153–3167, May 2011.

[40] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. Interference alignment for secrecy. *IEEE Transactions on Information Theory*, 57(6):3323–3332, Jun. 2011.

[41] O. O. Koyluoglu and H. El Gamal. Cooperative encoding for secrecy in interference channels. *IEEE Transactions on Information Theory*, 57(9):5682–5694, Sep. 2011.

[42] X. He and A. Yener. The Gaussian many-to-one interference channel with confidential messages. *IEEE Transactions on Information Theory*, 57(5):2730–2745, May 2011.

[43] J. Xie and S. Ulukus. Unified secure DoF analysis of K-user Gaussian interference channels. In *IEEE ISIT*, Jul. 2013.

[44] Y. Liang and H. V. Poor. Secure communication over fading channels. In *Allerton Conf.*, Sep. 2006.

[45] Z. Li, R. D. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *Allerton Conf.*, Sep. 2006.

[46] Z. Li, R. D. Yates, and W. Trappe. Achieving secret communication for fast Rayleigh fading channels. *IEEE Transactions on Wireless Communications*, 9(9):2792–2799, Sep. 2010.

[47] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Transactions on Information Theory*, 54(9):4005–4019, Sep. 2008.

[48] J. Xie and S. Ulukus. Secure degrees of freedom regions of multiple access and interference channels: The polytope structure. *IEEE Transactions on Information Theory*, 62(4):2044–2069, Apr. 2016.

[49] C. S. Vaze and M. K. Varanasi. The degrees of freedom regions of MIMO broadcast, interference, and cognitive radio channels with no CSIT. *IEEE Transactions on Information Theory*, 58(8):5354–5374, Aug. 2012.

[50] C. S. Vaze and M. K. Varanasi. The degrees of freedom regions of two-user and certain three-user MIMO broadcast channels with delayed CSIT. *IEEE Transactions on Information Theory*, submitted, Dec. 2011. Also available at [arXiv:1101.0306].

[51] R. Tandon, S. Mohajer, H. V. Poor, and S. Shamai. Degrees of freedom region of the MIMO interference channel with output feedback and delayed CSIT. *IEEE Transactions on Information Theory*, 59(3):1444–1457, Mar. 2013.

[52] S. A. Jafar and S. Shamai. Degrees of freedom region of the MIMO X channel. *IEEE Transactions on Information Theory*, 54(1):151–170, Jan. 2008.

[53] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani. Communication over MIMO X-channels: Interference alignment, decomposition, and performance analysis. *IEEE Transactions on Information Theory*, 54(8):3457–3470, Aug. 2008.

[54] D. T. H. Kao and S. Avestimehr. Linear degrees of freedom of the MIMO X-channel with delayed CSIT. In *IEEE ISIT*, Jun. 2014.

[55] A. Ghasemi, A. S. Motahari, and A. K. Khandani. On the degrees of freedom of X-channel with delayed CSIT. In *IEEE ISIT*, Jul. 2011.

[56] R. Tandon, S. Mohajer, H. V. Poor, and S. Shamai. On X-channels with feedback and delayed CSI. In *IEEE ISIT*, Jul. 2012.

[57] A. Zaidi, Z. H. Awan, S. Shamai, and L. Vandendorpe. Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT. *IEEE Transactions on Information Forensics and Security*, 8(11):1760–1774, Nov. 2013.

[58] X. He and A. Yener. MIMO wiretap channels with unknown and varying eavesdropper channel states. *IEEE Transactions on Information Theory*, 60(11):6844–6869, Nov. 2014.

[59] X. He, A. Khisti, and A. Yener. MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom. *IEEE Transactions on Information Theory*, 59(8):4733–4745, Aug. 2013.

[60] X. He and A. Yener. MIMO broadcast channel with an unknown eavesdropper: Secrecy degrees of freedom. *IEEE Transactions on Information Theory*, 62(1):246–255, Jan. 2014.

[61] A. Agrawal, Z. Rezki, A. J. Khisti, and M. Alouini. Noncoherent capacity of secret-key agreement with public discussion. *IEEE Transactions on Information Forensics and Security*, 6(3):565–574, Sep. 2011.

[62] M. van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 43(2):712–714, Mar. 1997.

[63] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers. In *Allerton Conf.*, Oct. 2012.

[64] J. Xie and S. Ulukus. Secure degrees of freedom region of the Gaussian multiple access wiretap channel. In *Signals, Systems and Computers, 2013 Asilomar Conference on*, pages 293–297, Nov. 2013.

[65] A. J. Goldsmith and P. P. Varaiya. Capacity of fading channels with channel side information. *IEEE Transactions on Information Theory*, 43(6):1986–1992, Nov. 1997.

[66] G. Bresler and D. Tse. The two user Gaussian interference channel: a deterministic view. *European Transactions on Telecommunications*, 19:333–354, Apr. 2008.

[67] A. S. Avestimehr, S. N. Diggavi, and D. Tse. Wireless network information flow: A deterministic approach. *IEEE Transactions on Information Theory*, 57(4):1872–1905, Apr. 2011.

[68] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* Wiley-Interscience, 2nd edition, July 2006.

[69] V. R. Cadambe and S. A. Jafar. Interference alignment and the degrees of freedom of wireless X networks. *IEEE Transactions on Information Theory*, 55(9):3893–3908, Sep. 2009.

[70] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. On the secure DoF of the single-antenna MAC. In *IEEE ISIT*, Jun. 2010.

[71] G. Bresler, D. Cartwright, and D. Tse. Feasibility of interference alignment for the MIMO interference channel. *IEEE Transactions on InformationTheory*, 60(9):5573–5586, Sep. 2014.

[72] P. Mukherjee and S. Ulukus. Fading wiretap channel with no CSI anywhere. In *IEEE ISIT*, Jul. 2013.

[73] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the multiple access wiretap channel with no eavesdropper CSI. In *IEEE ISIT*, Jul. 2015.

[74] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the interference channel with no eavesdropper CSI. In *IEEE ITW*, Oct. 2015.

[75] P. Mukherjee, J. Xie, and S. Ulukus. Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT. *IEEE Transactions on Information Theory*, submitted Jun. 2015. Also available at [arXiv:1506.06114].

[76] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the MIMO multiple access wiretap channel. In *Asilomar Conf.*, Nov. 2015.

[77] P. Mukherjee and S. Ulukus. Real interference alignment for the MIMO multiple access wiretap channel. In *IEEE ICC*, Jun. 2016.

[78] P. Mukherjee and S. Ulukus. Secure degrees of freedom of the multiple access wiretap channel with multiple antennas. *IEEE Transactions on Information Theory*, submitted Feb. 2016. Also available at [arXiv:1604.03541].

[79] P. Mukherjee and S. Ulukus. MIMO one hop networks with no Eve CSIT. In *Allerton Conf.*, Sep. 2016.

[80] P. Mukherjee, R. Tandon, and S. Ulukus. MISO broadcast channels with confidential messages and alternating CSIT. In *IEEE ISIT*, Jun. 2014.

[81] P. Mukherjee, R. Tandon, and S. Ulukus. Secrecy for MISO broadcast channels with heterogeneous CSIT. In *IEEE ISIT*, Jun. 2015.

[82] P. Mukherjee, R. Tandon, and S. Ulukus. Secrecy for MISO broadcast channels via alternating CSIT. In *IEEE ICC*, Jun. 2015.

[83] P. Mukherjee, R. Tandon, and S. Ulukus. Secure degrees of freedom region of the two-user MISO broadcast channel with alternating CSIT. *IEEE Transactions on Information Theory*, submitted Feb. 2016. Also available at [arXiv:1502.02647].

[84] P. Mukherjee, R. Tandon, and S. Ulukus. Even symmetric parallel linear deterministic interference channels are inseparable. In *Allerton Conf.*, Oct. 2013.

[85] P. Mukherjee, T-Y. Liu, S. Ulukus, S-C. Lin, and Y-W. P. Hong. Secure DoF of MIMO Rayleigh block fading wiretap channels with no CSI anywhere. In *IEEE ICC*, Jun. 2014.

[86] P. Mukherjee, T-Y. Liu, S. Ulukus, S-C. Lin, and Y-W. P. Hong. Secure degrees of freedom of MIMO Rayleigh block fading wiretap channels with no CSI anywhere. *IEEE Transactions on Wireless Communications*, 14(5):2655–2669, May 2015.

[87] P. Mukherjee and S. Ulukus. Real interference alignment for vector channels. In *IEEE ISIT*, Jul. 2016.

[88] P. Mukherjee and S. Ulukus. Covert bits through queues. In *IEEE CNS*, Oct. 2016.