ABSTRACT

Title of dissertation: SIGNALLING AND RESOURCE ALLOCATION FOR SECURE COMMUNICATION IN GAUSSIAN WIRELESS CHANNELS

Shabnam Shafiee, Doctor of Philosophy, 2008

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

Gaussian wireless channels are studied under two forms of security attacks: (i) the jamming attack, where the adversary is active and transmits corruptive signal, but is not interested in the content of the communication, (ii) the eavesdropping attack, where the adversary is passive and overhears the communication and tries to obtain the message that has been transmitted.

The active attack is studied in a multi-user setting. The behavior of two users and one jammer in an additive white Gaussian channel (AWGN) with and without fading is investigated, when they participate in a non-cooperative zero-sum game, with the channel's input/output mutual information as the objective function. We assume that the jammer can eavesdrop the channel and can use the information obtained to perform correlated jamming. We also differentiate between the availability of perfect and noisy information about the user signals at the jammer. Under various assumptions on the channel characteristics, and the extent of channel state information available at the users and the jammer, we show the existence, or otherwise non-existence of a si-

multaneously optimal set of strategies for the users and the jammer, and characterize those strategies whenever they exist.

For the passive eavesdropping attack, we study multiple-input multiple-output (MIMO) AWGN channels. We first consider a multiple-input single-output (MISO) channel, where the transmitter has multiple antennas, while the receiver and the eavesdropper have single antennas each. We find achievable rates for this channel. With the channel input restricted to Gaussian signalling with no pre-processing of information, optimal transmission strategies that maximize the achievable secrecy rates are found, in terms of the input covariance matrices. It is shown that, under the optimal communication strategy, the system reduces to a single-input single-output (SISO) channel. We then extend the achievability results to fading Gaussian MISO channels. Finally, as a step toward generalizing the problem to one with multiple antennas at the receiver, we discuss the Gaussian 2-2-1 channel with a transmitter and a receiver with two antennas each, and a single antenna eavesdropper. We develop an achievability scheme similar to those of the SISO and MISO channels, and further show that in fact, it achieves the secrecy capacity of this 2-2-1 channel.

Signalling and Resource Allocation for Secure Communication in Gaussian Wireless Channels

by

Shabnam Shafiee

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
2008

Advisory Committee:

Professor Şennur Ulukuş, Chair/Advisor
Professor Prakash Narayan
Professor Richard La
Professor Steven Tretter
Professor Lawrence Washington

DEDICATION

To my parents Kobra Noori and Ali-Mohammad Shafiee.

ACKNOWLEDGMENTS

Finishing this journey has been very special in many ways. My whole life has dramatically changed since I started this program, and looking back at the years, it would have not been possible if the following people had not given me their best support.

First and foremost, I would like to thank my advisor, Professor Şennur Ulukuş. She introduced me to the fascinating field of wireless communication, and gave me the opportunity to work on very interesting problems in this field. I really appreciate the time and attention she gave me which was always beyond my expectation.

I would like to thank my committee members, Professor Narayan, Professor La, Professor Tretter and Professor Washington for their time and valuable feedbacks. I would like to thank the faculty and staff of the department of electrical and computer engineering and the institute for systems research for their constant support and help.

During my studies, I had the opportunity of having fruitful discussions with some of my friends in my adviser's group and beyond. I thank them all. I am specially thankful to Dr. Behzad Samadi and Dr. Nan Liu.

I am grateful for the invaluable support I have received from my many dearest friends, specially Shabnam Javid, Melody Djam, Dr. Azadeh Faridi, Dr. Nasim Vakili, Dr. Amirali Sharifi, and Dr. Ali Dadpay.

My sincere gratitude goes to my parents and siblings for all they gave me through-

out. I owe everything to my mother's unconditional love, and the undoubted trust she has always had in me. Words are short in describing what she has given me, and what I feel for her.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

What makes wireless communication attractive compared to wired communication comes at many fundamental costs. The inherent openness of wireless communications makes it vulnerable to eavesdropping and jamming attacks. An adversary can overhear the ongoing communication by setting up an antenna, or can jam the communication signal by transmitting a corruptive signal in the open wireless media. As fast and aggressive as the wireless technology is growing in all aspects of human life, it becomes crucial to address this vulnerability through secure communications. The two aforementioned kinds of attacks, jamming and eavesdropping attacks, are of different nature, and the information theoretic modeling and study of them proves to be substantially different.

To study the jamming attack, we adopt a game theoretic formulation as in [1], [2] and [3]. We consider a multi-user AWGN subject to correlated jamming. We find the best transmitter/jammer strategies when the users and the jammer participate in a zero-sum game. The game objective to be minimized by the jammer and maximized by the users, is the channel input-output mutual information. Both the users and the jammer are assumed to be power constrained. The jammer can have full or partial

knowledge of the transmitted signal which may be obtained through eavesdropping. In the non-fading channel, we show that the game has a saddle point solution which is Gaussian signalling for the users, and linear jamming for the jammer. Here we define linear jamming as employing a linear combination of the available information about the user signals plus Gaussian noise, where the available information is the user signals in the case of perfect information, and a noisy version of a linear combination of the user signals in the case of eavesdropping. We show that the power that the jammer allocates for jamming each user's signal is proportional to that user's power. We then assume that the user channels are subject to fading. We assume the possibility of the jammer gaining information about the user channel states by eavesdropping on the channel state feedback from the receiver to the users. We show that if the jammer is not aware of the user channel states, it would disregard its eavesdropping information and only transmit Gaussian noise. If the jammer knows the user channel states but does not have information of the user signals, the game has a solution which is characterized as Gaussian signalling and linear jamming at each channel state, together with the optimal user and jammer power allocation strategies over the channel states. The optimal power allocations in this case are such that, only one user transmits during any given channel state. If the jammer knows the user channel states and the user signals, the game does not always have a saddle point solution, in which case, we characterize the max-min user strategies, and the corresponding jammer best response. The max-min user strategy corresponds to the user's best move, in a situation where the user chooses its strategy only once, and after the user chooses its strategy, the jammer can observe it and choose the corresponding best

jamming. Our results on the jamming attack are published in [4], [5], and [6].

To study the passive attack, we follow Wyner's information theoretic formulation in [7] where an unauthorized wire-tapper is eavesdropping the ongoing communication. The measure of secrecy is the message equivocation rate at the wire-tapper, which is defined as the entropy of the message at the wire-tapper, given its observation. We first consider a Gaussian MISO channel under various assumptions on the channel attenuations. When the channel attenuations are constants, known to all parties, we characterize the maximum secrecy rate achievable through Gaussian signalling, and show that the Gaussian signalling that achieves the best secrecy rate is of beam-forming nature. The secrecy rate found here for the Gaussian MISO wire-tap channel is later shown to actually be the secrecy capacity of this channel [8, 9]. We then study the Gaussian MISO channel when the eavesdropping channel experiences fading. We characterize achievable secrecy rates through Gaussian signalling. It is shown that, when the eavesdropping channel experiences fading, the optimal Gaussian signalling has a unit-rank covariance matrix, and therefore, the system reduces to a SISO channel. We identify conditions under which, positive secrecy rates are achievable. Finally, we consider a Gaussian MIMO channel where both the transmitter and the receiver have two antennas each, and the eavesdropper has a single antenna. We call this channel the Gaussian 2-2-1 MIMO wire-tap channel. We find the secrecy capacity in two steps: we first propose an achievable scheme, which is a Gaussian signalling scheme with no pre-processing of information, and then, we develop a tight upper bound that meets the rate achieved with our proposed signalling scheme. The techniques that we develop are specific to the Gaussian 2-2-1 channel,

and whether they can be used for the general m-n-k channel is unclear. We first show that the optimal Gaussian signalling scheme has a unit-rank transmit covariance matrix, hence with Gaussian signalling, beam-forming is optimal. Then, we consider a channel where the eavesdropper's signal is given to the receiver. The secrecy capacity of this channel is an upper bound to the secrecy capacity of the original channel. We tighten this bound by allowing correlation between the additive noises of the receiver and the eavesdropper. For a certain such correlation, we prove that the optimal Gaussian signalling is unit-rank in this upper bound also. We then evaluate our upper bound and show that it meets the rate achievable with our proposed signalling scheme. Our results on the eavesdropping attack are published in [10], [11], and [12].

Chapter 2

Mutual Information Games in Multi-user Channels with Correlated Jamming

Correlated jamming refers to jamming with full or partial knowledge of the signal to be jammed. Correlated jamming has been studied in the information-theoretic context under various assumptions on the channel model [1–3]. In [1] the best transmitter/jammer strategies are found for an AWGN channel with one user and one jammer who participate in a two person zero-sum game. The game objective to be minimized by the jammer and maximized by the user is the channel input-output mutual information. Both the user and the jammer are power constrained. The jammer can have full or partial knowledge of the transmitted signal which may be obtained through eavesdropping. In [2], the problem is extended to a single-user fading channel where the transmitter and the receiver each have multiple antennas (MIMO channel), and it is assumed that the jammer has full knowledge of the user signal. This model has been further extended in [3] to consider fading in the jamming channel; the channel between the jammer and the receiver. In [3] various assumptions are made on the availability of the user channel state at the user, and the jamming channel state at

the jammer.

Here, we extend the previous results to a *multi-user* AWGN channel subject to correlated jamming. As it is customary, without loss of generality and to avoid unnecessary details, we consider a system of two users and one jammer who has full or partial knowledge of the user signals through eavesdropping, and examine the existence of optimum user and jammer strategies towards achieving maximum channel input/output mutual information. In the non-fading two user AWGN channel, we show that the game has a solution which is Gaussian signalling for the users, and linear jamming for the jammer. Here we define linear jamming as employing a linear combination of the available information about the user signals plus Gaussian noise, where the available information is the user signals in the case of perfect information, and a noisy version of a linear combination of the user signals in the case of eavesdropping. We show that the power that the jammer allocates for jamming each user's signal is proportional to that user's power.

We then assume that the user channels are subject to fading. As opposed to [3], where the user channel states could only be known at the users, we assume the possibility of the jammer gaining information about the user channel states by eavesdropping on the channel state feedback from the receiver to the users. We show that if the jammer is not aware of the user channel states, it would disregard its eavesdropping information and only transmit Gaussian noise. If the jammer knows the user channel states but does not have information of the user signals, the game has a solution which is characterized as Gaussian signalling and linear jamming at each channel state, together with the optimal user and jammer power allocation strategies

over the channel states. The optimal power allocations in this case are such that, only one user transmits during any given channel state. If the jammer knows the user channel states and the user signals, the game does not always have a saddle point solution, in which case, we characterize the max-min user strategies, and the corresponding jammer best response. The max-min user strategy corresponds to the user's best move, in a situation where the user chooses its strategy only once, and after the user chooses its strategy, the jammer can observe it and choose the corresponding best jamming. Note that if the game had a solution, max-min and min-max strategies would have been the same, and would have also been the same as the game saddle point solution.

Whenever the jamming mutual information game is concerned, and only then, the term capacity refers to the channel's information capacity, which is defined as the channel's maximum input/output mutual information, maximized over the choice of the channel input distributions [13]. For channels with known statistics and behavior, this definition coincides with the amount of information that can be reliably transmitted over the channel. Here though, this definition does not have such operational meaning.

2.1 System Model

Figure 2.1 shows a communication system with two users and one jammer. We consider several different settings based on the channel characteristics and the jammer's information. In the absence of fading, the attenuations of the user channels are

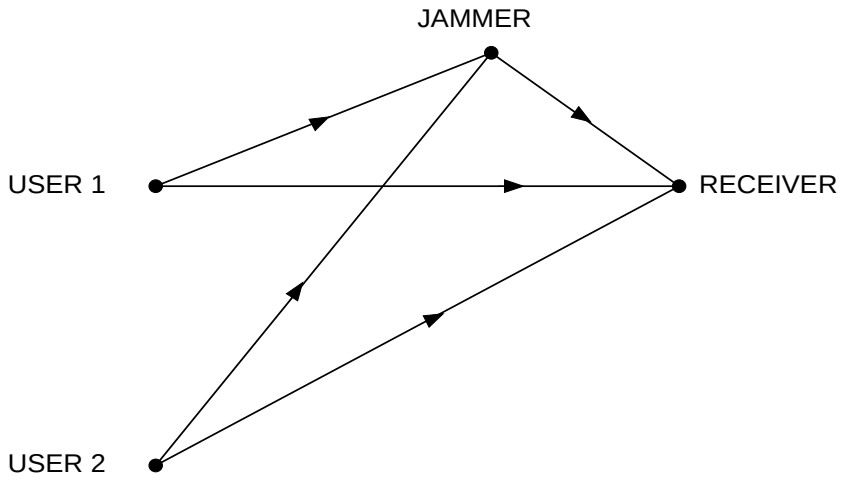

Figure 2.1: A communication system with two users and one jammer.

known to everyone. Therefore, we can assume that the attenuations are scalars. The AWGN channel with two users and one jammer is modelled as

$$Y = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + \sqrt{\gamma}J + N \tag{2.1}$$

where X_i is the i^{th} user's signal, h_i is the attenuation of the i^{th} user's channel, J is the jammer's signal, γ is the attenuation of the jammer's channel and N is a zero-mean Gaussian random variable with variance σ_N^2. To model fading in the received powers, we consider h_i and γ as fading random variables, and to further model the phase of the channel coefficients, we substitute the scalar attenuations $\sqrt{h_i}$ and $\sqrt{\gamma}$, with complex fading random variables H_i for the amplitude fading coefficient of the i^{th} user's channel, and Γ for the amplitude fading coefficient of the jammer's channel

$$Y = H_1X_1 + H_2X_2 + \Gamma J + N \tag{2.2}$$

All fading random variables are assumed to be i.i.d. The user and jammer power constraints are

$$E[X_i^2] \leq P_i, \quad i = 1, 2 \tag{2.3}$$

$$E[J^2] \leq P_J \tag{2.4}$$

Regarding the knowledge of the jammer about the transmitted signals, we analyze both cases of perfect information and imperfect information gained through eavesdropping. In the first case, we assume that the jammer knows the signals of the users perfectly, i.e., it knows X_1 and X_2 at the beginning of its transmission. In the second case, we assume an AWGN eavesdropping channel for the jammer

$$Y_e = \sqrt{g_1}X_1 + \sqrt{g_2}X_2 + N_e \tag{2.5}$$

where Y_e is the signal received at the jammer, g_i is the attenuation of the i^{th} user's eavesdropping channel and N_e is a zero-mean Gaussian random variable with variance σ_e^2. Therefore, in this case, the jammer knows a noisy version of a linear combination of the user signals, X_1 and X_2. To model fading in the received powers, we consider $\sqrt{g_i}$ as real fading variables, and to model fading in the received amplitudes, we substitute them with complex amplitude fading random variables G_i. The receiver is assumed to know the user channel states, while various assumptions are made on the amount of information that the users and the jammer have about the channel fading realization of the communication and eavesdropping channels; these assumptions are

stated at the beginning of each subsection.

2.2 Jamming in Non-fading Multi-user AWGN Channels

In this section, we find the best user/jammer strategies when the channels are non-fading, both when the jammer knows the exact user signals, and when it eavesdrops the users' channel and obtains a noisy version of a linear combination of the user signals.

2.2.1 Jamming with Complete Information

Here the system model is (2.1) where the attenuations are constant scalars, and X_1 and X_2 are known to the jammer. The jammer and the two users are involved in a zero-sum game with the input/output mutual information as the objective function. We investigate the existence and uniqueness of a saddle point solution for this game [14]. A saddle point is a combination of strategies, one for each player, such that no player has an incentive for unilaterally changing its own strategy, meaning that, no player will gain more, by unilaterally deviating from the saddle point solution. Note that in a zero-sum game, if the objective function is convex over the set of the strategies of the players that are minimizing it, and concave over the set of the strategies of the players that are maximizing it, then the mathematical saddle point of the objective function corresponds to the game's saddle point solution. However, in general, all mathematical saddle points of an objective function may not necessarily correspond to a game solution, e.g., matrix games [14].

The arguments in [13, Theorem 2.7.4] can be easily extended to the two user system to show that if $(X_1, X_2, Y) \sim f(x_1)f(x_2)f(y|x_1, x_2)$, the input/output mutual information $I(X_1, X_2; Y)$ is a concave function of $f(x_1)$ for fixed $f(x_2)$ and $f(y|x_1, x_2)$, a concave function of $f(x_2)$ for fixed $f(x_1)$ and $f(y|x_1, x_2)$, and a convex function of $f(y|x_1, x_2)$ for fixed $f(x_1)$ and $f(x_2)$. Due to the convexity/concavity of the mutual information with respect to the channel transition probability distribution/user input probability distribution, and given that the set of the user and jammer signallings which satisfy the corresponding power constraints is convex and compact, $I(X_1, X_2; Y)$ has a saddle point in that set, which is the saddle point solution of the game [15, Theorem 16, page 75], [16, Proposition 2.6.9]. In the sequel, we show that when the users employ Gaussian signalling, the best jamming strategy is linear jamming (linear combination of the user signals plus Gaussian noise), and when the jammer employs linear jamming, the best strategy for the users is Gaussian signalling, which proves that Gaussian input distributions for the users and linear jamming for the jammer is a saddle point of the input/output mutual information, and therefore, a saddle point solution for the game. Due to the interchangeability property of game solutions [15, Theorem 8, page 48], if there is any other pair of strategies which is a game solution as well, it has to result in the same mutual information value as the game solution corresponding to Gaussian signaling and linear jamming [15, Theorem 7, page 48].

First, assume that the jammer employs linear jamming

$$J = \rho_1 X_1 + \rho_2 X_2 + N_J \tag{2.6}$$

The power constraint on the jammer will force the following condition

$$\rho_1^2 P_1 + \rho_2^2 P_2 + \sigma_{N_J}^2 \leq P_J \tag{2.7}$$

Using (2.1), the output of the channel will be

$$Y = (\sqrt{h_1} + \sqrt{\gamma}\rho_1)X_1 + (\sqrt{h_2} + \sqrt{\gamma}\rho_2)X_2 + \sqrt{\gamma}N_J + N \tag{2.8}$$

From the users' perspective, the channel becomes an AWGN multiple access channel, and therefore the best signalling scheme for the users is Gaussian [13].

Next, we should show that if the users perform Gaussian signalling, then the best jamming strategy is linear jamming. The channel output is as in (2.1), where X_1 and X_2 are independent Gaussian random variables, and J, the jammer signal, is an arbitrary random variable to be chosen by the jammer. We write the input/output mutual information of the channel

$$I(Y; X_1, X_2) = h(X_1, X_2) - h(X_1, X_2|Y) \tag{2.9}$$

The jammer's strategy can only affect the second term above. We develop a sequence

of upper bounds on the second term,

$$h(X_1, X_2|Y) = h(X_1 - a_1 Y, X_2 - a_2 Y|Y) \tag{2.10}$$

$$\leq h(X_1 - a_1 Y, X_2 - a_2 Y) \tag{2.11}$$

$$\leq \frac{1}{2} \log \left((2\pi e)^2 |\mathbf{\Lambda}| \right) \tag{2.12}$$

where $\mathbf{\Lambda}$ is the covariance matrix of $(X_1 - a_1 Y, X_2 - a_2 Y)$. The inequalities hold for arbitrary a_1 and a_2. We choose $a_1 = E[X_1 Y]/E[Y^2]$ and $a_2 = E[X_2 Y]/E[Y^2]$. We now prove the optimality of linear jamming in two steps. We first consider the set of all jamming signals which result in the same $\mathbf{\Lambda}$, and show that if this set includes a linear jammer, then that linear jammer is the optimal jammer over this set. Then, we consider the set of all feasible jamming signals and show that for any jamming signal in this set, there exists a linear jammer in this set resulting in the same $\mathbf{\Lambda}$. Here, the feasibility is in the sense of the jammer's available power.

Consider the set of all jamming signals which result in the same $\mathbf{\Lambda}$ in (2.12). Assume that there is a linear jamming signal in this set. This jamming signal is jointly Gaussian with X_1 and X_2, hence $X_1 - a_1 Y$, $X_2 - a_2 Y$ and Y are jointly Gaussian. Moreover, a_1 and a_2 are chosen such that $X_1 - a_1 Y$ and $X_2 - a_2 Y$ are uncorrelated with Y, therefore, since they are all Gaussian, $X_1 - a_1 Y$ and $X_2 - a_2 Y$ are independent of Y. We conclude that this jamming signal achieves both (2.11) and (2.12) with equality, therefore, it is optimal over this set.

Now we show that any $\mathbf{\Lambda}$ achievable by any feasible jamming signal, is also achiev-

able by a feasible linear jamming signal. For the chosen values of a_1 and a_2, $\mathbf{\Lambda}$ is

$$\mathbf{\Lambda} = \begin{bmatrix} P_1 - \frac{E[X_1Y]^2}{E[Y^2]} & -\frac{E[X_1Y]E[X_2Y]}{E[Y^2]} \\ -\frac{E[X_1Y]E[X_2Y]}{E[Y^2]} & P_2 - \frac{E[X_2Y]^2}{E[Y^2]} \end{bmatrix} \tag{2.13}$$

Using (2.1), $E[X_1Y]$, $E[X_2Y]$ and $E[Y^2]$ can be written in terms of $E[X_1J]$ and $E[X_2J]$ as

$$E[X_iY] = \sqrt{h_i}P_i + \sqrt{\gamma}E[X_iJ], \quad i = 1, 2 \tag{2.14}$$

$$E[Y^2] = h_1P_1 + h_2P_2 + 2\sqrt{h_1\gamma}E[X_1J] + 2\sqrt{h_2\gamma}E[X_2J] + \sigma_N^2 + P_J \tag{2.15}$$

Therefore, $|\mathbf{\Lambda}|$ can be expressed as a function of $E[X_1J]$ and $E[X_2J]$. Consider any jamming signal J. Define R as

$$R = J - X_1\frac{E[X_1J]}{P_1} - X_2\frac{E[X_2J]}{P_2} \tag{2.16}$$

Note that R is uncorrelated with X_1 and X_2. The power of this jamming signal is

$$E[J^2] = \frac{E[X_1J]^2}{P_1} + \frac{E[X_2J]^2}{P_2} + E[R^2] \tag{2.17}$$

For this jamming signal to be feasible, we should have

$$\frac{E[X_1J]^2}{P_1} + \frac{E[X_2J]^2}{P_2} \leq P_J \tag{2.18}$$

Now define a linear jamming signal as in (2.6), where $\rho_i = E[X_iJ]/P_i$, $i = 1, 2$,

and N_J is an independent Gaussian random variable with power $E[R^2]$. This linear jammer has the same power as J and therefore is feasible. Moreover, it results in the same $|\mathbf{\Lambda}|$ value as J. Hence, for any signal in the set of feasible jamming signals, there is an equivalent linear jamming signal which results in the same upper bound in (2.12). This means that, there exists a feasible linear jamming signal which is as effective as any other feasible jamming signal, and this concludes the proof.

The next step is to find ρ_1 and ρ_2 for the linear jamming signal in (2.6) which achieves the highest upper bound in (2.12). Since both (2.11) and (2.12) hold with equality, the linear jamming parameters that maximize (2.12), maximize (2.10), or equivalently, minimize the mutual information in (2.9). Following the literature [1,2], we call this mutual information value, the capacity. Using (2.8)

$$C = \frac{1}{2}\log\left(1 + \frac{(\sqrt{h_1} + \sqrt{\gamma}\rho_1)^2 P_1 + (\sqrt{h_2} + \sqrt{\gamma}\rho_2)^2 P_2}{\gamma\sigma_{N_J}^2 + \sigma_N^2}\right) \tag{2.19}$$

which is a monotonically increasing function of the SNR, therefore the jammer's equivalent objective is to minimize the SNR value. We have the following minimization problem

$$\begin{aligned} \min_{\{\rho_1,\rho_2,\sigma_{N_J}^2\}} \quad & \frac{(\sqrt{h_1} + \sqrt{\gamma}\rho_1)^2 P_1 + (\sqrt{h_2} + \sqrt{\gamma}\rho_2)^2 P_2}{\gamma\sigma_{N_J}^2 + \sigma_N^2} \\ \text{s.t.} \quad & \rho_1^2 P_1 + \rho_2^2 P_2 + \sigma_{N_J}^2 \leq P_J \end{aligned} \tag{2.20}$$

The Karush-Kuhn-Tucker (KKT) necessary conditions are

$$\frac{\sqrt{\gamma}(\sqrt{h_1}+\sqrt{\gamma}\rho_1)P_1}{\gamma\sigma_{N_J}^2+\sigma_N^2}+\lambda\rho_1 P_1=0 \tag{2.21}$$

$$\frac{\sqrt{\gamma}(\sqrt{h_2}+\sqrt{\gamma}\rho_2)P_2}{\gamma\sigma_{N_J}^2+\sigma_N^2}+\lambda\rho_2 P_2=0 \tag{2.22}$$

$$-\gamma\frac{(\sqrt{h_1}+\sqrt{\gamma}\rho_1)^2P_1+(\sqrt{h_2}+\sqrt{\gamma}\rho_2)^2P_2}{(\gamma\sigma_{N_J}^2+\sigma_N^2)^2}+\lambda-\delta=0 \tag{2.23}$$

where δ is the complementary slackness variable for $\sigma_{N_J}^2$. Equations (2.21) and (2.22) have the following solution

$$\rho_1=-\sqrt{h_1}\frac{\gamma P_J+\sigma_N^2}{\sqrt{\gamma}(h_1P_1+h_2P_2)} \tag{2.24}$$

$$\rho_2=-\sqrt{h_2}\frac{\gamma P_J+\sigma_N^2}{\sqrt{\gamma}(h_1P_1+h_2P_2)} \tag{2.25}$$

Therefore whenever these values of ρ_1 and ρ_2 are feasible, they characterize the best jammer strategy. Ultimately, including the limiting feasible values, the optimum jamming coefficients are

$$(\rho_1,\rho_2)=\begin{cases}(-\frac{\sqrt{h_1}}{\sqrt{\gamma}},-\frac{\sqrt{h_2}}{\sqrt{\gamma}}) & \text{if} \quad \gamma P_J\geq h_1P_1+h_2P_2\\ (-\rho\sqrt{h_1},-\rho\sqrt{h_2}) & \text{if} \quad \gamma P_J<h_1P_1+h_2P_2\end{cases} \tag{2.26}$$

where

$$\rho=\min\left\{\sqrt{\frac{P_J}{h_1P_1+h_2P_2}},\frac{\gamma P_J+\sigma_N^2}{\sqrt{\gamma}(h_1P_1+h_2P_2)}\right\} \tag{2.27}$$

and the jammer transmits as in (2.6). We observe that the amount of power the

jammer allocates for jamming each user is proportional to that user's effective received power which is $h_i P_i$ for user i, $i = 1, 2$.

Figure 2.2 shows an example of the jammer decision regions. In region A, $(\rho_1, \rho_2) = (-\sqrt{h_1}/\sqrt{\gamma}, -\sqrt{h_2}/\sqrt{\gamma})$ and the jammer only uses enough power to zero out the transmitted signals. In region B, $(\rho_1, \rho_2) = (-\sqrt{h_1}, -\sqrt{h_2})\sqrt{P_J/(h_1 P_1 + h_2 P_2)}$ and the jammer uses all of its power to cancel the transmitted signals as much as possible. In region C, $(\rho_1, \rho_2) = (-\sqrt{h_1}, -\sqrt{h_2})(\gamma P_J + \sigma_N^2)/(\sqrt{\gamma}(h_1 P_1 + h_2 P_2))$ and the jammer uses part of its power to cancel the transmitted signals, and the rest of its power to add Gaussian noise to the transmitted signal. Therefore, for low channel coefficients where the effective received powers of the users are small, the optimum jamming strategy is to subtract the user signals as much as possible, while in high channel coefficients, the jammer uses its power both for adding Gaussian noise and for correlating with the user signals.

2.2.2 Jamming with Eavesdropping Information

Now suppose that the jammer gains information about the user signals only through an AWGN eavesdropping channel,

$$Y_e = \sqrt{g_1} X_1 + \sqrt{g_2} X_2 + N_e \tag{2.28}$$

We define linear jamming as transmitting a linear combination of the signal received at the jammer Y_e and Gaussian noise, i.e.,

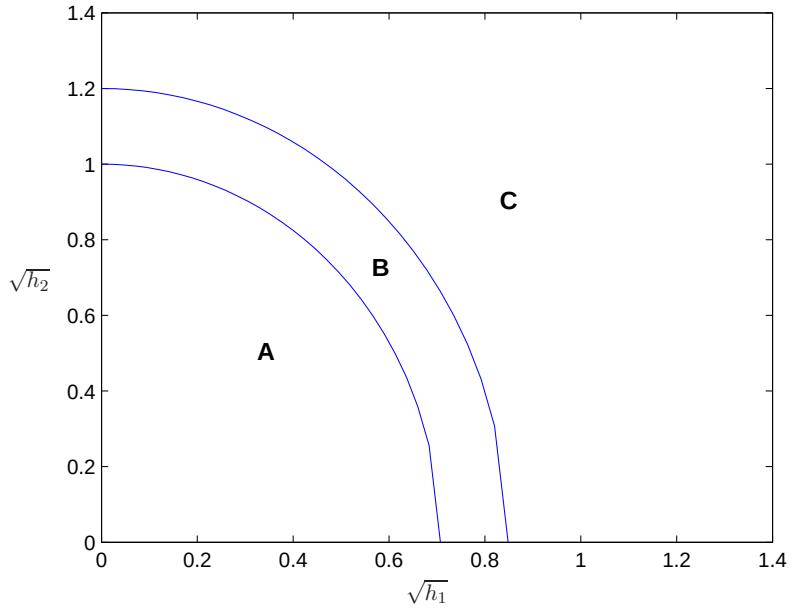

Figure 2.2: Jamming decision regions when $\gamma = 1$, $P_1 = 10$, $P_2 = 5$, $P_J = 5$ and $\sigma_N^2 = 1$.

$$J = \rho Y_e + N_J \tag{2.29}$$

Here, we will prove that in the eavesdropping case as well, linear jamming and Gaussian signalling is a game solution. The proof of the optimality of Gaussian signalling, when the jammer is linear is similar to the previous section as follows. Using (2.1), (2.28) and (2.29), if the jammer is linear, the received signal is

$$Y = (\sqrt{h_1} + \rho\sqrt{\gamma g_1})X_1 + (\sqrt{h_2} + \rho\sqrt{\gamma g_2})X_2 + \rho\sqrt{\gamma}N_e + \sqrt{\gamma}N_J \tag{2.30}$$

which is an AWGN multiple access channel, therefore, the best signalling for the users is Gaussian.

However, when it comes to showing the optimality of linear jamming when the users employ Gaussian signalling, the method of the previous section cannot be used, since from (2.28) and (2.29), the values of $E[X_1J]$ and $E[X_2J]$ that are achievable through linear jamming, should further satisfy

$$\frac{E[X_1J]}{\sqrt{g_1}} = \frac{E[X_2J]}{\sqrt{g_2}} \tag{2.31}$$

Therefore, linear jamming may not achieve all $|\mathbf{\Lambda}|$ values in (2.12) that are allowed under the power constraints. Here, we show the optimality of linear jamming, by setting up an equivalent multiple access channel. Define random variables Z_1 and Z_2 in terms of X_1 and X_2 as

$$Z_1 = X_1 + \frac{\sqrt{g_2}}{\sqrt{g_1}}X_2 \tag{2.32}$$

$$Z_2 = -\frac{\sqrt{g_1g_2}P_2}{g_1P_1 + g_2P_2}X_1 + \frac{g_1P_1}{g_1P_1 + g_2P_2}X_2 \tag{2.33}$$

It is straightforward to verify that Z_1 and Z_2 are uncorrelated, and hence, independent Gaussian random variables. Moreover, since the two pairs have a one-to-one relation, they result in the same input/output mutual information, i.e., $I(X_1, X_2; Y) = I(Z_1, Z_2; Y)$ [13]. Therefore, the game's objective function can be replaced with $I(Z_1, Z_2; Y)$. Now, using (2.1), (2.32) and (2.33), we can rewrite Y in terms of Z_1 and Z_2 as

$$Y = u_1Z_1 + u_2Z_2 + \sqrt{\gamma}J + N \tag{2.34}$$

where

$$u_1 = \frac{\sqrt{g_1}}{g_1 P_1 + g_2 P_2}(\sqrt{g_1 h_1} P_1 + \sqrt{g_2 h_2} P_2) \tag{2.35}$$

$$u_2 = \sqrt{h_2} - \sqrt{h_1}\frac{\sqrt{g_2}}{\sqrt{g_1}} \tag{2.36}$$

We can also write the eavesdropping signal received at the jammer using (2.28), (2.32) and (2.33) as

$$Y_e = \sqrt{g_1} Z_1 + N_e \tag{2.37}$$

Note that Y_e is independent of Z_2. Equations (2.34) and (2.37) define a two user, one jammer system, depicted in Figure 2.3, where the jammer has eavesdropping information only about one of the users, which is the key in proving the optimality of linear jamming as follows. We rewrite the equivalent input/output mutual information as

$$I(Z_1, Z_2; Y) = h(Z_1, Z_2) - h(Z_1, Z_2|Y) \tag{2.38}$$

The jammer's strategy can only affect the second term above,

$$h(Z_1, Z_2|Y) = h(Z_1 - a_1 Y, Z_2 - a_2 Y|Y) \tag{2.39}$$

$$\leq h(Z_1 - a_1 Y, Z_2 - a_2 Y) \tag{2.40}$$

$$\leq \frac{1}{2}\log(1 + |\mathbf{\Sigma}|) \tag{2.41}$$

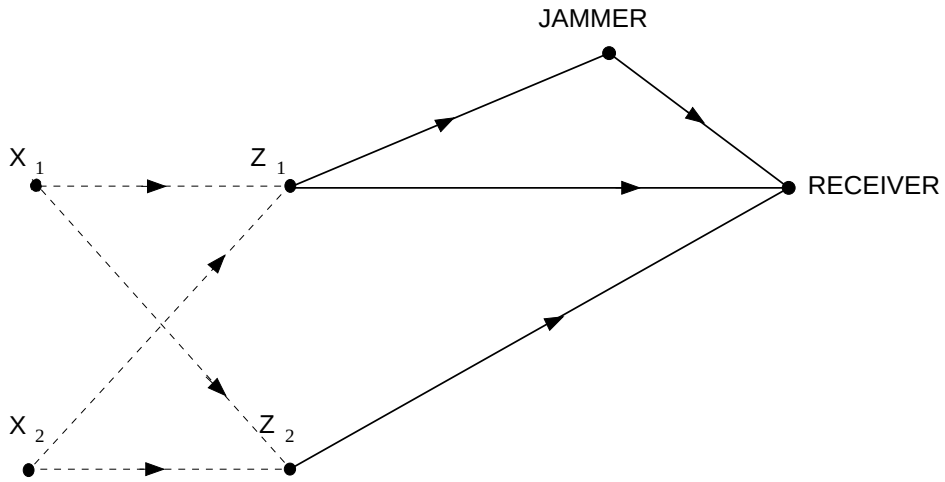

Figure 2.3: An interpretation of a communication system with two users and one jammer with eavesdropping information.

where $\mathbf{\Sigma}$ is the covariance matrix of $Z_1 - a_1 Y$ and $Z_2 - a_2 Y$. Following steps similar to those in the previous section, when the users are Gaussian, employing linear jamming together with a good choice of a_1 and a_2 can make both inequalities hold with equality, and $|\mathbf{\Sigma}|$ will only be a function of $E[Z_1 J]$ and $E[Z_2 J]$. However, Z_2 and J are independent and $E[Z_2 J] = 0$, therefore, $|\mathbf{\Sigma}|$ is only a function of $E[Z_1 J]$. In the sequel, we show that all $E[Z_1 J]$ values that are achievable by all feasible jamming signals, are also achievable by some feasible linear jamming signal, and therefore, linear jamming achieves (2.40) and (2.41) with equality and also achieves the largest possible upper bound in (2.41).

Using (2.37), the linear least squared error (LLSE) estimate of Z_1 from Y_e is [17]

$$\tilde{Z}_1(Y_e) = \frac{E[Z_1 Y_e]}{E[Y_e^2]} Y_e \tag{2.42}$$

$$= \frac{\sqrt{g_1} E[Z_1^2]}{\sigma_{N_e}^2 + g_1 E[Z_1^2]} Y_e \tag{2.43}$$

and the LLSE estimate error is

$$E[(\tilde{Z}_1(Y_e) - Z_1)^2] = \frac{\sigma_{N_e}^2 E[Z_1^2]}{\sigma_{N_e}^2 + g_1 E[Z_1^2]} \tag{2.44}$$

Since Z_1 and N_e are Gaussian, this estimate is also the minimum mean squared error (MMSE) estimate of Z_1, therefore, any other estimate of Z_1 results in a higher mean squared error. Now consider any jamming signal J which is a function of Y_e, i.e., $J = f(Y_e)$, where f is a potentially random function. The LLSE estimate of Z_1 from J is

$$\hat{Z}_1 = \frac{E[Z_1 J]}{E[J^2]} J \tag{2.45}$$

and the estimate error is

$$E[(\hat{Z}_1 - Z_1)^2] = E[Z_1^2] - \frac{E^2[Z_1 J]}{E[J^2]} \tag{2.46}$$

This is also another estimator of Z_1 from Y_e, hence the estimation error in $\hat{Z}_1$ is greater than or equal to the estimation error in $\tilde{Z}_1$

$$E[Z_1^2] - \frac{E^2[Z_1 J]}{E[J^2]} \geq \frac{\sigma_{N_e}^2 E[Z_1^2]}{\sigma_{N_e}^2 + g_1 E[Z_1^2]} \tag{2.47}$$

Therefore, the feasible values of $E[Z_1 J]$ should satisfy

$$E^2[Z_1 J] \leq \frac{g_1 E^2[Z_1^2] E[J^2]}{\sigma_{N_e}^2 + g_1 E[Z_1^2]} \tag{2.48}$$

$$= \frac{g_1 E^2[Z_1^2] P_J}{\sigma_{N_e}^2 + g_1 E[Z_1^2]} \tag{2.49}$$

Meanwhile, using (2.37), the achievable ρ values for a linear jammer satisfy

$$\rho^2 \leq \frac{P_J}{\sigma_{N_e}^2 + g_1 E[Z_1^2]} \tag{2.50}$$

Also, from (2.29) and (2.37), for a linear jammer, $E[Z_1 J] = \rho \sqrt{g_1} E[Z_1^2]$, which together with (2.50) results in that linear jamming can achieve all $E[Z_1 J]$ values satisfying

$$E^2[Z_1 J] \leq \frac{g_1 E^2[Z_1^2] P_J}{\sigma_{N_e}^2 + g_1 E[Z_1^2]} \tag{2.51}$$

The right hand sides of (2.49) and (2.51) are identical, where the former limits the $E[Z_1 J]$ values for all feasible jammers, and the latter describes all the $E[Z_1 J]$ values that are achievable with linear jamming. We conclude that for any signal in the set of feasible jamming signals, there is an equivalent linear jamming signal which results in the same upper bound in (2.41), which means that there exists a feasible linear jamming signal which is as effective as any other feasible jamming signal, and this concludes the proof.

We now derive the jamming coefficient for an optimal linear jammer with eaves-

dropping information. Using (2.28) and (2.29), the jamming signal is

$$J = \rho(\sqrt{g_1}X_1 + \sqrt{g_2}X_2 + N_e) + N_J \tag{2.52}$$

and the received signal is as in (2.30). The jammer's optimization problem is

$$\begin{aligned} \min_{\{\rho,\sigma^2_{N_J}\}} \quad & \frac{(\sqrt{h_1} + \rho\sqrt{\gamma g_1})^2 P_1 + (\sqrt{h_2} + \rho\sqrt{\gamma g_2})^2 P_2}{\gamma\rho^2\sigma^2_{N_e} + \gamma\sigma^2_{N_J} + \sigma^2_N} \\ \text{s.t.} \quad & \rho^2(g_1P_1 + g_2P_2 + \sigma^2_{N_e}) + \sigma^2_{N_J} \leq P_J \end{aligned} \tag{2.53}$$

The KKTs for this problem result in a third degree equation in ρ and can be solved using numerical optimization.

Figure 2.4 shows the SNR as a function of one of the channel coefficients h_1. The SNR is compared in two scenarios, when the jammer eavesdrops, and when it has full information about the user signals. We observe that at very low h_1, the patterns of the two scenarios differ considerably, while for very large values of h_1, they follow the same monotone SNR pattern. This is in fact expected, since at very small channel attenuations, the jammer with complete information is able to cancel a good portion of the user signals, while the noise in the eavesdropping channel restricts the eavesdropping jammer in doing the same. Also, when the channel attenuation is very high, in both scenarios, the jammer uses most of its power for adding noise, and therefore, they both follow the same pattern. However, when the jammer has full information about the user signals, the jamming coefficients are proportional to the user channel attenuations, and therefore, the jamming coefficient for the second user

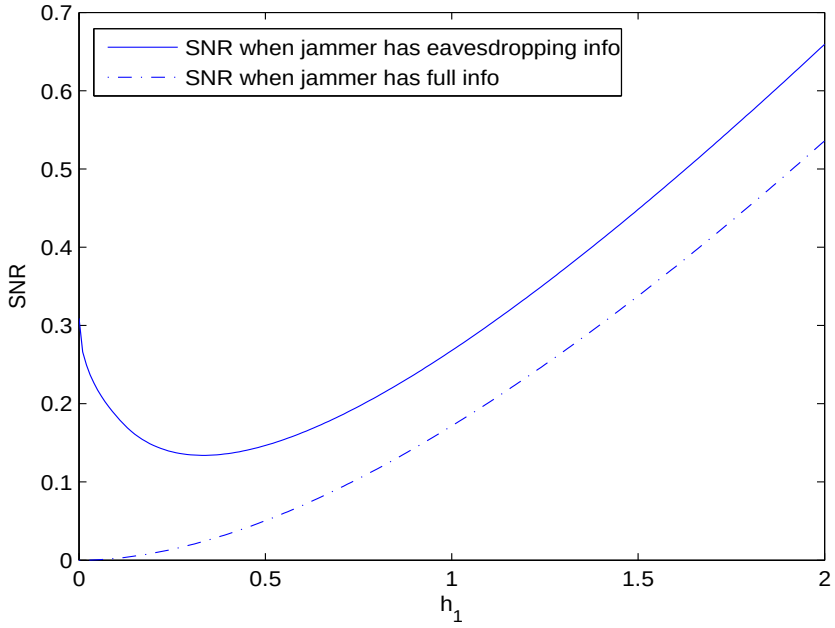

Figure 2.4: SNR as a function of h_1 when $h_2 = g_1 = g_2 = \gamma = 1$ and the powers are $P_1 = P_2 = P_J = \sigma_N^2 = 1$, for the cases when the jammer has full information and when it has eavesdropping information.

is very small compared to the first user, while when the jammer has eavesdropping information, the jamming coefficient is the same for both users. This causes the difference between the two scenarios at high SNR.

2.3 Jamming in Fading Multi-user AWGN Channels

We now investigate the optimum user/jammer strategies when the channels are fading. Throughout this section, we use the term CSI, for the channel state information on the links from the users to the receiver, and assume that the link between the jammer and the receiver is non-fading. This section is divided into three parts corresponding to three different assumptions: 1) no CSI at the transmitters, 2) uncorrelated jamming with full CSI at the transmitters, and 3) correlated jamming with

full CSI at the transmitters. In each part, the receiver is assumed to know the CSI, while various assumptions are made on the availability of the CSI at the jammer.

The problem of correlated jamming in single-user MIMO fading channels, with the assumption that the transmitter and the jammer do not have the CSI, but the receiver has the CSI, has been investigated in [2], and it has been shown that the best strategies for the user and the jammer is to evenly spread their powers over their corresponding transmit antennas, and transmit independent Gaussian signals, and the jammer is better off disregarding its information about the user signal. The problem of uncorrelated jamming in single-user MISO fading channels has also been investigated in [3], where the user and jammer are restricted to employ Gaussian signalling. In [3], both the user channel and the jammer channel are considered to have fading, and also it is assumed that the user and jammer may or may not have access to the CSI of their own channels, but they do not have access to the CSI of their opponent's channel.

2.3.1 No CSI at the Transmitters

When the transmitters do not have the CSI, it is reasonable to assume that the jammer does not have the CSI either. In the sequel, we show that the jammer's information about the transmitted signals will be irrelevant and therefore, it will not make any difference whether it has perfect or noisy information about the transmitted signals. This is a multi-user generalization of the results of [2] in a SISO system.

Assuming that the user links are fading and the jammer link is non-fading, the

received signal is

$$Y = H_1 X_1 + H_2 X_2 + \sqrt{\gamma} J + N \tag{2.54}$$

The receiver is assumed to know the fading coefficients while the users and the jammer only know the fading statistics. Here, we assume that all the random variables are complex valued and H_1 and H_2 are circularly symmetric complex Gaussian. Following [2] in finding the saddle point solution of the mutual information game by conditioning on the fading coefficients,

$$I(Y, H_1, H_2; X_1, X_2) = h(X_1, X_2) - h(X_1, X_2 | Y, H_1, H_2) \tag{2.55}$$

$$= h(X_1, X_2) - h(X_1 - A_1 Y, X_2 - A_2 Y | Y, H_1, H_2) \tag{2.56}$$

where A_1 and A_2 are functions of H_1 and H_2. The jammer's strategy can only affect the second term above

$$h(X_1 - A_1 Y, X_2 - A_2 Y | Y, H_1, H_2) \leq h(X_1 - A_1 Y, X_2 - A_2 Y | H_1, H_2) \tag{2.57}$$

$$\leq E\left[\frac{1}{2} \log\left((2\pi e)^2 |\mathbf{\Lambda}|\right)\right] \tag{2.58}$$

where $\mathbf{\Lambda}$ is the covariance matrix of

$$(X_1 - A_1 Y, X_2 - A_2 Y | H_1, H_2)$$

and the expectation in (2.58) is over the joint distribution of H_1 and H_2. Choosing

$$A_i = \frac{E[X_i Y|H_1, H_2]}{E[Y^2|H_1, H_2]},\ i = 1, 2 \tag{2.59}$$

makes $X_1 - A_1 Y$ and $X_2 - A_2 Y$ conditionally uncorrelated with Y, given H_1 and H_2. Following arguments similar to those in the previous section, since X_1 and X_2 are Gaussian, linear jamming makes J, and therefore Y jointly Gaussian with X_1 and X_2, and the above two inequalities hold with equality. Now, we need to show that linear jamming can also achieve the highest upper bound in the second inequality. First note that X_1, X_2 and J are independent of H_1 and H_2, hence

$$E[X_i Y|H_1, H_2] = H_i P_i + \sqrt{\gamma} E[X_i J|H_1, H_2] \tag{2.60}$$

$$= H_i P_i + \sqrt{\gamma} E[X_i J], \qquad i = 1, 2 \tag{2.61}$$

where (2.61) holds since X_1, X_2 and J are independent of H_1 and H_2. Therefore, the second upper bound above is only a function of $E[X_i J],\ i = 1, 2$. The rest of the arguments in the previous section follow, resulting in that linear jamming can achieve the highest upper bound in the second inequality, which concludes the proof.

The strategies corresponding to the game solution will be Gaussian signalling and linear jamming. The jamming signal is as in (2.6), and the received signal is

$$Y = (H_1 + \sqrt{\gamma}\rho_1)X_1 + (H_2 + \sqrt{\gamma}\rho_2)X_2 + \sqrt{\gamma} N_J + N \tag{2.62}$$

The last step is to find the best ρ_1 and ρ_2. Given that the jammer knows the statistics of the fading, its optimization problem is

$$\min_{\{\rho_1,\rho_2,\sigma^2_{N_J}\}} \quad \frac{1}{2}E\left[\log\left(1+\frac{|H_1+\sqrt{\gamma}\rho_1|^2P_1+|H_2+\sqrt{\gamma}\rho_2|^2P_2}{\gamma\sigma^2_{N_J}+\sigma^2_N}\right)\right] \tag{2.63}$$

$$\text{s.t.} \quad \rho_1^2P_1+\rho_2^2P_2+\sigma^2_{N_J}\leq P_J \tag{2.64}$$

The function in (2.63) is very similar to (2.19), except for the expectation taken over the channel states. The jamming coefficients ρ_1 and ρ_2 in (2.63) and (2.64) are independent of H_1 and H_2. Distributions of H_1 and H_2 are centered around zero, therefore intuitively, shifting them will make their norms larger. This fact can also be derived using [18, Theorem 1]. Therefore, the optimum jamming coefficients are $\rho_1 = \rho_2 = 0$, and the jammer disregards its complete information. We conclude that if the jammer's information is noisy, it cannot do any better than what it did when it had noiseless information, and therefore, it should disregard the incomplete information, whether the incompleteness is because of fading or AWGN or both in the jammer's eavesdropping channel.

2.3.2 Uncorrelated Jamming with CSI at the Transmitters

We now consider a two user fading channel with a jammer who does not have any information about the user signals and therefore, is uncorrelated with the users. We also assume that the user links are fading and the state of the user links are known to the users. The users are now able to distribute their powers optimally over the

user channel states. Capacity of fading channels with CSI both at the transmitter and the receiver when there is no jammer, has been investigated in [19] and [20], and optimum signalling and power allocation strategies have been derived. In this section, we consider the same problem when there is a jammer in the system. We first consider the single-user case and assume that the jamming channel is non-fading

$$Y = HX + \sqrt{\gamma}J + N \tag{2.65}$$

When the CSI is available both at the transmitter and the receiver, the maximum input/output mutual information is

$$C = I(X;Y|H) \tag{2.66}$$

where X is a random variable whose conditional distribution conditioned on H, is chosen to maximize C. The conditional input/output mutual information $I(X;Y|H)$ is a convex function of $f(y|x,h)$ for any fixed conditional input distribution $f(x|h)$, and a concave function of $f(x|h)$ for any fixed conditional transition distribution $f(y|x,h)$. Given the convexity and compactness of the space of the probability distributions, at each channel state, there is a saddle point which is to employ Gaussian signalling and linear jamming. This specifies the solution to the mutual information sub-game at any given channel state. Moreover, if a saddle point exists over all possible power allocation strategies of the user and the jammer, under user and jammer power constraints, that saddle point power allocation along with the signalling and

jamming strategies specified as the solution of the sub-games corresponding to each channel state, will give the overall solution.

We proceed with first assuming that even though the users have the CSI, the jammer does not have the CSI, and then assuming that the CSI is available both at the users and at the jammer. The latter is a reasonable assumption, since we can assume that the jammer eavesdrops the communication link from the receiver to the transmitter, where the receiver sends the CSI feedback information to the user.

If the jammer has no information about the fading channel state, the best strategy for the jammer is to transmit Gaussian noise. The received signal at fading level h is

$$Y = \sqrt{h}X + \sqrt{\gamma}N_J + N \tag{2.67}$$

and the capacity is

$$C = \frac{1}{2}E\left[\log\left(1 + \frac{hP(h)}{\sigma_N^2 + \gamma P_J}\right)\right] \tag{2.68}$$

where $P(h)$ is the user power at fading level h which should satisfy

$$E\left[P(h)\right] \leq P \tag{2.69}$$

The best user power allocation is waterfilling over the equivalent parallel AWGN

channels [19] with equivalent noise levels $(\sigma_N^2 + \gamma P_J)/h$, i.e.,

$$P(h) = \left(\frac{1}{\lambda} - \frac{\sigma_N^2 + \gamma P_J}{h}\right)^+ \tag{2.70}$$

where $(x)^+ = \max(x, 0)$, and λ is a constant chosen to enforce the user power constraint. The corresponding two user system, where the jammer is not aware of the user channel coefficients, is a straightforward extension of the results in [21] where only one user transmits at a time. The jammer will again use all its power to add Gaussian noise.

Next, we assume that the uncorrelated jammer has the CSI as well. The received signal in the single-user system is the same as in (2.67). At each channel state, the jammer transmits Gaussian noise at the power level allocated to that state. The capacity is

$$C = \frac{1}{2} E\left[\log\left(1 + \frac{hP(h)}{\sigma_N^2 + \gamma J(h)}\right)\right] \tag{2.71}$$

where $J(h)$ is the jammer power at fading level h. The user power constraint is the same as (2.69), and the jammer power constraint is

$$E\left[J(h)\right] \leq P_J \tag{2.72}$$

Since every term of the capacity corresponding to a channel state h is concave in $P(h)$ for fixed $J(h)$ and convex in $J(h)$ for fixed $P(h)$, the capacity is a concave function of P for fixed J and a convex function of J for fixed P. Given the convexity/concavity

properties of the capacity and using [15, Theorem 16, p. 75], [16, Proposition 2.6.9], and given the convexity and compactness of the space of the power allocations, the set of saddle points is compact and nonempty and therefore the mutual information game has a solution. At the game solution, the pair of strategies should satisfy the KKTs of the two optimization problems corresponding to the user and the jammer. The user maximizes (2.71) subject to (2.69), while the jammer minimizes (2.71) subject to (2.72). Writing the KKTs for each state-allocated user power, we get

$$-\frac{h}{\sigma_N^2+\gamma J(h)+hP(h)}+\lambda-\xi(h)=0 \tag{2.73}$$

where $\xi(h)$ is the complementary slackness variable for $P(h)$. Similarly, writing the KKTs for each state-allocated jammer power, we get

$$-\frac{\gamma hP(h)}{(\sigma_N^2+\gamma J(h))(\sigma_N^2+\gamma J(h)+hP(h))}+\mu-\delta(h)=0 \tag{2.74}$$

where $\delta(h)$ is the complementary slackness variable for $J(h)$.

The optimum strategies should solve (2.73) and (2.74) simultaneously. There are four possible cases at each fading level. Case 1: $P(h)>0$ and $J(h)>0$, case 2: $P(h)=0$ and $J(h)>0$, case 3: $P(h)>0$ and $J(h)=0$ and case 4: $P(h)=0$ and $J(h)=0$. If $P(h)=0$, (2.74) cannot be satisfied unless $\delta(h)>0$, therefore, case 2 never happens. This is expected, because if the user does not transmit at a fading level, the jammer does not gain anything by transmitting at that fading level. In case

1, both complementary slackness variables are zero, and (2.73) and (2.74) become

$$\frac{h}{\sigma_N^2 + \gamma J(h) + hP(h)} = \lambda \tag{2.75}$$

$$\frac{\gamma h P(h)}{(\sigma_N^2 + \gamma J(h))(\sigma_N^2 + \gamma J(h) + hP(h))} = \mu \tag{2.76}$$

which result in a linear relation between the user and jammer power allocations

$$\frac{\sigma_N^2 + \gamma J(h)}{\gamma P(h)} = \frac{\lambda}{\mu} \tag{2.77}$$

and solving for the user's power

$$P(h) = \frac{h}{\lambda(h + \gamma\frac{\lambda}{\mu})} \tag{2.78}$$

which is a monotonically increasing function of the fading variable h. Therefore, at any fading level where the user and jammer powers are nonzero, the jammer's power is a linear function of the user's, and they both allocate more power to better channel states. Case 1 is valid as long as (2.77) and (2.78) result in positive $J(h)$, which is for $P(h) > \sigma_N^2\mu/(\gamma\lambda)$ or $h > \sigma_N^2\gamma\lambda/(\gamma - \sigma_N^2\mu)$. For $h < \sigma_N^2\gamma\lambda/(\gamma - \sigma_N^2\mu)$, $J(h) = 0$ which results in cases 3 and 4 combined. In this case (2.73) will turn to waterfilling. Therefore, combining all of these, the optimum power allocations are

$$P(h) = \begin{cases} (\frac{1}{\lambda} - \frac{\gamma\sigma_N^2}{h})^+ & \text{if} \quad h < \frac{\sigma_N^2\gamma\lambda}{\gamma - \sigma_N^2\mu} \\ \frac{h}{\lambda(h+\gamma\frac{\lambda}{\mu})} & \text{if} \quad h \geq \frac{\sigma_N^2\gamma\lambda}{\gamma - \sigma_N^2\mu} \end{cases} \tag{2.79}$$

and

$$J(h) = \begin{cases} 0 & \text{if} \quad h < \frac{\sigma_N^2 \gamma \lambda}{\gamma - \sigma_N^2 \mu} \\ \frac{h}{\mu(h + \gamma \frac{\lambda}{\mu})} - \frac{\sigma_N^2}{\gamma} & \text{if} \quad h \geq \frac{\sigma_N^2 \gamma \lambda}{\gamma - \sigma_N^2 \mu} \end{cases} \tag{2.80}$$

where λ and μ are found using the user and jammer power constraints.

Figure 2.5 shows $P(h)$ and $J(h)$ for a simple example, where the fading is assumed to be Rayleigh with parameter 1. Figure 2.5 also includes the power allocation curve for a case where there is no jammer [19], which, compared to the case with a jammer, shows that the presence of the jammer changes the power allocation strategy of the user. When there is a jammer, from our closed form solutions in (2.79) and (2.80), and from Figure 2.5, we observe that both the user and the jammer keep quiet at very low fading levels. Then, as the user channel gets better, the user starts transmitting, with more power allocated to better channels, and eventually at even better channels, the jammer starts jamming, again with more power allocated to better channels.

We now discuss the two user system where the jammer is uncorrelated but it has access to CSI. The power allocation strategies will be functions of the two channel states $\mathbf{h} = (h_1, h_2)$. The capacity is

$$C = \frac{1}{2} E \left[\log \left(1 + \frac{h_1 P_1(\mathbf{h}) + h_2 P_2(\mathbf{h})}{\sigma_N^2 + J(\mathbf{h})} \right) \right] \tag{2.81}$$

The KKTs for the users result in

$$-\frac{h_i}{\sigma_N^2 + J(\mathbf{h}) + h_1 P_1(\mathbf{h}) + h_2 P_2(\mathbf{h})} + \lambda_i - \gamma_i(\mathbf{h}) = 0, \quad i = 1, 2 \tag{2.82}$$

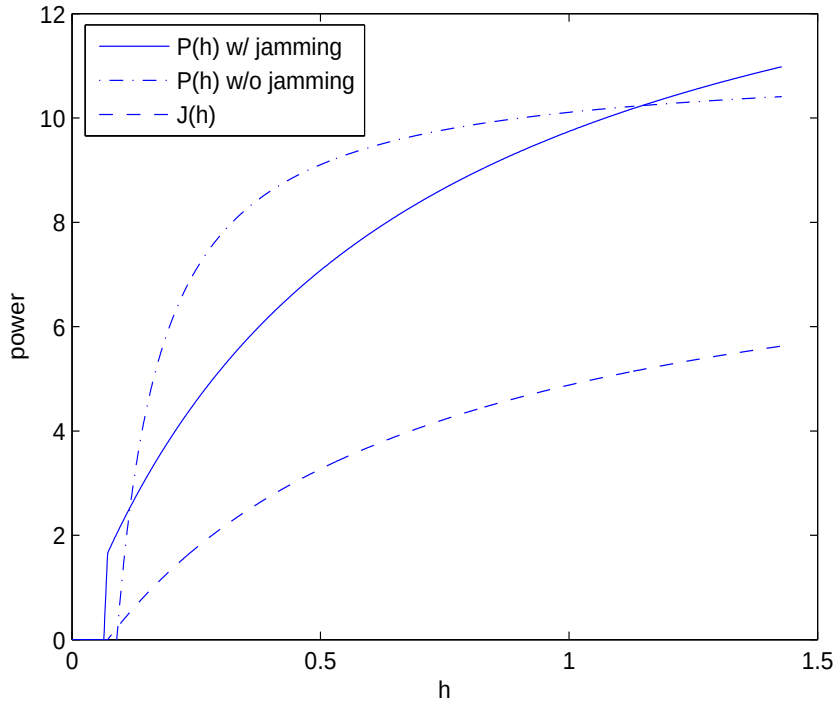

Figure 2.5: $P(h)$ and $J(h)$ for $E[P(h)] = 10$, $E[J(h)] = 5$ and $\sigma_N^2 = 1$.

where $\gamma_i(\mathbf{h})$ is the complementary slackness variables for $P_i(\mathbf{h})$, $i = 1, 2$. If at a pair of fading levels, both users transmit with nonzero powers, (2.82) results in

$$\frac{h_1}{h_2} = \frac{\lambda_1}{\lambda_2} \tag{2.83}$$

which happens with zero probability if the fading PDF is continuous. Therefore, similar to the system without a jammer in [21], only one user transmits at any given channel state. Define h as

$$h = \max\left(\frac{h_1}{\lambda_1}, \frac{h_2}{\lambda_2}\right) \tag{2.84}$$

Now, the users and the jammer power allocations are functions of h, therefore we can

replace $\mathbf{h}$ by h in the previous equations. Since the users do not transmit at the same time, we can use the single-user results to find the user power allocations

$$P_i(h) = \begin{cases} 0 & \text{if} \quad h \neq \frac{h_i}{\lambda_i} \\ \frac{1}{h_i} q(h) & \text{if} \quad h = \frac{h_i}{\lambda_i} \end{cases}, \; i = 1, 2 \tag{2.85}$$

where $q(h)$ is

$$q(h) = \begin{cases} (h - \sigma_N^2)^+ & \text{if} \quad h < \frac{\sigma_N^2}{1-\sigma_N^2 \mu} \\ \frac{h}{1+\frac{1}{h\mu}} & \text{if} \quad h \geq \frac{\sigma_N^2}{1-\sigma_N^2 \mu} \end{cases} \tag{2.86}$$

The jammer's power allocation is

$$J(h) = \begin{cases} 0 & \text{if} \quad h < \frac{\sigma_N^2}{1-\sigma_N^2 \mu} \\ \frac{1}{\mu(1+\frac{1}{h\mu})} - \sigma_N^2 & \text{if} \quad h \geq \frac{\sigma_N^2}{1-\sigma_N^2 \mu} \end{cases} \tag{2.87}$$

The strategies follow a pattern as in Figure 2.6, that is, the users do not transmit simultaneously, no party transmits at very low fading levels, as the channels get better, the user with a relatively better channel transmits, and eventually the jammer starts transmitting at even better channels. The threshold values u_1, u_2, v_1 and v_2 are to be chosen to satisfy the power constraints.

2.3.3 Correlated Jamming with CSI at the Transmitters

In this section, we consider a two user fading channel with a jammer who knows the user signals and therefore, is correlated with the users. We assume that the user links

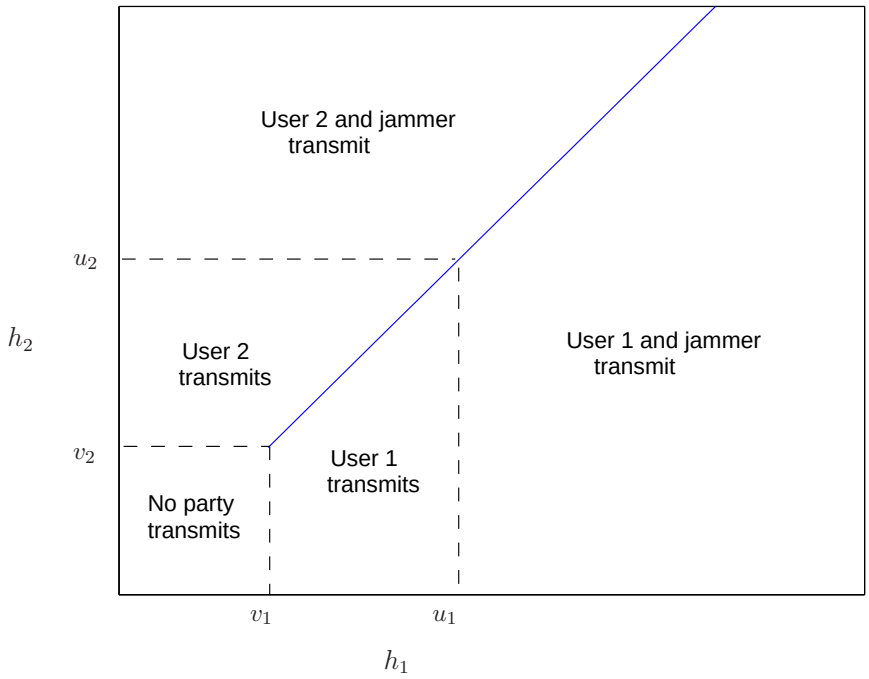

Figure 2.6: User/jammer transmission regions in uncorrelated jamming with CSI.

are fading and the state of the user links are known to the users and the correlated jammer. The users and the jammer are now able to distribute their powers optimally over the user channel states. The jammer link is again assumed to be non-fading. We first show that this game does not always have a saddle point solution, and then, we find the max-min user strategies and the corresponding jamming strategy. The max-min user power allocation corresponds to the users' best power allocation, in a situation where the user chooses its strategy only once, while after the user chooses its strategy, the jammer can observe it and choose the corresponding best jamming strategy. Note that if the game had a solution, max-min and min-max strategies would have been the same, and would also be the same as the game solution.

As in the previous sections we start with a single-user system. The input/output mutual information is as in (2.66), which is a weighted sum of the input/output

mutual information at each channel state. The user and jammer power constraints can be written as

$$E\left[E[X^2|H]\right] \leq P \tag{2.88}$$

$$E\left[E[J^2|H]\right] \leq P_J \tag{2.89}$$

$E[X^2|H = h]$ and $E[J^2|H = h]$ are the user and jammer powers allocated to the fading level $H = h$. Any pair of user and jammer strategies, results in a pair of user and jammer power allocation strategies over the user channel fading distribution. Therefore, the game's solution can be described as a pair of user and jammer power allocation strategies, along with the user and jammer signalling functions at each channel state. Using our results for the non-fading channels, we have that irrespective of the existence or non-existence of optimal power allocation functions for the user and the jammer, the sub-games always have a saddle point solution at each channel state, under any pair of user and jammer power allocation functions. The solution of the sub-games at each channel state is Gaussian signalling for the users and linear jamming for the jammer.

Since the jammer knows the channel state and the transmitted signal, the received signal is

$$Y = \left(\sqrt{h} + \rho(h)\right) X + N_J + N \tag{2.90}$$

where the variance of N_J is also a function of h, $\sigma^2_{N_J}(h)$. Given a pair of power

allocation functions $P(h)$ and $J(h)$, the capacity is

$$C = \frac{1}{2} E \left[\log \left(1 + \frac{\left(\sqrt{h} + \rho(h) \right)^2 P(h)}{\sigma_N^2 + \sigma_{N_J}^2(h)} \right) \right] \tag{2.91}$$

where for each channel state h, $\rho(h)$ and $\sigma_{N_J}^2(h)$ are the optimal linear jamming coefficients for an equivalent non-fading channel as given in Section 2.2.1, with attenuation h and user and jammer powers $P(h)$ and $J(h)$. The power constraints of the user and the jammer are as in (2.69) and (2.72).

The capacity here does not have the convexity/concavity properties in the user and jammer power allocation functions. In the sequel, we show that a pair of strategies, which is simultaneously optimal for the user and the jammer, does not always exist. We first assume that the user chooses its strategy once at the beginning of the communication, knowing that the jammer will employ the corresponding optimal jamming strategy. We then characterize the user and jammer strategies in this scenario. If the game had a saddle point solution, it would have been this pair of user and jammer strategies, however we prove the converse. We consider the resulting jamming strategy and assume that the jammer chooses this strategy at the beginning of the communication, and show that if the user had the possibility of changing its strategy, the current user strategy would have not been optimal.

First, given any user power allocation function $P(h)$, we find the jammer's best response, where a best response describes what a player does, given the other player's move [14]. In this case, a best response is the jammer's best power allocation strategy, given a fixed user power allocation strategy. The jammer's best response can also be

thought of as a pair of functions $\rho(h)$ and $\sigma^2_{N_J}(h)$ which minimizes the capacity

$$C = \frac{1}{2} E \left[\log \left(1 + \frac{\left(\sqrt{h} + \rho(h) \right)^2 P(h)}{\sigma^2_N + \sigma^2_{N_J}(h)} \right) \right] \tag{2.92}$$

and $\rho(h)$ and $\sigma^2_{N_J}(h)$ are constrained such that

$$E \left[\rho^2(h) P(h) + \sigma^2_{N_J}(h) \right] \leq P_J \tag{2.93}$$

and $\sigma^2_{N_J}(h)$ is nonnegative. The first order KKT conditions for the jammer are

$$\frac{\sqrt{h} + \rho(h)}{\sigma^2_N + \sigma^2_{N_J}(h) + (\sqrt{h} + \rho(h))^2 P(h)} + \lambda \rho(h) = 0 \tag{2.94}$$

$$-\frac{(\sqrt{h} + \rho(h))^2 P(h)}{(\sigma^2_N + \sigma^2_{N_J}(h))(\sigma^2_N + \sigma^2_{N_J}(h) + (\sqrt{h} + \rho(h))^2 P(h))} + \lambda + \xi(h) = 0 \tag{2.95}$$

where $\xi(h)$ is the complementary slackness variable for $\sigma^2_{N_J}(h)$. Whenever $\xi(h) > 0$, the jammer uses all its power to correlate with the user signal, and the optimum jamming coefficient should satisfy

$$\frac{\sqrt{h} + \rho(h)}{\sigma^2_N + (\sqrt{h} + \rho(h))^2 P(h)} + \lambda \rho(h) = 0 \tag{2.96}$$

which does not result in a closed form solution for the jammer best response. However, in order to derive the max-min user strategy, we need to have the jamming best response in terms of the user power allocation. To make the problem tractable, assume that $\sigma^2_N = 0$. Now at any channel state that the user transmits, the jammer should

also transmit, and the optimal jamming strategy should be such that $\sigma^2_{N_J}(h) > 0$, since otherwise, the capacity would be infinite. The KKTs result in

$$\rho(h) = -\min\left(\frac{1}{\lambda\sqrt{h}P(h)}, \sqrt{h}\right) \tag{2.97}$$

$$\sigma^2_{N_J}(h) = \left(\frac{1}{\lambda} - \frac{1}{\lambda^2 hP(h)}\right)^+ \tag{2.98}$$

The optimal jamming strategy is

$$\left(\rho(h), \sigma^2_{N_J}(h)\right) = \begin{cases} (-\sqrt{h}, 0) & \text{if} \quad hP(h) \leq \frac{1}{\lambda} \\ \left(-\frac{1}{\lambda\sqrt{h}P(h)}, \frac{1}{\lambda} - \frac{1}{\lambda^2 hP(h)}\right) & \text{if} \quad hP(h) > \frac{1}{\lambda} \end{cases} \tag{2.99}$$

where λ is chosen to satisfy the jammer's power constraint. The total power that the jammer allocates to each channel state is found as

$$\begin{aligned} J(h) &= \rho^2(h)P(h) + \sigma^2_{N_J}(h) \\ &= \begin{cases} hP(h) & \text{if} \quad hP(h) \leq \frac{1}{\lambda} \\ \frac{1}{\lambda} & \text{if} \quad hP(h) > \frac{1}{\lambda} \end{cases} \end{aligned} \tag{2.100}$$

which describes the best response of the jammer, to the user power allocation $P(h)$, and is shown in Figure 2.7. Note that Figure 2.7 shows the best response jammer power allocation as a function of $hP(h)$ and not $P(h)$. The capacity can now be

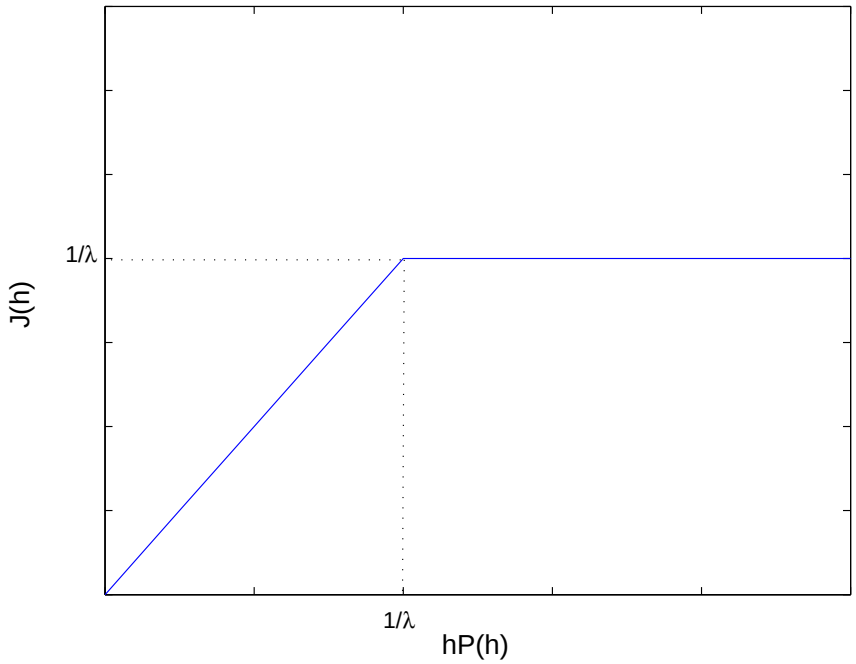

Figure 2.7: Jammer best response power allocation in correlated jamming with CSI.

written as a function of the user power allocation alone

$$C = \frac{1}{2} E \left[\log \left(1 + \frac{\left(\sqrt{h} - \min \left(\frac{1}{\lambda \sqrt{h} P(h)}, \sqrt{h} \right) \right)^2 P(h)}{\left(\frac{1}{\lambda} - \frac{1}{\lambda^2 h P(h)} \right)} \right) \right] \tag{2.101}$$

We now derive the best user power allocation that maximizes this capacity. First note that the function inside the expectation in (2.101) is zero for $hP(h) \leq 1/\lambda$, therefore, in the optimal user power allocation, $P(h)$ is either zero, or such that $hP(h) > 1/\lambda$. The capacity can now be written as

$$C = \frac{1}{2} E \left[\log \left(1 + \frac{\left(\sqrt{h} - \frac{1}{\lambda \sqrt{h} P(h)} \right)^2 P(h)}{\left(\frac{1}{\lambda} - \frac{1}{\lambda^2 h P(h)} \right)} \right) \right] \tag{2.102}$$

$$= \frac{1}{2} E \left[\log \left(\lambda \sqrt{h} P(h) \right) \right] \tag{2.103}$$

The KKT condition for the user power, whenever the user transmits, results in $P(h) = \frac{1}{\mu}$, for which the total power that the jammer allocates to the channel states is found as

$$J(h) = \begin{cases} 0 & \text{if} \quad h \leq \frac{\mu}{\lambda} \\ \frac{1}{\lambda} & \text{if} \quad h > \frac{\mu}{\lambda} \end{cases} \tag{2.104}$$

The user max-min power allocation and the corresponding jammer power allocations are illustrated in Figure 2.8 where μ and λ are chosen to satisfy the user and jammer power constraints.

Now, we show that the pair of user and jammer power allocations corresponding to the user's max-min solution does not correspond to the saddle point solution of the game. We consider the jamming strategy in (2.104) and assume that the jammer chooses this strategy at the beginning of the communication, and show that the current user strategy is not optimal. Consider two fading levels $u^+ > \mu/\lambda$ and $u^- < \mu/\lambda$ in the vicinity of $h = \mu/\lambda$ and close enough to $h = \mu/\lambda$ such that

$$u^- \simeq u^+ \simeq \mu/\lambda \tag{2.105}$$

We have $J(u^-) = 0$ and $J(u^+) = 1/\lambda$, hence, u^- and u^+ correspond to two channel states which are almost identical in their fading levels, while the jammer is active only in u^+. Obviously, it is not optimal for the user to transmit at u^+ while not transmitting at u^-, therefore, the pair of the user and jammer power allocations derived (which is the user max-min solution), is not a game solution, and the game

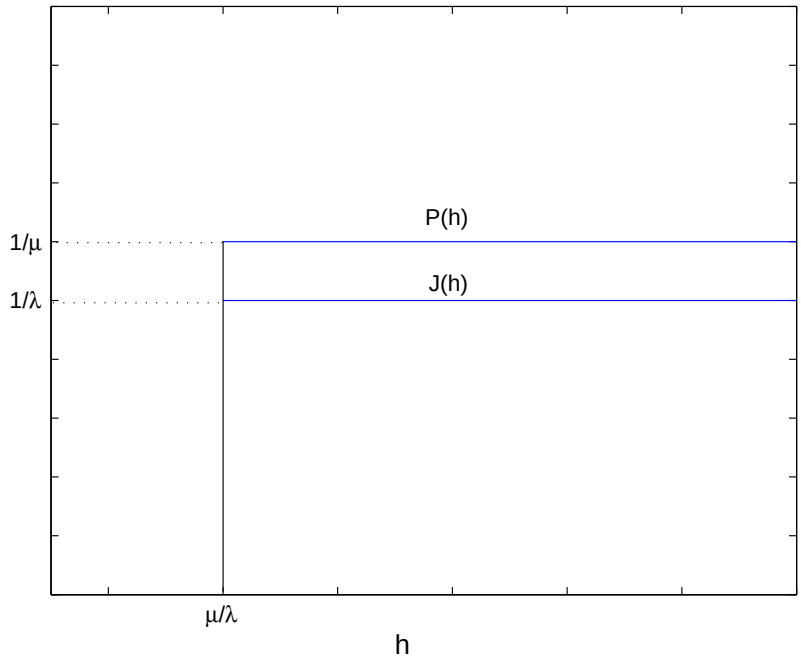

Figure 2.8: Max-min user power allocation and the corresponding jammer best response power allocation in correlated jamming with CSI.

does not admit a solution.

Even though the max-min solution derived above is not the game saddle point solution, it is the optimal pair of user and jammer strategies in a system where a conservative user would like to guarantee itself with some capacity value. It also describes the best strategy for a user which is less dynamic than the jammer in terms of changing the transmission strategy, and can choose its strategy only once.

We now extend the max-min results in the single-user system to a two user system. We show that if h_1 and h_2 are the fading levels of the first and the second user channels, again only one user transmits at any given $\mathbf{h} = (h_1, h_2)$. First, given any pair of user power allocation functions $P_1(\mathbf{h})$ and $P_2(\mathbf{h})$, we find the jammer's best response power allocation strategy. The jammer's best response can also be thought of as a set of

functions $\rho_1(\mathbf{h}), \rho_2(\mathbf{h})$ and $\sigma^2_{N_J}(\mathbf{h})$ which minimizes the capacity

$$C = \frac{1}{2} E \left[\log \left(1 + \frac{\left(\sqrt{h_1} + \rho_1(\mathbf{h})\right)^2 P_1(\mathbf{h}) + \left(\sqrt{h_2} + \rho_2(\mathbf{h})\right)^2 P_2(\mathbf{h})}{\sigma^2_N + \sigma^2_{N_J}(\mathbf{h})} \right) \right] \tag{2.106}$$

and $\rho_1(\mathbf{h}), \rho_2(\mathbf{h})$ and $\sigma^2_{N_J}(\mathbf{h})$ are constrained such that

$$E\left[\rho_1^2(\mathbf{h}) P_1(\mathbf{h}) + \rho_2^2(\mathbf{h}) P_2(\mathbf{h}) + \sigma^2_{N_J}(\mathbf{h})\right] \leq P_J \tag{2.107}$$

and $\sigma^2_{N_J}(\mathbf{h})$ is nonnegative. The first order KKT conditions for $\rho_1(\mathbf{h})$ and $\rho_2(\mathbf{h})$ are

$$\frac{\sqrt{h_1} + \rho_1(\mathbf{h})}{\sigma^2_N + \sigma^2_{N_J}(\mathbf{h}) + \left(\sqrt{h_1} + \rho_1(\mathbf{h})\right)^2 P_1(\mathbf{h}) + \left(\sqrt{h_2} + \rho_2(\mathbf{h})\right)^2 P_2(\mathbf{h})} + \lambda \rho_1(\mathbf{h}) = 0 \tag{2.108}$$

$$\frac{\sqrt{h_2} + \rho_2(\mathbf{h})}{\sigma^2_N + \sigma^2_{N_J}(\mathbf{h}) + \left(\sqrt{h_1} + \rho_1(\mathbf{h})\right)^2 P_1(\mathbf{h}) + \left(\sqrt{h_2} + \rho_2(\mathbf{h})\right)^2 P_2(\mathbf{h})} + \lambda \rho_2(\mathbf{h}) = 0 \tag{2.109}$$

which result in

$$\frac{\rho_1(\mathbf{h})}{\sqrt{h_1}} = \frac{\rho_2(\mathbf{h})}{\sqrt{h_2}} \tag{2.110}$$

Therefore, for the optimal pair of $\rho_1(\mathbf{h})$ and $\rho_2(\mathbf{h})$, we can define $\rho(\mathbf{h})$ and $P(\mathbf{h})$ such

that

$$\rho_i(\mathbf{h}) = \sqrt{h_i}\rho(\mathbf{h}),\ i = 1, 2 \tag{2.111}$$

$$P(\mathbf{h}) = h_1 P_1(\mathbf{h}) + h_2 P_2(\mathbf{h}) \tag{2.112}$$

and write the KKTs for the jammer's best response as

$$\frac{(1+\rho(\mathbf{h}))}{\sigma_N^2 + \sigma_{N_J}^2(\mathbf{h}) + (1+\rho(\mathbf{h}))^2 P(\mathbf{h})} + \lambda\rho(\mathbf{h}) = 0 \tag{2.113}$$

$$-\frac{(1+\rho(\mathbf{h}))^2 P(\mathbf{h})}{(\sigma_N^2 + \sigma_{N_J}^2(\mathbf{h}))(\sigma_N^2 + \sigma_{N_J}^2(\mathbf{h}) + (1+\rho(\mathbf{h}))^2 P(\mathbf{h}))} + \lambda + \xi(\mathbf{h}) = 0 \tag{2.114}$$

where $\xi(\mathbf{h})$ is the complementary slackness variable for $\sigma_{N_J}^2(\mathbf{h})$. From (2.113) and (2.114), the best response jamming strategy can be described in terms of $\mathbf{h}$ and $P(\mathbf{h})$. Now, for any pair of user power allocations $P_1(\mathbf{h})$ and $P_2(\mathbf{h})$ and the corresponding jamming best response, the capacity can be written as

$$C = \frac{1}{2} E\left[\log\left(1 + \frac{(1+\rho(\mathbf{h}))^2 P(\mathbf{h})}{\sigma_N^2 + \sigma_{N_J}^2(\mathbf{h})}\right)\right] \tag{2.115}$$

Assume that both users transmit at $\mathbf{h} = (h_1, h_2)$. Since the jamming best response is only a function of $\mathbf{h}$ and $P(\mathbf{h})$, the KKTs for the user power allocations can be written as

$$\frac{\mathrm{d}C}{\mathrm{d}P(\mathbf{h})}\frac{\mathrm{d}P(\mathbf{h})}{\mathrm{d}P_1(\mathbf{h})} + \lambda_1 = 0 \tag{2.116}$$

$$\frac{\mathrm{d}C}{\mathrm{d}P(\mathbf{h})}\frac{\mathrm{d}P(\mathbf{h})}{\mathrm{d}P_2(\mathbf{h})} + \lambda_2 = 0 \tag{2.117}$$

which, using (2.112), result in

$$\frac{h_1}{h_2} = \frac{\lambda_1}{\lambda_2} \tag{2.118}$$

Therefore, $P_1(\mathbf{h})$ and $P_2(\mathbf{h})$ cannot be non-zero at the same time, which means that, at any $\mathbf{h} = (h_1, h_2)$, only one user transmits. Given that only one user is active at any given time, the rest of the two user results immediately follow the results of the single-user case.

2.4 Summary and Conclusions

We characterized the saddle point solution of a mutual information game in a non-fading multiple access channel with a correlated jammer. We showed that in both cases, where the jammer knows the user signals, or it only has access to a noise corrupted version of the superposition of the user signals, the game has a solution, and the optimal strategies are Gaussian signalling for the users and linear jamming for the jammer.

In fading channels, except for the case when the jammer is correlated and both the user and the jammer have access to the user channel state, we showed that the mutual information game admits a saddle point solution, and characterized the corresponding user and jammer signalling and power allocation strategies. When the jammer is correlated and both the users and the jammer have access to the channel state, we showed that a set of simultaneously optimal power allocation functions for the users and the jammer does not always exist, and consequently characterized

the max-min user power allocation strategies and the corresponding jammer power allocation strategy.

Results of this chapter are published in [4], [5], and [6].

Chapter 3

Achievable Rates in Gaussian MISO Channels with Secrecy Constraints

The eavesdropping attack refers to the situation where an unauthorized adversary can overhear the ongoing communication. Wyner in [7] has studied this problem in an information theoretic context, where he considers a single-user wire-tap channel. The measure of secrecy is the message equivocation rate at the wire-tapper, which is defined as the entropy of the message at the wire-tapper, given the wire-tapper's observation. Wyner models the wire-tapper's channel as a *degraded* version of the channel from the transmitter to the legitimate receiver. This is in fact a reasonable assumption in a wired channel. For this channel, Wyner identifies the rate-equivocation region; the region comprised of points corresponding to the achievable communication rate, and the corresponding achievable equivocation rate. Once the rate-equivocation region is characterized, one can find the secrecy capacity, which is defined as the maximum communication rate which can be attained with perfect or complete secrecy. At the secrecy capacity, the communication rate and the equivocation rates are equal.

Wyner's result was extended to the Gaussian wire-tap channel in [22], and it was

shown that the optimal signalling strategy is Gaussian. The secrecy capacity was found to be the difference between the capacities of the main and the eavesdropping channels. It is interesting to notice that Gaussian signalling is optimal for both the main and the eavesdropping channels, but it puts the main channel at a further advantage.

Wyner's result was specific to the wire-tapping channel being a degraded version of the main channel, which is not necessarily the case in a wireless broadcast channel. Csiszar and Korner [23] studied the general single-transmitter, single-receiver, single-eavesdropper, discrete memoryless broadcast channel with secrecy constraints, and found an expression for the secrecy capacity, in the form of the maximization of the difference between two mutual informations involving an auxiliary random variable. The auxiliary random variable is interpreted as performing pre-processing on the information. The explicit calculation of the secrecy capacity for a given broadcast channel requires the solution of this maximization problem in terms of the joint distribution of the auxiliary random variable and the channel input.

The use of multiple transmit and receive antennas has been shown to increase the achievable rates when there are no secrecy constraints [24]. The Gaussian MIMO wire-tap channel is a special case of the single-transmitter, single-receiver, single-eavesdropper wire-tap channel. Since the Gaussian MIMO channel is not degraded in general, finding its secrecy capacity involves identifying the optimum joint distribution of the auxiliary random variable representing pre-processing and the channel input in the Csiszar-Korner formula. However, solving this optimization problem directly for non-degraded channels is difficult, forcing researchers typically to follow a two-

step solution, where in the first step a feasible solution is identified (an achievable scheme), and in the second step a tight upper bound that meets this feasible solution is developed (tight converse).

The first paper studying secrecy in Gaussian MIMO channels is [25], which proposes an achievable scheme, where the transmitter uses its multiple transmit antennas to transmit only in the null space of the eavesdropper's channel, thereby preventing any eavesdropping. Reference [26] studies the Gaussian single-input multiple-output (SIMO) wire-tap channel. It is shown that the Gaussian SIMO channel is essentially equivalent to a scalar Gaussian channel, therefore, the results of [22] can be used to find its secrecy capacity.

We first consider a Gaussian MISO channel under various assumptions on the channel attenuations. We assume that the channel attenuations are constants, known to all the parties. We characterize the maximum secrecy rate achievable through Gaussian signalling, and show that the Gaussian signalling that achieves the best secrecy rate is of beam-forming nature. Reference [27] reports a similar result, however, these similar results are derived independently and concurrently. Our problem is different than [25] in that we seek the optimum Gaussian signalling, while [25] investigates the performance of one specific Gaussian strategy. The results of [26] cannot be extended to our case, since the method used in [26] to find an equivalent scalar Gaussian channel cannot be used for a MISO Gaussian channel.

The secrecy rate found here for the Gaussian MISO wire-tap channel is later shown to actually be the secrecy capacity of this channel [8, 9]. Further, [8, 9] allows the eavesdropper to have multiple antennas (MISOME).

Secrecy capacity of Gaussian SISO fading channels is studied in [28–32]. Capacity-equivocation regions for fading channels are specified in [29] and [30], while [28] and [31] deal with characterizing the secrecy capacity and the corresponding power allocation strategies in fading Gaussian channels. In [32], only the eavesdropping channel is fading Gaussian, and the main channel is considered to be non-fading. Achievable secrecy rates under Gaussian signalling are characterized. The channel state of the eavesdropper is considered common knowledge in [28] and [31], while it is assumed unknown to the transmitter in [32]. We study the Gaussian MISO channel when the eavesdropping channel experiences fading. We characterize achievable secrecy rates through Gaussian signalling. It is shown that, when the eavesdropping channel experiences fading, the optimal Gaussian signalling has a unit-rank covariance matrix, and therefore, the system reduces to a SISO channel. We identify conditions under which, positive secrecy rates are achievable. Our formulation is partially similar to that of [32]. Reference [32] treats the SISO system, and we study the MISO problem, but in both cases, the main channel is constant, while the eavesdropping channel is fading and unknown to the transmitter. After we reduce the MISO system to SISO, our results overlap significantly with those of [32]. As it was also mentioned for the non-fading results of [27], here again, our results and those of [32] have been derived independently and concurrently. Our results are different than [28–32], in that they all consider single antennas for all the parties, while multiple transmit antennas are considered here. Also, our results are different than [27], in that the non-fading Gaussian MISO is studied there, while we investigate the effects of fading in Gaussian MISO channels.

Secure communications in multi-user networks, e.g., multiple access channel [33–37], broadcast channel [38], relay channel [39, 40], interference channel [41], and two-way channel [42] have been studied recently.

We use the following notations: Bold face lower and upper case letters are used to represent vectors and matrices, respectively. $\mathbf{x}^T$ and $||\mathbf{x}||$ denote the transpose and the Euclidean norm of the vector $\mathbf{x}$, respectively. trace($\mathbf{X}$) denotes the trace of the square matrix $\mathbf{X}$. Whether a variable is deterministic or random will be clear from the context.

3.1 System model

Figure 3.1 shows a communication system, with a transmitter equipped with multiple transmit antennas and a receiver and an eavesdropper, each with a single antenna. The user and eavesdropper channel attenuations can be represented by $t \times 1$ vectors $\mathbf{h}$ and $\mathbf{g}$, where t is the number of transmit antennas. The received signals at the receiver and the eavesdropper at time i are

$$y_i = \mathbf{h}^T \mathbf{x}_i + n_{y,i} \tag{3.1}$$

$$z_i = \mathbf{g}^T \mathbf{x}_i + n_{z,i} \tag{3.2}$$

where $\mathbf{x}_i$ is the transmitted signal at time i, and without loss of generality, $n_{y,i}$ and $n_{z,i}$ are unit-variance complex circularly symmetric Gaussian random variables. $\mathbf{h}$ is known and fixed. When the eavesdropper channel is non-fading, $\mathbf{g}$ is assumed to be known and fixed too. When the eavesdropper channel experiences fading, $\mathbf{g}$ is

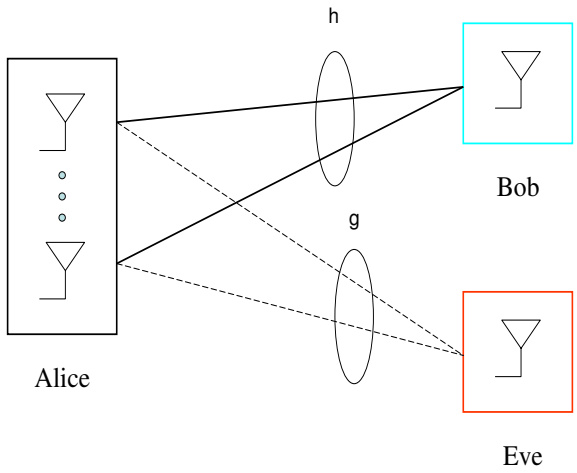

Figure 3.1: A communication system with a multi-antenna transmitter, and a single-antenna receiver and eavesdropper.

assumed to be a vector of i.i.d. zero mean unit-variance complex circularly symmetric Gaussian random variables.

A message m of rate R, is a random integer from the set $\{1, \ldots, 2^{nR}\}$, which is transmitted in n channel uses. The equivocation rate R_e, is the conditional entropy of the transmitted message, conditioned on the received signal at the eavesdropper. The equivocation rate is a measure of the amount of information that the eavesdropper can attain about the message, and quantifies the level of secrecy in the system. The secrecy capacity, C_S, is the largest rate R achievable with perfect secrecy, i.e., $R_e = R$.

3.2 Non-fading Eavesdropper Channel

Assume that $\mathbf{g}$ in (3.2) is fixed and known. From [23], the secrecy capacity of this system is

$$C_S = \max_{\mathbf{u}\to\mathbf{x}\to yz} I(\mathbf{u}; y) - I(\mathbf{u}; z) \tag{3.3}$$

Ideally, one should solve (3.3) for the optimal joint distribution of $\mathbf{u}$ and $\mathbf{x}$. We restrict ourselves to the potentially sub-optimal assumption that $\mathbf{x} = \mathbf{u}$, under which, the following rate is achievable with perfect secrecy

$$R_S = \max_{p(\mathbf{x})} \quad I(\mathbf{x}; y) - I(\mathbf{x}; z) \tag{3.4}$$

R_S would have been equivalent to the secrecy capacity C_S, if the main channel was "more capable" than the eavesdropping channel [23]. $p(\mathbf{x})$ must be chosen to maximize (3.4), but we restrict ourselves to the class of Gaussian pdfs. Our aim is to characterize the best achievable secrecy rates, under this restriction, and the input power constraint. This is in fact one further potentially sub-optimal assumption that we make, as, Gaussian signalling maximizes both terms on the right hand side of (3.4), but does not necessarily maximize the difference. Note that in the scalar Gaussian channel studied in [22], the two assumptions of $\mathbf{x} = \mathbf{u}$ and $\mathbf{x}$ being Gaussian are not sub-optimal, as the eavesdropping channel is a degraded version of the main channel.

The optimization problem of interest is now

$$R_S = \log(1 + \mathbf{h}^T \mathbf{\Sigma} \mathbf{h}) - \log(1 + \mathbf{g}^T \mathbf{\Sigma} \mathbf{g}) \tag{3.5}$$

where $\mathbf{\Sigma}$ is the covariance matrix for the channel input vector $\mathbf{x}$, and is constrained such that $\text{tr}(\mathbf{\Sigma}) \leq P$. There is no $\frac{1}{2}$ coefficient before the log terms, as, complex Gaussian vectors are involved. It remains to identify the covariance matrix $\mathbf{\Sigma}$ that maximizes R_S. This is equivalent to finding the $\mathbf{\Sigma}$ that maximizes

$$\rho(\mathbf{\Sigma}) = \frac{1 + \mathbf{h}^T \mathbf{\Sigma} \mathbf{h}}{1 + \mathbf{g}^T \mathbf{\Sigma} \mathbf{g}} \tag{3.6}$$

or, the pair $(\mathbf{V}, \mathbf{\Lambda})$ that maximizes

$$\rho(\mathbf{\Sigma}) = \frac{1 + \mathbf{a}^T \mathbf{\Lambda} \mathbf{a}}{1 + \mathbf{b}^T \mathbf{\Lambda} \mathbf{b}} \tag{3.7}$$

where $\mathbf{\Sigma} = \mathbf{V} \mathbf{\Lambda} \mathbf{V}^T$ is the eigenvalue decomposition for $\mathbf{\Sigma}$, $\mathbf{a} = \mathbf{V}^T \mathbf{h}$ and $\mathbf{b} = \mathbf{V}^T \mathbf{g}$. We first show that $\mathbf{\Lambda}$ should have only one non-zero component, equal to P, and therefore, the optimal $\mathbf{\Sigma}$ should be unit-rank.

The optimization function can be rewritten as

$$\rho(\mathbf{\Sigma}) = \frac{1 + \mathbf{a}^T \mathbf{\Lambda} \mathbf{a}}{1 + \mathbf{b}^T \mathbf{\Lambda} \mathbf{b}} \tag{3.8}$$

$$= \frac{1 + \sum_{i=1}^{t} a_i^2 \lambda_i}{1 + \sum_{i=1}^{t} b_i^2 \lambda_i} \tag{3.9}$$

For a fixed $\mathbf{V}$, we show that either all eigenvalues are zero, or there is only one nonzero

eigenvalue equal to P, depending on the parameters a_i and b_i.

1. If

$$a_i^2 < b_i^2, \qquad i = 1, \ldots, t \tag{3.10}$$

then for all values of $\mathbf{\Lambda}$, $\rho(\mathbf{\Sigma}) \leq 1$. Its maximum value $\rho(\mathbf{\Sigma}) = 1$ happens when $\mathbf{\Lambda} = 0$ and the user stays quiet. This situation can be interpreted as the case were the eavesdropping channel is strictly better than the user channel, and therefore, it is not possible to transmit information at any positive rate with perfect secrecy $R_e = R$. The corresponding rate-equivocation region in this case is empty.

2. If for some $1 \leq i \leq t$, $a_i^2 > b_i^2$, and there is unused power, increasing λ_i will increase $\rho(\mathbf{\Sigma})$. Therefore, if at least for one i, $a_i^2 > b_i^2$, the user should use all the available power. To show that the power should be used in only one direction, consider any two indices i and j, $1 \leq i, j \leq t$. Assume that $\lambda_i + \lambda_j = P_{ij} \leq P$. Fixing all other eigenvalues, the optimization function can be written as

$$\rho(\mathbf{\Sigma}) = \frac{a + b\lambda_i}{c + d\lambda_i} \tag{3.11}$$

where

$$a = 1 + \sum_{l=1, l\neq i,j}^{t} a_l^2 \lambda_l + a_j^2 P_{ij} \tag{3.12}$$

$$b = a_i^2 - a_j^2 \tag{3.13}$$

$$c = 1 + \sum_{l=1, l\neq i,j}^{t} b_l^2 \lambda_l + b_j^2 P_{ij} \tag{3.14}$$

$$d = b_i^2 - b_j^2 \tag{3.15}$$

Depending on the sign of $bc-ad$, this function is either monotonically increasing or monotonically decreasing in λ_i. Therefore, in the optimal solution, for any two indices i and j, $1 \leq i, j \leq t$, we should have either $(0, \lambda_i + \lambda_j)$ or $(\lambda_i + \lambda_j, 0)$ instead of (λ_i, λ_j). We conclude that there is only one nonzero eigenvalue, which is equal to P.

Since $\mathbf{\Sigma}$ is unit-rank, it can be written as $\mathbf{\Sigma} = P\mathbf{q}\mathbf{q}^T$ where $\mathbf{q}$ is constrained to be a unit-norm vector, i.e., $\mathbf{q}^T\mathbf{q} = 1$. Then, we can write the optimization problem as

$$\rho(\mathbf{q}) = \frac{\mathbf{q}^T\mathbf{q} + P(\mathbf{q}^T\mathbf{h})^2}{\mathbf{q}^T\mathbf{q} + P(\mathbf{q}^T\mathbf{g})^2} \tag{3.16}$$

$$= \frac{\mathbf{q}^T(\mathbf{I} + P\mathbf{h}\mathbf{h}^T)\mathbf{q}}{\mathbf{q}^T(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)\mathbf{q}} \tag{3.17}$$

$$= \frac{\mathbf{q}^T\mathbf{A}\mathbf{q}}{\mathbf{q}^T\mathbf{B}\mathbf{q}} \tag{3.18}$$

where

$$\mathbf{A} = \mathbf{I} + P\mathbf{h}\mathbf{h}^T \tag{3.19}$$

$$\mathbf{B} = \mathbf{I} + P\mathbf{g}\mathbf{g}^T \tag{3.20}$$

Now, $\rho(\mathbf{q})$ is insensitive to the scaling of $\mathbf{q}$, therefore, we can ignore the constraint on $\mathbf{q}$, find the general solution, and then scale it to have the unit-norm solution for the original problem. The problem in (3.18) is equivalent to

$$\rho(\mathbf{w}) = \frac{\mathbf{w}^T\mathbf{B}^{-1/2}\mathbf{A}\mathbf{B}^{-1/2}\mathbf{w}}{\mathbf{w}^T\mathbf{w}} \tag{3.21}$$

where $\mathbf{w} = \mathbf{B}^{1/2}\mathbf{q}$. The problem in (3.21) is a Rayleigh quotient [43] and is maximized when $\mathbf{w}$ is any scaled version of the eigenvector of $\mathbf{Z}$ corresponding to its largest eigenvalue, where

$$\mathbf{Z} = (\mathbf{I} + P\mathbf{g}\mathbf{g}^T)^{-1/2}(\mathbf{I} + P\mathbf{h}\mathbf{h}^T)(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)^{-1/2} \tag{3.22}$$

Calling this vector $\mathbf{w}^*$, the solution of the original optimization problem is

$$\mathbf{q}^* = \frac{(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)^{-1/2}\mathbf{w}^*}{\|(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)^{-1/2}\mathbf{w}^*\|} \tag{3.23}$$

It is well-known that the capacity achieving transmission strategy in a peaceful MISO channel without secrecy constraints, is to beam-form in the direction of the main channel $\mathbf{h}$ [24]. The above result shows that, with the addition of an eaves-

dropping channel, and the resulting secrecy constraints, the optimal strategy is still beam-forming, but the beam-forming direction $\mathbf{q}^*$, is "adjusted" to be as orthogonal to the eavesdropping channel direction as possible, while being as close to the main channel direction as possible.

3.3 Fading Eavesdropper Channel

We study two situations regarding the availability of the eavesdropper's channel state information. First, we assume that the channel state information of the eavesdropper is also available, similar to the setting used in [29], [30]. This can also be motivated by the assumption that the eavesdropper can be an idle user in a broadcast channel [23], [33], therefore, its channel information can be common knowledge just like the receiver channel information. Later, we make the more natural assumption that, only statistical information about the channel state of the eavesdropper is available.

If the eavesdropping channel state information is available, the transmitter can design a communication strategy for a set of parallel constant sub-channels corresponding to the set of possible fading levels of the eavesdropping channels, and also choose a power allocation strategy over those sub-channels [29]. The communication/equivocation rates at the receiver/eavesdropper, are the average communication/equivocation rates of the sub-channels [29,30], therefore, the user can choose the optimal strategy over each sub-channel independently. The focus of this chapter is on characterizing the optimal strategies at each sub-channel. It is left as future work

to determine the optimal power allocation strategies. Each sub-channel is equivalent to the non-fading MISO channel studied in the previous section.

Now, assume that there is only statistical information about the channel state of the eavesdropper. Again, the transmitter can design a communication strategy for a set of parallel constant sub-channels corresponding to the set of possible fading levels of the main channel, together with a power allocation strategy over those sub-channels. Again, we focus on characterizing the optimal strategies at each sub-channel and leave the optimal power allocation strategies for future work. Toward that end, assume that the channel of the intended receiver is constant, while the eavesdropper's channel is complex Gaussian fading. From [23], the ergodic secrecy capacity of this system is

$$C_S = \max_{\mathbf{u}\to\mathbf{x}\to y\mathbf{g}z} I(\mathbf{u};y) - I(\mathbf{u};\mathbf{g}z) \tag{3.24}$$

$$= \max_{\mathbf{u}\to\mathbf{x}\to y\mathbf{g}z} I(\mathbf{u};y) - I(\mathbf{u};z|\mathbf{g}) \tag{3.25}$$

Letting $\mathbf{x} = \mathbf{u}$, the following rate is achievable with perfect secrecy

$$R_S = \max_{p(\mathbf{x})} \quad I(\mathbf{x};y) - I(\mathbf{x};z|\mathbf{g}) \tag{3.26}$$

As before, we restrict ourselves to Gaussian, potentially sub-optimal $\mathbf{x}$, and characterize the best achievable secrecy rates. The optimization problem of interest is

therefore

$$R_S(\mathbf{\Sigma}) = \log(1 + \mathbf{h}^T\mathbf{\Sigma}\mathbf{h}) - E_{\mathbf{g}}\left[\log(1 + \mathbf{g}^T\mathbf{\Sigma}\mathbf{g})\right] \tag{3.27}$$

where $\mathbf{\Sigma}$ is the covariance matrix for the channel input vector $\mathbf{x}$, and is constrained such that $\text{tr}(\mathbf{\Sigma}) \leq P$, where P is the available input power. Let the eigenvalue decomposition for the input covariance matrix be $\mathbf{\Sigma} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^T$. The goal is to solve (3.27) for the maximizing $\mathbf{\Sigma}$, or equivalently, to solve for $\mathbf{V}$ and $\mathbf{\Lambda}$. The optimization function $R_S(\mathbf{\Sigma})$ can be rewritten as

$$R_S(\mathbf{V}, \mathbf{\Lambda}) = \log(1 + \mathbf{h}^T\mathbf{V}\mathbf{\Lambda}\mathbf{V}^T\mathbf{h}) - E_{\mathbf{g}}\left[\log(1 + \mathbf{g}^T\mathbf{V}\mathbf{\Lambda}\mathbf{V}^T\mathbf{g})\right] \tag{3.28}$$

where $\mathbf{\Lambda}$ is diagonal, and the constraints are $\mathbf{V}\mathbf{V}^T = \boldsymbol{I}$ and $\text{tr}(\mathbf{\Lambda}) \leq P$. Following [24], since $\mathbf{V}$ is unitary, and $\mathbf{g}$ is a vector of i.i.d. zero-mean complex circularly symmetric Gaussian random variables, $\mathbf{V}^T\mathbf{g}$ will have the same distribution as $\mathbf{g}$, and can be replaced by $\mathbf{g}$ in the expectation. Therefore,

$$R_S(\mathbf{V}, \mathbf{\Lambda}) = \log(1 + \mathbf{h}^T\mathbf{V}\mathbf{\Lambda}\mathbf{V}^T\mathbf{h}) - E_{\mathbf{g}}\left[\log(1 + \mathbf{g}^T\mathbf{\Lambda}\mathbf{g})\right] \tag{3.29}$$

We will first solve for the optimal $\mathbf{V}$, which affects only the first term on the right hand side of (3.29).

Define $\mathbf{a} = \mathbf{V}^T\mathbf{h}$. The constraint on $\mathbf{V}$ can be replaced by the following constraint

on $\mathbf{a}$

$$\mathbf{a}^T\mathbf{a} = \mathbf{h}^T\mathbf{V}\mathbf{V}^T\mathbf{h} = \mathbf{h}^T\mathbf{h} \tag{3.30}$$

The choice of $\mathbf{V}$ affects (3.29) only through the product term $\mathbf{a} = \mathbf{V}^T\mathbf{h}$. For any $\mathbf{a}$, one can find a matrix $\mathbf{V}$ that satisfies $\mathbf{a} = \mathbf{V}^T\mathbf{h}$, which is in fact a rotation matrix that maps $\mathbf{h}$ onto $\mathbf{a}$. Therefore, instead of solving for the best $\mathbf{V}$, one can solve for the best $\mathbf{a}$ in

$$R_S(\mathbf{V}, \mathbf{\Lambda}) = \log(1 + \mathbf{a}^T\mathbf{\Lambda}\mathbf{a}) - E_{\mathbf{g}}\left[\log(1 + \mathbf{g}^T\mathbf{\Lambda}\mathbf{g})\right] \tag{3.31}$$

for any given matrix $\mathbf{\Lambda}$. Without loss of generality, assume that the diagonal elements of $\mathbf{\Lambda}$ are in decreasing order, i.e., $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_t$. The optimal choice of $\mathbf{a}$ will then be such that

$$\mathbf{a}^T\mathbf{\Lambda}\mathbf{a} = \sum_{i=1}^{t} \lambda_i a_i^2 \tag{3.32}$$

is maximized. Given the constraint on $\mathbf{a}$ in (3.30), $\sum_{i=1}^{t} a_i^2 = \mathbf{h}^T\mathbf{h}$, and since λ_1 is larger than all other λ_i, in order to maximize the weighted sum $\sum_{i=1}^{t} \lambda_i a_i^2$, we should have

$$a_1^2 = \mathbf{h}^T\mathbf{h} \tag{3.33}$$

$$a_i = 0, \qquad i > 1 \tag{3.34}$$

This in turn shows that, the optimal unitary matrix $\mathbf{V}$, has the unit-norm vector $\frac{\mathbf{h}}{\|\mathbf{h}\|}$ as its first column, and $t-1$ arbitrary normal vectors orthogonal to $\mathbf{h}$, as the rest of its columns.

Given the optimal $\mathbf{V}$ as characterized above, it remains to find the optimal $\mathbf{\Lambda}$. The best achievable rate R_S can be written as a function of $\lambda_1, \ldots, \lambda_t$ only

$$R_S(\mathbf{\Lambda}) = \log(1 + \lambda_1 \|\mathbf{h}\|^2) - E_{\mathbf{g}} \left[\log \left(1 + \sum_{i=1}^{t} \lambda_i \|g_i\|^2 \right) \right] \tag{3.35}$$

where g_i, $i = 1, \ldots, t$ are the i.i.d. random variables in $\mathbf{g}$. Observe that the choice of λ_i, $i > 1$ only affects the second term on the right hand side of (3.35). For any fixed λ_1, given that λ_i and g_i^2 are all non-negative, the second term on the right hand side of (3.35) is increasing in λ_i, while the first term is fixed. Therefore, in order to maximize $R_S(\mathbf{\Lambda})$, the user is better off choosing $\lambda_i = 0$ for all $i > 1$, as the power constraint is $\text{trace}(\mathbf{\Sigma}) = \text{trace}(\mathbf{\Lambda}) = \sum_{i=1}^{t} \lambda_i \leq P$. This, together with (3.33) and (3.34), shows that the optimal user strategy is to transmit in the direction of $\mathbf{h}$. This beam-forming in the direction of $\mathbf{h}$ is in fact expected and intuitive, since we only have information about the main channel vector $\mathbf{h}$. This also happens to be the throughput maximizing direction in the peaceful channel without secrecy constraints as mentioned at the end of the previous section.

The secrecy rate R_S can now be written as a function of λ_1 only

$$R_S(\lambda_1) = \log(1 + \lambda_1 \|\mathbf{h}\|^2) - E_g \left[\log(1 + \lambda_1 \|g\|^2) \right] \tag{3.36}$$

where the random variable g has the same distribution as any g_i, $i = 1, \ldots, t$, and the power constraint is $\lambda_1 \leq P$.

We now characterize the best choice of λ_1 which maximizes R_S. Since there is only one parameter λ_1 to be determined, we drop the subscript and replace λ_1 by λ. First, observe that both the first and the second terms on the right hand side of (3.36) grow with λ. Let $\gamma = \|g\|^2$. Since g is complex circularly symmetric Gaussian, γ will have an exponential distribution with pdf

$$p_\gamma(\gamma) = \frac{1}{\alpha} e^{\frac{-\gamma}{\alpha}} \tag{3.37}$$

where $\alpha = 2\sigma^2$, and σ^2 is the variance of the Gaussian random variables corresponding to the real and imaginary parts of g. The parameter α characterizes the mean and the standard deviation of the exponential random variable γ. Rewriting the optimization function in terms of γ, we will have

$$R_S(\lambda) = \log(1 + \lambda\|\mathbf{h}\|^2) - E_\gamma\left[\log(1 + \lambda\gamma)\right] \tag{3.38}$$

We now discuss the behavior of $R_S(\lambda)$ as a function of λ. First, it can be observed that, since the function $f(x) = \log(1 + ax)$ is concave, using Jensen's inequality [13], we will have

$$E_\gamma\left[\log(1 + \lambda\gamma)\right] \leq \log(1 + \lambda E_\gamma\left[\gamma\right]) \tag{3.39}$$

which shows that, by choosing the right input covariance matrix, positive secrecy rate

is achievable if the combined effect of all t components of $\mathbf{h}$ is better than a single component of $\mathbf{g}$, which can occur even if $\mathbf{h}$ is much worse than $\mathbf{g}$ componentwise.

Figures 3.2 and 3.3 show $R_S(\lambda)$ as a function of λ, when γ is exponential with parameter $\alpha = 0.01$ and $\alpha = 0.1$ respectively. As both figures show, depending on the relative quality of the main and the eavesdropping channels, for some values of $\|\mathbf{h}\|^2$ and α, $R_S(\lambda)$ increases with λ, therefore, the user should use all its available power, and should beamform in the direction of $\mathbf{h}$. However, for some values of $\|\mathbf{h}\|^2$ and α, the achievable secrecy rate does not always grow with λ, and in fact, $R_S(\lambda)$ can decrease with λ. Given that our system reduces to SISO, the results reported for the SISO setting concurrently and independently in [32] agree with ours. There as well, $R_S(\lambda)$ is studied as a function of λ, and under different main and eavesdropping channel qualities. Based on the graphs presented, similar agreeing observations are made.

Based on the above observation, and as it is also discussed in [35], [25] and [32], the user is not always better off using all its available power. This raises the concern that the achievable scheme provided here, is potentially suboptimal. The source of the sub-optimality could be either the assumption that $\mathbf{x} = \mathbf{u}$ in (3.25), or later restricting $\mathbf{x}$ to be Gaussian. In [35], [25] and [32], the first assumption is targeted, and "pre-processing" of information at the transmitter is allowed, in the form of additionally injecting independent Gaussian noise by the user, or so called, "noise forwarding". Higher secrecy rates are then achieved, which shows that in fact, letting $\mathbf{x} = \mathbf{u}$ is sub-optimal. Note that, even though these techniques improve upon the achievable secrecy rates, they are yet potentially sub-optimal, and the problem of

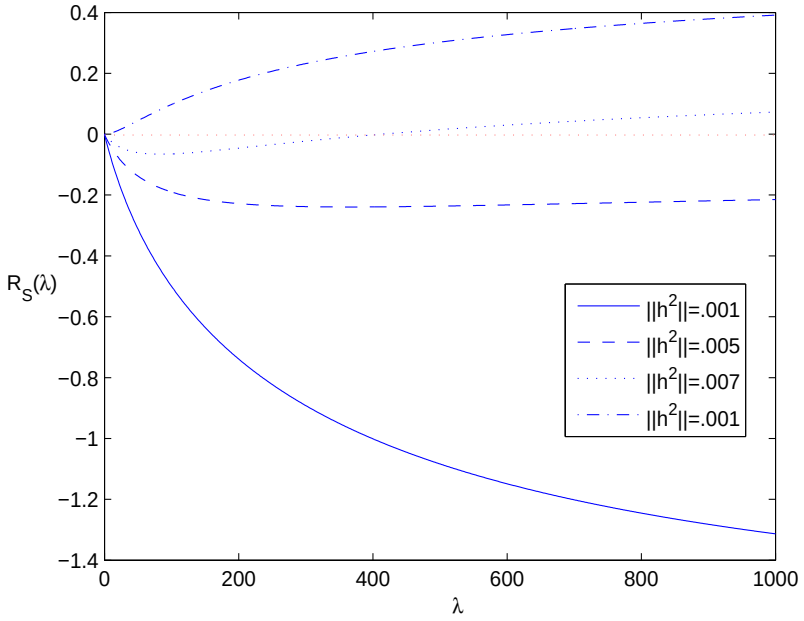

Figure 3.2: R_S as a function of λ, when γ is exponential with parameter $\alpha = .01$.

finding the optimal communication strategy remains open.

3.4 Summary and Conclusions

We studied a Gaussian MISO channel under various assumptions on the channel attenuations. When the channel attenuations are constants, known to all the parties, we found the maximum secrecy rate achievable through Gaussian signalling, and showed that the Gaussian signalling that achieves the best secrecy rate is of beamforming nature. We then studied the Gaussian MISO channel when the eavesdropping channel experiences fading. We found achievable secrecy rates through Gaussian signalling. It is shown that, when the eavesdropping channel experiences fading, the optimal Gaussian signalling has a unit-rank covariance matrix, and therefore, the system reduces to a SISO channel. We identified conditions under which, positive

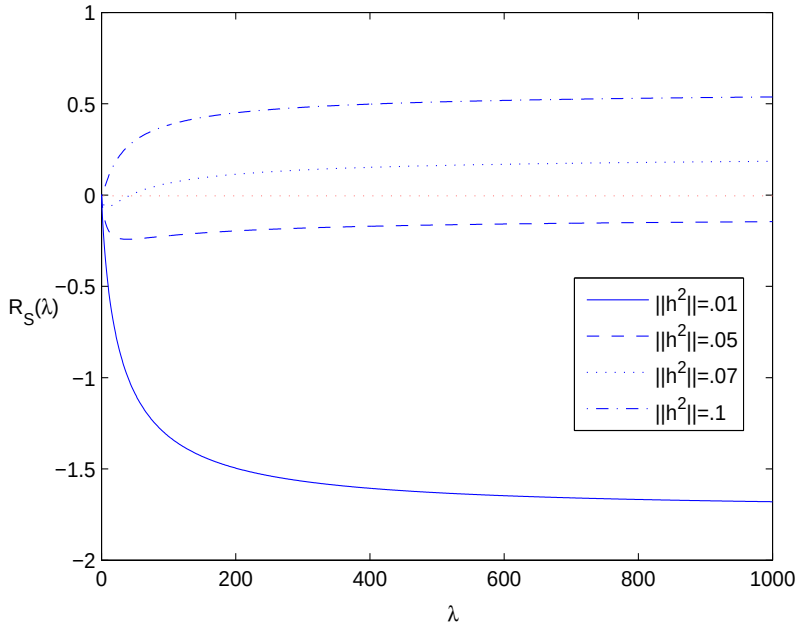

Figure 3.3: R_S as a function of λ, when γ is exponential with parameter $\alpha = .1$.

secrecy rates are achievable.

Results of this chapter are published in [10].

Chapter 4

Secrecy Capacity of the Gaussian 2-2-1 MIMO Wire-tap Channel

In the wire-tap channel studied in the previous chapter, the receiver has a single antenna. This crucial assumption results in the beam-forming transmission to be optimal, which consequently simplifies the derivations. The next step towards finding the secrecy capacity of the general Gaussian MIMO channel is to consider multiple antennas at the receiver. We consider a Gaussian MIMO channel where both the transmitter and the receiver have two antennas each, and the eavesdropper has a single antenna, hence we call this channel the Gaussian 2-2-1 MIMO wire-tap channel. We find the secrecy capacity in two steps: we first propose an achievable scheme, which is a Gaussian signalling scheme with no pre-processing of information, and then, we develop a tight upper bound that meets the rate achieved with our proposed signalling scheme. The techniques that we develop are specific to the Gaussian 2-2-1 channel, and whether they can be used for the general m-n-k channel is unclear. We first show that the optimal Gaussian signalling scheme has a unit-rank transmit covariance matrix, hence with Gaussian signalling, beam-forming is optimal. The

transmitter beam-forms in a direction that is as orthogonal to the direction of the eavesdropper, and as close to the two directions of the receiver as possible. Then, we develop an upper bound by considering a channel where the eavesdropper's signal is given to the receiver. The secrecy capacity of this channel is an upper bound to the secrecy capacity of the original channel. In addition, this channel is degraded, and no pre-processing of information is needed. Furthermore, Gaussian signalling is optimal for this channel. We further tighten this bound by allowing correlation between the additive noises of the receiver and the eavesdropper. For a certain such correlation, we prove that the optimal Gaussian signalling is unit-rank in this upper bound also. We then evaluate our upper bound and show that it meets the rate achievable with our proposed signalling scheme. In this 2-2-1 system, the fact that both in our achievable scheme and in our upper bound, the optimal transmit covariance matrices turn out to be unit-rank, proves to be crucial in enabling us to characterize the lower and upper bounds explicitly and showing that they are equal. The problem of extending this result to the more general Gaussian m-n-k channel is recently solved and the corresponding secrecy capacity is specified [44–46]. It is shown that, again Gaussian signalling and no pre-processing of information is optimal.

We use the following notations: Bold face lower and upper case letters are used to represent vectors and matrices, respectively. $\mathbf{x}^T$ and $||\mathbf{x}||$ denote the transpose and the Euclidean norm of the vector $\mathbf{x}$, respectively. trace($\mathbf{X}$) and $|\mathbf{X}|$ denote the trace and the determinant of the square matrix $\mathbf{X}$, respectively. Whether a variable is deterministic or random will be clear from the context.

4.1 System Model

Figure 4.1 shows a communication system, with a transmitter and a receiver each equipped with two antennas, and a single antenna eavesdropper. The 2-2-1 Gaussian MIMO wire-tap channel is characterized by

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}_y \tag{4.1}$$

$$z = \mathbf{g}^T\mathbf{x} + n_z \tag{4.2}$$

where $\mathbf{x}$ is the transmitted signal, and $\mathbf{y}$, z are the received signals at the legitimate user and the eavesdropper, respectively. $\mathbf{n}_y$ is a Gaussian random vector with zero-mean and identity covariance matrix, while n_z is a Gaussian random variable with zero-mean and unit-variance. $\mathbf{n}_y$, n_z are assumed to be independent. The transmitted signal satisfies an average power constraint,

$$\frac{1}{n}\sum_{i=1}^{n} E\left[\mathbf{x}_i^T\mathbf{x}_i\right] \leq P \tag{4.3}$$

The secrecy capacity $C(P)$ is defined as the maximum number of bits that can be correctly transmitted to the intended receiver while the eavesdropper is essentially no better informed about the transmitted information after observing the received signal than it was before [22].

When $\mathbf{H}$ is not full-rank, by performing singular value decomposition (SVD) on $\mathbf{H}$ and obtaining an equivalent channel by rotation, it can be shown that the system is equivalent to a 2-1-1 system, whose secrecy capacity has been found in [8, 9].

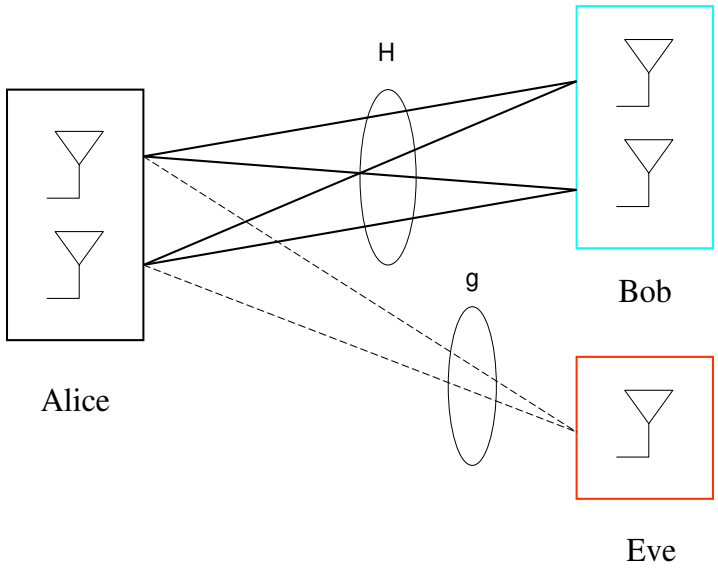

Figure 4.1: A communication system with a transmitter and a receiver each with two antennas, and a single-antenna eavesdropper.

Therefore, without loss of generality, for the rest of this chapter, we assume that $\mathbf{H}$ is full-rank, and hence is invertible. When

$$\left\|\mathbf{H}^{-T}\mathbf{g}\right\| \leq 1 \tag{4.4}$$

z can be written as a noisy version of $\mathbf{y}$, i.e., $\mathbf{r}^T\mathbf{y} + n$, which means that the channel is degraded. In this case, no pre-processing of information is necessary [23], and also it can be shown that Gaussian signalling is optimal. Thus, in this chapter, we concentrate on the more interesting and difficult case where $\mathbf{H}$ is full-rank and satisfies

$$\left\|\mathbf{H}^{-T}\mathbf{g}\right\| > 1 \tag{4.5}$$

4.2 An Achievable Scheme

By [23], the following secrecy rate is achievable,

$$[I(\mathbf{u};\mathbf{y}) - I(\mathbf{u};z)]^+ \tag{4.6}$$

where $\mathbf{u} \to \mathbf{x} \to \mathbf{y}z$. By taking $\mathbf{u} = \mathbf{x}$ and constraining the input signal $\mathbf{x}$ to be Gaussian with covariance matrix $\mathbf{S}$ such that $\text{trace}(\mathbf{S}) \leq P$, the following secrecy rate is achievable,

$$\left[\frac{1}{2}\log\left|\mathbf{I} + \mathbf{HSH}^T\right| - \frac{1}{2}\log(1 + \mathbf{g}^T\mathbf{Sg})\right]^+ \tag{4.7}$$

Thus, the following secrecy rate is achievable

$$\max_{\mathbf{S}\succeq\mathbf{0}:\text{trace}(\mathbf{S})\leq P} \quad \frac{1}{2}\log\left|\mathbf{I} + \mathbf{HSH}^T\right| - \frac{1}{2}\log(1 + \mathbf{g}^T\mathbf{Sg}) \tag{4.8}$$

unless the maximum value in (4.8) is negative, in which case, the achieved secrecy rate is zero.

Ignoring the $1/2$, we may rewrite the cost function in (4.8) as

$$\log\left|\mathbf{I} + \mathbf{HSH}^T\right| - \log\left(1 + \mathbf{g}^T\mathbf{Sg}\right) = \log\left|\mathbf{I} + \mathbf{H}^T\mathbf{HS}\right| - \log\left(1 + \mathbf{g}^T\mathbf{Sg}\right) \tag{4.9}$$

We first use the following lemma to show that the $\mathbf{S}$ that maximizes (4.8) is unit-rank.

Lemma 4.1 *If* $\mathbf{D}$ *is a* 2×2 *invertible matrix that satisfies*

$$\mathbf{g}^T \mathbf{D}^{-1} \mathbf{g} \geq 1 \tag{4.10}$$

then the optimal $\mathbf{S}$ *that solves the following optimization problem*

$$\max_{\mathbf{S} \succeq \mathbf{0}, \mathrm{tr}(\mathbf{S}) \leq P} \quad \log |\mathbf{I} + \mathbf{D}\mathbf{S}| - \log \left(1 + \mathbf{g}^T \mathbf{S} \mathbf{g}\right) \tag{4.11}$$

is unit-rank.

Proof 4.1 *The KKT necessary conditions for the optimization problem in (4.11) are*

$$\mathbf{S}^* \succeq \mathbf{0} \tag{4.12}$$

$$\mathit{trace}(\mathbf{S}^*) \leq P \tag{4.13}$$

$$\mathbf{C} \succeq \mathbf{0} \tag{4.14}$$

$$\lambda \geq 0 \tag{4.15}$$

$$\lambda(\mathit{trace}(\mathbf{S}^*) - P) = 0 \tag{4.16}$$

$$\mathbf{C}\mathbf{S}^* = \mathbf{0} \tag{4.17}$$

$$-(\mathbf{I} + \mathbf{D}\mathbf{S}^*)^{-1}\mathbf{D} + \frac{1}{1 + \mathbf{g}^T \mathbf{S}^* \mathbf{g}} \mathbf{g}\mathbf{g}^T - \mathbf{C} + \lambda \mathbf{I} = \mathbf{0} \tag{4.18}$$

We will prove the claim by contradiction. Assume that the optimal $\mathbf{S}$ *is full-rank. Then, from (4.17), it follows that* $\mathbf{C} = \mathbf{0}$*, i.e, (4.18) becomes*

$$(\mathbf{I} + \mathbf{D}\mathbf{S}^*)^{-1}\mathbf{D} = \frac{1}{1 + \mathbf{g}^T \mathbf{S}^* \mathbf{g}} \mathbf{g}\mathbf{g}^T + \lambda \mathbf{I} \tag{4.19}$$

Since $\mathbf{D}$ *is invertible*

$$(\mathbf{I}+\mathbf{D}\mathbf{S}^*)^{-1}=\frac{1}{1+\mathbf{g}^T\mathbf{S}^*\mathbf{g}}\mathbf{g}\mathbf{g}^T\mathbf{D}^{-1}+\lambda\mathbf{D}^{-1} \tag{4.20}$$

Using the matrix inversion lemma [43, page 19], we have

$$\mathbf{I}+\mathbf{D}\mathbf{S}^*=\frac{1}{\lambda}\mathbf{D}-\frac{1}{\lambda^2+\lambda^2\mathbf{g}^T\mathbf{S}^*\mathbf{g}+\lambda||\mathbf{g}||^2}\mathbf{D}\mathbf{g}\mathbf{g}^T \tag{4.21}$$

i.e.,

$$\mathbf{S}^*=\frac{1}{\lambda}\mathbf{I}-\frac{1}{\lambda^2+\lambda^2\mathbf{g}^T\mathbf{S}^*\mathbf{g}+\lambda||\mathbf{g}||^2}\mathbf{g}\mathbf{g}^T-\mathbf{D}^{-1} \tag{4.22}$$

We multiply both sides of (4.22) with $\mathbf{g}^T$ *on the left and* $\mathbf{g}$ *on the right. Let us define* $\gamma=\mathbf{g}^T\mathbf{S}^*\mathbf{g}$*, which is a non-negative real number. Then, we have*

$$\gamma=\frac{||\mathbf{g}||^2}{\lambda}-\frac{||\mathbf{g}||^4}{\lambda^2+\lambda^2\gamma+\lambda||\mathbf{g}||^2}-\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g} \tag{4.23}$$

i.e., we have

$$\gamma^2+\left(1+\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g}\right)\gamma+\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g}+\frac{||\mathbf{g}||^2}{\lambda}\left(\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g}-1\right)=0 \tag{4.24}$$

Because $\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g}-1\geq 0$*, the second-order equation in (4.24) has no non-negative roots, i.e., it either has no real roots, or it has two negative roots. Thus, we arrive at a contradiction. Therefore,* $\mathbf{C}$ *cannot be equal to* $\mathbf{0}$*, and consequently,* $\mathbf{S}$ *cannot be*

full-rank, and it has to be unit-rank.

Since $\mathbf{H}^T\mathbf{H}$ is invertible and satisfies (4.5), $\mathbf{D} = \mathbf{H}^T\mathbf{H}$ satisfies the condition of Lemma 4.1. Hence, the optimal $\mathbf{S}$ for the optimization problem in (4.8) is unit-rank.

Given that the optimal $\mathbf{S}$ is unit-rank, it can be written as

$$\mathbf{S} = P\mathbf{q}\mathbf{q}^T \tag{4.25}$$

The corresponding achievable secrecy rate is

$$R = \frac{1}{2}\log\left|\mathbf{I} + P\mathbf{H}\mathbf{q}\mathbf{q}^T\mathbf{H}^T\right| - \frac{1}{2}\log(1 + P\mathbf{g}^T\mathbf{q}\mathbf{q}^T\mathbf{g}) \tag{4.26}$$

$$= \frac{1}{2}\log\frac{\mathbf{q}^T(\mathbf{I} + P\mathbf{H}^T\mathbf{H})\mathbf{q}}{\mathbf{q}^T(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)\mathbf{q}} \tag{4.27}$$

where (4.27) is now in the Rayleigh quotient [43, page 176] form and the optimal achievable $\mathbf{q}$, which we will call $\mathbf{q}_a$, is

$$\mathbf{q}_a = \frac{\mathbf{B}^{-1/2}\mathbf{w}_a}{||\mathbf{B}^{-1/2}\mathbf{w}_a||} \tag{4.28}$$

where $\mathbf{w}_a$ is the eigenvector that corresponds to the largest eigenvalue of $\mathbf{B}^{-1/2}\mathbf{A}\mathbf{B}^{-1/2}$ with

$$\mathbf{A} = \mathbf{I} + P\mathbf{H}^T\mathbf{H} \tag{4.29}$$

$$\mathbf{B} = \mathbf{I} + P\mathbf{g}\mathbf{g}^T \tag{4.30}$$

In other words, $\mathbf{q}_a$ is the unit-norm eigenvector that satisfies

$$\left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T\right)^{-1}\left(\mathbf{I} + P\mathbf{H}^T\mathbf{H}\right)\mathbf{q}_a = \lambda_1\mathbf{q}_a \tag{4.31}$$

where λ_1 is the largest eigenvalue of the matrix

$$\left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T\right)^{-1/2}\left(\mathbf{I} + P\mathbf{H}^T\mathbf{H}\right)\left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T\right)^{-1/2} \tag{4.32}$$

Written explicitly, the achievable secrecy rate is

$$\frac{1}{2}\log\left(\frac{1 + P\mathbf{q}_a^T\mathbf{H}^T\mathbf{H}\mathbf{q}_a}{1 + P\mathbf{q}_a^T\mathbf{g}\mathbf{g}^T\mathbf{q}_a}\right) = \frac{1}{2}\log\lambda_1 \tag{4.33}$$

Next, we show that the secrecy rate in (4.33) is in fact strictly positive. By picking $\mathbf{S} = P\mathbf{g}^\perp\left(\mathbf{g}^\perp\right)^T$, where $\mathbf{g}^\perp$ is the unit-norm vector that is orthogonal to $\mathbf{g}$, an achievable secrecy rate is

$$\frac{1}{2}\log\left(1 + P\left\|\mathbf{H}\mathbf{g}^\perp\right\|^2\right) \tag{4.34}$$

Since $\mathbf{H}$ is full rank, $\mathbf{H}\mathbf{g}^\perp \neq \mathbf{0}$, i.e., the secrecy rate in (4.34) is strictly positive. Since the secrecy rate in (4.33) is the maximum over all $\mathbf{S}$ satisfying $\text{trace}(\mathbf{S}) \leq P$, we conclude that

$$\frac{1}{2}\log\lambda_1 \geq \frac{1}{2}\log\left(1 + P\left\|\mathbf{H}\mathbf{g}^\perp\right\|^2\right) > 0 \tag{4.35}$$

which also means that

$$\lambda_1 > 1 \tag{4.36}$$

4.3 A Tight Upper Bound

The following theorem provides a Sato like upper bound [47] on the secrecy capacity of the wire-tap channel described in (4.1) and (4.2).

Theorem 4.1 *An upper bound on the secrecy capacity of the wire-tap channel described in (4.1) and (4.2) is*

$$\max_{\mathbf{S}\succeq\mathbf{0},\mathrm{tr}(\mathbf{S})\leq P} U(\mathbf{S},\mathbf{a}) \tag{4.37}$$

for any $\mathbf{a}$ *with* $||\mathbf{a}|| < 1$*, where* $U(\mathbf{S},\mathbf{a})$ *is defined as*

$$U(\mathbf{S},\mathbf{a}) = \frac{1}{2}\log\frac{\left|\mathbf{I}+\mathbf{N}^{-1}\bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{(1+\mathbf{g}^T\mathbf{S}\mathbf{g})} \tag{4.38}$$

with $\mathbf{N}$ *defined as*

$$\mathbf{N} = \begin{bmatrix} \mathbf{I} & \mathbf{a} \\ \mathbf{a}^T & 1 \end{bmatrix} \tag{4.39}$$

and $\bar{\mathbf{H}}$ *defined as*

$$\bar{\mathbf{H}} = \begin{bmatrix} \mathbf{H} \\ \\ \mathbf{g}^T \end{bmatrix} \tag{4.40}$$

The proof of Theorem 4.1 is provided in the Appendix. Intuitively, this upper bound is obtained by considering the secrecy capacity of a new channel where the legitimate receiver also has access to the eavesdropper's signal. Since the legitimate user is more capable in the new channel, the secrecy capacity of the new channel will serve as an upper bound on the secrecy capacity of the original channel. The new channel is degraded, and therefore the secrecy capacity is easier to obtain.

The vector $\mathbf{a}$ introduced in Theorem 4.1 is the correlation between the Gaussian noises at the legitimate user and the eavesdropper, i.e.,

$$\mathbf{a} = E[\mathbf{n}_y n_z] \tag{4.41}$$

We note that $\mathbf{a}$ thus defined has to satisfy $||\mathbf{a}|| \leq 1$ for $\mathbf{N}$ in (4.39) to be positive semi-definite. Introducing correlation between $\mathbf{n}_y$ and n_z does not change the secrecy capacity of the channel, but changes the upper bound in (4.37). In fact, (4.37) remains a valid upper bound for any $\mathbf{a}$, with $||\mathbf{a}|| < 1$. Thus, we will smartly pick an $\mathbf{a}$ vector, and show that the upper bound with this $\mathbf{a}$ vector is in fact tight, to establish the secrecy capacity.

We rewrite $U(\mathbf{S}, \mathbf{a})$ as

$$U(\mathbf{S}, \mathbf{a}) = \frac{1}{2} \log \frac{\left|\mathbf{I} + \bar{\mathbf{H}}^T \mathbf{N}^{-1} \bar{\mathbf{H}} \mathbf{S}\right|}{(1 + \mathbf{g}^T \mathbf{S} \mathbf{g})} \tag{4.42}$$

By the definition of $\mathbf{N}$ in (4.39), we have

$$\mathbf{N}^{-1} = \begin{bmatrix} \mathbf{I} + \frac{1}{k}\mathbf{a}\mathbf{a}^T & -\frac{1}{k}\mathbf{a} \\ -\frac{1}{k}\mathbf{a}^T & \frac{1}{k} \end{bmatrix} \tag{4.43}$$

where $k = 1 - ||\mathbf{a}||^2$. Then,

$$\bar{\mathbf{H}}^T \mathbf{N}^{-1} \bar{\mathbf{H}} = \mathbf{H}^T \mathbf{H} + \frac{1}{k} \mathbf{H}^T \mathbf{a}\mathbf{a}^T \mathbf{H} - \frac{1}{k} \mathbf{g}\mathbf{a}^T \mathbf{H} - \frac{1}{k} \mathbf{H}^T \mathbf{a}\mathbf{g}^T + \frac{1}{k} \mathbf{g}\mathbf{g}^T \tag{4.44}$$

$$= \mathbf{H}^T \mathbf{H} + \frac{1}{k} \left(\mathbf{H}^T \mathbf{a} - \mathbf{g}\right) \left(\mathbf{H}^T \mathbf{a} - \mathbf{g}\right)^T \tag{4.45}$$

Let us define $\mathbf{A}(\mathbf{a})$ as

$$\mathbf{A}(\mathbf{a}) = \bar{\mathbf{H}}^T \mathbf{N}^{-1} \bar{\mathbf{H}} = \mathbf{H}^T \mathbf{H} + \frac{1}{k} \left(\mathbf{H}^T \mathbf{a} - \mathbf{g}\right) \left(\mathbf{H}^T \mathbf{a} - \mathbf{g}\right)^T \tag{4.46}$$

Then, $U(\mathbf{S}, \mathbf{a})$ in (4.42) is written as

$$U(\mathbf{S}, \mathbf{a}) = \frac{1}{2} \log \left|\mathbf{I} + \mathbf{A}(\mathbf{a})\mathbf{S}\right| - \frac{1}{2} \log \left(1 + \mathbf{g}^T \mathbf{S} \mathbf{g}\right) \tag{4.47}$$

Let us also define $\mathbf{q}_a^{\perp}$ to be the unit-norm vector that is orthogonal to $\mathbf{q}_a$, which is defined in (4.28).

We pick $\mathbf{a}$ to be of the form

$$\mathbf{a} = \mathbf{H}^{-T}\left(\alpha \mathbf{q}_a^{\perp} + \mathbf{g}\right) \tag{4.48}$$

for any real number α that makes $||\mathbf{a}|| < 1$. $\alpha = 0$ results in $\mathbf{a} = \mathbf{H}^{-T}\mathbf{g}$, which is a vector with norm greater than 1, and therefore, is not permissible.

Then, with this selection of $\mathbf{a}$, $\mathbf{A}(\mathbf{a})$ in (4.46) can be written as

$$\mathbf{A}(\mathbf{a}) = \mathbf{H}^T\mathbf{H} + \theta(\alpha)\mathbf{q}_a^{\perp}\left(\mathbf{q}_a^{\perp}\right)^T \tag{4.49}$$

where $\theta(\alpha)$ is defined as

$$\theta(\alpha) = \frac{\alpha^2}{1 - \mathbf{a}^T\mathbf{a}} \tag{4.50}$$

$$= \frac{\alpha^2}{1 - \left(\mathbf{H}^{-T}\left(\alpha \mathbf{q}_a^{\perp} + \mathbf{g}\right)\right)^T\left(\mathbf{H}^{-T}\left(\alpha \mathbf{q}_a^{\perp} + \mathbf{g}\right)\right)} \tag{4.51}$$

Then, we have

$$\frac{1}{\theta(\alpha)} = -\left(\mathbf{q}_a^{\perp}\right)^T\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{q}_a^{\perp} - \frac{2\mathbf{g}^T\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{q}_a^{\perp}}{\alpha} - \frac{\mathbf{g}^T\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{g} - 1}{\alpha^2} \tag{4.52}$$

This is a second-order polynomial in terms of $1/\alpha$, and it is easy to see that $1/\alpha^*$ maximizes $\theta(\alpha)$, with

$$\frac{1}{\alpha^*} = \frac{\mathbf{g}^T\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{q}_a^{\perp}}{1 - \mathbf{g}^T\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{g}} \tag{4.53}$$

Finally, we call the $\mathbf{a}$ vector that we pick $\mathbf{a}^*$, which is given as

$$\mathbf{a}^* = \mathbf{H}^{-T}\left(\alpha^* \mathbf{q}_a^{\perp} + \mathbf{g}\right) \tag{4.54}$$

First, we will prove that $\mathbf{a}^*$ has norm no greater than 1. Let us define $\mathbf{a}_0$ to be

$$\mathbf{a}_0 = \frac{\mathbf{g}^T \mathbf{q}_a}{||\mathbf{H}\mathbf{q}_a||^2} \mathbf{H}\mathbf{q}_a \tag{4.55}$$

$\mathbf{a}_0$ satisfies the form of $\mathbf{a}$ in (4.48) because $\mathbf{H}^T\mathbf{a}_0 - \mathbf{g}$ is orthogonal to $\mathbf{q}_a$, hence, it is along the direction of $\mathbf{q}_a^{\perp}$. Therefore, $\mathbf{a}_0$ must correspond to an α, which we call α_0. It can be seen that

$$||\mathbf{a}_0|| = \frac{\left|\mathbf{g}^T \mathbf{q}_a\right|}{||\mathbf{H}\mathbf{q}_a||} < 1 \tag{4.56}$$

because of (4.36) and the fact that $\mathbf{q}_a$ satisfies (4.33), i.e.,

$$1 < \lambda_1 = \frac{1 + P||\mathbf{H}\mathbf{q}_a||^2}{1 + P(\mathbf{g}^T \mathbf{q}_a)^2} \tag{4.57}$$

Hence, (4.56) means that $\alpha_0 \neq 0$ and furthermore, we have

$$\theta(\alpha_0) = \frac{\alpha_0^2}{1 - \mathbf{a}_0^T \mathbf{a}_0} > 0 \tag{4.58}$$

Therefore, we have

$$\frac{1}{\theta(\alpha^*)} \overset{(a)}{\geq} \frac{1}{\theta(\alpha_0)} > 0 \tag{4.59}$$

where (a) follows because α^* maximizes $\frac{1}{\theta(\alpha^*)}$. Finally, (4.59) implies $||\mathbf{a}^*|| < 1$ because of (4.50).

Next, we will show that the optimal $\mathbf{S}$ for $\max U(\mathbf{S}, \mathbf{a}^*)$ in (4.37) is unit-rank. Since the upper bound and achievable scheme differ only in replacing $\mathbf{A}(\mathbf{a}^*)$ with $\mathbf{H}^T\mathbf{H}$, as shown in (4.8) and (4.47), we will use Lemma 4.1 again to show the optimality of unit-rank $\mathbf{S}$ in (4.37). Since $\mathbf{H}^T\mathbf{H}$ is invertible and $\theta(\alpha^*) > 0$, matrix $\mathbf{A}(\mathbf{a}^*)$, in the form of (4.49), is invertible. In addition, in order to use Lemma 1, we need $\mathbf{g}^T\mathbf{A}(\mathbf{a}^*)^{-1}\mathbf{g} \geq 1$. In the following, we will show that $\mathbf{g}^T\mathbf{A}(\mathbf{a}^*)^{-1}\mathbf{g} = 1$. Using the matrix inversion lemma [43, page 19] on (4.49), we have

$$\mathbf{A}(\mathbf{a}^*)^{-1} = \left(\mathbf{H}^T\mathbf{H}\right)^{-1} - \frac{1}{\frac{1}{\theta(\alpha^*)} + \left(\mathbf{q}_a^{\perp}\right)^T \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{q}_a^{\perp}} \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{q}_a^{\perp} \left(\mathbf{q}_a^{\perp}\right)^T \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \tag{4.60}$$

Also, from (4.52) and (4.53), $1/\theta(\alpha^*)$ is equal to

$$\frac{1}{\theta(\alpha^*)} = -\left(\mathbf{q}_a^{\perp}\right)^T \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{q}_a^{\perp} + \frac{\left(\mathbf{g}^T \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{q}_a^{\perp}\right)^2}{\mathbf{g}^T \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{g} - 1} \tag{4.61}$$

$$= -\left(\mathbf{q}_a^{\perp}\right)^T \left(\left(\mathbf{H}^T\mathbf{H}\right)^{-1} - \frac{\left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{g}\mathbf{g}^T \left(\mathbf{H}^T\mathbf{H}\right)^{-1}}{\mathbf{g}^T \left(\mathbf{H}^T\mathbf{H}\right)^{-1} \mathbf{g} - 1} \right) \mathbf{q}_a^{\perp} \tag{4.62}$$

$$= -\left(\mathbf{q}_a^{\perp}\right)^T \left(\mathbf{H}^T\mathbf{H} - \mathbf{g}\mathbf{g}^T\right)^{-1} \mathbf{q}_a^{\perp} \tag{4.63}$$

Now, using straightforward algebra, starting from (4.60) and (4.61), it is easy to verify that

$$\mathbf{g}^T \mathbf{A}(\mathbf{a}^*)^{-1} \mathbf{g} = 1 \tag{4.64}$$

Thus, $\mathbf{D} = \mathbf{A}(\mathbf{a}^*)$ satisfies the conditions of Lemma 4.1, and therefore, $\arg\max U(\mathbf{S}, \mathbf{a}^*)$ is unit-rank.

Thus, for the selected $\mathbf{a}^*$, the optimization in the upper bound in (4.37) over $\mathbf{S} \succeq \mathbf{0}$ reduces to an optimization over $\mathbf{q}$, as $\mathbf{S} = P\mathbf{q}\mathbf{q}^T$,

$$\max_{\mathbf{S}\succeq\mathbf{0}, \text{trace}(\mathbf{S})\leq P} \quad U(\mathbf{S}, \mathbf{a}^*) = \max_{\mathbf{q}} \quad \frac{1}{2} \log \frac{\mathbf{q}^T \left(\mathbf{I} + P\mathbf{H}^T\mathbf{H} + P\theta(\alpha^*)\mathbf{q}_a^\perp \left(\mathbf{q}_a^\perp\right)^T \right) \mathbf{q}}{\mathbf{q}^T \left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T \right) \mathbf{q}} \tag{4.65}$$

where (4.65) is again in the Rayleigh quotient [43, page 176] form, and the solution to this optimization problem is the largest eigenvalue of the matrix

$$(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)^{-1/2} \left(\mathbf{I} + P\mathbf{H}^T\mathbf{H} + P\theta(\alpha^*)\mathbf{q}_a^\perp \left(\mathbf{q}_a^\perp\right)^T \right) (\mathbf{I} + P\mathbf{g}\mathbf{g}^T)^{-1/2} \tag{4.66}$$

which is the largest eigenvalue of the matrix

$$(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)^{-1} \left(\mathbf{I} + P\mathbf{H}^T\mathbf{H} + P\theta(\alpha^*)\mathbf{q}_a^\perp \left(\mathbf{q}_a^\perp\right)^T \right) \tag{4.67}$$

since the two matrices are related by a similarity transformation. Note that

$$(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)^{-1}\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\left(\mathbf{q}_a^{\perp}\right)^T\right)\mathbf{q}_a=(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)^{-1}\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}\right)\mathbf{q}_a \tag{4.68}$$

$$=\lambda_1\mathbf{q}_a \tag{4.69}$$

where (4.69) follows from (4.31).

Let us define vector $\mathbf{q}_1$ as

$$\mathbf{q}_1=-\theta(\alpha^*)\left(\mathbf{H}^T\mathbf{H}-\mathbf{g}\mathbf{g}^T\right)^{-1}\mathbf{q}_a^{\perp} \tag{4.70}$$

Note that

$$\mathbf{q}_1^T\mathbf{q}_a^{\perp}=-\theta(\alpha^*)\left(\mathbf{q}_a^{\perp}\right)^T\left(\mathbf{H}^T\mathbf{H}-\mathbf{g}\mathbf{g}^T\right)^{-1}\mathbf{q}_a^{\perp}=1 \tag{4.71}$$

where the last equality follows from (4.63). Also, (4.70) implies that

$$\mathbf{H}^T\mathbf{H}\mathbf{q}_1=\mathbf{g}\mathbf{g}^T\mathbf{q}_1-\theta(\alpha^*)\mathbf{q}_a^{\perp} \tag{4.72}$$

Then, we have

$$
\begin{aligned}
&(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)^{-1}\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\left(\mathbf{q}_a^{\perp}\right)^T\right)\mathbf{q}_1 \\
&\quad=(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)^{-1}\left(\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}\right)\mathbf{q}_1+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\right) && (4.73)\\
&\quad=(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)^{-1}\left(\mathbf{q}_1+P\mathbf{g}\mathbf{g}^T\mathbf{q}_1-P\theta(\alpha^*)\mathbf{q}_a^{\perp}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\right) && (4.74)\\
&\quad=(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)^{-1}(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)\mathbf{q}_1 && (4.75)\\
&\quad=\mathbf{q}_1 && (4.76)
\end{aligned}
$$

where (4.73) follows from (4.71), and (4.74) follows from (4.72). This means that the eigenvalues of the matrix in (4.67), and also the eigenvalues of the matrix in (4.66), are λ_1 and 1. Since $\lambda_1 > 1$, as shown in (4.36), the resulting maximum value in (4.65) is $\frac{1}{2}\log\lambda_1$. Hence, the upper bound on the secrecy capacity, i.e.,$\max_{\mathbf{S}\succeq\mathbf{0},\text{trace}(\mathbf{S})\leq P} U(\mathbf{S},\mathbf{a}^*)$, is $\frac{1}{2}\log\lambda_1$, which is equal to the lower bound on the secrecy capacity shown in (4.33).

4.4 Summary and Conclusions

We determined the secrecy capacity of the 2-2-1 Gaussian MIMO wire-tap channel, by solving for the optimum joint distribution for the auxiliary random variable and the channel input in the Csiszar-Korner formula. First, we proposed a lower bound on the secrecy capacity by evaluating the Csiszar-Korner formula for a specific selection of the auxiliary random variable and the channel input. Our achievable scheme is based on Gaussian signalling and no pre-processing of information. Even for this achievable scheme, which is completely characterized by the transmit covariance matrix $\mathbf{S}$, a

closed form solution for the secrecy rate does not exist. However, in our 2-2-1 case, we have shown that the optimal transmission scheme is unit-rank, i.e., beam-forming is optimal.

We showed the optimality of the proposed achievable scheme by constructing a tight upper bound that meets it. The upper bound is developed by considering the secrecy capacity of a channel where the eavesdropper's signal is given to the legitimate receiver. Even though this upper bound is well-defined for a general MIMO wire-tap channel, explicit evaluation and tightening of this upper bound has been possible by restricting ourselves to the 2-2-1 case. As in the lower-bound, and by selecting a certain correlation structure for the additive noises, we have shown that beam-forming is optimal for the upper bound as well. Furthermore, we have shown that the optimal beam-forming directions in the lower and upper bounds are the same. Finally, we have shown that the two bounds meet yielding the secrecy capacity.

The results of this chapter are published in [11] and [12].

4.5 Appendix

Proof of Theorem 4.1: A proof of similar results is presented for the case of m-1-n system, $m, n \geq 1$, in [9, Lemma 1, 2]. Our proof utilizes [9, Lemma 1], which generalizes to the case of multiple antennas at the legitimate receiver easily, and extends [9, Lemma 2] to the case where there are two antennas at the legitimate receiver.

An upper bound on the secrecy capacity of the wire-tap channel described in (4.1) and (4.2) is [9, Lemma 1]

$$\max_{p(\mathbf{x}):E[\mathbf{x}^T\mathbf{x}]\leq P} \quad I(\mathbf{x};\mathbf{y}|z) \tag{4.77}$$

Since we have

$$I(\mathbf{x};\mathbf{y}|z) = I(\mathbf{x};\mathbf{y},z) - I(\mathbf{x};z) \tag{4.78}$$

Intuitively, the upper bound is obtained by considering the secrecy capacity of a new channel where the legitimate receiver also has access to the eavesdropper's signal. Since the legitimate user is more capable in the new channel, the secrecy capacity of the new channel will serve as an upper bound on the secrecy capacity of the original channel. The new channel is degraded, and therefore the secrecy capacity formula is (4.78), obtained by setting $\mathbf{u} = \mathbf{x}$ as shown in [23].

In evaluating the right-hand side of (4.77), we introduce correlation between $\mathbf{n}_y$

and n_z, i.e., let us define $\mathbf{a}$ to be

$$\mathbf{a} = E[\mathbf{n}_y n_z] \tag{4.79}$$

We note that $\mathbf{a}$ thus defined has to satisfy $||\mathbf{a}|| \leq 1$. To avoid irregular cases, we will only consider $\mathbf{a}$ such that $||\mathbf{a}|| < 1$. We also note that $\mathbf{a}$ does not affect the secrecy capacity of the original channel, but it affects the upper bound in (4.77). Thus, (4.77) remains an upper bound for any $\mathbf{a}$ with $||\mathbf{a}|| < 1$.

We evaluate $I(\mathbf{x}; \mathbf{y}|z)$ as follows,

$$I(\mathbf{x}; \mathbf{y}|z) = h(\mathbf{y}|z) - h(\mathbf{y}|z, \mathbf{x}) \tag{4.80}$$

$$= h(\mathbf{y}|z) - h(\mathbf{n}_y|n_z) \tag{4.81}$$

Due to the Gaussianity of the noise,

$$h(\mathbf{n}_y|n_z) = h(\mathbf{n}_y, n_z) - h(n_z) = \frac{1}{2}\log(2\pi e)^2 |\mathbf{N}| \tag{4.82}$$

where $\mathbf{N}$ is defined as in (4.39). Let us define $\mathbf{S}$ as

$$\mathbf{S} = E[\mathbf{x}\mathbf{x}^T] \tag{4.83}$$

then

$$E[\mathbf{y}z] = E\left[(\mathbf{H}\mathbf{x} + \mathbf{n}_y)\left(\mathbf{x}^T\mathbf{g} + n_z\right)\right] = \mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a} \tag{4.84}$$

$$E[z^2] = 1 + \mathbf{g}^T\mathbf{S}\mathbf{g} \tag{4.85}$$

$$E[\mathbf{y}\mathbf{y}^T] = \mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T \tag{4.86}$$

The linear minimum mean squared error (LMMSE) estimator of $\mathbf{y}$ using z is

$$\hat{\mathbf{y}} = \frac{\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} z \tag{4.87}$$

and the resulting covariance matrix of the estimation error is

$$\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T - \frac{1}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} \left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)\left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)^T \tag{4.88}$$

Hence,

$$h(\mathbf{y}|z) = h\left(\mathbf{y} - \frac{\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} z \middle| z\right) \tag{4.89}$$

$$\leq h\left(\mathbf{y} - \frac{\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} z\right) \tag{4.90}$$

$$\leq \frac{1}{2}\log(2\pi e)^2 \left|\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T - \frac{1}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} \left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)\left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)^T\right| \tag{4.91}$$

Therefore,

$$I(\mathbf{x};\mathbf{y}|z) \leq \frac{1}{2}\log\frac{\left|\mathbf{I}+\mathbf{H}\mathbf{S}\mathbf{H}^T-\frac{1}{1+\mathbf{g}^T\mathbf{S}\mathbf{g}}\left(\mathbf{H}\mathbf{S}\mathbf{g}+\mathbf{a}\right)\left(\mathbf{H}\mathbf{S}\mathbf{g}+\mathbf{a}\right)^T\right|}{|\mathbf{N}|} \tag{4.92}$$

$$= \frac{1}{2}\log\frac{\left|\left(\mathbf{I}+\mathbf{H}\mathbf{S}\mathbf{H}^T\right)\left(1+\mathbf{g}^T\mathbf{S}\mathbf{g}\right)-\left(\mathbf{H}\mathbf{S}\mathbf{g}+\mathbf{a}\right)\left(\mathbf{H}\mathbf{S}\mathbf{g}+\mathbf{a}\right)^T\right|}{\left(1+\mathbf{g}^T\mathbf{S}\mathbf{g}\right)|\mathbf{N}|} \tag{4.93}$$

$$= \frac{1}{2}\log\frac{\left|\begin{bmatrix}\mathbf{I}+\mathbf{H}\mathbf{S}\mathbf{H}^T & \mathbf{H}\mathbf{S}\mathbf{g}+\mathbf{a}\\ \mathbf{g}^T\mathbf{S}\mathbf{H}^T+\mathbf{a}^T & 1+\mathbf{g}^T\mathbf{S}\mathbf{g}\end{bmatrix}\right|}{\left(1+\mathbf{g}^T\mathbf{S}\mathbf{g}\right)|\mathbf{N}|} \tag{4.94}$$

$$= \frac{1}{2}\log\frac{\left|\mathbf{N}+\bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{\left(1+\mathbf{g}^T\mathbf{S}\mathbf{g}\right)|\mathbf{N}|} \tag{4.95}$$

$$= \frac{1}{2}\log\frac{\left|\mathbf{I}+\mathbf{N}^{-1}\bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{\left(1+\mathbf{g}^T\mathbf{S}\mathbf{g}\right)} \tag{4.96}$$

where $\bar{\mathbf{H}}$ is defined as in (4.40). Thus, we have

$$\max_{p(\mathbf{x}):E[\mathbf{x}^T\mathbf{x}]\leq P} I(\mathbf{x};\mathbf{y}|z) \leq \max_{\mathbf{S}\succeq\mathbf{0},\text{trace}(\mathbf{S})\leq P} \frac{1}{2}\log\frac{\left|\mathbf{I}+\mathbf{N}^{-1}\bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{\left(1+\mathbf{g}^T\mathbf{S}\mathbf{g}\right)} \tag{4.97}$$

Therefore, an upper bound on the secrecy capacity of the wire-tap channel described in (4.1) and (4.2) is

$$\max_{\mathbf{S}\succeq\mathbf{0},\text{trace}(\mathbf{S})\leq P} U(\mathbf{S},\mathbf{a}) \tag{4.98}$$

for any $\mathbf{a}$ with $||\mathbf{a}|| < 1$, with $U(\mathbf{S},\mathbf{a})$ defined in (4.38).

Chapter 5

Conclusions

We studied two kinds of security attacks in Gaussian wireless channels: the jamming attack and the eavesdropping attack. For the jamming attack, we adopted a mutual information game formulation. First, we considered a non-fading multiple access channel with a correlated jammer, and characterized the saddle point solution of this mutual information game. We showed the game has a solution, whether the jammer knows the user signals or a noisy version of them. The optimal strategies are Gaussian signalling for the users and linear jamming for the jammer. Then, we studied the same problem in fading channels. When the jammer is correlated and both the users and the jammer have access to the channel state, we showed that a set of simultaneously optimal power allocation functions for the users and the jammer does not always exist, and consequently characterized the max-min user power allocation strategies and the corresponding jammer power allocation strategy. In all other cases, we showed that the mutual information game admits a saddle point solution, and characterized the corresponding user and jammer signalling and power allocation strategies. Our results for the jamming problem have been presented in [4] and [5], and submitted for journal publication in [6].

We then turned to the eavesdropping attack. First, we studied a Gaussian MISO wire-tap channel under various assumptions on the channel attenuations. When the channel attenuations are constants, known to all the parties, we found the maximum secrecy rate achievable through Gaussian signalling, and showed that the Gaussian signalling that achieves the best secrecy rate is of beam-forming nature. We then studied the Gaussian MISO channel when the eavesdropping channel experiences fading. We found achievable secrecy rates through Gaussian signalling. It is shown that, when the eavesdropping channel experiences fading, the optimal Gaussian signalling has a unit-rank covariance matrix, and therefore, the system reduces to a SISO channel. We identified conditions under which, positive secrecy rates are achievable. To generalize the results for a channel with multiple antennas at the receiver, we defined the Gaussian 2-2-1 wire-tap channel. We solved for the optimum joint distribution for the auxiliary random variable and the channel input in the Csiszar-Korner secrecy capacity formula. First, we obtained a lower bound on the secrecy capacity by evaluating the Csiszar-Korner formula for Gaussian signalling and no pre-processing of information. We showed that beam-forming is the optimal transmission strategy for achieving the highest lower bound of this form. We then developed a tight upper bound that meets this lower bound, by considering the secrecy capacity of a channel where the eavesdropper's signal is given to the legitimate receiver. Again we showed that beam-forming is optimal for the upper bound, and the optimal beam-forming directions in the lower and upper bounds are the same. This makes the two bounds meet and result in the secrecy capacity. Our results for the eavesdropping problem have been presented in [10] and [11], and submitted for journal publication in [12].

BIBLIOGRAPHY

[1] M. Médard, Capacity of correlated jamming channels. In *35th Annual Allerton Conference on Communications, Control and Computing*, Monticello, IL, September-October 1997.

[2] A. Kashyap, T. Basar and R. Srikant, Correlated jamming on MIMO Gaussian fading channels. *IEEE Trans. on Information Theory*, 50(9):2119–2123, September 2004.

[3] A. Bayesteh, M. Ansari and A. K. Khandani. Effect of jamming on the capacity of MIMO channels. In *42nd Annual Allerton Conference on Communications, Control and Computing*, Monticello, IL, September 2004.

[4] S. Shafiee and S. Ulukus. Correlated jamming in multiple access channels. In *Conference on Information Sciences and Systems*, Baltimore, MD, March 2005.

[5] S. Shafiee and S. Ulukus. Capacity of multiple access channels with correlated jamming. In *Military Communication Conference*, Atlantic City, NJ, October 2005.

[6] S. Shafiee and S. Ulukus. Mutual information games in multi-user channels with correlated jamming. *Submitted to IEEE Trans. on Information Theory.*

[7] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):2–10, October 1975.

[8] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar. On the Gaussian MIMO wiretap channel. In *IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[9] A. Khisti and G. Wornell. Secure transmission with multiple antennas: The MISOME wiretap channel. *Submitted to IEEE Trans. on Information Theory.*

[10] S. Shafiee and S. Ulukus. Achievable rates in Gaussian MISO channels with secrecy constraints. In *IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[11] S. Shafiee, N. Liu and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: the 2-2-1 channel. *Submitted to IEEE Trans. on Information Theory.*

[12] S. Shafiee, N. Liu and S. Ulukus. Secrecy capacity of the 2-2-1 Gaussian MIMO wire-tap channel. In *3rd International Symposium on Communications, Control and Signal Processing*, St. Julians, Malta, March 2008.

[13] T. M. Cover and J. A. Thomas. *Elements of information theory*, John Wiley & Sons, 1991.

[14] D. Fudenberg and J. Tirole. *Game theory*, MIT Press, 1991.

[15] E. Burger. *Introduction to the theory of games*, Prentice-Hall, 1963.

[16] D. P. Bertsekas. *Convex analysis and optimization*, Athena Scientific, 2003.

[17] H. V. Poor. *An introduction to signal detection and estimation*, 2nd Ed., Springer-Verlag, 1994.

[18] T. W. Anderson. The integral of a symmetric unimodal function over a symmetric convex set and some probability inequalities. In *Proceedings of American Mathematical Society*, 6(2):170–176, April 1955.

[19] A. Goldsmith and P. Varaiya. Capacity of fading channels with channel side information. *IEEE Trans. on Information Theory*, 43(6):1986–1992, November 1997.

[20] G. Caire and S. Shamai. On the capacity of some channels with channel state information. *IEEE Trans. on Information Theory*, 45(6):2007–2019, September 1999.

[21] R. Knopp and P. A. Humblet. Information capacity and power control in single-cell multiuser communications. In *IEEE International Conference on Communications*, Seattle, WA, June 1995.

[22] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. on Information Theory*, 24(4):451–456, July 1978.

[23] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. on Information Theory*, 24(3):339–348, May 1978.

[24] I. E. Telatar. Capacity of multi-antenna Gaussian channels. *European Trans. Telecommunications*, 10:585–595, November 1999.

[25] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, Toulouse, France, May 2006.

[26] P. Parada and R. Blahut. Secrecy capacity of SIMO and slow fading channels. In *IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[27] Z. Li, W. Trappe and R. Yates. Secret communication via multi-antenna transmission. In *41st Conference on Information Sciences and Systems*, Baltimore, Maryland, March 2007.

[28] J. Barros and M. R. D. Rodrigues. Secrecy capacity of wireless channels. In *IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.

[29] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. *Submitted to IEEE Trans. on Information Theory, Special Issue on Information Theoretic Security.*

[30] Z. Li, R. D. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2006.

[31] P. K. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *Submitted to IEEE Trans. on Information Theory*.

[32] Z. Li, R. D. Yates, and W. Trappe. Secure communication with a fading eavesdropper channel. In *IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[33] Y. Liang and H. V. Poor. Generalized multiple access channels with confidential messages. *Submitted to IEEE Trans. on Information Theory*.

[34] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.

[35] E. Tekin and A. Yener. Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy. In *44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2006.

[36] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *Submitted to IEEE Trans. on Information Theory*.

[37] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Multiple access channels with generalized feedback and confidential messages. In *IEEE Information Theory Workshop on Frontiers in Coding Theory*, Lake Tahoe, CA, September 2007.

[38] R. Liu and H. V. Poor. Multiple antenna secure broadcast over wireless networks. In *First International Workshop on Information Theory for Sensor Networks*, Santa Fe, NM, June 2007.

[39] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *Submitted to IEEE Trans. on Information Theory.*

[40] Y. Oohama. Relay channels with confidential messages. *Submitted to IEEE Trans. on Information Theory, Special Issue on Information Theoretic Security.*

[41] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *Submitted to IEEE Trans. on Information Theory, Special Issue on Information Theoretic Security.*

[42] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wiretap channels: Achievable rates and cooperative jamming. *Submitted to IEEE Trans. on Information Theory.*

[43] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, 1999.

[44] A. Khisti and G. Wornell. The MIMOME channel. In *45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, October 2007.

[45] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *Submitted to IEEE Trans. on Information Theory.*

[46] T. Liu and S. Shamai. A note on the secrecy capacity of the multi-antenna wiretap channel. *Submitted to IEEE Trans. on Information Theory.*

[47] H. Sato. An outer bound to the capacity region of broadcast channels. *IEEE Trans. on Information Theory*, 24(3):374–377, May 1978.