Technische Universität Dresden

Beamforming and Protection Strategies in Gaussian MISO Wiretap Systems with Partial Channel State Information

Sabrina Engelmann

von der Fakultät Elektrotechnik und Informationstechnik
der Technischen Universität Dresden

zur Erlangung des akademischen Grades

Doktoringenieur

(Dr.-Ing.)

genehmigte Dissertation

Vorsitzender:	Prof. Dr.-Ing. Dr. h.c. Frank H.P. Fitzek
Gutachter:	Prof. Dr.-Ing. Eduard A. Jorswieck
	Prof. Dr.-Ing. Aydin Sezgin
Tag der Einreichung:	02.02.2015
Tag der Verteidigung:	29.06.2015

Kurzfassung

In dieser Arbeit wird das Leistungsvermögen der Sicherheit auf der physikalischen Schicht anhand von zwei speziellen Systemmodellen untersucht. Im Detail werden Beamforming- und Absicherungsstrategien im gaußschen Multiple-Input Single-Output (MISO) Wiretap Channel (WTC) und dem gaußschen Two-hop Relay WTC mit mehreren Antennen am Sender und Empfänger studiert. In beiden Systemmodellen wird der Einfluss von partieller Kanalkenntnis zum Abhörer betrachtet und die so erreichbaren Sicherheitsraten mit denen verglichen, die bei voller Kanalkenntnis erreichbar sind.

Für den MISO WTC kann gezeigt werden, dass für Kanäle mit schnellem Schwund der Beamforming-Vektor in Hinblick auf die ergodische Sicherheitsrate unter Berücksichtigung des Grades der Kanalkenntnis optimiert werden kann. Zudem kann durch die intelligente Verwendung von künstlichem Rauschen (Artificial Noise, AN) die ergodische Sicherheitsrate signifikant erhöht werden. Hierbei nimmt der Grad der Kanalkenntnis direkt Einfluss auf die Aufteilung der Leistung zwischen Daten- und AN-Signal am Sender sowie auch auf die Richtung, in der das AN-Signal gesendet wird. Zudem kann gezeigt werden, dass dieselben Beamforming- und Absicherungsstrategien ebenfalls die Sicherheitsausfallwahrscheinlichkeit für Kanäle mit langsamem Schwund minimieren.

Im gaußschen Two-hop Relay WTC wird Information Leakage Neutralization (IN) als neuartige Absicherungsstrategie eingeführt. Diese Absicherungsstrategie erreicht nahezu dieselben instantanen Raten wie ein friedvolles System ohne Abhörer, wenn es bei voller Kanalkenntnis am Sender eingesetzt wird. Weiterhin sind durch die IN-Absicherungsstrategie höhere Raten erreichbar als durch den Einsatz von AN. Zusätzlich kann im Fall von voller Kanalkenntnis auf den Einsatz von Wiretap-Codes verzichtet werden. Auch im Fall partieller Kanalkenntnis, wo der Sender nur eine veraltete Schätzung des Kanals zwischen Relay und Abhörer besitzt, kann gezeigt werden, dass die IN-Absicherungsstrategie angewendet werden kann. Hierbei hängt es jedoch stark von den Kanalrealisierungen und dem Alter der Kanalschätzung ab, ob die IN- oder die AN-Absicherungsstrategie bessere Ergebnisse bringt und daher angewandt werden sollte.

Abstract

Within this thesis, we investigate the possibilities of physical layer secrecy for two special system models. In detail, we study beamforming and protection strategies in the Multiple-Input Single-Output (MISO) Gaussian Wiretap Channel (WTC) and the Gaussian two-hop relay WTC with multiple antennas at transmitter and receiver. In both system models, we examine the influence of partial Channel State Information (CSI) on the link to the eavesdropper and compare the achievable secrecy rates with the case of full CSI.

We show for the MISO WTC that in the fast fading scenario the Beamforming Vector (BV) can be optimized such that the ergodic secrecy rate is maximized with regard to the degree of channel knowledge. Further we show that the ergodic secrecy rate can be significantly increased by usage of Artificial Noise (AN), if applied in a smart way. This means that the degree of channel knowledge on the link to the eavesdropper influences the portion of power that is spent for AN at the transmitter as well as the direction, in which the AN signal is sent. In addition, we apply the same beamforming and protection strategies to the slow fading scenario and find that these techniques also reduce the secrecy outage probability.

For the two-hop relay WTC, we introduce Information Leakage Neutralization (IN) as a new protection strategy. If applied to a system model, where the transmitter has full CSI, the instantaneous secrecy rate performs almost as well as the instantaneous capacity of the peaceful system without an eavesdropper. The IN protected scheme outperforms the AN protected approach and performs much better than any beamforming scheme without additional protection mechanism. Another positive aspect of the IN protected scheme in the case of full CSI is that conventional channel codes can be applied instead of wiretap codes. For the case of partial CSI, where the transmitter has only an outdated estimate on the channel between relay and the eavesdropper, we show that the IN protected scheme can also be applied. Here, it strongly depends on the channel realizations and the delay of the estimate, whether the IN or the AN protection scheme should be applied.

Contents

Abbreviations

AF	Amplify-and-Forward
AN	Artificial Noise
BV	Beamforming Vector
CF	Compress-and-Forward
CSI	Channel State Information
DF	Decode-and-Forward
DMC	Discrete Memoryless Channel
DWTC	Degraded Wiretap Channel
IN	Information Leakage Neutralization
LBF	Linear Beamforming
LOS	Line-of-Sight
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MRC	Maximum Ratio Combining
MRT	Maximum Ratio Transmission
MSE	Mean Square Error
OFDM	Orthogonal Frequency-Division Multiplexing
OTP	One Time Pad
RDF	Resource Description Framework
SIMO	Single-Input Multiple-Output
SINR	Signal-to-Interference-plus-Noise Ratio
SISO	Single-Input Single-Output
SNR	Signal-to-Noise Ratio
WTC	Wiretap Channel
ZF	Zero Forcing

Symbols

$\mathbb{C}$	Set of complex numbers
$\mathbb{N}$	Set of natural numbers
$\mathbb{R}$	Set of real numbers
$\mathrm{H}(X)$	Entropy of the random variable X
$\mathrm{I}(X;Y)$	Mutual information between the random variables X and Y
$\mathrm{E}_X[\cdot]$	Expectation over the random variable X
$\Pr$	Probability
$\mathcal{N}$	Normal distribution
$\mathcal{CN}$	Complex normal distribution
R_S	Achievable secrecy rate
C_S	Secrecy capacity
$\mathcal{L}_\infty$	High-SNR power offset
$\mathcal{S}_\infty$	High-SNR slope
$[\cdot]^+$	Maximization function $\max\{\cdot, 0\}$
$\log_\mathrm{e}$	Natural logarithm
$\log_2$	Logarithm of basis 2
$\lim_{x\to c} f(x)$	Limit of $f(x)$ as x approaches c
$\underline{\lim}_{x\to c} f(x)$	Limit inferior of $f(x)$ as x approaches c
$\mathcal{X}$	A set or alphabet
$\mathrm{cl}(\mathcal{X})$	Closure of the set $\mathcal{X}$
$\sup(\mathcal{X})$	Supremum of set $\mathcal{X}$
$\lvert x\rvert$	Absolute value of the scalar x
$\boldsymbol{x}$	Column vector containing the elements $x_1, \ldots, x_n$
$^\mathrm{H}$ [x]	Hermitian transpose of $\boldsymbol{x}$
$\boldsymbol{X}$	Matrix
$\mathrm{trace}(\boldsymbol{X})$	Trace of the matrix $\boldsymbol{X}$
$\lVert\boldsymbol{X}\rVert$	Euclidean norm of the matrix $\boldsymbol{X}$
$\boldsymbol{\Pi}_X$	Projector onto the orthogonal complement of the column space of $\boldsymbol{X}$, i.e., $\boldsymbol{\Pi}_X = \boldsymbol{X}(\boldsymbol{X}^\mathrm{H}\boldsymbol{X})\boldsymbol{X}^\mathrm{H}$
$\boldsymbol{\Pi}_X^\perp$	Orthogonal projector onto the orthogonal complement of the column space of $\boldsymbol{X}$, i.e., $\boldsymbol{\Pi}_X^\perp = I - \boldsymbol{\Pi}_X$

Part I

Introduction

1 Motivation

In modern communication systems wireless technologies are more and more utilized. The advantage of the wireless medium, that mobile users are able to communicate from every point within the range of the base station, is accompanied by the disadvantage that this is also valid for any kind of eavesdropper.

During the last years, the interest in secrecy of communication is growing. The various scandals with regard to the intelligence services of different countries, mainly publicized by Edward Snowden[1], showed how easily communication can be wiretapped and overheard. As a result, many security related projects were further developed and revised for security problems. All of these projects are based on conventional cryptography, and some of them, e.g., OpenSSL[2], were found to have serious flaws in the implementation, in the case of OpenSSL the Heartbleed Bug[3], which allowed the eavesdropper to undermine the security of the provided tool.

Additionally, most cryptographic tools, which aim to increase the secrecy of private communication, require some understanding of the underlying mechanisms or at least some interaction between user and tool. First of all, the user needs to choose whether to take an asymmetric algorithm, also known as public key cryptography, or a symmetric algorithm. For the asymmetric algorithm, a key pair has to be generated initially consisting of a private key, which serves to decipher messages and needs to be kept secret, and a public key, which can be used by everyone in order to encipher messages. If we take GnuPG[4] as an example for such an asymmetric cryptographic algorithm, the user has to choose the encryption algorithm and the key length of the key pair, which requires some knowledge about up to date recommendations and

[1] A good overview on the revelations done by Edward Snowden can be found at http://en.wikipedia.org/wiki/Edward_Snowden.
[2] https://www.openssl.org
[3] http://heartbleed.com
[4] https://www.gnupg.org

security risks, in order to generate a good key pair, which guarantees secure communication for the next few years. Further, the user needs to publish the public key in an appropriate way.

For symmetric algorithms, only one key for encryption and decryption of a message is needed. Nevertheless, this key must be shared between transmitter and receiver in a secure way before a communication can be established. This also means, that every user, who wants to communicate with another user at any time in the future, already needs to share a secret key with him.

Further, up to now, there is only one information-theoretically secure encryption algorithm known. A cryptographic system is called information-theoretically secure if its security derives solely from the information theory. Further, an eavesdropper is not able to break the system with unlimited computational power.

This information-theoretically secure encryption algorithm is called One Time Pad (OTP) or Vernam Chiffre (see Chapter 2 for details). Unfortunately, due to the restriction that every key has to be used only once, this algorithm is not suitable for most applications in everyday life.

Therefore, we can summarize the following problems with regard to conventional cryptographic tools.

- The implementation of often complex cryptographic algorithm might be insecure.
- Setting up a cryptographic tool for secure communication might need some knowledge of the underlying mechanism by and the interaction with the user.
- In the case of symmetric cryptography, the key for communication needs to be shared beforehand.
- For everyday life suitable cryptographic algorithms do not provide information-theoretically secrecy.

During the last years, another approach to information-theoretically secrecy, which is located on the physical layer, is vividly discussed in literature. The basics for this novel approach were laid by Wyner in 1975 in his seminal paper [Wyn75]. This new method has the potential to overcome the before mentioned problems of conventional cryptography, as no key is needed and therefore no interaction between user and tool is necessary. Further, the realization of secrecy mechanisms on the physical

layer simplifies the implementation, which increases the security of the approach.

One scenario of modern communication, where such secrecy mechanisms can be helpful is the downlink transmission in mobile communication, where a base station with multiple-antennas transmits messages to mobile users, which have only single antenna each. If one of these messages is a private message, which is intended for only a single mobile user, all other mobile users within the range of the base station are eavesdroppers to this transmission link. This scenario is known as the Multiple-Input Single-Output (MISO) wiretap channel.

Within this thesis, we will analyze the possibilities of physical layer secrecy for two special MISO system models. The thesis is organized in three parts. In Part I, some basic results on physical layer secrecy are revised and presented. Further, all necessary tools and measures are introduced, that will be used for the analysis in the following parts. In Part II, we will investigate beamforming and protection strategies for the MISO Gaussian Wiretap Channel (WTC) with partial Channel State Information (CSI). The two-hop relay WTC with full and partial CSI is examined in Part III. Again, we study beamforming and protection strategies, where we introduce the novel approach of Information Leakage Neutralization (IN). All results are illustrated by numerical results.

2 Secrecy Rate and Secrecy Capacity

In 1949, Shannon establishes in his seminal paper [Sha49] information-theoretically secure communication. Within this paper, he proofed the information-theoretically secrecy of a symmetric cryptographic algorithm which is nowadays well known as One Time Pad (OTP), if used digitally, or Vernam Chiffre, for any other group greater than 2. This cryptographic algorithm was invented during the 1920s by Gilbert S. Vernam and Joseph O. Mauborgne.

(2.1) Definition (One Time Pad).
A message sequence m can be transmitted perfectly (information-theoretically) secure over an unsecure channel, if every bit i of the message m is encrypted by a function[1]

$$c[i] = m[i] + k[i] \mod 2 \quad \forall i \in [1, |m|]$$

and the key k satisfies the following conditions:

1. the key k needs to be at least as long as the message m, i.e., $|k| \geq |m|$,
2. the key k needs to be a random sequence, which is independent and identically distributed,
3. the key k is only used once to encrypt a message, and
4. the key k needs to be exchanged securely between transmitter and receiver beforehand. ✓

These conditions are combined in the following lemma.

(2.2) Corollary (Crypto Lemma[2]).
Let $(\mathcal{G}, +)$ be a compact abelian group with binary operation $+$, and let $C = M + K$, where M and K are random variables over $\mathcal{G}$ and K is

[1] The encryption function can be an arbitrary function that follows certain conditions. As the design of these functions is not in the focus of this thesis, this example shall be sufficient for illustration. Please refer to [Sha49] for details on the design of encryption functions.

[2] Lemma 2 in [For03].

independent of M and uniform over $\mathcal{G}$. Then C is independent of M and uniform over $\mathcal{G}$. ✓

The last condition of Definition (2.1) on the key k is quite unfortunate, as secure communication is only possible if transmitter and receiver have already shared key bits. The secrecy rate and secrecy capacity have the potential to overcome this disadvantage.

2.1 Degraded Wiretap Channel

As early as 1975, Wyner introduced in [Wyn75] the Wiretap Channel (WTC), where a transmitter, Alice, wants to send a confidential message to a receiver, Bob, in the presence of an eavesdropper, Eve. This system model was meant to work for a wired connection, where the eavesdropper is wiretapping the signal at the receiver, i.e., Eve only gets a degraded version of Bob's receive signal. This channel model is depicted in Figure 2.1 and was named in the literature the Degraded Wiretap Channel (DWTC).

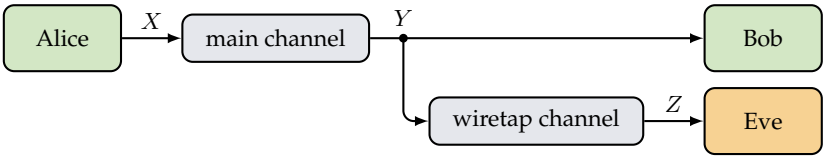


Figure 2.1: The degraded WTC.

Formally, a discrete memoryless DWTC $(\mathcal{X}, p_{Z|Y}p_{Y|X}, \mathcal{Y}, \mathcal{Z})$ consists of the finite input alphabet $\mathcal{X}$, the two finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ and the transition probabilities of two Discrete Memoryless Channels (DMC), i.e., $p_{Y|X}$ for the main and $p_{Z|Y}$ for the wiretap channel, such that

$$\forall n \geq 1 \quad \forall (x^n, y^n, z^n) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$$
$$p_{Y^n Z^n|X^n}(y^n, z^n|x^n) = \prod_{i=1}^{n} p_{Y|X}(y_i|x_i) p_{Z|Y}(z_i|y_i). \quad (2.1)$$

(2.3) Definition (Wiretap Code[3]).
A $(2^{nR_S}, n)$ code $\mathcal{C}_n$ of a DWTC $(\mathcal{X}, p_{Z|Y}p_{Y|X}, \mathcal{Y}, \mathcal{Z})$ consists of

- a message set $\mathcal{M} \in \{1, \ldots, 2^{nR}\}$,
- a source of local randomness at the encoder $(\mathcal{R}, p_R)$,
- an encoding function $f : \mathcal{M} \times \mathcal{R} \to \mathcal{X}^n$, which maps a message m and a realization of the local randomness r to a codeword x^n, and
- a decoding function $g : \mathcal{Y}^n \to \mathcal{M} \cup \{\mathrm{e}\}$, which maps each channel observation y^n to a message $\hat{m} \in \mathcal{M}$ or an error message e. ✓

The reliability of a code $\mathcal{C}_n$ is measured in terms of its average probability of error

$$\mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) \triangleq \Pr\left(\hat{M} \neq M | \mathcal{C}_n\right). \tag{2.2}$$

The secrecy of a code $\mathcal{C}_n$ is measured either in terms of the leakage of information to the eavesdropper

$$\mathbf{L}(\mathcal{C}_n) \triangleq \mathrm{I}(M; Z^n | \mathcal{C}_n) \tag{2.3}$$

or, equivalently, in terms of the equivocation, i.e., the uncertainty at the eavesdropper

$$\mathbf{E}(\mathcal{C}_n) \triangleq \mathrm{H}(M | Z^n \mathcal{C}_n). \tag{2.4}$$

(2.4) Definition (Weak Secrecy[4]).
A weak secrecy rate-equivocation pair (R_S, R_e) is achievable for the DWTC if there exists a sequence of $(2^{nR_S}, n)$ codes $\{\mathcal{C}_n\}_{n \geq 1}$ such that

$$\lim_{n\to\infty} \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) = 0 \qquad \text{(reliability condition)}, \tag{2.5}$$

$$\varliminf_{n\to\infty} \frac{1}{n}\mathbf{E}(\mathcal{C}_n) \geq R_e \quad \text{(weak secrecy condition)}. \tag{2.6}$$

The weak secrecy rate-equivocation region of a DWTC is

$$\mathcal{R}_S \triangleq \mathrm{cl}\left\{(R_S, R_e) : (R_S, R_e) \text{ is achievable}\right\}, \tag{2.7}$$

and the weak secrecy capacity of a DWTC is

$$C_S \triangleq \sup\left\{R_S : (R_S, R_S) \in \mathcal{R}_s\right\}. \tag{2.8}$$

✓

[3] Definition 3.1. in [BB11].
[4] Definition 3.2. in [BB11].

This definition of the secrecy rate-equivocation pair provides only weak secrecy, as the equivocation is considered as a rate, i.e., the eavesdropper gets no information in average, but maybe single bits.

A stronger notion of secrecy is given in the following definition.

(2.5) Definition (Strong Secrecy[5]).
A strong secrecy rate-equivocation pair (R_S, R_e) is achievable for the DWTC if there exists a sequence of $(2^{nR_S}, n)$ codes $\{\mathcal{C}_n\}_{n\geq 1}$ such that

$$\lim_{n\to\infty} \mathbf{P}_{\mathrm{e}}(\mathcal{C}_n) = 0 \qquad \text{(reliability condition)}, \tag{2.9}$$

$$\underline{\lim_{n\to\infty}} \left(\mathbf{E}(\mathcal{C}_n) - nR_e\right) \geq 0 \quad \text{(strong secrecy condition)}. \tag{2.10}$$

The strong secrecy rate-equivocation region of a DWTC is

$$\bar{\mathcal{R}}_S \triangleq \mathrm{cl}\left\{(R_S, R_e) : (R_S, R_e) \text{ is achievable}\right\}, \tag{2.11}$$

and the strong secrecy capacity of a DWTC is

$$\bar{C}_S \triangleq \sup\left\{R_S : (R_S, R_S) \in \mathcal{R}_s\right\}. \tag{2.12}$$

✓

For the discrete memoryless DWTC it was proved in [MW00] that the strong secrecy capacity equals the weak secrecy capacity. Throughout this thesis, all system models will be analyzed for weak secrecy according to Definition (2.4).

(2.6) Corollary (Secrecy Capacity of the Discrete Memoryless DWTC[6]).
The secrecy capacity for the discrete memoryless DWTC is given by

$$C_S = \max_{p_X} \mathrm{I}(X;Y|Z) = \max_{p_X} \left(\mathrm{I}(X;Y) - \mathrm{I}(X;Z)\right). \tag{2.13}$$

✓

Unfortunately, it is not an easy task to find the probability density function at the input that maximizes the difference of the two mutual information expressions. Although the mutual information is concave in p_X, this does not apply necessarily to the difference of two expressions.

[5] Defintion 3.3. in [BB11].
[6] The secrecy capacity was first established in Theorem 3 in [Wyn75].

Therefore, we apply a lower bound, which is easier to compute and therefore often used.

$$C_S = \max_{p_X} \left(\mathrm{I}(X;Y) - \mathrm{I}(X;Z) \right) \tag{2.14}$$

$$\geq \max_{p_X} \mathrm{I}(X;Y) - \max_{p_X} \mathrm{I}(X;Z) \tag{2.15}$$

$$= C_M - C_E \tag{2.16}$$

$$= R_S \tag{2.17}$$

The extension to the Gaussian case was done by Leung-Yan-Cheong and Hellman in [LH78]. We further extend this model to the complex Gaussian case. Here, the main channel h and the wiretap channel g are both complex Gaussian distributed channels with zero mean and variance 1 and independent of each other. Further, the additive white Gaussian noise terms are denoted by n_B and n_E and are distributed with zero mean and variance σ_B^2 and σ_E^2, respectively, and independent of each other. The transmitter Alice encodes the message m and sends the resulting codeword x in n channel uses with power constraint $\frac{1}{n}\sum_{i=1}^{n} |x_i|^2 = P$. The secrecy rate for this scenario is given by

$$R_S(P) = C_M - C_E \tag{2.18}$$

$$= \log_2 \left(1 + \mathrm{SNR}_B\right) - \log_2 \left(1 + \mathrm{SNR}_E\right) \tag{2.19}$$

$$= \log_2 \left(1 + \frac{|h|^2 P}{\sigma_B}\right) - \log_2 \left(1 + \frac{|g|^2 P}{\sigma_B + \sigma_E}\right). \tag{2.20}$$

Leung-Yan-Cheong and Hellman also proved that the achievable secrecy rate R_S, derived by the lower bound, is equal to the secrecy capacity C_S.

2.2 Non-Degraded Wiretap Channel

In the same year as Leung-Yan-Cheong and Hellman, Csiszár and Körner analyzed in [CK78] the broadcast channel with confidential messages. The transmitter wants to send a common message to both, Bob and Eve, and a confidential message only to Bob. A special case of this system model is the non-degraded WTC, where only the confidential message is sent.

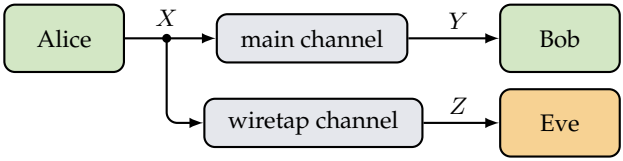


Figure 2.2: The non-degraded WTC.

In the broadcast channel, the main channel is not necessarily better than the wiretap channel. Therefore, the secrecy rate is not always positive and the secrecy capacity for the non-degraded WTC can be expressed as

$$C_S = \left[\max_{p_x} \left(\mathrm{I}(X;Y) - \mathrm{I}(X;Z) \right) \right]^+, \tag{2.21}$$

where $[\cdot]^+$ is the maximization function $\max(\cdot, 0)$. This system model corresponds much better to the wireless scenario than the DWTC.

Due to the maximization function, the transmitter only sends her message, if the main channel is advantageous. Otherwise, Alice will not transmit anything. This result, which is due to the fact that the Channel State Information (CSI) are fixed and therefore, the secrecy rate will not vary, is quite frustrating. This disadvantage can be overcome by additional degrees of freedom in the communication system, e.g., fading channel states and multiple antennas, as discussed in the following sections.

2.3 Fading Wiretap Channel

Wireless channels are in general subject to fading processes, i.e., the CSI values of the channels vary over the time. This means, that in the above channel model the channel coefficients h and g become random variables. These random variables change from time unit to time unit and are independent of each other and identically distributed.

In the literature, the fading behavior is often distinguished between slow and fast fading. There are different definitions for these terms available. Within this thesis, we will follow the definition of [TV08].

(2.7) Definition (Slow Fading).
The channel is a slow fading channel, if the coherence time is longer than the delay requirement of the application. ✓

This definition of a slow fading channel means that the channel states are random but remain constant for a sufficiently long time to transmit a whole codeword. The secrecy rate can be calculated for every time unit and is called instantaneous secrecy rate. A special case of slow fading is the quasi-static block-flat fading channel. Here, the channel states are constant over a complete block of transmission but vary independently from block to block.

(2.8) Definition (Fast Fading).
The channel is a fast fading channel, if the coherence time is much shorter than the delay requirement of the application. ✓

If the channel is in fast fading, a single codeword needs to be transmitted over several channel states. Therefore, the secrecy rate can only be calculated in average.

(2.9) Remark.
Both definitions do not only take the environment of the channel into account but also the application that the channel is used for. This is done by the delay requirement, which is different for every application, e.g., voice applications do typically have a short delay requirement of less than 100 ms and the tactile internet even less than 10 ms. ✓

As the channel states vary over time, there are always some realizations where the achievable secrecy rate is positive.

2.4 The Multiple-Input Single-Output Wiretap Channel

Multi-antenna systems have been an import research area for more than ten years. They offer high-data transmission and increased reliability for wireless communication [Gol+03].

In the area of information-theoretic secrecy, the increased number of degrees of freedom provided by the additional antennas are used to increase the secrecy by means of diversity. In [SU07] and [SLU09], the Gaussian Multiple-Input Single-Output (MISO) and Multiple-Input Multiple-Output (MIMO) WTC with a single antenna at the eavesdropper are

discussed and both provide the result that single-stream beamforming is optimal with regard to throughput. The fading MISO WTC, where the eavesdropper is also equipped with multiple antennas, is investigated in [KW10a]. In [KW10b], this analysis is extended to the MIMO case. Therein, the authors study two special cases: perfect channel knowledge and no channel knowledge of the channel to the eavesdropper.

Within this thesis, we focus in Part II on the non-degraded fading WTC with multiple antennas at the transmitter. In contrast to the previously introduced Single-Input Single-Output (SISO) WTC, the transmitter has n_T antennas in order to transmit her message. Therefore, the channels $\boldsymbol{h}$ and $\boldsymbol{g}$ to the legitimate receiver and the eavesdropper, respectively, are vector channels, where the single components might be spatially correlated. Due to the vector channel, Alice can now apply a Beamforming Vector (BV) $\boldsymbol{w}$ with a sum power constraint of $\|\boldsymbol{w}\|^2 = 1$ in order to optimize the power allocation per channel component and therewith also control the direction of the transmission.

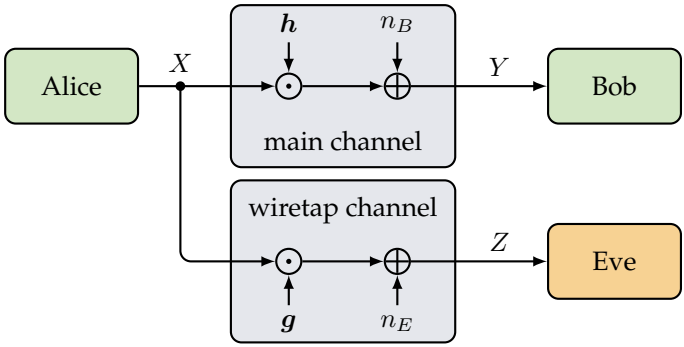


Figure 2.3: System model of the MISO non-degraded WTC with additive noise.

Let us assume quasi-static block-flat fading for the vector channels $\boldsymbol{h}$ between Alice and Bob and $\boldsymbol{g}$ between Alice and Eve. The channel model depicted in Figure 2.3 can be written as

$$y = \boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}x + n_B \quad \text{and} \quad z = \boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}x + n_E, \tag{2.22}$$

where $x \in \mathcal{X}$ is the complex channel input, $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$ are the complex channel outputs at Bob and Eve, respectively. The channel

vectors $\boldsymbol{h}$ and $\boldsymbol{g}$ are random zero-mean complex Gaussian distributed vectors with covariance matrix $\boldsymbol{I}$. The BV is given by $\boldsymbol{w}$, whose elements are complex values. The scalars n_B and n_E denote the white Gaussian noise at the receivers and are independent and identically distributed circular symmetric complex Gaussian random variables with zero-mean and variance σ^2. The inverse noise power $1/\sigma^2$ is denoted by ρ.

For such a MISO WTC, the instantaneous secrecy rate is computed in [SU07] and given by

$$R_S = \left[\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \log_2\left(1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2\right)\right]^+. \tag{2.23}$$

The optimal beamforming strategy to achieve the secrecy capacity of the MISO channel was derived by [SU07] and is given in the next Theorem.

(2.10) Theorem (Optimal Beamforming Strategy for the MISO WTC[7]). *The optimal Beamforming Vector $\boldsymbol{w}$ with transmit power constraint $\|\boldsymbol{w}\|^2 = 1$ is given by*

$$\boldsymbol{w} = \psi, \tag{2.24}$$

where ψ is the generalized eigenvector that belongs to the maximum generalized eigenvalue $\nu_{\max}$ of the matrix pencil

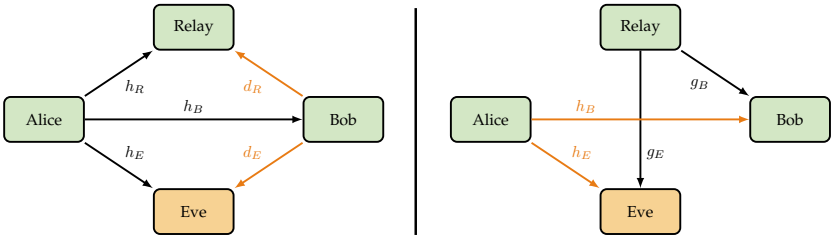
$$(\boldsymbol{I} + \rho\boldsymbol{h}\boldsymbol{h}^{\mathrm{H}}, \boldsymbol{I} + \rho\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}). \qquad \checkmark$$

This secrecy capacity is only achievable if Alice has full CSI on the channels $\boldsymbol{h}$ and $\boldsymbol{g}$ to Bob and Eve respectively. Such an assumption might be reasonable, when Eve is part of the communication system. We will discuss in Part II the case, where Alice has only partial CSI on the channel $\boldsymbol{g}$ to the eavesdropper.

2.5 The Relay Wiretap Channel

Another channel model, which is often discussed in literature, is the relay WTC.

[7] This result was derived in [SU07, Section III].



(a) Phase I (b) Phase II

Figure 2.4: System model of a SISO relay WTC.

Here, the transmitter Alice wants to send a confidential message to the intended receiver Bob with the aid of a trustworthy relay, which operates in half-duplex mode, i.e., it can either receive or transmit a message. Thus, the communication from Alice to Bob is done in two phases, as depicted in Figure 2.4. Unfortunately, the eavesdropper Eve is able to overhear not only the first phase, where Alice communicates her message to the relay and Bob, but also the second phase, where the relay forwards the message to Bob. Therefore, Eve gets information on the sent message from two communication phases.

Additionally, Alice and Bob have the possibility to protect the two communication phases by transmitting a protection signal x_n over the channels h_E and d_E, which are illustrated in orange in Figure 2.4. Such a protection signal may be Artificial Noise (AN) (see Section 4.1). Nevertheless, they need to take care not to disturb the legitimate receivers too much over the channels d_R and h_B.

For the calculation of the achievable secrecy rate, it is important in which forwarding mode the relay operates. Nowadays, the following modes are frequently discussed in literature [KMY06].

- Amplify-and-Forward (AF): This is the most simple mode. The receive signal is only amplified, before it is further transmitted to the intended receiver. Therefore, the noise term of the transmission from Alice to the relay is also amplified and forwarded. Additionally, the relay does not learn the original message, as no decoding is done.

- Decode-and-Forward (DF): The relay first decodes the signal, i.e., the noise is removed from the receive signal, and than forwards the signal to Bob. This mode has the advantage that Bob gets a less noisy receive signal at the end. Unfortunately, the same applies to Eve. Additionally, the relay also gets aware of the decoded message.
- Compress-and-Forward (CF): In this mode, the relay compresses the receive signal without decoding and sends the quantized version to the destination. The relay is, similar to the AF mode, ignorant of the message send by the transmitter.

One of the first papers on secrecy in relay WTCs is [LE08]. Here, the authors analyze the impact of DF and CF operation modes at the relay on the achievable secrecy rate in a SISO relay WTC. Additionally, the results are compared to the case where the relay only functions as a helper and sends AN. In [GTS11a] and [GTS11b], the relay operation modes AF and DF as well as the AN strategy are further analyzed with regard to the outage performance (see Section 3.2) and optimal power allocation in the Rayleigh slow fading case, if the channels to the eavesdropper are known only statistically.

The extension to the relay network with multiple relays and multiple eavesdroppers is done in [Don+10]. In this paper, the authors derive an optimal power allocation for maximizing the secrecy rate under a global power constraint in the SISO relay WTC with full CSI on all channels.

A slightly modified version of the relay WTC is the two-hop relay WTC, where no direct link h_B between transmitter and receiver is available. Therefore, the communication needs to go over the relay. Further, it is not possible anymore, that the relay functions as an external helper, which only sends AN signals in order to disturb the eavesdropper.

The maximization of the achievable secrecy rates in such a SISO two-hop relay WTC is investigated in [DYJ11]. In this paper, the relay is working in DF operation mode and the source and the relay are sending additionally AN signals, which are known a priori by the relay and the destination. Therefore, this transmission scheme equals a cryptographic encryption, as the AN signal is functioning as a key, which has to be exchanged securely before transmission. An optimal power allocation at source and relay is derived for the two cases of full CSI and partial CSI on the channels to Eve.

The achievable secrecy rates in the MIMO two-hop relay WTC, where every node has multiple antennas, are determined in [HS11]. The relay applies the DF operation mode. The authors proposed the idea, that Bob may send AN during the first phase in order to confuse Eve. Additionally, Alice splits her power to send the data signal and an AN signal. Further, the authors analyze the case of full CSI as well as the case of partial CSI on the channels to the eavesdropper.

In Part III, we investigate the two-hop relay WTC, based on the nondegraded MISO Gaussian WTC, which is introduced in Section 2.4. Alice and Bob have n_T and n_D antennas, respectively, while the relay and Eve have only single antenna each. Therefore, all channels, except g_E, are vector channels. Further, the relay operates in AF mode. We assume individual power constraints at the transmit nodes denoted by $p_{S,1} \leq P_{S,1}$ (first phase), $p_{S,2} \leq P_{S,2}$ (second phase) at the source Alice and $p_R \leq P_R$ at the relay (second phase). Bob is not transmitting in this channel model, i.e., the channels $\boldsymbol{d}_R$ and $\boldsymbol{d}_E$ in the first phase are nonexistent.

The channels are named according to Figure 2.4, where the direct link between Alice and Bob is not available. The vectors $\boldsymbol{w}_{S,1}$ and $\boldsymbol{w}_{S,2}$ are the BVs at Alice in the first and second communication phase, respectively. The receive beamforming vector at the intended receiver Bob in the second phase is given by $\boldsymbol{w}_B$. The received signals at the relay and the eavesdropper in the first phase are given by

$$\begin{aligned} y_R &= \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_R \quad \text{and} \\ y_{E,1} &= \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_{E,1}, \end{aligned}$$

respectively. Accordingly, the received signals in the second phase at the destination and the eavesdropper are given by

$$\begin{aligned} y_B &= \sqrt{\alpha} \boldsymbol{w}_B^{\mathrm{H}} \boldsymbol{g}_B (\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_R) + n_B \quad \text{and} \\ y_{E,2} &= \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,2} x_n + \sqrt{\alpha} g_E (\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_R) + n_{E,2}. \end{aligned}$$

The scalars n_B, n_R, $n_{E,1}$, and $n_{E,2}$ are additive white complex Gaussian noise with zero mean and variance σ^2 at the intended receiver Bob, the relay and the eavesdropper in the first and second phase, respectively. The scalar x_n is a signal sent by the source in order to protect the main signal x. The scaling factor α, which satisfies the power constraint at the

relay, is derived by

$$\alpha \leq \frac{|x_R|^2}{|y_R|^2},$$

where x_R is the forwarded signal at the relay.

An achievable secrecy rate R_S for the Gaussian two-hop relay WTC with multiple antennas at the transmitter and the receiver is then given by

$$\begin{aligned}
R_S &= \left[C(\Gamma_B) - C(\Gamma_E)\right]^+, \quad \text{where} \\
\Gamma_B &= \frac{\alpha\rho p_{S,1} \left|\boldsymbol{w}_B^{\mathrm{H}}\boldsymbol{g}_B\right|^2 \left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2}{\alpha \left|\boldsymbol{w}_B^{\mathrm{H}}\boldsymbol{g}_B\right|^2 + 1}, \\
\Gamma_E &= \rho p_{S,1} \left|\boldsymbol{h}_E^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2 + \frac{\alpha\rho p_{S,1} |g_E|^2 \left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2}{\rho p_{S,2} \left|\boldsymbol{h}_E^{\mathrm{H}}\boldsymbol{w}_{S,2}\right|^2 + \alpha |g_E|^2 + 1}, \quad \text{and} \\
\alpha &= \frac{\rho p_R}{\rho p_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2 + 1}.
\end{aligned}$$

$C(\mathrm{SINR})$ is the Gaussian rate expression given by $C(\mathrm{SINR}) = \log_2(1 + \mathrm{SINR})$. The inverse noise power is denoted by $\rho = 1/\sigma^2$.

In Part III, a novel protection mechanism for the above channel model is introduced, where for the case of full CSI the information leakage to the eavesdropper can be completely neutralized. Further, this Information Leakage Neutralization (IN) scheme is compared to AN and several beamforming schemes without further protection mechanisms. The case of partial CSI on the channel g_E from the relay to the eavesdropper is also analyzed.

3 Influence of Partial Channel State Information on Secrecy Rates

The assumption of perfect channel knowledge is widely used for the calculation of secrecy capacities and secrecy rates and might be reasonable if the eavesdropper Eve is part of the communication system. For example in [JM09], a MISO interference channel with confidential messages is studied under the assumption that the receivers are legitimated to receive the message sent to them but eavesdrop the message intended for the second receiver. However, if the eavesdropper is not a regular user of the communication system this assumption is unreasonable and the transmitter has therefore only partial channel knowledge, given by estimation or prediction, or even no Channel State Information (CSI) of the channel to the eavesdropper. In [MS11], the impact of imprecise channel estimates of both the channels to the intended receiver and the eavesdropper in the WTC is analyzed. In [LM11], the case of imperfect CSI on the channels to the intended receiver and the eavesdropper, where the uncertainty is modeled by a deterministic model, was investigated. In [Lin+11], the authors investigate the influence of AN on the secrecy rate of the WTC with quantized feedback on the main channel and no CSI on the eavesdropper's channel.

In the following, we present certain performance measures, which take the channel uncertainty on the wiretap channel into account. A short overview of this topic is also available in [LPS10]. The right choice of the performance measure depends mainly on the channel statistics (following the definition from [TV08]): The ergodic secrecy rate is the right measure for the fast fading scenario while the secrecy outage rate fits the slow fading scenario.

3.1 Ergodic Secrecy Rate

If the channel experiences fast fading (see Section 2.3), the secrecy of the communication is measured in terms of the ergodic secrecy rate as

described in [SU07, Section IV].

(3.1) Definition (Ergodic Secrecy Rate).
The ergodic secrecy rate is defined as

$$R_S = \left[\mathrm{E}_{\boldsymbol{h}} \left[\log_2 \left(1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) \right] - \mathrm{E}_{\boldsymbol{g}} \left[\log_2 \left(1 + \rho \left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) \right] \right]^+, \quad (3.1)$$

i.e., the expectation is taken over the achievable secrecy rate with respect to the random channels. The power is constrained via the BV $\boldsymbol{w}$ to $\|\boldsymbol{w}\|^2 = P$ and P being the available power at the transmitter. ✓

Please note that in Definition (3.1) the expectation in the first term is taken with respect to $\boldsymbol{h}$. As Alice knows $\boldsymbol{h}$ perfectly, the BV $\boldsymbol{w}$ can be chosen for each channel realization. The second term of Definition (3.1) is with respect to $\boldsymbol{g}$, which is only statistically known. The ergodic secrecy rate simplifies to

$$R_S = \left[\log_2 \left(1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) - \mathrm{E}_{\boldsymbol{g}} \left[\log_2 \left(1 + \rho \left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) \right] \right]^+. \quad (3.2)$$

During the last years, the ergodic secrecy rate was investigated for different channel models. The authors of [EU09] investigated the parallel broadcast channel, where both receivers try to eavesdrop each other. In [LPS08], the broadcast channel with public and confidential messages was analyzed. Here, only one receiver shall be able to decode the confidential message, but both receivers need to be able to decode the public message. For both models, the ergodic secrecy rate for the case of full CSI under fast fading was studied.

The assumption of full CSI on all channels was relaxed in [Lin+13]. In this work, the authors examine the fast fading MISO WTC with statistical CSI at the transmitter for the channel to the eavesdropper. An achievable ergodic secrecy rate is derived under usage of AN signals, which are not restricted to the null space of the intended receiver. In [LL14], the MIMO fast fading Rayleigh WTC with a multiple-antenna eavesdropper and statistical CSI to both Bob and Eve is under research. For the case of sum power constraint at the transmitter, the ergodic secrecy capacity was found. A more general approach to find the ergodic secrecy capacity in the SISO WTC was studied in [LJ14], where the authors characterize the relation between the ergodic secrecy capacity of fast fading wiretap channels and the stochastic orders.

3.2 Secrecy Outage Probability

In delay-critical applications, the issue of outage events is of big importance. In [PB05], the authors investigate the slow fading (see Section 2.3) Single-Input Multiple-Output (SIMO) WTC with full CSI and discuss the occurrence of outage events due to the fading nature of the channels. In [BR06], the secrecy outage probability was first defined for the SISO WTC under Rayleigh fading and an average power constraint, where only the main channel CSI is known. The authors showed that the fading nature of the wireless channel provides a positive secrecy rate in average, even if the eavesdropper has an advantage regarding the signal-to-noise ratio. In [Blo+08], the authors extended this model to the case where a disturbed version of the eavesdropper's CSI is available. In [LPS08], the optimal power allocation scheme for the SISO fading broadcast channel with full CSI has been investigated, when the transmitter has to fulfill rate requirements.

(3.2) Definition (Secrecy Outage Probability).
The secrecy outage probability is defined as

$$P_R(E) = \epsilon,$$

where E is an outage event. The secrecy outage probability describes the probability that a data packet cannot be transmitted securely to the intended receiver in the next block. ✓

For the secrecy outage event, there are different definitions used. The one more often used is defined in [BR06] and given as

$$E_1 = \{R_S < R_S^\epsilon\}\,. \tag{3.3}$$

Therein, R_S is the achievable secrecy rate of the system model, which is investigated, and R_S^ϵ is a given target secrecy rate, which can be achieved by usage of a secure code. The outage event E_1 contains two different types of outages. Due to the fading nature of the channels, we have an outage every time when the channel to Eve is better than the channel to Bob, i.e., the main channel has no advantage over the channel to the eavesdropper. For the case of full CSI, we know exactly when this event occurs and set the rate to zero to prevent security breaches. Therefore, we treat this kind of outage not as a secrecy outage. The second kind of outage occurs due to the estimation errors on the channel to Eve

when the CSI is only partially known. In this case, perfect secrecy is not always given and a security breach cannot be prevented with absolute certainty.

A definition of the secrecy outage event, that states these different outage events more explicitly is given in [Gun+13]. The transmitter wants to send data with target secrecy rate R_S^ϵ, which again can be achieved by usage of a secure code. Additionally, Alice transmits with a rate equal to the difference between the achievable secrecy rate R_S and the used target secrecy rate R_S^ϵ randomly generated key bits, which can be used to encrypt the data stream, when the achievable secrecy rate is lower than the target secrecy rate. The secrecy outage event is then given by

$$E_2 = \left\{ \log_2 \left(1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) < R_S^\epsilon \right\} \cup \left\{ \frac{1}{n} H(W|Z^{(N)}) < R_S^\epsilon - \epsilon_0 \right\}, \tag{3.4}$$

where the first part is the usual outage event, i.e., when the reliability condition in Equation (2.5) is not fulfilled, which also occurs in fading channels without secrecy constraints and the second part models the secrecy outage event that occurs when the secrecy constraint in Equation (2.6) is not fulfilled. In the case where the main channel to Bob is perfectly known to Alice, the first term gets zero by an appropriate choice of the BV $\boldsymbol{w}$.

In [YE11], the authors define the secrecy outage event [YE11, eq. (7)] as

$$E_3 = \left\{ \log_2 \left(1 + \rho \left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) > R_T - R_S^\epsilon \right\} \tag{3.5}$$

with fixed source transmission rate R_T and the main channel decoding error event [YE11, eq. 8] is defined as

$$E_4 = \left\{ \log_2 \left(1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) < R_T \right\}. \tag{3.6}$$

The difference between Equation (3.5) and Equation (3.3) is the assumption of channel knowledge on the channel $\boldsymbol{h}$ between Alice and Bob. If $\boldsymbol{h}$ is fully known at the transmitter, Alice chooses $R_T = \log_2(1 + \rho|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2)$ and from Equation (3.5) follows Equation (3.3). The difference between Equation (3.6) and Equation (3.4) is the definition of the main channel outage event. In Equation (3.6), the intended receiver decodes at

the source transmission rate R_T whereas in Equation (3.4) the receiver decodes at secrecy rate R_S^ϵ.

For the analysis in Part II, we use the secrecy outage event in Equation (3.3).

3.3 Robust Secrecy Rate

A third performance measure, which takes the channel uncertainty into account, is the robust secrecy rate, which is an achievable secrecy rate calculated over the worst case eavesdropper out of a set of possible eavesdropper channel states or positions. Often, this is done with the help of the compound wiretap channel, which is a generalization of the WTC, where every channel from the transmitter to the eavesdropper has a number of states. More details on the compound wiretap channel and the robust secrecy rate can be found in [LPS10] and references therein.

An achievable worst case secrecy rate in a MISO WTC with k possible states for the eavesdropper channel is given by

$$R_S = \max \min_k \left[\log_2 \left(1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) - \log_2 \left(1 + \rho \left| \boldsymbol{g}_k^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) \right]^+ .$$

The authors of [LM11] investigated the robust secrecy rate in the MISO WTC with multiple eavesdroppers, which are each equipped with multiple antennas. The transmitter has only partial channel knowledge to the intended receiver and the eavesdropper, which is modeled as spherical CSI uncertainty. In [WJ10a], the MIMO WTC, where all parties have multiple antennas, was studied. The CSI to Eve was unknown to the transmitter, but it was known, that the logical location of the eavesdropper is drawn from a certain set. The worst case secrecy rate was maximized for this scenario and upper and lower bounds on the worst case secrecy capacity under a sum power constraint at the transmitter derived.

4 Protection Mechanisms

The previously introduced secrecy rates can be further optimized. For this purpose, it is sometimes useful to apply an additional protection mechanism in order to transmit the confidential message securely to the intended receiver. Nowadays, the most used protection mechanism in literature is Artificial Noise (AN), which is described in Section 4.1. A novel approach in relay networks is given by Information Leakage Neutralization (IN), which is introduced in Section 4.2.

4.1 Artificial Noise

In [NG05], the authors first proposed the idea to utilize Artificial Noise (AN), some Gaussian random signal, in order to generate additional interference at the eavesdropper. In their paper, the authors split the power at the transmitter, who is equipped with multiple antennas, into one part to transmit the actual data stream and a second part for the AN signal. By transmitting the artificial noise in the null space, i.e., $\boldsymbol{h}^{\mathrm{H}}\boldsymbol{W} = 0$ in the channel model of Section 2.4, where $\boldsymbol{W}$ is the transmit covariance matrix of the AN signal, additional interference at the legitimate receiver Bob is avoided. Therefore, the transmission rate to Bob is unchanged while the eavesdropper's rate is decreased.

(4.1) Definition (Achievable Secrecy Rate with Artificial Noise).
An achievable secrecy rate R_S for the MISO WTC, where the transmitter splits the transmit power in order to send a data stream and an AN signal, is given by

$$R_S = \left[\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \log_2\left(1+\frac{\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left\|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}\right\|^2}\right)\right]^+,$$

where the AN signal is send in the null space of the intended receiver, i.e., $\boldsymbol{h}^{\mathrm{H}}\boldsymbol{W} = 0$. The transmit power at Alice is constraint to $\|\boldsymbol{w}\|^2 = \phi$ and $\mathrm{trace}\,(\boldsymbol{W}\boldsymbol{W}) = (1-\phi)$. ✓

The AN protection mechanism, sometimes also called friendly or cooperative jamming, has been applied to several system models. In [MS09], the authors extended the results of [NG05] to the MIMO multi receiver scenario, where they investigated the broadcast as well as the multicast channel with a single eavesdropper, whose CSI is unknown to the transmitter. For the data streams, SINR requirements have to be fulfilled, while the remainder of the transmit power is used to transmit AN signals in the null space of all receivers. The optimal power allocation strategy in a MISO system with multiple non-colluding eavesdroppers, which are jammed by AN, was investigated in [ZM09].

In [Tan+08], the authors analyzed the WTC with a helping interferer, who is only sending AN signals, while the transmitter can use the complete transmit power to send the confidential message to the receiver. Additionally, the authors propose the idea to use random Gaussian code words at the helper, so that the legitimate receiver can decode the interference, while the eavesdropper is not able to do so. The case, where the helper has multiple antennas was studied in [Don+09]. In [WJ10b], the optimality of Zero Forcing (ZF) in the MISO WTC with a helping interferer, which has multiple antennas, was analyzed. Further, AN was also applied to relay WTCs, as already mentioned in Section 2.5.

More detailed information on the function of AN can be found in [BB11, Chapter 8] and an overview of different system models with AN is provided in [HY10].

4.2 Information Leakage Neutralization

For the two-hop relay WTC as described in Section 2.5, another approach which aims on the protection of the data signal is possible. This approach is based on interference neutralization, which is a technique to cancel interference or a signal at a specific receiver, under the condition that the signal has to travel over a relay. This technique was applied to deterministic interference relay networks [Moh+08], two-hop relay channels [Ber+09], and to instantaneous relay networks [HJ12]. If applied to secrecy rate scenarios, this protection mechanism is called Information Leakage Neutralization (IN). This was done recently for the MISO Gaussian two-hop relay WTC with full CSI [Ger+12] as well as partial CSI [EHJ13] on the channel between the relay and the eavesdropper as well

as for instantaneous relay networks [HJE13; HJG13], where the other users of the system are the eavesdroppers.

If the transmitter has full channel state information of all channels in the system, Alice can construct a signal x_n, that fulfills

$$\begin{aligned} -\sqrt{\alpha} g_E \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1} x &= \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,2} x_n \\ \Rightarrow x_n &= -\frac{\sqrt{\alpha} g_E \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1}}{\boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,2}} x. \end{aligned}$$

By sending this signal x_n during the second transmission phase, the transmitter can neutralize the eavesdropped signal at Eve that she receives over the relay in the second phase.

In order to successfully neutralize the relayed signal during the second phase, an additional power constraint for the transmission of the IN signal has to be fulfilled.

(4.2) Definition (IN power constraint).
The power allocated for the IN signal has to fulfill

$$\mathrm{E}_x\left[|x_n|^2\right] = \frac{\alpha p_{S,1} |g_E|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1}\right|^2}{\left|\boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,2}\right|^2} \leq p_{S,2}$$

where $\alpha = \frac{\rho p_R}{\rho p_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1}\right|^2 + 1}$. ✓

(4.3) Remark.
If Alice applies ZF with respect to Eve during the first phase, the IN protection scheme implies that Eve gets no data signal at all. Therefore, Alice can perform conventional channel coding instead of the more complex secrecy binning that is normally used for wiretap systems. ✓

5 High-SNR Slope and High-SNR Power Offset

In order to compare different transmission and protection schemes in the high-Signal-to-Noise Ratio (SNR) regime, we use the concept of the high-SNR power offset introduced in [LTV05]. The achievable rate as a function of the SNR $\rho = 1/\sigma^2$ is denoted by $R(\rho)$.

(5.1) Definition (High-SNR slope).
The high-SNR slope is defined as

$$\mathcal{S}_\infty = \lim_{\rho\to\infty} \frac{R(\rho)}{\log_2(\rho)}$$

in bits/s/Hz/(3 dB). ✓

(5.2) Definition (High-SNR power offset).
The high-SNR power offset is given as

$$\mathcal{L}_\infty = \lim_{\rho\to\infty} \left(\log_2(\rho) - \frac{R(\rho)}{\mathcal{S}_\infty} \right)$$

in 3 dB units. ✓

In the high-SNR regime, the throughput behaves like

$$R(\rho) = \mathcal{S}_\infty \left(\frac{\rho[dB]}{3[dB]} - \mathcal{L}_\infty \right) + O(1).$$

For more detailed insights, see [LTV05, Section II].

The high-SNR power offset is useful in order to compare two systems with the same high-SNR slope $\mathcal{S}_\infty$ with regard to there shifted throughput curves at high-SNR.

Part II

Beamforming and Protection Strategies for Wiretap Channels

6 System Model

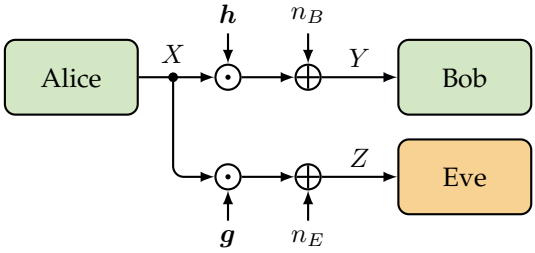


Figure 6.1: System model of the MISO non-degraded WTC with additive noise.

The system considered in this chapter is based on the MISO Gaussian WTC presented in Section 2.4. The transmitter, Alice, has n_T antennas, while the receiver, Bob, and the eavesdropper, Eve, have only single antenna each.

As before, denote the quasi-static block-flat fading vector channel between Alice and Bob as $\boldsymbol{h}$ and between Alice and Eve as $\boldsymbol{g}$. The signal model depicted in Figure 6.1 can be written as

$$y = \boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}x + n_B \quad \text{and} \quad z = \boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}x + n_E, \tag{6.1}$$

where $x \in \mathcal{X}$ is the complex channel input, $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$ are the complex channel outputs at Bob and Eve, respectively. The channel vectors $\boldsymbol{h}$ and $\boldsymbol{g}$ are zero-mean complex Gaussian distributed random vectors with covariance matrix $\boldsymbol{I}$. The BV is given by $\boldsymbol{w}$, whose elements are complex values. The scalars n_B and n_E denote the white Gaussian noise at the receivers and are independent and identically distributed circular symmetric complex Gaussian random variables with zero-mean and variance σ^2. The inverse noise power $1/\sigma^2$ is denoted by ρ.

Alice has full CSI to Bob, but only partial CSI to Eve. The CSI on $\boldsymbol{g}$ could for example be outdated, a sophisticated guess, or even completely

unknown to Alice. Therefore, an appropriate model for the channel vector $\boldsymbol{g}$ should take these cases into account.

(6.1) Definition.
The uncertainty at Alice on the channel $\boldsymbol{g}$ is modeled as

$$\boldsymbol{g} = \sqrt{\kappa}\,\boldsymbol{d} + \sqrt{1-\kappa}\,\tilde{\boldsymbol{g}}, \tag{6.2}$$

where $\boldsymbol{d}$ is the known deterministic component of the channel between Alice and Eve and $\tilde{\boldsymbol{g}}$ is a random zero-mean circular symmetric complex valued Gaussian vector with covariance matrix $\boldsymbol{I}$. The scalar κ in Equation (6.2) indicates the degree of knowledge Alice has about the channel $\boldsymbol{g}$ to Eve[1], i.e., for $\kappa = 1$, Alice has full CSI about the channel to Eve, while $\kappa = 0$ represents the case, where Alice has no CSI about the wiretap channel and $\boldsymbol{g} = \tilde{\boldsymbol{g}}$. ✓

(6.2) Remark.
For the case of full CSI, we have $\kappa = 1$. Therefore, the MISO wiretap channel in Equation (6.2) reduces to $\boldsymbol{g} = \boldsymbol{d}$ and the result on the optimal beamforming strategy presented in Theorem (2.10) applies.

This result is taken as an upper bound for all beamforming and protection strategies discussed in this part. ✓

For data transmission, the transmitter performs single-stream beamforming, where we define following BVs.

(6.3) Definition (Beamforming Directions).
The transmitter allocates her power such that the data stream is send in a certain direction [TV08]. These Beamforming Vectors (BVs) are given by

$$\boldsymbol{w}_{\text{MRT}} = \frac{\boldsymbol{h}}{\|\boldsymbol{h}\|}, \quad \boldsymbol{w}_{\text{ZF}} = \frac{\boldsymbol{\Pi}_{\boldsymbol{d}}^{\perp}\boldsymbol{h}}{\|\boldsymbol{\Pi}_{\boldsymbol{d}}^{\perp}\boldsymbol{h}\|}, \quad \boldsymbol{w}_{\text{ZF}}^{\perp} = \frac{\boldsymbol{\Pi}_{d}\boldsymbol{h}}{\|\boldsymbol{\Pi}_{d}\boldsymbol{h}\|},$$

$$\text{and} \quad \boldsymbol{w}_{\text{LBF}}(\tau) = \sqrt{\tau}\boldsymbol{w}_{\text{ZF}}^{\perp} + \sqrt{1-\tau}\boldsymbol{w}_{\text{ZF}}. \tag{6.3}$$

The vector $\boldsymbol{w}_{\text{MRT}}$ is the Maximum Ratio Transmission (MRT) BV in the direction of $\boldsymbol{h}$, the vector $\boldsymbol{w}_{\text{ZF}}$ is the ZF BV in the direction of the

[1] In channel modeling, this scenario corresponds to a fading channel with Line-of-Sight (LOS) component and $\kappa = {}^{K}/_{1+K}$ where K is the K-factor.

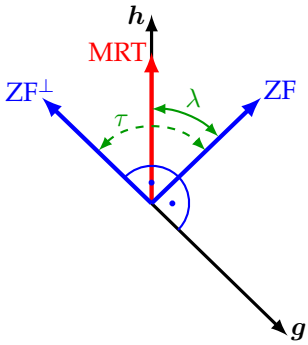


Figure 6.2: Graphical interpretation of BVs in 2D.

projection of $\boldsymbol{h}$ onto the null space of $\boldsymbol{d}$, and the vector $\boldsymbol{w}_{\text{ZF}}^{\perp}$ is the vector in the direction of the projection of $\boldsymbol{h}$ onto $\boldsymbol{d}$. The vector $\boldsymbol{w}_{\text{LBF}}(\tau)$ denotes the linear combination between the BVs $\boldsymbol{w}_{\text{ZF}}$ and $\boldsymbol{w}_{\text{ZF}}^{\perp}$, where $\tau \in [0, 1]$ has to be chosen appropriately. ✓

(6.4) Remark.
An alternative parameterization for the beamformer $\boldsymbol{w}_{\text{LBF}}(\tau)$ in Equation (6.3) is given by

$$\boldsymbol{w}_{\text{LBF}}(\lambda) = \frac{\lambda\, \boldsymbol{w}_{\text{MRT}} + (1-\lambda)\, \boldsymbol{w}_{\text{ZF}}}{\|\lambda\, \boldsymbol{w}_{\text{MRT}} + (1-\lambda)\, \boldsymbol{w}_{\text{ZF}}\|}. \tag{6.4}$$

The mapping from $\tau \in [0, 1]$ in Equation (6.3) to $\lambda \in [0, 1]$ in Equation (6.4) is derived in the proof of Corollary 2 in [JLD08] and is given by

$$\boldsymbol{w}_{\text{LBF}}(\tau) = \underbrace{\left(\sqrt{\tau \frac{\ell_1 + \ell_2}{\ell_1}}\right)}_{\frac{\lambda}{\|\lambda \boldsymbol{w}_{\text{MRT}} + (1-\lambda)\boldsymbol{w}_{\text{ZF}}\|}} \boldsymbol{w}_{\text{MRT}} + \underbrace{\left(\sqrt{1-\tau} - \sqrt{\tau \frac{\ell_2}{\ell_1}}\right)}_{\frac{1-\lambda}{\|\lambda \boldsymbol{w}_{\text{MRT}} + (1-\lambda)\boldsymbol{w}_{\text{ZF}}\|}} \boldsymbol{w}_{\text{ZF}}$$

with $\ell_1 = \|\boldsymbol{\Pi}_{\boldsymbol{d}} \boldsymbol{h}\|^2$ and $\ell_2 = \|\boldsymbol{\Pi}_{\boldsymbol{d}}^{\perp} \boldsymbol{h}\|^2$.

This parameterization has the advantage that the beamformer $\boldsymbol{w}_{\text{LBF}}(\lambda)$ can be found over a smaller set of BVs, i.e., $\boldsymbol{w}_{\text{LBF}}(\lambda)$ varies between $\boldsymbol{w}_{\text{ZF}}$

and $\boldsymbol{w}_{\text{MRT}}$, while $\boldsymbol{w}_{\text{LBF}}(\tau)$ goes from $\boldsymbol{w}_{\text{ZF}}$ to $\boldsymbol{w}_{\text{ZF}}^{\perp}$. The two sets of BVs are equivalent, if $\tau \in [0, \tau^{\text{MRT}}]$ with $\tau^{\text{MRT}} = \|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|^2/\|\boldsymbol{h}\|^2$. ✓

Figure 6.2 shows the BVs $\boldsymbol{w}_{\text{MRT}}$ (red vector), $\boldsymbol{w}_{\text{ZF}}$ and $\boldsymbol{w}_{\text{ZF}}^{\perp}$ (blue vectors) given in Definition (6.3) as well as the two parameterizations of $\boldsymbol{w}_{\text{LBF}}(\tau)$ and $\boldsymbol{w}_{\text{LBF}}(\lambda)$ for a two-dimensional vector space. It can be seen that the λ-parameterization (green solid angle) covers a smaller set of BVs than the τ-parameterization (green dashed angle), as mentioned before.

7 Beamforming with Partial Channel State Information

In this chapter, we characterize the optimal transmit strategy with partial CSI at Alice ($\boldsymbol{h}$ and $\boldsymbol{d}$ perfectly known at Alice) as specified in Definition (6.1). As performance measures, we use the ergodic secrecy rate, as introduced in Section 3.1, and the secrecy outage probability, described in Section 3.2.

We distinguish between optimal beamforming strategies, where Alice performs single-stream beamforming and transmits the intended signal with full transmit power, and protection mechanisms, where Alice splits her transmit power in order to protect the message additionally (see Chapter 4).

Within this chapter, we present results that were previously published on international conferences or in IEEE journals. The results on the ergodic secrecy rate presented in Sections 7.1.1 and 7.2.1 were published in [GWJ10]. Furthermore, the results on the optimal beamforming strategies for the performance measure of the secrecy outage probability provided in Section 7.1.2 were first presented in [GSJ11] and later complemented by the protection strategies given in Section 7.2.2 in [GSJ12].

7.1 Optimal Beamforming Strategies

First, let us analyze the optimal beamforming strategies if Alice only transmits her data without any kind of protection mechanism. As already described above, Alice performs single-stream beamforming in order to transmit her signal to the intended receiver Bob. As the wiretap channel is only partially known, the result from Section 2.4 cannot be applied.

7.1.1 Ergodic Secrecy Rate

In fast fading environments, the chosen performance measure is the ergodic secrecy rate (see Section 3.1).

(7.1) Definition (Ergodic Secrecy Rate).
The ergodic secrecy rate for the MISO wiretap channel with full CSI on the channel $\boldsymbol{h}$ to the intended receiver Bob and partial CSI on the channel $\boldsymbol{g}$ to the eavesdropper, as specified in Definition (6.1), is given by

$$R_S(\boldsymbol{w}) = \left[\mathrm{E}_h\left[\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right)\right] - \mathrm{E}_g\left[\log_2\left(1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2\right)\right]\right]^+.$$

Note that the expectation in the first term is with respect to $\boldsymbol{h}$. However, the BV $\boldsymbol{w}$ can be chosen for each realization of $\boldsymbol{h}$ since Alice knows the channel $\boldsymbol{h}$ perfectly. Therefore, the ergodic secrecy rate reduces to

$$R_S(\boldsymbol{w}) = \left[\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \mathrm{E}_g\left[\log_2\left(1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2\right)\right]\right]^+. \quad \checkmark$$

(7.2) Optimization Problem.
Alice transmits the intended signal with full transmit power. This corresponds to the programming problem

$$\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} R_S(\boldsymbol{w}). \qquad \checkmark$$

(7.3) Proposition.
Let $\tau \in [0,1]$. The optimal Beamforming Vector $\boldsymbol{w}$ solving the Optimization Problem (7.2) is given by $\boldsymbol{w}_{\mathrm{LBF}}(\tau)$ in Equation (6.3).

The resulting secrecy rate is given by

$$R_S(\tau) = \left[\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2\right) - \mathrm{E}_{\boldsymbol{g}}\left[\log_2\left(1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2\right)\right]\right]^2. \tag{7.1}$$

$\checkmark$

Therefore, the Optimization Problem (7.2) reduces to an optimization problem over the real valued parameter τ.

Proof.
In the proof, we show that $\boldsymbol{w}_{\mathrm{LBF}}(\tau)$ in Equation (6.3) achieves the maximum of the Optimization Problem (7.2) for certain $\tau \in [0, 1]$.

We treat the ergodic secrecy rate R_S in Definition (7.1) as a function of the BV. We regard a BV

$$\tilde{\boldsymbol{v}}(\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_{n_T}) = \gamma_1 \boldsymbol{w}_{\mathrm{ZF}}^{\perp} + \gamma_2 \boldsymbol{w}_{\mathrm{ZF}} + \sum_{l=3}^{n_T} \gamma_l \boldsymbol{u}_l \tag{7.2}$$

with $\|\tilde{\boldsymbol{v}}\|^2 = 1$ and an orthonormal basis $\{\boldsymbol{u}_3, \ldots, \boldsymbol{u}_{n_T}\}$ that spans the orthogonal complement of span$\{\boldsymbol{w}_{\mathrm{ZF}}^{\perp}, \boldsymbol{w}_{\mathrm{ZF}}\}$ in $\mathbb{C}^{n_T}$. Furthermore, all $\boldsymbol{\gamma} = [\gamma_1, \ldots, \gamma_{n_T}]$ in Equation (7.2) are complex and $\sum_{l=1}^{n_T} |\gamma_l|^2 = 1$.

The power allocated to other directions than $\boldsymbol{w}_{\mathrm{ZF}}^{\perp}$ and $\boldsymbol{w}_{\mathrm{ZF}}$ has no impact on $|\boldsymbol{h}^{\mathrm{H}} \tilde{\boldsymbol{v}}|^2$, i.e., cannot improve the channel capacity from Alice to Bob, as the receiver Bob is on the plane span$\{\boldsymbol{w}_{\mathrm{ZF}}^{\perp}, \boldsymbol{w}_{\mathrm{ZF}}\}$ and all other directions are orthogonal to this plane, as described above. Moreover, allocating power to $\gamma_3, \ldots, \gamma_{n_T}$ in Equation (7.2) increases $|\boldsymbol{g}^{\mathrm{H}} \tilde{\boldsymbol{v}}|^2$, and hence decreases the secrecy rate, compared to the case where $\gamma_i = 0$ for all $i = 3, \ldots, n_T$, except for the case when the eavesdropper is also on the plane span$\{\boldsymbol{w}_{\mathrm{ZF}}^{\perp}, \boldsymbol{w}_{\mathrm{ZF}}\}$, where the value remains unchanged. Consequently, the BV $\boldsymbol{v}(\gamma_1, \gamma_2, 0, \ldots, 0)$ with $\|\boldsymbol{v}\|^2 \leq \|\tilde{\boldsymbol{v}}\|^2$ achieves a higher or equal secrecy rate than the BV $\tilde{\boldsymbol{v}}$, i.e.,

$$R_S(\tilde{\boldsymbol{v}}) \leq R_S(\boldsymbol{v}).$$

According to Lemma (A.1) in Appendix A, the secrecy rate R_S increases with increasing power allocated to the BV. Therefore, the following relation holds

$$R_S(\boldsymbol{v}) \leq R_S(\boldsymbol{w})$$

for a normalized BV $\boldsymbol{w} = \frac{1}{\|\boldsymbol{v}\|}\boldsymbol{v}$ with $\|\boldsymbol{w}\|^2 = 1 \geq \|\boldsymbol{v}\|^2$.

Thus, the maximization of the Optimization Problem (7.2) can only be achieved by a BV of norm one that allocates power in the directions of

$\boldsymbol{w}_{\text{ZF}}^{\perp}$ and $\boldsymbol{w}_{\text{ZF}}$, i.e.,

$$\begin{aligned}\boldsymbol{w}(\sqrt{\tau}e^{i\varphi_1}, \sqrt{1-\tau}e^{i\varphi_2}, 0, \dots, 0) \\ = e^{i\varphi_1}\left(\sqrt{\tau}\,\boldsymbol{w}_{\text{ZF}}^{\perp} + \sqrt{1-\tau}\,e^{i(\varphi_2-\varphi_1)}\boldsymbol{w}_{\text{ZF}}\right),\end{aligned} \tag{7.3}$$

where the complex valued coefficients are written in their polar form with $\tau, \varphi_1, \varphi_2 \in \mathbb{R}_{0+}$. Therewith, we found a parameterization for the BV $\boldsymbol{w}$ similar to the one used in Equation (6.3), but with parameters that are still complex valued. In the following, we show that it is sufficient to use real valued parameters.

We observe that $e^{i\varphi_1}$ in Equation (7.3) has no impact on $|\boldsymbol{h}^{\text{H}}\boldsymbol{w}|^2$ and $|\boldsymbol{g}^{\text{H}}\boldsymbol{w}|^2$ in Optimization Problem (7.2). Consequently, we choose $\varphi_1 = 0$. Further, $\varphi_2 = 0$ maximizes $|\boldsymbol{h}^{\text{H}}\boldsymbol{w}|^2$ while keeping the distribution of $|\boldsymbol{g}^{\text{H}}\boldsymbol{w}|^2$ unchanged. Therefore, we set $\varphi_2 = 0$ and obtain the parameterization in Equation (6.3). □

From Proposition (7.3), it can be seen that τ depends only on the SNR ρ and the degree of channel knowledge on $\boldsymbol{g}$, given by κ. Knowing this, we can make three observations, which are given in the following corollaries.

(7.4) Corollary (Beamforming without CSI).

For $\kappa = 0$, the optimal τ that maximizes the ergodic secrecy rate $R_S(\tau)$ in Equation (7.1) is given by $\tau = \tau^{\text{MRT}} = {\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|}/{\|\boldsymbol{h}\|}$, i.e., MRT is optimal.✓

Proof.
For the proof, we use the parameterization $\boldsymbol{w}_{\text{LBF}}(\lambda)$, where the transformation from $\boldsymbol{w}_{\text{LBF}}(\tau)$ to $\boldsymbol{w}_{\text{LBF}}(\lambda)$ is done according to Remark (6.4). It holds

$$\begin{aligned}\left|\boldsymbol{h}^{\text{H}}\boldsymbol{w}(\lambda)\right|^2 &= \left|\frac{\lambda\boldsymbol{h}^{\text{H}}\boldsymbol{w}_{\text{MRT}} + (1-\lambda)\boldsymbol{h}^{\text{H}}\boldsymbol{w}_{\text{ZF}}}{\|\lambda\boldsymbol{w}_{\text{MRT}} + (1-\lambda)\boldsymbol{w}_{\text{ZF}}\|}\right|^2 \\ &= \left|\frac{\lambda\boldsymbol{h}^{\text{H}}\boldsymbol{w}_{\text{MRT}}}{\|\lambda\boldsymbol{w}_{\text{MRT}}\|}\right|^2 \\ &\leq \left|\boldsymbol{h}^{\text{H}}\boldsymbol{w}_{\text{MRT}}\right|^2 \\ &= \left|\boldsymbol{h}^{\text{H}}\boldsymbol{w}(1)\right|^2\end{aligned}$$

for all $\lambda \in [0,1]$. Furthermore, $|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}(\lambda)|^2$ is independent of $\boldsymbol{w}$ (and thus of λ) for $\kappa = 0$.

For the parameterization $\boldsymbol{w}_{\mathrm{LBF}}(\tau)$, this result corresponds to

$$\tau^* = \tau^{\mathrm{MRT}} = \frac{\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|^2}{\|\boldsymbol{h}\|^2},$$

which yields the MRT BV

$$\boldsymbol{w}(\tau^{\mathrm{MRT}}) = \frac{\boldsymbol{h}}{\|\boldsymbol{h}\|} = \boldsymbol{w}_{\mathrm{MRT}}.$$ □

(7.5) Corollary (Beamforming with full CSI).

For $\kappa = 1$, the optimal τ that maximizes the ergodic secrecy rate $R_S(\tau)$ in Equation (7.1) is given by $\tau = \tau_{max}$ where

$$\boldsymbol{w}(\tau_{max}) = \psi$$

with ψ given in Equation (2.24). ✓

Proof.
For $\kappa = 1$ holds $\boldsymbol{g} = \boldsymbol{d}$ and the Optimization Problem (7.2) reduces to

$$\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} \log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \log_2\left(1+\rho\left|\boldsymbol{d}^{\mathrm{H}}\boldsymbol{w}\right|^2\right)$$
$$= \max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} \log_2\left(\frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left|\boldsymbol{d}^{\mathrm{H}}\boldsymbol{w}\right|^2}\right)$$

which has the same solution as

$$\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} \frac{\boldsymbol{w}^{\mathrm{H}}\left(I+\rho\boldsymbol{h}\boldsymbol{h}^{\mathrm{H}}\right)\boldsymbol{w}}{\boldsymbol{w}^{\mathrm{H}}\left(I+\rho\boldsymbol{d}\boldsymbol{d}^{\mathrm{H}}\right)\boldsymbol{w}}$$

in Theorem (2.10). □

(7.6) Corollary (Beamforming for high SNR with full CSI).

For high SNR, i.e., $\rho \to \infty$, and $\kappa = 1$, the optimal τ, that maximizes the ergodic secrecy rate $R_S(\tau)$ in Equation (7.1), converges to zero, i.e., zero forcing is used for transmission. ✓

Proof.
For the proof, we use the high-SNR slope as defined in Chapter 5. We optimize

$$\begin{aligned}&\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} \mathcal{S}_\infty(\boldsymbol{w}) \\ &= \max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} \lim_{\rho\to\infty} \frac{\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \log_2\left(1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2\right)}{\log_2(\rho)}. \end{aligned} \tag{7.4}$$

Note that in Equation (7.4) the high-SNR slope $\mathcal{S}_\infty(\boldsymbol{w})$ is one if and only if $|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2 = 0$ and zero otherwise. Therefore, for high SNR, we have to choose $\tau = 0$. □

7.1.2 Secrecy Outage Probability

For slow fading scenarios, the chosen measure is the secrecy outage probability as presented in Section 3.2.

(7.7) Optimization Problem.
We optimize the transmit strategy such that the target secrecy rate R_S^ϵ for a given secrecy outage probability ϵ is maximized. This corresponds to the programming problem

$$\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=1} R_S^\epsilon \quad \text{s.t.} \quad \Pr\left(\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2} < R_S^\epsilon\right) = \epsilon. \tag{7.5}$$

According to Theorem (B.1) in Appendix B.1, there exists an equivalent minimization problem for a fixed target secrecy rate R_S^ϵ, which is given by

$$\min_{\|\boldsymbol{w}\|^2=1} \epsilon \quad \text{s.t.} \quad \epsilon = \Pr\left(\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2} < R_S^\epsilon\right). \tag{7.6}$$

Here, the purpose is to minimize the secrecy outage probability ϵ for a given target secrecy rate R_S^ϵ over all unit norm BVs $\boldsymbol{w}$. Our further investigations will concentrate on this problem. ✓

(7.8) Proposition.
Let $\tau \in [0,1]$. Then the optimal Beamforming Vector $\boldsymbol{w}$ solving the Optimization Problem (7.7) is given by $\boldsymbol{w}_{\text{LBF}}(\tau)$ in Equation (6.3).

The secrecy outage probability ϵ can be expressed as

$$\epsilon = Q_1\left(\sqrt{\frac{2\kappa\tau}{1-\kappa}}\|\boldsymbol{d}\|, \sqrt{\frac{2 - 2^{R_S^\epsilon+1} + 2\rho\left|\boldsymbol{h}^{\text{H}}\boldsymbol{w}_{\text{LBF}}(\tau)\right|^2}{2^{R_S^\epsilon}\rho(1-\kappa)}}\right), \tag{7.7}$$

where Q_1 denotes the Marcum Q-function of the first order. ✓

Therefore, the Optimization Problem (7.7) reduces to an optimization problem over the real valued parameter τ.

Proof.
The proof consists of two steps. At first, we show that Equation (6.3) achieves the maximum of the Optimization Problem (7.7) for certain $\tau \in [0,1]$. This part of the proof follows the same lines as the proof of Proposition (7.3). Afterwards, we derive the expression for the secrecy outage probability ϵ in Equation (7.7).

First step First, we treat the secrecy rate R_S in Equation (2.23) as a function of the BV for arbitrary but fixed $\boldsymbol{g}$. We regard a BV

$$\tilde{\boldsymbol{v}}(\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_{n_T}) = \gamma_1 \boldsymbol{w}_{\text{ZF}}^{\perp} + \gamma_2 \boldsymbol{w}_{\text{ZF}} + \sum_{l=3}^{n_T} \gamma_l \boldsymbol{u}_l \tag{7.8}$$

with $\|\tilde{\boldsymbol{v}}\|^2 = 1$ and an orthonormal basis $\{\boldsymbol{u}_3, \ldots, \boldsymbol{u}_{n_T}\}$ that spans the orthogonal complement of $\text{span}\{\boldsymbol{w}_{\text{ZF}}^{\perp}, \boldsymbol{w}_{\text{ZF}}\}$ in $\mathbb{C}^{n_T}$. Furthermore, all $\boldsymbol{\gamma} = [\gamma_1, \ldots, \gamma_{n_T}]$ in Equation (7.8) are complex and $\sum_{l=1}^{n_T} |\gamma_l|^2 = 1$.

The power allocated to other directions than $\boldsymbol{w}_{\text{ZF}}^{\perp}$ and $\boldsymbol{w}_{\text{ZF}}$ has no impact on $|\boldsymbol{h}^{\text{H}}\tilde{\boldsymbol{v}}|^2$, i.e., cannot improve the channel capacity from Alice to Bob, as the receiver Bob is on the plane $\text{span}\{\boldsymbol{w}_{\text{ZF}}^{\perp}, \boldsymbol{w}_{\text{ZF}}\}$ and all other directions are orthogonal to this plane, as described above. Moreover, allocating power to $\gamma_3, \ldots, \gamma_{n_T}$ in Equation (7.8) increases $|\boldsymbol{g}^{\text{H}}\tilde{\boldsymbol{v}}|^2$, and hence decreases the secrecy rate, compared to the case where $\gamma_i = 0$ for all $i = 3, \ldots, n_T$, except for the case when the eavesdropper is also on

the plane span$\{\boldsymbol{w}_{\text{ZF}}^{\perp}, \boldsymbol{w}_{\text{ZF}}\}$, where the value remains unchanged. Consequently, the BV $\boldsymbol{v}(\gamma_1, \gamma_2, 0, \ldots, 0)$ with $\|\boldsymbol{v}\|^2 \leq \|\tilde{\boldsymbol{v}}\|^2$ achieves a higher or equal secrecy rate than the BV $\tilde{\boldsymbol{v}}$, i.e.,

$$R_S(\tilde{\boldsymbol{v}}) \leq R_S(\boldsymbol{v}). \tag{7.9}$$

According to Lemma (B.2) in Appendix B.2, the secrecy rate R_S increases with increasing power allocated to the BV. Therefore, the following relation holds

$$R_S(\boldsymbol{v}) \leq R_S(\boldsymbol{w}) \tag{7.10}$$

for a normalized BV $\boldsymbol{w} = \boldsymbol{v}/\|\boldsymbol{v}\|$ with $\|\boldsymbol{w}\|^2 = 1 \geq \|\boldsymbol{v}\|^2$. The relations in Equations (7.9) and (7.10) hold true for every realization of the random variable $\boldsymbol{g}$. Combining Equations (7.9) and (7.10) and evaluating the distribution function of the continuous random variables $R_S(\tilde{\boldsymbol{v}})$, $R_S(\boldsymbol{v})$, and $R_S(\boldsymbol{w})$ at R_S^{ϵ} yields the following relations for the corresponding secrecy outage probabilities

$$\Pr\left(R_S(\tilde{\boldsymbol{v}}) < R_S^{\epsilon}\right) \geq \Pr\left(R_S(\boldsymbol{v}) < R_S^{\epsilon}\right) \geq \Pr\left(R_S(\boldsymbol{w}) < R_S^{\epsilon}\right).$$

Thus, the minimization in Equation (7.6) of Optimization Problem (7.7) can only be achieved by a BV of norm one that allocates power in the directions of $\boldsymbol{w}_{\text{ZF}}^{\perp}$ and $\boldsymbol{w}_{\text{ZF}}$, i.e.,

$$\begin{aligned} &\boldsymbol{w}(\sqrt{\tau}e^{i\varphi_1}, \sqrt{1-\tau}e^{i\varphi_2}, 0, \ldots, 0) \\ &\quad = e^{i\varphi_1}\left(\sqrt{\tau}\,\boldsymbol{w}_{\text{ZF}}^{\perp} + \sqrt{1-\tau}\,e^{i(\varphi_2-\varphi_1)}\boldsymbol{w}_{\text{ZF}}\right), \end{aligned} \tag{7.11}$$

where the complex valued coefficients are written in their polar form with $\tau, \varphi_1, \varphi_2 \in \mathbb{R}_{0+}$. Therewith, we found a parameterization for the BV $\boldsymbol{w}$ similar to the one used in Equation (6.3), but with parameters that are still complex valued. In the following, we show that it is sufficient to use real valued parameters.

We observe that $e^{i\varphi_1}$ in Equation (7.11) has no impact on $|\boldsymbol{h}^{\text{H}}\boldsymbol{w}|^2$ and $|\boldsymbol{g}^{\text{H}}\boldsymbol{w}|^2$ in the Optimization Problem (7.7). Consequently, we choose $\varphi_1 = 0$. Further, $\varphi_2 = 0$ maximizes $|\boldsymbol{h}^{\text{H}}\boldsymbol{w}|^2$ while keeping the distribution of $|\boldsymbol{g}^{\text{H}}\boldsymbol{w}|^2$ unchanged. Therefore, we set $\varphi_2 = 0$ and obtain the parameterization in Equation (6.3).

Second step In the second step of the proof we derive the secrecy outage probability ϵ in Equation (7.7) from the distribution of the random variables.

By applying the uncertainty model of Definition (6.1) and defining

$$z = \frac{1}{\rho}(2^{-R_S^\epsilon} - 1) + 2^{-R_S^\epsilon} \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2 \quad \text{and} \tag{7.12}$$

$$\nu = \mu + \sqrt{2}\, \tilde{\boldsymbol{g}}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \quad \text{with} \quad \mu = \sqrt{\frac{2\kappa\tau}{1-\kappa}} \frac{\boldsymbol{d}^{\mathrm{H}}\boldsymbol{h}}{\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|} \tag{7.13}$$

we can express the secrecy outage probability ϵ of the Optimization Problem (7.7) as

$$\begin{aligned}
&\Pr\left(\log_2 \frac{1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w} \right|^2}{1 + \rho \left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w} \right|^2} < R_S^\epsilon \right) \\
&= \Pr\left(\left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2 > \frac{1}{\rho}(2^{-R_S^\epsilon} - 1) + 2^{-R_S^\epsilon} \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2 \right) \\
&= \Pr\left(\left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2 > z \right) \\
&= \Pr\left(\left| \sqrt{\frac{2\kappa\tau}{1-\kappa}} \frac{\boldsymbol{d}^{\mathrm{H}}\boldsymbol{h}}{\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|} + \sqrt{2}\, \tilde{\boldsymbol{g}}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2 > \frac{2z}{1-\kappa} \right) \\
&= \Pr\left(|\nu|^2 > \frac{2z}{1-\kappa} \right),
\end{aligned} \tag{7.14}$$

where the random variable $\tilde{\boldsymbol{g}}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau)$ is complex Gaussian distributed with zero mean and variance one, which follows from the distribution of $\tilde{\boldsymbol{g}}$ and the power constraint $\|\boldsymbol{w}\|^2 = 1$. Therefore, the random variable ν is complex Gaussian distributed with mean μ and variance 2. Consequently, the random variable $|\nu|^2$ is non-central χ^2 distributed with two degrees of freedom and non-centrality parameter $|\nu|^2$.

The secrecy outage probability ϵ can then be expressed as [Pro00]

$$\epsilon = \Pr\left(|\nu|^2 > \frac{2z}{1-\kappa} \right) = Q_1\left(|\nu|, \sqrt{\frac{2z}{1-\kappa}} \right)$$

$$= Q_1 \left(\sqrt{\frac{2\kappa\tau}{1-\kappa}} \|\boldsymbol{d}\|, \sqrt{\frac{2 - 2^{R_S^\epsilon+1} + 2\rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2}{2^{R_S^\epsilon} \rho (1-\kappa)}} \right). \qquad \square$$

(7.9) Corollary (Uniqueness of Solution).
For every given target secrecy rate R_S^ϵ, there exists a unique parameterization τ for the optimal BV in Equation (6.3) that solves the Optimization Problem (7.7). ✓

The proof of this Corollary is given in Appendix B.3.

The optimal τ can be found using any search algorithm over the complete set of BVs, e.g., bisection method. As this is quite slow and inefficient, we will give a suboptimal but closed form solution in Section 7.1.2.

As for the ergodic secrecy rate, we can characterize the optimal transmit strategy for the case where no CSI on the transmitter site is given.

(7.10) Corollary (Beamforming without CSI).

For $\kappa = 0$, the optimal parameter τ that maximizes the secrecy outage probability in Equation (7.7) is $\tau^{\mathrm{MRT}} = {\|\boldsymbol{\Pi}_{\boldsymbol{d}} \boldsymbol{h}\|^2}/{\|\boldsymbol{h}\|^2}$. ✓

Proof.
If the transmitter has no CSI on the channel to the eavesdropper, i.e., $\kappa = 0$, the secrecy outage probability ϵ given in Equation (7.14) reduces to

$$\epsilon = \Pr\left(|y|^2 > z \right) = \int_z^\infty 2e^{-2y} dy \qquad (7.15)$$
$$= e^{-2z},$$

where $y = |\boldsymbol{g}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau)|^2$ and z is defined in Equation (7.12). Equation (7.15) follows from the fact that the random variable $|y|^2$ is exponentially distributed with rate parameter 2, i.e., $|y|^2 \sim \mathrm{Exp}(2)$.

Due to the exponential distribution and for a fixed value of the secrecy outage probability ϵ, the condition of the Optimization Problem (7.7) can be transformed into

$$\epsilon = e^{-2z} \quad \Leftrightarrow \quad R_S^\epsilon = \log_2 \frac{1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2}{1 - \frac{\rho}{2} \ln \epsilon}$$

and the maximization problem in Equation (7.5) of the Optimization Problem (7.7) can be expressed as

$$\max_{0\leq\tau\leq 1} \log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2}{1-\frac{\rho}{2}\ln\epsilon},$$

which has the same solution as the strict concave maximization problem (see Appendix B.4 for the proof of concavity) given by

$$\max_{0\leq\tau\leq 1} \left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2. \tag{7.16}$$

As this maximization problem is identical to the maximization of the transmission in a peaceful system without eavesdropper and the channel to the receiver Bob is perfectly known, the optimal parameterization for the BV is given by

$$\tau^* = \tau^{\mathrm{MRT}} = \frac{\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|^2}{\|\boldsymbol{h}\|^2},$$

which yields the MRT BV

$$\boldsymbol{w}(\tau^{\mathrm{MRT}}) = \frac{\boldsymbol{h}}{\|\boldsymbol{h}\|} = \boldsymbol{w}_{\mathrm{MRT}}. \qquad \square$$

A Suboptimal Alternative

Using the Markov inequality [Bil95], which is given by

$$\Pr(X \geq a) \leq \frac{\mathrm{E}[X]}{a},$$

we get an upper bound on the secrecy outage probability derived by Proposition (7.8).

For the approximation of the secrecy outage probability ϵ under usage of the Markov inequality, we use the probability expression of Optimization Problem (7.7), which yields

$$\Pr\left(|\nu|^2 > \frac{2z}{1-\kappa}\right) \leq \frac{\mathrm{E}\left[|\nu|^2\right]}{\frac{2z}{1-\kappa}} \tag{7.17}$$

with z and ν defined in Equations (7.12) and (7.13), respectively. Recall that $|\nu|^2 \sim \chi_2^2(|\mu|^2)$. Therefore, the expectation is given by

$$\mathrm{E}\left[|\nu|^2\right] = 4 + |\mu|^2 .$$

We insert this expectation into Equation (7.17) and get

$$\Pr\left(|\nu|^2 \geq \frac{2z}{1-\kappa}\right) \leq \frac{(1-\kappa)\left(4+|\mu|^2\right)}{2z}. \tag{7.18}$$

Finally, we re-substitute the variable z (defined in Equation (7.12)) and get the programming problem

$$\min_{0\leq\tau\leq\tau^{\mathrm{MRT}}} \frac{(1-\kappa)\left(4+|\mu|^2\right)}{2\left(\frac{1}{\rho}\left(2^{-R_S^\epsilon}-1\right)+2^{-R_S^\epsilon}\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2\right)}$$

with $\tau^{\mathrm{MRT}} = {\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|^2}/{\|\boldsymbol{h}\|^2}$. The optimal parameter τ that solves this programming problem can be given in closed form[1]. This suboptimal scheme is used for the illustrations in Chapter 8 as a reference value for the secrecy outage probability.

7.2 Optimal Protection Strategies

In this section, we present beamforming schemes for the ergodic secrecy rate and the secrecy outage probability under usage of AN as protection strategy. In [NG05], the authors first introduced a method to increase the secrecy rate by using AN. Later, AN is applied to a MISO system, where the data transmission scheme used is MRT and the artificial noise is transmitted uniformly in the null space of $\boldsymbol{h}$ in [ZM09]. Contrary to the transmission scheme in [ZM09], we consider the optimal beamforming of Section 7.1 and further optimize the transmit directions for the AN signals.

Figure 7.1 shows the beamforming directions for the AN strategy which is used in Propositions (7.13) and (7.19). The shaded plane in Figure 7.1

[1]The closed form expression is a long term which is not provided here. Nevertheless, it can easily be derived by taking the first derivative of the right-hand side of Equation (7.18) with respect to τ and solving the resulting expression for τ.

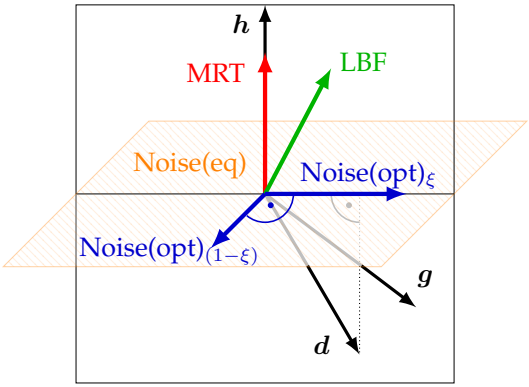


Figure 7.1: Graphical interpretation of BVs and AN directions in 3D.

(named Noise(eq)) is the null space of $\boldsymbol{h}$. The noise power is split by the parameter $\xi \in [0, 1]$ in order to use different directions. For $\xi = 0$, the AN is equally distributed in this plane. If $\xi > 0$, the artificial noise is split into two parts, where one is sent in the direction of the projection of $\boldsymbol{d}$ onto the orthogonal basis of $\boldsymbol{h}$ (depicted in Figure 7.1 by Noise(opt)$_\xi$). The other part is sent into the null space of $\boldsymbol{h}$, but also orthogonal to the direction Noise(opt)$_\xi$. For a system with three transmit antennas, and therefore three dimensions for transmission, this would relate to the direction Noise(opt)$_{(1-\xi)}$ in Figure 7.1.

7.2.1 Ergodic Secrecy Rate

Again, we first study the fast fading case. Therefore, we analyze the ergodic secrecy rate (see Section 3.1).

(7.11) Definition (Ergodic Secrecy Rate with AN).
The ergodic secrecy rate R_S for the MISO wiretap channel, where the transmitter Alice additionally protects the data transmission by sending AN in the null space of the main channel $\boldsymbol{h}$ (see Section 4.1), is given by

$$R_S(\boldsymbol{w}, \boldsymbol{W}) = \left[\mathrm{E}_{\boldsymbol{h}} \left[\log_2 \left(1 + \rho \left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w} \right|^2 \right) \right] - \mathrm{E}_{\boldsymbol{g}} \left[\log_2 \left(1 + \frac{\rho \left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w} \right|^2}{1 + \rho \left\| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{W} \right\|^2} \right) \right] \right]^+ .$$

If the channel to the intended receiver Bob is known perfectly, the expectation over $\boldsymbol{h}$ in the first term can be skipped, as the transmitter Alice can choose an appropriate BV $\boldsymbol{w}$ for every realization of $\boldsymbol{h}$. The ergodic secrecy rate is then given by

$$R_S(\boldsymbol{w}, \boldsymbol{W}) = \left[\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \mathrm{E}_{\boldsymbol{g}}\left[\log_2\left(1+\frac{\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left\|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}\right\|^2}\right)\right]\right]^+. \quad \checkmark$$

(7.12) Optimization Problem.
Alice splits her transmit power in order to transmit data and, simultaneously, protect the data transmission by sending AN in the null space of the main channel $\boldsymbol{h}$, i.e., $\boldsymbol{h}^{\mathrm{H}}\boldsymbol{W} = 0$. This leads to the programming problem

$$\max_{\substack{\boldsymbol{w},\boldsymbol{W}:\|\boldsymbol{w}\|^2=\phi \\ \mathrm{trace}(\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}})=(1-\phi) \\ \boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}=0}} R_S(\boldsymbol{w}, \boldsymbol{W}),$$

where $0 \leq \phi \leq 1$. The BV $\boldsymbol{w}$ is used for data transmission whereas the matrix $\boldsymbol{W}$ of dimension $(n_T - 1) \times (n_t - 1)$ is used to create artificial noise. ✓

(7.13) Proposition.
The optimal transmit strategy solving the Optimization Problem (7.12) is characterized by a power splitting parameter ϕ with $0 \leq \phi \leq 1$ for data transmission and artificial noise. Furthermore, the optimal Beamforming Vector for the data is $\boldsymbol{w}_{\mathrm{LBF}}(\tau)$ as in Equation (6.3) with $0 \leq \tau \leq 1$. The artificial noise power is split into two parts ξ and $(1-\xi)$ with $0 \leq \xi \leq 1$. The artificial noise is constructed by an orthonormal basis for the orthogonal complement of $(\boldsymbol{h}, \boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}/\|\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}\|)$ denoted by $\boldsymbol{u}_1, ..., \boldsymbol{u}_{n_T-2}$. Then the artificial noise is created by

$$\boldsymbol{r}_x = \sqrt{\xi}\frac{\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}}{\|\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}\|}r_0 + \frac{\sqrt{1-\xi}}{n_T-2}\sum_{k=1}^{n_T-2}\boldsymbol{u}_k r_k, \tag{7.19}$$

where $r_0, \ldots, r_{n_T-2}$ are i.i.d. complex zero-mean Gaussian random variables with variance one.

The ergodic secrecy capacity from the solution of Optimization Problem (7.12) is given by

$$R_S(\tau,\phi,\xi) = \left[\log_2\left(1+\Gamma_B\right) - \mathrm{E}_{\boldsymbol{g}}[\log_2\left(1+\Gamma_E\right)]\right]^+ \quad \text{with} \tag{7.20}$$

$$\Gamma_B = \rho\phi\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2 \quad \text{and}$$

$$\Gamma_E = \frac{\rho\phi\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2}{1+\rho(1-\phi)\left(\xi\left|\boldsymbol{g}^{\mathrm{H}}\frac{\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}}{\|\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}\|}\right|^2 + \frac{(1-\xi)}{n_T-2}\sum_{k=1}^{n_T-2}\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{u}_k\right|^2\right)}. \quad \checkmark$$

Proof.
The proof consists of two steps. At first, the optimal beamforming strategy is derived. Then the optimal power allocation for the AN is obtained.

First step The Optimization Problem (7.12) can be transformed into two nested maximization problems

$$\max_{\substack{\boldsymbol{W}:\mathrm{trace}(\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}})=(1-\phi)\\ \boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}=0}}\left(\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=\phi} R_S(\boldsymbol{w},\boldsymbol{W})\right). \tag{7.21}$$

The inner optimization problem is almost identical to the Optimization Problem (7.2) with increased noise plus interference in the second term, i.e.,

$$\max_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=\phi}\left[\log_2\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \mathrm{E}_{\boldsymbol{g}}\left[\log_2\left(1+\frac{\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}{z}\right)\right]\right]^+ \tag{7.22}$$

where $z \geq 1$ contains the noise variance plus AN. Therefore, the optimal BV of the inner optimization in Equation (7.21) is identical to the optimal BV of the Optimization Problem (7.2), which is given in Proposition (7.3).

Second step The second part of Proposition (7.13) is proved by showing that the AN is optimally allocated in the (n_T-1)-dimensional subspace in Equation (7.19). The main observation is that there is only one distinguished direction: the deterministic component $\boldsymbol{d}$ of the channel to Eve. Therefore, we allocate power $\xi(1-\phi)$ for the AN in direction $\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}$.

Obviously, the remaining $(n_T - 2)$-dimensional subspace is spanned by the corresponding vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n_T-2}$.

Let us allocate powers $\boldsymbol{\pi} = [\pi_1, \ldots, \pi_{n_T-2}]$ with $\sum_{l=1}^{n_T-2} \pi_l = (1-\xi)(1-\phi)$ to the directions $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n_T-2}$, respectively, and consider the second term of the ergodic secrecy rate $R_S(\tau, \phi, \xi)$ in Equation (7.20), which is given by

$$f(\boldsymbol{\pi}) = -\mathrm{E}_{\boldsymbol{g}}\left[\log_2\left(1 + \frac{a}{b + \sum_{k=1}^{n_T-2} \pi_k \left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{u}_k\right|^2}\right)\right] \quad \text{with} \tag{7.23}$$

$$a = \rho\phi \left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}_{\mathrm{LBF}}(\tau)\right|^2 \geq 0 \quad \text{and}$$

$$b = 1 + \rho(1-\phi)\xi \left|\boldsymbol{g}^{\mathrm{H}} \frac{\boldsymbol{\Pi}_{\boldsymbol{h}}^{\perp}\boldsymbol{d}}{\|\boldsymbol{\Pi}_{\boldsymbol{h}}^{\perp}\boldsymbol{d}\|}\right|^2 > 0.$$

Note that $|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{u}_k|^2 = \|\sqrt{1-\kappa}\,\tilde{\boldsymbol{g}}^{\mathrm{H}}\boldsymbol{u}_k\|^2$ with $k = 1, 2, \ldots, n_T - 2$, because $\boldsymbol{u}_k$ is orthogonal to both $\boldsymbol{h}$ and $\boldsymbol{\Pi}_{\boldsymbol{h}}^{\perp}\boldsymbol{d}$, which implies that $\boldsymbol{u}_k$ is orthogonal to $\boldsymbol{\Pi}_{\boldsymbol{h}}\boldsymbol{d} + \boldsymbol{\Pi}_{\boldsymbol{h}}^{\perp}\boldsymbol{d} = \boldsymbol{d}$.

The random variable $\tilde{\boldsymbol{g}}$ is circular symmetric complex Gaussian distributed. Therefore, f is a symmetric function in $\boldsymbol{\pi} = [\pi_1, \ldots, \pi_{n_T-2}]$, i.e., for any permutation $[i_1, \ldots, i_{n_T-2}]$ of the set $\{1, 2, \ldots, n_T - 2\}$ it holds

$$f(\pi_1, \ldots, \pi_{n_T-2}) = f(\pi_{i_1}, \ldots, \pi_{i_{n_T-2}}).$$

Further, the function is concave with respect to $\boldsymbol{\pi} = [\pi_1, \ldots, \pi_{n_T-2}]$ in the interval $[0, \infty)$, because the second derivative of f with respect to $\boldsymbol{\pi}$ is negative. These two properties imply that the function is a Schur-concave function [MO79; JB07] and the maximum is achieved for $\pi_1 = \pi_2 = \ldots = \pi_{n_T-2} = {}^{(1-\xi)(1-\phi)}/_{n_T-2}$. □

As before in Section 7.1.1, τ depends only on the SNR ρ and the degree of channel knowledge κ. Additionally, ϕ depends on the SNR ρ, while ξ depends only on the channel knowledge κ, as this parameter shifts the transmit power with growing κ from an equally distributed transmission in the null space of Bob to the deterministic channel direction $\boldsymbol{d}$. Again, there can be made four observations, which are given in the following corollaries.

(7.14) Corollary (Beamforming without CSI).

For $\kappa = 0$, the optimal ξ, which maximizes the ergodic secrecy rate $R_S(\tau, \phi, \xi)$ in Equation (7.20) converges to

$$\xi = \frac{(1-\xi)}{n_T - 2} \quad \Leftrightarrow \quad \xi = \frac{1}{n_T - 1} \quad \text{if} \quad n_T > 1. \tag{7.24}$$

This is due to the fact that we have no distinguished direction $\boldsymbol{d}$ for $\kappa = 0$. Therefore, it is optimal to distribute the AN uniformly in the null space of $\boldsymbol{h}$. ✓

(7.15) Corollary (Beamforming with full CSI).

For $\kappa = 1$, the optimal ξ, which maximizes the ergodic secrecy rate $R_S(\tau, \phi, \xi)$ in Equation (7.20) converges to one. This can be seen straightforward, as it is not reasonable to transmit artificial noise in any other direction than the one to Eve. ✓

From Corollaries (7.14) and (7.15) follows that the optimal ξ in the ergodic secrecy rate $R_S(\tau, \phi, \xi)$ given in Equation (7.20) is from the interval $[1/n_T - 1, 1]$.

(7.16) Corollary (Beamforming for low SNR).

For low SNR, i.e., $\rho \to 0$, the optimal ϕ, which maximizes the ergodic secrecy rate $R_S(\tau, \phi, \xi)$ in Equation (7.20) converges to one, i.e., the artificial noise part converges to zero. ✓

Proof.
The Taylor series expansion of Equation (7.20) at $\rho = 0$ of the first degree shows that for asymptotic low SNR the programming problem can be rewritten as

$$\max_{\phi: 0 \leq \phi \leq 1} \left[\frac{\phi}{\ln 2} \left(\left| \boldsymbol{h}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2 - \left| \boldsymbol{g}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau) \right|^2 \right) \right]^+ . \tag{7.25}$$

This programming problem can only be maximized, if the expression $|\boldsymbol{h}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau)|^2 - |\boldsymbol{g}^{\mathrm{H}} \boldsymbol{w}_{\mathrm{LBF}}(\tau)|^2$ is non-negative. This is always given, as the definition of the secrecy rate is such that Alice only transmits, if the rate is positive. Obviously, the maximum of the above programming problem is given by $\phi = 1$. □

(7.17) Corollary (Beamforming for high SNR with full CSI).

For $\kappa = 1$ and high SNR, i.e., $\rho \to \infty$, the optimal ϕ, which maximizes the ergodic secrecy rate $R_S(\tau, \phi, \xi)$ in Equation (7.20) converges to one, i.e., the artificial noise part converges to zero.

This is a generalization of Corollary (7.6), which states that for high SNR and full CSI the optimal transmit strategy is given by ZF, i.e., the eavesdropper receives no signal and therefore it is not necessary to protect the signal by transmission of AN. ✓

7.2.2 Secrecy Outage Probability

Let us now study the protection strategy AN for the slow fading scenario, where the chosen measure is the secrecy outage probability (see Section 3.2).

(7.18) Optimization Problem.
Alice splits her transmit power in order to transmit data and, simultaneously, protect the data transmission by sending AN in the null space of the main channel $\boldsymbol{h}$, i.e., $\boldsymbol{h}^{\mathrm{H}}\boldsymbol{W} = 0$. This yields the programming problem

$$\max_{\substack{\boldsymbol{w},\boldsymbol{W},\phi:\|\boldsymbol{w}\|^2=\phi \\ \mathrm{trace}(\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}})=(1-\phi) \\ \boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}=0}} R_S^{\epsilon} \quad \text{s.t.} \quad \Pr\left(\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\frac{\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left\|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}\right\|^2}} < R_S^{\epsilon} \right) = \epsilon, \tag{7.26}$$

where $0 \leq \phi \leq 1$. The BV $\boldsymbol{w}$ is used for data transmission whereas the matrix $\boldsymbol{W}$ of the dimension $(n_T - 1) \times (n_T - 1)$ is used to create artificial noise. Again, according to Theorem (B.1) in Appendix B.1, we can give the equivalent minimization problem for a fixed target secrecy rate R_S^{ϵ}

$$\min_{\substack{\boldsymbol{w},\boldsymbol{W},\phi:\|\boldsymbol{w}\|^2=\phi \\ \mathrm{trace}(\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}})=(1-\phi) \\ \boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}=0}} \epsilon \quad \text{s.t.} \quad \epsilon = \Pr\left(\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\frac{\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left\|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}\right\|^2}} < R_S^{\epsilon} \right). \tag{7.27}$$

✓

(7.19) Proposition.
The optimal transmit strategy solving the Optimization Problem (7.18) can be characterized by a power splitting parameter ϕ with $0 \leq \phi \leq 1$ for data transmission and artificial noise. Furthermore, the optimal Beamforming Vector for the data is $\boldsymbol{w}_{\text{LBF}}(\tau)$ as given in Equation (6.3) with $0 \leq \tau \leq 1$. The artificial noise power is split into two parts ξ and $(1-\xi)$ with $0 \leq \xi \leq 1$. The artificial noise is constructed by an orthonormal basis for the orthogonal complement of $(\boldsymbol{h}, \boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}/\|\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}\|)$ denoted by $\boldsymbol{u}_1, ..., \boldsymbol{u}_{n_T-2}$. Then the artificial noise is created by

$$\boldsymbol{r}_x = \sqrt{\xi}\frac{\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}}{\|\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}\|}r_0 + \frac{\sqrt{1-\xi}}{n_T-2}\sum_{k=1}^{n_T-2}\boldsymbol{u}_k r_k$$

where $r_0, \ldots, r_{n_T-2}$ are i.i.d. complex zero-mean Gaussian random variables with variance one.

The secrecy rate that implements these power splitting mechanisms is given by

$$\begin{aligned} R_S(\tau,\phi,\xi) &= \left[\log_2(1+\Gamma_B) - \log_2(1+\Gamma_E)\right]^+ \quad \text{with} \\ \Gamma_B &= \rho\phi\left|\boldsymbol{h}^{\text{H}}\boldsymbol{w}_{\text{LBF}}(\tau)\right|^2 \quad \text{and} \\ \Gamma_E &= \frac{\rho\phi\left|\boldsymbol{g}^{\text{H}}\boldsymbol{w}_{\text{LBF}}(\tau)\right|^2}{1+\rho(1-\phi)\left(\xi\left|\boldsymbol{g}^{\text{H}}\frac{\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}}{\|\boldsymbol{\Pi}_h^{\perp}\boldsymbol{d}\|}\right|^2 + \frac{(1-\xi)}{n_T-2}\sum_{k=1}^{n_T-2}\left|\boldsymbol{g}^{\text{H}}\boldsymbol{u}_k\right|^2\right)}. \quad \checkmark \end{aligned} \tag{7.28}$$

Proof.
The proof consists of two steps. At first, the optimal beamforming strategy is derived. Then the optimal power allocation for the AN is obtained.

First step The minimization problem Equation (7.27) given in Optimization Problem (7.18) can be transformed into two nested minimiza-

tion problems

$$\min_{\substack{\boldsymbol{W}:\mathrm{trace}(\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}})=(1-\phi)\\ \boldsymbol{h}^{\mathrm{H}}\boldsymbol{W}=0}} \left(\min_{\boldsymbol{w}:\|\boldsymbol{w}\|^2=\phi} \epsilon \right. \\ \left. \text{s.t.} \quad \epsilon = \Pr\left(\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\frac{\rho|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2}{1+\rho\|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{W}\|^2}} < R_S^{\epsilon} \right) \right). \tag{7.29}$$

The inner optimization problem is almost identical to Equation (7.6) of Optimization Problem (7.7) with increased noise plus interference in the second term. Therefore, the optimal BV of the inner optimization in Equation (7.29) is identical to the optimal BV of Optimization Problem (7.7), which is given in Proposition (7.8).

Second step The second part of the proof of Proposition (7.19) is almost identical to the proof of Proposition (7.13). Solely, the function $f(\boldsymbol{\pi})$ in Equation (7.23) differs and is for this proof given by

$$f(\boldsymbol{\pi}) = \log_2\left(1 + \frac{a}{b + \sum_{k=1}^{n_T-2} \pi_k \left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{u}_k\right|^2}\right)$$

with a and b as in Equation (7.23). □

Similar to the ergodic secrecy rate analysis in Section 7.2.1, we can make some observations on the behavior of the secrecy outage probability for certain special cases.

(7.20) Beamforming without CSI.
If no CSI is available, Corollary (7.14) holds. ✓

From this fact follows that the optimal ξ, which maximizes the secrecy rate $R_S(\tau, \phi, \xi)$ given in Equation (7.28), is in the interval $[1/n_T-1, 1]$.

(7.21) Corollary (Beamforming for low SNR).
For low SNR, i.e., $\rho \to 0$, the optimal ϕ in Optimization Problem (7.18) converges to one, i.e., the AN part converges to zero. ✓

Proof.
Let us consider the minimum energy per information bit $(E_b/N_0)^{\text{sec}}_{\text{min}}$ that is required to communicate reliable under secrecy constraints. This performance measure for vanishing SNR per bandwidth is defined in [Gur09] as

$$\left(\frac{E_b}{N_0}\right)^{\text{sec}}_{\text{min}} = \frac{\log_{\text{e}} 2}{R'_S(0)}, \tag{7.30}$$

where $R'_S(0)$ is the first derivative of R_S with respect to the SNR ρ at the point $\rho = 0$. Calculating

$$R'_S(0) = \phi \left(\left| \boldsymbol{h}^{\text{H}} \boldsymbol{w} \right|^2 - \left| \boldsymbol{g}^{\text{H}} \boldsymbol{w} \right|^2 \right) \tag{7.31}$$

we can see that the AN term has been canceled out and $R'_S(0)$ is independent of the AN. Combining Equations (7.30) and (7.31), we get

$$\left(\frac{E_b}{N_0}\right)^{\text{sec}}_{\text{min}} = \frac{\log_{\text{e}} 2}{\phi \left(\left| \boldsymbol{h}^{\text{H}} \boldsymbol{w} \right|^2 - \left| \boldsymbol{g}^{\text{H}} \boldsymbol{w} \right|^2 \right)}.$$

The secrecy outage probability is expressed as

$$\begin{aligned} &\Pr\left(\left(\frac{E_b}{N_0}\right)^{\text{sec}}_{\text{min}} > \left(\frac{E_b}{N_0}\right)^{\text{target}}_{\text{min}} \right) = \epsilon \\ = &\Pr\left(\frac{\log_{\text{e}} 2}{\left(\frac{E_b}{N_0}\right)^{\text{target}}_{\text{min}}} > \phi \left(\left| \boldsymbol{h}^{\text{H}} \boldsymbol{w} \right|^2 - \left| \boldsymbol{g}^{\text{H}} \boldsymbol{w} \right|^2 \right) \right) = \epsilon. \end{aligned}$$

It can be seen that this term is minimal for $\phi = 1$, which yields the $(E_b/N_0)^{\text{sec}}_{\text{min}}$ for the secrecy rate without AN. □

8 Illustrations

If not stated otherwise, all simulations show the ergodic secrecy rates discussed in Sections 7.1.1 and 7.2.1, for a fading MISO wiretap channel with the uncertainty model specified in Definition (6.1) with four transmit antennas from the transmitters point of view.

For the simulations, we kept the random channel realization $\boldsymbol{g}$ fixed for one simulation and varied over the degree of channel knowledge κ. We first generated the channel $\boldsymbol{g}$ and the random component $\tilde{\boldsymbol{g}}$. Out of these vectors, the deterministic part $\boldsymbol{d} = \sqrt{\kappa}\,\boldsymbol{g} + \sqrt{1-\kappa}\,\tilde{\boldsymbol{g}}$ of the channel $\boldsymbol{g}$ to Eve is calculated.

The secrecy rates are calculated with the channel realizations $\boldsymbol{h}$ and $\boldsymbol{g}$ and the beamforming vectors derived by Alice based on her limited knowledge about $\boldsymbol{g}$. All rates are upper bounded by the secrecy capacity that can be achieved for full CSI with the beamforming strategy given in Theorem (2.10) (GEIG). For the simulations, we calculated the secrecy rates derived by the Linear Beamforming (LBF) strategy given in Proposition (7.3) and by the Linear Beamforming with AN (LBF + optAN) strategy given in Proposition (7.13). For comparison, we computed the secrecy rates derived by LBF plus equally distributed AN into the null space of $\boldsymbol{h}$ (LBF + eqAN). This corresponds to the secrecy rate given in Equation (7.20) for a fixed $\xi = {}^{1}/_{n_T-1}$. For comparison, we also calculated the secrecy rates for MRT, ZF, and MRT and ZF plus equally distributed AN in the null space of $\boldsymbol{h}$ (MRT + eqAN and ZF + eqAN, respectively).

Figure 8.1 shows simulation results for the MISO WTC with four transmit antennas. It can be seen, that in the case of no channel knowledge, i.e., $\kappa = 0$, the LBF strategy is equal to the MRT, but superior to the ZF strategy. This corresponds to Corollary (7.4). Similarly, the LBF + optAN and LBF + eqAN strategies are equal to the MRT + optAN. As stated in Corollary (7.5), in case of full CSI, i.e., $\kappa = 1$, ZF and all LBF strategies achieve the upper bound given by the generalized eigenvector in Theorem (2.10). All beamforming strategies with AN yield better

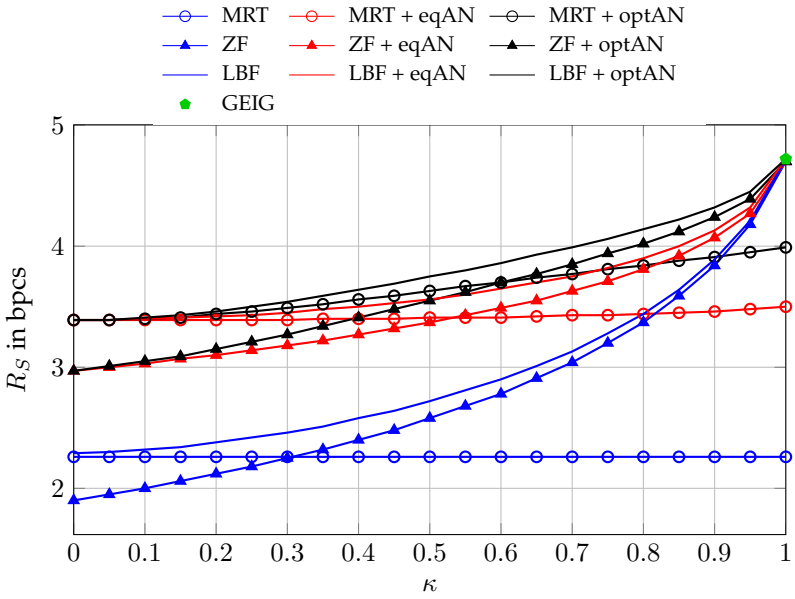


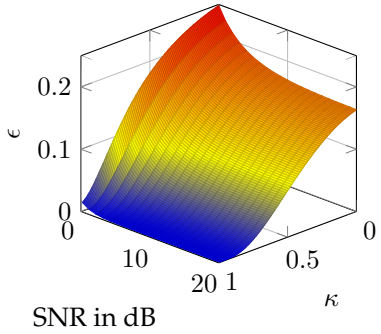
Figure 8.1: Ergodic secrecy rates R_S in bits/complex symbol over κ in the MISO WTC with $n_T = 4$ for different transmission schemes with and without AN.

results than the strategies without AN for $\kappa < 1$. The gap between strategies with and without AN increases with increasing SNR.

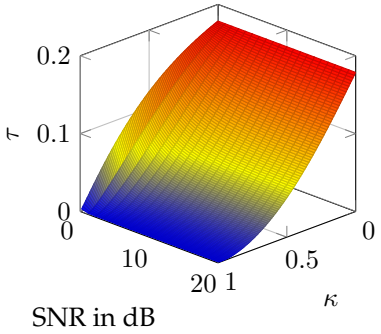
The simulations represent the secrecy outage probabilities for a fading MISO WTC with the uncertainty model specified in Definition (6.1) with four transmit antennas from the transmitters point of view. The positions of the intended receiver and the eavesdropper are modeled by the angle ψ between the channel $\boldsymbol{h}$ and the known deterministic channel component $\boldsymbol{d}$ of the channel $\boldsymbol{g}$, which is given by

$$\psi = \arccos \frac{\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{d}\right|}{\|\boldsymbol{h}\|\,\|\boldsymbol{d}\|}.$$

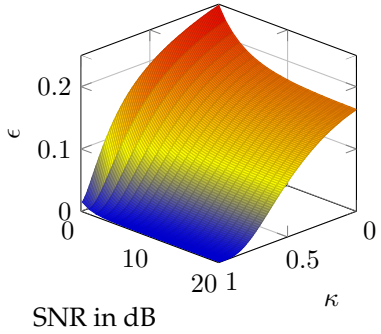
For the simulations, we calculate the secrecy outage probability derived by the Linear Beamforming (LBF) strategy given by Proposition (7.8), where we find the optimal τ by bisection method. This is possible due



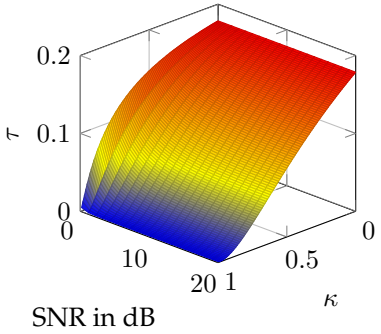
(a) Secrecy outage probability ϵ



(b) Optimal τ



(c) Markov bound on the secrecy outage probability ϵ



(d) Optimal τ calculated for the Markov bound

Figure 8.2: Comparison of the secrecy outage probabilities ϵ derived by Proposition (7.8) and the Markov bound on ϵ given in Section 7.1.2 as well as the corresponding optimal BV parameter τ, plotted over κ and the SNR for $R_S^\epsilon = 0.8$ bits/complex symbol and $\psi = 65°$ in the MISO WTC with $n_T = 4$.

to the fact that the optimization problem has a unique solution as stated in Corollary (7.9). Additionally, the Markov upper bound, described in Section 7.1.2, is computed for comparison.

In Figure 8.2a, the secrecy outage probability ϵ over the SNR and the channel knowledge κ is plotted for a target secrecy rate of $R_S^\epsilon = 0.8$ bits/complex symbol. The intuitive conclusion that the probability of

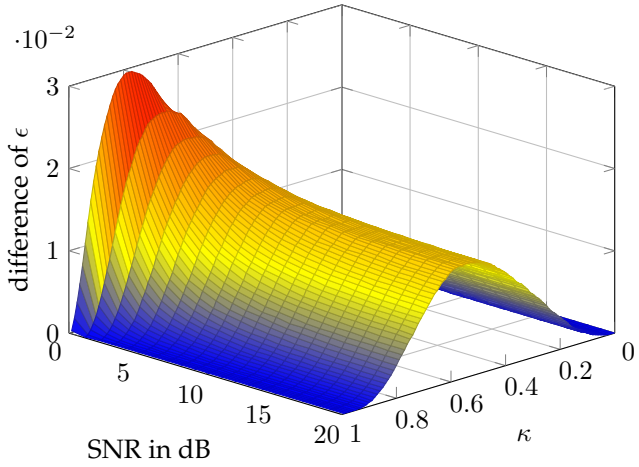
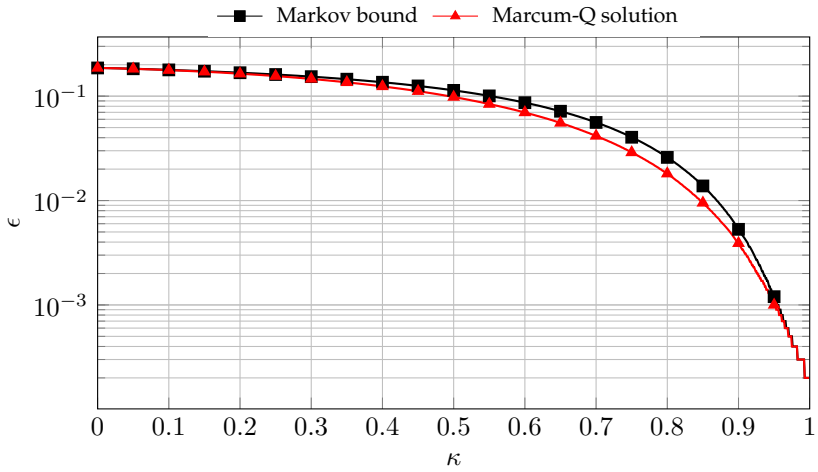


Figure 8.3: Difference of the secrecy outage probabilities ϵ in Figures 8.2a and 8.2c.

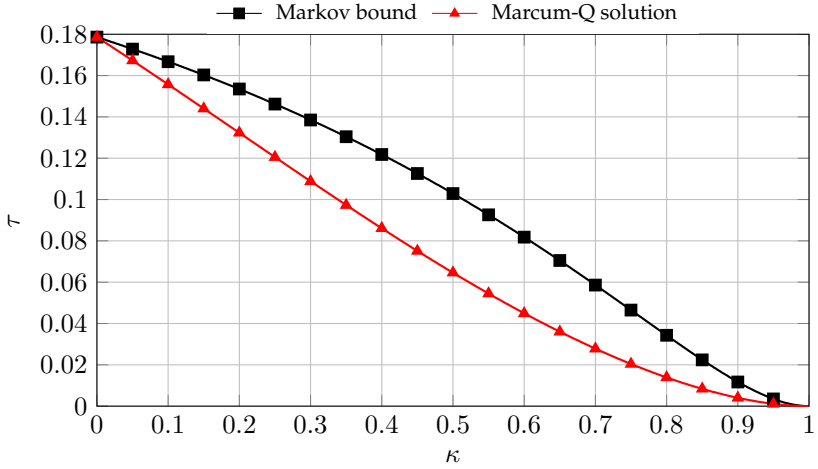
occurrence of an outage event goes to zero as the degree of channel knowledge goes to one, i.e., full channel knowledge, can be confirmed by the figure. Figure 8.2b shows the optimal τ which achieves the secrecy outage probabilities given in Figure 8.2a. For $\kappa = 0$, i.e., no channel knowledge, the optimal beamforming strategy is given by MRT according to Corollary (7.10). MRT is achieved for $\tau = 0.1786$ for the given channel realizations. With growing channel knowledge κ, the optimal beamforming strategy goes to ZF. This convergence goes faster in the high SNR regime.

For comparison, the Markov upper bound on the secrecy outage probability, as described in Section 7.1.2, and the corresponding τ are plotted in Figures 8.2c and 8.2d. It can be observed, that the Markov bound has a similar behavior as the secrecy outage probability derived by Proposition (7.8). This can be seen in detail in Figure 8.3, where the difference between the secrecy outage probability derived by the Marcum Q-function and the Markov bound is plotted. For this example, the gap between the two curves is less than 0.03 in absolute.

Figure 8.4a compares once again the secrecy outage probability ϵ derived by Proposition (7.8) and the Markov bound, and is plotted over the

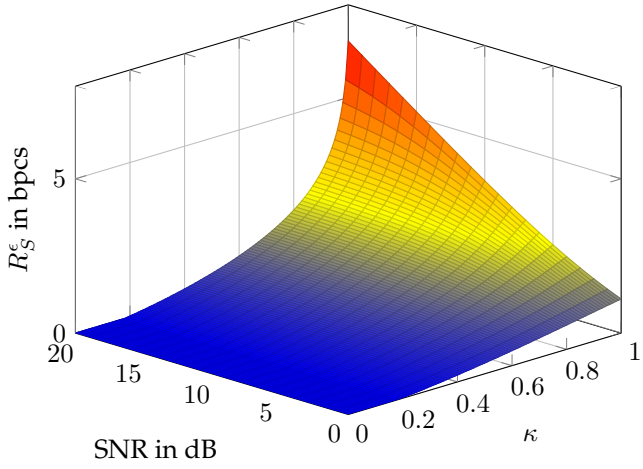


(a) Secrecy outage probability ϵ.

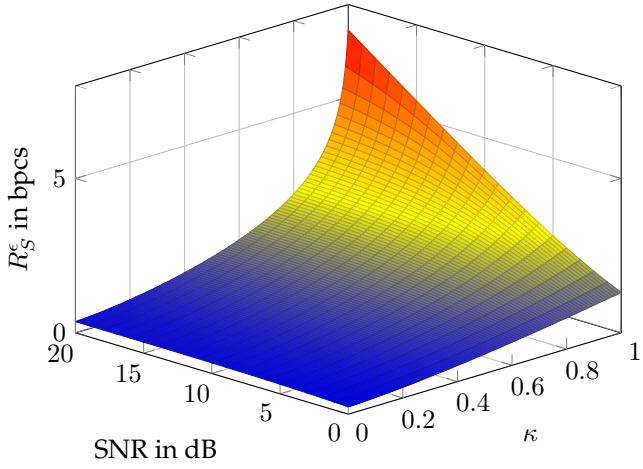


(b) Optimal τ.

Figure 8.4: Comparison of the secrecy outage probability ϵ, derived by Proposition (7.8), and the Markov upper bound given in Section 7.1.2 as well as the corresponding optimal BV parameter τ over κ for $R_S^{\epsilon} = 0.8$ bits/complex symbol, an SNR of 5 dB, and $\psi = 65°$.



(a) Secrecy outage probability $\epsilon = 0.05$.



(b) Secrecy outage probability $\epsilon = 0.1$.

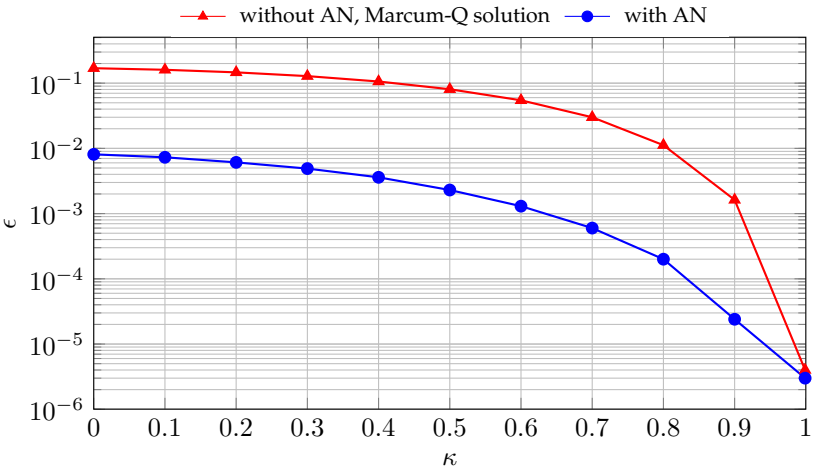
Figure 8.5: Maximized target secrecy rate R_S^ϵ over κ and the SNR for a fixed secrecy outage probability ϵ and $\psi = 65°$.

degree of channel knowledge κ for a fixed SNR of 5 dB and an angle $\psi = 65°$ between the channel vectors $\boldsymbol{h}$ and $\boldsymbol{d}$. For $\kappa < 0.3$ and $\kappa > 0.95$,

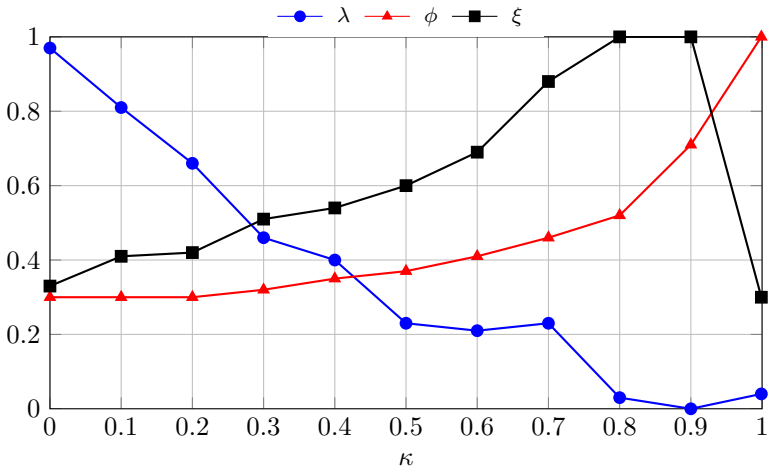
the curves perform almost identically. Although the secrecy outage probabilities behave quite similarly, the corresponding τ are quite different, as can be seen in Figure 8.4b. For this channel realization, MRT is achieved for $\tau = 0.1786$.

Figure 8.5 shows the achievable target secrecy rates R_S^ϵ for a given secrecy outage probability ϵ. If we fix the secrecy outage probability $\epsilon = 0.05$, we can observe in Figure 8.5a that for low channel knowledge, the target secrecy rate is zero. If we allow more secrecy outages, we can achieve a positive target secrecy rate, as can be seen in Figure 8.5b, where the secrecy outage probability is fixed to $\epsilon = 0.1$. Obviously, the highest target secrecy rates can be achieved for full channel knowledge and a high SNR. Additionally, the figures show that for full CSI the target secrecy rates are independent of the secrecy outage probability ϵ. This is due to the fact that we do not have secrecy outages for full CSI, i.e., the transmitter only sends over the channel if a positive secrecy rate can be achieved. The target secrecy rate R_S^ϵ is therefore only dependent on the SNR.

Figure 8.6 shows the secrecy outage probabilities ϵ with and without AN in comparison as well as the parameters λ, ϕ, and ξ that are used to derive the secrecy outage probability with AN. In Figure 8.6a, it can be seen that AN reduces the secrecy outage probability by more than factor 10 over a wide range of κ. Especially for almost full CSI, e.g., $\kappa = 0.8$, the advantage is even bigger, as the transmitter can disturb the eavesdropper with a higher precision. For κ increasing to 1, the gap between both the probabilities decreases. This is due to the fact that for the case with full CSI on the channel to the eavesdropper no secrecy outages occur. Observing the three power splitting parameters in Figure 8.6b, we can see that for no CSI, i.e., $\kappa = 0$, the optimal beamforming strategy is given by MRT, i.e., $\lambda = 1$. Furthermore, the AN is equally distributed in the null space of the main channel, i.e., $\xi = 1/n_T - 1 = 1/3$. When κ increases to one, the AN direction approaches $\mathbf{\Pi}_h^\perp d / \|\mathbf{\Pi}_h^\perp d\|$, i.e., $\xi = 1$. For the case of almost full CSI, i.e., $\kappa = 0.999$, the optimal beamforming strategy approaches the generalized eigenvector beamformer as described in Theorem (2.10). The transmitter sends only data without AN, i.e., $\phi = 1$, thus ξ does not matter any longer and the value assigned in the figure has no meaning. All parameters for the AN case are calculated by exhaustive search over the complete set, i.e., $\lambda \in [0, 1]$, $\phi \in [0, 1]$ and $\xi \in [1/n_T - 1, 1]$. In order to reduce the simulation time to an acceptable value, the step



(a) Secrecy outage probability ϵ.



(b) Optimal λ, ϕ and ξ used for secrecy outage probability ϵ derived by Proposition (7.19).

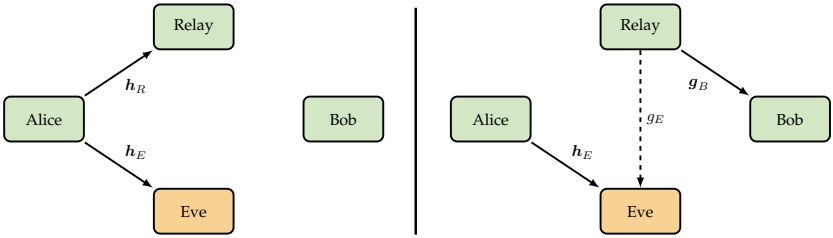
Figure 8.6: Comparison of secrecy outage probabilities ϵ, derived by Propositions (7.8) and (7.19) and Section 7.1.2, and the optimal parameters λ, ϕ and ξ for the AN case over κ for $R_S^\epsilon = 0.8$ bits/complex symbol, an SNR of 10 dB, and $\psi = 65°$.

width of the different parameters is chosen quite coarse, which results in a small inaccuracy in some cases.

Part III

Beamforming and Protection Strategies for Two-Hop Relay Channels

9 System Model



(a) Phase I (b) Phase II

Figure 9.1: System model of the non-regenerative two-hop relay WTC with multiple antennas at Alice and Bob.

The two-hop relay WTC considered in this chapter is based on the non-degraded MISO Gaussian WTC described in Section 2.4. The transmitter Alice wants to send a confidential message over a relay to the intended receiver Bob, while the eavesdropper Eve tries to decode this message. Therefore, we have a four-node relay network without direct link between Alice and Bob as illustrated in Figure 9.1 and described in detail in Section 2.5. The relay is operating in Amplify-and-Forward (AF) mode and the relay and the eavesdropper have single antenna each while Alice and Bob have n_T and n_D antennas, respectively. The receiver does not necessarily need multiple antennas, i.e., $n_D \geq 1$. The channels from the transmitter to the relay and the eavesdropper are denoted by $\boldsymbol{h}_R$ and $\boldsymbol{h}_E$, respectively. The channels from the relay to the destination and the eavesdropper are then labeled as $\boldsymbol{g}_B$ and g_E. All nodes are operating in half duplex mode. Hence, the communication from Alice to Bob requires two phases.

We assume individual power constraints at the transmit nodes denoted by $P_{S,1} = \mathrm{E}[|x|^2]$ (first phase), $P_{S,2} = \mathrm{E}[|x_n|^2]$ (second phase) at the source Alice and P_R at the relay (second phase). Furthermore, we assume

local CSI at the transmitter, i.e., Alice has perfect knowledge about her channels to the relay and the eavesdropper. Additionally, we assume that the relay communicates the channel estimation of the channel g_E to Alice, which results in Alice having an outdated g_E.

(9.1) Definition.
The uncertainty at Alice on the channel g_E is modeled as

$$g_E = \hat{g}_E + \Delta g_E, \tag{9.1}$$

where $\hat{g}_E$ is the estimation on the channel g_E and Δg_E is the estimation error, which is bounded by $|\Delta g_E|^2 \leq \epsilon$. For $\epsilon = 0$, Alice has full CSI on the channel g_E. ✓

If the channel estimation is done at the relay using training-sequences, the estimation error ϵ can be modeled as a scaled version of the channel estimation Mean Square Error (MSE) [Bjö+12; ZWN08]. Bob is assumed to have local CSI, i.e., $\boldsymbol{g}_B$, for decoding purposes.

Denote the transmit beamformer of Alice in the first phase by $\boldsymbol{w}_{S,1}$. The received signals at the relay and the eavesdropper in the first phase are given by

$$\begin{aligned} y_R &= \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_R \quad \text{and} \\ y_{E,1} &= \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_{E,1}, \end{aligned}$$

respectively. Accordingly, the received signals in the second phase at the destination and the eavesdropper are given by

$$\begin{aligned} y_B &= \sqrt{\alpha} \boldsymbol{w}_B^{\mathrm{H}} \boldsymbol{g}_B (\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_R) + n_B \quad \text{and} \\ y_{E,2} &= \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,2} x_n + \sqrt{\alpha} g_E (\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1} x + n_R) + n_{E,2}, \end{aligned}$$

respectively, where $\sqrt{\alpha}$ is the multiplication scalar at the relay. The scalars n_B, n_R, $n_{E,1}$, and $n_{E,2}$ are additive white complex Gaussian noise with zero mean and variance σ^2. The inverse noise power is denoted by $\rho = 1/\sigma^2$. The scalar x_n is a signal sent by the source in order to protect the main signal x, e.g., interference neutralization or artificial noise signals. The receive beamforming vector at the intended receiver Bob in the second phase is given by $\boldsymbol{w}_B$. The secrecy rate is then

$$R_S = \left[C(\Gamma_B) - C(\Gamma_E) \right]^+, \tag{9.2}$$

where we define $C(\mathrm{SINR}) = \log_2(1 + \mathrm{SINR})$. The Signal-to-Interference-plus-Noise Ratio (SINR) expressions are given according to the received signals as

$$\Gamma_B = \frac{\alpha\rho p_{S,1} \left|\boldsymbol{w}_B^{\mathrm{H}} \boldsymbol{g}_B\right|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1}\right|^2}{\alpha \left|\boldsymbol{w}_B^{\mathrm{H}} \boldsymbol{g}_B\right|^2 + 1}, \quad \text{and}$$

$$\Gamma_E = \rho p_{S,1} \left|\boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,1}\right|^2 + \frac{\alpha\rho p_{S,1} \left|g_E\right|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1}\right|^2}{\rho p_{S,2} \left|\boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{S,2}\right|^2 + \alpha \left|g_E\right|^2 + 1} \tag{9.3}$$

with

$$\alpha = \frac{\rho p_R}{\rho p_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{S,1}\right|^2 + 1}. \tag{9.4}$$

To satisfy the power constraints at transmitter and relay, we need to have $0 \leq p_{S,1} \leq P_{S,1}$, $0 \leq p_{S,2} \leq P_{S,2}$ and $0 \leq p_R \leq P_R$, respectively.

In Equation (9.3), the two observations made by the eavesdropper can be identified. In the first term, we see the transmitted signal from the first phase, where Alice sends with power $p_{S,1}$ and transmit beamforming vector $\boldsymbol{w}_{S,1}$. The second term corresponds to the second transmission phase. Here, the eavesdropper gets the data signal over the relay, which is then disturbed by the protection signal sent by Alice and the amplified noise from the relay.

For the transmission of data and the protection signal, Alice performs single-stream beamforming, while Bob performs receive beamforming in order to maximize his receive signal. We define following BVs.

(9.2) Definition (Beamforming Directions).
The transmitter allocates her power such that the data stream and the protection signal is send in a certain direction [TV08]. Similarly, the receiver uses a receive beamforming vector to maximize his receive signal. These vectors are given by

$$\boldsymbol{w}_{\mathrm{MRC}} = \frac{\boldsymbol{g}_B}{\|\boldsymbol{g}_B\|}, \qquad \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} = \frac{\boldsymbol{\Pi}_{\boldsymbol{h}_E}^{\perp} \boldsymbol{h}_R}{\|\boldsymbol{\Pi}_{\boldsymbol{h}_E}^{\perp} \boldsymbol{h}_R\|},$$

$$\boldsymbol{w}_{\mathrm{MRT}}^{\mathrm{Relay}} = \frac{\boldsymbol{h}_R}{\|\boldsymbol{h}_R\|}, \qquad \boldsymbol{w}^{\mathrm{Eve}} = \frac{\boldsymbol{\Pi}_{\boldsymbol{h}_E} \boldsymbol{h}_R}{\|\boldsymbol{\Pi}_{\boldsymbol{h}_E} \boldsymbol{h}_R\|},$$

$$\boldsymbol{w}_{\text{MRT}}^{\text{Eve}} = \frac{\boldsymbol{h}_E}{\|\boldsymbol{h}_E\|}, \quad \boldsymbol{w}_{\text{LBF}}(\tau) = \sqrt{\tau}\boldsymbol{w}_{\text{ZF}}^{\text{Eve}} + \sqrt{1-\tau}\boldsymbol{w}^{\text{Eve}},$$

where $\boldsymbol{w}_{\text{MRC}}$ is the Maximum Ratio Combining (MRC) receive beamforming vector at Bob. The vectors $\boldsymbol{w}_{\text{MRT}}$ and $\boldsymbol{w}_{\text{MRT}}^{\text{Eve}}$ are the Maximum Ratio Transmission (MRT) BVs in the directions of $\boldsymbol{h}_R$ and $\boldsymbol{h}_E$, respectively, applied at Alice. The Zero Forcing (ZF) beamforming vector regarding Eve is given by $\boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$, i.e., the signal is sent in the direction of the projection of $\boldsymbol{h}_R$ onto the null space of $\boldsymbol{h}_E$, and the vector $\boldsymbol{w}^{\text{Eve}}$ is the beamforming vector in the direction of the projection of $\boldsymbol{h}_R$ onto $\boldsymbol{h}_E$. The vector $\boldsymbol{w}_{\text{LBF}}(\tau)$ denotes the linear combination between the BVs $\boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$ and $\boldsymbol{w}^{\text{Eve}}$, where $\tau \in [0,1]$ has to be chosen appropriately. Please note that this definition of $\boldsymbol{w}_{\text{LBF}}(\tau)$ differs from the one given in Definition (6.3). ✓

Irrespective of the transmission scheme used by Alice and the channel realizations, the legitimate receiver Bob maximizes his own receive signal by applying MRC [TV08, p. 3.3.1], i.e., $\boldsymbol{w}_B = \boldsymbol{w}_{\text{MRC}}$.

10 Full Channel State Information

In this chapter, we assume that Alice has full CSI on all channels including channel g_E between the relay and Eve, i.e., $\epsilon = 0$ in Definition (9.1).

For this scenario, we will determine the high-SNR slope and the high-SNR power offset for different transmission strategies in the two-hop channel with and without eavesdropper. Further, the high-SNR power offsets of these transmission strategies will be compared analytically.

Some parts of the presented results of this chapter were published in [Ger+12].

10.1 Beamforming Strategies

First, we will analyze beamforming strategies, where Alice transmits her signal in the first phase and the relay sends the amplified signal to Bob and Eve. No further protection of the sent signal is considered in this section.

10.1.1 Peaceful System

In the peaceful system, Eve is not present. Therefore, we have a normal two-hop channel, where Alice wants to maximize her transmission rate to Bob.

The optimal transmit strategy for the peaceful system is given by MRT, i.e., $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\text{MRT}}$ [TV08, Chapter 5.3.2]. Furthermore, Alice and the relay should send their signals with full power in order to maximize the transmission rate. The secrecy capacity is therefore given as

$$R_P = C\left(\frac{\alpha\rho P_{S,1}\left\|\boldsymbol{g}_B\right\|^2\left\|\boldsymbol{h}_R\right\|^2}{\alpha\left\|\boldsymbol{g}_B\right\|^2+1}\right) \tag{10.1}$$

with $\alpha = \frac{\rho P_R}{\rho P_{S,1}\|\boldsymbol{h}_R\|^2+1}$.

High-SNR Analysis

Following Definition (5.1), the high-SNR slope of the peaceful system is given by

$$\mathcal{S}_{\infty}^{\mathrm{P}} = 1$$

and the high-SNR power offset (Definition (5.2)) is calculated to

$$\mathcal{L}_{\infty}^{\mathrm{P}} = \log_2\left(\frac{1}{P_{S,1}\left\|\boldsymbol{h}_R\right\|^2} + \frac{1}{P_R\left\|\boldsymbol{g}_B\right\|^2}\right). \tag{10.2}$$

10.1.2 Eavesdropper System

In this system, the eavesdropper Eve is present, but Alice is using only beamforming in order to protect the communication, i.e., no additional jamming signal is sent and therefore $P_{S,2} = 0$.

The SINR terms are then given by

$$\Gamma_B = \frac{\alpha\rho p_{S,1}\left\|\boldsymbol{g}_B\right\|^2\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2}{\alpha\left\|\boldsymbol{g}_B\right\|^2+1},$$

$$\Gamma_E = \rho p_{S,1}\left|\boldsymbol{h}_E^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2 + \frac{\alpha\rho p_{S,1}\left|g_E\right|^2\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2}{\alpha\left|g_E\right|^2+1}$$

and $\alpha = \frac{\rho p_R}{\rho p_{S,1}\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{S,1}\right|^2+1}$.

Power Allocation

Let us have a look on the single transmission phases, in order to find the optimal power allocations at transmitter and relay. The first transmission phase in this scenario is similar to the MISO channel studied in Section 2.4. Nevertheless, the beamforming strategy presented in Theorem (2.10) is not necessarily optimal, as we need to take the second transmission phase into account. The optimal beamforming strategy is given by $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\mathrm{LBF}}(\tau)$, which also includes the generalized eigenvalue beamformer given in Theorem (2.10). As the maximization of the

achievable secrecy rate is done over the beamforming strategy, Alice can transmit the data signal with full power $p_{S,1} = P_{S,1}$.

The second phase is similar to the SIMO wiretap channel [JM09]. The relay has no further degrees of freedom and depends on the channel realizations of g_E and $\boldsymbol{g}_B$. If the channel $\boldsymbol{g}_B$ to Bob is better than the channel g_E to Eve, the relay maximizes the transmission rate by sending the signal with full power. Otherwise, the achievable secrecy rate is zero and the relay should not transmit any signal. This would imply, that the relay either needs to buffer the signal until an advantageous channel realization appears or the signal is discarded. For our system model, we assume that the relay has no buffer and is operating in a simple way, i.e., the relay transmits the data signal regardless of the actual channel realizations. Therefore, the relay transmits the signal with full power, i.e., $p_R = P_R$.

High-SNR Analysis

For this transmission scheme, the high-SNR slope, defined in Definition (5.1), is given by

$$\mathcal{S}_{\infty}^{\text{Eve}} = 0.$$

10.2 Protection Strategies

Unfortunately, the high-SNR slope of the above transmission scheme in the eavesdropper system is always zero. To overcome this disadvantage, we need additional mechanisms to protect the communication in the second phase. In the following, we will present two different protection schemes. For both schemes it is advantageous to choose $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$, i.e., ZF in the first phase, so that the signal at Eve is set to zero.

10.2.1 Eavesdropper System with Artificial Noise

In this setting, Alice transmits in the first phase the data symbol with ZF as described before, i.e., $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$. In the second phase, she additionally sends an AN signal. As we have no direct link between the transmitter and the intended receiver, Alice can choose the BV such that

Alice	sends data with $\boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$	sends AN with $\boldsymbol{w}_{\text{MRT}}^{\text{Eve}}$
Relay	receives data	sends amplified data
Bob	–	receives amplified data
Eve	–	receives amplified data + AN
	Phase I	Phase II

Table 10.1: Summary of send and receive operations of all nodes in the two communication phases for the AN protection strategy.

the interference at the eavesdropper is maximized, i.e., $\boldsymbol{w}_{S,2} = \boldsymbol{w}_{\text{MRT}}^{\text{Eve}}$. A summary of all send and receive operations can be found in Table 10.1. The SINR terms are given accordingly as

$$\Gamma_B = \frac{\alpha\rho p_{S,1} \left\|\boldsymbol{g}_B\right\|^2 \left|\boldsymbol{h}_R^{\text{H}} \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}\right|^2}{\alpha \left\|\boldsymbol{g}_B\right\|^2 + 1}, \tag{10.3}$$

$$\Gamma_E = \frac{\alpha\rho p_{S,1} \left|g_E\right|^2 \left|\boldsymbol{h}_R^{\text{H}} \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}\right|^2}{\rho p_{S,2} \left\|\boldsymbol{h}_E\right\|^2 + \alpha \left|g_E\right|^2 + 1} \tag{10.4}$$

with $\alpha = \frac{\rho p_R}{\rho p_{S,1} \left|\boldsymbol{h}_R^{\text{H}} \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}\right|^2 + 1}$.

Power Allocation

The optimal power allocation for Alice is easily determined. As Alice transmits in the first phase with $\boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$ in order to avoid information leakage to the eavesdropper, she maximizes the achievable transmission rate by sending with full power, i.e., $p_{S,1} = P_{S,1}$. In the second phase, Alice transmits an AN signal in order to disturb Eves receive signal. Bobs receive signal is not affected, as there is no direct link between transmitter and receiver available. Therefore, the SINR term Γ_E in Equation (10.4) is minimized and the achievable secrecy rate is maximized if we choose $p_{S,2} = P_{S,2}$.

For the power allocation at the relay, the following maximization problem can be formulated

(10.1) Optimization Problem.
For the two-hop relay channel in Chapter 9, the achievable secrecy rate

$$R_S^{\mathrm{AN}} = \left[C\left(\frac{\alpha\rho P_{S,1} \|\boldsymbol{g}_B\|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}{\alpha\|\boldsymbol{g}_B\|^2+1} \right) - C\left(\frac{\alpha\rho P_{S,1}|g_E|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}{\rho P_{S,2}\|\boldsymbol{h}_E\|^2+\alpha|g_E|^2+1} \right) \right]^+$$
$$\text{with} \quad \alpha = \frac{\rho p_R}{\rho P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 + 1}$$

for the eavesdropper system with AN can be maximized over the power p_R at the relay

$$\max_{0 \le p_R \le P_R} R_S^{\mathrm{AN}}. \qquad \checkmark$$

(10.2) Proposition.
The achievable secrecy rate R_S^{AN} is unimodal in p_R, $0 \le p_R \le P_R$, with a maximum at

$$\tilde{p}_R = \frac{\sqrt{\|\boldsymbol{g}_B\|^2 |g_E|^2 \left(\rho P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 + 1\right) \left(\rho P_{S,2} \|\boldsymbol{h}_E\|^2 + 1\right)}}{\rho \|\boldsymbol{g}_B\|^2 |g_E|^2}.$$

The optimal power allocation p_R^* at the relay solving the Optimization Problem (10.1) is given by

$$p_R^* = \min\left(\tilde{p}_R, P_R\right). \qquad \checkmark$$

The proof is given in Appendix C.1.

High-SNR Analysis

Due to the different possible power allocations, we need to distinguish two cases for the calculation of the high-SNR slope and the high-SNR power offset.

First case $p_R^* = \tilde{p}_R$
For this case, the relay can use the optimal transmit power $\tilde{p}_R$ in order to forward the signal, and the high-SNR slope is calculated to

$$\mathcal{S}_\infty^{\mathrm{AN}} = 1.$$

Further, the high-SNR power offset is given by

$$\mathcal{L}_\infty^{\mathrm{AN}}(\tilde{p}_R) = \log_2 \left(\frac{1}{P_{S,1} \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2} + \frac{p_R \left| g_E \right|^2}{P_{S,2} \left\| \boldsymbol{h}_E \right\|^2} \cdot \frac{1}{p_R \left\| \boldsymbol{g}_B \right\|^2} + \frac{2 \left| g_E \right|^2}{\sqrt{P_{S,1} P_{S,2} \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2 \left\| \boldsymbol{g}_B \right\|^2 \left\| \boldsymbol{h}_E \right\|^2 \left| g_E \right|^2}} \right). \quad (10.5)$$

Second case $p_R^* = P_R$
If the power at the relay is limited by the power constraint P_R, the high-SNR slope is also calculated to

$$\mathcal{S}_\infty^{\mathrm{AN}} = 1,$$

while the high-SNR power offset is given by

$$\mathcal{L}_\infty^{\mathrm{AN}}(P_R) = \log_2 \left(\frac{1}{P_{S,1} \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2} + \frac{1}{P_R \left\| \boldsymbol{g}_B \right\|^2} + \frac{P_R \left| g_E \right|^2}{P_{S,2} \left\| \boldsymbol{h}_E \right\|^2} \left(\frac{1}{P_{S,1} \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2} + \frac{1}{P_R \left\| \boldsymbol{g}_B \right\|^2} \right) \right). \quad (10.6)$$

10.2.2 Eavesdropper System with Information Leakage Neutralization

For this transmission scheme, Alice chooses ZF as beamforming strategy in the first phase, in order to prevent Eve from eavesdropping. In the

Alice	sends data with $\boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$	sends IN with $\boldsymbol{w}_{\text{MRT}}^{\text{Eve}}$
Relay	receives data	sends amplified data
Bob	–	receives amplified data
Eve	–	–
	Phase I	Phase II

Table 10.2: Summary of send and receive operations of all nodes in the two communication phases for the IN protection strategy.

second phase, she sends the IN signal as introduced in Section 4.2, i.e.,

$$x_n = -\frac{\sqrt{\alpha} g_E \boldsymbol{h}_R^{\text{H}} \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}}{\boldsymbol{h}_E^{\text{H}} \boldsymbol{w}_{S,2}} x.$$

Alice chooses the transmit beamforming vector in this phase such that the protection by the neutralization signal at Eve is maximized, i.e., $\boldsymbol{w}_{S,2} = \boldsymbol{w}_{\text{MRT}}^{\text{Eve}}$. Again, a summary of the send and receive operations at all nodes can be found in Table 10.2.

The secrecy rate is then given by

$$R_S^{\text{IN}} = C\left(\frac{\alpha \rho p_{S,1} \left\|\boldsymbol{g}_B\right\|^2 \left|\boldsymbol{h}_R^{\text{H}} \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}\right|^2}{\alpha \left\|\boldsymbol{g}_B\right\|^2 + 1}\right), \tag{10.7}$$

where $\alpha = \frac{\rho p_R}{\rho p_{S,1} \left|\boldsymbol{h}_R^{\text{H}} \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}\right|^2 + 1}$.

Power Allocation

Unfortunately, this scheme depends on the power usage at the relay and/or on the power constraint at the transmitter. In the following, we derive an adaptive power constraint for Alice. Alternatively, we can optimize the power allocation at the relay.

Adaptation of the Power Constraint at Alice
We assume that the relay transmits with full power P_R. In order to successfully neutralize the forwarded signal at the eavesdropper, the transmit power at Alice has to fulfill the IN power constraint according to Definition (4.2), which we rewrite to

$$\mathrm{E}_x\left[|x_n|^2\right] = p_{S,1}p_{S,2} + \frac{p_{S,2}}{\rho\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2} - \frac{p_{S,1}P_R\left|g_E\right|^2}{\left\|\boldsymbol{h}_E\right\|^2} \geq 0.$$

We assume individual power constraints in the first and second phase and set, without loss of generality, $p_{S,1} = p_{S,2} = p_S$, where $0 \leq p_S \leq P_S$ and $P_S = P_{S,1} = P_{S,2}$. Therefore, the inequality can be written as

$$p_S^2 + p_S\left(\frac{1}{\rho\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2} - \frac{P_R\left|g_E\right|^2}{\left\|\boldsymbol{h}_E\right\|^2}\right) \geq 0.$$

The power constraint per phase at Alice has to be at least

$$P_S^* \geq \begin{cases} \frac{P_R|g_E|^2}{\|\boldsymbol{h}_E\|^2} - \frac{1}{\rho\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2} & \text{if} \quad \|\boldsymbol{h}_E\|^2 \leq \rho P_R\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2|g_E|^2 \\ 0 & \text{otherwise} \end{cases}$$

in order to successfully cancel the receive signal from the relay at the eavesdropper Eve.

This result implies that there are cases where Alice needs much more power than she has available to successfully eliminate this signal at Eve. As this is not realistic in general, we optimize the power allocation at the relay instead.

Optimal Power Allocation at the Relay
If we permit the relay to transmit not only with full power, but also with a fraction of the maximal available power P_R, i.e., $0 \leq p_R \leq P_R$, the power constraint for the IN can be met, while Alice transmits with full power in both phases.

(10.3) Optimization Problem.
For the two-hop relay channel in Chapter 9, the achievable secrecy rate R_S^{IN} for the eavesdropper system with IN in Equation (10.7) can be

maximized over the transmit power p_R at the relay with subject to the IN power constraint given in Definition (4.2)

$$\max_{0\leq p_R\leq P_R} \quad \frac{\rho p_R P_{S,1} \|\boldsymbol{g}_B\|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}{p_R \|\boldsymbol{g}_B\|^2 + \left(P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 + \frac{1}{\rho}\right)}$$

$$\text{s.t.} \quad \frac{\rho p_R P_{S,1} |g_E|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}{\left(\rho P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 + 1\right) \|\boldsymbol{h}_E\|^2} \leq P_{S,2}. \qquad (10.8)$$ ✓

We can reformulate the IN power constraint to

$$p_R \leq \frac{P_{S,2} \|\boldsymbol{h}_E\|^2}{|g_E|^2} \left(1 + \frac{1}{\rho P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}\right).$$

In the following, let us denote the IN power constraint with

$$p_R^{\mathrm{IN}} := \frac{P_{S,2} \|\boldsymbol{h}_E\|^2}{|g_E|^2} \left(1 + \frac{1}{\rho P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}\right).$$

(10.4) Corollary.
The optimal power allocation p_R^* at the relay solving the Optimization Problem (10.3) is given by

$$p_R^* = \min\left(p_R^{\mathrm{IN}}, P_R\right). \qquad \checkmark$$

Corollary (10.4) follows directly from the power constraint at the relay and the IN power constraint formulated in Definition (4.2).

High-SNR Analysis

Because of the two possible power allocations, we have to distinguish two different cases for the calculation of the high-SNR slope and the high-SNR power offset.

First case $p_R^* = p_R^{\mathrm{IN}}$
For this case the transmit power at the relay is bounded by the IN power constraint and the secrecy rate is given by

$$R_S^{\mathrm{IN}}(p_R^{\mathrm{IN}}) = C\left(\rho \frac{P_{S,1}P_{S,2}\left\|\boldsymbol{h}_E\right\|^2 \left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 \left\|\boldsymbol{g}_B\right\|^2}{P_{S,2}\left\|\boldsymbol{h}_E\right\|^2 \left\|\boldsymbol{g}_B\right\|^2 + P_{S,1}\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 \left|g_E\right|^2}\right).$$

The high-SNR slope in Definition (5.1) for $R_S^{\mathrm{IN}}(p_R^{\mathrm{IN}})$ is given by

$$\mathcal{S}_\infty^{\mathrm{IN}}(p_R^{\mathrm{IN}}) = 1$$

and the high-SNR power offset in Definition (5.2) can be calculated to

$$\mathcal{L}_\infty^{\mathrm{IN}}(p_R^{\mathrm{IN}}) = \log_2\left(\frac{1}{P_{S,1}\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2} + \frac{p_R\left|g_E\right|^2}{P_{S,2}\left\|\boldsymbol{h}_E\right\|^2} \cdot \frac{1}{p_R\left\|\boldsymbol{g}_B\right\|^2}\right). \quad (10.9)$$

Second case $p_R^* = P_R$
If the power at the relay is limited by the power constraint P_R, the secrecy rate is given by

$$R_S^{\mathrm{IN}}(P_R) = C\left(\rho \frac{P_R P_{S,1}\left\|\boldsymbol{g}_B\right\|^2 \left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}{P_R\left\|\boldsymbol{g}_B\right\|^2 + P_{S,1}\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 + \frac{1}{\rho}}\right).$$

Once again, the high-SNR slope is calculated to

$$\mathcal{S}_\infty^{\mathrm{IN}}(P_R) = 1$$

and the high-SNR power offset is given by

$$\mathcal{L}_\infty^{\mathrm{IN}}(P_R) = \log_2\left(\frac{1}{P_{S,1}\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2} + \frac{1}{P_R\left\|\boldsymbol{g}_B\right\|^2}\right). \quad (10.10)$$

10.3 Comparison of High-SNR Power Offsets

Let us now take a closer look on the three schemes, where the high-SNR slope equals one, i.e., the peaceful system, the eavesdropper system with AN and the eavesdropper system with IN, and compare the high-SNR power offset expressions.

Comparing the expression for the peaceful system in Equation (10.2) and the one for the eavesdropper system with IN when the system is limited by the transmit power constraint at the relay in Equation (10.10), we find, that they only differ in the first term. In the peaceful system the transmitter uses MRT to send the data signal to the relay, while in the IN protected system the transmitter has to use ZF, which results in the power offset difference.

Similar observations can be made, if we compare the expressions of the eavesdropper system with AN limited by the transmit power constraint P_R in Equation (10.6) with those of the peaceful system in Equation (10.2). Again, the first term only differs in the transmission strategy at Alice, while the second term is identical. However, the AN protected scheme has in addition the same terms scaled by the ratio ${P_R|g_E|^2}/{P_{S,2}\|\boldsymbol{h}_E\|^2}$, which is the power forwarded by the relay in direction of Eve divided by the jamming power at Alice in direction of Eve.

This ratio is again visible, if we have a look at the eavesdropper system with AN with optimal transmit power allocation $\tilde{p}_R$ in Equation (10.5) and for the eavesdropper system with IN limited by the IN power constraint p_R^{IN} in Equation (10.9).

The observations for the IN scheme are expressed analytically in the following corollary.

(10.5) Corollary.
The difference in the high-SNR power offset between the peaceful system and the eavesdropper system with IN is given by

$$\begin{aligned}\Delta\mathcal{L}_\infty(P_R) &= \mathcal{L}_\infty^{\text{P}} - \mathcal{L}_\infty^{\text{IN}}(P_R) \\ &= \log_2\left(\frac{\left(P_R\left\|\boldsymbol{g}_B\right\|^2 + P_{S,1}\left\|\boldsymbol{h}_R\right\|^2\right)\left|\boldsymbol{h}_R^{\text{H}}\boldsymbol{w}_{\text{ZF}}^{\text{Eve}}\right|^2}{\left(P_R\left\|\boldsymbol{g}_B\right\|^2 + P_{S,1}\left|\boldsymbol{h}_R^{\text{H}}\boldsymbol{w}_{\text{ZF}}^{\text{Eve}}\right|^2\right)\left\|\boldsymbol{h}_R\right\|^2}\right)\end{aligned}$$

if the transmit power at the relay is limited by the transmit power constraint P_R or

$$\begin{aligned}\Delta\mathcal{L}_\infty(p_R^{\mathrm{IN}}) &= \mathcal{L}_\infty^{\mathrm{P}} - \mathcal{L}_\infty^{\mathrm{IN}}(p_R^{\mathrm{IN}}) \\ &= \log_2\left(\frac{\left(P_{S,1}\left\|\boldsymbol{h}_R\right\|^2 + P_R\left\|\boldsymbol{g}_B\right\|^2\right) P_{S,2}\left\|\boldsymbol{h}_E\right\|^2 \left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}{\left(P_{S,1}\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 |g_E|^2 + P_{S,2}\left\|\boldsymbol{g}_B\right\|^2\left\|\boldsymbol{h}_E\right\|^2\right) P_R\left\|\boldsymbol{h}_R\right\|^2}\right)\end{aligned}$$

if the transmit power is limited by the IN power constraint p_R^{IN}. ✓

(10.6) Remark.
In the case where the transmit power at the relay is limited by the transmit power constraint P_R, the high-SNR power offset difference gets zero, i.e., $\Delta\mathcal{L}_\infty(P_R) = 0$, if and only if $\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} = \boldsymbol{w}_{\mathrm{MRT}}$, i.e., the channels $\boldsymbol{h}_R$ and $\boldsymbol{h}_E$ are orthogonal. ✓

Furthermore, the protection scheme with AN depends on the channel realizations and the SNR, as can be seen from following proposition.

(10.7) Proposition.
For the eavesdropper system with AN, the achievable secrecy rate R_S^{AN} becomes positive if

$$\rho > \left[\frac{|g_E|^2 - \left\|\boldsymbol{g}_B\right\|^2}{P_{S,2}\left\|\boldsymbol{g}_B\right\|^2\left\|\boldsymbol{h}_E\right\|^2}\right]^+. \qquad ✓$$

The proof is given in Appendix C.2.

11 Partial Channel State Information

The previously met assumption of full CSI on all channels at the transmitter Alice is very unrealistic. In this chapter, we assume, that the relay feeds the channel estimation of the channel g_E back to Alice, which results in an outdated CSI of g_E at Alice as specified in Definition (9.1). We examine applicable beamforming and protection strategies and investigate the optimal power allocation of these schemes during the two transmit phases at the transmitter and the relay. Further, we will note that only the IN scheme is affected by this partial channel knowledge.

Within this chapter, we present results that were partially published in [EHJ13].

11.1 Beamforming Strategies

Again, we first analyze the pure beamforming strategies without any protection mechanisms during the second transmission phase. The focus of the analysis will be mainly on the power allocation.

11.1.1 Peaceful System

The scenario of the peaceful system with partial CSI is identical to the scenario with full CSI. This is due to the fact that the channel g_E between the relay and the eavesdropper, which is considered as not perfectly known, is not present in this scenario. Therefore, the same results as in Section 10.1.1 apply.

11.1.2 Eavesdropper System

Similarly, the eavesdropper system with full and partial CSI give identical beamforming strategies at Alice. This is due to the fact that Alice has no possibility to influence the receive signal at Eve during the second

phase. Therefore, she will apply the same beamforming strategy as discussed in Section 10.1.2.

11.2 Protection Strategies

The fact that we have only partial CSI has significant influence if we analyze the protection strategies during the second phase. Again, we assume that Alice performs ZF during the first transmission phase, i.e., $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\text{ZF}}^{\text{Eve}}$, so that no information leaks to the eavesdropper during this phase. Further, she uses MRT during the second phase, i.e., $\boldsymbol{w}_{S,2} = \boldsymbol{w}_{\text{MRT}}^{\text{Eve}}$, in order to maximize the effect of the protection strategy.

11.2.1 Eavesdropper System with Artificial Noise

For the system model in Chapter 9, we assume that the relay feeds the CSI of the channel g_E to the eavesdropper back to Alice. This does not only imply that Alice has only an outdated CSI, but also that the relay knows the current CSI on this channel.

For the transmitter, it is unimportant to know the actual CSI in order to jam Eve. Therefore, the power allocation at Alice is identical to the case of full CSI in Section 10.2.1. As the relay knows the actual channel state, the Optimization Problem (10.1) is still valid and we also get the same power allocation at the relay as before in Section 10.2.1.

11.2.2 Eavesdropper System with Information Leakage Neutralization

For the eavesdropper system with IN, Alice needs to know the CSI of the channel g_E between relay and Eve perfectly in order to eliminate the receive signal at the eavesdropper completely.

For the case, where Alice only has partial CSI, e.g., outdated information on the channel g_E, we can analyze the performance impact. In order to

examine this performance impact of IN due to the partial CSI, we define the information leakage power of the desired eavesdropping signal,

$$L(x_n) = \left| \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{\mathrm{MRT}}^{\mathrm{Eve}} x_n + \sqrt{\alpha} g_E \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x \right|^2,$$

where $\alpha = \frac{\rho p_R}{\rho p_{S,1} \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2 + 1}$.

Given only an estimate $\hat{g}_E$ of the channel g_E at Alice, we show in the following that the worst case[1] information leakage power is minimized by sending the information again, i.e., x_n is a function of x, and treating the imperfectly known channel $\hat{g}_E$ as if it is known perfectly.

(11.1) Proposition.
The optimal IN transmit signal x_n with regard to the minimized leakage power $L(x_n)$ and the worst case channel estimation error $|\Delta g_E|^2$ is given by

$$\arg\min_{x_n} \max_{|\Delta g_E|^2 \leq \epsilon} L(x_n) = -\frac{\sqrt{\alpha} \hat{g}_E \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}}{\boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{\mathrm{MRT}}^{\mathrm{Eve}}} x.$$

✓

The proof is given in Appendix D.1.

From Proposition (11.1) and the BVs in Definition (9.2), the worst case receive signal at Eve in the second phase can be calculated to

$$\begin{aligned} y_{E,2} &= \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{\mathrm{MRT}}^{\mathrm{Eve}} x_n + \sqrt{\alpha} g_E (\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x + n_R) + n_{E,2} \\ &= \sqrt{\alpha} \Delta g_E \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x + \Delta g_E \left(\hat{g}_E - \sqrt{\epsilon} \right) n_R + n_{E,2} \end{aligned}$$

and the corresponding worst case SINR is therefore given by

$$\max_{|\Delta g_E|^2 \leq \epsilon} \Gamma_E = \frac{\alpha \rho p_{S,1} \epsilon \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2}{\alpha \left(|\hat{g}_E| - \sqrt{\epsilon} \right)^2 + 1}.$$

An achievable secrecy rate for the two-hop wiretap channel with partial CSI is given by

$$R_S^{\mathrm{IN}} = C \left(\frac{\alpha \rho p_{S,1} \left\| \boldsymbol{g}_B \right\|^2 \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2}{\alpha \left\| \boldsymbol{g}_B \right\|^2 + 1} \right) - C \left(\frac{\alpha \rho p_{S,1} \epsilon \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2}{\alpha \left(|\hat{g}_E| - \sqrt{\epsilon} \right)^2 + 1} \right).$$

[1] Please note that the worst case is always from Alice' point of view. This means that for Eve it is the best case.

(11.2) Remark.
In order to achieve this secrecy rate, a wiretap code is needed again, as we cannot prevent information leakage completely due to the partial channel knowledge of g_E at Alice. ✓

11.2.3 Optimization Problem

We are interested in the optimal power allocations at the transmitter and the relay. Due to the fact that Alice performs ZF with respect to Eve during the first phase, she will always transmit with full power $p_{S,1} = P_{S,1}$ in order to maximize the receive signal at the relay. Therefore, it remains to optimize the power allocations for the second phase at the relay and the transmitter which maximize the secrecy rate R_S^{IN}.

From Equation (9.4) and Definition (4.2), the IN power constraint at the relay is

$$p_R \leq \frac{p_{S,2} \left\|\boldsymbol{h}_E\right\|^2 \left(\rho P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 + 1\right)}{\rho P_{S,1} \left|\hat{g}_E\right|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}. \tag{11.1}$$

(11.3) Remark.
Note that $p_{S,2}$ correlates with p_R as the power values must be chosen jointly such that the leakage signals from source and relay add to zero.✓

(11.4) Optimization Problem.
For the two-hop relay channel with partial CSI, the achievable secrecy rate R_S^{IN} for the eavesdropper channel with IN can be maximized over the power p_R at the relay

$$\begin{aligned} &\max_{p_R} R_S^{\mathrm{IN}} \\ &\text{s.t.} \quad p_R \leq \frac{P_{S,2} \left\|\boldsymbol{h}_E\right\|^2 \left(\rho P_{S,1} \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2 + 1\right)}{\rho P_{S,1} \left|\hat{g}_E\right|^2 \left|\boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}, \\ &\qquad 0 \leq p_R \leq P_R. \end{aligned}$$

✓

11.2.4 Analysis of Monotony of the Secrecy Rate

For convenience of notation, let us denote the effective received SNR at the relay as

$$\tilde{\rho} = \rho P_{S,1} \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2 \tag{11.2}$$

and define the worst case channel gain as

$$|\tilde{g}_E|^2 = \left(|\hat{g}_E| - \sqrt{\epsilon} \right)^2 .$$

(11.5) Proposition.
The optimal power allocation p_R^* at the relay solving the Optimization Problem (11.4) is given in Table 11.1, where

$$\begin{aligned}
p_R^{\max} &= \frac{P_{S,2}\|\boldsymbol{h}_E\|^2}{|\hat{g}_E|^2} \left(1 + \frac{1}{\tilde{\rho}}\right), \\
\tilde{p}_R &= \frac{(1+\tilde{\rho}) \left(\sqrt{\epsilon \|\boldsymbol{g}_B\|^2 \left(\tilde{\rho}\left(\|\boldsymbol{g}_B\|^2 - \epsilon\right) + s\right)} s + \|\boldsymbol{g}_B\|^2 \left(|\tilde{g}_E|^2 - \epsilon\right) \right)}{\rho \|\boldsymbol{g}_B\|^2 \left(\epsilon \tilde{\rho} s + \epsilon \|\boldsymbol{g}_B\|^2 - |\tilde{g}_E|^4\right)}, \\
p_R^0 &= \frac{(\tilde{\rho}+1)\left(\|\boldsymbol{g}_B\|^2 - \epsilon\right)}{\rho \|\boldsymbol{g}_B\|^2 \left(\epsilon - |\tilde{g}_E|^2\right)}, \text{ and} \\
s &= \|\boldsymbol{g}_B\|^2 - |\tilde{g}_E|^2 .
\end{aligned}$$

✓

The corresponding optimal power allocation $p_{S,2}^*$ is given by

$$p_{S,2}^* = \frac{p_R^* \tilde{\rho} \, |\hat{g}_E|^2}{\|\boldsymbol{h}_E\|^2 (\tilde{\rho} + 1)}.$$

The proof is given in Appendix D.2.

From Table 11.1, there are only four different outcomes of the power allocation p_R^* depending on the behavior of the secrecy rate R_S^{IN}.

As long as the channel gain $\|\boldsymbol{g}_B\|^2$ to the intended receiver is greater than the uncertainty over the channel $|g_E|^2$, i.e., the estimation error ϵ (case i) to iii)), the secrecy rate is positive at certain values of p_R. In particular, in the case where R_S^{IN} is quasi-concave (case ii b) and iii)), the secrecy rate starts positive for $p_R = 0$ and becomes negative for large values of p_R. If the secrecy rate is monotonic increasing in p_R (case i) and ii a)), the optimal power allocation is either bounded by the power constraint P_R

Case	Behavior of R_S^{IN} with regard to p_R	Optimal power allocation p_R^*
i) $\lvert\tilde{g}_E\rvert^2 > \lVert\boldsymbol{g}_B\rVert^2 > \epsilon$	monotonic increasing	$p_R^* = \min\left(p_R^{\max}, P_R\right)$
ii) $\lVert\boldsymbol{g}_B\rVert^2 > \lvert\tilde{g}_E\rvert^2 > \epsilon$		
a) $\left(\lvert\tilde{g}_E\rvert^4 + \lvert\tilde{g}_E\rvert^2 \epsilon\tilde{\rho}\right)$ $> \epsilon \lVert\boldsymbol{g}_B\rVert^2 (1+\tilde{\rho})$	monotonic increasing	$p_R^* = \min\left(p_R^{\max}, P_R\right)$
b) $\left(\lvert\tilde{g}_E\rvert^4 + \lvert\tilde{g}_E\rvert^2 \epsilon\tilde{\rho}\right)$ $< \epsilon \lVert\boldsymbol{g}_B\rVert^2 (1+\tilde{\rho})$	quasi-concave	$p_R^* = \min\left(\tilde{p}_R, p_R^{\max}, P_R\right)$
iii) $\lVert\boldsymbol{g}_B\rVert^2 > \epsilon > \lvert\tilde{g}_E\rvert^2$	quasi-concave	$p_R^* = \min\left(\tilde{p}_R, p_R^{\max}, P_R\right)$
iv) $\lvert\tilde{g}_E\rvert^2 > \epsilon > \lVert\boldsymbol{g}_B\rVert^2$	quasi-convex	$p_R^* = \begin{cases} p_R^{\max} & \text{if } p_R^0 < p_R^{\max} < P_R \\ P_R & \text{if } p_R^0 < P_R \leq p_R^{\max} \\ 0 & \text{otherwise} \end{cases}$
v) $\epsilon > \lvert\tilde{g}_E\rvert^2 > \lVert\boldsymbol{g}_B\rVert^2$	rate not positive	$p_R^* = 0$
vi) $\epsilon \geq \lVert\boldsymbol{g}_B\rVert^2 \geq \lvert\tilde{g}_E\rvert^2$	rate not positive	$p_R^* = 0$

Table 11.1: The behavior of the secrecy rate R_S^{IN} with regard to p_R and the optimal power allocation p_R^*.

at the relay or by the power constraint $P_{S,2}$ at the transmitter, i.e., $p_R^{\max}$ is optimal.

As soon as the estimation error ϵ becomes greater than the worst case channel gain $\lvert\tilde{g}_E\rvert^2$, i.e., the uncertainty about the channel from the relay to the eavesdropper is greater than the noise Eve will get in the worst case scenario (from Alice' point of view), the secrecy rate becomes decreasing with growing p_R. As $\lVert\boldsymbol{g}_B\rVert^2$ is still greater than ϵ, the secrecy rate is quasi-concave and has a maximum at the optimal power allocation $\tilde{p}_R$ (case ii b) and iii)).

For the case where the worst case estimation error ϵ is greater than the channel gain $\lVert\boldsymbol{g}_B\rVert^2$ (case iv)), the secrecy rate R_S^{IN} is zero if only a small amount of power is allocated. As soon as we allocate more power than p_R^0, the secrecy rate becomes monotonic increasing as long as the worst case channel gain $\lvert\tilde{g}_E\rvert^2$ to Eve is greater than the estimation error and the channel to Bob. Therefore, the optimal power allocation is again either bounded by the power constraint P_R at the relay or by the power

constraint $P_{S,2}$ at the transmitter, as long as these power constraints are greater than p_R^0. Otherwise, the secrecy rate is zero and no power should be allocated.

Finally, if the estimation error ϵ is greater than the channel $\|\boldsymbol{g}_B\|^2$ to the intended receiver Bob and the worst case channel gain $|\tilde{g}_E|^2$ to the eavesdropper (case v) and vi)), the secrecy rate is always zero and therefore no power should be allocated at the relay and the transmitter. This corresponds to the case where the transmitter has almost no or has no CSI about the channel from the relay to the eavesdropper. Therefore, Alice is not able to compute any IN signal in order to null out the information leaked to Eve. In these two cases, Alice should use AN in order to protect the second phase.

(11.6) Proposition.
As the SNR goes to infinity, the secrecy rate R_S^{IN} with partial CSI approaches

$$\lim_{\rho\to\infty} R_S^{\mathrm{IN}} = \log_2\left(\frac{p_R|\tilde{g}_E|^2\|\boldsymbol{g}_B\|^2+p_{S,1}\|\boldsymbol{g}_B\|^2\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}{p_R\epsilon\|\boldsymbol{g}_B\|^2+p_{S,1}\epsilon\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2}\right).$$

✓

Proposition (11.6) follows from direct calculations.

12 Illustrations

For the simulations, we used a geometric channel model with a path loss coefficient of $a = 2$. As depicted in Figure 12.1, the nodes were placed on a 20 by 20 grid with the following positions:

Alice:	[04 10]	Bob:	[16 10]
Relay:	[10 12]	Eve:	[10 07]

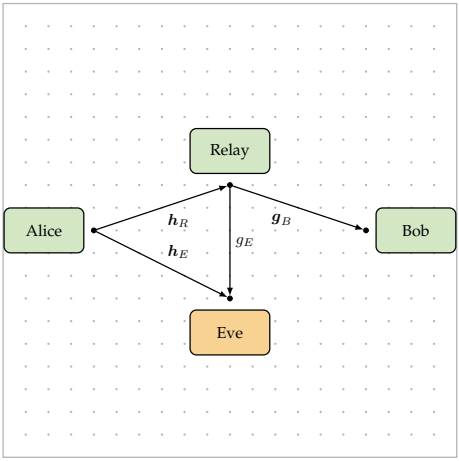


Figure 12.1: Positions of transmitter Alice, relay, eavesdropper Eve and legitimated receiver Bob on a 20 by 20 grid.

The channels were generated randomly and weighted by the distances between the nodes. The transmitter was equipped with four antennas, while the receiver had only two antennas. The power constraints at the transmitter and the relay were set to $P_{S,1} = P_{S,2} = P_R = 10$ dB.

In the case of IN with full CSI, the power at the relay was adapted according to Corollary (10.4), while for the AN case, the power allocation in Proposition (10.2) was used.

For the IN scheme with partial CSI, the maximum estimation error ϵ over the channel g_E is calculated to $\epsilon = {}^{1}/_{\mathrm{SNR}^2} + \delta$, where δ is a constant which represents the delay caused by the need of feeding back the CSI from the relay to the receiver. The corresponding simulations represent the power allocation presented in Proposition (11.5).

For the simulations, two channel realizations were specifically chosen as examples.

(12.1) Example.
Channel realization, with a weak link between the relay and the eavesdropper:

$$|\boldsymbol{h}_R|^2 = \begin{bmatrix} 0.000372 \\ 0.000039 \\ 0.000172 \\ 0.000720 \end{bmatrix}, \; |\boldsymbol{h}_E|^2 = \begin{bmatrix} 0.000642 \\ 0.000304 \\ 0.002434 \\ 0.000327 \end{bmatrix},$$

$$|\boldsymbol{g}_B|^2 = \begin{bmatrix} 0.000656 \\ 0.000649 \end{bmatrix}, \text{ and } |g_E|^2 = 0.000855.$$

(12.2) Example.
Channel realization, where the channel gain of the link between the relay and the eavesdropper is advantageous:

$$|\boldsymbol{h}_R|^2 = \begin{bmatrix} 0.002616 \\ 0.000547 \\ 0.000730 \\ 0.002477 \end{bmatrix}, \; |\boldsymbol{h}_E|^2 = \begin{bmatrix} 0.000437 \\ 0.000405 \\ 0.000566 \\ 0.000234 \end{bmatrix},$$

$$|\boldsymbol{g}_B|^2 = \begin{bmatrix} 0.000180 \\ 0.000037 \end{bmatrix}, \text{ and } |g_E|^2 = 0.007324.$$

Figures 12.2 and 12.3 show the instantaneous channel capacity for the peaceful system according to Equation (10.1) denoted by R_P and the achievable instantaneous secrecy rate of the two protection schemes IN, introduced in Section 10.2.2 and labeled as R_S^{IN}, and AN, described in Section 10.2.1 and denoted by R_S^{AN}, where Alice has full CSI on all channels. Additionally, the figures show the achievable instantaneous secrecy rates R_S^{LBF}, R_S^{ZF} and R_S^{MRT}, which are derived by the rate expressions in Section 10.1.2 with beamforming vectors $\boldsymbol{w}_{\mathrm{LBF}}(\tau)$, $\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}$ and $\boldsymbol{w}_{\mathrm{MRT}}$, respectively. In Figure 12.2, we use the channel realizations according

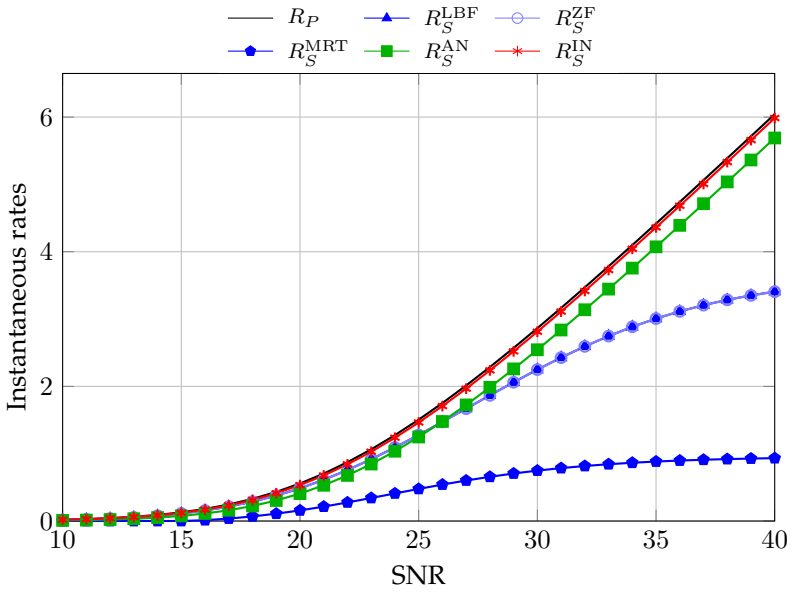


Figure 12.2: Instantaneous capacity for the peaceful system and instantaneous achievable secrecy rates for various beamforming and protection schemes over the SNR with $n_T = 4$, $n_D = 2$, and $P_{S,1} = P_{S,2} = P_R = 10$dB (Example (12.1)).

to Example (12.1). It can be seen, that both protection schemes have the same slope as the peaceful system. Furthermore, the IN protected scheme is almost as good as the peaceful system and better than the AN protected scheme. Due to the missing protection of the data signal in the second phase, the three beamforming schemes perform badly in the high SNR regime. This can be seen even better in Figure 12.3.

For Figure 12.3, the channel realizations of Example (12.2) were used. Due to the worse channel between Alice and Eve, Alice has not enough power to send the IN signal and the power at the relay has to be decreased in order to meet the IN power constraint. This results in a lower transmission rate to Bob and therefore also a lower achievable secrecy rate. For the same reason, the AN scheme performs even worse, as the AN signal disturbs Eve not enough. Furthermore, the AN rate is zero

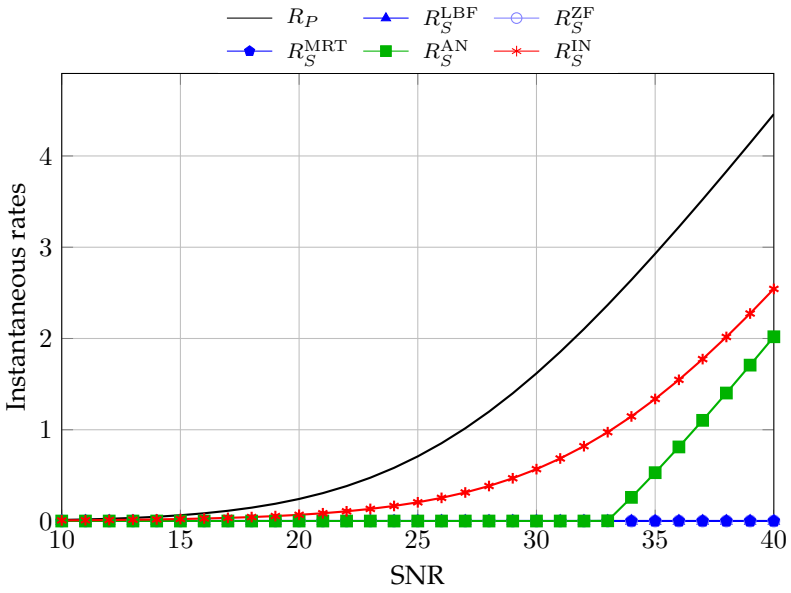


Figure 12.3: Instantaneous capacity for the peaceful system and instantaneous achievable secrecy rates for various beamforming and protection schemes over the SNR with $n_T = 4$, $n_D = 2$, and $P_{S,1} = P_{S,2} = P_R = 10$dB (Example (12.2)).

for $\rho \leq 26.7325$ and gets positive for $\rho > 26.7325$, as stated in Proposition (10.7). For these special channel realizations, all beamforming rates are zero, as the effective channel from Alice over the relay to Eve is better than the effective channel from Alice over the relay to Bob.

Figures 12.4 and 12.5 show how the IN scheme performs for partial CSI at Alice. The achievable instantaneous secrecy rate R_S^{IN} for the IN scheme with partial CSI is compared to several base line systems:

- The channel capacity R_P of the peaceful system without eavesdropper as described in Section 10.1.1,
- The achievable secrecy rate R_S^{LBF} of the eavesdropper system, where Alice only uses an optimized beamformer as presented in Section 10.1.2,

- The achievable secrecy rate R_S^{AN} of the AN protected scheme described in Section 10.2.1, and
- The IN protected secrecy rate R_S^{IN} with full CSI as presented in Section 10.2.2.

Note, that the IN protection scheme is the only scheme that is influenced by the partial CSI on the channel g_E, as discussed in the previous chapter.

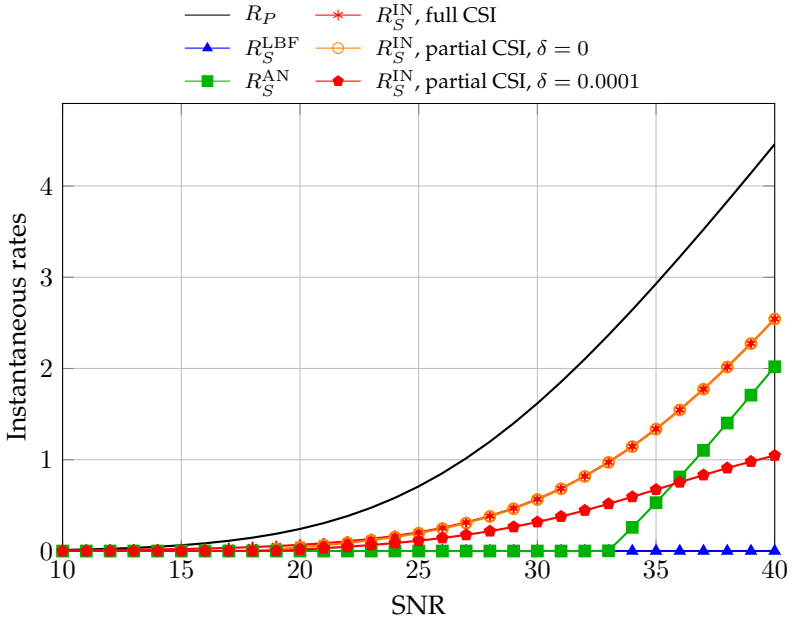


Figure 12.4: Instantaneous capacity for the peaceful system and instantaneous achievable secrecy rates for various protection schemes over the SNR with $n_T = 4$, $n_D = 2$, $P_{S,1} = P_{S,2} = P_R = 10$dB and varying delay δ (Example (12.2)).

The instantaneous rates in Figure 12.4 are achievable with the channel realizations of Example (12.2). For the secrecy rate R_S^{IN} for partial CSI in Figure 12.4, where the delay δ equals zero, the transmitter has instantly the channel estimation over the channel g_E. Although this scenario is quite unrealistic, we can see clearly, that the IN schemes for full and

partial CSI perform identically well. If the delay is greater than zero, e.g., $\delta = 0.0001$, the IN scheme for partial CSI is performing worse than the IN scheme for full CSI in the high SNR regime. This is due to the fact that with outdated CSI the system gets limited in the high SNR regime as stated in Proposition (11.6). For the chosen channel realizations, the IN schemes outperform the AN scheme. Especially in the mid SNR range, the AN scheme still achieves zero secrecy rates, while the IN schemes achieve positive rates. Due to the missing protection of the data signal in the second phase, the beamforming scheme is zero.

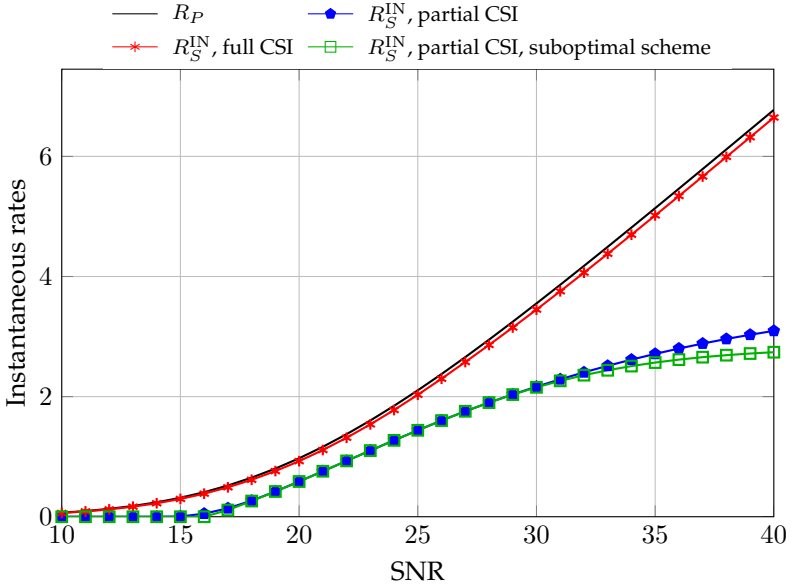


Figure 12.5: Instantaneous achievable secrecy rates over SNR for IN protected schemes with full and partial CSI ($\delta = 0.0001$), $n_T = 4$, $n_D = 2$, $P_{S,1} = P_{S,2} = 10$dB and $P_R = 50$dB (Example (12.1)).

If we apply a simplified power allocation algorithm, where the power at the relay and the transmitter in the second phase are either bounded by the power constraint $P_{S,2}$ or by the power constraint P_R, we achieve a suboptimal secrecy rate R_S^{IN}. Figure 12.5 shows for $\delta = 0.0001$ and

$P_R = 50$dB how this suboptimal scheme performs compared to the optimal IN schemes for full and partial CSI. For the mid SNR range the achievable rates of the optimal and the suboptimal scheme for partial CSI are identical , while in the high SNR regime the gap is growing. For most channel realizations, the suboptimal scheme performs as good as the optimal IN scheme, e.g., in cases i) and ii) a) in Table 11.1. Therefore, a simplified power allocation algorithm can be applied, if we accept that for a few channel realizations the achievable secrecy rate is lower than the optimum.

Part IV

Conclusion

13 Conclusion and Open Topics

Conclusion

Within this thesis, we investigated the possibilities of physical layer secrecy for two special system models. In detail, we studied beamforming and protection strategies in the MISO Gaussian WTC and the Gaussian two-hop relay WTC with multiple antennas at transmitter and receiver. In both system models, we examined the influence of partial CSI on the link to the eavesdropper and compared the achievable secrecy rates with the case of full CSI.

We showed for the MISO WTC that in the fast fading scenario the BV can be optimized such that the ergodic secrecy rate is maximized with regard to the degree of channel knowledge. Further it was shown that the ergodic secrecy rate can be significantly increased by usage of AN, if applied in a smart way. This means that the degree of channel knowledge on the link to the eavesdropper influences the portion of power that is spent for AN at the transmitter as well as the direction, in which the AN signal is sent.

In addition, we found that the same beamforming and protection strategies applied to the slow fading scenario also reduces the secrecy outage probability. Besides, a simplified, however suboptimal beamforming scheme, where the BV can be given in closed form, was established.

For the two-hop relay WTC, we introduced Information Leakage Neutralization (IN) as a new protection strategy. If applied to a system model, where the transmitter has full CSI, the instantaneous secrecy rate performs almost as well as the instantaneous capacity of the peaceful system without an eavesdropper. The gap between both rates results from the fact, that for the peaceful system the transmitter can use MRT, which maximizes the rate, while in the IN protected system the transmitter needs to send with ZF in order to prevent information leakage during the first transmission phase. In any case, the IN protected scheme outperforms the AN protected approach and performs much better than

any beamforming scheme without additional protection mechanism. Another positive aspect of the IN protected scheme in the case of full CSI is that conventional channel codes can be applied instead of wiretap codes.

For the case of partial CSI, where the transmitter has only an outdated estimate on the channel between relay and the eavesdropper, we could show that the IN protected scheme can also be applied. The optimal joint power allocation at the transmitter and the relay could be determined in order to maximize the achievable instantaneous secrecy rate. Here, it strongly depends on the channel realizations and the delay of the estimate, whether the IN or the AN protection scheme should be applied.

Open Topics

The MISO WTC is quite well investigated nowadays. There are only few open topics available for this scenario. One open question is whether it is optimal to send the AN signal only into the null space of the intended receiver or if it is better to accept some interference at the receiver in order to achieve a higher disturbance at the eavesdropper. The results in [Lin+13] indicate that a generalized AN signal, which is not restricted to the null space of the intended receiver, achieves higher ergodic secrecy rates. The influence of this generalized AN signal if applied to the protection scheme presented in II still has to be analyzed.

More open topics are available if we focus on the two-hop relay WTC. A precise characterization, whether the AN or the IN protection scheme is preferable for certain channel conditions, is still open. Moreover, the analysis in Part III considers only achievable instantaneous secrecy rates. A measure like the secrecy outage probability would give a much better understanding, how much information is leaked to the eavesdropper if the link between relay and the eavesdropper is not perfectly known at the transmitter. Additionally, other links like the direct link between sender and eavesdropper may be only partially known. Whether the IN protection scheme can be applied in this case needs to be investigated.

Part V

Appendix

A Proof for the MISO WTC under Fast Fading

Monotony of the Ergodic Secrecy Rate

(A.1) Lemma (Monotony of $R_S(a)$ in a).
The function

$$R_S(a\boldsymbol{w}) = \left[\log_2\left(1 + a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2\right) - \mathrm{E}_{\boldsymbol{g}}\left[\log_2(1 + a\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2)\right]\right]^+$$

with $a \geq 0$ is monotonically increasing in a. ✓

Proof.
In order to proof the monotony of $R_S(a\boldsymbol{w})$ in a, we need to distinguish two cases.

First case $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2 \leq \mathrm{E}_{\boldsymbol{g}}\left[|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2\right]$
In this case, $R_S(a\boldsymbol{w})$ is always zero due to the maximization function.

Second case $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2 > \mathrm{E}_{\boldsymbol{g}}\left[|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2\right]$
Here, $R_S(a\boldsymbol{w})$ gives always positive values. Therefore, we take a look at the first derivative of $R_S(a\boldsymbol{w})$ with respect to a, which is given by

$$\begin{aligned}
a\frac{\partial R_S(a\boldsymbol{w})}{\partial a} &= \frac{1}{\ln 2}\left(\frac{a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1 + a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2} - \mathrm{E}_{\boldsymbol{g}}\left[\frac{a\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1 + a\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}\right]\right) \\
&= \frac{1}{\ln 2}\left(\frac{a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2 + 1 - 1}{1 + a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2} - \mathrm{E}_{\boldsymbol{g}}\left[\frac{a\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2 + 1 - 1}{1 + a\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}\right]\right) \\
&= \frac{1}{\ln 2}\left(1 - \frac{1}{1 + a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2} - \mathrm{E}_{\boldsymbol{g}}\left[1 - \frac{1}{1 + a\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}\right]\right)
\end{aligned}$$

$$= \frac{1}{\ln 2}\left(\mathrm{E}_{\boldsymbol{g}}\left[\frac{1}{1+a\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2}\right] - \frac{1}{1+a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}\right)$$

$$\geq \frac{1}{\ln 2}\left(\frac{1}{1+a\rho\,\mathrm{E}_{\boldsymbol{g}}\left[\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2\right]} - \frac{1}{1+a\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}\right), \qquad \text{(A.1)}$$

where we can multiply the derivative with a without loss of generality as we are only interested in the monotonic behavior of the function. Equation (A.1) follows by Jensen's inequality.

This derivative is always non-negative for $a \geq 0$, $\rho > 0$, and $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2 \geq \mathrm{E}_{\boldsymbol{g}}\left[|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2\right]$.

From the combination of both cases, we conclude that $R_S(a\boldsymbol{w})$ is monotonically increasing in a. □

B Proofs for the MISO WTC under Slow Fading

B.1 Equivalence of the Dual Problem

(B.1) Theorem.
Let $\{F_w\}$ be a family of continuous distribution functions on $\mathbb{R}$ with index set W. Then, the following two optimization problems are equivalent.

1. *For $\epsilon \in [0,1]$ fixed, consider*

$$\max_{w \in W} x \quad s.t. \quad F_w(x) = \epsilon. \tag{B.1}$$

2. *For $x \in \mathbb{R}$ fixed, consider*

$$\min_{w \in W} \epsilon \quad s.t. \quad F_w(x) = \epsilon. \tag{B.2}$$

✓

Proof.
For $\epsilon \in [0,1]$ fixed consider x^* to be the solution of Equation (B.1). Then, there exist two disjoint sets $W' = \{w : F_w(x^*) = \epsilon\}$ and $W'' = \{w : F_w(x^*) \neq \epsilon\}$ with $W = W' \cup W''$. In particular, since F_w is monotonically increasing for all $w \in W$ it holds

$$W'' = \{w : F_w(x^*) > \epsilon\}.$$

Otherwise, x^* would not be the solution of Equation (B.1). Therefore, with $x = x^*$ fixed, ϵ is the solution of Equation (B.2). To proof also the converse, let $x \in \mathbb{R}$ be fixed and consider ϵ^* as the solution of Equation (B.2). Using the same argumentation as for the first case, it can be shown that x is the solution of Equation (B.1) given $\epsilon = \epsilon^*$. □

B.2 Monotony of the Secrecy Rate

(B.2) Lemma (Monotony of $R_S(a)$ in a).
For fixed $\boldsymbol{g}$, the function

$$R_S(a\boldsymbol{w}) = \left[\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2 a^2}{1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2 a^2}\right]^+$$

with $a \geq 0$ is monotonically increasing in a. ✓

Proof.
In order to prove the monotony of $R_S(a\boldsymbol{w})$ in a, we have to distinguish two cases.

First case $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2 \leq |\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2$
In this case, $R_S(a\boldsymbol{w}) = 0$, independent of the value chosen for the parameter a. This is due to the maximization function $[\cdot]^+$.

Second case $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2 > |\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2$
In this case, the first derivative with respect to a is given by

$$\frac{\partial}{\partial a} R_S(a\boldsymbol{w}) = \frac{2\rho a\left(\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2 - \left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2\right)}{\left(1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2 a^2\right)\left(1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2 a^2\right)\ln 2},$$

which is always non-negative for $a \geq 0$, $\rho > 0$, and $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2 > |\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2$.

From the combination of both cases, we conclude that $R_S(a\boldsymbol{w})$ is monotonically increasing in a. □

B.3 Uniqueness of the Solution

Proof of Corollary (7.9).
We consider the optimization problem

$$\arg \max_{\|\boldsymbol{w}\|^2=1} R_S^{\epsilon} \quad \text{s.t. } \Pr\left(\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2} < R_S^{\epsilon} \right) = \epsilon, \tag{B.3}$$

which gives the optimal beamforming strategy for the maximization problem in Equation (7.5), and we show the uniqueness of this beamforming strategy in three steps.

First step
The function $f : \mathbb{R}_+^2 \to \mathbb{R}$ with $f(u,v) = \log_2 \frac{1+\rho v}{1+\rho u}$ and $\rho \in \mathbb{R}_+$ is differentiable and strictly decreasing in u for any $v \in \mathbb{R}_+$, since the first derivative of f with respect to u is negative for all $u \in \mathbb{R}_+$

$$\frac{\partial}{\partial u} f(u,v) = -\frac{\rho}{(1+\rho u)\ln 2} < 0.$$

Hence, it follows that the secrecy rate $f(|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2, |\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2)$ is strictly decreasing in $|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2$.

Second step
The target secrecy rate R_S^{ϵ} can be expressed as $R_S^{\epsilon} = \log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho x}$ with $x \in (0, |\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2]$. Therewith, the inequality in the constraint of the maximization problem in Equation (B.3) can be formulated as

$$\log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2} < \log_2 \frac{1+\rho\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}\right|^2}{1+\rho x} \quad \Leftrightarrow \quad \left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2 > x.$$

Due to the strict monotony of f, the target secrecy rate R_S^{ϵ} can be maximized by minimizing x. Consequently, the maximization problem in Equation (B.3) can be converted to the minimization problem

$$\arg \min_{\|\boldsymbol{w}\|^2=1} x \quad \text{s.t. } \Pr\left(\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2 > x\right) = \epsilon. \tag{B.4}$$

Third step
Using the parameterization in Equation (6.3) for the BV w and the probability distribution of $|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2$, which is $|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}|^2 \sim \chi_2^2(|\sqrt{2\kappa/1-\kappa}\boldsymbol{d}^{\mathrm{H}}\boldsymbol{w}|^2)$, we can express the probability constraint in Equation (B.4) as

$$\epsilon = 1 - \Pr\left(\left|\boldsymbol{g}^{\mathrm{H}}\boldsymbol{w}\right|^2 \leq x\right) \tag{B.5}$$

$$= Q_1\left(\sqrt{\frac{2\kappa\tau}{1-\kappa}}\left\|\boldsymbol{d}\right\|, \sqrt{\frac{2x}{1-\kappa}}\right) \tag{B.6}$$

with $\kappa \in [0,1)$, $\tau \in [0,1]$, $x \in (0, |\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}|^2]$, where Q_1 is the Marcum Q-function of the first order.

Since Q_1 is a continuous distribution function, there exists for all $\epsilon \in [0,1]$ a pair (x,τ) that fulfills the secrecy outage probability constraint. From the monotony properties of the Marcum Q-function [SBZ10] follows that for every fixed pair (x,ϵ) we have at most one unique τ that fulfills the secrecy outage probability constraint.

Hence, there exists only one pair (x^*,τ^*) that solves the minimization problem in Equation (B.4) and thus the maximization problem in Equation (B.3). □

B.4 Proof of the Concavity

Proof of Concavity of Equation (7.16).
In order to show the concavity of $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)|^2$ in τ, we compute its second derivative with respect to τ and show that it is always negative. Using the parameterization from Equation (6.3) for the beamformer $\boldsymbol{w}$, we get

$$\begin{aligned}
\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)\right|^2 &= \left|\sqrt{\tau}\frac{\boldsymbol{h}^{\mathrm{H}}\boldsymbol{\Pi}_d\boldsymbol{h}}{\|\boldsymbol{\Pi}_d\boldsymbol{h}\|} + \sqrt{1-\tau}\frac{\boldsymbol{h}^{\mathrm{H}}\boldsymbol{\Pi}_d^{\perp}\boldsymbol{h}}{\left\|\boldsymbol{\Pi}_d^{\perp}\boldsymbol{h}\right\|}\right|^2 \\
&= \left|\sqrt{\tau}\left\|\boldsymbol{\Pi}_d\boldsymbol{h}\right\| + \sqrt{1-\tau}\left\|\boldsymbol{\Pi}_d^{\perp}\boldsymbol{h}\right\|\right|^2 \\
&= \tau\left\|\boldsymbol{\Pi}_d\boldsymbol{h}\right\|^2 + (1-\tau)\left\|\boldsymbol{\Pi}_d^{\perp}\boldsymbol{h}\right\|^2 \\
&\quad + 2\sqrt{\tau}\sqrt{1-\tau}\left\|\boldsymbol{\Pi}_d\boldsymbol{h}\right\|\left\|\boldsymbol{\Pi}_d^{\perp}\boldsymbol{h}\right\|.
\end{aligned}$$

The first derivative of $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)|^2$ with respect to τ is calculated as

$$\frac{\partial}{\partial\tau}\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)\right|^2 = \|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|^2 + \frac{\sqrt{1-\tau}}{\sqrt{\tau}}\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|\left\|\boldsymbol{\Pi}_{\boldsymbol{d}}^{\perp}\boldsymbol{h}\right\| - \frac{\sqrt{\tau}}{\sqrt{1-\tau}}\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|\left\|\boldsymbol{\Pi}_{\boldsymbol{d}}^{\perp}\boldsymbol{h}\right\| - \left\|\boldsymbol{\Pi}_{\boldsymbol{d}}^{\perp}\boldsymbol{h}\right\|^2. \tag{B.7}$$

The second derivative with respect to τ is computed as

$$\frac{\partial^2}{\partial^2\tau}\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)\right|^2 = -\frac{1}{2}\frac{\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|\left\|\boldsymbol{\Pi}_{\boldsymbol{d}}^{\perp}\boldsymbol{h}\right\|}{\sqrt{\tau^3}\sqrt{(1-\tau)^3}},$$

which is always negative for $\tau \in (0,1)$. Therefore, $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)|^2$ is strictly concave in τ. □

(B.3) Optimal Parameterization for BV.
The maximum of $|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)|^2$ can be found by setting Equation (B.7) equal to zero

$$\frac{\partial}{\partial\tau}\left|\boldsymbol{h}^{\mathrm{H}}\boldsymbol{w}(\tau)\right|^2 = 0.$$

By solving this equation for τ, we get the solution

$$\tau^* = \frac{\|\boldsymbol{\Pi}_{\boldsymbol{d}}\boldsymbol{h}\|^2}{\|\boldsymbol{h}\|^2},$$

which corresponds to MRT, i.e., $\boldsymbol{w}(\tau^*) = \boldsymbol{w}_{\mathrm{MRT}}$. ✓

C Proofs for the Two-Way Relay WTC under Full CSI

C.1 Monotony of the Achievable Secrecy Rate with AN

Proof of Proposition (10.2).
In order to prove the Optimization Problem (10.1), we need to show that the function R_S^{AN} is unimodal in p_R over the range $[0, P_R]$ and has a maximum.

First, let us determine the extreme values of the function R_S^{AN}. For convenience of notation, let us denote the effective received SNR at the relay as

$$\tilde{\rho} = \rho P_{S,1} \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} \right|^2$$

and the effectively received SNR at the eavesdropper in the first phase as

$$\bar{\rho} = \rho P_{S,2} \left\| \boldsymbol{h}_E \right\|^2 .$$

The first derivative of R_S^{AN} with respect to p_R is given by

$$\frac{\partial R_S^{\mathrm{AN}}}{\partial p_R} = \frac{1}{\ln 2} \frac{\tilde{\rho}\rho\left(1+\bar{\rho}\tilde{\rho}-\rho^2\|\boldsymbol{g}_B\|^2|g_E|^2 p_R^2+\bar{\rho}+\tilde{\rho}\right)\left(\|\boldsymbol{g}_B\|^2\bar{\rho}+\|\boldsymbol{g}_B\|^2-|g_E|^2\right)}{\left(1+\rho\|\boldsymbol{g}_B\|^2 p_R+\tilde{\rho}\right)\left(1+\bar{\rho}\tilde{\rho}+|g_E|^2 p_R\rho+\bar{\rho}+\tilde{\rho}\right)\left(\|\boldsymbol{g}_B\|^2 p_R\rho+1\right)\left(1+|g_E|^2 p_R\rho+\bar{\rho}\right)}. \tag{C.1}$$

Computing the zeros, we obtain

$$\tilde{p}_R = \pm \frac{\sqrt{\|\boldsymbol{g}_B\|^2 |g_E|^2 (\tilde{\rho}+1)(\bar{\rho}+1)}}{\rho \|\boldsymbol{g}_B\|^2 |g_E|^2}.$$

Due to the fact that p_R is a power value, the only feasible solution is the positive zero.

The derivative in Equation (C.1) is non-negative in the range $p_R \in [0, \tilde{p}_R]$ and therefore, the achievable secrecy rate R_S^{AN} is monotonically increasing in p_R. Additionally, the derivative in Equation (C.1) is always non-positive in the range $p_R \in [\tilde{p}_R, \infty]$, i.e., R_S^{AN} is monotonically decreasing in p_R. From these two facts follows that the achievable secrecy rate R_S^{AN} is unimodal with a maximum at $\tilde{p}_R$.

Due to the power constraint at the relay, the optimal power allocation is given by

$$p_R^* = \min\left(\tilde{p}_R, P_R\right). \qquad \square$$

C.2 Positive Values of the Achievable Secrecy Rate with AN

Proof of Proposition (10.7).
For the proof, we just need to calculate the zeros of the function $R_S^{\mathrm{AN}}(\rho)$, which are given by

$$\begin{aligned}\rho_1 &= 0 \quad \text{and}\\ \rho_2 &= \frac{|g_E|^2 - \|\boldsymbol{g}_B\|^2}{P_{S,2}\|\boldsymbol{g}_B\|^2 \|\boldsymbol{h}_E\|^2},\end{aligned}$$

and to take a look at the monotonic behavior of $R_S^{\mathrm{AN}}(\rho)$ in ρ.

The first derivative of the achievable secrecy rate $R_S^{\mathrm{AN}}(\rho)$ with respect to ρ is given by

$$\frac{\partial R_S^{\mathrm{AN}}(\rho)}{\partial \rho} = \frac{1}{\ln 2}\rho\beta p_R\left(t_1 + t_2 + t_3 + t_4\right),$$

where

$$\begin{aligned}t_1 &= \frac{\|\boldsymbol{g}_B\|^2 \eta\left(|g_E|^2 p_R + \eta\right)\left(\|\boldsymbol{g}_B\|^2 p_R + \beta\right)\rho^3}{z},\\ t_2 &= \frac{2\|\boldsymbol{g}_B\|^2 \eta\left(p_R\left(\|\boldsymbol{g}_B\|^2 + |g_E|^2\right) + \eta + \beta\right)\rho^2}{z},\\ t_3 &= \frac{\left(\beta\left(\|\boldsymbol{g}_B\|^2 - |g_E|^2\right) + p_R\left(\|\boldsymbol{g}_B\|^4 - |g_E|^4\right) + \eta\left(4\|\boldsymbol{g}_B\|^2 - |g_E|^2\right)\right)\rho}{z},\end{aligned}$$

$$t_4 = \frac{2\left(\|\boldsymbol{g}_B\|^2 - |g_E|^2\right)}{z},$$

$$z = \left(1+\rho\left(|g_E|^2 p_R + \eta + \beta\right) + \rho^2\eta\beta\right)\left(1+\rho\left(|g_E|^2 p_R + \eta\right)\right)\cdot$$
$$\left(1+\rho p_R \|\boldsymbol{g}_B\|^2\right)\left(1+\rho\left(\|\boldsymbol{g}_B\|^2 p_R + \beta\right)\right),$$

$$\beta = P_{S,1}\left|\boldsymbol{h}_R^{\mathrm{H}}\boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}\right|^2, \quad \text{and}$$

$$\eta = P_{S,2}\|\boldsymbol{h}_E\|^2.$$

In order to analyze the monotonic behavior of the function, we need to distinguish two cases.

First case $\|\boldsymbol{g}_B\|^2 \geq |g_E|^2$
In this case, ρ_2 is negative and therefore, the function $R_S^{\mathrm{AN}}(\rho)$ should be positive for all values $\rho \geq \rho_1 = 0$.

If we take a look at the first derivative, we can easily see, that all four fractions t_1 to t_4 are positive and therefore, $R_S^{\mathrm{AN}}(\rho)$ is monotonically increasing in ρ.

Second case $\|\boldsymbol{g}_B\|^2 < |g_E|^2$
In this case, the function $R_S^{\mathrm{AN}}(\rho)$ should become positive for all values $\rho \geq \rho_2 = \frac{|g_E|^2 - \|\boldsymbol{g}_B\|^2}{P_{S,2}\|\boldsymbol{g}_B\|^2\|\boldsymbol{h}_E\|^2}$.

In order to show this, we take a closer look on all values smaller than ρ_2 and all values greater than ρ_2.

a) $0 \leq \rho \leq \rho_2$
If ρ is in the interval $[0, \rho_2]$, the function $R_S^{\mathrm{AN}}(\rho)$ is zero. This is due to the maximization function $[\cdot]^+$.

a) $\rho > \rho_2$
The first derivative of $R_S^{\mathrm{AN}}(\rho)$ in ρ has a positive slope

$$\left.\frac{\partial R_S^{\mathrm{AN}}(\rho)}{\partial \rho}\right|_{\rho=\rho_2} = \frac{\left(\|\boldsymbol{g}_B\|^2-|g_E|^2\right)^2 \beta\eta P_R \|\boldsymbol{g}_B\|^2}{|g_E|^2\left(\eta+P_R\left(|g_E|^2-\|\boldsymbol{g}_B\|^2\right)\right)\left(\eta\|\boldsymbol{g}_B\|^2+P_R\|\boldsymbol{g}_B\|^2\left(|g_E|^2-\|\boldsymbol{g}_B\|^2\right)+\beta\left(|g_E|^2-\|\boldsymbol{g}_B\|^2\right)\right)} > 0.$$

The denominator is positive, as we regard the case $\|\boldsymbol{g}_B\|^2 < |g_E|^2$. The numerator is always positive due to the square function. Therefore, the achievable secrecy rate $R_S^{\mathrm{AN}}(\rho)$ has a positive slope in the zero ρ_2, i.e., the function becomes positive for $\rho > \rho_2$. □

D Proofs for the Two-Way Relay WTC under Partial CSI

D.1 Optimal IN Transmit Signal

Proof of Proposition (11.1).
We prove this proposition by contradiction. Let us assume that Alice uses a channel estimation γ_E to get the IN transmit signal

$$x_n = -\frac{\sqrt{\alpha}\gamma_E \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}}}{\boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{\mathrm{MRT}}^{\mathrm{Eve}}} x.$$

We can thenformulate following optimization problem.

(D.1) Optimization Problem.
We minimize the worst case leakage power over the estimated channel

$$\min_{\gamma_E} \max_{|\Delta g_E|^2 \leq \epsilon} L(\gamma_E)$$

with

$$\begin{aligned} L(\gamma_E) &= \left| \boldsymbol{h}_E^{\mathrm{H}} \boldsymbol{w}_{\mathrm{MRT}}^{\mathrm{Eve}} x_n + \sqrt{\alpha} g_E \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x \right|^2 \\ &= \left| \sqrt{\alpha} \left(\hat{g}_E + \Delta g_E - \gamma_E \right) \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x \right|^2 . \end{aligned} \tag{D.1}$$

✓

We need to show that the leakage power is minimized if we choose γ_E to the estimated channel $\hat{g}_E$, i.e.,

$$L(\gamma_E^* = \hat{g}_E) \leq L(\gamma_E) \quad \forall \gamma_E.$$

Let us first examine the leakage power with $\gamma_E^* = \hat{g}_E$. Using Equation (D.1) we get

$$\max_{|\Delta g_E|^2 \leq \epsilon} L(\gamma_E^* = \hat{g}_E) = \max_{\left|\Delta g_E^2\right| \leq \epsilon} \left| \sqrt{\alpha} \left(\Delta g_E \right) \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x \right|^2$$

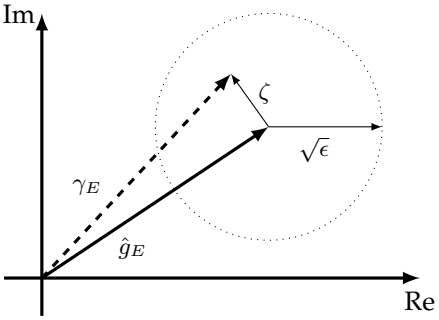


Figure D.1: Illustration of the estimated channel $\hat{g}_E$, the estimation error ϵ and a suboptimal estimation $\gamma_E = \hat{g}_E + \zeta$.

$$= \epsilon\alpha \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x \right|^2 .$$

If we now take a look at some other $\gamma_E = \hat{g}_E + \zeta$, where ζ is some estimation error with $|\zeta|^2 \leq \epsilon$, Equation (D.1) becomes

$$\begin{aligned} &\max_{|\Delta g_E|^2 \leq \epsilon} L(\gamma_E = \hat{g}_E + \zeta) \\ &= \max_{|\Delta g_E|^2 \leq \epsilon} \left| \sqrt{\alpha} \left(\Delta g_E - \zeta \right) \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x \right|^2 \\ &= \left(\epsilon + |\zeta|^2 \right) \alpha \left| \boldsymbol{h}_R^{\mathrm{H}} \boldsymbol{w}_{\mathrm{ZF}}^{\mathrm{Eve}} x \right|^2 . \end{aligned}$$

It is easy to see that $L(\gamma_E^* = \hat{g}_E) \leq L(\gamma_E = \hat{g}_E + \zeta)$ and therefore it holds that $L(\hat{g}_E) \leq L(\gamma_E), \forall \gamma_E$. The used estimates for the proof are illustrated in Figure D.1. □

D.2 Optimal Power Allocation for the IN Scheme

Proof of Proposition (11.5).
In order to obtain the results given in Table 11.1, we take the first derivative of the achievable secrecy rate R_S^{pCSI} with regard to the power at the relay p_R, which is given by

$$\frac{\partial R_S^{\mathrm{pCSI}}}{\partial p_R} = t_1 + t_2 + t_3 + t_4, \tag{D.2}$$

where $\tilde{\rho}$ is defined in Equation (11.2),

$$
\begin{aligned}
t_1 =& \frac{(\tilde{\rho}+1)^2 \rho\tilde{\rho}\left(\|\boldsymbol{g}_B\|^2 - \epsilon\right)}{z},\\
t_2 =& \frac{\rho^3 p_R^2 \tilde{\rho}\|\boldsymbol{g}_B\|^2\left(|\tilde{g}_E|^4 - \epsilon\|\boldsymbol{g}_B\|^2\right)}{z},\\
t_3 =& \frac{2\rho^2 p_R \tilde{\rho}\|\boldsymbol{g}_B\|^2(1+\tilde{\rho})\left(|\tilde{g}_E|^2 - \epsilon\right)}{z},\\
t_4 =& \frac{\rho^3 p_R^2 \tilde{\rho}^2\|\boldsymbol{g}_B\|^2\epsilon\left(|\tilde{g}_E|^2 - \|\boldsymbol{g}_B\|^2\right)}{z}, \quad \text{and}\\
z =& \left(\tilde{\rho} + \rho p_R\|\boldsymbol{g}_B\|^2 + 1\right)\left(\rho p_R\|\boldsymbol{g}_B\|^2 + 1\right)\cdot\\
& \left(\rho p_R\tilde{\rho}\epsilon + \tilde{\rho} + \rho p_R|\tilde{g}_E|^2 + 1\right)\left(\tilde{\rho} + \rho p_R|\tilde{g}_E|^2 + 1\right).
\end{aligned}
$$

Furthermore, we denote the maximal power, which the relay can use such that the transmitter is still able to neutralize the data signal in the second phase as

$$
p_R^{\max} = \frac{P_{S,2}\|\boldsymbol{h}_E\|^2}{\hat{g}_E}\left(1 + \frac{1}{\tilde{\rho}}\right).
$$

We analyze the following six cases, which can be split into two groups:

1. $\|\boldsymbol{g}_B\|^2 > \epsilon$
   For all cases with $\|\boldsymbol{g}_B\|^2 > \epsilon$, t_1 is positive and therefore the function R_S^{pCSI} is monotonically increasing in p_R at the point $p_R = 0$, i.e., R_S^{pCSI} is positive for certain values of p_R.

   In order to find the optimal p_R we need to take a closer look at the three following cases.

   i) $|\tilde{g}_E|^2 > \|\boldsymbol{g}_B\|^2 > \epsilon$
      In this case, all four fractions in Equation (D.2) are positive and therefore R_S^{pCSI} is monotonic increasing in p_R. The optimal power allocation at the relay with regard to the IN power constraint is then given as

$$
p_R^* = p_R^{\max}.
$$

Taking the power constraint at the relay into account, the optimal power allocation is given by

$$p_R^* = \min\left(p_R^{\max}, P_R\right).$$

ii) $\|\boldsymbol{g}_B\|^2 > |\tilde{g}_E|^2 > \epsilon$
We need to distinguish two additional cases.

a) $\left(|\tilde{g}_E|^4 + |\tilde{g}_E|^2 \epsilon\tilde{\rho}\right) \geq \epsilon \|\boldsymbol{g}_B\|^2 (1+\tilde{\rho})$:
Again, all four fractions in Equation (D.2) are positive. Therefore, R_S^{pCSI} is monotonically increasing in p_R and the optimal power allocation at the relay is given by

$$p_R^* = p_R^{\max}.$$

As before, if we consider the power constraint at the relay the optimal power allocation is given by

$$p_R^* = \min\left(p_R^{\max}, P_R\right).$$

b) $\left(|\tilde{g}_E|^4 + |\tilde{g}_E|^2 \epsilon\tilde{\rho}\right) < \epsilon \|\boldsymbol{g}_B\|^2 (1+\tilde{\rho})$:
In this case, the function R_S^{pCSI} is unimodal with a positive maximum at

$$\tilde{p}_R = \frac{(1+\tilde{\rho})\left(\sqrt{\epsilon\|\boldsymbol{g}_B\|^2\left(\tilde{\rho}\left(\|\boldsymbol{g}_B\|^2-\epsilon\right)+s\right)s}+\|\boldsymbol{g}_B\|^2\left(|\tilde{g}_E|^2-\epsilon\right)\right)}{\rho\|\boldsymbol{g}_B\|^2\left(\epsilon\tilde{\rho}s+\epsilon\|\boldsymbol{g}_B\|^2-|\tilde{g}_E|^4\right)},$$

where $s = \|\boldsymbol{g}_B\|^2 - |\tilde{g}_E|^2$. Therefore, the optimal power allocation at the relay is given by

$$p_R^* = \min\left(\tilde{p}_R, p_R^{\max}, P_R\right).$$

The first argument of the minimization function is the optimal power allocation point $\tilde{p}_R$ while the second argument is the maximum power that can be used so that Alice is still able to neutralize the data signal at the eavesdropper with full power $P_{S,2}$ in the second phase. The third argument is due to the power constraint at the relay.

iii) $\|\boldsymbol{g}_B\|^2 > \epsilon > |\tilde{g}_E|^2$
The function R_S^{pCSI} is unimodal and for small p_R monotonically increasing (and positive) and becomes monotonically decreasing with growing p_R. The maximum is again at $\tilde{p}_R$ as given in Item 1(ii)b. Therefore, the optimal power allocation at the relay is again given by

$$p_R^* = \min\left(\tilde{p}_R, p_R^{\max}, P_R\right).$$

2. $\|\boldsymbol{g}_B\|^2 \leq \epsilon$
For $\|\boldsymbol{g}_B\|^2 \leq \epsilon$, the function R_S^{pCSI} is monotonically decreasing for small p_R. Whether the function becomes positive at some point, we will analyze in the following.

iv) $|\tilde{g}_E|^2 > \epsilon > \|\boldsymbol{g}_B\|^2$
In this case, the secrecy rate R_S^{pCSI} is unimodal. As long as $t_2 + t_3 + t_4$ is smaller than $-t_1$, the function is decreasing. The local minimum is achieved for $t_2 + t_3 + t_4 = -t_1$. From this point on the function is monotonically increasing.

This behavior can easily be observed by having a close look on the fractions t_1 to t_4. t_1 is independent of the power at the relay. Therefore, for small values of p_R, $t_2 + t_3 + t_4$ is smaller than $-t_1$ and thus R_S^{pCSI} is decreasing in p_R. Furthermore, all of these rate values are negative. With growing p_R, $t_2 + t_3 + t_4$ becomes greater than $-t_1$ and the function is monotonically increasing. The rate values become positive for

$$p_R > \frac{(\tilde{\rho}+1)\left(\|\boldsymbol{g}_B\|^2 - \epsilon\right)}{\rho\|\boldsymbol{g}_B\|^2\left(\epsilon - |\tilde{g}_E|^2\right)}.$$

Let us denote this threshold as $p_R^0 = \frac{(\tilde{\rho}+1)\left(\|\boldsymbol{g}_B\|^2 - \epsilon\right)}{\rho\|\boldsymbol{g}_B\|^2\left(\epsilon - |\tilde{g}_E|^2\right)}$.

As the function is monotonically increasing for values between p_R^0 and $p_R^{\max}$, the optimal p_R^* is $p_R^* = p_R^{\max}$ if $p_R^{\max} > p_R^0$. Otherwise $p_R^* = 0$ and therefore the secrecy rate is also $R_S^{\text{pCSI}} = 0$.

Let us summarize these results and include the power constraint at the relay. The optimal power allocation at the relay in the second phase can then be written as

$$p_R^* = \begin{cases} p_R^{\max} & \text{if } \frac{(\tilde{\rho}+1)\left(\|\boldsymbol{g}_B\|^2-\epsilon\right)}{\rho\|\boldsymbol{g}_B\|^2\left(\epsilon-|\tilde{g}_E|^2\right)} < p_R^{\max} < P_R \\ P_R & \text{if } \frac{(\tilde{\rho}+1)\left(\|\boldsymbol{g}_B\|^2-\epsilon\right)}{\rho\|\boldsymbol{g}_B\|^2\left(\epsilon-|\tilde{g}_E|^2\right)} < P_R \leq p_R^{\max} \\ 0 & \text{otherwise} \end{cases}.$$

v) $\epsilon > |\tilde{g}_E|^2 > \|\boldsymbol{g}_B\|^2$
In this case, the secrecy rate is always zero, as the limit for p_R to infinity is always negative

$$\lim_{p_R \to \infty} R_S^{\text{pCSI}} = \log_2\left(\frac{\tilde{\rho}\,|\tilde{g}_E|^2 + |\tilde{g}_E|^2}{\tilde{\rho}\epsilon + |\tilde{g}_E|^2}\right) \leq 0.$$

vi) $\epsilon \geq \|\boldsymbol{g}_B\|^2 \geq |\tilde{g}_E|^2$
In this case, all four fractions in Equation (D.2) are negative and therefore R_S^{pCSI} is monotonically decreasing in p_R. The optimal power allocation at the relay is then given by $p_R^* = 0$, i.e., it is best not to send at all.

As mentioned in Remark (11.3), the optimal power allocation $p_{S,2}^*$ for the transmission of the IN signal in the second phase corresponds to the the optimal power allocation p_R^* and follows directly from the IN power constraint in Equation (11.1). □

E Further Contributions

Within this thesis, the focus is on beamforming strategies and protection mechanisms in order to maximize the secrecy rate in simple system models under partial CSI. The two chosen system models are the Gaussian wiretap channel and the Gaussian two-hop relay wiretap channel.

During my time at the Chair for Communications Theory, I also worked on following papers that did not contribute to this thesis.

The publication [Ger08] results from my student project supervised by Dr. Sebastian Clauß and Prof. Andreas Pfitzmann. The paper discusses and compares two different approaches to encrypt RDF-Graphs (Resource Description Framework).

[Ger08] Sabrina Gerbracht. "Possibilities to Encrypt an RDF-Graph". In: *Proc. of International Conference on Information & Communication Technologies: from Theory to Applications (ICTTA)*. 2008

In [JWG10], an overview on physical layer secrecy is given. The book chapter focuses mainly on achievable secrecy rates in different single user and multi user scenarios.

[JWG10] Eduard A. Jorswieck, Anne Wolf, and Sabrina Gerbracht. "Secrecy on the Physical Layer in Wireless Networks". In: *Trends in Telecommunications Technologies*. Ed. by Christos J. Bouras. INTECH, 2010. Chap. 20, pp. 413–435

In [JG09], the sum secrecy rate of the Gaussian two-user Orthogonal Frequency-Division Multiplexing (OFDM) broadcast WTC is maximized over the power. It could be shown, that the OFDM subcarriers can be divided in two subsets. The first subset contains all subcarriers, where the channel from the transmitter to the first receiver is better. All other subcarriers are collected in the second subset. Messages to the first receiver can now be transmitted confidentially over the channels in subset one, while the confidential messages for the second receiver

are transmitted over the channels in subset two. The power over all subcarriers is allocated by a water filling algorithm.

[JG09] Eduard A. Jorswieck and Sabrina Gerbracht. “Secrecy Rate Region of Downlink OFDM Systems: Efficient Resource Allocation”. In: *Proc. of International OFDM-Workshop (InOWo)*. 2009

In [HJG13], the possibilities of IN in the multi-carrier multi-antenna multi-user relay channel are investigated. A journal version of this scenario is published in [HJE13].

[HJG13] Ka-Ming (Zuleita) Ho, Eduard A. Jorswieck, and Sabrina Gerbracht. “Efficient Information Leakage Neutralization on a Relay-Assisted Multi-Carrier Interference Channel”. In: *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. 2013

[HJE13] Ka-Ming (Zuleita) Ho, Eduard A. Jorswieck, and Sabrina Engelmann. “Information Leakage Neutralization for the Multi-Antenna Non-Regenerative Relay-Assisted Multi-Car-rier Interference Channel”. In: *IEEE Journal on Selected Areas in Communications* 31.9 (Sept. 2013), pp. 1672–1686

In [Ric+15] an achievable secrecy rate for the two-way relay channel under usage of physical layer network coding is established.

[Ric+15] Johannes Richter, Christian Scheunert, Sabrina Engelmann, and Eduard A. Jorswieck. “Secrecy in the Two-Way Relay Channel with Compute-and-Forward”. In: *Proc. of IEEE Communications Theory Symposium (ICC)*. 2015

Another topic in physical layer security, that is currently discussed in literature with increasing interest, is the generation of secret keys from channel parameters. In [JWE13], the generation of secret keys in the MIMO channel with precoding at both Alice and Bob is investigated. The special case, where one communication partner has only a single antenna, i.e., MISO/SIMO, is analyzed in [EWJ14]. With this simplified system model, it is possible to characterize the optimal precoding matrix in order to maximize the secret key rate.

[JWE13] Eduard A. Jorswieck, Anne Wolf, and Sabrina Engelmann. "Secret Key Generation from Reciprocal Spatially Correlated MIMO Channels". In: *Proc. of IEEE Global Communication Conference (GLOBECOM)*. 2013

[EWJ14] Sabrina Engelmann, Anne Wolf, and Eduard A. Jorswieck. "Precoding for Secret Key Generation in Multiple Antenna Channels with Statistical Channel State Information". In: *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. 2014

Further, physical layer techniques were compared to and combined by traditional upper layer approaches. In [Ric+13], physical layer secure network coding and different cryptographic network coding schemes in the two-hop relay channel were compared by certain parameters, e.g., throughput and achievable secrecy rates. In [Pfe+14], physical layer key generation, which is up to now only possible between two nodes with a direct link, and upper layer techniques were combined in order to establish an end-to-end key between arbitrary nodes of a network.

[Ric+13] Johannes Richter, Elke Franz, Sabrina Engelmann, Stefan Pfennig, and Eduard A. Jorswieck. "Physical Layer Security vs. Network Layer Secrecy: Who Wins on the Untrusted Two-Way Relay Channel?" In: *Proc. of International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD)*. 2013

[Pfe+14] Stefan Pfennig, Elke Franz, Sabrina Engelmann, and Anne Wolf. "End-to-End Key Establishment using Physical Layer Key Generation with Specific Attacker Models". In: *Proc. of Workshop on Communication Security (WCS)*. 2014

List of Figures

Bibliography

[BR06] João Barros and Miguel R. D. Rodrigues. "Secrecy Capacity of Wireless Channels". In: *Proc. of IEEE International Symposium on Information Theory (ISIT)*. 2006.

[Ber+09] Stefan Berger, Marc Kuhn, Armin Wittneben, Timo Unger, and Anja Klein. "Recent Advances in Amplify-and-Forward Two-Hop Relaying". In: *IEEE Communications Magazine* 47.7 (July 2009), pp. 50–56.

[Bil95] Patrick Billingsley. *Probability and Measure*. Third edition. Wiley, 1995.

[Bjö+12] Emil Björnson, Gan Zheng, Mats Bengtsson, and Björn E. Ottersten. "Robust Monotonic Optimization Framework for Multicell MISO Systems". In: *IEEE Transactions on Signal Processing* 60.5 (May 2012), pp. 2508–2523.

[BB11] Matthieu R. Bloch and João Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. First edition. Cambridge University Press, 2011.

[Blo+08] Matthieu R. Bloch, João Barros, Miguel R. D. Rodrigues, and Steven W. McLaughlin. "Wireless Information-Theoretic Security". In: *IEEE Transaction on Information Theory* 54.6 (June 2008), pp. 2515–2534.

[CK78] Imre Csiszár and János Körner. "Broadcast Channels with Confidential Messages". In: *IEEE Transactions on Information Theory* 24.3 (May 1978), pp. 339–348.

[Don+09] Lun Dong, Zhu Han, Athina P. Petropulu, and H. Vincent Poor. "Cooperative Jamming for Wireless Physical Layer Security". In: *Proc. of IEEE Workshop on Statistical Signal Processing (SSP)*. 2009.

[Don+10] Lun Dong, Zhu Han, Athina P. Petropulu, and H. Vincent Poor. "Improving Wireless Physical Layer Security via Cooperating Relays". In: *IEEE Transactions on Signal Processing* 58.3 (Mar. 2010), pp. 1875–1888.

[DYJ11] Lun Dong, Homayoun Yousefi'zadeh, and Hamid Jafarkhani. "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper". In: *Proc. of IEEE International Conference on Communications (ICC)*. 2011.

[EU09] Ersen Ekrem and Sennur Ulukus. "Ergodic Secrecy Capacity Region of the Fading Broadcast Channel". In: *Proc. of IEEE International Conference on Communications (ICC)*. 2009.

[EHJ13] Sabrina Engelmann, Ka-Ming (Zuleita) Ho, and Eduard A. Jorswieck. "Interference Leakage Neutralization in Two-Hop Wiretap Channels with Partial CSI". In: *Proc. of IEEE International Symposium on Wireless Communication Systems (ISWCS)*. 2013.

[EWJ14] Sabrina Engelmann, Anne Wolf, and Eduard A. Jorswieck. "Precoding for Secret Key Generation in Multiple Antenna Channels with Statistical Channel State Information". In: *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. 2014.

[For03] G. David Jr. Forney. "On the Role of MMSE Estimation in Approaching the Information-Theoretic Limits of Linear Gaussian Channels: Shannon meets Wiener". In: *Proc. of Allerton Conference on Communication, Control, and Computing*. 2003.

[GTS11a] Frédéric Gabry, Ragnar Thobaben, and Mikael Skoglund. "Outage Performance and Power Allocation for Decode-and-Forward Relaying and Cooperative Jamming for the Wiretap Channel". In: *Proc. of IEEE International Conference on Communications (ICC)*. 2011.

[GTS11b] Frédéric Gabry, Ragnar Thobaben, and Mikael Skoglund. "Outage Performances for Amplify-and-Forward, Decode-and-Forward and Cooperative Jamming Strategies for the Wiretap Channel". In: *Proc. of IEEE Wireless Communications and Networking Conference*. 2011.

[Ger08] Sabrina Gerbracht. "Possibilities to Encrypt an RDF-Graph". In: *Proc. of International Conference on Information & Communication Technologies: from Theory to Applications (ICTTA)*. 2008.

[Ger+12] Sabrina Gerbracht, Eduard A. Jorswieck, Gan Zheng, and Björn E. Ottersten. "Non-regenerative Two-Hop Wiretap Channels using Interference Neutralization". In: *Proc. of IEEE International Workshop on Information Forensics and Security (WIFS)*. 2012.

[GSJ11] Sabrina Gerbracht, Christian Scheunert, and Eduard A. Jorswieck. "Beamforming for Secrecy Rate Maximization under Outage Constraints and Partial CSI". In: *Proc. of the Asilomar Conference on Signals, Systems, and Computers*. 2011.

[GSJ12] Sabrina Gerbracht, Christian Scheunert, and Eduard A. Jorswieck. "Secrecy Outage in MISO Systems With Partial Channel Information". In: *IEEE Transactions on Information Forensics and Security* 7.2 (Apr. 2012), pp. 704–716.

[GWJ10] Sabrina Gerbracht, Anne Wolf, and Eduard A. Jorswieck. "Beamforming for Fading Wiretap Channels with Partial Channel Information". In: *Proc. of International ITG Workshop on Smart Antennas (WSA)*. 2010.

[Gol+03] Andrea J. Goldsmith, Syed A. Jafar, Nihar Jindal, and Sriram Vishwanath. "Capacity Limits of MIMO Channels". In: *IEEE Journal on Selected Areas in Communications* 21.5 (June 2003), pp. 684–702.

[Gun+13] Onur Gungor, Jian Tan, Can E. Köksal, Hesham El Gamal, and Ness B. Shroff. "Secrecy Outage Capacity of Fading Channels". In: *IEEE Transactions on Information Theory* 59.9 (Sept. 2013), pp. 5379–5397.

[Gur09] Mustafa C. Gursoy. "Secure Communication in the Low-SNR Regime: A Characterization of the Energy-Secrecy Tradeoff". In: *Proc. of IEEE International Symposium on Information Theory (ISIT)*. 2009.

[HY10] Xiang He and Aylin Yener. "Cooperative Jamming: The Tale of Friendly Interference for Secrecy". In: *Securing Wireless Communications at the Physical Layer*. Ed. by Ruoheng Liu and Wade Trappe. Springer, 2010. Chap. 4, pp. 65–88.

[HJ12] Ka-Ming (Zuleita) Ho and Eduard A. Jorswieck. "Instantaneous Relaying: Optimal Strategies and Interference Neutralization". In: *IEEE Transactions on Signal Processing* 60.12 (Dec. 2012), pp. 6655–6668.

[HJE13] Ka-Ming (Zuleita) Ho, Eduard A. Jorswieck, and Sabrina Engelmann. "Information Leakage Neutralization for the Multi-Antenna Non-Regenerative Relay-Assisted Multi-Carrier Interference Channel". In: *IEEE Journal on Selected Areas in Communications* 31.9 (Sept. 2013), pp. 1672–1686.

[HJG13] Ka-Ming (Zuleita) Ho, Eduard A. Jorswieck, and Sabrina Gerbracht. "Efficient Information Leakage Neutralization on a Relay-Assisted Multi-Carrier Interference Channel". In: *Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. 2013.

[HS11] Jing Huang and A. Lee Swindlehurst. "Cooperative Jamming for Secure Communications in MIMO Relay Networks". In: *IEEE Transactions on Signal Processing* 59.10 (Oct. 2011), pp. 4871–4884.

[JB07] Eduard A. Jorswieck and Holger Boche. "Majorization and Matrix Monotone Functions in Wireless Communications". In: vol. 3. Foundations and Trends in Communications and Information Theory 6. Now publishers, 2007, pp. 553–701.

[JG09] Eduard A. Jorswieck and Sabrina Gerbracht. "Secrecy Rate Region of Downlink OFDM Systems: Efficient Resource Allocation". In: *Proc. of International OFDM-Workshop (InOWo)*. 2009.

[JLD08] Eduard A. Jorswieck, Erik G. Larsson, and Danyo Danev. "Complete Characterization of the Pareto Boundary for the MISO Interference Channel". In: *IEEE Transactions on Signal Processing* 56.10 (Oct. 2008), pp. 5292–5296.

[JM09] Eduard A. Jorswieck and Rami Mochaourab. "Secrecy Rate Region of MISO Interference Channel: Pareto Boundary and Non-Cooperative Games". In: *Proc. of International ITG Workshop on Smart Antennas (WSA)*. 2009.

[JWE13] Eduard A. Jorswieck, Anne Wolf, and Sabrina Engelmann. "Secret Key Generation from Reciprocal Spatially Correlated MIMO Channels". In: *Proc. of IEEE Global Communication Conference (GLOBECOM)*. 2013.

[JWG10] Eduard A. Jorswieck, Anne Wolf, and Sabrina Gerbracht. "Secrecy on the Physical Layer in Wireless Networks". In: *Trends in Telecommunications Technologies*. Ed. by Christos J. Bouras. INTECH, 2010. Chap. 20, pp. 413–435.

[KW10a] Ashish Khisti and Gregory W. Wornell. "Secure Transmission with Multiple Antennas – I: The MISOME Wiretap Channel". In: *IEEE Transactions on Information Theory* 56.7 (July 2010), pp. 3088–3104.

[KW10b] Ashish Khisti and Gregory W. Wornell. "Secure Transmission with Multiple Antennas – II: The MIMOME Wiretap Channel". In: *IEEE Transactions on Information Theory* 56.11 (Nov. 2010), pp. 5515–5532.

[KMY06] Gerhard Kramer, Ivana Marić, and Roy D. Yates. "Cooperative Communications". In: vol. 1. Foundations and Trends in Networking 3–4. Now publishers, 2006, pp. 271–425.

[LE08] Lifeng Lai and Hesham El Gamal. "The Relay–Eavesdropper Channel: Cooperation for Secrecy". In: *IEEE Transactions on Information Theory* 54.9 (Sept. 2008), pp. 4005–4019.

[LH78] Sik K. Leung-Yan-Cheong and Martin E. Hellman. "The Gaussian Wire-Tap Channel". In: *IEEE Transactions on Information Theory* 24.4 (July 1978), pp. 451–456.

[LM11] Qiang Li and Wing-Kin Ma. "Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming". In: *IEEE Transactions on Signal Processing* 59.8 (Aug. 2011), pp. 3799–3812.

[LPS08] Yingbin Liang, H. Vincent Poor, and Shlomo Shamai (Shitz). "Secure Communication Over Fading Channels". In: *IEEE Transactions on Information Theory* 54.6 (June 2008), pp. 2470–2492.

[LPS10] Yingbin Liang, H. Vincent Poor, and Shlomo Shamai (Shitz). "Secret Communication Under Channel Uncertainty". In: *Securing Wireless Communications at the Physical Layer*. Ed. by Ruoheng Liu and Wade Trappe. Springer, 2010. Chap. 6, pp. 113–141.

[LJ14] Pin-Hsun Lin and Eduard A. Jorswieck. "On the Fast Fading Gaussian Wiretap Channel with Statistical Channel State Information at Transmitter". Sept. 2014. submitted to IEEE Transactions on Information Forensics and Security.

[Lin+13] Pin-Hsun Lin, Szu-Hsiang Lai, Shih-Chun Lin, and Hsuan-Jung Su. "On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels". In: *IEEE Journal on Selected Areas in Communications* 31.9 (Sept. 2013), pp. 1728–1740.

[Lin+11] Shih-Chun Lin, Tsung-Hui Chang, Ya-Lan Liang, Y.-W. Peter Hong, and Chong-Yung Chi. "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem". In: *IEEE Transactions on Wireless Communications* 10.3 (Mar. 2011), pp. 901–915.

[LL14] Shih-Chun Lin and Cheng-Liang Lin. "On Secrecy Capacity of Fast Fading MIMOME Wiretap Channels with Statistical CSIT". In: *IEEE Transactions on Wireless Communications* 13.6 (June 2014), pp. 3293–3306.

[LTV05] Angel Lozano, Antonio M. Tulino, and Sergio Verdú. "High-SNR Power Offset in Multiantenna Communication". In: *IEEE Transactions on Information Theory* 51.12 (Dec. 2005), pp. 4134–4151.

[MO79] Albert W. Marshall and Ingram Olkin. "Inequalities: Theory of Majorization and Its Applications". In: vol. 143. Mathematics in Science and Engineering. Academic Press, 1979.

[MW00] Ueli M. Maurer and Stefan Wolf. "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free". In: *Proc. of Workshop on Advances in Cryptology (EUROCRYPT)*. Vol. 1807/2000. Lecture Notes in Computer Science. Springer, 2000, pp. 351–368.

[Moh+08] Soheil Mohajer, Suhas N. Diggavi, Christina Fragouli, and David N. C. Tse. "Transmission Techniques for Relay-Interference Networks". In: *Proc. of Conference on Communication, Control, and Computing*. 2008.

[MS09] Amitav Mukherjee and A. Lee Swindlehurst. "Utility of Beamforming Strategies for Secrecy in Multiuser MIMO Wiretap Channels". In: *Proc. of Annual Allerton Conference on Communication, Control, and Computing*. 2009.

[MS11] Amitav Mukherjee and A. Lee Swindlehurst. "Robust Beamforming for Security in MIMO Wiretap Channels with Imperfect CSI". In: *IEEE Transactions on Signal Processing* 59.1 (Jan. 2011), pp. 351–361.

[NG05] Rohit Negi and Satashu Goel. "Secret Communication using Artificial Noise". In: *Proc. of Vehicular Technology Conference (VTC)*. 2005.

[PB05] Patricio Parada and Richard E. Blahut. "Secrecy Capacity of SIMO and Slow Fading Channels". In: *Proc. of IEEE International Symposium on Information Theory (ISIT)*. 2005.

[Pfe+14] Stefan Pfennig, Elke Franz, Sabrina Engelmann, and Anne Wolf. "End-to-End Key Establishment using Physical Layer Key Generation with Specific Attacker Models". In: *Proc. of Workshop on Communication Security (WCS)*. 2014.

[Pro00] John G. Proakis. *Digital Communications*. Fourth edition. McGraw-Hill, 2000.

[Ric+13] Johannes Richter, Elke Franz, Sabrina Engelmann, Stefan Pfennig, and Eduard A. Jorswieck. "Physical Layer Security vs. Network Layer Secrecy: Who Wins on the Untrusted Two-Way Relay Channel?" In: *Proc. of International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD)*. 2013.

[Ric+15] Johannes Richter, Christian Scheunert, Sabrina Engelmann, and Eduard A. Jorswieck. "Secrecy in the Two-Way Relay Channel with Compute-and-Forward". In: *Proc. of IEEE Communications Theory Symposium (ICC)*. 2015.

[SLU09] Shabnam Shafiee, Nan Liu, and Sennur Ulukus. "Towards the Secrecy Capacity of the Gaussian MIMO Wire-Tap Channel: The 2-2-1 Channel". In: *IEEE Transactions on Information Theory* 55.9 (Sept. 2009), pp. 4033–4039.

[SU07] Shabnam Shafiee and Sennur Ulukus. "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints". In: *Proc. of IEEE International Symposium on Information Theory (ISIT)*. 2007.

[Sha49] Claude E. Shannon. "Communication Theory of Secrecy Systems". In: *Bell Systems Technical Journal* 28 (1949), pp. 656–715.

[SBZ10] Yin Sun, Árpád Baricz, and Shidong Zhou. "On the Monotonicity, Log-Concavity, and Tight Bounds of the Generalized Marcum and Nuttall Q-Functions". In: *IEEE Transactions on Information Theory* 56.3 (Mar. 2010), pp. 1166–1186.

[Tan+08] Xiaojun Tang, Ruoheng Liu, Predrag Spasojević, and H. Vincent Poor. "Interference Assisted Secret Communication". In: *Proc. of Information Theory Workshop (ITW)*. 2008.

[TV08] David N. C. Tse and Pramod Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2008.

[WJ10a] Anne Wolf and Eduard A. Jorswieck. "Maximization of Worst-Case Secrecy Rates in MIMO Wiretap Channels". In: *Proc. of the Asilomar Conference on Signals, Systems, and Computers*. 2010.

[WJ10b] Anne Wolf and Eduard A. Jorswieck. "On the Zero Forcing Optimality for Friendly Jamming in MISO Wiretap Channels". In: *Proc. of IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. 2010.

[Wyn75] Aaron D. Wyner. "The Wire-tap Channel". In: *Bell Systems Technical Journal* 54.8 (1975), pp. 1355–1387.

[YE11] Melda Yuksel and Elza Erkip. "Diversity-Multiplexing Tradeoff for the Multiple-Antenna Wire-tap Channel". In: *IEEE Transactions on Wireless Communications* 10.3 (Mar. 2011), pp. 901–915.

[ZWN08] Gan Zheng, Kai-Kit Wong, and Tung-Sang Ng. "Robust Linear MIMO in the Downlink: A Worst-Case Optimization with Ellipsoidal Uncertainty Regions". In: *EURASIP Journal on Advances in Signal Processing* 2008.1 (2008).

[ZM09] Xiangyun Zhou and Matthew R. McKay. "Physical Layer Security with Artificial Noise: Secrecy Capacity and Optimal Power Allocation". In: *Proc. of International Conference on Signal Processing and Communication Systems (ICSPCS)*. 2009.