20

Secrecy on the Physical Layer in Wireless Networks

Eduard A. Jorswieck, Anne Wolf, and Sabrina Gerbracht*
Technische Universität Dresden
Germany

1. Introduction

This chapter provides a comprehensive state-of-the-art description of the emerging field of physical layer security. We will consider wireless security from an information theoretic view, which allows us to talk about provable secrecy and to derive ultimate secrecy limits. Our main focus is on the optimization of transmit strategies and resource allocation schemes under secrecy constraints.

We will consider the following scenario, which is illustrated in Figure 1: Alice wants to send a private message to Bob, which should be kept perfectly secret from Eve. Eve listens and tries to decode the message that Alice sends to Bob.

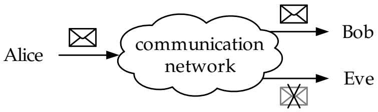


Fig. 1. Communication system with a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve).

In this communication system, Alice is the transmitter, Bob is the intended or legitimate receiver, and Eve is the eavesdropper. We assume that Bob and Eve perfectly know their individual channel realization and that Alice has full channel state information (CSI), i.e., she knows all channel realizations perfectly. This assumption, which is essential for our further discussion, seems to be unrealistic in the wiretap setting in which Eve probably only listens. However, this assumption will be justified, if Bob and Eve are both users in a cellular environment using up- and downlink transmission.

Within this chapter, we give an overview on the research problems and current results concerning secrecy on the physical layer. In the first section, we describe the attacker model and some conventional cryptographic methods. Afterwards, we introduce the wiretap channel and define the secrecy on the physical layer. In the second part of the chapter, we present results for the achievable secrecy rates or the secrecy capacity in various single-user systems including single-antenna, multi-antenna and multi-carrier systems and provide power allocation strategies for secrecy rate optimizations. In the third section, we extend these results to

*Part of this work is supported by DFG under grant Jo 801/2-1.

multi-user systems. We study basic elements that can be used to model more complex networks and give an overview on current research results on the secrecy capacity regions or the secrecy rate regions. The chapter is completed with a discussion of the results and open research problems.

1.1 Attacker Model

We consider a wireless communication system and focus on a cellular system. The transmitter has perfect CSI for the channels to all potential receivers, irrespective of the fact, whether the receiver is a legitimate receiver or an eavesdropper. The receivers only know their own channels perfectly using channel estimation based on pilot signals. Every user of the system has knowledge of the structure of the system, including all technical details, e.g., codebooks and transmit strategies.

system	• wireless communication (cellular system)
transmitter	
knowledge?	• perfect CSI for the channels to both, the legitimate receiver and the eavesdropper • structure of the system (including all technical details, e.g., codebooks and transmit strategies)
legitimate receiver	
knowledge?	• only perfect CSI for his own channel • structure of the system (including all technical details, e.g., codebooks and transmit strategies)
eavesdropper	
who?	• member of the system
objective?	• passive attack, eavesdrops the communication between transmitter and legitimate receiver, undermines confidentiality of communication (without interfering)
how?	• within range of transmitter • tries to decode the intercepted message
knowledge?	• only perfect CSI for his own channel • structure of the system (including all technical details, e.g., codebooks and transmit strategies)

Table 1. Attacker model at a glance.

The attacker is a passive attacker. He wants to undermine the confidentiality by eavesdropping the communication of one or more legitimate users of the system without interfering the communication between transmitter and receivers. For this reason, we use the terms attacker and eavesdropper synonymously. The attacker himself is also a user of the system. He is in reach of the transmitter and tries to decode the intercepted message. He has perfect CSI for the channel from the transmitter to himself, but he does not know the channel between the transmitter and the legitimate receiver. Since the eavesdropper is a user of the system, the transmitter knows the channel to the attacker and is able to fend the attack.
An overview of all important facts of the attacker model can be found in Table 1.

1.2 Cryptography

Currently, the mostly used method to ensure confidentiality in communication systems is the end-to-end cryptography (Schneier, 1996). What all cryptographic algorithms have in common is the fundamental attacker model. The sender, namely Alice, wants to send a message to the receiver, called Bob. Eve, the eavesdropper, should not obtain any knowledge of the message content. In order to achieve this, Alice performs a number of mathematical operations on the original message, predetermined by the cryptographic algorithm and the encryption key. Bob, who knows which algorithm was used, decrypts the cipher message with his key. Eve may know the algorithm, but as long as she does not know the key, it is difficult for her to decipher the message.

There are two basic concepts in the field of cryptography, the symmetric and the asymmetric cryptography. One of the main differences between both concepts is located in the key management.

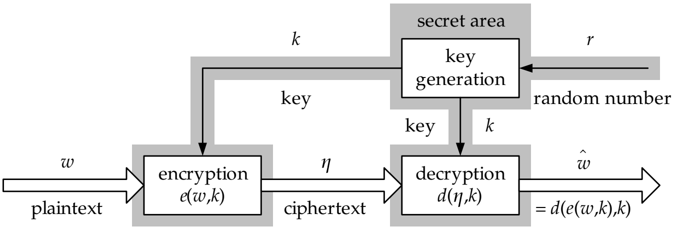


Fig. 2. The basic concept of symmetric cryptography, including key generation, key management, encryption and decryption.

The classical method of symmetric cryptography requires identical keys at sender and receiver, as it can be seen in Figure 2. The difficulty is to transmit the key from Alice to Bob (or vice versa) in a secure and secret way before the communication. In order to avoid this problem, Whitfield Diffie and Martin Hellman invented in 1976 the basic principles of asymmetric cryptography, also called public-key cryptography (Diffie & Hellman, 1976). Diffie and Hellman implemented a key exchange protocol. The first real cryptographic algorithm was designed by Ronald L. Rivest, Adi Shamir, and Leonard Adleman in 1977 at the Massachusetts Institute of Technology (MIT), named RSA by the initial letters of the three inventors (Rivest et al., 1978).

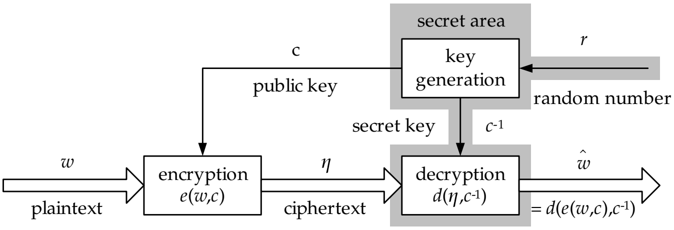


Fig. 3. The basic concept of asymmetric cryptography, including key generation, key management, encryption and decryption.

As the name public-key cryptography suggests, Alice und Bob do not share the same key anymore. Figure 3 shows that Bob initially generates a key pair consisting of a public key and a private key. Alice, and everyone else, can now encrypt a message, which she would like to send to Bob, with the published key, whereas only Bob is able to decrypt the ciphertext with his private key that he has kept secret. Because of this concept, it is not longer necessary to exchange the encryption key secretly.

Today, we mostly use a mixture of these both concepts. The main message is encrypted by a symmetric encryption algorithm, whereas the symmetric key is enciphered by public-key cryptography. By this method, we can combine the advantages of both concepts: the fast computable encryption and decryption of the symmetric cryptography with the very simple key management of the asymmetric cryptography.

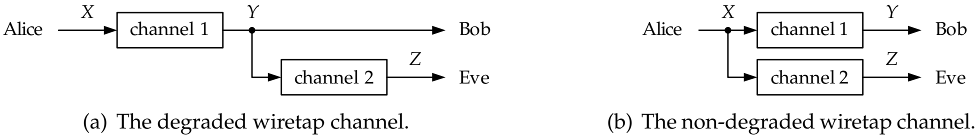
Since all cryptographic algorithms are assigned to the application layer, it is in the user's hand to ensure the secrecy of his data. In this chapter we want to present a possibility to enhance the security of the transmitted information without the requirement of cryptographic protocols and the engagement of the user. This type of secrecy is realized on the physical layer.

1.3 Notation

We use the following mathematical notations throughout the chapter:

- $[\cdot]^+ = \max(0, \cdot)$.
- $\boldsymbol{A}^\dagger$ is the adjoint matrix of the matrix $\boldsymbol{A}$, i.e., the conjugate transpose matrix of $\boldsymbol{A}$.
- $\boldsymbol{A} \succeq 0$ means that the matrix $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ is positive semidefinite, where we use the following definition for positive semidefiniteness, which automatically implies that $\boldsymbol{A}$ is Hermitian: $\boldsymbol{z}^\dagger \boldsymbol{A} \boldsymbol{z}$ is real and $\boldsymbol{z}^\dagger \boldsymbol{A} \boldsymbol{z} \geq 0$ for all complex vectors $\boldsymbol{z} \in \mathbb{C}^n$.
- $|x|$ is the absolute value of a (complex) variable x.
- $\|\boldsymbol{x}\|$ is the Euclidean norm of a (real or complex) vector $\boldsymbol{x}$ with $\|\boldsymbol{x}\| = \sqrt{\boldsymbol{x}^\dagger \boldsymbol{x}} = \sqrt{\sum_{i=1}^n |x_i|^2}$, if we assume a vector of length n.
- Vectors and matrices are denoted by lower and upper case bold symbols, respectively.
- Vectors are column vectors if not stated otherwise.

1.4 The Wiretap Channel



(a) The degraded wiretap channel. (b) The non-degraded wiretap channel.

Fig. 4. Two models for the wiretap channel.

The first important results in this research area were presented by Wyner and by Csiszár and Körner. They provided the theoretical basis and introduced two basic system models that are still used today: the wiretap channel (Wyner, 1975), which was later referred to as degraded wiretap channel, and the non-degraded wiretap channel (Csiszár & Körner, 1978). Both system models are depicted in Figure 4.

From a system theoretic view, the models are characterized by random variables at the channel inputs and channel outputs. For the channel input of channel 1 (Alice), we use the random variable X. The channel output of channel 1 (Bob) and channel 2 (Eve) are referred to as Y and Z, respectively. The corresponding channel input or output alphabets are written as $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$.

In Wyner's degraded wiretap channel, Bob receives a signal that was transmitted over channel 1, the so-called main channel, whereas Eve observes a signal that was additionally sent over channel 2, the so-called wiretapper channel. Therefore, Eve's received signal is always a degraded or noisier version of Bob's received signal, i.e., the random variables form a markov chain $X \rightarrow Y \rightarrow Z$. This fact simplifies the analysis and derivation of ultimate secrecy limits in Wyner's model compared to the model of Csiszár and Körner. In the non-degraded wiretap channel of Csiszár and Körner, the channels to Bob and Eve are supposed to be independent from each other. In principle, this model does not allow a statement, which channel is the better one. However, it is more suitable for the discussion of secrecy in mobile communication systems.

1.5 Secrecy on the Physical Layer from an Information Theoretic View

From an information theoretic view, the system can be characterized as follows. A message from the message set $\mathcal{W} = \{1, 2, \ldots, M\}$ with $M = 2^{n\,R_S}$ is to be transmitted in n channel uses while ensuring information theoretic security. The messages are chosen at random and thus are modeled by a random variable W with alphabet $\mathcal{W}$. Then, the message is encoded by the encoding function

$$f_{\text{enc}}: \quad \mathcal{W} \rightarrow \mathcal{X}^n, \quad w \mapsto \boldsymbol{x}^{(n)},$$

which takes the channel state information at the transmitter into account. Since the messages are random, the input to the channel is random too, and is modeled by the random vector $\boldsymbol{X}^{(n)}$. The output of the channel at the legitimate receiver is denoted by $\boldsymbol{Y}^{(n)}$. It is decoded by the decoding function

$$f_{\text{dec}}: \quad \mathcal{Y}^n \rightarrow \mathcal{W}, \quad \boldsymbol{y}^{(n)} \mapsto \hat{w},$$

which takes the channel state information at the receiver into account. An (M, n)-code comprises a message set $\mathcal{W}$, an encoding function f_{enc} and a decoding function f_{dec}.
The average decoding error probability $P_e^{(n)}$ of such a code is defined as

$$P_e^{(n)} = \frac{1}{M} \sum_{w=1}^{M} \Pr(f_{\text{dec}}(\boldsymbol{Y}^{(n)}) \neq w \,|\, \boldsymbol{X}^{(n)} = f_{\text{enc}}(w)),$$

which is the real decoding error probability, if the messages are uniformly distributed.
The level of secrecy is measured by the uncertainty of Eve about the message W, which was sent by Alice, under the condition that Eve receives $\boldsymbol{Z}^{(n)}$. This measure is called equivocation rate and is given with the conditional entropy function H by

$$R_e^{(n)} = \frac{1}{n} H(W|\boldsymbol{Z}^{(n)}). \tag{1}$$

We are interested in secure data transmissions with an achievable secrecy rate R_S. A secrecy rate R_S is said to be achievable over the wiretap channel if for any $\epsilon > 0$, there exists an integer $n(\epsilon)$ and a sequence of (M, n)-codes of rate

$$R_S = \frac{1}{n} \log_2 M, \tag{2}$$

such that for all $n \geq n(\epsilon)$, the average decoding error probability becomes arbitrarily small, i.e.,

$$P_e^{(n)} \leq \epsilon, \tag{3}$$

and the security constraint

$$\frac{1}{n} H(W|\boldsymbol{Z}^{(n)}) \geq R_S - \epsilon \tag{4}$$

is fulfilled.

For perfect secrecy, i.e., $\epsilon = 0$, the secrecy capacity C_S is the supremum of all achievable rates that guarantee the secrecy of the transmitted data. This means, it can be proven that it is the tightest upper bound on the amount of information that can be reliably transmitted to the receiver and perfectly kept secret from the eavesdropper.

By now, we only focus on Gaussian wiretap channels and Gaussian wiretap channels with an additional attenuation of the transmit signal. For the degraded Gaussian wiretap channel, which was introduced by (Leung-Yan-Cheong & Hellman, 1978) and whose structure is equal to that of Wyner's wiretap channel (cf. Figure 4), the secrecy capacity is given by the maximum difference of mutual informations:

$$C_S = \max_{f_X \in \mathcal{F}} \big[I(X;Y) - I(X;Z) \big], \tag{5}$$

where $\mathcal{F}$ is the set of all probability density functions (pdfs) at the channel input under power constraint at the transmitter. Since Eve always receives a degraded version of Bob's signal, the secrecy capacity in (5) is always non-negative. For the non-degraded Gaussian wiretap channel, which is structured like the model of Csiszár and Körner (cf. Figure 4), the secrecy capacity is given by a slightly modified term:

$$C_S = \max_{f_X \in \mathcal{F}} \big[I(X;Y) - I(X;Z) \big]^+, \tag{6}$$

i.e., the secrecy capacity C_S is set to zero, if Eve has a better channel realization than Bob. In the following, we will use the non-degraded system model, if it is not stated otherwise. The mutual information terms $I(X;Y)$ and $I(X;Z)$ are concave in f_X. This allows us to formulate a lower bound R_S for the secrecy capacity C_S:

$$C_S = \max_{f_X \in \mathcal{F}} \big[I(X;Y) - I(X;Z) \big]^+ \geq \Big[\underbrace{\max_{f_X \in \mathcal{F}} (I(X;Y))}_{\substack{\text{channel capacity} \\ \text{from Alice to Bob}}} - \underbrace{\max_{f_X \in \mathcal{F}} (I(X;Z))}_{\substack{\text{channel capacity} \\ \text{from Alice to Eve}}} \Big]^+ = R_S. \tag{7}$$

Note that the secrecy rate R_S is defined with the difference of the channel capacities from Alice to Bob and from Alice to Eve. This lower bound R_S is often used for a simplified calculation of achievable secrecy rates since it is known how to maximize the mutual information terms. For some scenarios, it has already been proven that the secrecy rate R_S equals the secrecy capacity C_S, e.g., for the single-user system with multiple antennas (see Section 2.3) or for the MISO and MIMO broadcast channel (see Section 3.1).

1.6 The Basic System Model and Preliminaries

Now, we consider Gaussian channels with an additional attenuation of the transmit signal. As a basis for all system models, which are used throughout this chapter, we introduce the following system model for each channel use:

$$\begin{aligned} y &= h \cdot x + \phi \quad \text{and} \\ z &= g \cdot x + \psi \end{aligned} \tag{8}$$

with Alice' transmit signal x, channel coefficients h and g to model the signal attenuation for the channels from Alice to Bob and from Alice to Eve, additive white Gaussian noise ϕ and ψ and signals y and z at the receivers of Bob and Eve, respectively. Figure 5 illustrates how the basic system model is independently used n times to transmit the codeword of length n that is chosen for the message.

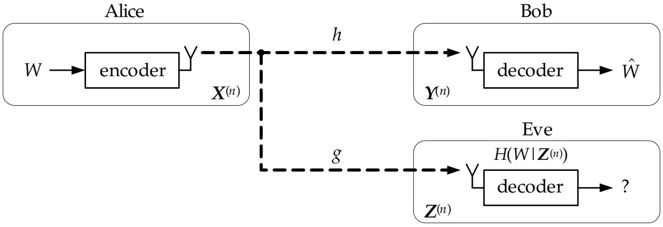


Fig. 5. The basic system model.

For the system model, we make the following assumptions:

- The variables ϕ, ψ and x are stochastically independent.
- The noise variables ϕ and ψ are circular symmetric complex Gaussian distributed with zero mean and variance σ^2. We write $\phi, \psi \sim \mathcal{CN}(0, \sigma^2)$.
- At the transmitter, we have a power constraint P, i.e., for a codeword x of length n

$$\frac{1}{n} \sum_{i=1}^{n} |x_i|^2 \leq P. \tag{9}$$

  In order to achieve the channel capacities in (7), the variable x has to be circular symmetric complex Gaussian distributed with zero mean and variance P. We write $x \sim \mathcal{CN}(0, P)$.
- We define the so called channel gains α and β by

$$\alpha = |h|^2 \quad \text{and} \quad \beta = |g|^2. \tag{10}$$

In this model, Bob's and Eve's signal-to-noise ratio (SNR) is given by $\frac{\alpha P}{\sigma^2}$ and $\frac{\beta P}{\sigma^2}$, respectively. Therewith, the secrecy rate R_S can be quantified in bit per complex symbol (bpcs) and expressed as a function of the transmit power constraint P:

$$R_S(P) = \left[\log_2\left(1 + \frac{\alpha P}{\sigma^2}\right) - \log_2\left(1 + \frac{\beta P}{\sigma^2}\right)\right]^+ \quad \text{[bpcs]}, \tag{11}$$

where a Gaussian codebook maximizes both mutual information terms in (7). This is the secrecy rate of the non-degraded Gaussian wiretap channel with channel gains α and β.

Based on the model above, we define a system with slow quasi-static block flat fading. In order to model flat fading, the channel coefficients h and g in (8) become random variables, which we call channel states. We assume slow quasi-static block fading, i.e., the channel states are random but remain constant for a sufficiently long time to transmit a whole codeword. The next channel state is independent of all other channel states before and is identically distributed.

For every channel state, the secrecy rate can be calculated according to (11). Therefore, the secrecy rate is called instantaneous secrecy rate. Depending on the statistics assumed for the channel coefficients, we can calculate average or outage secrecy rates as defined in (Bloch et al., 2008). In the following sections, we present instantaneous secrecy rates for given channel coefficients and average secrecy rates, where we make the following assumptions for the distribution of the channel states: The channel coefficients h and g are stochastically independent of each other, the transmit signal, and the noise variables. They are circular symmetric complex Gaussian distributed with zero mean and variance 1. We write $h, g \sim \mathcal{CN}(0, 1)$. This means, we add Rayleigh fading to the Gaussian wiretap channel.

The interesting observation in (Bloch et al., 2008) for wiretapped fading channels is that even if the average channel quality between transmitter and eavesdropper is better than the average channel between transmitter and intended receiver, the average secrecy capacity can still be positive.

1.7 Extension to a Multi-Carrier or a Multi-Antenna System Model

The system model in Section 1.6 can be extended to a multi-carrier or a multi-antenna system model:

- For an ideal multi-carrier system with L carriers, the system model in (8) is used L times in parallel. For each carrier ℓ, we have the same assumptions and the same relations between the variables as listed in Section 1.6. Besides, the transmit signals and the noise variables are assumed to be independent between the L carriers. For corresponding variables, we assume an identical distribution. If we assume random channel coefficients, the L parallel channel coefficients for the channels from Alice to Bob are correlated in general. The same applies to the L parallel channel coefficients for the channels from Alice to Eve. The power constraint P at the transmitter becomes a sum power constraint over all L carriers, i.e., $\sum_{\ell=1}^{L} P_\ell = P$.
- In multi-antenna (muliple-input multiple-output, MIMO) systems, we assume that Alice has m_A transmit antennas, Bob has m_B receive antennas, and Eve has m_E receive antennas. Then, the system model in Section 1.6 is expanded by using vectors and matrices instead of scalars. The assumptions and relations between the variables mentioned in this context in Section 1.6 are still valid or can be formulated analogously. Each noise vector consists of independent and identically distributed components. However, the channels from Alice to Bob can be spatially correlated. The same applies to the channels from Alice to Eve. The power constraint P at the transmitter becomes a sum power constraint over all antennas, which is written as $\mathrm{trace}(\boldsymbol{Q}) = P$ with the covariance matrix $\boldsymbol{Q}$ of the transmit signal vector $\boldsymbol{x}$.

In the multi-carrier or multi-antenna scenario, Alice has more degrees of freedom than before. Now, she can variate the power allocation (under the sum power constraint) over L carriers or m_A antennas to achieve a high secrecy rate for the data transmission to Bob. Note that both models can be combined to have a MIMO multi-carrier system. In the following parts of

Section 2, we will derive an optimal power allocation that maximizes the achievable secrecy rate to Bob for multi-carrier or multi-antenna scenarios.

The channel capacities, which we use in the secrecy rate formula in (11) or in secrecy rate expressions derived from it, are concave functions in P or $\boldsymbol{Q}$. But the difference of two concave functions generally is neither convex nor concave. Therefore, finding the optimal power allocation over L carriers or m_A antennas under a sum power constraint is a difficult, non-convex optimization problem.

1.8 Extension to a Multi-User Scenario

So far, we have considered a single-user scenario, where Alice wants to transmit a private message to Bob, and Eve is a passive eavesdropper who wants to decode this message. Now, we want to introduce a multi-user scenario with one transmitter (Alice) and K receivers. Alice wants to transmit private messages to each of the K users and to keep these messages secret from all other users. In such a system, we have K secrecy rates or a K-dimensional secrecy rate region. In this chapter, we will confine ourselves to the 2-user scenario with the receivers Bob and Eve, who are now both: legitimate receiver of one message and potential eavesdropper of the other.

In some multi-user scenarios that we present in Section 3, the signals for the different users can interfere. For the evaluation of the achievable secrecy rates for the 2-user case, we slightly modify the definition of the secrecy rate in (7). For the individual secrecy rates, we use the signal-to-interference-and-noise ratio (SINR) for the legitimate user, where the complete interference from the other user's signal is simply treated as additional noise, and the signal-to-noise ratio (SNR) for the eavesdropper. Under power constraint $P_\mathrm{B} + P_\mathrm{E} = P$, Alice allocates power P_B and P_E for the data transmission to Bob and Eve, respectively. This results in the following expression for the achievable secrecy rate $R_{S\,\mathrm{B}}$ for the transmission to Bob:

$$R_{S\,\mathrm{B}}(P_\mathrm{B}, P_\mathrm{E}) = \left[\log_2\left(1 + \frac{\alpha P_\mathrm{B}}{\sigma^2 + \alpha P_\mathrm{E}}\right) - \log_2\left(1 + \frac{\beta P_\mathrm{B}}{\sigma^2}\right)\right]^+ \quad \text{[bpcs]}. \tag{12}$$

This is a worst-case assumption since we assume that Eve performs successive interference cancellation (SIC), i.e., first, she is able to detect her own data, afterwards she subtracts it from her received signal and tries to decode the message for Bob.

The achievable secrecy rate for the transmission to Eve can be formulated in the same way:

$$R_{S\,\mathrm{E}}(P_\mathrm{B}, P_\mathrm{E}) = \left[\log_2\left(1 + \frac{\beta P_\mathrm{E}}{\sigma^2 + \beta P_\mathrm{B}}\right) - \log_2\left(1 + \frac{\alpha P_\mathrm{E}}{\sigma^2}\right)\right]^+ \quad \text{[bpcs]}. \tag{13}$$

2. Secrecy Capacity in Single-User Systems

2.1 Single-Antenna Systems

For a single-user single-antenna system, we have already presented the secrecy rate in Section 1.6. For this single-input single-output (SISO) system, the secrecy rate given in (11) is exactly the secrecy capacity given in (6). In this scenario, Alice only has the choice to transmit the message to Bob or not, according to the channel coefficients for the channels to Bob and Eve. In a completely static system, this would result in a constant secrecy rate that is either positive or zero all the time. But in a time-varying system where we assume slow quasi-static block flat fading, the situation changes from block to block: we have instantaneous channel realizations and thus instantaneous secrecy rates, which can be averaged in time.

2.2 Multi-Carrier Systems

In this section, we extend the basic model from Section 1.6 to the multi-carrier wiretap channel, where Alice wants to send a private message to Bob in a system with L parallel carriers. This message should be kept secret from the eavesdropper Eve. This is a single-antenna scenario since every member of the system has only one transmit or receive antenna. We study the resource allocation under the secrecy constraint and a sum power constraint over all carriers.

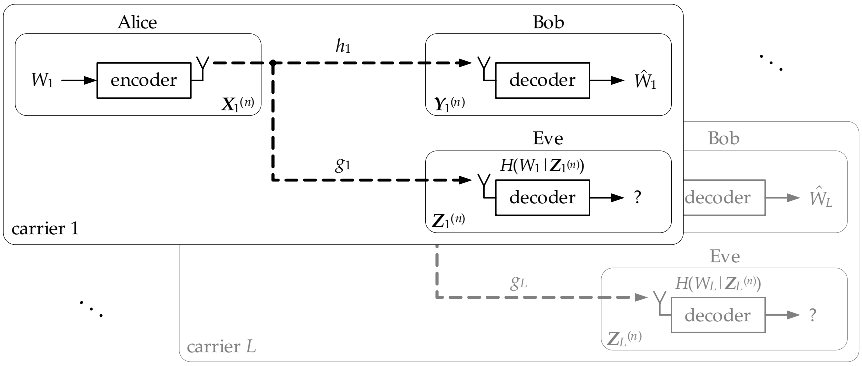


Fig. 6. The multi-carrier wiretap channel with L carriers.

The system model is modified as described in Section 1.7 and illustrated in Figure 6. On carrier ℓ with $1 \leq \ell \leq L$, Bob and Eve observe the received signals y_ℓ and z_ℓ, respectively:

$$\begin{aligned} y_\ell &= h_\ell x_\ell + \phi_\ell \quad \text{and} \\ z_\ell &= g_\ell x_\ell + \psi_\ell \end{aligned} \tag{14}$$

with Alice' transmit signal x_ℓ, channel coefficients h_ℓ, g_ℓ, and noise variables ϕ_ℓ and ψ_ℓ. The assumptions listed for the basic system model in Section 1.6 also apply to this model. The channel gains α_ℓ, β_ℓ are defined according to equation (10).

In this multi-carrier system, the secrecy rate is the sum over all secrecy rates per carrier, which can be computed according to (7), and is given by

$$R_S(\boldsymbol{P}_\text{B}) = \sum_{\ell=1}^{L} \left[\log_2 \left(1 + \frac{\alpha_\ell P_{\text{B}\,\ell}}{\sigma^2} \right) - \log_2 \left(1 + \frac{\beta_\ell P_{\text{B}\,\ell}}{\sigma^2} \right) \right]^+ \quad \text{[bpcs]}, \tag{15}$$

where $P_{\text{B}\,\ell}$ is the power that Alice allocates to carrier ℓ in order to transmit the message to Bob. The power allocation over all carriers can be written in a vector $\boldsymbol{P}_\text{B} = (P_{\text{B}\,1}, \ldots, P_{\text{B}\,L})$.

We derive the single-user optimal power allocation for maximizing the secrecy rate in this multi-carrier system under sum power constraint P over all carriers:

$$\max_{\boldsymbol{P}_\text{B}} R_S(\boldsymbol{P}_\text{B}) \quad \text{subject to} \quad \sum_{\ell=1}^{L} P_{\text{B}\,\ell} \leq P \quad \text{and} \quad P_{\text{B}\,\ell} \geq 0. \tag{16}$$

This is a non-convex optimization problem with objective function R_S.

The optimal power allocation that solves (16) is to allocate zero power to all carriers with $\alpha_\ell \leq \beta_\ell$:

$$\forall\, \ell \in \{1, 2, \ldots, L\} : \quad \alpha_\ell \leq \beta_\ell \quad \Longrightarrow \quad P_{\text{B}\,\ell} = 0. \tag{17}$$

The proof is based on the necessary Karush-Kuhn-Tucker (KKT) optimality conditions (Jorswieck & Wolf, 2008). Furthermore, it was shown that the remaining optimization problem

$$\max_{\boldsymbol{P}_{\mathrm{B}}} R_S(\boldsymbol{P}_{\mathrm{B}}) \quad \text{subject to} \quad \sum_{\ell=1}^{L} P_{\mathrm{B}\,\ell} \leq P, \quad P_{\mathrm{B}\,\ell} \geq 0 \quad \text{and} \quad P_{\mathrm{B}\,\ell} = 0 \ \text{for}\ \alpha_\ell \leq \beta_\ell \tag{18}$$

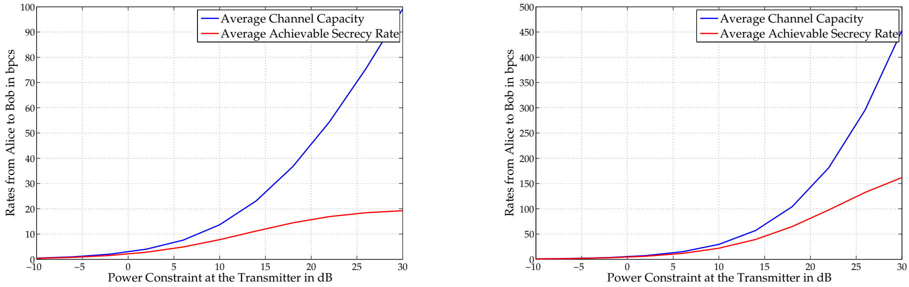
is convex (see (Boyd & Vandenberghe, 2004) for general convex optimization theory).
The optimal power allocation is a type of waterfilling (see (Cover & Thomas, 2006) for standard waterfilling). We give the solution in implicit form with

$$P_{\mathrm{B}\,\ell} = \begin{cases} 0 & \text{if } \alpha_\ell \leq \beta_\ell \\ \left[-\frac{\sigma^2(\alpha_\ell+\beta_\ell)}{2\alpha_\ell\beta_\ell} + \sqrt{\frac{\sigma^4(\alpha_\ell-\beta_\ell)^2}{4(\alpha_\ell\beta_\ell)^2} + \frac{1}{\mu}\frac{\sigma^2(\alpha_\ell-\beta_\ell)}{\ln(2)\alpha_\ell\beta_\ell}} \right]^+ & \text{otherwise} \end{cases} \tag{19}$$

and $\mu > 0$ such that

$$\sum_{\ell=1}^{L} P_{\mathrm{B}\,\ell} = P. \tag{20}$$

However, the typical order of the channels is different from standard waterfilling. For small SNR, the carriers are ordered according to $(\alpha_\ell - \beta_\ell)$, i.e., the carrier with largest $(\alpha_\ell - \beta_\ell)$ is supported first, whereas for high SNR, the carriers are ordered according to $\frac{\alpha_\ell}{\beta_\ell}$.



(a) 20 carriers

(b) 200 carriers

Fig. 7. Average channel capacities and average achievable secrecy rates for transmission from Alice to Bob in a multi-carrier system with 20 and 200 independent carriers.

In Figure 7, we compare the average achievable secrecy rate with the average channel capacity of the single-user multi-carrier channel for different numbers of carriers. The main observation is that the high SNR channel capacity grows without bound whereas the secrecy rate is bounded because the mutual information between the transmitter and the eavesdropper is subtracted from the rate. If the number of carriers is increased, the asymptotic behavior will remain the same. However, the high SNR bound is shifted to the right. We see that in multi-carrier systems with a large number of carriers (and corresponding multipath fading), the costs of security are decreased, i.e., the high SNR bound is increased.

2.3 Multi-Antenna Systems

In this section, we extend the basic model from Section 1.6 to the multi-antenna wiretap channel. As in the scenarios above, Alice wants to send a private message to Bob, which should be kept secret from the eavesdropper Eve. Now, we consider a multi-antenna system, where Alice has m_A transmit antennas, Bob and Eve have m_B and m_E receive antennas, respectively. We study the resource allocation under the secrecy constraint and a sum power constraint over all transmit antennas.

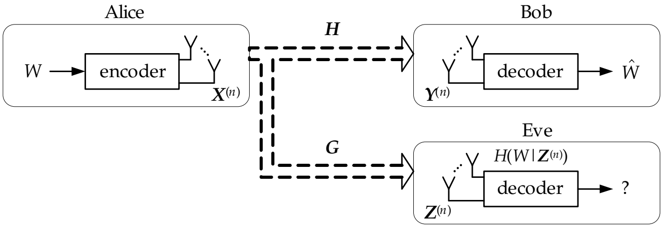
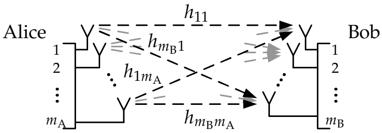


Fig. 8. The multi-antenna wiretap channel.



$$\boldsymbol{H} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1m_\mathrm{A}} \\ h_{21} & h_{22} & \dots & h_{2m_\mathrm{A}} \\ \vdots & \vdots & \ddots & \vdots \\ h_{m_\mathrm{B}1} & h_{m_\mathrm{B}2} & \dots & h_{m_\mathrm{B}m_\mathrm{A}} \end{pmatrix}$$

Fig. 9. The structure of a channel matrix using the example of channel matrix $\boldsymbol{H}$ for the channels from Alice to Bob.

The system model, which is depicted in Figure 8, is modified as described in Section 1.7. It can be described by

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{H} \cdot \boldsymbol{x} + \boldsymbol{\phi} \quad \text{and} \\ \boldsymbol{z} &= \boldsymbol{G} \cdot \boldsymbol{x} + \boldsymbol{\psi}. \end{aligned} \tag{21}$$

The complex channel coefficients are written as the components of $\boldsymbol{H}$ and $\boldsymbol{G}$, which are channel matrices of dimension $[m_\mathrm{B} \times m_\mathrm{A}]$ and $[m_\mathrm{E} \times m_\mathrm{A}]$, respectively. Figure 9 illustrates the structure of such a channel matrix. Alice' transmit signals are written in a column vector $\boldsymbol{x}$ of dimension $[m_\mathrm{A} \times 1]$. The noise variables $\boldsymbol{\phi}$ and $\boldsymbol{\psi}$ are column vectors of dimension $[m_\mathrm{B} \times 1]$ and $[m_\mathrm{E} \times 1]$, respectively, with independent components. Bob's and Eve's received signals $\boldsymbol{y}$ and $\boldsymbol{z}$ are column vectors of dimension $[m_\mathrm{B} \times 1]$ and $[m_\mathrm{E} \times 1]$, respectively. The assumptions listed for the basic system model in Section 1.6 analogously apply to this model. The transmit vector $\boldsymbol{x}$, and the noise vectors $\boldsymbol{\phi}$ and $\boldsymbol{\psi}$ are stochastically independent, i.e., the components of one vector are stochastically independent of the components of the other vectors. The noise vectors are composed of independent and circular symmetric complex Gaussian distributed components. Their covariance matrices are normalized to the identity matrix. For fading scenarios, the channel matrices $\boldsymbol{H}$ and $\boldsymbol{G}$ are assumed to be stochastically independent of each other, the transmit vector $\boldsymbol{x}$, and the noise vectors $\boldsymbol{\phi}$ and $\boldsymbol{\psi}$.

In this multi-antenna system, the secrecy rate, which is the secrecy capacity for this scenario (Oggier & Hassibi, 2008), is given by

$$R_S(\boldsymbol{Q}) = \Big[\log_2 \det(\boldsymbol{I}_{m_\mathrm{B}} + \boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^\dagger) - \log_2 \det(\boldsymbol{I}_{m_\mathrm{E}} + \boldsymbol{G}\boldsymbol{Q}\boldsymbol{G}^\dagger)\Big]^+ \quad \text{[bpcs].} \tag{22}$$

$\boldsymbol{I}_{m_\mathrm{B}}$ and $\boldsymbol{I}_{m_\mathrm{E}}$ are identity matrices of dimension $[m_\mathrm{B} \times m_\mathrm{B}]$ and $[m_\mathrm{E} \times m_\mathrm{E}]$, respectively. $\boldsymbol{Q}$ is the covariance matrix of the input signal vector $\boldsymbol{x}$, i.e., $\boldsymbol{Q} = \mathrm{Cov}\,(\boldsymbol{x}) = \mathbb{E}\left(\boldsymbol{x}\boldsymbol{x}^\dagger\right)$.
We derive the single-user optimal power allocation for maximizing the secrecy rate in this multi-antenna system under sum power constraint P over all transmit antennas:

$$\max_{\boldsymbol{Q}} R_S(\boldsymbol{Q}) \quad \text{subject to} \quad \mathrm{trace}(\boldsymbol{Q}) \leq P \quad \text{and} \quad \boldsymbol{Q} \succeq 0. \tag{23}$$

This is a non-convex optimization problem, which we analyze for some special cases.

Multiple-Input Single-Output (MISO) Systems

In the MISO case, where Bob and Eve have only one receive antenna each, the channel matrices $\boldsymbol{H}$ and $\boldsymbol{G}$ in (21) reduce to row vectors $\boldsymbol{h}$ and $\boldsymbol{g}$ of dimension $[1 \times m_\mathrm{A}]$:

$$\boldsymbol{h} = (h_1, \ldots, h_{m_\mathrm{A}}) \quad \text{and} \quad \boldsymbol{g} = (g_1, \ldots, g_{m_\mathrm{A}}). \tag{24}$$

The secrecy rate in (22) can be written as

$$R_S(\boldsymbol{Q}) = \Big[\log_2(1 + \boldsymbol{h}\boldsymbol{Q}\boldsymbol{h}^\dagger) - \log_2(1 + \boldsymbol{g}\boldsymbol{Q}\boldsymbol{g}^\dagger)\Big]^+ \quad \text{[bpcs].} \tag{25}$$

This scenario was analytically solved in (Li et al., 2007). The authors used an invertible coordinate transformation with a unitary transformation matrix

$$\boldsymbol{T} = \left(\frac{\boldsymbol{h}^\dagger}{\|\boldsymbol{h}\|}, \quad \frac{(\boldsymbol{g} - \frac{\|\boldsymbol{g}\|}{\|\boldsymbol{h}\|}\zeta\boldsymbol{h})^\dagger}{\|\boldsymbol{g}\|\sqrt{1-\zeta^\dagger\zeta}}, \quad \text{further } (m_\mathrm{A}-2) \text{ columns} \right) \quad \text{with} \quad \zeta = \frac{\boldsymbol{g}\boldsymbol{h}^\dagger}{\|\boldsymbol{g}\|\,\|\boldsymbol{h}\|}, \tag{26}$$

where the last $(m_\mathrm{A}-2)$ columns are an orthonormal basis for the $(m_\mathrm{A}-2)$ dimensions and orthogonal to the first two columns. Therewith, the transformed channel vectors $\boldsymbol{h}\,\boldsymbol{T}$ and $\boldsymbol{g}\,\boldsymbol{T}$ have zeros in the subspace spanned by the last $(m_\mathrm{A}-2)$ columns of $\boldsymbol{T}$. Focussing only on the subspace spanned by the first two columns of $\boldsymbol{T}$ the transformed channel vectors $\boldsymbol{h}\,\boldsymbol{T}$ and $\boldsymbol{g}\,\boldsymbol{T}$ can be represented by $\bar{\boldsymbol{h}}$ and $\bar{\boldsymbol{g}}$ with

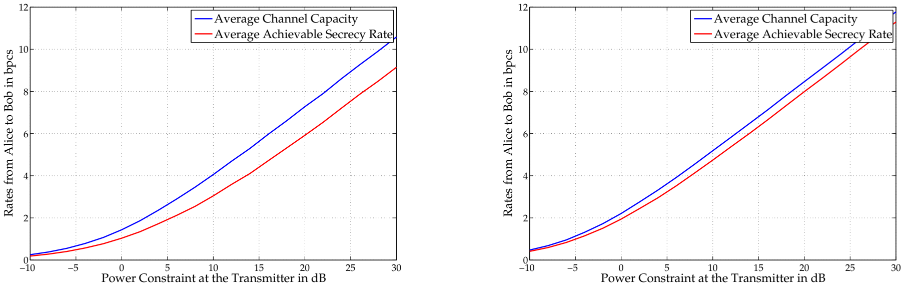
$$\bar{\boldsymbol{h}} = \|\boldsymbol{h}\|\,(1, 0) \quad \text{and} \quad \bar{\boldsymbol{g}} = \|\boldsymbol{g}\|\,(\zeta, \sqrt{1-\zeta^\dagger\zeta}). \tag{27}$$

In the transformed space, the covariance matrix with the optimal power allocation for the optimization problem derived from (23) for the MISO scenario is

$$\bar{\boldsymbol{Q}} = P\bar{\boldsymbol{q}}\bar{\boldsymbol{q}}^\dagger, \tag{28}$$

where $\bar{\boldsymbol{q}}$ is the generalized eigenvector corresponding to the largest generalized eigenvalue of the two matrices $(\boldsymbol{I}_2 + P\bar{\boldsymbol{h}}^\dagger\bar{\boldsymbol{h}})$ and $(\boldsymbol{I}_2 + P\bar{\boldsymbol{g}}^\dagger\bar{\boldsymbol{g}})$. The covariance matrix $\bar{\boldsymbol{Q}}$ has unit-rank, which means that only one data stream is supported at the transmitter and beamforming can be applied with vector $\bar{\boldsymbol{q}}$. Finally, the optimal covariance matrix $\boldsymbol{Q}$ in the orginal space is

obtained by adding zeros for the subspace spanned by the last $(m_{\mathrm{A}}-2)$ columns of $\boldsymbol{T}$ and the inverse coordinate transformation.
In Figure 10, the difference between the average achievable secrecy rate and the average channel capacity of the single-user MISO scenario is illustrated for different numbers of transmit antennas.



(a) Two transmit antennas

(b) Four transmit antennas

Fig. 10. Average channel capacities and average achievable secrecy rates in a MISO system with two and four transmit antennas and uncorrelated channels.

Single-Input Multiple-Output (SIMO) Systems

In the SIMO case, where Alice has only one transmit antenna and Bob and Eve have an arbitrary number of receive antennas, the channel matrices $\boldsymbol{H}$ and $\boldsymbol{G}$ in (21) reduce to column vectors of dimension $[m_{\mathrm{B}} \times 1]$ and $[m_{\mathrm{E}} \times 1]$, respectively:

$$\boldsymbol{h} = (h_1, \ldots, h_{m_{\mathrm{B}}})^{\mathrm{T}} \quad \text{and} \quad \boldsymbol{g} = (g_1, \ldots, g_{m_{\mathrm{E}}})^{\mathrm{T}}. \tag{29}$$

Similar to the single-antenna (SISO) case in Section 2.1, Alice has only the choice either to transmit the message to Bob with power P or not. This SIMO scenario can be transformed in an equivalent SISO scenario with modified channel statistics. Bob and Eve can apply matched filters at the receivers. In the equivalent SISO scenario, Bob's SNR is $\frac{\|\boldsymbol{h}\|^2 P}{\sigma^2}$ and Eve's SNR is $\frac{\|\boldsymbol{g}\|^2 P}{\sigma^2}$, where P is the transmit power constraint and σ^2 is the noise variance for each receive antenna.

Some Special Multiple-Input Multiple-Output (MIMO) Systems

In the MIMO 2-2-1 scenario, where Alice has two transmit antennas, Bob has two receive antennas, whereas Eve has only one single receive antenna, the channel matrices $\boldsymbol{H}$ and $\boldsymbol{G}$ in (21) reduce to a matrix $\boldsymbol{H}$ of dimension $[2 \times 2]$ and a row vector $\boldsymbol{g}$ of dimension $[1 \times 2]$. The optimization problem derived from (23) for the MIMO 2-2-1 scenario was analytically solved in (Shafiee et al., 2008). The authors transformed the problem into a Rayleigh quotient problem, whose solution is the optimal covariance matrix $\boldsymbol{Q}$:

$$\boldsymbol{Q} = P\boldsymbol{q}\boldsymbol{q}^{\dagger}, \tag{30}$$

where $\boldsymbol{q}$ is the eigenvector that corresponds to the largest eigenvalue of the matrix $(\boldsymbol{I}_2 + P\boldsymbol{g}^\dagger\boldsymbol{g})^{-1/2}(\boldsymbol{I}_2 + P\boldsymbol{H}^\dagger\boldsymbol{H})(\boldsymbol{I}_2 + P\boldsymbol{g}^\dagger\boldsymbol{g})^{-1/2}$.

For the general MIMO scenario, where each user can have an arbitrary number of antennas, it has been proven in (Oggier & Hassibi, 2008) that the secrecy rate in (22) is equal to the secrecy capacity of the system in (21).

In (Liu, Hou & Sherali, 2009), the authors presented a global optimization algorithm called branch-and-bound with reformulation and linearization technique (BB/RLT). This method guarantees finding a global optimal solution for the non-convex optimization problem in (23). Another characterization of the optimal transmit covariance matrix $\boldsymbol{Q}$ is derived in (Liu, Liu, Poor & Shamai (Shitz), 2009). This approach is discussed in the multi-user context in Section 3.1.

3. Secrecy Rate Region in Multi-User Systems

In this section, we extend some of the previously presented results to the multi-user case. Due to the fact that there is more than one user, we will not use anymore the terms secrecy rate and secrecy capacity, but secrecy rate region and secrecy capacity region.

In the literature, the case of one confidential (private) and one public message is often discussed. We focus on the case, where only confidential messages are sent. For convenience, we confine ourselves to systems with only two users. The extension to more than two users can be done straightforward.

3.1 Broadcast Channels

The broadcast channel (BC) is the logical extension of the basic system presented in Section 1.6 to the multi-user scenario. In this channel model, Alice additionally sends a message to Eve that should be concealed from Bob. This new system setting is shown in Figure 11.

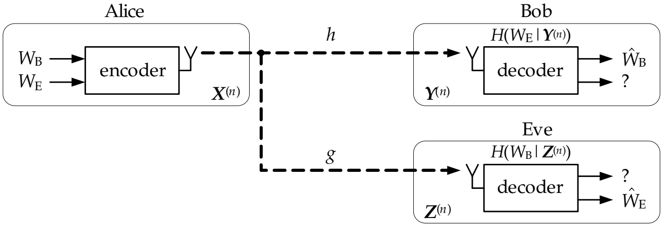


Fig. 11. The basic model of the broadcast channel with two confidential messages.

The extensions of the basic model discussed in Section 2 can also be applied to the broadcast channel. Based on the results of the single-user multi-carrier scenario in Section 2.2, we consider now a cellular broadcast channel with two users, namely Bob and Eve and reuse the system model shown in Figure 6.

The system model is equivalent to the model given in (14)

$$\begin{aligned} y_\ell &= h_\ell x_\ell + \phi_\ell \quad \text{and} \\ z_\ell &= g_\ell x_\ell + \psi_\ell, \end{aligned} \tag{31}$$

but now Bob and Eve eavesdrop each other. The assumptions listed in Section 1.6 also apply to this model. The channel gains α_ℓ and β_ℓ are defined according to (10).

On carrier ℓ, Alice allocates power $P_{\mathrm{B}\,\ell}$ for data transmission to Bob and $P_{\mathrm{E}\,\ell}$ for data transmission to Eve. The sum power constraint translates to

$$\sum_{\ell=1}^{L}(P_{\mathrm{B}\,\ell}+P_{\mathrm{E}\,\ell}) \leq P. \tag{32}$$

We collect the power allocation for Bob and Eve in appropriate vectors, i.e., $\boldsymbol{P}_{\mathrm{B}} = (P_{\mathrm{B}\,1},\ldots,P_{\mathrm{B}\,L})$ and $\boldsymbol{P}_{\mathrm{E}} = (P_{\mathrm{E}\,1},\ldots,P_{\mathrm{E}\,L})$.

The achievable secrecy rates per carrier are modified according to the explanations in Section 1.7 and 1.8. The achievable secrecy rates for data transmission to Bob and Eve are the sum over all secrecy rates per carrier and given by

$$\begin{aligned} R_{S\,\mathrm{B}}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}) &= \sum_{\ell=1}^{L}\left[\log_2\left(1+\frac{\alpha_\ell P_{\mathrm{B}\,\ell}}{\sigma^2+\alpha_\ell P_{\mathrm{E}\,\ell}}\right)-\log_2\left(1+\frac{\beta_\ell P_{\mathrm{B}\,\ell}}{\sigma^2}\right)\right]^+ \quad \text{[bpcs]} \quad \text{and} \\ R_{S\,\mathrm{E}}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}) &= \sum_{\ell=1}^{L}\left[\log_2\left(1+\frac{\beta_\ell P_{\mathrm{E}\,\ell}}{\sigma^2+\beta_\ell P_{\mathrm{B}\,\ell}}\right)-\log_2\left(1+\frac{\alpha_\ell P_{\mathrm{E}\,\ell}}{\sigma^2}\right)\right]^+ \quad \text{[bpcs]}. \end{aligned} \tag{33}$$

The system operator might be interested in the sum of the individual secrecy rates in (33). The sum secrecy rate is defined as

$$R_S^{(\mathrm{sum})}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}) = R_{S\,\mathrm{B}}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}) + R_{S\,\mathrm{E}}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}). \tag{34}$$

The corresponding programming problem maximizes the sum secrecy rate in (34):

$$\max_{\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}} R_S^{(\mathrm{sum})}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}) \quad \text{subject to} \quad \sum_{\ell=1}^{L}(P_{\mathrm{B}\,\ell}+P_{\mathrm{E}\,\ell}) \leq P, \quad P_{\mathrm{B}\,\ell} \geq 0 \quad \text{and} \quad P_{\mathrm{E}\,\ell} \geq 0. \tag{35}$$

In (Jorswieck & Wolf, 2008), it was shown that it is optimal to support only the best user per carrier. From that fact and the power constraint $P_{\mathrm{A}\,\ell} = P_{\mathrm{B}\,\ell} + P_{\mathrm{E}\,\ell}$ per carrier follows the user allocation per carrier, which is

$$P_{\mathrm{B}\,\ell} = \begin{cases} P_{\mathrm{A}\,\ell} & \text{if } \alpha_\ell > \beta_\ell \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad P_{\mathrm{E}\,\ell} = \begin{cases} 0 & \text{if } \alpha_\ell \geq \beta_\ell \\ P_{\mathrm{A}\,\ell} & \text{otherwise} \end{cases}. \tag{36}$$

Then, the power allocation per carrier is derived from equation (19) by replacing $(\alpha_\ell - \beta_\ell)$ by $(\max(\alpha_\ell,\beta_\ell) - \min(\alpha_\ell,\beta_\ell))$.

Note that the case $\alpha_\ell = \beta_\ell$ can be ignored in the fading scenario, if we assume a continuous distribution for the channel coefficients and hence the channel gains, since $\Pr(\alpha_\ell = \beta_\ell) = 0$. Moreover, for the spectral power allocation in (19), it is all the same, which user is assumed to be supported. The algorithm allocates zero power to this carrier and therefore the secrecy rate on this carrier will be zero.

The previously described sum secrecy rate maximization for the broadcast channel can be easily extended to the weighted sum secrecy rate maximization as discussed in (Jorswieck & Gerbracht, 2009). The weighted sum secrecy rate is given by

$$R_S^{(\mathrm{wsum})}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}},\lambda) = \lambda R_{S\,\mathrm{B}}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}) + (1-\lambda) R_{S\,\mathrm{E}}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}}) \tag{37}$$

with $0 \leq \lambda \leq 1$. Herewith, the system operator is able to fulfill certain Quality of Service (QoS) constraints.

The programming problem that maximizes the weighted sum secrecy rate is given by

$$\max_{\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}},\lambda} R_S^{(\mathrm{wsum})}(\boldsymbol{P}_{\mathrm{B}},\boldsymbol{P}_{\mathrm{E}},\lambda) \quad \text{subject to} \quad \sum_{\ell=1}^{L}(P_{\mathrm{B}\,\ell}+P_{\mathrm{E}\,\ell}) \leq P, \quad P_{\mathrm{B}\,\ell} \geq 0 \quad \text{and} \quad P_{\mathrm{E}\,\ell} \geq 0.$$

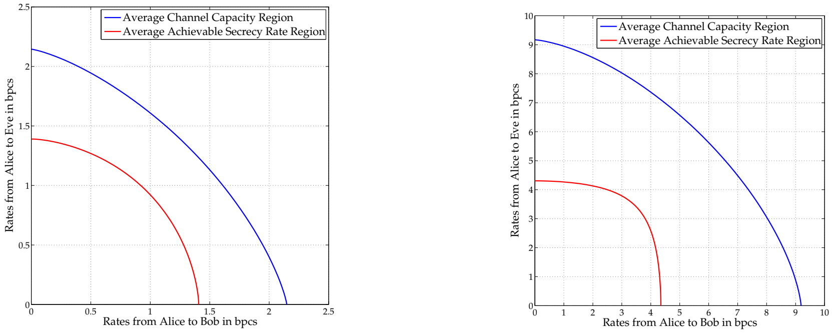
The user allocation is equivalent to the case without weighting factor in (36). It is optimal to support only the best user per carrier.

Furthermore, the spectral power allocation, which is similar to the one in the single-user multi-carrier scenario in Section 2.2, is a kind of waterfilling. The optimal power allocation is given by

$$P_{\mathrm{A}\,\ell} = \begin{cases} \left[-\frac{\sigma^2(\alpha_\ell+\beta_\ell)}{2\alpha_\ell\beta_\ell} + \sqrt{\frac{\sigma^4(\alpha_\ell-\beta_\ell)^2}{4\alpha_\ell^2\beta_\ell^2} + \frac{\lambda}{\mu}\frac{\sigma^2(\alpha_\ell-\beta_\ell)}{\ln(2)\alpha_\ell\beta_\ell}}\right]^+ & \text{if } \ell \in \mathcal{L}_1 \\ \left[-\frac{\sigma^2(\alpha_\ell+\beta_\ell)}{2\alpha_\ell\beta_\ell} + \sqrt{\frac{\sigma^4(\beta_\ell-\alpha_\ell)^2}{4\alpha_\ell^2\beta_\ell^2} + \frac{1-\lambda}{\mu}\frac{\sigma^2(\beta_\ell-\alpha_\ell)}{\ln(2)\alpha_\ell\beta_\ell}}\right]^+ & \text{if } \ell \in \mathcal{L}_2 \end{cases},$$

where $\mathcal{L}_1 = \{\ell \in \{1,\ldots,L\} : \alpha_\ell > \beta_\ell\}$, $\mathcal{L}_2 = \{1,\ldots,L\} \setminus \mathcal{L}_1$ and $\mu > 0$ such that

$$\sum_{\ell=1}^{L} P_{\mathrm{A}\,\ell} = P. \tag{38}$$



(a) SNR = 0 dB

(b) SNR = 10 dB

Fig. 12. The average channel capacity region and the average achievable secrecy rate region for the multi-carrier broadcast channel with eight carriers and two users.

Figure 12 shows the achievable average secrecy rate region for the broadcast channel with eight carriers compared to the average channel capacity region, which was found by exhaustive search. We observe that the gap between the achievable secrecy rate region and the capacity region grows with increasing SNR. For SNR $\to \infty$, we know that the secrecy rate region does not grow without bound. It is limited by the second term in the equations in (33).

Now, we present the secrecy capacity region for the real-valued MIMO broadcast channel, which can be found in (Liu, Liu, Poor & Shamai (Shitz), 2009). The system model is given by

$$\begin{aligned} \boldsymbol{Y} &= \boldsymbol{H}\boldsymbol{x} + \boldsymbol{\Phi} \quad \text{and} \\ \boldsymbol{Z} &= \boldsymbol{G}\boldsymbol{x} + \boldsymbol{\Psi}, \end{aligned} \tag{39}$$

where $\boldsymbol{H}$ and $\boldsymbol{G}$ are real channel matrices of size $[m_\mathrm{B} \times m_\mathrm{A}]$ and $[m_\mathrm{E} \times m_\mathrm{A}]$, respectively. The noise is modeled by vectors of dimension $[m_\mathrm{B} \times 1]$ and $[m_\mathrm{E} \times 1]$. For the distribution of the noise vectors, we assume $\boldsymbol{\Phi}$, $\boldsymbol{\Psi} \sim \mathcal{N}(0, \boldsymbol{I}_{m_k})$ with $k \in \{\mathrm{B}, \mathrm{E}\}$. The channel input $\boldsymbol{x}$ is a vector of the size $[m_\mathrm{A} \times 1]$. Furthermore, we have an average power constraint, defined by $\mathbb{E}\left(\|\boldsymbol{x}\|^2\right) \leq P$.

The achievable secrecy rates are given by

$$\begin{aligned}
&R_{S\,\mathrm{B}}(\boldsymbol{Q}_\mathrm{B}) \\
&= \left[\frac{1}{2}\log_2\det\left(\frac{\boldsymbol{I}_{m_\mathrm{B}} + \boldsymbol{H}\boldsymbol{Q}_\mathrm{B}\boldsymbol{H}^\mathrm{T}}{\boldsymbol{I}_{m_\mathrm{E}} + \boldsymbol{G}\boldsymbol{Q}_\mathrm{B}\boldsymbol{G}^\mathrm{T}}\right)\right]^+ \ [\text{bps}] \quad \text{and} \\
&R_{S\,\mathrm{E}}(\boldsymbol{Q}_\mathrm{B}, \boldsymbol{Q}_\mathrm{E}) \\
&= \left[\frac{1}{2}\log_2\det\left(\frac{\boldsymbol{I}_{m_\mathrm{E}} + \boldsymbol{G}(\boldsymbol{Q}_\mathrm{B} + \boldsymbol{Q}_\mathrm{E})\boldsymbol{G}^\mathrm{T}}{\boldsymbol{I}_{m_\mathrm{E}} + \boldsymbol{G}\boldsymbol{Q}_\mathrm{B}\boldsymbol{G}^\mathrm{T}}\right) - \frac{1}{2}\log_2\det\left(\frac{\boldsymbol{I}_{m_\mathrm{B}} + \boldsymbol{H}(\boldsymbol{Q}_\mathrm{B} + \boldsymbol{Q}_\mathrm{E})\boldsymbol{H}^\mathrm{T}}{\boldsymbol{I}_{m_\mathrm{B}} + \boldsymbol{H}\boldsymbol{Q}_\mathrm{B}\boldsymbol{H}^\mathrm{T}}\right)\right]^+ \ [\text{bps}],
\end{aligned} \tag{40}$$

where $\boldsymbol{Q}_\mathrm{B}$ and $\boldsymbol{Q}_\mathrm{E}$ are the covariance matrices for the transmission to Bob and to Eve, respectively. They are positive semidefinite matrices with $\mathrm{trace}(\boldsymbol{Q}_\mathrm{B} + \boldsymbol{Q}_\mathrm{E}) \leq P$.

For this system model, it has been shown in (Liu, Liu, Poor & Shamai (Shitz), 2009) that the secrecy capacity region is given by

$$\mathcal{R} = \bigcup_{0 \leq \mathrm{trace}(\boldsymbol{Q}_\mathrm{B} + \boldsymbol{Q}_\mathrm{E}) \leq P} \left(R_{S\,\mathrm{B}}(\boldsymbol{Q}_\mathrm{B}), R_{S\,\mathrm{E}}(\boldsymbol{Q}_\mathrm{B}, \boldsymbol{Q}_\mathrm{E})\right). \tag{41}$$

Even though the secrecy capacity region has been proven for the MIMO and the MISO broadcast channel (Liang et al., 2009), it is still an open problem to find the secrecy capacity region for the single-antenna case. So far, there are no results known about the optimal transmit strategies in MIMO and MISO broadcast channels.

3.2 Multiple Access Channels

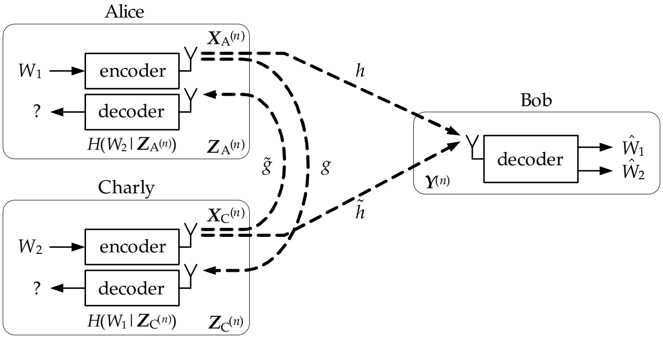


Fig. 13. The multiple access channel (one example).

The multiple access channel (MAC) is difficult to analyze in a system setting concerning secrecy on the physical layer. The conventional channel model for the MAC consists of two or more transmitters, e.g., mobile devices, and only one receiver, e.g., the base station. In this model, there is nobody who could eavesdrop the sent messages in accordance with the attacker model in Section 1.1. However, if the uplink transmission (MAC) and the downlink transmission (BC) are studied together, every user in the system can eavesdrop all other users. But from the transmitter's point of view, the channel model would always be a broadcast channel, where all other mobile devices and the base station serve as receivers.

There are currently a lot of research activities concerning the MAC in the secrecy context. One of the models assumed for the MAC in this case is depicted in Figure 13 and studied in (Liang et al., 2009). Another channel model is described in (Tekin & Yener, 2006). It deals with the degraded MAC, where the eavedropper obtains a degraded version of the receiver's signal.

3.3 Interference Channels

In this section, we will present two results for the interference channel (IFC). The first one will be a weak interference, single-antenna channel, whereas the second one is a multi-antenna interference channel. For both channel models, we need an additional sender, called Charly, as it can be seen in Figure 14.

Alice wants to send a private message to Bob, which should be kept secret from Eve. Furthermore, Charly wants to send a confidential message to Eve, which should be concealed from Bob. These communication channels have the channel coefficients h and g. The interference or eavesdropper channels from Alice to Eve and from Charlie to Bob have the coefficients $\tilde{g}$ and $\tilde{h}$, respectively.

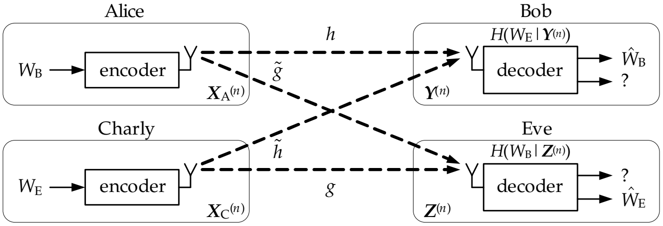


Fig. 14. The interference channel.

The basic system model from Section 1.6 has to be modified to be suitable for the interference channel. Nevertheless, the assumptions listed for the basic system model also apply to this model. For the interference channel, the system model, which was studied in (Zhang & Gursoy, 2009), is given by

$$\begin{aligned} y &= hx_{\mathrm{A}} + \tilde{h}x_{\mathrm{C}} + \phi \quad \text{and} \\ z &= gx_{\mathrm{C}} + \tilde{g}x_{\mathrm{A}} + \psi, \end{aligned} \tag{42}$$

where h, g, $\tilde{h}$ and $\tilde{g}$ are deterministic channel coefficients. $\boldsymbol{x}_{\mathrm{A}}$ and $\boldsymbol{x}_{\mathrm{C}}$ are the channel inputs at the transmitters. ϕ and ψ are independent and circular symmetric complex Gaussian random variables with $\mathcal{CN}(0, \sigma^2)$. The channel causes weak interference, i.e., $\frac{\tilde{\alpha}}{\alpha} < 1$ and $\frac{\tilde{\beta}}{\beta} < 1$, where the channel gains $\tilde{\alpha}$ and $\tilde{\beta}$ of the eavesdropper channels are defined according to (10) by $\tilde{\alpha} = |\tilde{h}|^2$ and $\tilde{\beta} = |\tilde{g}|^2$. The individual power constraint at the transmitters are given by

$$\mathbb{E}\left(|x_{\mathrm{A}}|^2\right) \leq P_{\mathrm{A}} \quad \text{and} \quad \mathbb{E}\left(|x_{\mathrm{C}}|^2\right) \leq P_{\mathrm{C}}. \tag{43}$$

The system model has to be modified according to Section 1.8. The consideration of interference results in the achievable secrecy rates given by

$$\begin{aligned} R_{S\,\mathrm{B}}(P_{\mathrm{B}}, P_{\mathrm{E}}) &= \left[\log_2\left(1+\frac{\alpha P_{\mathrm{B}}}{\sigma^2+\tilde{\alpha}P_{\mathrm{E}}}\right)-\log_2\left(1+\frac{\tilde{\beta}P_{\mathrm{B}}}{\sigma^2}\right)\right]^+ \quad [\mathrm{bpcs}] \quad \text{and} \\ R_{S\,\mathrm{E}}(P_{\mathrm{B}}, P_{\mathrm{E}}) &= \left[\log_2\left(1+\frac{\beta P_{\mathrm{E}}}{\sigma^2+\tilde{\beta}P_{\mathrm{B}}}\right)-\log_2\left(1+\frac{\tilde{\alpha}P_{\mathrm{E}}}{\sigma^2}\right)\right]^+ \quad [\mathrm{bpcs}], \end{aligned} \tag{44}$$

where P_{B} is the power allocated by Alice for data transmission to Bob and P_{E} is the power allocated by Charly for data transmission to Eve.
The achievable secrecy rate region is given by

$$\mathcal{R} = \bigcup_{\substack{0\le P_{\mathrm{B}}\le P_{\mathrm{A}},\\ 0\le P_{\mathrm{E}}\le P_{\mathrm{C}}}} \left(R_{S\,\mathrm{B}}(P_{\mathrm{B}}, P_{\mathrm{E}}), R_{S\,\mathrm{E}}(P_{\mathrm{B}}, P_{\mathrm{E}})\right). \tag{45}$$

Now, we present some results for the multi-antenna interference channel, which are discussed in (Jorswieck & Mochaourab, 2009) in a game-theoretic context. Both transmitters use m_{A} and m_{C} antennas, whereas Eve and Bob receive the messages with only one antenna each. The system model is modified according to Sections 1.7 and 1.8 and is described by

$$\begin{aligned} y &= \boldsymbol{h}\cdot\boldsymbol{x}_{\mathrm{A}}+\tilde{\boldsymbol{h}}\cdot\boldsymbol{x}_{\mathrm{C}}+\phi \quad \text{and} \\ z &= \boldsymbol{g}\cdot\boldsymbol{x}_{\mathrm{C}}+\tilde{\boldsymbol{g}}\cdot\boldsymbol{x}_{\mathrm{A}}+\psi, \end{aligned} \tag{46}$$

where $\boldsymbol{h}$ and $\tilde{\boldsymbol{g}}$ are row vectors of dimension $[1\times m_{\mathrm{A}}]$ and $\tilde{\boldsymbol{h}}$ and $\boldsymbol{g}$ are row vectors of dimension $[1\times m_{\mathrm{C}}]$ with complex channel coefficients. $\boldsymbol{x}_{\mathrm{A}}$ and $\boldsymbol{x}_{\mathrm{C}}$ are vectors of dimension $[m_{\mathrm{A}}\times 1]$ and $[m_{\mathrm{C}}\times 1]$ and are independent, circular symmetric, and complex Gaussian distributed, i.e., $\boldsymbol{x}_{\mathrm{A}}\sim\mathcal{CN}(0,\boldsymbol{v}_{\mathrm{A}}\boldsymbol{v}_{\mathrm{A}}^{\dagger})$ and $\boldsymbol{x}_{\mathrm{C}}\sim\mathcal{CN}(0,\boldsymbol{v}_{\mathrm{C}}\boldsymbol{v}_{\mathrm{C}}^{\dagger})$. The beamforming vectors $\boldsymbol{v}_{\mathrm{A}}$ and $\boldsymbol{v}_{\mathrm{C}}$ are of dimensions $[m_{\mathrm{A}}\times 1]$ and $[m_{\mathrm{C}}\times 1]$ with $\|\boldsymbol{v}_{\mathrm{A}}\|^2=\|\boldsymbol{v}_{\mathrm{C}}\|^2=1$. ϕ and ψ are independent white Gaussian noise with variance σ^2, i.e., $\phi,\psi\sim\mathcal{CN}(0,\sigma^2)$. Both transmitters have a power constraint P.
The achievable secrecy rate pair for the Gaussian MISO IFC is given by

$$\begin{aligned} R_{S\,\mathrm{B}}(\boldsymbol{v}_{\mathrm{A}},\boldsymbol{v}_{\mathrm{C}}) &= \left[\log_2\left(1+\frac{|\boldsymbol{h}\cdot\boldsymbol{v}_{\mathrm{A}}|^2P}{\sigma^2+|\tilde{\boldsymbol{h}}\cdot\boldsymbol{v}_{\mathrm{C}}|^2P}\right)-\log_2\left(1+\frac{|\tilde{\boldsymbol{g}}\cdot\boldsymbol{v}_{\mathrm{A}}|^2P}{\sigma^2}\right)\right]^+ \quad [\mathrm{bpcs}] \quad \text{and} \\ R_{S\,\mathrm{E}}(\boldsymbol{v}_{\mathrm{A}},\boldsymbol{v}_{\mathrm{C}}) &= \left[\log_2\left(1+\frac{|\boldsymbol{g}\cdot\boldsymbol{v}_{\mathrm{C}}|^2P}{\sigma^2+|\tilde{\boldsymbol{g}}\cdot\boldsymbol{v}_{\mathrm{A}}|^2P}\right)-\log_2\left(1+\frac{|\tilde{\boldsymbol{h}}\cdot\boldsymbol{v}_{\mathrm{C}}|^2P}{\sigma^2}\right)\right]^+ \quad [\mathrm{bpcs}]. \end{aligned} \tag{47}$$

The efficient beamforming vectors are described in the following. According to (Jorswieck & Mochaourab, 2009), we denote the maximum ratio transmission beamforming vector of user k as $\boldsymbol{v}_k^{(MRT)}$ and the zero-forcing beamforming vector as $\boldsymbol{v}_k^{(ZF)}$, where $k\in\{\mathrm{A},\mathrm{C}\}$. We obtain

$$\begin{aligned} \boldsymbol{v}_{\mathrm{A}}(\lambda_{\mathrm{A}}) &= \frac{\lambda_{\mathrm{A}}\cdot\boldsymbol{v}_{\mathrm{A}}^{(\mathrm{MRT})}+(1-\lambda_{\mathrm{A}})\cdot\boldsymbol{v}_{\mathrm{A}}^{(\mathrm{ZF})}}{\left\|\lambda_{\mathrm{A}}\cdot\boldsymbol{v}_{\mathrm{A}}^{(\mathrm{MRT})}+(1-\lambda_{\mathrm{A}})\cdot\boldsymbol{v}_{\mathrm{A}}^{(\mathrm{ZF})}\right\|} \quad \text{and} \\ \boldsymbol{v}_{\mathrm{C}}(\lambda_{\mathrm{C}}) &= \frac{\lambda_{\mathrm{C}}\cdot\boldsymbol{v}_{\mathrm{C}}^{(\mathrm{MRT})}+(1-\lambda_{\mathrm{C}})\cdot\boldsymbol{v}_{\mathrm{C}}^{(\mathrm{ZF})}}{\left\|\lambda_{\mathrm{C}}\cdot\boldsymbol{v}_{\mathrm{C}}^{(\mathrm{MRT})}+(1-\lambda_{\mathrm{C}})\cdot\boldsymbol{v}_{\mathrm{C}}^{(\mathrm{ZF})}\right\|} \end{aligned} \tag{48}$$

with transmit strategies $0 \leq \lambda_{\mathrm{A}}, \lambda_{\mathrm{C}} \leq 1$.
The maximization of the secrecy rate from Alice to Bob depends on the given interference caused by Charly. The rate can be described as the best response, if λ_{C} is given:

$$\lambda_{\mathrm{A}}^{*}(\lambda_{\mathrm{C}}) = \arg \max_{0 \leq \lambda_{\mathrm{A}} \leq 1} R_{S\,\mathrm{B}}(\lambda_{\mathrm{A}}, \lambda_{\mathrm{C}}). \tag{49}$$

Equivalently, Charly's best response to Alice' transmit strategy is given by

$$\lambda_{\mathrm{C}}^{*}(\lambda_{\mathrm{A}}) = \arg \max_{0 \leq \lambda_{\mathrm{C}} \leq 1} R_{S\,\mathrm{E}}(\lambda_{\mathrm{A}}, \lambda_{\mathrm{C}}). \tag{50}$$

From Alice' and Charly's point of view, the interference channel equals the broadcast channel. Because of this fact, they do not have the possibility to influence, but to react to the interference generated by each other. The optimal solution for the maximization problems in (49) and (50) can be found by an iterative algorithm described in (Jorswieck & Mochaourab, 2009). This optimum is not the best solution, which is possible in this scenario. It is an achievable and stable point, the so-called Nash Equilibrium, that will be reached, if Alice and Charly do not cooperate. Another approach to solve these non-convex optimization problems is to use a monotonic optimization framework. This has been proven useful for the MISO interference channel in (Jorswieck & Larsson, 2009) in order to optimize the transmit strategies.

4. Discussion and Open Problems

The information theoretic description of secrecy capacities and secrecy capacity regions (Liang et al., 2009) is an important research area to support a better understanding of security on the physical layer. Based on the secrecy capacity expressions or achievable secrecy rates, the transmit strategies, including power allocation, beamforming and subcarrier allocation, are optimized in order to choose a certain operating point. In this chapter, we focus on the optimization of the physical layer transmit strategies for typical wireless communication scenarios.

In single-user scenarios, the system design is more complicated with additional secrecy constraints, since the secrecy capacity expressions are in general not concave or convex in the transmit strategies. The secrecy rate terms usually consist of a difference of two parts. The first one corresponds to the amount of data that can be reliably transmitted to the intended user and it is therefore concave in the transmit strategies. The second one corresponds to the amount of data that is overheard by the eavesdropper and it is thus also concave in the transmit strategies. The resulting transmit optimization problems are non-convex optimization problems since the difference of two concave functions is not necessarily convex or concave. However, in the multi-carrier case, the problem can be reduced to a convex optimization problem that can be efficiently computed. We conjecture that also the multiple antenna (MIMO) scenario will be completely solved in the very next future.

In multi-user scenarios, the secrecy rate regions of all four elements of network information theory, the broadcast, the multiple access, the relay, and the interference channel were recently studied. The attacker models of the MAC and the relay case are more difficult than the well-motivated ones of the broadcast and the interference channel. Therefore, we focus on the broadcast and interference channel. The resource allocation for the parallel broadcast channel without secrecy is involved due to a hard combinatorial problem – the matching of carriers to users. Interestingly, with secrecy constraints, the resulting programming problem is much simpler and the optimal power and resource allocation can be solved efficiently. A similar observation in the context of interference channels with beamforming and without cooperation shows that the secrecy constraint leads to a more altruistic and less selfish behavior. In both cases, the additional term in the utility functions simplifies and improves the resulting transmit optimization.

In addition to the resource allocation and transmit optimization problems discussed in this chapter, there are many important practical issues to be solved. The assumption to have perfect CSI at the transmitter(s) and receiver(s) is idealistic. The impact of channel estimation errors and limited feedback on the achievable secrecy rates needs to be analyzed. The assumption to apply Gaussian codebooks is idealistic, too. Finite modulation and coding schemes lead to more difficult bit and power allocation problems at the transmitter. Recent results in the development of channel codes for secure communications are not discussed in this chapter due to length constraints. However, there is interesting current work on the analysis and development of channel codes that are able to achieve the secrecy capacity. Finally, the attacker model studied in this chapter is important but not the only one possible. Future work will also consider malicious user behavior as well as byzantine attacks. There are many interesting open problems in the broad area of physical layer security in wireless communications.

Acknowledgement

The authors want to thank Martin Mittelbach for his review of this chapter, critical comments and productive discussions.

5. References

Bloch, M., Barros, J., Rodrigues, M. R. D. & Laughlin, S. W. M. (2008). Wireless Information-Theoretic Security, *IEEE Transactions on Information Theory* **54**(6): 2515–2534.

Boyd, S. & Vandenberghe, L. (2004). *Convex Optimization*, Cambridge University Press. **URL:** *http://www.stanford.edu/ boyd/cvxbook/*

Cover, T. M. & Thomas, J. A. (2006). *Elements of Information Theory*, Wiley & Sons.

Csiszár, I. & Körner, J. (1978). Broadcast Channels with Confidential Messages, *IEEE Transactions on Information Theory* **24**(3): 339–348.

Diffie, W. & Hellman, M. E. (1976). New directions in cryptography, *IEEE Transactions on Information Theory* **22**(6): 644–654.

Jorswieck, E. A. & Gerbracht, S. (2009). Secrecy Rate Region of Downlink OFDM Systems: Efficient Resource Allocation, *14th International OFDM-Workshop (InOWo)*, Hamburg, Germany.

Jorswieck, E. A. & Larsson, E. (2009). Monotonic Optimization Framework for the MISO IFC, *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3633–3636.

Jorswieck, E. A. & Mochaourab, R. (2009). Secrecy Rate Region of MISO Interference Channel: Pareto Boundary and Non-Cooperative Games, *International ITG Workshop on Smart Antennas*, Berlin, Germany.

Jorswieck, E. A. & Wolf, A. (2008). Resource Allocation for the Wire-tap Multi-carrier Broadcast Channel, *Proceedings of International Workshop on Multiple Access Communications (MACOM)*, Saint Petersburg, Russia.

Leung-Yan-Cheong, S. & Hellman, M. (1978). The Gaussian wire-tap channel, *IEEE Transactions on Information Theory* **24**(4): 451–456.

Li, Z., Trappe, W. & Yates, R. (2007). Secret Communication via Multi-antenna Transmission, *41st Annual Conference on Information Sciences and Systems (CISS)*, pp. 905–910.

Liang, Y., Poor, H. V. & Shamai (Shitz), S. (2009). *Information Theoretic Security*, Vol. 5 of *Foundations and Trends in Communications and Information Theory*, now publishers, pp. 355–580.

Liu, J., Hou, Y. T. & Sherali, H. D. (2009). Optimal power allocation for achieving perfect secrecy capacity in MIMO wire-tap channels, *43rd Annual Conference on Information Sciences and Systems (CISS)*, pp. 606–611.

Liu, R., Liu, T., Poor, H. V. & Shamai (Shitz), S. (2009). Multiple-Input Multiple-Output Gaussian Broadcast Channels with Confidential Messages, *CoRR* **abs/0903.3786**. submitted.

Oggier, F. & Hassibi, B. (2008). The Secrecy Capacity of the MIMO Wiretap Channel, *IEEE International Symposium on Information Theory (ISIT)*, pp. 524–528.

Rivest, R. L., Shamir, A. & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21**(2): 120–126.

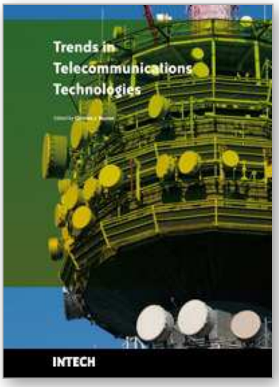
Schneier, B. (1996). *Applied Cryptography*, Wiley & Sons.

Shafiee, S., Liu, N. & Ulukus, S. (2008). Secrecy Capacity of the 2-2-1 Gaussian MIMO Wire-tap Channel, *3rd International Symposium on Communications, Control and Signal Processing (ISCCSP)*, pp. 207–212.

Tekin, E. & Yener, A. (2006). The Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy Constraints, *IEEE International Symposium on Information Theory (ISIT)*, pp. 1164–1168.

Wyner, A. D. (1975). The Wire-tap Channel, *Bell System Technical Journal* **54**(8): 1355–1387.

Zhang, J. & Gursoy, M. C. (2009). Low-SNR Analysis of Interference Channels under Secrecy Constraints, *CoRR* **abs/0901.3132**. submitted.



Trends in Telecommunications Technologies
Edited by Christos J Bouras

ISBN 978-953-307-072-8
Hard cover, 768 pages
Publisher InTech
Published online 01, March, 2010
Published in print edition March, 2010

The main focus of the book is the advances in telecommunications modeling, policy, and technology. In particular, several chapters of the book deal with low-level network layers and present issues in optical communication technology and optical networks, including the deployment of optical hardware devices and the design of optical network architecture. Wireless networking is also covered, with a focus on WiFi and WiMAX technologies. The book also contains chapters that deal with transport issues, and namely protocols and policies for efficient and guaranteed transmission characteristics while transferring demanding data applications such as video. Finally, the book includes chapters that focus on the delivery of applications through common telecommunication channels such as the earth atmosphere. This book is useful for researchers working in the telecommunications field, in order to read a compact gathering of some of the latest efforts in related areas. It is also useful for educators that wish to get an up-to-date glimpse of telecommunications research and present it in an easily understandable and concise way. It is finally suitable for the engineers and other interested people that would benefit from an overview of ideas, experiments, algorithms and techniques that are presented throughout the book.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Eduard A. Jorswieck, Anne Wolf, and Sabrina Gerbracht (2010). Secrecy on the Physical Layer in Wireless Networks, Trends in Telecommunications Technologies, Christos J Bouras (Ed.), ISBN: 978-953-307-072-8, InTech, Available from: http://www.intechopen.com/books/trends-in-telecommunications-technologies/secrecy-on-the-physical-layer-in-wireless-networks

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821