Non-regenerative Two-Hop Wiretap Channels using Interference Neutralization

Sabrina Gerbracht and Eduard A. Jorswieck

Communications Theory, Communications Laboratory
Dresden University of Technology, Dresden, Germany
Email: {sabrina.gerbracht,eduard.jorswieck}@tu-dresden.de

Gan Zheng and Björn Ottersten

Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg, Luxembourg
E-mail: {gan.zheng,bjorn.ottersten}@uni.lu

***Abstract*—In this paper, we analyze the achievable secrecy rates in the two-hop wiretap channel with four nodes, where the transmitter and the receiver have multiple antennas while the relay and the eavesdropper have only a single antenna each. The relay is operating in amplify-and-forward mode and all the channels between the nodes are known perfectly by the transmitter. We discuss different transmission and protection schemes like artificial noise (AN). Furthermore, we introduce interference neutralization (IN) as a new protection scheme. We compare the different schemes regarding the high-SNR slope and the high-SNR power offset and illustrate the performance by simulation results. It is shown analytically as well as by numerical simulations that the high SNR performance of the proposed IN scheme is better than the one of AN.**

***Index Terms*—Secrecy rate, two-hop wiretap channel, artificial noise, amplify-and-forward, interference neutralization**

I. Introduction

Wireless networks are widely-used for communication nowadays. In order to secure the conversation over this broadcast media, secrecy on the physical layer has been investigated over the past few years. The research is based on the seminal work [1], which describes how to achieve secrecy on the discrete and degraded wiretap channel without the use of cryptography. This work was extended in [2] to the degraded Gaussian wiretap channel and in [3] to the non-degraded case, which is of special interest for all wireless communication models. For a comprehensive overview on the topic of secrecy on the physical layer we refer the reader to [4], [5] and [6].

In cooperative communications, the wiretapper has usually access to multiple signal transmissions. Hence the chance of eavesdropping messages is increased. However, the cooperative nodes could also help to confuse the eavesdropper. Because of this tradeoff, the multihop scenario is interesting yet difficult. One of the first papers on secrecy in relay wiretap channels is [7]. Here, the authors analyze the impact of amplify-and-forward (AF) and decode-and-forward (DF) strategies at the relay on the achievable secrecy rate in a single-input single-output (SISO) relay wiretap channel. Additionally, the results are compared to the case where the relay only functions as a helper and sends artificial noise (AN). In [8] and [9], these relay strategies are further analyzed with regard to the outage performance and optimal power allocation, if the channels to the eavesdropper are known only statistically.

This work is supported by the German Research Foundation (DFG) in the Collaborative Research Center 912 “Highly Adaptive Energy-Efficient Computing”.

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

The optimization of secrecy rates in the four node two-hop wiretap channel, where there is no direct link between the transmitter and the receiver, is investigated in [11]. In this paper, the relay is working in DF mode and the source and the relay are sending AN signals, which are known a priori by the relay and the destination. Therefore, this transmission scheme equals a cryptographic encryption, as the AN is functioning as key, which has to be exchanged securely before transmission.

The achievable secrecy rates in the multiple-input multiple-output (MIMO) channel model, where every node has multiple antennas, are determined in [12]. All nodes are working in half duplex mode and therefore, the communication from Alice to Bob is taking two time slots. 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.

Interference Neutralization (IN) 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 [13], two-hop relay channels [14] and instantaneous relay networks [15].

In our paper, we use the advantage of multiple antennas at the transmitter in order to secure the first phase of the communication between Alice and Bob by beamforming. In the second phase, we apply AN and IN and compare our results with regards to the high-SNR power offset.

The paper is organized as follows. In Section II, the system model is presented and the high-SNR measures used for the analysis are introduced. Section III contains the descriptions of the different transmission and protection schemes and a discussion about there performance in the high SNR regime. The analytically derived results are illustrated by numerical simulations in Section IV. Section V concludes the paper.

Throughout this paper, we use the following notations if not stated otherwise. Vectors and matrices are marked as bold lower and upper case letters, respectively. $\boldsymbol{X}^H$ denotes the Hermitian transpose of matrix $\boldsymbol{X}$. $|\cdot|$ and $\|\cdot\|$ represent the absolute value of a scalar and the Euclidean norm of a vector, respectively. The identity matrix of rank n is denoted by $\boldsymbol{I}_n$. $\Pi_X^{\perp}$ is the orthogonal projector onto the orthogonal complement of the column space of $\boldsymbol{X}$, i.e., $\Pi_X^{\perp} = \boldsymbol{I} - \Pi_X$ where $\Pi_X = \boldsymbol{X}(\boldsymbol{X}^H\boldsymbol{X})^{-1}\boldsymbol{X}^H$.

$[\cdot]^+$ describes the max-function $\max\{\cdot, 0\}$. The expectation is noted by $\mathbb{E}[\cdot]$ and all logarithms are to the base 2.

II. Preliminaries

A. System Model

The system considered in this paper is based on the non-degraded Gaussian wiretap channel described in [2]. 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 1. The relay and the eavesdropper are equipped with a single antenna each while Alice and Bob have n_T and n_R antennas, respectively. The receiver does not necessarily need multiple antennas, i.e. $n_R \geq 1$. 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 $\boldsymbol{g}_D$ and g_E. All nodes are operating in half duplex mode and therefore can either transmit or receive signals.

We assume individual power constraints at the transmit nodes, denoted by $P_{S,1} = \mathbb{E}[|x|^2]$ (first phase), $P_{S,2} = \mathbb{E}[|x_n|^2]$ (second phase) at the source Alice and P_R at the relay. We assume perfect channel state information (CSI) at the transmitter, i.e., Alice has perfect knowledge about all channels. Bob needs to have local CSI in order to maximize his receive signal by applying maximum ratio combining (MRC).

The received signals at the relay and the eavesdropper in the first phase are given by

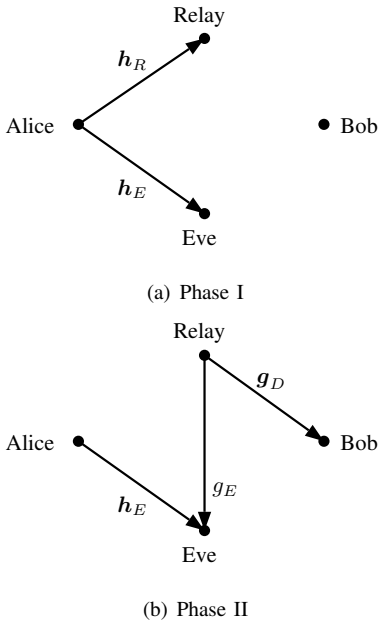
$$y_R = \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x + n_R \quad \text{and}$$
$$y_{E,1} = \boldsymbol{h}_E^H \boldsymbol{w}_{S,1} x + n_{E,1},$$

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

$$y_D = \sqrt{\alpha}\boldsymbol{w}_D^H \boldsymbol{g}_D(\boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x + n_R) + n_D \quad \text{and}$$
$$y_{E,2} = \boldsymbol{h}_E^H \boldsymbol{w}_{S,2} x_n + \sqrt{\alpha} g_E(\boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x + n_R) + n_{E,2},$$

respectively, where α is the scaling factor at the relay to satisfy the power constraint.

The scalars n_D, 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 $\rho = \frac{1}{\sigma^2}$. 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 vectors $\boldsymbol{w}_{S,1}$ and $\boldsymbol{w}_{S,2}$ are the transmit beamforming vectors at Alice in the first and second phase, respectively. The receive beamforming vector at the intended receiver Bob in the second phase is given by $\boldsymbol{w}_D$.



(a) Phase I

(b) Phase II

Figure 1. System model

The secrecy rate is then

$$R_S = [C(\Gamma_D) - C(\Gamma_E)]^+, \tag{1}$$

where we define $C(\text{SINR}) = \log(1 + \text{SINR})$. The SINR expressions are given according to the received signals as

$$\Gamma_D = \frac{\alpha\rho P_{S,1} \left|\boldsymbol{w}_D^H \boldsymbol{g}_D\right|^2 \left|\boldsymbol{h}_R^H \boldsymbol{w}_{S,1}\right|^2}{\alpha \left|\boldsymbol{w}_D^H \boldsymbol{g}_D\right|^2 + 1}, \quad \text{and} \tag{2}$$

$$\Gamma_E = \rho P_{S,1} \left|\boldsymbol{h}_E^H \boldsymbol{w}_{S,1}\right|^2 + \frac{\alpha\rho P_{S,1} |g_E|^2 \left|\boldsymbol{h}_R^H \boldsymbol{w}_{S,1}\right|^2}{\rho P_{S,2} \left|\boldsymbol{h}_E^H \boldsymbol{w}_{S,2}\right|^2 + \alpha |g_E|^2 + 1} \tag{3}$$

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

In (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.

B. High-SNR Slope and High-SNR Power Offset

In order to compare our different schemes in the high-SNR regime, we use the concept of the high-SNR power offset from [16]. The achievable rate as a function of the SNR ρ is denoted by $R(\rho)$. Then the high-SNR slope is defined as

$$\mathcal{S}_\infty = \lim_{\rho\to\infty} \frac{R(\rho)}{\log(\rho)} \tag{4}$$

in bits/s/Hz/(3 dB) and the high-SNR power offset is given as

$$\mathcal{L}_\infty = \lim_{\rho\to\infty}\left(\log(\rho) - \frac{R(\rho)}{\mathcal{S}_\infty}\right) \tag{5}$$

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 [16, 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.

III. Transmission and Protection Schemes

Alice performs single-stream beamforming and transmits the intended signal with full transmit power. We define the following beamforming vectors

$$\begin{aligned}
\boldsymbol{w}^{\text{MRC}} &= \frac{\boldsymbol{g}_D}{\|\boldsymbol{g}_D\|}, & \boldsymbol{w}_{\text{Eve}}^{\perp} &= \frac{\Pi_{\boldsymbol{h}_E}^{\perp}\boldsymbol{h}_R}{\left\|\Pi_{\boldsymbol{h}_E}^{\perp}\boldsymbol{h}_R\right\|},\\
\boldsymbol{w}_{\text{Relay}}^{\text{MRT}} &= \frac{\boldsymbol{h}_R}{\|\boldsymbol{h}_R\|}, & \boldsymbol{w}_{\text{Eve}} &= \frac{\Pi_{\boldsymbol{h}_E}\boldsymbol{h}_R}{\|\Pi_{\boldsymbol{h}_E}\boldsymbol{h}_R\|},\\
\boldsymbol{w}_{\text{Eve}}^{\text{MRT}} &= \frac{\boldsymbol{h}_E}{\|\boldsymbol{h}_E\|}, & \boldsymbol{w}^{\text{LBF}}(\lambda) &= \sqrt{\lambda}\boldsymbol{w}_{\text{Eve}}^{\perp} + \sqrt{1-\lambda}\boldsymbol{w}_{\text{Eve}},
\end{aligned}$$

where $\boldsymbol{w}^{\text{MRC}}$ is the maximum ratio combining (MRC) receive beamforming vector at Bob. The vectors $\boldsymbol{w}_{\text{Relay}}^{\text{MRT}}$ and $\boldsymbol{w}_{\text{Eve}}^{\text{MRT}}$ are the maximum ratio transmission (MRT) beamforming vectors in the directions of $\boldsymbol{h}_R$ and $\boldsymbol{h}_E$, respectively, applied at Alice. The zero forcing (ZF) transmit beamforming vector regarding Eve is given by $\boldsymbol{w}_{\text{Eve}}^{\perp}$, 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 $\boldsymbol{w}^{\text{LBF}}$ denotes the linear combination between the beamforming vectors $\boldsymbol{w}_{\text{Eve}}^{\perp}$ and $\boldsymbol{w}_{\text{Eve}}$, where $\lambda \in [0,1]$ has to be chosen appropriately.

In all following schemes the best Bob can do in order to maximize his receive signal is MRC. This is due to the facts that Bob is only interested in the signal coming from the relay and that the channel is a SIMO link. Therefore, we set $\boldsymbol{w}_D = \boldsymbol{w}^{\text{MRC}}$ for all schemes.

A. 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 in this system is MRT, i.e., $\boldsymbol{w}_{\boldsymbol{S},\boldsymbol{1}} = \boldsymbol{w}_{\text{Relay}}^{\text{MRT}}$. The secrecy capacity is therefore given as

$$R_P = C\left(\frac{\alpha\rho P_{S,1}\|\boldsymbol{g}_D\|^2\|\boldsymbol{h}_R\|^2}{\alpha\|\boldsymbol{g}_D\|^2+1}\right) \tag{6}$$

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

The high-SNR slope of the peaceful system is given by

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

The high-SNR power offset is then calculated to

$$\mathcal{L}_\infty^{\text{P}} = \log\left(\frac{1}{P_{S,1}\|\boldsymbol{h}_R\|^2} + \frac{1}{P_R\|\boldsymbol{g}_D\|^2}\right). \tag{7}$$

B. 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

$$\Gamma_D = \frac{\alpha\rho P_{S,1}\left|\boldsymbol{w}_D^H\boldsymbol{g}_D\right|^2\left|\boldsymbol{h}_R^H\boldsymbol{w}_{S,1}\right|^2}{\alpha\left|\boldsymbol{w}_D^H\boldsymbol{g}_D\right|^2+1},$$

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

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

The optimal transmit beamforming vector is given by $\boldsymbol{w}_{S,1} = \boldsymbol{w}^{\text{LBF}}(\lambda)$ for a certain $\lambda \in [0,1]$.

Unfortunately, the high-SNR slope of this transmission scheme 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 of these schemes it is advantageous to choose $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\text{Eve}}^{\perp}$, i.e., zero forcing (ZF) in the first phase, so that the signal at Eve is set to zero.

C. Eavesdropper System with Artificial Noise

In this setting, Alice transmits in the first phase the data symbol with ZF as described before, i.e., $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\text{Eve}}^{\perp}$. In the second phase, she additionally sends an AN signal in the direction of Eve, i.e., $\boldsymbol{w}_{S,2} = \boldsymbol{w}_{\text{Eve}}^{\text{MRT}}$. The SINR terms are given accordingly as

$$\Gamma_D = \frac{\alpha\rho P_{S,1}\|\boldsymbol{g}_D\|^2\left|\boldsymbol{h}_R^H\boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2}{\alpha\|\boldsymbol{g}_D\|^2+1}, \tag{8}$$

$$\Gamma_E = \frac{\alpha\rho P_{S,1}\left|g_E\right|^2\left|\boldsymbol{h}_R^H\boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2}{\rho P_{S,2}\|\boldsymbol{h}_E\|^2 + \alpha\left|g_E\right|^2+1} \tag{9}$$

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

We achieve the achievable secrecy rate if we combine (8) and (9) with (1). By applying this secrecy rate to (4), we obtain the high-SNR slope

$$\mathcal{S}_\infty^{\text{AN}} = 1. \tag{10}$$

Similarly, by the usage of (10) and the secrecy rate together with (5), we receive the high-SNR power offset

$$\mathcal{L}_\infty^{\text{AN}} = \log\left(\frac{1}{P_{S,1}\left|\boldsymbol{h}_R^H\boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2} + \frac{1}{P_R\|\boldsymbol{g}_D\|^2} + \frac{P_R\left|g_E\right|^2}{P_{S,2}\|\boldsymbol{h}_E\|^2}\left(\frac{1}{P_{S,1}\left|\boldsymbol{h}_R^H\boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2} + \frac{1}{P_R\|\boldsymbol{g}_D\|^2}\right)\right). \tag{11}$$

D. Eavesdropper System with Interference Neutralization

Due to the fact, that the transmitter has perfect channel state information of all channels in the system, Alice can construct a signal x_n, that fulfills

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

and therefore neutralizes the eavesdropped signal at Eve that she receives over the relay in the second phase. This method is known as interference neutralization (IN) in the literature.

Alice chooses ZF as beamforming strategy in the first phase, in order to prevent Eve from eavesdropping. In the second phase, she sends the IN signal, i.e.,

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

Alice chooses the transmit beamforming vector in this phase such that the transmission of the neutralization signal at Eve is maximized, i.e., $\boldsymbol{w}_{S,2} = \boldsymbol{w}_{\text{Eve}}^{\text{MRT}}$.

The secrecy rate is then given by

$$R_S^{\text{IN}} = C\left(\frac{\alpha \rho P_{S,1} \|\boldsymbol{g}_D\|^2 \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2}{\alpha \|\boldsymbol{g}_D\|^2 + 1} \right),$$

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

As this scheme implies that Eve gets no data signal at all, Alice can perform conventional channel coding instead of the more complex secrecy binning that is normally used for wiretap systems.

Unfortunately, this scheme does not work under any condition, but is dependent 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 as shown in Section III-D2.

1) Adaptation of Power Constraint at Alice: In order to successfully neutralize the signal at the eavesdropper, Alice has to transmit with $P_{S,2}$, which has to fulfill the following inequality.

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

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

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

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

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

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

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

2) Optimizing the 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. Therefore, we can formulate a maximization problem over the transmit power at the relay subject to the IN power constraint as follows

$$\begin{aligned} \max_{0 \leq p_R \leq P_R} \quad & \frac{\rho p_R P_{S,1} \|\boldsymbol{g}_D\|^2 \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2}{p_R \|\boldsymbol{g}_D\|^2 + \left(P_{S,1} \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2 + \frac{1}{\rho} \right)} \\ \text{s.t} \quad & \frac{\rho p_R P_{S,1} |g_E|^2 \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2}{\left(\rho P_{S,1} \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2 + 1 \right) \|\boldsymbol{h}_E\|^2} \leq P_{S,2}. \end{aligned} \tag{12}$$

We can reformulate the IN power constraint to

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

Let us denote $\tilde{p}_R := \frac{P_{S,2} \|\boldsymbol{h}_E\|^2}{|g_E|^2} \left(1 + \frac{1}{\rho P_{S,1} \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2} \right)$. The secrecy rate R_S^{IN} is maximized for $p_R = \min(\tilde{p}_R, P_R)$. Therefore, we have to distinguish two different cases for the calculation of the high-SNR slope and the high-SNR power offset.

a) First case $\tilde{p}_R < P_R$: For this case the transmit power at the relay is bounded by the IN power constraint and the secrecy rate is given by

$$R_S^{\text{IN}}(\tilde{p}_R) = C\left(\rho \frac{P_{S,1} P_{S,2} \|\boldsymbol{h}_E\|^2 \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2 \|\boldsymbol{g}_D\|^2}{P_{S,2} \|\boldsymbol{h}_E\|^2 \|\boldsymbol{g}_D\|^2 + P_{S,1} \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2 |g_E|^2} \right).$$

The high-SNR slope (4) for $R_S^{\text{IN}}(\tilde{p}_R)$ is given by

$$\mathcal{S}_{\infty}^{\text{IN}}(\tilde{p}_R) = 1$$

and the high-SNR power offset (5) can be calculated to

$$\mathcal{L}_{\infty}^{\text{IN}}(\tilde{p}_R) = \log\left(\frac{1}{P_{S,1} \left| \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp} \right|^2} + \frac{|g_E|^2}{P_{S,2} \|\boldsymbol{h}_E\|^2 \|\boldsymbol{g}_D\|^2} \right) \tag{13}$$

b) Second case $\tilde{p}_R \geq P_R$: If the power at the relay is limited by the power constraint P_R, the secrecy rate is given by

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

Once again, the high-SNR slope is calculated to

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

and the high-SNR power offset is given by

$$\mathcal{L}_{\infty}^{\text{IN}}(P_R) = \log\left(\frac{1}{P_{S,1}\left|\boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2} + \frac{1}{P_R\|\boldsymbol{g}_D\|^2}\right). \quad (14)$$

E. 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 (7) and the one for the eavesdropper system with IN when the system is limited by the transmit power constraint at the relay (14), 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 eavesdropper system with AN (11) with the peaceful system (7). 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 $\frac{P_R|g_E|^2}{P_{S,2}\|\boldsymbol{h}_E\|^2}$, 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 IN limited by the IN power constraint.

These observations are expressed analytically in the following proposition.

Proposition 1. *The difference in high-SNR power offset between the peaceful system and the eavesdropper system with IN is given by*

$$\Delta\mathcal{L}_{\infty} = \log\left(\frac{\left(P_R\|\boldsymbol{g}_D\|^2 + P_{S,1}\|\boldsymbol{h}_R\|^2\right)\left|\boldsymbol{h}_R^H \boldsymbol{w}_{Eve}^{\perp}\right|^2}{\left(P_R\|\boldsymbol{g}_D\|^2 + P_{S,1}\left|\boldsymbol{h}_R^H \boldsymbol{w}_{Eve}^{\perp}\right|^2\right)\|\boldsymbol{h}_R\|^2}\right)$$

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

$$\Delta\mathcal{L}_{\infty} = \log\left(\frac{\left(P_{S,1}\|\boldsymbol{h}_R\|^2 + P_R\|\boldsymbol{g}_D\|^2\right)P_{S,2}\|\boldsymbol{h}_E\|^2\left|\boldsymbol{h}_R^H \boldsymbol{w}_{Eve}^{\perp}\right|^2}{\left(P_{S,1}\left|\boldsymbol{h}_R^H \boldsymbol{w}_{Eve}^{\perp}\right|^2|g_E|^2 + P_{S,2}\|\boldsymbol{g}_D\|^2\|\boldsymbol{h}_E\|^2\right)P_R\|\boldsymbol{h}_R\|^2}\right)$$

if the transmit power is limited by the transmit power constraint P_R.

The proof is omitted due to space limitations.

Remark 1. *In the case where the transmit power at the relay is limited by the IN power constraint, the high-SNR power offset difference gets zero, i.e., $\Delta\mathcal{L}_{\infty} = 0$, iff $\boldsymbol{w}_{Eve}^{\perp} = \boldsymbol{w}_{Relay}^{MRT}$, i.e., the channels $\boldsymbol{h}_R$ and $\boldsymbol{h}_E$ are orthogonal.*

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

Proposition 2. *For the eavesdropper system with AN, the achievable secrecy rates becomes positive if*

$$\rho \geq \frac{|g_E|^2 - \|\boldsymbol{g}_D\|^2}{P_{S,2}\|\boldsymbol{g}_D\|^2\|\boldsymbol{h}_E\|^2}.$$

The proof is straightforward and therefore omitted.

IV. Numerical Results

For the simulations, we used a geometric channel model with a path loss coefficient of $a = 2$. 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]

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, the power at the relay was adapted to the constraints in (12).

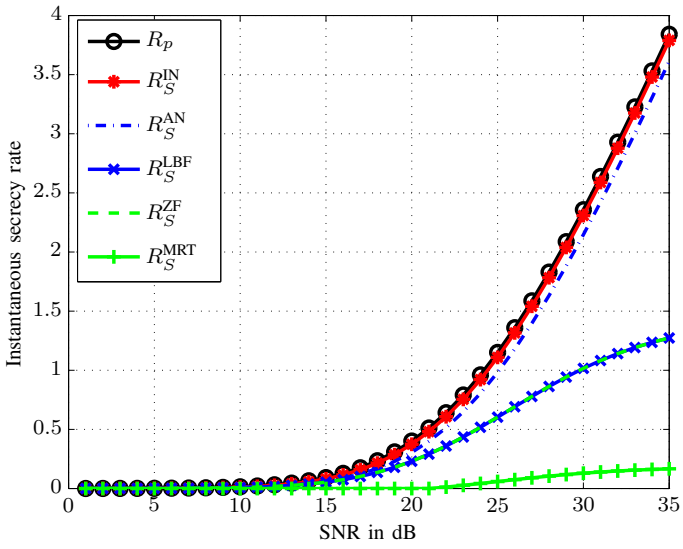


Figure 2. Rates in the 2-hop wiretap channel over the SNR.

The figures show the instantaneous achievable secrecy rates for the peaceful system according to (6) denoted by R_p and the two protection schemes IN, as introduced in Section III-D and labeled as R_S^{IN}, and AN, described in Section III-C denoted by R_S^{AN}. Additionally, the figures show the achievable secrecy rates R_S^{LBF}, R_S^{ZF} and R_S^{MRT}, which are derived by the rate

expressions in Section III-B with beamforming vectors $\boldsymbol{w}^{\text{LBF}}$, $\boldsymbol{w}_{\text{Eve}}^{\perp}$ and $\boldsymbol{w}_{\text{Relay}}^{\text{MRT}}$, respectively. In Figure 2, we used channel realizations, where the link between Alice and the relay is better than the other links:

$$|\boldsymbol{h}_R|^2 = \begin{bmatrix} 0.0002 \\ 0.0001 \\ 0.0008 \\ 0.0015 \end{bmatrix}, \; |\boldsymbol{h}_E|^2 = \begin{bmatrix} 0.0002665 \\ 0.0002332 \\ 0.0000017 \\ 0.0007034 \end{bmatrix},$$

$$|\boldsymbol{g}_D|^2 = \begin{bmatrix} 0.0000461 \\ 0.0004659 \end{bmatrix}, \text{ and } |g_E|^2 = 0.00016337$$

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 3.

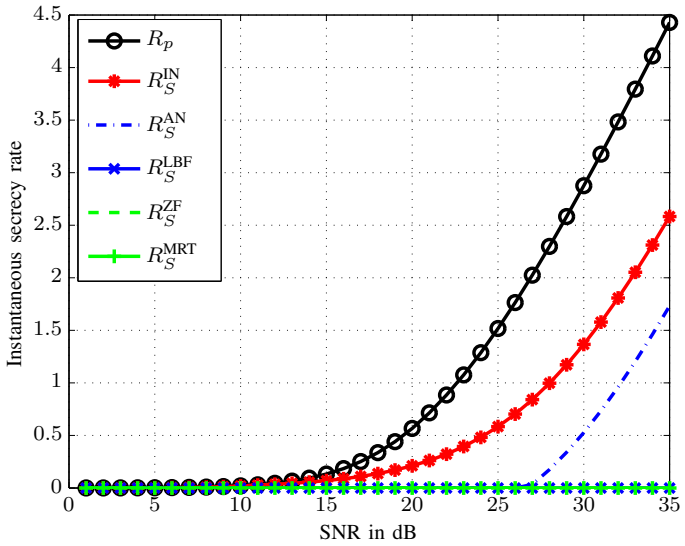


Figure 3. Rates in the 2-hop wiretap channel over the SNR.

For Figure 3, the channel gains were such that the link between the relay and the eavesdropper was advantageous:

$$|\boldsymbol{h}_R|^2 = \begin{bmatrix} 0.0003638 \\ 0.0000578 \\ 0.0009261 \\ 0.0002946 \end{bmatrix}, \; |\boldsymbol{h}_E|^2 = \begin{bmatrix} 0.0006966 \\ 0.0001848 \\ 0.0000114 \\ 0.0001544 \end{bmatrix},$$

$$|\boldsymbol{g}_D|^2 = \begin{bmatrix} 0.0004682 \\ 0.0006272 \end{bmatrix}, \text{ and } |g_E|^2 = 0.0065$$

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 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 for $\rho < 26.7325$ and gets positive values for $\rho \geq 26.7325$, as stated in Proposition 2. 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.

V. Summary

In this paper, we analyzed achievable secrecy rates in the MISO two-hop wiretap channel with four nodes, where the relay is operating in amplify-and-forward mode and all the links between the nodes are known perfectly. We discussed different transmission and protection schemes and introduced interference neutralization as a new protection scheme. We showed, that the interference neutralization scheme has the lowest power offset compared to the peaceful system and outperforms AN.

Future work will include the analysis of the influence of imperfect channel state information.

References

[1] A. D. Wyner, "The Wire-tap Channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," ser. Foundations and Trends in Communications and Information Theory. NOW Publishers, 2009, vol. 5, no. 4-5, pp. 355–580.

[5] E. A. Jorswieck, A. Wolf, and S. Gerbracht, "Secrecy on the Physical Layer in Wireless Networks," in *Trends in Telecommunications Technologies*, C. J. Bouras, Ed. INTECH, 2010, ch. 20, pp. 413–435. [Online]. Available: http://sciyo.com/articles/show/title/secrecy-on-the-physical-layer-in-wireless-networks

[6] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, 2011.

[7] L. Lai and H. El Gamal, "The Relay–Eavesdropper Channel: Cooperation for Secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[8] F. Gabry, R. Thobaben, and M. Skoglund, "Outage Performance and Power Allocation for Decode-and-Forward Relaying and Cooperative Jamming for the Wiretap Channel," in *IEEE International Conference on Communications Workshops (ICC)*, Jun. 2011, pp. 1–5.

[9] ——, "Outage performances for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel," in *IEEE Wireless Communications and Networking Conference*, Mar. 2011, pp. 1328–1333.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[11] L. Dong and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," in *Proc. IEEE International Conference on Communications (ICC)*, 2011.

[12] J. Huang and A. L. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, 2011.

[13] S. Mohajer, S. N. Diggavi, C. Fragouli, and D. Tse, "Transmission Techniques for Relay-Interference Networks," in *Annual Allerton Conference on Communication, Control, and Computing*, Sep. 2008, pp. 467–474.

[14] S. Berger, M. Kuhn, A. Wittneben, T. Unger, and A. Klein, "Recent Advances in Amplify-and-Forward Two-Hop Relaying," *IEEE Commun. Mag*, vol. 47, no. 7, pp. 50–56, Jul. 2009.

[15] Z. K. M. Ho and E. Jorswieck, "Instantaneous relaying: Optimal strategies and interference neutralization," *IEEE Trans. Signal Process.*, no. 99, 2012.

[16] A. Lozano, A. M. Tulino, and S. Verdú, "High-SNR Power Offset in Multiantenna Communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134–4151, Dec. 2005.