Interference Leakage Neutralization in Two-Hop Wiretap Channels with Partial CSI

Sabrina Engelmann, Zuleita K.-M. Ho, and Eduard A. Jorswieck

Communications Theory, Communications Laboratory
Department of Electrical Engineering and Information Technology
Technische Universität Dresden, Germany
Email: {sabrina.engelmann,zuleita.ho,eduard.jorswieck}@tu-dresden.de

***Abstract*—In this paper, we analyze the four-node relay wiretap channel, where the relay performs amplify-and-forward. There is no direct link between transmitter and receiver available. The transmitter has multiple antennas, which assist in securing the transmission over both phases. In case of full channel state information (CSI), the transmitter can apply information leakage neutralization in order to prevent the eavesdropper from obtaining any information about the signal sent. This gets more challenging, if the transmitter has only an outdated estimate of the channel from the relay to the eavesdropper. For this case, we optimize the worst case secrecy rate by choosing intelligently the beamforming vectors and the power allocation at the transmitter and the relay.**

***Index Terms*—Worst case secrecy rate, two-hop wiretap channel, amplify-and-forward, interference leakage 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 years. A comprehensive overview on the topic of secrecy on the physical layer can be found in [1], [2], [3].

In multi-hop communications, the wiretapper has usually access to multiple signal transmissions. Hence the chance of eavesdropping messages is increased. However, the cooperative nodes can also be an encumbrance to the eavesdropper. Because of this tradeoff, the multi-hop scenario is interesting yet difficult. One intuitive idea to enhance secrecy is to confuse the eavesdropper by artificial noise (AN) signals. This has been widely adopted including in relay wiretap channels [4], the four-node two-hop channel and in scenarios with imperfect channel information [5], [6]. The drawback of the AN scheme is the dependency on wiretap codes. In order to lift this dependency, we utilize interference neutralization, which is a technique to cancel interference algebraically by carefully choosing the multi-hop strategies [7], [8]. If applied to secrecy rate scenarios, the technique is called interference leakage neutralization (IN) [9].

In our previous work [10] with full channel state information (CSI), we showed that IN performs better compared to AN protected schemes, especially in the mid SNR regime. Here, we extend these results to the case of partial CSI. All nodes have only local CSI and the transmitter has additionally an outdated estimation of the channel between the relay and the eavesdropper. We compute the feasibility conditions of IN and maximize the worst case secrecy rates by optimizing the power allocations at the transmitter and the relay. Depending on the channel realizations and the quality of the CSI, IN can outperform AN.

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. $\Pi_{\boldsymbol{X}}^{\perp}$ is the orthogonal projector onto the orthogonal complement of the column space of $\boldsymbol{X}$, i.e., $\Pi_{\boldsymbol{X}}^{\perp} = \boldsymbol{I} - \Pi_X$ 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 two-hop wiretap channel considered in this paper is based on the non-degraded Gaussian wiretap channel described in [11]. The transmitter Alice wants to send a confidential message over a relay, which is operating in amplify-and-forward mode, 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 have 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.

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. Furthermore, we assume local channel state information (CSI) at the transmitter, i.e., Alice has perfect knowledge about her channels to the relay and the eavesdropper. Furthermore, we

This work was funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16 KIS 0009, Prophylaxe). The authors alone are responsible for the content of the paper.

This work has been performed in the framework of the European research project DIWINE, which is partly funded by the European Union under its FP7 ICT Objective 1.1 - The Network of the Future.

assume that the relay communicates the channel estimation of the channel g_E to Alice, which results in Alice having an outdated g_E and we model this as

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

where $\hat{g}_E$ is the estimation on the channel g_E and Δg_E is the estimation error, which is bounded by $|\Delta g_E|^2 \leq \epsilon$. If the channel estimation is done at the relay using training-sequences, the estimation error ϵ can be modeled as a scaled version of the channel estimation mean square error (MSE) [12], [13]. Bob is assumed to have local CSI, i.e., $\boldsymbol{g}_D$, for decoding purposes.

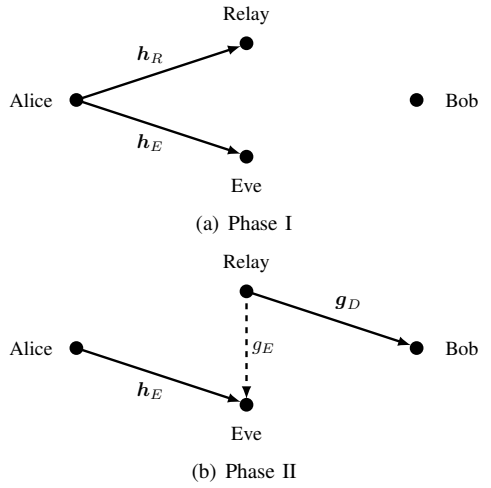

Figure 1. The system model of a four-node two-hop wiretap channel with a half-duplex relay.

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

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

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 $\sqrt{\alpha}$ is the multiplication scalar at the relay. 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 receive beamforming vector at the intended receiver Bob in the second phase is given by $\boldsymbol{w}_D$. The secrecy rate is then

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

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

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

with

$$\alpha = \frac{\rho p_R}{\rho p_{S,1} \left| \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} \right|^2 + 1}. \tag{3}$$

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

In (2), 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. Beamforming Vectors

In this subsection we summarize the optimum beamforming vectors. In the first phase, Alice applies zero forcing (ZF) with regard to Eve in order to prevent Eve from overhearing the signal sent to the relay, i.e., $\boldsymbol{w}_{S,1} = \boldsymbol{w}_{\text{Eve}}^{\perp}$. In the second phase, Alice sends a signal that only serves the purpose of protecting the main data signal. As this signal is explicitly designed for Eve, Alice applies maximum ration transmission (MRT) to Eve, i.e., $\boldsymbol{w}_{S,2} = \boldsymbol{w}_{\text{Eve}}^{\text{MRT}}$. Bob maximizes his receive signal with maximum ratio combining, i.e., $\boldsymbol{w}_D = \boldsymbol{w}^{\text{MRC}}$. These three beamforming vectors are defined as

$$\boldsymbol{w}_{\text{Eve}}^{\text{MRT}} = \frac{\boldsymbol{h}_E}{\|\boldsymbol{h}_E\|^2}, \quad \boldsymbol{w}_{\text{Eve}}^{\perp} = \frac{\Pi_{\boldsymbol{h}_E}^{\perp} \boldsymbol{h}_R}{\left\| \Pi_{\boldsymbol{h}_E}^{\perp} \boldsymbol{h}_R \right\|}, \text{ and } \boldsymbol{w}^{\text{MRC}} = \frac{\boldsymbol{g}_D}{\|\boldsymbol{g}_D\|^2}.$$

III. Interference Leakage Neutralization with Full CSI

In the case of perfect CSI, the estimation error zero, i.e., $\epsilon = 0$ and $\hat{g}_E = g_E$. Therefore the transmitter can construct a signal x_n, that fulfills

$$-\sqrt{\alpha} g_E \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x = \boldsymbol{h}_E^H \boldsymbol{w}_{S,2} x_n$$

and neutralizes the eavesdropped signal at Eve that she receives over the relay in the second phase.

Applying the beamforming vectors as discussed in Section II-B, the IN signal is given by

$$x_n = -\frac{\sqrt{\alpha} g_E \boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp}}{\boldsymbol{h}_E^H \boldsymbol{w}_{\text{Eve}}^{\text{MRT}}} x. \tag{4}$$

The secrecy rate with $p_{S,1} = P_{S,1}$ is calculated to[1]

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

Remark 1. *Due to the fact that Eve gets no data signal at all, Alice can perform conventional channel coding instead of the more complex secrecy binning that is required to achieve* (1) *in general.*

[1]We will show later in Section IV-A that the optimal transmit power of the transmitter in the first phase is full power, i.e., $p_{S,1} = P_{S,1}$.

In order to successfully neutralize the signal at the eavesdropper, $p_{S,2}$ has to fulfill

$$\mathbb{E}_x\left[|x_n|^2\right] = \frac{\alpha P_{S,1}|g_E|^2\left|\boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2}{\|\boldsymbol{h}_E\|^2} = p_{S,2} \leq P_{S,2}. \quad (5)$$

In the following, we examine the effect of partial CSI and the optimum strategies for worst case secrecy maximization,

IV. Interference Leakage Neutralization with Partial CSI

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

$$L(x_n) = \left|\boldsymbol{h}_E^H \boldsymbol{w}_{S,2} x_n + \sqrt{\alpha} g_E \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x\right|^2.$$

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

Proposition 1. *The optimal IN transmit signal x_n with regard to the minimized leakage power $L(x_n)$ and the worst case channel estimation error $|\Delta g_E|^2$ is given by*

$$\arg\min_{x_n} \max_{|\Delta g_E|^2 \leq \epsilon} L(x_n) = -\frac{\sqrt{\alpha}\hat{g}_E \boldsymbol{h}_R^H \boldsymbol{w}_{S,1}}{\boldsymbol{h}_E^H \boldsymbol{w}_{S,2}} x.$$

Proof: We prove this proposition by contradiction.

Let us assume Alice uses a channel estimation γ_E to get the IN transmit signal

$$x_n = -\frac{\sqrt{\alpha}\gamma_E \boldsymbol{h}_R^H \boldsymbol{w}_{S,1}}{\boldsymbol{h}_E^H \boldsymbol{w}_{S,2}} x.$$

The optimization problem is therefore given as

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

with

$$\begin{aligned} L(\gamma_E) &= \left|\boldsymbol{h}_E^H \boldsymbol{w}_{S,2} x_n + \sqrt{\alpha} g_E \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x\right|^2 \\ &= \left|\sqrt{\alpha}\left(\hat{g}_E + \Delta g_E - \gamma_E\right) \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x\right|^2. \end{aligned} \quad (6)$$

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

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

Let us first examine the leakage power with $\gamma_E^* = \hat{g}_E$. Using (6) we get

$$\begin{aligned} \max_{|\Delta g_E|^2 \leq \epsilon} L(\gamma_E^* = \hat{g}_E) &= \max_{|\Delta g_E|^2 \leq \epsilon} \left|\sqrt{\alpha}\left(\Delta g_E\right) \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x\right|^2 \\ &= \epsilon\alpha \left|\boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x\right|^2. \end{aligned}$$

If we now take a look at some other $\gamma_E = \hat{g}_E + \zeta$, where ζ is some estimation error with $|\zeta|^2 \leq \epsilon$, (6) becomes

$$\begin{aligned} &\max_{|\Delta g_E|^2 \leq \epsilon} L(\gamma_E = \hat{g}_E + \zeta) \\ &= \max_{|\Delta g_E|^2 \leq \epsilon} \left|\sqrt{\alpha}\left(\Delta g_E - \zeta\right) \boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x\right|^2 \\ &= \left(\epsilon + |\zeta|^2\right) \alpha \left|\boldsymbol{h}_R^H \boldsymbol{w}_{S,1} x\right|^2. \end{aligned}$$

It is easy to see that $L(\gamma_E^* = \hat{g}_E) \leq L(\gamma_E = \hat{g}_E + \zeta)$ and therefore it holds that $L(\hat{g}_E) \leq L(\gamma_E) \quad \forall \gamma_E$. □

From Proposition 1 and the beamforming vectors in Section II-B, the receive signal at Eve in the second phase can be calculated to

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

and the corresponding worst case SINR is therefore given as

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

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

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

Remark 2. *In order to achieve this secrecy rate, a wiretap code is needed again.*

A. Optimization Problem

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

From (3) and (5), the transmit power at the relay is

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

Note that p_R correlates with $p_{S,2}$ as the power values must be chosen jointly such that the leakage signals from source and relay add to zero. The maximization problem over the power p_R is given as

$$\begin{aligned} \max_{p_R} \; & R_S^{\text{pCSI}} \quad (7) \\ \text{s.t.} \; & p_R \leq \frac{P_{S,2}\|\boldsymbol{h}_E\|^2\left(\rho P_{S,1}\left|\boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2 + 1\right)}{\rho P_{S,1}|\hat{g}_E|^2\left|\boldsymbol{h}_R^H \boldsymbol{w}_{\text{Eve}}^{\perp}\right|^2}, \\ & 0 \leq p_R \leq P_R. \end{aligned}$$

B. Analysis of Monotonicity

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

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

and define the worst case channel gain as

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

Proposition 2. *The optimal power allocation $\tilde{p}_R$ at the relay solving the optimization problem* (7) *is given in Table I, where*

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

$$p_R^* = \frac{(1+\tilde{\rho})\left(\sqrt{\epsilon\|\boldsymbol{g}_D\|^2(\tilde{\rho}(\|\boldsymbol{g}_D\|^2 - \epsilon) + s)s} + \|\boldsymbol{g}_D\|^2\left(|\tilde{g}_E|^2 - \epsilon\right)\right)}{\rho\|\boldsymbol{g}_D\|^2\left(\epsilon\tilde{\rho}s + \epsilon\|\boldsymbol{g}_D\|^2 - |\tilde{g}_E|^4\right)}, \text{ and}$$

$$s = \|\boldsymbol{g}_D\|^2 - |\tilde{g}_E|^2.$$

Case	Behavior of R_S^{pCSI} with regard to p_R	Optimal power allocation $\tilde{p}_R$
i) $\lvert\tilde{g}_E\rvert^2 \geq \lVert\boldsymbol{g}_D\rVert^2 \geq \epsilon$	monotonic increasing	$\tilde{p}_R = \min\left(p_R^{\max}, P_R\right)$
ii) $\lVert\boldsymbol{g}_D\rVert^2 \geq \lvert\tilde{g}_E\rvert^2 \geq \epsilon$		
a) $\left(\lvert\tilde{g}_E\rvert^4 + \lvert\tilde{g}_E\rvert^2 \epsilon\tilde{\rho}\right) \geq \epsilon\lVert\boldsymbol{g}_D\rVert^2 (1+\tilde{\rho})$	monotonic increasing	$\tilde{p}_R = \min\left(p_R^{\max}, P_R\right)$
b) $\left(\lvert\tilde{g}_E\rvert^4 + \lvert\tilde{g}_E\rvert^2 \epsilon\tilde{\rho}\right) < \epsilon\lVert\boldsymbol{g}_D\rVert^2 (1+\tilde{\rho})$	quasi-concave	$\tilde{p}_R = \min\left(p_R^*, p_R^{\max}, P_R\right)$
iii) $\lVert\boldsymbol{g}_D\rVert^2 \geq \epsilon \geq \lvert\tilde{g}_E\rvert^2$	quasi-concave	$\tilde{p}_R = \min\left(p_R^*, p_R^{\max}, P_R\right)$
iv) $\lvert\tilde{g}_E\rvert^2 \geq \epsilon \geq \lVert\boldsymbol{g}_D\rVert^2$	quasi-convex	$\tilde{p}_R = \begin{cases} p_R^{\max} & \text{if } \frac{(\tilde{\rho}+1)\left(\lVert\boldsymbol{g}_D\rVert^2-\epsilon\right)}{\rho\lVert\boldsymbol{g}_D\rVert^2\left(\epsilon-\lvert\tilde{g}_E\rvert^2\right)} < p_R^{\max} < P_R \\ P_R & \text{if } \frac{(\tilde{\rho}+1)\left(\lVert\boldsymbol{g}_D\rVert^2-\epsilon\right)}{\rho\lVert\boldsymbol{g}_D\rVert^2\left(\epsilon-\lvert\tilde{g}_E\rvert^2\right)} < P_R \leq p_R^{\max} \\ 0 & \text{otherwise} \end{cases}$
v) $\epsilon \geq \lvert\tilde{g}_E\rvert^2 \geq \lVert\boldsymbol{g}_D\rVert^2$	negative	$\tilde{p}_R = 0$
vi) $\epsilon \geq \lVert\boldsymbol{g}_D\rVert^2 \geq \lvert\tilde{g}_E\rvert^2$	negative	$\tilde{p}_R = 0$

Table I
THE BEHAVIOR OF THE SECRECY RATE R_S^{pCSI} WITH REGARD TO p_R AND THE OPTIMAL POWER ALLOCATION $\tilde{p}_R$.

The corresponding optimal power allocation $\tilde{p}_{S,2}$ is given by

$$\tilde{p}_{S,2} = \frac{\tilde{p}_R\tilde{\rho}\,\lvert\hat{g}_E\rvert^2}{\lVert\boldsymbol{h}_E\rVert^2(\tilde{\rho}+1)}.$$

The proof is omitted due to space limitations.

From Table I, there are only four different power allocations p_R^* out of the six cases depending on the behavior of the secrecy rate R_S^{pCSI}.

As long as the channel gain $\lVert\boldsymbol{g}_D\rVert^2$ to the intended receiver is greater than the uncertainty over the channel $\lvert g_E\rvert^2$, i.e., the estimation error ϵ (case i) to iii)), the secrecy rate is positive. In particular, in the case where R_S^{pCSI} is quasi-concave (case ii b) and iii)), the secrecy rate becomes negative for large values of p_R. If the secrecy rate is monotonic increasing in p_R(case i) and ii a)), the optimal power allocation is either bounded by the power constraint P_R at the relay or by the power constraint $P_{S,2}$ at the transmitter.

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

For the case where the worst case estimation error ϵ is greater than the channel gain $\lVert\boldsymbol{g}_D\rVert^2$ (case iv)), the secrecy rate R_S^{pCSI} is zero if only a small amount of power is allocated. As soon as we allocate more power than $p_R^0 = \frac{(\tilde{\rho}+1)\left(\lVert\boldsymbol{g}_D\rVert^2-\epsilon\right)}{\rho\lVert\boldsymbol{g}_D\rVert^2\left(\epsilon-\lvert\tilde{g}_E\rvert^2\right)}$, the secrecy rate becomes monotonic increasing as long as the worst case channel gain $\lvert\tilde{g}_E\rvert^2$ to Eve is greater than the estimation error and the channel to Bob. Therefore, the optimal power allocation is again either bounded by the power constraint P_R at the relay or by the power constraint $P_{S,2}$ at the transmitter, as long as these power constraints are greater than p_R^0. Otherwise, the secrecy rate is zero and no power should be allocated.

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

V. NUMERICAL RESULTS

For the simulations, we use a geometric channel model with a path loss coefficient of $a = 2$. The nodes are 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 are generated randomly and weighted by the distances between the nodes. The transmitter is equipped with four antennas, while the receiver has only two antennas. The power constraints at the transmitter and the relay are set to $P_{S,1} = P_{S,2} = P_R = 10$ dB. The maximum estimation error ϵ over the channel g_E is calculated to $\epsilon = \frac{1}{\text{SNR}^2} + \delta$, where δ is a constant which represents the delay caused by the need of feeding back the CSI from the relay to the receiver.

The IN scheme for partial CSI (R_S^{pCSI}) is compared to several base line systems:

- The peaceful system without eavesdropper. The capacity R_p is achieved if Alice performs MRT to the relay.
- The IN secrecy rate R_S^{fCSI} with full CSI as presented in Section III.
- The AN noise scheme, where Alice sends a random AN signal in the second phase in order to disturb Eve (R_S^{AN}).
- The unprotected scheme, where Alice only uses an optimized beamformer, which is a linear combination between MRT and ZF (R_S^{BF}) during the first phase.

Note, that the IN scheme is the only scheme that is influences by the partial CSI on the channel g_E as all other schemes do

not transmit over this channel.

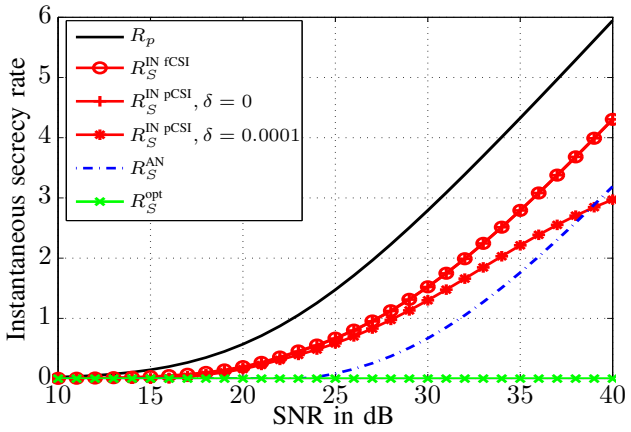

Figure 2. Instantaneous capacity for the peaceful system and instantaneous secrecy rates for various protection schemes over SNR with $n_T = 4$, $n_R = 2$, and $P_{S,1} = P_{S,2} = P_R = 10$dB.

For the secrecy rate $R_S^{\text{IN pCSI}}$ in Figure 2, where the delay δ equals zero, the transmitter has instantly the channel estimation over the channel g_E. Although this scenario is quite unrealistic, we can see clearly, that the IN schemes for full and partial CSI perform identically well. If the delay is greater than zero, e.g., $\delta = 0.0001$, the IN scheme for partial CSI is performing worse than the IN scheme for full CSI in the high SNR regime. This is due to the fact that with outdated CSI the system gets limited by the negative term in high SNR. For the chosen channel realizations, the IN schemes outperform the AN scheme. Especially in the mid SNR range, the AN scheme still achieves zero secrecy rates, while the IN schemes achieve positive rates. Due to the missing protection of the data signal in the second phase, the beamforming scheme performs badly.

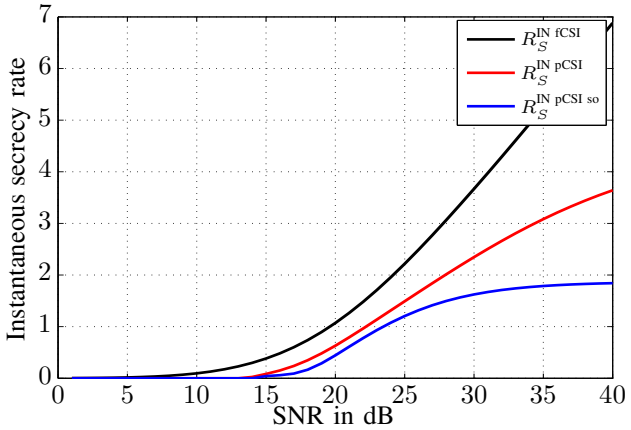

Figure 3. Instantaneous secrecy rates over SNR for IN protected schemes with full and partial CSI ($\delta = 0.0001$), $n_T = 4$, $n_R = 2$, $P_{S,1} = P_{S,2} = 10$dB and $P_R = 50$dB.

If we apply a simplified power allocation algorithm, where the power at the relay and the transmitter in the second phase are either bounded by the power constraint $P_{S,2}$ or by the power constraint P_R, we achieve the suboptimal secrecy rate $R_S^{\text{IN pCSI so}}$. Figure 3 shows for $\delta = 0.0001$ and $P_R = 50$dB how this suboptimal scheme performs compared to the optimal IN scheme for full and partial CSI. For the mid SNR range the difference between both schemes is marginal, while in the high SNR regime the gap is growing fast.

VI. Summary

In this paper, we analyzed the four-node relay wiretap channel, where the relay performs amplify-and-forward and where no direct link between transmitter and receiver is available. The transmitter has multiple antennas, which assist in securing the transmission over both phases. In case of full CSI, the transmitter can apply IN and prevent the eavesdropper from obtaining any information about the signal sent. We showed that if the transmitter has only an outdated estimation over the channel from the relay to the eavesdropper, IN can still be applied in certain cases. For these cases, we determine the worst case secrecy rate and optimize the power allocations at transmitter and relay. Numerical simulations visualize the theoretical results.

References

[1] 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.

[2] 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://dx.doi.org/10.5772/8472

[3] M. Bloch and J. a. Barros, *Physical-Layer Security*, first edit ed. Cambridge University Press, 2011.

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

[5] 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 *Proc. of IEEE International Conference on Communications (ICC)*, Jun. 2011, pp. 1–5.

[6] ——, "Outage Performances for Amplify-and-Forward, Decode-and-Forward and Cooperative Jamming Strategies for the Wiretap Channel," in *Proc. of IEEE Wireless Communications and Networking Conference*, Mar. 2011, pp. 1328–1333.

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

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

[9] K.-M. Z. Ho and E. A. Jorswieck, "Instantaneous Relaying: Optimal Strategies and Interference Neutralization," *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6655–6668, Dec. 2012.

[10] S. Gerbracht, E. A. Jorswieck, G. Zheng, and B. Ottersten, "Non-regenerative Two-Hop Wiretap Channels using Interference Neutralization," in *Proc. of IEEE International Workshop on Information Forensics and Security (WIFS)*, Dec. 2012, pp. 258–263.

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

[12] E. Björnson, G. Zheng, M. Bengtsson, and B. Ottersten, "Robust Monotonic Optimization Framework for Multicell MISO Systems," *IEEE Transactions on Signal Processing*, vol. 60, no. 5, pp. 2508–2523, May 2012.

[13] G. Zheng, K.-K. Wong, and T.-S. Ng, "Robust Linear MIMO in the Downlink: A Worst-Case Optimization with Ellipsoidal Uncertainty Regions," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, 2008.