Beating Resource Constrained Eavesdroppers: A Physical Layer Security Study

Albert Sunny, Siddhartha Sarma and Joy Kuri
Department of Electronic Systems Engineering
Indian Institute of Science, Bangalore, India
Email: {albert, siddharth, kuri}@dese.iisc.ernet.in

***Abstract*—In this paper, by augmenting *beamforming* with *signal nulling*, we present a scheme to improve the equivocation in wireless relay networks. Assuming global channel state information, memoryless adversaries, and the decode-and-forward relaying strategy, we seek to maximize the average achievable secrecy rate between the source and the legitimate destination, subject to an overall power budget per message. Then, exploiting the structure of the optimization problem, we present an online sequential approach to compute an achievable average rate. Finally, we use numerical evaluations to compare our method with the conventional schemes.**

***Index Terms*—Beamforming, Signal Nulling, Physical Layer Security, Resource Allocation, Relay Networks, Memoryless Eavesdroppers**

I. Introduction

Physical layer security, an information theoretic approach to security in wireless networks, was proposed by Wyner almost four decades ago [1]. Its provable security has driven researchers and scientists alike, to look at physical layer security as an alternative to the traditional cryptographic schemes. Physical layer security enables secure transmission at non-zero data rate between two communicating nodes, by exploiting the degraded nature of the eavesdropper channel and the inherent randomness of the wireless medium [1], [2]. A rate at which data can be transferred from the source to the legitimate destination keeping eavesdropper ignorant about the message is termed an achievable *secrecy rate* in the physical layer security literature.

In many practical scenarios, a single node acting on its own may not be sufficient to ensure non-zero secrecy rate. To tackle such scenarios and to improve the data rate of secure transmissions, researchers have proposed several cooperative communication schemes. In such cooperative communication schemes, in addition to the source node, one or more nodes are employed to aid the source in improving the data rate of its secure transmissions. These additional nodes are used as relays, jammers or as both. The role of relays in improving transmission rates in wireless networks is well established in the literature [3], [4]. In contrast, jamming in wireless networks is a double-edged sword. While it can effectively degrade the *signal-to-noise ratio* (SNR) at eavesdroppers, if not used carefully, it can also degrade reception at legitimate receivers. A workaround to this issue is to either null the jamming signal at the destination with the help of multiple jammers, or pass information about the jamming signal to the legitimate receiver [5], [6], [7]. While the use of multiple jammers is a quick and easy fix, it almost always leads to synchronization related issues. On the other hand, making the the jamming signal available at the legitimate receiver a priori is not very practical.

In many real-world wireless networks, it is desirable to transfer messages to a selected node, while keeping other nodes in the network ignorant of the information contained within the messages (*e.g.* Pay TV broadcast, Wi-fi access networks). In such networks, every node (user) in the network can be considered as an adversary (eavesdropper) with respect to every other node. Such nodes are resource limited (*e.g.* power and memory constrained sensor nodes), and do not wish to invest much of their resources for eavesdropping. The notion of similar weak adversaries has appeared in the literature before [8], [9]. Motivated by this, we present a framework where a previously transmitted secure message is used as the jamming signal, to improve the secrecy rate of the current message. The main contributions of this paper are as follows

- We incorporate two well-appreciated cooperative schemes, beamforming and signal nulling, into a single power allocation framework for improving secrecy rate.
- We pose the problem of maximizing the average achievable secrecy rate, subject to an overall power budget.
- By exploiting the structure of the optimization problem, we propose an approach to obtain an achievable average rate.

The remainder of the paper is organized as follows. In Section II, we compare and contrast our approach with similar schemes existing in the literature. In Section III, we present the system model. In Section IV, we discuss our two phase cooperative scheme and the formulation of our optimization problem, in detail. In Section V, we present a lower bound for the problem formulated in Section IV. The numerical evaluations of various schemes are presented in Section VI. Finally, we conclude the paper in Section VII.

II. Related Works

In recent years, several researchers have demonstrated the potential of cooperative schemes in improving the achievable

978-3-9018-8273-9/15/

secrecy rates of wireless systems [10], [11], [12], [13]. In [10], [11], [12], the authors use cooperative nodes to inject weighted jamming signals, to degrade the eavesdropper channel. In [13], the authors study scenarios where the destination itself injects artificial noise and uses self-interference subtraction to confound the eavesdroppers. Several variants of the destination assisted secure communication scheme can also be found in [14], [15], [16].

While the cooperative scheme presented in this paper can be classified as cooperative relaying and jamming for decode-and-forward (DF) relay networks studied in [17], [18], [19], [20], we would like to highlight the fact that the problem we have looked at is significantly different from the ones addressed by the above mentioned papers. In [17], [18], [19], [20], the authors have considered separate relays and jammers, and then evaluated the achievable secrecy rate under power constraints. In contrast, we do not have any dedicated jammer in our model.

The first phase of our proposed scheme is similar to the scheme in [15]. However, unlike them, we do not assume the availability of information regarding the jamming noise signal at the receiver. In our scheme, we use the previous securely-transmitted message for jamming. But such a scheme may result in *information leakage*. Therefore, to limit the information leaked, we devise an optimal power allocation problem with leakage constraints. Similar leakage constrained power allocation problems have also been considered in [21].

The second phase of our scheme is similar to cooperative beamforming. In [22], [11] the authors have highlighted the role of *cooperative beamforming* in improving the secrecy rate of decode and forward networks with total and individual power constraints. While the cooperative schemes in [22], [11] beamform just one signal, we simultaneously beamform two signals to the destination. Though such an approach resembles the artificial noise assisted transmission considered in [5], [23], [24], we use the previous securely-transmitted message in place of artificial noise. Since the previous secure message is available only at the legitimate destination and not at the eavesdropper, our scheme will only degrade the SNR at eavesdropper and not at the legitimate destination.

III. System Model

We consider a *Decode-and-Forward* (DF) relay network consisting of a source s, a trusted relay node r, a legitimate destination d (see Fig. 1). All the nodes in the network are equipped with a *single antenna* and function in *half-duplex* mode. In this paper, for simplicity, we consider a single eavesdropper e. However, the cooperative scheme presented in this paper can be extended to networks with multiple eavesdroppers. We note that memoryless eavesdroppers are a special case of resource constrained eavesdroppers. Therefore, for ease of illustration, as in [9], we assume the eavesdropper to be memoryless.

The background noise at node $i \in \{d, r, e\}$ is assumed to be $Z_i \sim \mathcal{CN}(0, \sigma^2)$ *i.e.,* a circularly symmetric complex Gaussian noise. All channels are assumed to undergo flat fading. Let $h_{ij} \in \mathbb{C}$ denote the complex baseband channel gain between nodes $i \in \{s, r, d\}$ and $j \in \{r, d, e\}$. Information about the eavesdropper's channel can be obtained in networks where the eavesdroppers themselves are users in the network [11]. Therefore, as in [11], [25], [6], we assume perfect channel state information (CSI). We also assume that the source and relay have knowledge of the eavesdropper's channel condition. This assumption is especially valid in networks with broadcast and unicast transmission, where each terminal acts as a legitimate receiver for one signal and as an eavesdropper for some other signal.

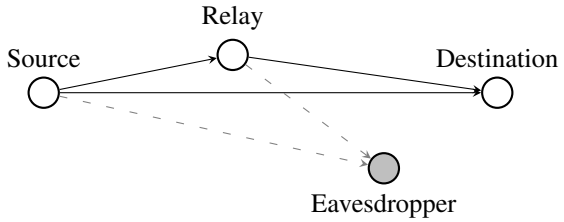

Fig. 1. A network with a trusted relay, a passive eavesdropper and a source destination pair

We would like to transfer a sequence of independent message $\{W_j, j \geq 0\}$ from the source to the destination using physical layer security, keeping the eavesdropper ignorant of the information contained in the messages. A source encoder maps message W_j to an independent *Gaussian codeword* $\mathbf{X}_j^n \in \mathcal{X}^n$. A codeword $\mathbf{X}_j^n$ consists of n symbols, each of them belonging to the alphabet set $\mathcal{X} \subset \mathbb{C}$. Without loss of generality, we assume that for all $j \geq 0$, $\mathbb{E}[\mathbf{X}_j^n] = \mathbf{0}_{n\times 1}$ and $\frac{1}{n}\mathbb{E}[||\mathbf{X}_j^n||_2^2] = 1$. The encoding, decoding and the cooperative scheme are public knowledge, only the information contained in the messages is private. As in [11], we consider a time division multiple access system, in which there are n time units in each transmission slot. Let $\mathbf{Y}_{i,l}^n$ denote the signal recieved by node $i \in \{r, d, e\}$ in the l^{th} transmission slot.

IV. A Cooperative Two Phase Scheme

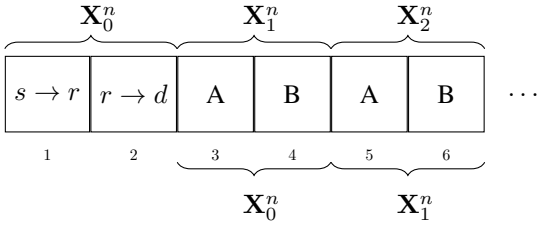

Fig. 2. Figure denoting the codewords and the schemes used in different transmission slots; (A) and (B) phases are used in alternating transmission slots. The codewords at the top of figure denote the new codewords being transferred, and those at the bottom are used to improve the secrecy rate.

A simple scheme to transfer the codewords from the source to the destination is via *direct* source-destination transmission,

which requires only n time units (*one* transmission slot). However such a naive scheme may result in poor secrecy rates. To achieve better secrecy rates, we propose a cooperative two phase transmission scheme that transmits the codeword using *signal nulling* and *beamforming*.

In our two phase scheme, with the help of the securely transferred previous message, we alternatively use A and B phases to transfer new messages from the source to the destination (see Fig. 2 for a detailed illustration).

A. Consequence of Memoryless Eavesdropper

As in [9], we consider the *eavesdropper to be memoryless* i.e., the eavesdropper decodes the message only from the signal received in the current transmission slot. A direct consequence of this assumption is the following $\forall j \geq 0$

$$\begin{aligned} I_j &= I(W_j; \{\mathbf{Y}_{i,l}^n, l \geq 1\}) \\ &\overset{(a)}{\leq} \max_{l \geq 1} I(W_j; \mathbf{Y}_{i,l}^n) \overset{(b)}{=} \max_{l \in \{2j+1, 2j+2, 2j+3, 2j+4\}} I(W_j; \mathbf{Y}_{i,l}^n) \end{aligned} \quad (1)$$

where $I(J;K)$ denotes the mutual information between random variables J and K, and (b) follows due to the fact that codeword corresponding to message $W_j, j \geq 0$ is used only in four transmission slots i.e., slots $2j+1$, $2j+2$, $2j+3$ and $2j+4$ (see Fig.2). We note that inequality (a) supplies an upper bound on the leakage I_j. For ease of analysis, we replace inequality (a) with equality, thereby considering the case with the maximum possible information leakage.

B. Transferring the initial message W_0

For our scheme to work, we need to transfer the initial message W_0 securely from the source to the legitimate destination via the trusted relay. For ease of analysis, we transfer message W_0 using the two hop scheme. Under an average power constraint of p_{max} units per time unit per message, the achievable secrecy rate with respect to message W_0 is given as [22]

$$R_0 = \max_{0 \leq p+q \leq 2p_{max}} \frac{1}{2} \cdot \left[\min \left\{ \log_2 \left(\frac{\sigma^2 + |h_{sr}|^2 \cdot p}{\sigma^2 + |h_{se}|^2 \cdot p} \right), \log_2 \left(\frac{\sigma^2 + |h_{rd}|^2 \cdot q}{\sigma^2 + |h_{re}|^2 \cdot q} \right) \right\} \right]^+ \quad (2)$$

where $[\cdot]^+$ denotes the projection onto the set of non-negative real numbers. The first term in the RHS of (2) represents the secrecy rate of *source-relay* (SR) channel and the second term represents the secrecy rate of *relay-destination* (RD) channel [2]. Since the eavesdropper is memoryless, we can write the end-to-end secrecy rate as the minimum of the secrecy rate of the SR and RD channels.

The factor $1/2$ appears in (2) due to the fact that two transmission slots are needed to transfer message W_0 from the source to the destination. Let the 2-tuple (p^*, q^*) denote the optimizer of problem (2). Then, the maximum information leaked to the memoryless eavesdropper about message W_0 in the first two transmission slots is given as

$$I(W_0; \mathbf{Y}_{e,1}^n, \mathbf{Y}_{e,2}^n) = \log_2 \left(1 + \frac{\max\{|h_{se}|^2 p^*, |h_{re}|^2 q^*\}}{\sigma^2} \right)$$

Now, we present the detailed cooperative transmission scheme for message $W_j, j \geq 1$.

C. Phase A (Signal Nulling)

In the $(2j+1)^{\text{th}}$ transmission slot, the source transmits $\beta_j \cdot \mathbf{X}_j^n + \alpha_j \cdot \mathbf{X}_{j-1}^n$ and the destination transmits $\gamma_j \cdot \mathbf{X}_{j-1}^n$, simultaneously. Here $\alpha_j, \beta_j, \gamma_j \in \mathbb{C}$. The signal received at the eavesdropper and the relay, in this slot, is given as

$$\begin{aligned} \mathbf{Y}_{i,2j+1}^n &= h_{si}(\alpha_j \cdot \mathbf{X}_{j-1}^n + \beta_j \cdot \mathbf{X}_j^n) + h_{di} \cdot \gamma_j \cdot \mathbf{X}_{j-1}^n + \mathbf{Z}_i^n \\ &= (h_{si} \cdot \alpha_j + h_{di} \cdot \gamma_j) \cdot \mathbf{X}_{j-1}^n + h_{si} \cdot \beta_j \cdot X_j + \mathbf{Z}_i^n, \end{aligned} \quad (3)$$

for all $i \in \{r, e\}$. Here, $\mathbf{Z}_i^n$ is a $n \times 1$ vector of i.i.d random variables sampled from the circularly symmetric complex Gaussian distribution with variance σ^2.

Since the relay has already obtained the message corresponding to codeword $\mathbf{X}_{j-1}^n$ two slots ago, the source and the destination can choose α_j and γ_j such that codeword $\mathbf{X}_{j-1}^n$ has an *effective gain of zero* at the relay *i.e.,* $h_{sr}\alpha_j + h_{dr}\gamma_j = 0$. Now, substituting $\gamma_j = -\frac{h_{sr}}{h_{dr}} \cdot \alpha_j$ in equation (3), we obtain

$$\begin{aligned} \mathbf{Y}_{r,2j+1}^n &= h_{sr} \cdot \beta_j \cdot \mathbf{X}_j^n + \mathbf{Z}_r^n \\ \mathbf{Y}_{e,2j+1}^n &= \frac{\alpha_j(h_{se}h_{dr} - h_{sr}h_{de})}{h_{dr}} \mathbf{X}_{j-1}^n + h_{se}\beta_j \cdot \mathbf{X}_j^n + \mathbf{Z}_e^n \end{aligned}$$

Let p_1^j units be the average power constraint for the transmissions in the odd transmission slot. Then, we have the following equalities

$$\begin{aligned} p_1^j &= \frac{1}{n} \left(\mathbb{E}\left[||\alpha_j \cdot \mathbf{X}_{j-1}^n + \beta_j \cdot \mathbf{X}_j^n||_2^2 \right] + \mathbb{E}\left[||\gamma_j \cdot \mathbf{X}_{j-1}^n||_2^2 \right] \right) \\ &\overset{(c)}{=} |\alpha_j|^2 + |\beta_j|^2 + |\gamma_j|^2 = (1 + |h_{sr}|^2/|h_{dr}|^2) \cdot a_j + b_j \end{aligned}$$

where $a_j = |\alpha_j|^2$, $b_j = |\beta_j|^2$ and (c) follows since the codewords are independent of each other. Further, we also have

$$\begin{aligned} I(W_j; \mathbf{Y}_{r,2j+1}^n) &= \log_2 \left(1 + \frac{|h_{sr}|^2 \cdot b_j}{\sigma^2} \right) \\ I(W_j; \mathbf{Y}_{e,2j+1}^n) &= \log_2 \left(1 + \frac{|h_{se}|^2 \cdot b_j}{(\sigma^2 + \eta \cdot a_j)} \right) \\ I(W_{j-1}; \mathbf{Y}_{e,2j+1}^n) &= \log_2 \left(1 + \frac{\eta \cdot a_j}{(\sigma^2 + |h_{se}|^2 \cdot b_j)} \right) \end{aligned}$$

where $\eta = |h_{se}h_{dr} - h_{sr}h_{de}|^2/|h_{dr}|^2$

D. Phase B (Beamforming)

After the $(2j+1)^{\text{th}}$ transmission slot, the relay node successfully decodes the received signal $\mathbf{Y}_{r,2j+1}^n$ to obtain message W_j. Then in the $(2j+2)^{\text{th}}$ transmission slot, the source and the relay transmit $u_{1,j} \cdot (\mathbf{X}_j^n + \mathbf{X}_{j-1}^n)$ and $u_{2,j} \cdot (\mathbf{X}_j^n + \mathbf{X}_{j-1}^n)$, respectively. Here, $u_{1,j}, u_{2,j} \in \mathbb{C}$. The signal received at the destination and the eavesdropper is

$$\mathbf{Y}_{i,2j+2}^n = \mathbf{h}_i^T \mathbf{u}_j \cdot (\mathbf{X}_j^n + \mathbf{X}_{j-1}^n) + \mathbf{Z}_i^n \quad i \in \{d, e\}$$

where $\mathbf{h}_i = [h_{si}, h_{ri}]^T$ and $\mathbf{u}_j = [u_{1,j}, u_{2,j}]^T$. Since the destination has successfully decoded message W_{j-1} at the end of the $(2j)^{\text{th}}$ transmission slot, it can subtract an appropriate scaled version of codeword $\mathbf{X}_{j-1}^n$ from $\mathbf{Y}_{d,2j+2}^n$, to obtain the following signal

$$\mathbf{Y}_{d,2j+2}^n = \mathbf{h}_i^T \mathbf{u}_j \cdot \mathbf{X}_j^n + \mathbf{Z}_d^n$$

Let p_2^j units be the average power constraint for the transmissions in an even transmission slot. Then, we have the following inequalities

$$p_2^j = \frac{1}{n}(\mathbb{E}\left[||u_{1,j}(\mathbf{X}_j^n + \mathbf{X}_{j-1}^n)||_2^2\right] + \mathbb{E}\left[||u_{2,j}(\mathbf{X}_j^n + \mathbf{X}_{j-1}^n)||_2^2\right]) \overset{(d)}{=} 2\mathbf{u}_j^\dagger \mathbf{u}_j$$

where (d) follows since the codewords are independent of each other. Further, we also have the following equalities

$$I(W_j; \mathbf{Y}_{d,2j+2}^n) = \log_2\left(1 + \frac{\mathbf{u}_j^\dagger \mathbf{H}_d \mathbf{u}_j}{\sigma^2}\right)$$

$$I(W_j; \mathbf{Y}_{e,2j+2}^n) = \log_2\left(1 + \frac{\mathbf{u}_j^\dagger \mathbf{H}_e \mathbf{u}_j}{\sigma^2 + \mathbf{u}_j^\dagger \mathbf{H}_e \mathbf{u}_j}\right)$$

$$I(W_{j-1}; \mathbf{Y}_{e,2j+2}^n) = \log_2\left(1 + \frac{\mathbf{u}_j^\dagger \mathbf{H}_e \mathbf{u}_j}{\sigma^2 + \mathbf{u}_j^\dagger \mathbf{H}_e \mathbf{u}_j}\right)$$

where $\mathbf{H}_i = \mathbf{h}_i \mathbf{h}_i^\dagger$, $\forall i \in \{d, e\}$.

Proposition 1. *For all $j \geq 1$, we have*

$$I(W_j; \mathbf{Y}_{e,2j+2}^n) = I(W_{j-1}; \mathbf{Y}_{e,2j+2}^n) \leq \log_2\left(1 + f(\mathbf{h}_e, p_2^j)\right) \quad (4)$$

where $f(\mathbf{h}_e, p_2^j) = \left(1 + \frac{2\sigma^2}{p_2^j \cdot (\mathbf{h}_e^\dagger \mathbf{h}_e)}\right)^{-1}$

Proof: Refer to the appendix for the proof. ∎

When p_2^j is large, it can be shown that the bound given by inequality (4) is tight. Therefore, for ease of analysis, we replace the inequality in (4) with equality.

E. Problem Formulation

Since wireless networks are often subject to power constraints, we seek to maximize the average secrecy rate of the messages subject to an average power budget of p_{max} units per time unit per message. In our scheme, message transfers from the source to the destination happens in two transmission slots. Therefore, the effective capacity of the end-to-end main channel is given as the minimum of the capacity of the individual channels. After m message have been transferred from the source to the destination, it can be shown that the secrecy rate achievable with respect to message $W_i, 0 \leq i \leq m-1$ is given as

$$\text{main channel capacity} - \text{eavesdropper channel capacity} = \frac{1}{2}\Big[\min\Big\{I(W_j; \mathbf{Y}_{d,1}^n, \cdots, \mathbf{Y}_{d,2m}^n), I(W_j; \mathbf{Y}_{r,1}^n, \cdots, \mathbf{Y}_{r,2m}^n)\Big\} - I(W_j; \mathbf{Y}_{e,1}^n, \cdots, \mathbf{Y}_{e,2m+2}^n)\Big]^+ \quad (5)$$

The factor $1/2$ appears in the above expression due to the fact that two transmission slots are required to transfer every message from the source to the legitimate destination. Now, our problem of maximizing the achievable average secrecy can be formally stated as

$$\max \liminf_{m\to\infty} \frac{1}{m}\left(R_0 + \sum_{j=1}^{m-1} \frac{1}{2}\Big[\min\Big\{I(W_j; \mathbf{Y}_{d,1}^n, \cdots, \mathbf{Y}_{d,2m}^n), I(W_j; \mathbf{Y}_{r,1}^n, \cdots, \mathbf{Y}_{r,2m}^n)\Big\} - I(W_j; \mathbf{Y}_{e,1}^n, \cdots, \mathbf{Y}_{e,2m+2}^n)\Big]^+\right) \quad (6)$$

Subject to:

$$I(W_0; \mathbf{Y}_{e,3}^n) \leq I(W_0; \mathbf{Y}_{e,1}^n, \mathbf{Y}_{e,2}^n) \quad (7)$$

$$I(W_0; \mathbf{Y}_{e,4}^n) \leq I(W_0; \mathbf{Y}_{e,1}^n, \mathbf{Y}_{e,2}^n) \quad (8)$$

$$(1 + |h_{sr}|^2/|h_{dr}|^2) \cdot a_j + b_j + 2\mathbf{u}_j^\dagger \mathbf{u}_j \leq 2p_{max} \quad (9)$$

$$a_j \geq 0, b_j \geq 0, \mathbf{u}_j \in \mathbb{C}^2 \quad \forall j \geq 1$$

Since the scheme for initial message message W_0 is fixed and different from other messages, constraints (7) and (8) are needed to ensure that message W_0 has a secrecy rate of R_0 units. The factor $1/2$ appears in the above optimization problem due to the fact that *two transmission slots* are needed to securely transfer the messages from the source to the destination.

Since the relay node successfully decodes message W_j in the $(2j+1)^{\text{th}}$ transmission slot, we have

$$I(W_j; \mathbf{Y}_{r,1}^n, \cdots, \mathbf{Y}_{r,2m}^n) = I(W_j; \mathbf{Y}_{r,2j+1}^n) = \log_2\left(1 + \frac{|h_{sr}|^2 \cdot b_j}{\sigma^2}\right) \quad (10)$$

Due to the independence of the messages and the fact that the destination receives the codeword corresponding to message $W_j, 1 \leq j \leq m-1$ only in the $(2j+2)^{\text{nd}}$ transmission slot, we have

$$I(W_j; \mathbf{Y}_{d,1}^n, \cdots, \mathbf{Y}_{d,2m}^n) = I(W_j; \mathbf{Y}_{d,2j+2}^n) = \log_2\left(1 + \frac{\mathbf{u}_j^\dagger \mathbf{H}_d \mathbf{u}_j}{\sigma^2}\right) \quad (11)$$

After plugging in equations (1), (11) and (10) in (6), we obtain the following, simplified, optimization problem

$$\max \liminf_{m\to\infty} \frac{1}{m}\left(R_0 + \sum_{j=1}^{m-1} \frac{1}{2}\left[\log_2\left(1 + g(\mathbf{u}_j, b_j)\right) - I_j\right]^+\right) \quad (12)$$

Subject to:

$$\begin{gathered} I(W_0; \mathbf{Y}_{e,3}^n) \leq I(W_0; \mathbf{Y}_{e,1}^n, \mathbf{Y}_{e,2}^n) \\ I(W_0; \mathbf{Y}_{e,4}^n) \leq I(W_0; \mathbf{Y}_{e,1}^n, \mathbf{Y}_{e,2}^n) \\ p_1^j + p_2^j \leq 2p_{max} \\ (1 + |h_{sr}|^2/|h_{dr}|^2) \cdot a_j + b_j = p_1^j \quad , \quad 2\mathbf{u}_j^\dagger \mathbf{u}_j = p_2^j \\ a_j \geq 0, b_j \geq 0, \mathbf{u}_j \in \mathbb{C}^2 \quad \forall j \geq 1 \end{gathered} \quad (13)$$

where $g(\mathbf{u}_j, b_j) = \min\{\mathbf{u}_j^\dagger \mathbf{H}_d \mathbf{u}_j, |h_{sr}|^2 b_j\}/\sigma^2$ denotes the effective SNR of the virtual source-destination channel. The maximum leakage of message $W_j, j \geq 1$ after using its codeword in four transmission slots is given as

$$I_j = \max \left\{ \log_2 \left(1 + \frac{|h_{se}|^2 \cdot b_j}{(\sigma^2 + \eta \cdot a_j)}\right), \log_2 \left(1 + f(\mathbf{h}_e, p_2^j)\right) \right.$$
$$\left. \log_2 \left(1 + \frac{\eta \cdot a_{j+1}}{(\sigma^2 + |h_{se}|^2 \cdot b_{j+1})}\right), \log_2(1 + f(\mathbf{h}_e, p_2^{j+1})) \right\} \quad (14)$$

Proposition 2. *There exists an optimal solution* $\{(\overline{a}_j, \overline{b}_j, \overline{\mathbf{u}}_j), j \geq 1\}$ *of* (12)*, such that* $\overline{b}_j = \frac{\overline{\mathbf{u}}_j^\dagger \mathbf{H}_d \overline{\mathbf{u}}_j}{|h_{sr}|^2}$ $\forall j \geq 1$

Proof: Refer to the appendix for the proof. ∎

V. An Achievable Average Rate

While the optimization problem (12) can be solved optimally for small values of m, for larger values, the optimization problem becomes intractable. Therefore, in this section, we propose an online sequential problem that computes an achievable average rate of problem (12).

To help us obtain an achievable average rate, for each $j \geq 1$, we replace I_j with $\hat{I}_j$ in the objective function (12) and add the following constraint to the optimization problem (12).

$$\log_2 \left(1 + \frac{\eta \cdot a_j}{(\sigma^2 + |h_{se}|^2 \cdot b_j)}\right) \leq \hat{I}_{j-1} \quad \forall j \geq 1 \quad (15)$$
$$\log_2(1 + f(\mathbf{h}_e, p_2^j)) \leq \hat{I}_{j-1} \quad \forall j \geq 1 \quad (16)$$

where

$$\hat{I}_j = \begin{cases} \max \left\{ \log_2 \left(1 + \frac{|h_{se}|^2 b_j}{(\sigma^2 + \eta \cdot a_j)}\right), \log_2 \left(1 + f(\mathbf{h}_e, p_2^j)\right) \right\} & j \geq 1 \\ \log_2 \left(1 + \frac{\max\{|h_{se}|^2 p^*, |h_{re}|^2 q^*\}}{\sigma^2}\right) & j = 0 \end{cases}$$

Corollary 1. *For all* $j \geq 1$*, we have*

$$\left[\log_2 \left(1 + \frac{\min\{\mathbf{u}_j^\dagger \mathbf{H}_d \mathbf{u}_j, |h_{sr}|^2 b_j\}}{\sigma^2}\right) - \hat{I}_j \right]^+ = \min\{R_1^j(a_j, b_j), R_2^j(\mathbf{u}_j, p_2^j)\}$$

where

$$R_1^j(a_j, b_j) = \left[\log_2 \left(\frac{(\sigma^2 + |h_{sr}|^2 b_j) \cdot (\sigma^2 + \eta a_j)}{\sigma^2(\sigma^2 + \eta a_j + |h_{se}|^2 b_j)} \right) \right]^+$$
$$R_2^j(\mathbf{u}_j, p_2^j) = \left[\log_2 \left(\frac{\sigma^2 + \mathbf{u}_j^\dagger \mathbf{H}_d \mathbf{u}_j}{\sigma^2(1 + f(\mathbf{h_e}, p_2^j))} \right) \right]^+$$

Proof: By rearranging the mutual information terms in the objective function (12), and by applying Proposition 2, the result follows. ∎

We would like to remark that $R_1^j(a_j, b_j)$ and $R_2^j(\mathbf{u}_j, p_2^j)$ represent the secrecy rate of source-relay and relay-destination channel, respectively. Now, we can obtain an achievable average secrecy rate, by solving the following optimization problem

$$\max \liminf_{t \to \infty} \frac{1}{m} \left(R_0 + \sum_{j=1}^{m-1} \frac{1}{2} \min \left\{ R_1^j(a_j, b_j), R_2^j(\mathbf{u}_j, p_2^j) \right\} \right) \quad (17)$$

Subject to:

$$\log_2 \left(1 + \frac{\eta \cdot a_j}{(\sigma^2 + |h_{se}|^2 \cdot b_j)}\right) \leq \hat{I}_{j-1} \quad j \geq 1$$
$$\log_2(1 + f(\mathbf{h}_e, p_{j,2})) \leq \hat{I}_{j-1} \quad j \geq 1$$
$$p_1^j + p_2^j \leq 2p_{max}$$
$$(1 + |h_{sr}|^2/|h_{dr}|^2) \cdot a_j + b_j = p_1^j \quad , \quad 2\mathbf{u}_j^\dagger \mathbf{u}_j = p_2^j$$
$$a_j \geq 0, b_j \geq 0, \mathbf{u}_j \in \mathbb{C}^2 \quad \forall j \geq 1$$

We note that to solve problem (17), we need to jointly optimize the variable over the sequence $\{(a_j, b_j, \mathbf{u}_j), j \geq 1\}$. However, such an optimization problem may not be tractable for larger values of m. Therefore, we present a causal version of the above problem; where the achievable rate in the j^{th} transmission slot is maximized by considering only the previous $(j-1)$ transmission slot

$$R_{avg} = \liminf_{m \to \infty} \frac{1}{m} \left(R_0 + \sum_{j=1}^{m-1} R_j \right) \quad (18)$$

where for all $j \geq 1$, we have

$$R_j = \max_{a_j, b_j, \mathbf{u}_j, p_2^j} \frac{1}{2} \min \left\{ R_1^j(a_j, b_j), R_2^j(\mathbf{u}_j, p_2^j) \right\}$$

Subject to:

$$\log_2 \left(1 + \frac{\eta \cdot a_j}{(\sigma^2 + |h_{se}|^2 \cdot b_j)}\right) \leq \hat{I}_{j-1}$$
$$\log_2(1 + f(\mathbf{h}_e, p_{j,2})) \leq \hat{I}_{j-1}$$
$$p_1^j + p_2^j \leq 2p_{max}$$
$$(1 + |h_{sr}|^2/|h_{dr}|^2) \cdot a_j + b_j = p_1^j \quad , \quad 2\mathbf{u}_j^\dagger \mathbf{u}_j = p_2^j$$
$$a_j \geq 0, b_j \geq 0, \mathbf{u}_j \in \mathbb{C}^2$$

Proposition 3. *The average rate* R_{avg} *is achievable.*

Proof: Let $\{(\overline{a}_j, \overline{b}_j, \overline{\mathbf{u}}_j), j \geq 1\}$ be the optimizer of problem (18). Since the constraints in problem (18) and (17) are identical, the sequence $\{(\overline{a}_j, \overline{b}_j, \overline{\mathbf{u}}_j), j \geq 1\}$ is a feasible point of problem (18). Also, for every $j \geq 1$, we have $\min \left\{ R_1^j(\overline{p}_{j,1}), R_2^j(\overline{p}_{j,2}) \right\} = R_j$ ∎

Since we have established that the average secrecy rate obtained by the causal formulation is achievable, we focus our attention on solving the j^{th} step optimization problem i.e., obtaining R_j. We note that

$$R_j = \max_{a_j, b_j, \mathbf{u}_j, p_2^j} \frac{1}{2} \min \left\{ R_1^j(a_j, b_j), R_2^j(\mathbf{u}_j, p_2^j) \right\}$$
$$= \frac{1}{2} \min \left\{ \max_{a_j, b_j} R_1^j(a_j, b_j), \max_{\mathbf{u}_j, p_2^j} R_2^j(\mathbf{u}_j, p_2^j) \right\}$$

Now, we decompose the problem of computing R_j into the following two subproblems.

A. Phase A Subproblem

The first subproblem is as follows

$$\max_{a_j, b_j} R_1^j(a_j, b_j) \quad (19)$$

Subject to:

$$\log_2 \left(1 + \frac{\eta \cdot a_j}{(\sigma^2 + |h_{se}|^2 \cdot b_j)}\right) \leq \hat{I}_{j-1} \quad (20)$$

$$(1+|h_{sr}|^2/|h_{dr}|^2)\cdot a_j + b_j = p_1^j \qquad (21)$$
$$a_j \geq 0, b_j \geq 0$$

Now, substituting (21) in (19) and (20), we can rewrite the *Phase A subproblem* as the following one dimensional optimization problem

$$\phi^j(p_1^j) = \max_{a_j} \left[\log_2\left(\frac{(\sigma^2+|h_{sr}|^2(p_1^j-a_j))\cdot(\sigma^2+\eta a_j)}{\sigma^2(\sigma^2+\eta a_j+|h_{se}|^2(p_1^j-a_j))}\right)\right]^+$$
$$\text{Subject to: } 0 \leq a_j \leq \min\left\{p_1^j, \frac{(\sigma^2+|h_{se}|^2\cdot p_1^j)}{(|h_{se}|^2+\eta\cdot(2^{\hat{I}_{j-1}}-1)^{-1})}\right\}$$

Proposition 4. *For all $j \geq 1$, $\phi^j(p_1^j)$ is an increasing concave function of p_1^j.*

Proof: Refer to the appendix for the proof. ■

B. Phase B Subproblem

The other subproblem is given as

$$\max_{\mathbf{u}_j} R_2^j(\mathbf{u_j}, p_2^j)$$
Subject to:
$$2\mathbf{u}_j^\dagger \mathbf{u}_j = p_2^j \quad \text{and} \quad \mathbf{u}_j \in \mathbb{C}^2$$

After plugging in the values of $R_2^j(\mathbf{u_j}, p_2^j)$, we can rewrite the *Phase B* optimization problem as

$$\psi^j(p_2^j) = \max_{\mathbf{u}_j}\left[\log_2\left(\frac{\sigma^2+\mathbf{u}_j^\dagger \mathbf{H}_d \mathbf{u}_j}{\sigma^2(1+f(\mathbf{h_e}, p_2^j))}\right)\right]^+$$
Subject to:
$$2\mathbf{u}_j^\dagger \mathbf{u}_j = p_2^j \quad \text{and} \quad \mathbf{u}_j \in \mathbb{C}^2$$

With a bit of effort, it can be shown that the optimum of the above problem is given as

$$\psi^j(p_2^j) = \left[\log_2\left(\frac{(2\sigma^2+(\mathbf{h}_d^\dagger\mathbf{h}_d)\cdot p_2^j)(2\sigma^2+\mathbf{h}_e^\dagger\mathbf{h}_e\cdot p_2^j)}{4\sigma^2\cdot(\sigma^2+(\mathbf{h}_e^\dagger\mathbf{h}_e)\cdot p_2^j)}\right)\right]^+$$
$$\geq \left[\log_2\left(1+\frac{(\mathbf{h}_d^\dagger\mathbf{h}_d)\cdot p_2^j}{2\sigma^2}\right)\right]^+ \quad \forall p_2^j \geq 0 \qquad (22)$$

For ease of analysis, we replace inequality in (22) with equality. We note that by replacing inequality (22) with equality, we obtain a lower bound on the achievable average rate. We also note that this lower bound is an increasing strictly concave function in p_2^j.

C. Optimal Solution

Now, we can rewrite the causal optimization problem in the j^{th} transmission slot as

$$P_1: \max_{p_1^j, p_2^j} \frac{1}{2}\min\{\phi^j(p_1^j), \psi^j(p_2^j)\}$$
Subject to:
$$p_1^j + p_2^j \leq 2p_{max} \qquad (23)$$
$$\log_2(1+f(\mathbf{h}_e, p_{j,2})) \leq \hat{I}_{j-1}$$

At optimality, in problem P_1, it can be shown that inequality (23) is active. Therefore, we can rewrite problem P_1 as follows

$$P_2: \max_{0\leq p_j} \frac{1}{2}\min\{\phi^j(2p_{max}-p_j), \psi^j(p_j)\}$$
$$\text{Subject to: } p_j \leq \begin{cases} 2p_{max} & \text{if } \hat{I}_{j-1} \in (0,1) \\ \frac{2\sigma^2}{((2^{\hat{I}_{j-1}}-1)^{-1}-1)\cdot \mathbf{h}_e^\dagger \mathbf{h}_e} & \text{otherwise} \end{cases}$$

Proposition 5. *Problem P_2 has a unique global maximizer.*

Proof: $\min\{\phi^j(2p_{max}-x), \psi^j(x)\}$ is strictly concave in x, since it is the minimum of a concave and a strictly concave functions. Since problem D_2 maximizes a concave function over an interval (a convex set), the proposition follows. ■

Since P_2 is a concave function defined over an interval, we perform golden section [26] line search over the interval $[0, 2p_{max}]$, to obtain the optimizer for problem P_2.

Let p_j^* be the optimizer of problem P_2, and a_j^* be the optimizer of $\phi^j(2p_{max}-p_j^*)$. Then, we have

$$\hat{I}_j = \max\left\{\log_2\left(1+\frac{|h_{se}|^2(2p_{max}-p_j^*-a_j^*)}{(\sigma^2+\eta\cdot a_j^*)}\right), \log_2\left(1+f(\mathbf{h}_e, p_j^*)\right)\right\}$$

We would like to remark the fact that our initial formulation (6) has been transformed (by substituting equalities for inequalities, $\hat{I}_j$ instead of I_j, etc) into problem P_2. We would also like to highlight that these transformations have enabled us to obtain a computationally tractable optimization problem, the solution of which gives us an achievable average rate (see Proposition 3).

VI. Numerical Evaluation

In this section, we investigate the performance of the proposed cooperative two phase scheme through numerical evaluations. We evaluate the achievable secrecy rate for four schemes namely; *Direct*: where the source transmits directly to the destination, *Two-hop*: where the source transmits to the destination via the relay node, *Beamforming*: the conventional two-phase beamforming method proposed in [11][Section IV.A] and *Our scheme (the relaxed formulation)*: is the two phase method presented in Section IV of this paper.

We consider a simple two-dimensional node placement. The positions of the source and the legitimate destination are fixed at $(-35m, 0)$ and $(35m, 0)$, respectively. To highlight the effect of distances on channel gains, as in [11], we assume the channel gain between nodes i and j to be $h_{ij} \sim \mathcal{CN}(0, d_{ij}^{-c/2})$, where d_{ij} is the Euclidean distance between nodes i and j and $c = 4$ is the path loss exponent. The noise power σ^2 is chosen to be $-60\,dBm$. We performed Monte Carlo experiments consisting of 10^4 independent trials to obtain the average results. Error bars in the plots have been suppressed, to enhance legibility.

First, we consider a scenario with an eavesdropper located at $(0m, -50m)$. We fixed the power budget p_{max} at $27\,dBm$

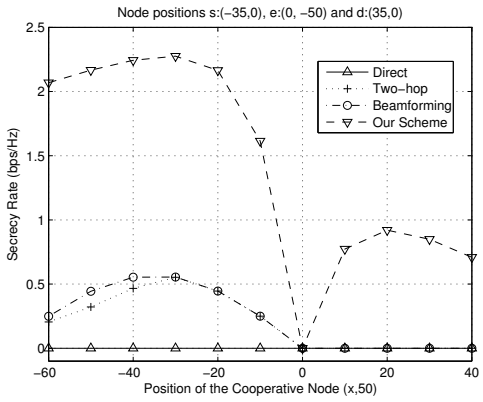

Fig. 3. Achievable secrecy rate of the four schemes as a function of the relay position; p_{max} is set as $27\,dBm$, source node is at $(-35m, 0)$, destination is at $(35m, 0)$, and the eavesdropper is at $(0m, -50m)$.

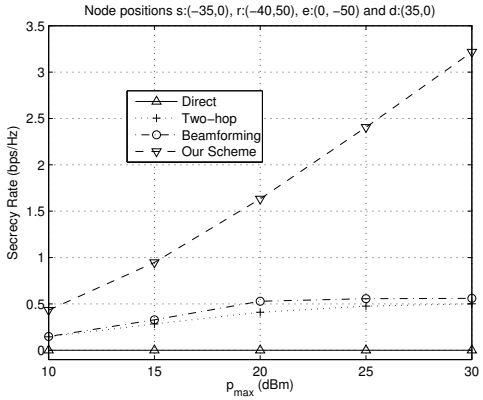

Fig. 4. Achievable secrecy rate of four schemes as a function of power budget p_{max}; relay node is fixed at $(-40m, 50m)$, source node is at $(-35m, 0)$, destination is at $(35m, 0)$, and the eavesdropper is at $(0m, -50m)$.

and move the relay node along the straight line with endpoints $(-60m, 50m)$ and $(40m, 50m)$. The results for this scenario are shown in Fig. 3. As expected, the *Direct* scheme is unable to achieve non-zero secrecy rate. This is due to the fact that the main channel is more degraded than the eavesdropper's channel. While the *Two-Hop* and *Beamforming* schemes are able to achieve good secrecy rates, they fail to achieve non-zero secrecy rate for cases when the relay node is beyond the point $(0m, 50m)$. This is due to the fact that in such cases, the highly degraded source-relay channel is unable to provide non-zero secrecy rate between the source and the relay. However, the scheme proposed in this paper is able to provide higher secrecy for every relay position, thus demonstrating its superior performance.

Next, we fix the relay node at $(-40m, 50m)$ and evaluate the achievable secrecy rate of four schemes for different power budgets (p_{max}). The results of the evaluation are presented in Fig. 4. From Fig. 4, we can see that the scheme proposed in this paper performs better than the other three conventional schemes.

VII. Conclusion

In this paper, we have presented a scheme to improve the equivocation in wireless relay networks with resource constrained eavesdropper. Assuming global channel state information and the decode-and-forward relaying strategy, we posed the problem of maximizing the average achievable secrecy rate, subject to an overall power budget per message. Further, by exploiting the structure of the optimization problem, we also propose an approach to obtain an achievable average rate. Finally, through numerical evaluation, we demonstrated that our scheme out performs other conventional schemes in the setting of weak eavesdropper.

In the future, we would like to study the performance of networks with incomplete CSI and with multiple relay nodes.

Appendix A
Proof of Proposition 1

Since p_2^j is the second phase power budget, we have $\forall \mathbf{u}_j \in \mathbb{C}^2$

$$\frac{\mathbf{u}_j^\dagger \mathbf{H}_e \mathbf{u}_j}{\sigma^2 + \mathbf{u}_j^\dagger \mathbf{H}_e \mathbf{u}_j} \leq \max_{\mathbf{v}_j^\dagger \mathbf{v}_j^\dagger = \frac{p_2^j}{2}} \frac{\mathbf{v}_j^\dagger \mathbf{H}_e \mathbf{v}_j}{\sigma^2 + \mathbf{v}_j^\dagger \mathbf{H}_e \mathbf{v}_j} = \lambda_{max}$$

where λ_{max} is the largest scalar λ that satisfies the following equation

$$\mathbf{H}_e \mathbf{x} = \lambda \left(\mathbf{H}_e + \frac{2\sigma^2}{p_2^j} \cdot \mathbf{I} \right) \mathbf{x}$$

After rearranging the above equation, we obtain the following

$$\mathbf{H}_e \mathbf{x} = \beta \cdot \mathbf{x} \text{ where } \beta = \frac{2\lambda\sigma^2}{(1-\lambda)p_2^j}$$

Note that β is the Eigen value of matrix $\mathbf{H}_e$. Since $\mathbf{H}_e$ is a rank one matrix, the only possible value for β are 0 and $\mathbf{h}_e^\dagger \mathbf{h}_e$. This in turn implies that $\lambda \in \left\{ 0, \left(1 + \frac{2\sigma^2}{p_2^j \cdot (\mathbf{h}_e^\dagger \mathbf{h}_e)}\right)^{-1} \right\}$ ■

Proof of Proposition 2

We will prove this lemma by construction. Let $\{(\overline{a}_j, \overline{b}_j, \overline{\mathbf{u}}_j), j \geq 1\}$ be an optimal solution of (12), such that for some index $j_0 \geq 1$, we have $\overline{\mathbf{u}}_{j_0}^\dagger \mathbf{H}_d \overline{\mathbf{u}}_{j_0} \neq |h_{sr}|^2 \overline{b}_{j_0}$. We only provide the proof for the case when $\overline{\mathbf{u}}_{j_0}^\dagger \mathbf{H}_d \overline{\mathbf{u}}_{j_0} < |h_{sr}|^2 \overline{b}_{j_0}$. The other case can be proved in a similar manner.

Let us define $\hat{b}_{j_0} = \frac{\overline{\mathbf{u}}_{j_0}^\dagger \mathbf{H}_d \overline{\mathbf{u}}_{j_0}}{|h_{sr}|^2}$ and $\hat{a}_{j_0} = 2p_{max} - \hat{b}_{j_0} - 2\mathbf{u}_j^\dagger \mathbf{u}_j$. It is easy to see that $\hat{b}_{j_0} < \overline{b}_{j_0}$ and $\hat{a}_{j_0} > \overline{a}_{j_0}$. Therefore, we have

$$\begin{aligned} \min\{\overline{\mathbf{u}}_{j_0}^\dagger \mathbf{H}_d \overline{\mathbf{u}}_{j_0}, |h_{sr}|^2 \overline{b}_{j_0}\} &= \overline{\mathbf{u}}_{j_0}^\dagger \mathbf{H}_d \overline{\mathbf{u}}_{j_0} \\ &= \min\{\overline{\mathbf{u}}_{j_0}^\dagger \mathbf{H}_d \overline{\mathbf{u}}_{j_0}, |h_{sr}|^2 \hat{b}_{j_0}\} \end{aligned}$$

Further, from equation (14), we can see that I_j evaluated at $b_j = \hat{b}_{j_0}$ and $a_j = \hat{a}_{j_0}$ is less than or equal to I_j evaluated at $b_j = \overline{b}_{j_0}$ and $a_j = \overline{a}_{j_0}$. Therefore, the sequence $(\hat{a}_{j_0}, \hat{b}_{j_0}, \hat{\mathbf{u}}_{j_0}) \cup \{(\overline{a}_j, \overline{b}_j, \overline{\mathbf{u}}_j), j \geq 1, j \neq j_0\}$ is able to achieve

a higher secrecy rate, than the optimum of (12). This in turn implies that the sequence $(\hat{a}_{j_0}, \hat{b}_{j_0}, \hat{\mathbf{u}}_{j_0}) \cup \{(\overline{a}_j, \overline{b}_j, \overline{\mathbf{u}}_j), j \geq 1, j \neq j_0\}$ is also an optimizer of (12). ∎

Proof of Proposition 4

Let

$$f(p_1^j, a_j) = \log_2 \left(\frac{(\sigma^2 + |h_{sr}|^2(p_1^j - a_j)) \cdot (\sigma^2 + \eta a_j)}{\sigma^2(\sigma^2 + \eta a_j + |h_{se}|^2(p_1^j - a_j))} \right)$$

Let us define the set

$$\mathcal{S} = \left\{ b : 0 \leq b \leq \min \left\{ p_1^j, \frac{(\sigma^2 + |h_{se}|^2 \cdot p_1^j)}{(|h_{se}|^2 + \eta \cdot (2^{\hat{I}_{j-1}} - 1)^{-1})} \right\}, f(p_1, b) > 0 \right\}$$

Since we have non-zero secrecy between the source the cooperative node, we have $f(p_1^j, 0) = \log_2 \left(\frac{\sigma^2 + |h_{sr}|^2 p_1^j}{\sigma^2 + |h_{se}|^2 p_1^j} \right) > 0$. Now, by taking the first and second partial derivative of $f(p_1^j, a_j)$ with respect to a_j, we can see that

$$\frac{\partial f(p_1^j, a_j)}{\partial a_j} \geq 0 \quad \text{and} \quad \frac{\partial^2 f(p_1^j, a_j)}{\partial (a_j)^2} \leq 0 \quad \forall a_j \in \mathcal{S}$$

Let $a_j(p_1^j)$ be an optimizer of $\phi^j(p_1^j)$. It is clear that $a_j(p_1^j) \in \mathcal{S}$. Then, by the application of Taylor series and differential calculus, we can obtain the following

$$\frac{d(\phi^j(p_1^j))}{d(p_1^j)} = \frac{\partial f(p_1^j, a_j)}{\partial a_j}\Big|_{a_j = a_j(p_1^j)} \geq 0$$

$$\frac{d^2(\phi^j(p_1^j))}{d(p_1^j)^2} = \frac{\partial^2 f(p_1^j, a_j)}{\partial (a_j)^2}\Big|_{a_j = a_j(p_1^j)} \leq 0$$

∎

References

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

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

[3] T. Cover and A. Gamal, "Capacity Theorems for the Relay Channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, Sep 1979.

[4] J. Laneman, D. Tse, and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, Dec 2004.

[5] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," in *IEEE International Conference on Communications (ICC)*, Jun 2011, pp. 1–5.

[6] H. Deng, H.-M. Wang, W. Wang, and Q. Yin, "Secrecy Transmission with a Helper: To Relay or not to Relay," in *IEEE International Conference on Communications Workshops (ICC)*, June 2014, pp. 825–830.

[7] H.-M. Wang, Q. Yin, and X.-G. Xia, "Improving the Physical-Layer Security of Wireless Two-way Relaying via Analog Network Coding," in *IEEE Global Telecommunications Conference (GLOBECOM)*. IEEE, 2011, pp. 1–6.

[8] B. Dey, S. Jaggi, M. Langberg, and A. Sarwate, "Upper Bounds on the Capacity of Binary Channels With Causal Adversaries," *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3753–3763, June 2013.

[9] A. Mazumdar, "On the Capacity of Memoryless Adversary," in *IEEE International Symposium on Information Theory (ISIT)*, June 2014, pp. 2869–2873.

[10] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, March 2011.

[11] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[12] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, October 2013.

[13] K.-H. Park, T. Wang, and M.-S. Alouini, "On the Jamming Power Allocation for Secure Amplify-and-Forward Relaying via Cooperative Jamming," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1741–1750, September 2013.

[14] X. He and A. Yener, "Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Dec 2008, pp. 1–5.

[15] Y. Liu, J. Li, and A. Petropulu, "Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682–694, April 2013.

[16] B. Yang, W. Wang, B. Yao, and Q. Yin, "Destination Assisted Secret Wireless Communication With Cooperative Helpers," *IEEE Signal Processing Letters*, vol. 20, no. 11, pp. 1030–1033, Nov 2013.

[17] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay Selection for Secure Cooperative Networks with Jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, Oct 2009.

[18] S. Huang, J. Wei, Y. Cao, and C. Liu, "Joint Decode-and-Forward and Cooperative Jamming for Secure Wireless Communications," in *7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, Sept 2011, pp. 1–4.

[19] L. Wang, C. Cao, M. Song, and Y. Cheng, "Joint Cooperative Relaying and Jamming for Maximum Secrecy Capacity in Wireless Networks," in *IEEE International Conference on Communications (ICC)*, June 2014, pp. 4448–4453.

[20] C. Wang and H.-M. Wang, "Joint Relay Selection and Artificial Jamming Power Allocation for Secure DF Relay Networks," in *IEEE International Conference on Communications Workshops (ICC), 2014*, June 2014, pp. 819–824.

[21] S. Bashar and Z. Ding, "Optimum Power Allocation against Information Leakage in Wireless Network," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Nov 2009, pp. 1–6.

[22] J. Zhang and M. C. Gursoy, "Collaborative Relay Beamforming for Secrecy," in *International Conference on Communications (ICC)*. IEEE, 2010, pp. 1–5.

[23] X. Guan, Y. Cai, Y. Wang, and W. Yang, "Increasing Secrecy Capacity via Joint Design of Cooperative Beamforming and Jamming," in *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, Sept 2011, pp. 1274–1278.

[24] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and M. Lin, "Optimal Joint Cooperative Beamforming and Artificial Noise Design for Secrecy Rate Maximization in AF Relay Networks," in *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, June 2013, pp. 360–364.

[25] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative Secure Beamforming for AF Relay Networks With Multiple Eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, Jan 2013.

[26] E. K. Chong and S. H. Zak, *An Introduction to Optimization*. John Wiley & Sons, 2013, vol. 76.