2014 7th International Symposium on Telecommunications (IST'2014)

The Achievable Secrecy Rate of Multi-Antenna AF Relaying Using Joint Transmit and Receive Beamforming

Meysam Mirzaee and Soroush Akhlaghi
Shahed University, Tehran, Iran
Emails: me.mirzaee,akhlaghi@shahed.ac.ir

***Abstract*—Physical layer security has attracted a great deal of attentions in recent years. This is achieved through using the physical layer characteristics to help sender to transfer data reliably with perfect secrecy. Using multiple-antenna relay node can improve the secrecy capacity of such channel. In this paper, we study the cooperative wiretap channel in which secure data transmission is achieved with the help of a MIMO Amplify and Forward (AF) relay. In such network, it is assumed multiple eavesdroppers attempt to listen to the relay transmitted signal and try to decode the source message. We assume the relay makes use of separated transmit/receive beamforming vectors, dubbed rank-one beamforming matrix. The beamforming vectors are computed such that the achievable secrecy rate is maximized, assuming the relay is subject to a maximum transmit power constraint. Accordingly, it is shown that the problem of finding proper receive beamforming vector can be translated into a scalar optimization problem, where using that the transmit beamforming vector can be obtained through solving a Semi-Definite Programming (SDP) problem.**

***Index Terms*—Achievable secrecy rate, physical layer security, cooperative wiretap channel, receive and transmit beamforming.**

I. Introduction

In wireless communication networks, due to broadcast nature of medium, any unauthorized receiver can listen to source's signal. This fact motivated researchers to study in this area and propose some approaches to improve security. One of this approaches is physical layer security proposed by Wyner in his landmark paper [1]. He considered the discrete memoryless wiretap channel and proved that when the received signal of eavesdropper is a degraded version of received signal of destination, we can securely transmit data with non-zero rate.

After Wyner, Cheong and Hellman studied the Gaussian wiretap channel in [2] and computed the secrecy capacity of it. It is widely recognized that the channel condition have a great effect on the secrecy capacity. More specifically, when the source-eavesdropper channel is stronger than that of the source-destination channel, the secrecy capacity becomes zero. Using multiple antenna at relay node may overcome this issue [3].

On the other hand, equipping all nodes of network with multiple antennas may have considerable cost and size, thereby it maybe practically infeasible in many networks. However, multiple antennas can be incorporated in some nodes of network or some single-antenna nodes can cooperative to mimic a multiple-antenna node. In cooperative communications, the benefits of multi-antenna systems can be obtained by incorporating single antenna nodes, [4] and [5]. In this networks, some nodes receive the signal from a source and retransmit it to the destination, meaning these nodes act as a relay node. Amplify and Forward (AF) is one of the prominent strategies to be employed at relay nodes. In this strategy, the relay multiplies its received signal by a scaling factor and then transmits it to the destination. This strategy has low complexity and so it has some practical implications.

In recent years, physical layer security in cooperative communication networks has been studied in both of information theory (e.g. [6]) and signal processing (e.g. [7]–[9]) viewpoints. In signal processing area, the achievable secrecy rate of a network having multiple single-antenna relays is investigated in [7]–[9]. In these works, the scaling factors of relay nodes are computed such that the achievable secrecy rate is maximized. In [7], a sub-optimum solution is computed while the obtained secrecy rate is not close to optimal solution. In [8], a near to optimum solution is obtained through using a search method with considerable complexity. In [9], the optimal solution of secrecy rate maximization problem is computed using Charness-Cooper transformation and bi-section methods.

In [10], a Multi-Input Multi-Output (MIMO) AF relay is used in wiretap channel, where the beamforming matrix is computed for two different models of eavesdropper's channel. In the first model, the rician fading model is considered for eavesdropper's channel and it is assumed that only the statistical information of eavesdropper's channel is available to the other nodes. In this case, the approximated ergodic secrecy rate is optimized. In the second model, the uncertainty region is considered for eavesdropper's channel vector and it is modeled as a sphere. In this case, the worst case secrecy rate is optimized. For each case, three different scenarios are studied for beamforming matrix of relay node including: Rank-1 beamforming, Match and Forward (MF) beamforming and Zero-Forcing (ZF) beamforming.

In this paper, we study a cooperative wiretap channel in which one source node sends its private message to respective

978-1-4799-5359-2/14/$31.00

destination with the help of one multi-antenna AF relay node. Also, some eavesdroppers aim at listening to the transmitted message. We assume that the relay first applies receive beamforming to its received vector and then sends the signal using a transmit beamforming vector. The goal is to jointly compute these two beamforming vectors such that the achievable secrecy rate under relay power constraint is maximized. To this end, the task of finding receive beamforming vector is translated into a single-parameter optimization problem, which can be tackled by the use of a simple one-dimensional search. Also, to compute the transmit beamforming vector, the corresponding optimization problem reformed into a SDP problem where its solution can be found by CVX package [11]. Moreover, we provide some arguments to limit the interval of search that reduces the complexity. Numerical results indicated that the optimal receive beamforming performs very close to matched filtering in most of cases.

The reminder of this paper is organized as follows. Section II introduces the considered model and basic mathematical relations. Section III defines the optimization problem and provide the proposed solution of it. Numerical results are represented in IV. At the end, Section V concludes this paper.

II. System Model

In this paper, a wireless relay network with $M+3$ nodes is considered. In this model, the source node S sends its signal to the AF multi-antenna relay node R and then the relay transmits a scaled version of its received signal to the destination node D. Also, M eavesdropper nodes, i.e., $E_1, ..., E_M$, receive the transmitted signal of relay and attempt to decode the source message. We assume that the relay has N antennas, while other nodes are equipped with single antenna (see Fig. 1). Moreover, it is assumed that there is not a direct link between transmission ends and the destination as well as eavesdroppers get their information from the relay. Moreover, we assume a quasi-static flat fading environment where the problem is solved for each channel realizations. Finally, the relay node is aware of all channel gains where these channels are assumed to be statistically independent.

In this model, the data is transferred from source to destination in two hops. In the first hop, the encoder $f_n : \mathcal{W} \to \chi_s^n$ at source maps the message W to a codeword $x_s^n \in \chi_s^n$. This codeword is transmitted to the relay node in n transmissions and the message W is distributed over the index set $\mathcal{W} = \{1, 2, ..., 2^{nR}\}$ uniformly, where R, nR and χ_s^n respectively denote the transmission rate of source, the message entropy and the transmitted vector space.

In tth transmission, i.e., tth time slot, the source symbol $x_s(t)$ is transmitted which has zero mean and unit power, i.e., $E\left[|x_s(t)|^2\right] = 1$. In this time slot, the relay receives the vector $\mathbf{y}_r(t)$ that is given by,

$$\mathbf{y}_r(t) = \sqrt{P_s}\mathbf{h}_r x_s(t) + \mathbf{z}_r(t) \quad \text{for } t = 1, \ldots, n \ , \tag{1}$$

where $\mathbf{h}_{r_{N\times 1}}$ is the channel coefficients vector from source to the relay and $\mathbf{z}_r \sim \mathcal{CN}(\mathbf{0}, \sigma_r^2\mathbf{I}_N)$ is the received Additive White Gaussian Noise (AWGN) vector at the relay. Also, the transmit power of source for each symbol is indicated by P_s.

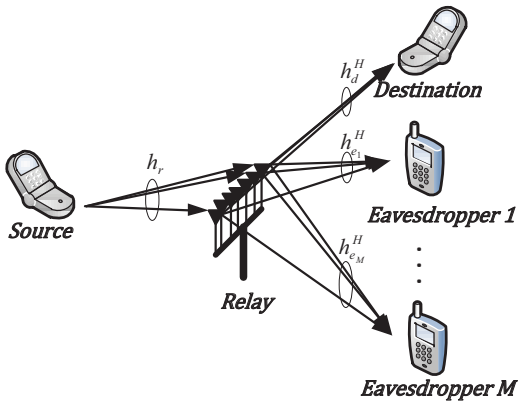

Fig. 1. System Model

In tth time slot of second hop, the relay applies receive and transmit beamforming to $\mathbf{y}_r(t)$ and makes the vector $\mathbf{x}_r$ that is given by[1],

$$\mathbf{x}_r = \mathbf{u}\mathbf{v}^H\mathbf{y}_r \ . \tag{2}$$

where $\mathbf{v}^H$ and $\mathbf{u}$ are receive and transmit beamforming vectors of relay, respectively. The vector $\mathbf{x}_r$ is transmitted to destination in this time slot and the following signals are received at destination and eavesdroppers, respectively,

$$y_d = \mathbf{h}_d^H\mathbf{x}_r + z_d = \sqrt{P_s}\mathbf{h}_d^H\mathbf{u}\mathbf{v}^H\mathbf{h}_r x_s + \mathbf{h}_d^H\mathbf{u}\mathbf{v}^H\mathbf{z}_r + z_d \tag{3}$$

$$y_{e_m} = \mathbf{h}_{e_m}^H\mathbf{x}_r + z_{e_m} = \sqrt{P_s}\mathbf{h}_{e_m}^H\mathbf{u}\mathbf{v}^H\mathbf{h}_r x_s + \mathbf{h}_{e_m}^H\mathbf{u}\mathbf{v}^H\mathbf{z}_r + z_{e_m}, \quad \forall m \in \mathcal{M} \tag{4}$$

where $\mathbf{h}_{d_{N\times 1}}$ and $\mathbf{h}_{e_{m\,N\times 1}}$ are the vectors having complex conjugate of channel gains from the relay to the destination and the mth eavesdropper, respectively, and $\mathcal{M} = \{1, 2, ..., M\}$. Also, $z_d \sim \mathcal{CN}(0, \sigma_d^2)$ and $z_{e_m} \sim \mathcal{CN}(0, \sigma_{e_m}^2)$ denote received noises at destination and eavesdroppers, respectively.

Moreover, the transmit power of relay can be computed as,

$$\begin{aligned} P_r &= E\{\|\mathbf{x}_r\|^2\} = E\{\text{tr}(\mathbf{u}\mathbf{v}^H\mathbf{y}_r\mathbf{y}_r^H\mathbf{v}\mathbf{u}^H)\} \\ &= \text{tr}\Big(\mathbf{u}\mathbf{v}^H\big(P_s\mathbf{h}_r\mathbf{h}_r^H + \sigma_r^2\mathbf{I}_N\big)\mathbf{v}\mathbf{u}^H\Big) \\ &= \text{tr}\Big(\mathbf{u}^H\mathbf{u}\mathbf{v}^H\big(P_s\mathbf{h}_r\mathbf{h}_r^H + \sigma_r^2\mathbf{I}_N\big)\mathbf{v}\Big) \\ &= \mathbf{u}^H\mathbf{u}\mathbf{v}^H(P_s\mathbf{R}_r + \sigma_r^2\mathbf{I}_N)\mathbf{v}. \end{aligned} \tag{5}$$

where $\mathbf{R}_r \triangleq \mathbf{h}_r\mathbf{h}_r^H$.

The achievable secrecy rate for Gaussian input can be computed as [7],

$$R_s = \min_{m\in\mathcal{M}} \ \frac{1}{2}\Big\{\log_2(1 + SNR_d) - \log_2(1 + SNR_{e_m})\Big\}^+, \tag{6}$$

[1]For notational convenience, we ignore the index of symbols in the rest of paper.

where,

$$SNR_d = \frac{P_s \mathbf{h}_d^H \mathbf{u}\mathbf{v}^H \mathbf{h}_r \mathbf{h}_r^H \mathbf{v}\mathbf{u}^H \mathbf{h}_d}{\sigma_r^2 \mathbf{h}_d^H \mathbf{u}\mathbf{v}^H \mathbf{v}\mathbf{u}^H \mathbf{h}_d + \sigma_d^2} = \frac{P_s \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_d^2}. \quad (7)$$

and similarly,

$$SNR_{e_m} = \frac{P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_{e_m}^2}, \quad \forall m \in \mathcal{M}. \quad (8)$$

In the next section, we would like to find the best beamforming vectors $\mathbf{u}$ and $\mathbf{v}$ such that the achievable secrecy rate is maximized.

III. Problem Statement

In this section, we explore the optimal beamforming vectors of relay node to maximize the achievable secrecy rate under the relay power constraint. Mathematically, the following optimization problem is solved,

$$\begin{aligned} \max_{\mathbf{u},\mathbf{v}} \quad & R_s \\ \text{s.t.} \quad & P_r \le P_T. \end{aligned} \quad (9)$$

where, P_T is the maximum available transmit power at the relay node.

By substituting (7) and (8) in (6), the achievable secrecy rate is given by,

$$R_s = \min_{m \in \mathcal{M}} \frac{1}{2} \left\{ \log_2 \frac{\left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_d^2}\right)}{\left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_{e_m}^2}\right)} \right\}^+. \quad (10)$$

Using (5) and (10), the problem (9) can be rewritten as,

$$\begin{aligned} \max_{\mathbf{u},\mathbf{v}} \min_{m \in \mathcal{M}} \frac{1}{2} \log_2 & \left(\left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_d^2}\right) / \right. \\ & \left. \left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_{e_m}^2}\right) \right) \\ \text{s.t.} \quad & \mathbf{u}^H \mathbf{u}\mathbf{v}^H (P_s \mathbf{R}_r + \sigma_r^2 \mathbf{I}_N) \mathbf{v} \le P_T. \end{aligned} \quad (11)$$

Due to the monotony property of logarithm function, the optimization problem can be simplified as,

$$\begin{aligned} \max_{\mathbf{u},\mathbf{v}} \min_{m \in \mathcal{M}} & \left(\left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_d^2}\right) / \right. \\ & \left. \left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_{e_m}^2}\right) \right) \\ \text{s.t.} \quad & \mathbf{u}^H \mathbf{u}\mathbf{v}^H (P_s \mathbf{R}_r + \sigma_r^2 \mathbf{I}_N) \mathbf{v} \le P_T. \end{aligned} \quad (12)$$

Generally, problem (12) is not a convex problem and is difficult to solve. To overcome this difficulty, we can add a slack variable τ and substitute (12) by following optimization problem,

$$\begin{aligned} \max_{\mathbf{u},\mathbf{v},\tau} \quad & \tau \left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_d^2}\right) \\ \text{s.t.} \quad & \left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_{e_m}^2}\right) \le \frac{1}{\tau}, \quad \forall m \in \mathcal{M}, \\ & \mathbf{u}^H \mathbf{u}\mathbf{v}^H (P_s \mathbf{R}_r + \sigma_r^2 \mathbf{I}_N) \mathbf{v} \le P_T \ , \end{aligned} \quad (13)$$

To solve (13), we first assume that τ is fixed and the problem (13) is solved for each value of τ. Next, one dimensional search is done over τ and the best value of τ is selected.

Now, for a fixed value of τ, we have,

$$\begin{aligned} \max_{\mathbf{u},\mathbf{v}} \quad & \frac{\mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_d^2} \\ \text{s.t.} \quad & \left(1 + \frac{P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_{e_m}^2}\right) \le \frac{1}{\tau}, \quad \forall m \in \mathcal{M}, \\ & \mathbf{u}^H \mathbf{u}\mathbf{v}^H (P_s \mathbf{R}_r + \sigma_r^2 \mathbf{I}_N) \mathbf{v} \le P_T. \end{aligned} \quad (14)$$

Or, equivalently, as,

$$\begin{aligned} \max_{\mathbf{u},\mathbf{v}} \quad & \frac{\mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v}}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u}\mathbf{v}^H \mathbf{v} + \sigma_d^2} \\ \text{s.t.} \quad & \tau P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{R}_r \mathbf{v} + \\ & \qquad (\tau - 1)\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u}\mathbf{v}^H \mathbf{v} \le (1 - \tau)\sigma_{e_m}^2, \\ & \qquad \forall m \in \mathcal{M} \\ & \mathbf{u}^H \mathbf{u}\mathbf{v}^H (P_s \mathbf{R}_r + \sigma_r^2 \mathbf{I}_N) \mathbf{v} \le P_T. \end{aligned} \quad (15)$$

Without loss of generality, we can assume that one of two vectors $\mathbf{u}$ and $\mathbf{v}$ is unit norm and the energy of another vector is determined by solving (15). We assume that $\mathbf{v}$ is of unit-norm and write it as,

$$\mathbf{v} = \sqrt{\alpha} \frac{\mathbf{h}_r}{\|\mathbf{h}_r\|} + \sqrt{1 - \alpha} \mathbf{h}_{r_\perp} \quad (16)$$

where, $\mathbf{h}_{r_\perp}$ is the unit-norm vector that belongs to the null-space of $\mathbf{h}_r$ and α is a real variable between zero and one. So, we have,

$$\mathbf{v}^H \mathbf{R}_r \mathbf{v} = \alpha \|\mathbf{h}_r\|^2 \quad (17)$$

and therefore, (15) is replaced by,

$$\begin{aligned} \max_{\mathbf{u},\alpha} \quad & \frac{\alpha \mathbf{u}^H \mathbf{R}_d \mathbf{u} \|\mathbf{h}_r\|^2}{\sigma_r^2 \mathbf{u}^H \mathbf{R}_d \mathbf{u} + \sigma_d^2} \\ \text{s.t.} \quad & \alpha \tau P_s \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u} \|\mathbf{h}_r\|^2 + \\ & \qquad (\tau - 1)\sigma_r^2 \mathbf{u}^H \mathbf{R}_{e_m} \mathbf{u} \le (1 - \tau)\sigma_{e_m}^2, \\ & \qquad \forall m \in \mathcal{M} \\ & \mathbf{u}^H \mathbf{u}(\alpha P_s \|\mathbf{h}_r\|^2 + \sigma_r^2) \le P_T. \end{aligned} \quad (18)$$

Now, the variable α is assumed as a fixed value and for each

value of it, the following optimization problem is solved,

$$\begin{aligned}\max_{\mathbf{u}} \quad & \frac{\mathbf{u}^H\mathbf{R}_d\mathbf{u}}{\sigma_r^2\mathbf{u}^H\mathbf{R}_d\mathbf{u}+\sigma_d^2}\\ \text{s.t.} \quad & \left(\alpha\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2\right)\mathbf{u}^H\mathbf{R}_{e_m}\mathbf{u}\le(1-\tau)\sigma_{e_m}^2, \quad \forall m\in\mathcal{M}\\ & \|\mathbf{u}\|^2\le\frac{P_T}{\alpha P_s\|\mathbf{h}_r\|^2+\sigma_r^2}. \end{aligned} \tag{19}$$

The objective function of (19) is an increasing function of $\mathbf{u}^H\mathbf{R}_d\mathbf{u}$ and so, (19) can be simplified to,

$$\begin{aligned}\max_{\mathbf{u}} \quad & \mathbf{u}^H\mathbf{R}_d\mathbf{u}\\ \text{s.t.} \quad & \left(\alpha\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2\right)\mathbf{u}^H\mathbf{R}_{e_m}\mathbf{u}\le(1-\tau)\sigma_{e_m}^2, \quad \forall m\in\mathcal{M}\\ & \|\mathbf{u}\|^2\le\frac{P_T}{\alpha P_s\|\mathbf{h}_r\|^2+\sigma_r^2}. \end{aligned} \tag{20}$$

According to (13), at least one of the *M* first constraints is satisfied with equality. So, the optimum value of τ is between zero and one. Thus, the corresponding constraint should be held with equality in (20). The right hand side of *M* first constraints in (20) is non-negative. In the left hand side, $\mathbf{u}^H\mathbf{R}_{e_m}\mathbf{u}$ is non-negative, since the matrix $\mathbf{R}_{e_m}$ is positive semi-definite. But the term $\alpha\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2$ may be positive or negative value in general. To satisfy one of constraints with equality, this term must not get the negative value. So, we should have,

$$\alpha_{\text{opt}}(\tau)\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2\ge 0, \tag{21}$$

Therefore, (20) can be rewritten as,

$$\begin{aligned}\max_{\mathbf{u}} \quad & \mathbf{u}^H\mathbf{R}_d\mathbf{u}\\ \text{s.t.} \quad & \mathbf{u}^H\mathbf{R}_{e_m}\mathbf{u}\le\frac{(1-\tau)\sigma_{e_m}^2}{\alpha\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2}, \quad \forall m\in\mathcal{M}\\ & \|\mathbf{u}\|^2\le\frac{P_T}{\alpha P_s\|\mathbf{h}_r\|^2+\sigma_r^2}. \end{aligned} \tag{22}$$

Using the definition $\mathbf{U}=\mathbf{u}\mathbf{u}^H$, we arrive at,

$$\begin{aligned}\max_{\mathbf{U}} \quad & \text{tr}(\mathbf{R}_d\mathbf{U})\\ \text{s.t.} \quad & \text{tr}(\mathbf{R}_{e_m}\mathbf{U})\le\frac{(1-\tau)\sigma_{e_m}^2}{\alpha\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2}, \quad \forall m\in\mathcal{M}\\ & \text{tr}(\mathbf{U})\le\frac{P_T}{\alpha P_s\|\mathbf{h}_r\|^2+\sigma_r^2}\\ & \text{Rank }\mathbf{U}=1 \ \text{ and } \ \mathbf{U}\succcurlyeq 0. \end{aligned} \tag{23}$$

The rank constraint is not convex and therefore (23) is a non-convex problem. To overcome this issue, we ignore the rank constraint, i.e., Semi-Definite Relaxation (SDR) method, and arrive at,

$$\begin{aligned}\max_{\mathbf{u}} \quad & \text{tr}(\mathbf{R}_d\mathbf{U})\\ \text{s.t.} \quad & \text{tr}(\mathbf{R}_{e_m}\mathbf{U})\le\frac{(1-\tau)\sigma_{e_m}^2}{\alpha\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2}, \quad \forall m\in\mathcal{M}\\ & \text{tr}(\mathbf{U})\le\frac{P_T}{\alpha P_s\|\mathbf{h}_r\|^2+\sigma_r^2},\\ & \mathbf{U}\succcurlyeq 0. \end{aligned} \tag{24}$$

The problem (24) is a Semi-Definite Programming (SDP) problem, see [12], and can be solved by software packages such as CVX [11]. Generally, the optimal solution of (24) is an upper bound for the optimal solution of (23). If the optimum value of $\mathbf{U}$ is of rank one, the vector $\mathbf{u}$ can be computed using the principle eigenvector of $\mathbf{U}$. Otherwise, randomization methods can be used to obtain the approximated rank-one matrix and a lower bound for the optimal solution of (23), see [13]–[15].

Remark 1: In numerical results, we saw that the solution of (24) is of rank-one in almost all cases. So, it can be considered as a close-to-optimal solution of (23). Also, more than 99% of situations, we get $\alpha_{\text{opt}}=1$. It means that the receive beamforming at the relay is matched filtering.

Remark 2: There exist some facts at the optimization problems that can be used to limit the search interval of α_{opt} and τ_{opt}.

We know,

$$\mathbf{u}^H\mathbf{R}_{e_m}\mathbf{u}\le\|\mathbf{h}_{e_m}\|^2\|\mathbf{u}\|^2\le\frac{\|\mathbf{h}_{e_m}\|^2P_T}{\alpha P_s\|\mathbf{h}_r\|^2+\sigma_r^2}, \quad \forall m\in\mathcal{M}, \tag{25}$$

where the first inequality is taken from the definition of $\mathbf{R}_{e_m}$, $\mathbf{R}_{e_m}=\mathbf{h}_{e_m}\mathbf{h}_{e_m}^H$, and the second one comes from the relay power constraint of (19). If we have,

$$\frac{\|\mathbf{h}_{e_m}\|^2P_T}{\alpha P_s\|\mathbf{h}_r\|^2+\sigma_r^2}<\frac{(1-\tau)\sigma_{e_m}^2}{\alpha\tau P_s\|\mathbf{h}_r\|^2+(\tau-1)\sigma_r^2}, \quad \forall m\in\mathcal{M}, \tag{26}$$

or equivalently,

$$\begin{aligned}&\alpha P_s\|\mathbf{h}_r\|^2(\tau P_T\|\mathbf{h}_{e_m}\|^2-(1-\tau)\sigma_{e_m}^2)<\\ &\qquad(1-\tau)\sigma_r^2(\sigma_{e_m}^2+P_T\|\mathbf{h}_{e_m}\|^2), \quad \forall m\in\mathcal{M}, \end{aligned} \tag{27}$$

none of the *M* first constraints of (22) are satisfied with equality and so the solution of (22) can not give the solution of (13).

On the other hand, we should not have,

$$\tau\le\frac{\sigma_{e_m}^2}{P_T\|\mathbf{h}_{e_m}\|^2+\sigma_{e_m}^2}, \quad \forall m\in\mathcal{M}, \tag{28}$$

since the left hand side of (27) must not get the negative value. If (28) is satisfied, (27) is satisfied for all values of m and this is not desired.

So, from (27), the following inequalities should not be held.

$$\alpha<\frac{\sigma_r^2(1-\tau)(\sigma_{e_m}^2+P_T\|\mathbf{h}_{e_m}\|^2)}{P_s\|\mathbf{h}_r\|^2(\tau P_T\|\mathbf{h}_{e_m}\|^2-(1-\tau)\sigma_{e_m}^2)}, \quad \forall m\in\mathcal{M}. \tag{29}$$

By other words, the following inequality must be satisfied,

$$\alpha \geq \min_{m\in\mathcal{M}} \left\{ \frac{\sigma_r^2(1-\tau)(\sigma_{e_m}^2 + P_T\|\mathbf{h}_{e_m}\|^2)}{P_s\|\mathbf{h}_r\|^2(\tau P_T\|\mathbf{h}_{e_m}\|^2 - (1-\tau)\sigma_{e_m}^2)} \right\}. \quad (30)$$

Based on (21) and (30), the linear search for finding $\alpha_{\text{opt}}(\tau)$ can be done in the following interval,

$$\alpha_l \leq \alpha_{\text{opt}}(\tau) \leq 1, \quad (31)$$

where,

$$\alpha_l = \max\left\{ \frac{(1-\tau)\sigma_r^2}{\tau P_s\|\mathbf{h}_r\|^2}, \min_{m\in\mathcal{M}} \left\{ \frac{\sigma_r^2(1-\tau)(\sigma_{e_m}^2 + P_T\|\mathbf{h}_{e_m}\|^2)}{P_s\|\mathbf{h}_r\|^2(\tau P_T\|\mathbf{h}_{e_m}\|^2 - (1-\tau)\sigma_{e_m}^2)} \right\} \right\}. \quad (32)$$

If $\alpha_l > 1$, there is not suitable value for α and the respective τ can not be an optimal solution.

According to (21), at the optimal solution, we should have,

$$\tau \geq \frac{\sigma_r^2}{\alpha_{\text{opt}} P_s\|\mathbf{h}_r\|^2 + \sigma_r^2}, \quad (33)$$

and since $\alpha_{\text{opt}} \leq 1$, we have,

$$\tau \geq \frac{\sigma_r^2}{P_s\|\mathbf{h}_r\|^2 + \sigma_r^2}. \quad (34)$$

Therefore, based on (28) and (34), the sufficient interval to search the τ_{opt} is given by,

$$\tau_l \leq \tau_{\text{opt}} \leq 1, \quad (35)$$

where,

$$\tau_l = \max\left\{ \frac{\sigma_r^2}{P_s\|\mathbf{h}_r\|^2 + \sigma_r^2}, \min_{m\in\mathcal{M}} \left\{ \frac{\sigma_{e_m}^2}{P_T\|\mathbf{h}_{e_m}\|^2 + \sigma_{e_m}^2} \right\} \right\}. \quad (36)$$

Using (31) and (35) the computational complexity of searches is effectively reduced.

IV. Numerical Results

In this section, numerical results including the achievable secrecy rate and relay transmit power are provided. We use monte carlo simulation in which the maximization problem is solved for many realizations of the channels and we represent the average of their results. The channel coefficients are generated as complex Gaussian random variables with zero mean and unit variance. Also, we assume that all noises have unit power and transmit power of source is $P_s = 10$dBW [2].

In Fig. 2, the achievable secrecy rate versus available power at relay, i.e., P_T, for different values of *M* and *N* is depicted. This figure shows that when we increase P_T, the secrecy rate is also increased and it tends to a constant value. We know that when the transmit power of relay is increased, destination and eavesdroppers receive signals with higher SNR and so the secrecy rate cannot tend to infinity. Also, we see that greater secrecy rate can be obtained by increasing the number of relay's antennas and decreasing the number of eavesdroppers. Fig. 3 shows the transmit power of relay versus the maximum allowable transmit power of it. We see that the relay consumes all of its available power and it means that the power constraint of optimization problem is held with equality at optimal point.

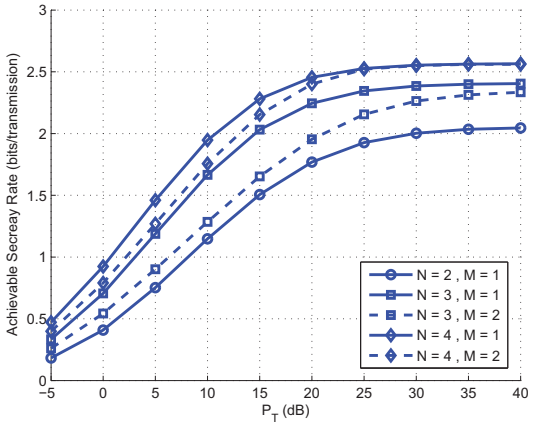

Fig. 2. Achievable Secrecy Rate versus P_T for various values of *N* and *M*.

In Fig. 4, the achievable secrecy rate of our work is compared with three various schemes when $N = 3$ and $M = 2$. In each of these schemes, the receive beamforming vector is set as matched filter. In scheme 1, the transmit beamforming vector is found such that the achievable secrecy rate is maximized under the relay power constraint. In fact, the optimization problem of previous section is solved only for $\alpha = 1$. We see that the results of scheme 1 coincides with our results, because in our results, we saw that the receive beamforming is equivalent to matched filtering in more than 99% of situations. In scheme 2, the transmit beamforming vector is set in the direction of relay-destination channel such as [16]. It is seen that our work has significant improvement, since [16] doesn't consider the presence of eavesdropper. Scheme 3 assumes that the transmit beamforming vector is in the null-space of relay-eavesdroppers channels. By other words, the relay transmits its signal such that no desired signal is received at eavesdroppers. One can see that in low values of P_T, scheme 3 has less secrecy rate than our work and they tend to each other when P_T is increased.

V. Conclusion

This paper aimed at maximizing the achievable secrecy rate of MIMO AF relaying wire-tap channel. The relay uses receive and transmit beamforming at its receiver and transmitter, respectively. We formulated the problem as linear search and SDP problem. The linear search was proposed to find receive beamforming vector and SDP problem for computing transmit beamforming vector.

[2]Please note that here it is assumed the transmit SNR at the source is 10dB. Thus, noting the received noise at destination is of unit power, thus the transmit power at the source becomes 10dBW.

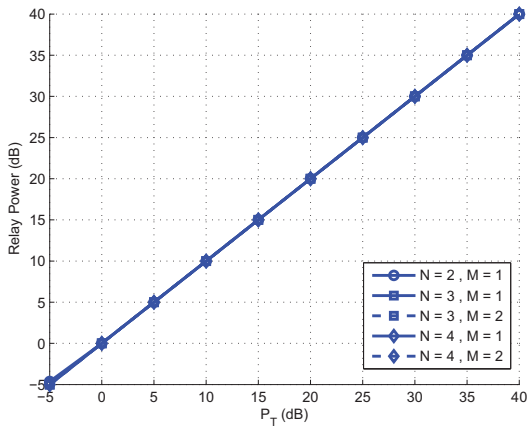

Fig. 3. Relay Transmit Power versus P_T for various values of N and M.

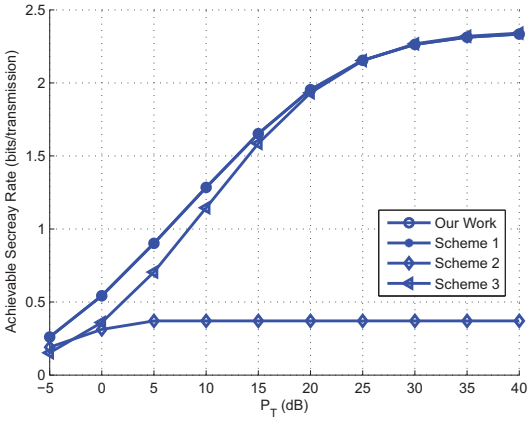

Fig. 4. Comparing results of our work with three various schemes for $N = 3$ and $M = 2$.

REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[4] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[5] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity-part I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[6] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[7] 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.

[8] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. 44th Annu. Conf. Inform. Sci., Syst. (CISS)*, Princeton, NJ, USA, Mar. 2010, pp. 1–6.

[9] 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 Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[10] X.-D. Zhang X. Wang, K. Wang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, June 2013.

[11] M. Grant and S. Boyd, "Cvx: Matlab software for disciplined convex programming," 2008, [Online]. Available: http://stanford.edu/boyd/cvx.

[12] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge Univ. Press, Cambridge, U.K., 2004.

[13] W.-K. Ma, T. N. Davidson, K. M. Wong, Z.-Q. Luo, and P.-C. Ching, "Quasi-maximum-likelihood multiuser detection using semi-definite relaxation with application to synchronous cdma," *IEEE Trans. Signal Process.*, vol. 50, no. 4, pp. 912–922, Apr. 2002.

[14] P. Tseng, "Further results on approximating nonconvex quadratic optimization by semidefinite programming relaxation," *SIAM J. Optim.*, vol. 14, no. 1, pp. 268–283, July 2003.

[15] S. Zhang, "Quadratic maximization and semidefinite relaxation," *Math. Program.*, vol. 87, pp. 453–465, 2000.

[16] V. Havary-Nassab, S. Shahbazpanahi, and A. Grami, "Joint receive-transmit beamforming for multi-antenna relaying schemes," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4966–4972, Sep. 2010.