Improving Physical Layer Security in AF Relay Networks via Beam-forming and Jamming

DOI:
10.1109/VTCFall.2016.7881043

Document Version
Accepted author manuscript

Improving Physical Layer Security in AF Relay Networks via Beam-forming and Jamming

Abdelhamid Salem, and Khairi A. Hamdi,
School of Electrical & Electronic Engineering, University of Manchester, Manchester, UK
emails: {abdelhamid.salem, k.hamdi}@manchester.ac.uk

***Abstract*—In this paper the cooperation of beam-forming and artificial noise (AN) in two-hop amplify-and-forward (AF) relaying system is proposed to enhance the security. we consider a half duplex AF relaying network with a multi-antenna source node and a destination in the presence of a passive eavesdropper. Since channel state information (CSI) of the eavesdropper is unknown, the AN transmitted by the source in the first phase and by the relays in the second phase is in all directions except the legitimate node one. As such two scenarios are considered here,: i) when all the relays amplify and forward the information source signal ii) when only the best relay is selected to amplify and forward the information source signal. The beam-former weights and the power allocation are obtained by solving an optimization problem. Results reveal that the proposed system can provide considerable improvements in terms of secrecy rate. It is also found that increasing the AN power, relative to the information signal power, will further improve the secrecy rate.**

***Index Terms*—Physical layer security, beam-forming, cooperative relaying, jamming, secrecy rate.**

I. INTRODUCTION

THE fundamental broadcast nature of wireless network makes it vulnerable to eavesdrop information signals. This has rapidly increased the attention to the issue of security in wireless communication networks. It is widely known that the main purpose of security in such communication medium is to prevent illegitimate receivers from understanding confidential information signals between the transmitter and the legitimate receiver. Physical layer security is able to secure communications even in the presence of eavesdroppers with unlimited computation ability. This concept is not new; in fact, it was first developed a few decades ago by Wyner, [1]. It was reported that secure communications is possible if the eavesdropper channel is a degraded version of the destination channel. In light of this, the rate at which the transmitter can send secret messages to the receiver while the unauthorized receiver is unable to understand them is known as *secrecy rate*. Considerable amount of research has been conducted on the topic of improving physical layer security in wireless communication via cooperating relays. For example, the authors in [2] [3] studied the physical layer security for different cooperative schemes. These authors presented that the cooperation can greatly improve the security. In addition, to further enhance communication security, joint cooperative beam-forming and jamming has been proposed in [4], [5], whereas physical layer security with artificial noise (AN) in the context of power allocation is presented in [6]. In [7] a joint cooperative beam-forming and jamming scheme is proposed to enhance the security of an AF relay network, where a part of relay nodes adopt distributed beam-forming while others jam the eavesdropper.

In this paper, we propose a joint beam-forming and AN scheme in the two phases in an AF relay system, when the channel state information (CSI) of the eavesdropper is unknown. Two scenarios are considered here, : i) all the relays amplify and forward the information source signal ii) only the best relay is chosen to amplify and forward the information source signal. In the former case, the source transmits information signals with AN to confuse the eavesdropper in the first phase; however, since the CSI of the eavesdropper is unknown, the source transmits AN isotropically in the null space of the relays' channels. In the second phase all the relays amplify and forward the received signal with AN, again, isotropically in the null space of the destination channel. In the latter scenario, in the initial phase the transmitter selects the best relay. In phase I the source transmits the information signal to the selected relay using beam-forming along with AN isotropically in the null space of the best relay channel. In phase II, the best relay amplifies and forwards the information signal using beam-forming while the other relays transmit AN isotropically in the null space of the destination channel. With this design, the two phases are secure in both scenarios. In light of this, we investigate the effectiveness of power allocation on the secrecy rate of the system. Results reveal that considerable secrecy rate improvements can be attained with the proposed system. In particular, it is shown that increasing the information signal power and decreasing the noise power will reduce the secrecy rate. In addition, splitting the source power evenly between the information and AN while increasing the AN power at the relay will result in improved secrecy rate.

We use the following notations in this paper: Bold uppercase and bold lowercase letters denote matrices and vectors, respectively. Conjugate operation, transpose operation and conjugate transpose are denoted by $(.)^*$, $(.)^T$ and $(.)^H$, respectively. The notation $|.|$ denotes the absolute value of a scalar; $\|a\|$ denotes the 2-norm of the vector a. Circularly symmetric is denoted by $\mathcal{CN}\left(\mu,\sigma^2\right)$; $\log(.)$ denotes logarithm of base-2; I identity matrix and $\mathrm{diag}\{\mathbf{a}\}$ represents a diagonal matrix whose diagonal elements are the elements of the vector $\mathbf{a}$.

II. SYSTEM MODEL

We consider AF relays network model consisting of one source node equipped with N antennas sending information signal to a destination via M helping relays in the

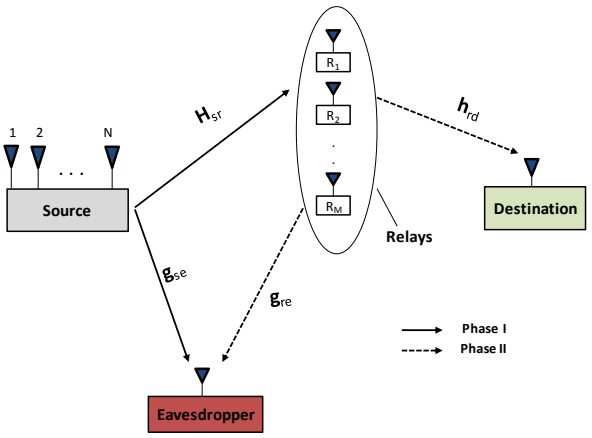

Figure 1. Joint cooperative beam-forming and jamming technique.

existence of a passive eavesdropper. In this model, the eavesdropper, the relays and the destination have a single antenna each. All channel coefficients between these nodes $\mathbf{H_{sr}} \in \mathbb{C}^{\mathbf{M}\times\mathbf{N}}$, $\mathbf{h_{rd}} \in \mathbb{C}^{\mathbf{1}\times\mathbf{M}}$, $\mathbf{g_{se}} \in \mathbb{C}^{\mathbf{1}\times\mathbf{N}}$, $\mathbf{g_{re}} \in \mathbb{C}^{1\times M}$**,** as shown in Fig. 1, are assumed to undergo quasi stationary flat-fading. Due to the poor quality of the source-destination channel, we assume that there is no direct link between the two nodes, and there is full cooperation between the relays[1]. The noise at any node is assumed to be zero mean white Gaussian. As mentioned in the introduction, we propose, here, a joint beam-forming and AN in the two phases, for two different scenarios as follows.

A. Scenario (I)

In this Scenario all the relays amplify and forward the information source signal. In the first phase the source sends information signal with AN, since the CSI of the eavesdropper is unknown the AN is isotropic in all directions and lies in the null space of the relays' channel while in the second phase all the relays amplify and forward the received signal with AN isotropically in the null space of the destination channel, as follow

- Phase I: the signal transmitted by the source can be written as [5], [6]

$$\mathbf{s} = \boldsymbol{\delta} + \Theta \tag{1}$$

where $\boldsymbol{\delta}$ is $N \times 1$ information signal and Θ is $N \times 1$ AN vector. The information signal can be written as $\boldsymbol{\delta} = \sqrt{P_x}\boldsymbol{\rho}x$, where $\boldsymbol{\rho}$ is beam-forming vector matching to the right singular vector of $\mathbf{H_{sr}}$ with highest singular value [9] and x is the information signal with transmitting power P_x. The AN component can also be expressed as $\Theta = \mathbf{Un}$, where $\mathbf{U}$ is a matrix, whose columns form an orthonormal basis for the null space of $\mathbf{H_{sr}}$ such that $\mathbf{H_{sr}U} = \mathbf{0}$ and $\mathbf{U^H U} = \mathbf{I}$ and $\mathbf{n}$ is Gaussian vector, the transmitter selects elements of $\mathbf{n}$ to be $i.i.d$ Gaussian random variables with zero mean and variance σ_n^2 [10]. Therefore, the signal received at the relays is given by

$$\mathbf{y_r} = \mathbf{H_{sr}}\boldsymbol{\delta} + \mathbf{n_r} \tag{2}$$

where $\mathbf{n_r}$is the $M \times 1$ noise vector at the relays, with $\mathrm{E}\left[\mathbf{n_r}\mathbf{n_r^\dagger}\right] = \mathbf{I}_M\sigma_r^2$. The signal received at the eavesdropper can be written as

$$y_e^{(1)} = \mathbf{g_{se}}\boldsymbol{\delta} + \mathbf{g_{se}}\Theta + n_e \tag{3}$$

where n_e is the noise at the eavesdropper with variance σ_e^2.

- Phase II: the signal transmitted by the relays is

$$\mathbf{x_r} = \mathrm{diag}\left\{\mathbf{w}\right\}\mathbf{y_r} + \mathbf{n}_a \tag{4}$$

where $\mathbf{w}$ is the $M \times 1$ relay beam-former vector, $\mathbf{n}_a$ is the $M \times 1$ AN component in form $\mathbf{n}_a = \mathbf{Vz}$, with $\mathbf{V}$ is a matrix, each column of $\mathbf{V}$ is orthogonal on $\mathbf{h_{rd}}$, i.e. $\mathbf{h_{rd}V} = 0$, $\mathbf{z}$ is Gaussian vector, the elements of $\mathbf{z}$ are $i.i.d$ Gaussian random variables with zero mean and variance σ_z^2. The power of the transmitted signal by each relay should be less than or equal the relay power. The received signals at the destination and eavesdropper in the second phase can be written as

$$y_d = \mathbf{w^H}\mathrm{diag}\left\{\mathbf{h_{rd}}\right\}\mathbf{H_{sr}}\boldsymbol{\delta} + \mathbf{w^H}\mathrm{diag}\left\{\mathbf{h_{rd}}\right\}\mathbf{n}_r + n_d \tag{5}$$

$$y_e^{(2)} = \mathbf{w^H}\mathrm{diag}\left\{\mathbf{g_{re}}\right\}\mathbf{H_{sr}}\boldsymbol{\delta} + \mathbf{w^H}\mathrm{diag}\left\{\mathbf{g_{re}}\right\}\mathbf{n_r} + \mathbf{g_{re}}\mathbf{n}_a + n_e, \tag{6}$$

respectively, where n_d is the noise at the destination with variance σ_d^2. From (5) and (6), the rate at the destination and the eavesdropper can be expressed as in (7) and (8), shown at the top of the next page, respectively.

$$R_d = \frac{1}{2}\log\left(1 + \frac{\mathbf{w^H R_a w}}{\mathbf{w^H R_{rd} w} + \sigma_d^2}\right) \tag{7}$$

where $\mathbf{R_a} = \mathbf{a}\mathbf{a}^H$, $\mathbf{a} = \sqrt{P_x}\mathrm{diag}\left\{\mathbf{h_{rd}}\right\}\mathbf{H_{sr}}\boldsymbol{\rho}$, $\mathbf{R_{rd}} = \sigma_r^2\mathrm{diag}\left\{\mathbf{h_{rd}}\right\}\mathrm{diag}\left\{\mathbf{h_{rd}^H}\right\}$, $\mathbf{R_b} = \mathbf{b}\mathbf{b}^H$, $\mathbf{b} = \sqrt{P_x}\mathrm{diag}\left\{\mathbf{g_{re}}\right\}\mathbf{H_{sr}}\boldsymbol{\rho}$ and $\mathbf{R_{re}} = \sigma_r^2\mathrm{diag}\left\{\mathbf{g_{re}}\right\}\mathrm{diag}\left\{\mathbf{g_{re}^H}\right\}$.

B. Scenario (II)

In this case, we propose three phases to send the information signal, in the initial phase the best relay is selected. The conventional relay selection criterion can be expressed as [11]–[13]

$$\text{Optimal relay} = \max_{i\in M}\{\min\{\left\|\mathbf{h}_{si}\right\|^2, \left|h_{id}\right|^2\}\}. \tag{9}$$

where $\mathbf{h}_{si}$ is $1 \times N$ channels between the source and the i^{th} relay, and h_{id} is the channel between the i^{th} relay and the destination. The conventional relay selection policy ensures that the relay with the best path between the source and the destination is selected. Secondly, In the first phase, the source sends information signal with AN which is in the null space

[1]In many applications, the relay can not be equipped with multiple antennas due to the cost and the limitation of size, in these cases, exploiting multiple relays with cooperative communication is natural extension [8].

$$R_e = \frac{1}{2}\log\left(1 + \frac{P_x\left|\mathbf{g_{se}}\boldsymbol{\rho}\right|^2}{\mathbf{g_{se}}\mathbf{U}\mathbf{U}^{\mathbf{H}}\mathbf{g}_{\mathbf{se}}^{\mathbf{H}}\sigma_n^2 + \sigma_e^2} + \frac{\mathbf{w}^{\mathbf{H}}\mathbf{R_b}\mathbf{w}}{\mathbf{w}^{\mathbf{H}}\mathbf{R_{re}}\mathbf{w} + \mathbf{g_{re}}\mathbf{V}\mathbf{V}^{\mathbf{H}}\mathbf{g}_{\mathbf{re}}^{\mathbf{H}}\sigma_z^2 + \sigma_e^2}\right) \tag{8}$$

of the best relay channel. Thirdly, In the second phase, the best relay amplifies and forwards the information signal to the destination while the other relays send AN in all the directions except in the destination direction as follow

- Phase I

The transmitted signal by the source is given by (1), the AN here will broadcast in the null space of the best relay's channel $(\mathbf{h_{sr^*}})$, i.e. $\mathbf{h_{sr^*}}\mathbf{U} = 0$**.** Therefore, the signal received at the best relay is

$$y_r = \mathbf{h_{sr^*}}\boldsymbol{\delta} + n_r. \tag{10}$$

where n_r is the noise at the best relay with variance σ_r^2. The received signal at the eavesdropper is then

$$y_e^{(1)} = \mathbf{g_{se}}\boldsymbol{\delta} + \mathbf{g_{se}}\Theta + n_e \tag{11}$$

- Phase II

Since the CSI of the eavesdropper is unknown, all the $(M-1)$ relays send AN isotropically in the null space of the destination channel, and the best relay amplifies and forwards the information signal to the destination. The signal transmitted by the relays can be written as

$$x_r = \begin{cases} y_r w_r & \text{transmitted by the best relay} \\ \tilde{\mathbf{n}} & \text{transmitted by the}(M-1)\text{relays} \end{cases} \tag{12}$$

where w_r is the weight of the best relay and $\tilde{\mathbf{n}}$ is the $(M-1)\times 1$ AN vector sent from the $(M-1)$ relays. The AN transmitted by the relays can be written as $\tilde{\mathbf{n}} = \mathbf{V}\mathbf{z}$, where $\mathbf{V}$ is the projection matrix onto the null space of the channel vector between the $M-1$ relays and the destination $\mathbf{h_{rd_{(m-1)}}}$, i.e. $\mathbf{h_{rd_{(m-1)}}}\mathbf{V} = \mathbf{0}$ and $\mathbf{z}$ is Gaussian vector, the elements of $\mathbf{z}$ are $i.i.d.$ Gaussian random variables with zero mean and variance $\sigma_{\tilde{z}}^2$. The received signal at the destination can be given by

$$y_d = h_{rd^*}w_r\mathbf{h_{sr^*}}\boldsymbol{\delta} + h_{rd^*}w_r n_r + n_d. \tag{13}$$

where h_{rd^*} is the channel between the best relay and the destination. The signal received at the eavesdropper can be written as

$$y_e^{(2)} = \mathbf{g_{re_{(m-1)}}}\tilde{\mathbf{n}} + g_{re^*}w_r\mathbf{h_{sr^*}}\boldsymbol{\delta} + g_{re^*}w_r n_r + n_e \tag{14}$$

where $\mathbf{g_{re_{(m-1)}}}$ is $1\times(M-1)$ channel vector between the $(M-1)$ relays and the eavesdropper whereas g_{re^*} is the channel between the best relay and the eavesdropper. Now, from (13) we can write the rate at the destination as

$$R_d = \frac{1}{2}\log\left(1 + \frac{P_x\left|\mathbf{h_{sr^*}}\boldsymbol{\rho}\right|^2\left|h_{rd^*}\right|^2\left|w_r\right|^2}{\sigma_r^2\left|w_r\right|^2\left|h_{rd^*}\right|^2 + \sigma_d^2}\right). \tag{15}$$

To maximize the received signal at the best relay in the first phase the beam-forming vector $\boldsymbol{\rho}$ should be $\boldsymbol{\rho} = \frac{\mathbf{h_{sr^*}^H}}{\|\mathbf{h_{sr^*}}\|}$ [9]. Therefore, the rate at the destination is

$$R_d = \frac{1}{2}\log\left(1 + \frac{P_x w_r R_{sd} w_r^*}{\sigma_r^2 w_r r_{rd} w_r^* + \sigma_d^2}\right) \tag{16}$$

where $R_{sd} = \mathbf{h_{sr^*}}\,h_{rd^*}\,h_{rd^*}^H\,\mathbf{h_{sr^*}^H}$, $r_{rd} = h_{rd^*}\,h_{rd^*}^H$. On the other hand, the rate at the eavesdroppers is given by (17), shown at the top of the next page.

III. Power Allocation Secrecy Scheme

To consider the physical layer security, the achievable maximum secrecy rate is measured as

$$R_s = \max[R_d - R_e]^+ \tag{18}$$

where $[x]^+ = \max(0,\, x)$. In this section, the power allocation at the relays as well as at the source is investigated.

A. Relays Power Allocation

Since the CSI of the eavesdropper is unknown, the power used for information transmission at the relays is minimized to threshold value of a signal-to-noise ratio (SNR) at the destination γ_d. As a result, more power can be now used for AN transmission by the relays in order to confuse the eavesdropper [7]. To start with, we first fix the power at the source while allocating the transmitted power at the relays. The total power at the relays is $P_R = P_I + P_n$, where P_I is the power for information transmission and P_n is the power for AN.

1) Scenario (I): In this case, the power for information transmission at the relays is given by, $P_I = \mathbf{w}^H T\mathbf{w}$, where $T = \mathrm{E}\left(\left|y_r\right|^2\right)$. From (7) the SNR at the destination is

$$\mathrm{SNR} = \frac{\mathbf{w^H}\mathbf{R_a}\mathbf{w}}{\mathbf{w^H}\mathbf{R_{rd}}\mathbf{w} + \sigma_d^2} \tag{19}$$

According to the discussion above, the problem of power allocation can be solved mathematically as

$$\min_{\mathbf{w}} \mathbf{w}^H T\mathbf{w}$$

$$s.t..... \frac{\mathbf{w^H}\mathbf{R_a}\mathbf{w}}{\mathbf{w^H}\mathbf{R_{rd}}\mathbf{w} + \sigma_d^2} \geqslant \gamma_d. \tag{20}$$

It should be pointed out that a similar optimization problem was solved in [14]. We can simplify (20) as , $\tilde{W} = T^{\frac{1}{2}}\mathbf{w}$ and $\tilde{W}^H = T^{\frac{1}{2}}\mathbf{w}^H$. The inequality constraint in (20) is convinced with equality at the optimum; therefore, we can write the optimization problem as

$$R_e = \frac{1}{2}\log\left(1+\frac{P_x\left|\mathbf{g_{se}}\boldsymbol{\rho}\right|^2}{\sigma_n^2\mathbf{g_{se}}\mathbf{U}\mathbf{U}^{\mathbf{H}}\mathbf{g}_{\mathbf{se}}^{\mathbf{H}}+\sigma_e^2}+\frac{P_x\left|w_r\right|^2\left|\mathbf{h_{sr^*}}\boldsymbol{\rho}\right|^2\left|g_{re^*}\right|^2}{\mathbf{g_{re_{(m-1)}}}\mathbf{V}\mathbf{V}^{\mathbf{H}}\mathbf{g}_{\mathbf{re_{(m-1)}}}^{\mathbf{H}}\sigma_{\tilde{z}}^2+\left|w_r\right|^2\left|g_{re^*}\right|^2\sigma_r^2+\sigma_e^2}\right). \quad (17)$$

$$\min_{\tilde{W}}\left\|\tilde{W}\right\|^2$$

$$s.t.\ldots\ldots\ldots\tilde{W}^H T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\mathbf{R_{rd}})T^{-\frac{1}{2}}\tilde{W}=\gamma_d\sigma_d^2 \quad (21)$$

Lagrange multiplier function can be given as [15]

$$L(\tilde{W},\lambda)=\left\|\tilde{W}\right\|^2-\lambda([\tilde{W}^H T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\mathbf{R_{rd}})T^{-\frac{1}{2}}\tilde{W}]-\gamma_d\sigma_d^2). \quad (22)$$

By differentiate $L(\tilde{W},\lambda)$ with respect to $\tilde{W}^H$, we get

$$\frac{\partial L}{\partial\tilde{W}^H}=\tilde{W}-\lambda T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\mathbf{R_{rd}})\,T^{-\frac{1}{2}}\tilde{W} \quad (23)$$

Equating (23) to zero, we obtain

$$T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\,\mathbf{R_{rd}})\,T^{-\frac{1}{2}}\tilde{W}=\frac{1}{\lambda}\tilde{W} \quad (24)$$

From (24), it is clear that $\tilde{W}$ is one of the eigenvectors of the matrix $T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\,\mathbf{R_{rd}})T^{-\frac{1}{2}}\tilde{W}$ and $\frac{1}{\lambda}$ is the corresponding eigenvalue. Multiplying both sides of (24) with $\lambda\tilde{W}^H$ yields

$$\left\|\tilde{W}\right\|^2=\tilde{W}^H\tilde{W}=\lambda\tilde{W}^H T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\mathbf{R_{rd}})T^{-\frac{1}{2}}\tilde{W}=\lambda\sigma_d^2\gamma_d \quad (25)$$

Minimizing $\left\|\tilde{W}\right\|^2$ is equivalent to minimizing λ. Hence, $1/\lambda$ has to be the largest eigenvalue of $T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\mathbf{R_{rd}})T^{-\frac{1}{2}}$. Finally the solution is $\tilde{W}=\beta\mu$, where $\mu=\mathrm{p}\{T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\mathbf{R_{rd}})T^{-\frac{1}{2}}\}$, $\mathrm{p}\{x\}$ represents the normalized principal eigenvector of a matrix x and β is chosen to satisfy the equality constrain .i.e.

$$\beta=\sqrt{\frac{\gamma_d\sigma_d^2}{\mu^H T^{-\frac{1}{2}}(\mathbf{R_a}-\gamma_d\mathbf{R_{rd}})T^{-\frac{1}{2}}\mu}} \quad (26)$$

Therefore, the optimal weight value is given by $\mathbf{w}=\tilde{W}T^{-\frac{1}{2}}$. Now, we can easily find the AN power at the relays as (P_R-P_I), this power is equally distributed between the relays.

2) Scenario (II): In this case, the transmission power of the information signal at the best relay P_I is given by

$$P_I=w_r^* T\,w_r \quad (27)$$

where $T=E\left(\left|y_r\right|^2\right)$. From (16) the SNR at the destination can be expressed as

$$\mathrm{SNR}=\frac{P_x w_r^* R_{sd} w_r}{\sigma_r^2 w_r^* r_{rd} w_r+\sigma_d^2} \quad (28)$$

Similarly as in the previous scenario, we can solve the problem of power allocation at the relays as follows

$$\min_{w_r} w_r^* T\,w_r$$

$$s.t.\ldots\ldots\ldots\frac{P_x w_r^* R_{sd} w_r}{\sigma_r^2 w_r^* r_{rd} w_r+\sigma_d^2}\geqslant\gamma_d \quad (29)$$

Using same procedures as in the first scenario, we can derive the optimal weight value as $w_r=\beta\mu T^{-\frac{1}{2}}$, where $\mu=\mathrm{p}\{T^{-\frac{1}{2}}(P_x R_{sd}-\gamma_d\sigma_r^2 r_{rd})T^{-\frac{1}{2}}\}$, and β is selected to satisfy the equality constrain .i.e.

$$\beta=\sqrt{\frac{\gamma_d\sigma_d^2}{\mu^H T^{-\frac{1}{2}}(P_x R_{sd}-\gamma_d\sigma_r^2 r_{rd})\,T^{-\frac{1}{2}}\mu}} \quad (30)$$

Now, the AN power at the $(M-1)$ relays can be calculated as (P_R-P_I), which is, again, equally distributed between the relays.

B. Source Power Allocation

The total power at the source is $P_s=P_x+\sigma_n^2(N-1)$, where P_x is the power for information transmission and σ_n^2 is the power for AN. As such, the relationship between the information signal power (P_x) and the total source power (P_s) can be written as $P_x=\varepsilon P_s$, where $\varepsilon\in[0,1)$ is the fraction factor, whereas the relationship between the AN power and the total power is $\sigma_n^2=\frac{(1-\varepsilon)P_s}{N-1}$. To allocate the source power, we consider the following two approaches [6], [16]. In the first approach, the fraction factor is progressively varied from 0 to 1, then the impact of this variation on the secrecy rate can be observed. In the second, the power at the source is equally distributed between the information signal and AN, i.e. $\varepsilon=0.5$.

IV. NUMERICAL RESULTS

In this section we present numerical results of the expressions derived in the previous sections. For simplicity and without loss of generality, our results in this section are based on eight transmitting antennas $(N=8)$, the number of relays is $(M=4)$, one eavesdropper and one destination. In addition, the channel coefficients are randomly generated, Monte Carlo simulations are conducted with 10^6 independent trials.

Fig. 2 depicts the secrecy rate as a function of the fraction factor ε for the two different scenarios discussed previously when $\gamma_d=12,16\,\text{and}\,20$ dB, the noise power at all the nodes is $\sigma^2=-20$ dBm and $P_S=P_R=20$ dBm. The first observation one can see from these results is that, in both scenarios the secrecy rate deteriorates when the fraction factor is increased regardless of the value of γ_d and approaches zero when the AN in the first phase is zero, and this explain increasing the signal power without AN in the first phase

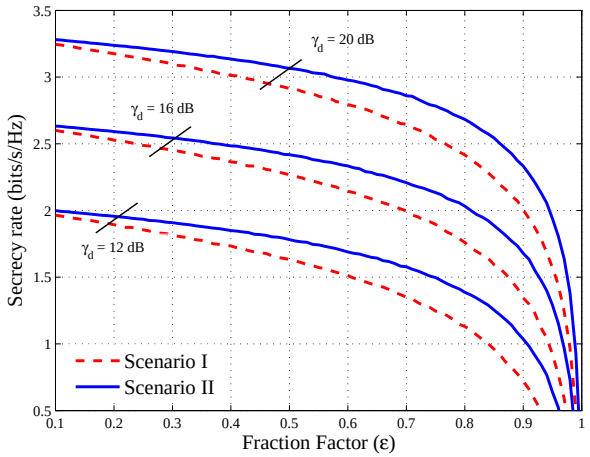

Figure 2. The achievable secrecy rate versus fraction factor for various values of γ_d.

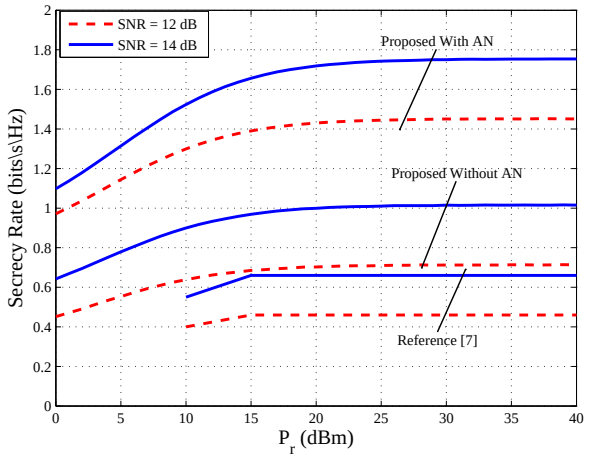

Figure 3. Comparison of the secrecy rate of the proposed scheme scenario II and the scheme proposed in [7] for various values of γ_d

makes the system insecure. It is also apparent that, as γ_d is increased the secrecy rate improves. Interestingly enough, however, it is clear that the secrecy rate for scenario II is clearly better than that of scenario I and this is clearly justified by the water-filling theorem [9].

On the other hand, To make fair comparison between our scheme and the scheme proposed in [7], our results here are based on number of relays is $M = 8$, we chose scenario II for comparison. Fig. 3 illustrates the achievable secrecy rate of the proposed system versus P_r with and without AN when $P_s = 12$ dBm, $N = 16$, $\sigma^2 = -20$ dBm and $\gamma_d = 12$ and 14 dB. It should be highlighted that in this figure the source power is evenly divided between the information and noise signals, i.e. $P_x = \sigma_n^2 = 0.5\,P_s$. For comparison's sake, results for the system introduced in [7] are also included. It is clearly visible that the proposed system always has better performance compared to the system in [7] for all given SNR values. It can also be seen that, for all cases, the secrecy rate gradually enhances as P_r is increased and reaches a plateau when P_r is sufficiently large, $P_r \gtrsim 15$ dBm.

V. Conclusion

In this paper, we have proposed a joint beam-forming and AN to improve the physical layer security in the two-hop AF cooperative relays system. Two scenarios were analyzed, when all the relays amplify and forward the information signal and when the best relay is chosen to amplify and forward the information signal. In both scenarios the power allocation at the source and the relays were considered. Numerical results have shown that considerable secrecy rate improvements can be achieved with the proposed system. Furthermore, as we expected, according to the water-filling theorem, the secrecy rate is found to be better when the best relay is selected compared to the case when all the relays send the message.

References

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, pp. 1875–1888, Mar. 2010.

[3] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, pp. 4985–4997, Oct. 2011.

[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[5] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. Veh. Technol. Conf. (VTC)*, vol. 3, pp. 1906–1910, Sept. 2005.

[6] X. Zhou and M. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *Proc. Int. Conf. Signal Process. Commun. Systems (ICSPCS)*, pp. 1–5, Sept. 2009.

[7] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure af relay systems with individual power constraint and no eavesdropper's csi," *Signal Processing Letters, IEEE*, vol. 20, pp. 39–42, Jan 2013.

[8] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *Information Forensics and Security, IEEE Transactions on*, vol. 8, pp. 2007–2020, Dec 2013.

[9] P. K. Tim Brown and E. D. Carvalho, *Practical Guide to MIMO Radio Channel: with MATLAB Examples*. 2012.

[10] C.-C. J. K. Y.-W. Peter Hong, Pang-Chang Lan, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Singapore Heidelberg New York Dordrecht London: Springer, 2014.

[11] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 2189–2203, April 2014.

[12] I. Krikidis, J. Thompson, S. Mclaughlin, and N. Goertz, "Max-min relay selection for legacy amplify-and-forward systems with interference," *IEEE Trans. Wireless Commun*, vol. 8, pp. 3016–3027, June 2009.

[13] A. Bletsas, A. Khisti, D. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel Areas Commun.*, vol. 24, pp. 659–672, March 2006.

[14] V. Havary-Nassab, S. Shahbazpanahi, A. Grami, and Z.-Q. Luo, "Distributed beamforming for relay networks based on second-order statistics of the channel state information," *IEEE Trans. Signal Process.*, vol. 56, pp. 4306–4316, Sept 2008.

[15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge UK: Cambridge University. Press, 2004.

[16] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of mimo ofdm systems by beamforming and artificial noise generation," *Physical Communication*, vol. 4, pp. 313 – 321, 2011.