Performance Analysis of Secrecy Capacity for Two Hop AF Relay Networks with Zero Forcing

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

***Abstract*—In this paper, we analyze the secrecy capacity of a multiple-input multiple-out (MIMO) half duplex amplify-and-forward (AF) relay network in the presence of one passive eavesdropper. Zero forcing (ZF) processing is utilized at various locations to improve the capacity when the eavesdropper is equipped with a single antenna. The impact of the proposed ZF-based technique on the secrecy capacity is investigated for three different scenarios depending on where the ZF is applied, namely, 1) ZF at the relay and destination, 2) ZF at the source and relay, 3) ZF at the relay. For these configurations, analytical expressions for the ergodic-secrecy capacity are derived, and simulation results are provided throughout the paper to validate our analysis. Results reveal that reducing the number of source and/or destination antennas will enhance the ergodic-secrecy capacity and the significance of this enhancement is dependent on the particular scenario adopted. Furthermore, it will be shown that, in general, secrecy capacity improves with increasing the relay power.**

***Index Terms*—AF relay, MIMO, physical layer security, secrecy capacity, zero forcing (ZF).**

I. Introduction

The fundamental broadcast nature of wireless networks 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 the eavesdropper from utilizing the information signals between the transmitter and receiver. Traditionally, security in wireless networks is realized by operating on the higher layer protocols of the network with which perfect security is not always guaranteed, particularly when the eavesdropper has sufficiently high computational power. On the contrary, the physical layer security is able to secure communications even in the presence of eavesdroppers with unlimited computation ability. The concept of physical layer security is not new, in fact, it was first developed few decades ago by Wyner, [1], and it is showed that secure communications is possible if the eavesdropper channel is a degraded version of the main channel. In light of this, the secrecy rate is defined as the rate at which the transmitter can send secret messages to the receiver while the unauthorized eavesdropper is unable to understand it. In addition, the maximum secrecy rate is referred to as the capacity rate.

There has been considerable amount of research on improving the physical layer security via cooperative relays. For instance, the authors in [2], [3] found that cooperative communications can greatly improve security in comparison to the non-cooperative systems. Furthermore, these authors studied different relaying schemes to find the optimal relay weights that maximize the secrecy rate or minimize the transmit power. In [4], however, the secrecy capacity is evaluated over Gaussian multiple-input multiple-output (MIMO) wiretap channel consisting of a transmitter with two antennas, a receiver with two antennas and an eavesdropper with a single antenna. Very recently, the problem of computing the perfect secrecy capacity of Gaussian MIMO wire-tap channels is analyzed in [5], [6]. Additionally, it is found in [7] that transmit antenna selection scheme in conjunction with receive selection combining can further enhance the physical layer security in MIMO wiretap channels. In MIMO relay networks, due to various sources sending multiple independent signals simultaneously, interference occurs at the relays (first phase) and at the destination (second phase). In this environment, interference cancellation techniques such as zero forcing (ZF) should be implemented at the source, relay and/or destination. The sum rate of MIMO two-way AF relay networks with ZF is analyzed in [8] whereas the authors in [9] evaluated the performance of ZF-based two-hop relay networks.

To the best of our knowledge, the impact of ZF on the security of MIMO two-hop AF relay networks has not been addressed yet. Unlike these studies, in this paper we analyze mathematically the security in two-hop AF relay networks for several scenarios based on the design strategy of ZF, i.e. in terms of its location. The rationale for selecting ZF, and not others, is mainly because of its simplicity and ease of implementation. Therefore, the contribution of this paper is threefold. Analytical expressions are derived to calculate the ergodic-secrecy capacity for the proposed system under the following configurations 1) ZF at the relay and destination, 2) ZF at the source and relay, 3) ZF at relay. throughout the paper, simulation results are also included to confirm the validity of our analysis. The results show that reducing the number of source or/and destination antennas can considerably enhance the secrecy capacity. Furthermore, it is found that the capacity gain is also influenced by the design strategy of ZF being adopted as well as the relay power.

The notations used in this paper are: 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 $|.|$ represents the absolute value of a scalar

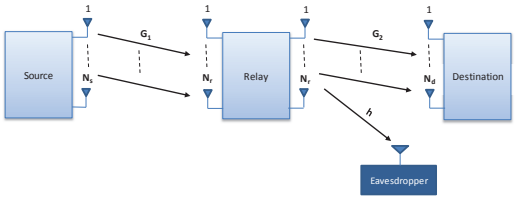

Figure 1. Block diagram of two-hop AF relay network with ZF processing in the presence of one eavesdropper.

whereas $\|.\|$ denotes Euclidean norm. Circularly symmetric is denoted by $\mathcal{CN}\left(\mu,\sigma^2\right)$; $\log\left(.\right)$ represents logarithm of base-2; I identity matrix and diag$\{\mathbf{a}\}$ represents a diagonal matrix whose diagonal elements are the elements of the vector $\mathbf{a}$; Tr $(.)$ is the trace of a matrix; $[A]_{k,k}$ is the element (k,k), $[A]_k$ is the column k in matrix A and $E\left(.\right)$ denotes expectation.

II. System Model

We consider an AF relay network model consisting of N_s source nodes sending independent information signals to N_d destination nodes via N_r relay nodes with the existence of a passive eavesdropper equipped with a single antenna to eavesdrop one specific signal as illustrated in Fig. 1. As seen from this figure, the channels coefficients between the nodes are denoted as $\mathbf{G}_1 \sim \mathcal{CN}_{N_r,N_s}\left(0_{N_r\times N_s},\mathbf{I}_{N_r}\otimes\mathbf{I}_{N_s}\right)$, $\mathbf{G}_2 \sim \mathcal{CN}_{N_d,N_r}\left(0_{N_d\times N_r},\mathbf{I}_{N_d}\otimes\mathbf{I}_{N_r}\right)$ and $\mathbf{h} \sim \mathcal{CN}_{1,N_r}\left(0_{1\times N_r},\mathbf{I}_{N_r}\right)$. Due to the poor quality of the source-destination channel, we assume that there is no direct link between the two nodes. It is also assumed that the noise at the nodes is zero mean white Gaussian with variance $\left(\sigma^2\right)$, i.e. $\mathcal{CN}\left(0,\,\sigma^2\right)$. In general, communication between the source and destination in relay networks is accomplished over two phases. In the first phase, the source nodes broadcast signals to the relay nodes, whereas in the second the relay nodes forward the received signal to the destination nodes. With this in mind, we assume that the eavesdropper is located close to the relay nodes, see Fig. 1, i.e. security becomes an issue in the second phase. To start with, the received signal vector at the relays is expressed as

$$\mathbf{y}_r = a_s\,\mathbf{G}_1\mathbf{W}_s\,\mathbf{x}+\mathbf{n}_r \tag{1}$$

where $\mathbf{y}_r=[y_1,.....,y_{N_r}]^T$, $\mathbf{W}_s$ is the $N_s\times N_s$ source weight matrix, $\mathbf{x}$ is $N_s\times 1$ transmitted signal vector with variance $\mathbf{I}_{N_s}$, $\mathbf{n}_r$ is $N_r\times 1$ additive wight Gaussian noise (AWGN) vector at the relay nodes with variance σ_r^2 and a_s is the normalization constant that was designed to constrain the transmit power at the source (P_s) given by

$$a_s=\sqrt{\frac{P_s}{\mathrm{Tr}\left(\mathrm{E}\left[\mathbf{W}_s\mathbf{W}_s^H\right]\right)}} \tag{2}$$

Therefore, the received signal vector at the destination is

$$\mathbf{y}_d = a_s\,a_r\,\mathbf{W}_d\,\mathbf{G}_2\mathbf{W}_r\mathbf{G}_1\mathbf{W}_s\mathbf{x}+a_r\,\mathbf{W}_d\,\mathbf{G}_2\mathbf{W}_r\mathbf{n}_r+\mathbf{W}_d\,\mathbf{n}_d \tag{3}$$

where $\mathbf{y}_d=[y_1,.....,y_{N_d}]^T$, $\mathbf{W}_r$ is the $N_r\times N_r$ relay weight matrix, $\mathbf{W}_d$ is the $N_d\times N_d$ destination weight matrix, $\mathbf{n}_d$ is $N_d\times 1$ AWGN vector at the destination nodes with variance σ_d^2 and a_r is the normalization constant designed to constrain the transmit power at the relay and is given by [9]

$$a_r=\sqrt{\frac{\frac{P_r}{\sigma_r^2}\mathrm{Tr}\left(\mathrm{E}\left[\mathbf{W}_s\mathbf{W}_s^H\right]\right)}{\frac{P_s}{\sigma_r^2}\mathrm{Tr}\left(\mathrm{E}\left[\mathbf{Q}\right]\right)+\mathrm{Tr}\left(\mathrm{E}\left[\mathbf{W}_r\mathbf{W}_r^H\right]\right)}} \tag{4}$$

where $\mathbf{Q}=\mathbf{W}_r\,\mathbf{G}_1\,\mathbf{W}_s\,\mathbf{W}_s^H\,\mathbf{G}_1^H\,\mathbf{W}_r^H$. At the receiver, the signal-to-interference noise ratio (SINR) for the k^{th} transmitted signal can be written as follows

$$\gamma_{dk}=\frac{a_s^2\,a_r^2\,\left[\mathbf{W}_d\,\mathbf{G}_2\,\mathbf{W}_r\,\mathbf{G}_1\,\mathbf{W}_s\,\mathbf{W}_s^H\,\mathbf{G}_1^H\,\mathbf{W}_r^H\,\mathbf{G}_2^H\,\mathbf{W}_d^H\right]_{k,k}}{\left[a_r^2\,\mathbf{W}_d\,\mathbf{G}_2\,\mathbf{W}_r\,\mathbf{W}_r^H\,\mathbf{G}_2^H\,\mathbf{W}_d^H\,\sigma_r^2+\mathbf{W}_d\,\mathbf{W}_d^H\,\sigma_d^2\right]_{k,k}} \tag{5}$$

. Assuming that the transmitter does not have any knowledge of the receiver and eavesdropper CSIs, the ergodic secrecy capacity can then be obtained as [10][11]

$$\bar{C}_s=\left[\mathrm{E}\left(C_d\right)-\mathrm{E}\left(C_e\right)\right]^+ \tag{6}$$

where $[l]^+=\max\left(0,l\right)$, C_d and C_e are the destination and eavesdropper capacities given by $C_d=\left(\frac{1}{2}\right)\log\left(1+\gamma_d\right)$ and $C_e=\left(\frac{1}{2}\right)\log\left(1+\gamma_e\right)$, respectively, where γ_d and γ_e are the SINRs at the destination and eavesdropper, respectively.

III. System 1: ZF at the relay and destination Nodes

In this system, we analyze the secrecy capacity when ZF receivers are applied at both the relay and the destination nodes. Assuming the relay nodes know the channel matrix between the source and the relay nodes $(\mathbf{G}_1)$ and that the destination nodes know the channel matrix between the relay and the destination nodes $(\mathbf{G}_2)$. Due to mathematical intractability, we assume that $N_r>N_s$ and $N_d>N_r$. The weights at all the nodes are given by [9]

$$\mathbf{W}_s=\mathbf{I}_{N_s}$$

$$\mathbf{W}_r=\mathbf{P}\left(\mathbf{G}_1^H\,\mathbf{G}_1\right)^{-1}\mathbf{G}_1^H$$

$$\mathbf{W}_d=\left(\mathbf{G}_2^H\,\mathbf{G}_2\right)^{-1}\mathbf{G}_2^H \tag{7}$$

where $\mathbf{P}$ is the $\mathbf{I}_{N_r\times N_s}$ matrix to ensure that the N_r signals are transmitted at the relays. Substituting (7) into (5), the SINR of the k^{th} transmitted signal at the destination can be written as

$$\gamma_{dk}=\frac{a_s^2\,a_r^2}{a_r^2\left[\left(\mathbf{G}_1^H\,\mathbf{G}_1\right)^{-1}\right]_{k,k}\sigma_r^2+\sigma_d^2\left[\left(\mathbf{G}_2^H\,\mathbf{G}_2\right)^{-1}\right]_{k,k}} \tag{8}$$

The received signal at the eavesdropper of the k^{th} transmitted signal is expressed as

$$y_{ek} = a\,\mathbf{h}\,\mathbf{W}_r\,\mathbf{g}_{1k}\,x_k + \mathbf{a}\sum_{i=1,i\neq k}^{N_s}\mathbf{h}\mathbf{W}_r\,\mathbf{g}_{1i}\,x_i + a_r\,\mathbf{h}\mathbf{W}_r\,\mathbf{n}_r + n_e \tag{9}$$

where n_e is the AWGN at the eavesdropper with variance σ_e^2, $a = a_s\,a_r$, $\mathbf{g}_{1k}$ and $\mathbf{g}_{1i}$ are the k^{th} and the i^{th} columns in the matrix $\mathbf{G}_1$. Similarly, the SINR of the k^{th} transmitted signal at the eavesdropper is given as

$$\gamma_{ek} = \frac{a_s^2\,a_r^2\,\left|\mathbf{h}\,\mathbf{W}_r\,\mathbf{g}_{1k}\right|^2}{a_s^2\,a_r^2\sum\limits_{i=1,i\neq k}^{N_s}\left|\mathbf{h}\mathbf{W}_r\,\mathbf{g}_{1i}\right|^2 + a_r^2\,\left\|\mathbf{h}\mathbf{W}_r\right\|^2\,\sigma_r^2 + \sigma_e^2} \tag{10}$$

Substituting the weights given by (7) into (2) and (4), the normalization constants at the source and the relay nodes can be expressed, respectively, as

$$a_s = \sqrt{\frac{P_s}{N_s}} \tag{11}$$

$$a_r = \sqrt{\frac{\frac{P_r}{\sigma_r^2}\,N_s\,(N_r - N_s)}{\frac{P_r}{\sigma_r^2}\,N_r\,(N_r - N_s) + N_s^2}}. \tag{12}$$

Based on the SINR expressions (8) and (10), we can now derive the secrecy capacity of this system as follows. To analyze the ergodic capacity at the destination of the k^{th} transmitted signal, (8) can be written as

$$\gamma_{dk} = \frac{\gamma_{rs}}{\gamma_r\,X + Y} \tag{13}$$

where $\gamma_{rs} = \frac{a_r^2\,a_s^2}{\sigma_d^2}$, $\gamma_r = \frac{a_r^2\,\sigma_r^2}{\sigma_d^2}$, $X = \left[\left(\mathbf{G}_1^H\,\mathbf{G}_1\right)^{-1}\right]_{k,k}$ and $Y = \left[\left(\mathbf{G}_2^H\,\mathbf{G}_2\right)^{-1}\right]_{k,k}$. Using lemma 1 in [12], the ergodic capacity at the destination can be expressed as

$$\mathrm{E}\left(C_d\right) = \frac{1}{2\,\ln\left(2\right)}\int_0^\infty \frac{1}{z}\left(\mathcal{M}_R\left(z\right) - \mathcal{M}_{(\gamma_{rs}+R)}\left(z\right)\right)dz \tag{14}$$

where $\mathcal{M}_R\left(z\right)$ is the Moment Generating Function (MGF) of the random variable R, $(R = \gamma_r\,X + Y)$. Since X and Y are independent, the MGF of R is

$$\mathcal{M}_R\left(z\right) = \mathcal{M}_{\gamma_r\,X}\left(z\right)\,\mathcal{M}_Y\left(z\right) \tag{15}$$

and

$$\mathcal{M}_{(\gamma_{rs}+R)}\left(z\right) = e^{-z\,\gamma_{rs}}\mathcal{M}_R\left(z\right) \tag{16}$$

Now, using the Probability Density Function (PDF) of X presented in [9], [8] and the identities in [13], we can calculate the MGF of $\gamma_r\,X$ as

$$\mathcal{M}_{\gamma_r\,X}(z) = \frac{2\,\left(\gamma_r\,z\right)^{\frac{1+N_r-N_s}{2}}\,\mathrm{J}_{1+N_r-N_s}\left(2\sqrt{\gamma_r\,z}\right)}{\Gamma\left(N_r - N_s + 1\right)} \tag{17}$$

where $\mathrm{J}\left(.\right)$ is the modified Bessel function of the second kind [13]. Following the same procedure above, we can get $\mathcal{M}_Y$

$$\mathcal{M}_Y\left(z\right) = \frac{2\,z^{\frac{1+N_d-N_r}{2}}\,\mathrm{J}_{1+N_d-N_r}\left(2\sqrt{z}\right)}{\Gamma\left(N_d - N_r + 1\right)} \tag{18}$$

Substituting (17) and (18) into (15) and then into (14), we obtain the ergodic capacity at the destination.

Similarly, we now calculate the ergodic capacity at the eavesdropper, (10) can be simplified as

$$\gamma_{ek} = \frac{a_s^2\,a_r^2\,\left|\left[\mathbf{h}\right]_k\right|^2}{a_s^2\,a_r^2\sum\limits_{i=1,i\neq k}^{N_s}\left|\left[\mathbf{h}\right]_k\right|^2 + a_r^2\,\left\|\mathbf{h}\mathbf{W}_r\right\|^2\,\sigma_r^2 + \sigma_e^2} \tag{19}$$

In interference limited systems, the noise power can be neglected compared to the interference power; hence, (19) becomes

$$\gamma_{ek} = \frac{a_s^2\,a_r^2\,\left|\left[\mathbf{h}\right]_k\right|^2}{a_s^2\,a_r^2\sum\limits_{i=1,i\neq k}^{N_s}\left|\left[\mathbf{h}\right]_i\right|^2} \tag{20}$$

Let $X = \left|\left[\mathbf{h}\right]_k\right|^2$, $Y = \sum\limits_{i=1,i\neq k}^{N_s}\left|\left[\mathbf{h}\right]_i\right|^2$ and using lemma 1 in [12], the ergodic capacity at the eavesdropper can be given as

$$\mathrm{E}\left(C_e\right) = \frac{1}{2\,\ln\left(2\right)}\int_0^\infty \frac{1}{z}\left(\mathcal{M}_Y\left(z\right) - \mathcal{M}_{(X+Y)}\left(z\right)\right)dz \tag{21}$$

Since both Y and $X + Y$ have chi-square destribution with $N_s - 1$ and N_s degrees of freedom, their MGFs are found, respectively, to be

$$\mathcal{M}_Y\left(z\right) = \left(2\,z + 1\right)^{-\left(\frac{N_s-1}{2}\right)} \tag{22}$$

$$\mathcal{M}_{X+Y}\left(z\right) = \left(2\,z + 1\right)^{-\left(\frac{N_s}{2}\right)} \tag{23}$$

By substituting $\mathcal{M}_Y\left(z\right)$ and $\mathcal{M}_{X+Y}\left(z\right)$ in (21), an expression for the ergodic-capacity at the eavesdropper can be obtained as in (24)- at the top of the next page-, where $\psi^0\left(.\right)$ is the Polygamma function.

Finally, the ergodic-secrecy capacity of this system can be obtained by substituting (14) and (24) into (6).

IV. System 2: ZF at the source and the relay Nodes

In this scenario, we analyze the secrecy capacity where zero forcing precoders are used at the source and relay nodes. In this analysis, we assume that the source and relay nodes know $\mathbf{G}_1$ and $\mathbf{G}_2$, respectively. We also assume that $N_s > N_r$ and $N_r > N_d$. To start with, the weights at the nodes in this system are given by [9]

$$\mathbf{W}_s = \mathbf{G}_1^H\left(\mathbf{G}_1\,\mathbf{G}_1^H\right)^{-1}\mathbf{P}_1$$

$$\mathbf{W}_r = \mathbf{G}_2^H\left(\mathbf{G}_2\,\mathbf{G}_2^H\right)^{-1}\mathbf{P}_2$$

$$\mathrm{E}\left(C_e\right)=\frac{1}{2\ln\left(2\right)}\left[-\psi^0\left(\frac{1}{2}\left(-1+N_s\right)\right)+\psi^0\left(\frac{N_s}{2}\right)\right] \tag{24}$$

$$\mathbf{W}_d=\mathbf{I}_{N_d} \tag{25}$$

where $\mathbf{P}_1$ is the $\mathbf{I}_{N_r\times N_s}$ matrix to ensure that the N_r out of N_s signals are transmitted at the source, and $\mathbf{P}_2$ is the $\mathbf{I}_{N_d\times N_r}$ matrix to ensure that the N_d out of N_r signals are transmitted at the relays.

Substituting the values of $\mathbf{W}_s$, $\mathbf{W}_r$ and $\mathbf{W}_d$ given by (25) in (5), the SINR of the k^{th} transmitted signal at the destination can be written as

$$\gamma_{dk}=\frac{a_s^2\,a_r^2}{a_r^2\,\sigma_r^2+\sigma_d^2} \tag{26}$$

Also, the received signal at the eavesdropper of the k^{th} signal received at the destination is given by

$$y_{ek}=a\,\mathbf{h}\left[\mathbf{W}_r\right]_k x_k+a\sum_{i=1,i\neq k}^{N_d}\left(\mathbf{h}\left[\mathbf{W}_r\right]_i x_i\right)+a_r\,\mathbf{h}\mathbf{W}_r\,\mathbf{n}_r+n_e \tag{27}$$

where $a=a_s a_r$. Hence, the SINR of the k^{th} signal at the eavesdropper can be found to be

$$\gamma_{ek}=\frac{a_s^2\,a_r^2\,\left|\mathbf{h}\left[\mathbf{W}_r\right]_k\right|^2}{a_s^2\,a_r^2\sum\limits_{i=1,i\neq k}^{N_d}\left(\left|\mathbf{h}\left[\mathbf{W}_r\right]_i\right|^2\right)+a_r^2\,\left\|\mathbf{h}\mathbf{W}_r\right\|^2\,\sigma_r^2+\sigma_e^2} \tag{28}$$

Similarly as in the previous system and by substituting the weights given by (25) into (2) and (4), the normalization constants at the source and the relay nodes are written, respectively, as

$$a_s=\sqrt{\frac{P_s\left(N_s-N_r\right)}{N_r}} \tag{29}$$

$$a_r=\sqrt{\frac{\frac{P_r}{\sigma_r^2}N_r\left(N_r-N_d\right)}{\frac{P_s}{\sigma_r^2}N_d\left(N_s-N_r\right)+N_r\,N_d}}. \tag{30}$$

To calculate the ergodic-secrecy capacity, we first determine the ergodic capacity at the destination which can be expressed as

$$\mathrm{E}\left(C_d\right)=\frac{1}{2}\,\log\left(1+\gamma_{dk}\right) \tag{31}$$

In order to derive the ergodic capacity at the eavesdropper, we rewrite (28) as

$$\gamma_{ek}=\frac{a_s^2\,a_r^2\,\left|\mathbf{h}\left[\mathbf{W}_r\right]_k\right|^2}{a_s^2\,a_r^2\sum\limits_{i=1,i\neq k}^{N_d}\left|\mathbf{h}\left[\mathbf{W}_r\right]_i\right|^2} \tag{32}$$

Let $X=\left|\mathbf{h}\left[\mathbf{W}_r\right]_k\right|^2$, $\Upsilon=\sum\limits_{i=1,i\neq k}^{N_d}\left|\mathbf{h}\left[\mathbf{W}_r\right]_i\right|^2$, $\beta=X+\Upsilon$ and by using lemma 1 in [12], we can express the ergodic capacity at the eavesdropper as follows

$$\mathrm{E}\left(C_e\right)=\frac{1}{2\,\ln\left(2\right)}\int_0^\infty\frac{1}{z}\left(\mathcal{M}_\Upsilon\left(z\right)-\mathcal{M}_\beta\left(z\right)\right)dz \tag{33}$$

Using the PDF of β derived in [14], the MGF of β can be found to be

$$\mathcal{M}_\beta\left(z\right)=\frac{2\,N_d^{\left(\frac{1}{2}+N_1-\frac{N_2}{2}\right)}\,Z^{\frac{1}{2}\left(-1+N_2\right)}\,\mathrm{J}_{N_2-1}\left(2\sqrt{N_d\,Z}\right)}{N!} \tag{34}$$

where $N_1=N_r-N_d+1$, $N_2=N_r-N_d+2$ and $N=N_r-N_d$. Similarly, $\mathcal{M}_\Upsilon\left(z\right)$ is found as given in (35) - at the top of the next page. Now, by substituting $\mathcal{M}_\Upsilon\left(z\right)$ and $\mathcal{M}_\beta\left(z\right)$ into (33), we can get the eavesdropper ergodic capacity.

Finally, the ergodic-secrecy capacity of this system can be obtained by substituting (31) and (33) in (6).

V. System 3: ZF at the relay Nodes

In this section, the secrecy capacity is evaluated when ZF precoders and receivers are applied at the relay nodes. In this analysis it is assumed that the relay and source nodes know $\mathbf{G}_1$ and $\mathbf{G}_2$, respectively, and that $N_r>N_s$ and $N_s=N_d$. To begin with, in this system, the weights at all the nodes are given by [9][15]

$$\mathbf{W}_s=\mathbf{I}_{N_s}$$

$$\mathbf{W}_r=\mathbf{G}_2^H\left(\mathbf{G}_2\,\mathbf{G}_2^H\right)^{-1}\left(\mathbf{G}_1\,\mathbf{G}_1^H\right)^{-1}\mathbf{G}_1^H$$

$$\mathbf{W}_d=\mathbf{I}_{N_d} \tag{36}$$

Substituting these weights in (5), the SINR of the k^{th} transmitted signal at the destination becomes

$$\gamma_{dk}=\frac{a_s^2\,a_r^2}{a_r^2\left[\left(\mathbf{G}_1^H\,\mathbf{G}_1\right)^{-1}\right]_{k,k}\sigma_r^2+\sigma_d^2} \tag{37}$$

Additionally, the received signal at the eavesdropper of the k^{th} transmitted signal can be given as

$$y_{ek}=a\,\mathbf{h}\mathbf{W}_r\left[\mathbf{G}_1\right]_k x_k+a\sum_{i=1,i\neq k}^{N_d}\mathbf{h}\mathbf{W}_r\left[\mathbf{G}_1\right]_i x_i \tag{38}$$

$$+a_r\mathbf{h}\mathbf{W}_r\,\mathbf{n}_r+n_e$$

where $a=a_s\,a_r$. Consequently, the SINR of the k^{th} transmitted signal at the eavesdropper is

$$\mathcal{M}_{\Upsilon}(z)=\frac{2\,(N_d-1)^{\left(\frac{1}{2}+N_1-\frac{N_2}{2}\right)}\;Z^{\frac{1}{2}(-1+N_2)}\,\mathrm{J}_{N_2-1}\left(2\sqrt{(N_d-1)\;Z}\right)}{N!} \tag{35}$$

$$\gamma_{ek}=\frac{a_s^2\,a_r^2\,\left|\mathbf{h}\mathbf{W}_r\left[\mathbf{G}_1\right]_k\right|^2}{a_s^2\,a_r^2\sum\limits_{i=1,i\neq k}^{N_s}\left(\left|\mathbf{h}\mathbf{W}_r\left[\mathbf{G}_1\right]_i\right|^2\right)+a_r^2\left\|\mathbf{h}\mathbf{W}_r\right\|^2\sigma_r^2+\sigma_e^2} \tag{39}$$

Now, by substituting the weights given by (36) into (2) and (4), the normalization constants at the source and the relay nodes can be given, respectively, as

$$a_s=\sqrt{\frac{P_s}{N_s}} \tag{40}$$

$$a_r=\sqrt{\frac{\frac{P_r}{\sigma_r^2}\;(N_r-N_d)}{\frac{P_s}{\sigma_r^2}}} \tag{41}$$

To derive the ergodic capacity at the destination, (37) can be rewritten as

$$\gamma_{dk}=\frac{t}{\left[\left(\mathbf{G}_1^H\,\mathbf{G}_1\right)^{-1}\right]_{k,k}+b} \tag{42}$$

where $t=\frac{P_s}{\sigma_r^2 N_s}$, $b=\frac{\sigma_d^2 P_s}{\sigma_r^2 P_r(N_r-N_d)}$. Now, substituting $\phi=\left[\left(\mathbf{G}_1^H\,\mathbf{G}_1\right)^{-1}\right]_{k,k}$ and using lemma 1 in [12], we can get the ergodic capacity at the destination as

$$\mathrm{E}\left(C_d\right)=\frac{1}{2\ln(2)}\int_0^{\infty}\frac{1}{z}\left(1-e^{-zt}\right)e^{-zb}\mathcal{M}_{\phi}(z)\,dz \tag{43}$$

To obtain the MGF of ϕ, we follow same steps used to find $\mathcal{M}_X(z)$ in Sec. III. Therefore,

$$\mathcal{M}_{\phi}(z)=\frac{2\,z^{\frac{1+N_r-N_s}{2}}\,\mathrm{J}_{1+N_r-N_s}\left(2\sqrt{z}\right)}{\Gamma\left(N_r-N_s+1\right)} \tag{44}$$

Now, to derive the ergodic capacity at eavesdropper, (39), in interference limited systems, can be simplified as

$$\gamma_{ek}=\frac{a_s^2\,a_r^2\,\left|\mathbf{h}\,\left[\mathbf{W}_{r1}\right]_k\right|^2}{a_s^2\,a_r^2\sum\limits_{i=1,i\neq k}^{N_d}\left|\mathbf{h}\,\left[\mathbf{W}_{r1}\right]_i\right|^2} \tag{45}$$

where $\mathbf{W}_{r1}=\mathbf{G}_2^H\left(\mathbf{G}_2\,\mathbf{G}_2^H\right)^{-1}$. Let $\zeta=\left|\mathbf{h}\left[\mathbf{W}_{r1}\right]_k\right|^2$, $\varrho=\sum\limits_{i=1,i\neq k}^{N_d}\left|\mathbf{h}\left[\mathbf{W}_{r1}\right]_i\right|^2$ and by using lemma 1 in [12], we can write the ergodic capacity at the eavesdropper as

$$\mathrm{E}\left(C_e\right)=\frac{1}{2\,\ln(2)}\int_0^{\infty}\frac{1}{z}\left(\mathcal{M}_{\varrho}(z)-\mathcal{M}_{\tau}(z)\right)dz \tag{46}$$

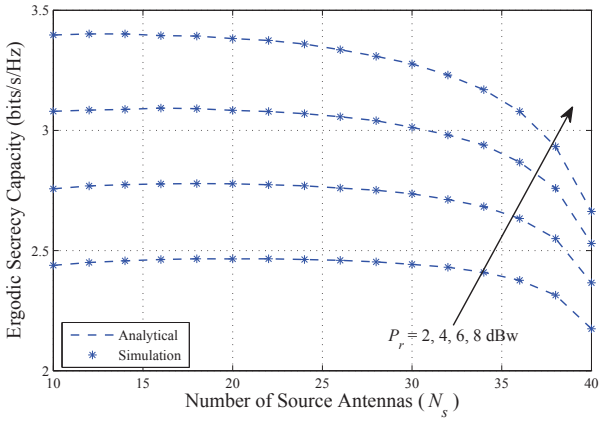

Figure 2. The secrecy capacity versus the number of source antennas for different values of P_r.

where $\tau=\varrho+\zeta$. It is found that $\mathcal{M}_{\varrho}(z)$ and $\mathcal{M}_{\tau}(z)$ are identical to $\mathcal{M}_{\Upsilon}(z)$ and $\mathcal{M}_{\beta}(z)$ derived in Sec. IV, respectively. Finally, the ergodic-secrecy capacity of this system can be obtained by substituting (43) and (46) into (6).

VI. Numerical results

In this section numerical results of the secrecy capacity for the three aforementioned systems are presented and discussed. To validate our analysis, Monte Carlo simulations with 1000000 independent trials are also provided throughout. In all our evaluations, the channel coefficients are randomly generated in each simulation run, the noise power at all nodes is set as $\sigma_r^2=\sigma_d^2=\sigma_e^2=10$ dBm and the source power is $P_s=10$ dBw whereas the power of the relay nodes are varied as $P_r=2,\,4,\,6,$ and 8 dBw.

A. System 1: ZF at the Relay and Destination Nodes

For simplicity and without loss of generality, our results in this subsection are based on the following $N_d=50$ and $N_r=42$ whereas N_s is varied from 10 to 40.

Fig. 2 depicts the analytical and simulated results for the secrecy capacity as a function of the number of source antennas for $P_r=2,\,4\,,6$ and 8 dBw. It is clear that the analytical results and simulated ones are in good agreement. In general, it is obvious that the secrecy capacity degrades with increasing the number of source antennas irrespective of the value of P_r. It can also be seen that the secrecy capacity improves as P_r is increased. For instance, at $N_s=20$, it is clear that there is a 0.25 bits/s/Hz capacity gain when $P_r=4$ dBw relative to the case when $P_r=2$ dBw whereas this gain becomes around 1 bits/s/Hz for $P_r=8$ dBW compared to the same P_r value. Furthermore, it should be highlighted that this enhancement becomes less significant as N_s goes beyond 35.

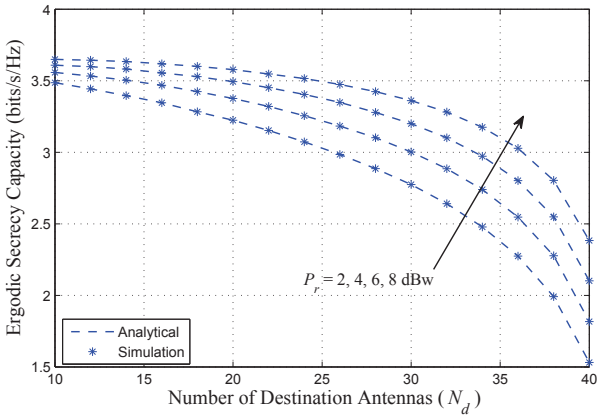

Figure 3. The secrecy capacity versus the number of destination antennas for various values of P_r.

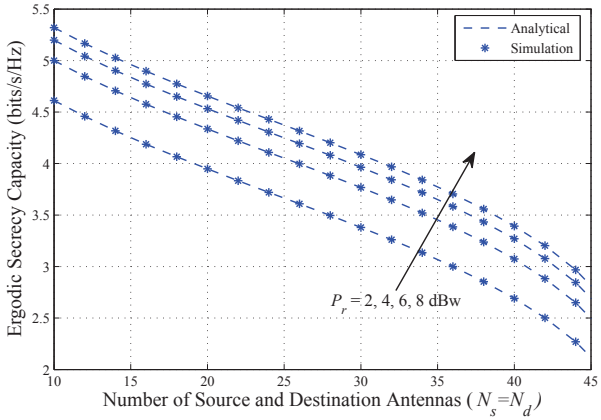

Figure 4. The secrecy capacity versus the number of source and destination antennas for various values of P_r.

B. System 2: ZF at the Source and the Relay Nodes

The results obtained in this subsection are based on $N_s = 50$ and $N_r = 42$ while N_d is varied from 10 to 40. Fig. 3 shows some analytical and simulated results for the secrecy capacity versus the number of destination antennas with $P_r = 2, 4, 6$ and 8 dBw. From these results, it is clearly visible that, the secrecy capacity gradually deteriorates as the number of destination antennas is increased from 10 to 25. This deterioration, however, becomes more significant as N_s goes beyond 25. As anticipated, it is also clear that when N_d approaches N_r, i.e. 42, the secrecy capacity approaches to zero. This can be justified by the fact that under such a condition the normalization power constants a_r (30) approaches which subsequently leads to zero capacity. In addition, it is worthy pointing out that increasing P_r will result in enhancing the ergodic secrecy capacity regardless of the number of destination antennas deployed.

C. System3: ZF at the Relay Nodes

In this section, we set $N_r = 50$ and equally vary N_s and N_d from 10 to 45. Fig. 4 illustrates the achievable secrecy capacity of this system versus the number of source and destination antennas for $P_r = 2, 4, 6$ and 8 dBw. The general trend that can be seen from this figure is that the secrecy capacity worsens as N_s and N_d are increased for all the P_r values under consideration. The other observation one can notice is that, for a given N_s and N_d values, increasing P_r results in improving the ergodic secrecy capacity. It is also worthwhile mentioning that this enhancement becomes of less significance as P_r goes beyond 6 dBw.

VII. Conclusion

In this paper, we have analyzed the secrecy capacity in general MIMO two-hop AF relay networks in the presence a passive eavesdropper when ZF is performed in different locations: a) at the relay and destination nodes, b) at the source and relay nodes, and c) at the relay nodes. In each case, we have derived analytical expressions for the secrecy capacity which are also validated with simulations. The results demonstrated that the secrecy capacity can be controlled by the number of source and/or destination nodes depending on the ZF strategy utilized. Furthermore, it is found that the secrecy capacity can be improved as the transmit power at the relay nodes is increased.

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. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4033–4039, Sept. 2009.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 524–528, Jul. 2008.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas 2014;part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Lett. Commun.*, vol. 17, pp. 1754–1757, Sept. 2013.

[8] G. Amarasuriya, C. Tellambura, and M. Ardakani, "Sum rate analysis of two-way MIMO AF relay networks with zero-forcing," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 4456–4469, Sept. 2013.

[9] R. H. Y. Louie, Y. Li, and B. Vucetic, "Zero forcing in general two-hop relay networks," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 191–202, Jan. 2010.

[10] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *Information Theory, IEEE Transactions on*, vol. 54, pp. 4687–4698, Oct 2008.

[11] P.-C. L. C.-C. J. K. Y.-W. Peter Hong, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. 2014.

[12] K. Hamdi, "A useful lemma for capacity analysis of fading interference channels," *IEEE Trans. Commun.*, vol. 58, pp. 411–416, Feb. 2010.

[13] I. S. G. . I. M. Ryzhik, *Table of Integrals, Series, and Products*. 1980.

[14] X. Shao, J. Yuan, and Y. Shao, "Error performance analysis of linear zero forcing and MMSE precoders for MIMO broadcast channels," *IET Commun.*, vol. 1, pp. 1067–1074, Oct. 2007.

[15] H. Suraweera, H. Q. Ngo, T. Duong, C. Yuen, and E. Larsson, "Multi-pair amplify-and-forward relaying with very large antenna arrays," in *Proc. Int. Conf. Commun.*, pp. 4635–4640, Jun. 2013.