Improving the Security of Cooperative Relaying Networks with Multiple Antennas

Yuzhen Huang[*], Caijun Zhong[†‡], Jinglong Wang[*], Trung Q. Duong[§], Qihui Wu[*], and George K. Karagiannidis[¶]
[*]College of Communications Engineering, PLA University of Science and Technology, China
[†]Institute of Information and Communication Engineering, Zhejiang University, China
[‡]National Mobile Communications Research Laboratory, Southeast University, China
[§]School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, UK
[¶]Aristotle University of Thessaloniki, Thessaloniki, Greece
Email: yzh_huang@sina.com, caijunzhong@zju.edu.cn, wjl543@sina.com, trung.q.duong@qub.ac.uk,
wqhtxdk@yahoo.cn, geokarag@ieee.org

***Abstract*—In this paper, we investigate the secrecy performance of dual-hop amplify-and-forward (AF) multi-antenna relaying systems over Rayleigh fading channels by taking into account the direct link between the source and destination. To improve the secrecy performance, two linear processing schemes at relay and maximal ratio combining (MRC) at destination are proposed, namely, Zero-forcing/MRC (ZF/MRC) and Maximal ratio transmission/MRC (MRT/MRC). For these schemes, we present new tight analytical expressions of the secrecy outage probability. In addition, we examine the performance in high signal-to-noise ratio (SNR) regimes, and present simple secrecy outage approximations for all schemes. The results reveal that: 1) The MRT/MRC scheme achieves a full diversity order of $M+1$, while the ZF/MRC scheme achieves a diversity order of M, where M is the number of antennas at relay. 2) The ZF/MRC scheme outperforms the MRT/MRC scheme in the low SNR regime, while becomes inferior to the MRT/MRC scheme in the high SNR regime.**

I. Introduction

Due to the broadcast nature of wireless medium, wireless transmissions are inherently vulnerable to eavesdropping. The traditional means of combatting eavesdropping is to employ cryptographic schemes in the upper layers, which nevertheless faces the problem of secret key distribution and management in addition to the high complexity of data encryption and decryption processing. Against this background, in the pioneer work [1], the concept of physical layer security was introduced to address the security of wireless communications. The key idea behind this paradigm is to exploit the random characteristics of wireless channels, e.g., fading and noise, to transmit the confidential messages. Later on, in [2], the concept of wiretap channel was introduced and it was proven that perfect security can be achieved when the eavesdropper's channel is a degraded version of the main one. Since then, physical layer security has been widely investigated in various communication scenarios, for example, Gaussian wiretap channel [3] and broadcast wiretap channel [4].

To further enhance the secrecy performance, multiple antenna techniques, which provide extra spatial degrees of freedom, have also gained significant interests [5]–[8]. In [5], the secrecy capacity of the Gaussian wiretap channel with multiple antennas was analyzed. In [6], transmit antenna selection scheme was proposed for secrecy enhancement in MIMO wiretap channels, with different receiver combining schemes. In [7], the authors quantified the effect of antenna correlation on the secrecy performance of multi-antenna wiretap channels in terms of the probability of positive secrecy capacity and the secrecy outage probability. The work in [8] investigated the effect of outdated CSI on the secrecy performance of MIMO wiretap channels with multiple eavesdroppers in non-identical Nakagami fading.

In parallel, employing cooperative relaying to improve the secrecy performance has also received substantial interest [9]–[13]. In [9], the basic four-terminal relay-eavesdropper channel was introduced and an outer-bound on the optimal rate-equivocation region was derived. Later in [10]–[12], different cooperative schemes, such as decode-and-forward (DF), amplify-and-forward (AF) and cooperative jamming (CJ), were designed to enhance the security of dual-hop relaying networks. While in [13], the authors analyzed the secrecy outage probability of dual-hop DF relaying systems, with different suboptimal relay selections.

Although these prior works have significantly improved the knowledge on the secrecy performance of dual-hop relaying networks, they have neglected the impact of the direct link between the transmitter and destination nodes, which may results in an underestimation of the secrecy performance. Only in a recent work [14], the direct link between the legitimate source and destination node was considered, where it was shown that the direct link can be exploited to further enhance the secrecy performance. Motivated by this, in the current work, we consider a more general multi-antenna dual-hop AF relaying network, taking into account the direct link between the source and destination nodes.

To exploit the extra degrees of freedom provided by multi-antennas at relay, we propose a heuristic two-stage relay processing scheme to enhance the security of dual-hop relaying networks, i.e., the relay first uses maximum ratio combining (MRC) to maximize the signal to noise ratio (SNR) of the source-relay link, and then forwards the transformed signal to the desired destination with simple linear processing methods in an attempt to further degrade the quality of eavesdropper's channel. To this end, two popular linear pro-

978-1-5090-1698-3/16/$31.00 ©2016 IEEE

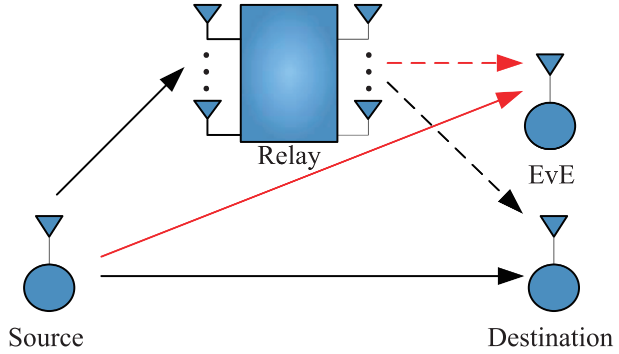

Fig. 1. System model.

cessing methods with MRC at destination will be investigated, i.e., 1) zero-forcing/MRC (ZF/MRC), and 2) maximal ratio transmission/MRC (MRT/MRC). The main contributions of the paper include approximate closed-form expressions for the secrecy outage probability of ZF/MRC and MRT/MRC schemes. Moreover, an asymptotic secrecy outage analysis is carried out in the high SNR regime. In addition, the analytical results demonstrate that the ZF/MRC outperforms MRT/MRC in the low SNR regime, while in the high SNR regime, the MRT/MRC attains better secrecy performance than the ZF/MRC.

II. System Model

We consider a dual-hop multiple antenna AF relaying networks, as illustrated in Fig. 1, where the source (A), the destination (B), and the eavesdropper (E) are equipped with a single antenna, while the relay (R) is equipped with M antennas. Furthermore, we consider the realistic scenario where the direct link between A and B exists, and we assume a half-duplex relaying mode, where the entire communication between A and B is completed in two time slots. During the first phase, A encodes the block information $\mathbf{w}$ into the codeword $\mathbf{x} = [x(1), \cdots, x(i), \cdots, x(n)]$ with $\frac{1}{n}\sum_{i=1}^{n} \mathrm{E}\left[|x(i)|^2\right] \le P_s$ using the capacity achieving codebook for the wiretap channel. The received signals at R, B, and E at time i are given, respectively, by

$$\mathbf{y}_{\mathrm{R}}(i) = \sqrt{P_s}\mathbf{h}_{\mathrm{AR}}x(i) + \mathbf{n}_{\mathrm{R}} \tag{1}$$

$$y_{\mathrm{B},1}(i) = \sqrt{P_s}h_{\mathrm{AB}}x(i) + n_{\mathrm{B},1} \tag{2}$$

$$y_{\mathrm{E},1}(i) = \sqrt{P_s}h_{\mathrm{AE}}x(i) + n_{\mathrm{E},1}, \tag{3}$$

where P_s is the transmit power at A, $\mathbf{h}_{\mathrm{AR}}$ is an $M \times 1$ channel vector for the A → R link with entries following identical and independently distributed Rayleigh fading with parameter λ_1, h_{AB} and h_{AE} denote the channel coefficients for the A → B and A → E links with parameters λ_0 and λ_4, respectively, $\mathbf{n}_{\mathrm{R}}$ is the additive white Gaussian noise (AWGN) at R with $\mathrm{E}\left[\mathbf{n}_{\mathrm{R}}\mathbf{n}_{\mathrm{R}}^{\dagger}\right] = \sigma^2\mathbf{I}$, $n_{\mathrm{B},1}$ and $n_{\mathrm{E},1}$ denote the zero-mean AWGN at B and E with variance σ^2, respectively.

In the second phase, R retransmits a transformed version of $\mathbf{y}_{\mathrm{R}}(i)$ to B, and the signal at B is given by

$$y_{\mathrm{B},2}(i) = \mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{W}\mathbf{y}_{\mathrm{R}}(i) + n_{\mathrm{B},2}, \tag{4}$$

where $\mathbf{h}_{\mathrm{RB}}$ is an $M \times 1$ channel vector for the R → B link, and its entries follow i.i.d. $\mathcal{CN}(0, \lambda_2)$, $n_{\mathrm{B},2}$ is the AWGN with variance σ^2, and $\mathbf{W}$ denotes the transformation matrix at R node with $\mathrm{E}\left[\|\mathbf{W}\mathbf{y}_{\mathrm{R}}(i)\|_F^2\right] = P_r$, where P_r denotes the transmit power constraint at relay.

Similarly, the received signal at E during the second phase can be expressed as

$$y_{\mathrm{E},2}(i) = \mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{W}\mathbf{y}_{\mathrm{R}}(i) + n_{\mathrm{E},2}, \tag{5}$$

where $\mathbf{h}_{\mathrm{RE}}$ is an $M \times 1$ channel vector for the R → E link, and its entries follow i.i.d. $\mathcal{CN}(0, \lambda_3)$, and $n_{\mathrm{E},2}$ is the AWGN with variance σ^2.

Since the two independent copies of the source signal received by B and E, hence, we assume that the MRC is adopted at both B and E to strengthen the signal detection. Hence, by combining (1), (2), (4) and (5), the instantaneous SNRs of the main and the eavesdropper's channels are given by

$$\begin{aligned}\gamma_{\mathrm{B}} &= \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}} \\ &= \frac{P_s}{\sigma^2}|h_{\mathrm{AB}}|^2 + \frac{P_s}{\sigma^2}\frac{\left|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{W}\mathbf{h}_{\mathrm{AR}}\right|^2}{1 + \left\|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{W}\right\|_F^2}\end{aligned} \tag{6}$$

and

$$\begin{aligned}\gamma_{\mathrm{E}} &= \gamma_{\mathrm{AE}} + \gamma_{\mathrm{RE}} \\ &= \frac{P_s}{\sigma^2}|h_{\mathrm{AE}}|^2 + \frac{P_s}{\sigma^2}\frac{\left|\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{W}\mathbf{h}_{\mathrm{AR}}\right|^2}{1 + \left\|\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{W}\right\|_F^2}.\end{aligned} \tag{7}$$

According to [2], the achievable secrecy rate of relaying wiretap channels can be represented as

$$C_{\mathrm{S}} \triangleq \frac{1}{2}\left[\log_2(1 + \gamma_{\mathrm{B}}) - \log(1 + \gamma_{\mathrm{E}})\right]^{+}, \tag{8}$$

where the factor 1/2 accounts for the fact that the total communication takes place in two time slots, and

$$[x]^{+} = \max(x, 0) = \begin{cases} x, & x \ge 0 \\ 0, & x < 0 \end{cases} \tag{9}$$

It is important to note that due to the non-convex nature of the problem, the optimal transform matrix $\mathbf{W}$, which maximizes the achievable secrecy rate, seems not to be analytically tractable. To address this problem, in this paper, we design a heuristic two-stage relay processing strategy, i.e., the relay first uses MRC to maximize the SNR of the A → B link, and then delivers the transformed signal to the B with linear processing methods to degrade the quality of the eavesdropper's channel. Hence, the heuristic relay precoder $\mathbf{W}$ is a rank-1 matrix, i.e., $\mathbf{W} = \alpha\mathbf{w}_2\frac{\mathbf{h}_{\mathrm{AR}}^{\dagger}}{\|\mathbf{h}_{\mathrm{AR}}\|_F}$, where α is the power constraint factor, $\frac{\mathbf{h}_{\mathrm{AR}}^{\dagger}}{\|\mathbf{h}_{\mathrm{AR}}\|_F}$ is utilized for matching the A → R channel link, and $\mathbf{w}_2$ is a $M \times 1$ linear processing vector, which depends on the linear processing scheme employed by the relay. Specifically, we consider two different linear processing schemes with MRC at destination, namely, ZF/MRC and MRT/MRC, as detailed below.

A. ZF/MRC

The objective of ZF scheme is to maximize the received SNR at B while avoiding the leakage of confidential information to the E. According to the ZF principle, we have

$$\begin{aligned} &\max_{\mathbf{w}_2} \left|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{w}_2\right| \\ &s.t.\ \left|\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{w}_2\right| = 0,\ \&\ \left\|\mathbf{w}_2\right\|_F = 1. \end{aligned} \tag{10}$$

By using the projection matrix theory, the weight vector $\mathbf{w}_2$ is given by

$$\mathbf{w}_2 = \frac{\boldsymbol{\Xi}^{\perp}\mathbf{h}_{\mathrm{RB}}}{\left\|\boldsymbol{\Xi}^{\perp}\mathbf{h}_{\mathrm{RB}}\right\|_F}, \tag{11}$$

where $\boldsymbol{\Xi}^{\perp} = \left(\mathbf{I} - \mathbf{h}_{\mathrm{RE}}\left(\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{h}_{\mathrm{RE}}\right)^{-1}\mathbf{h}_{\mathrm{RE}}^{\dagger}\right)$ is the projection idempotent matrix with rank $M-1$. To satisfy the transmit power constraint at relay with AF protocol, the constant α^2 is given by

$$\alpha^2 = \frac{P_r}{\mathbf{h}_{\mathrm{AR}}^{\dagger}\mathbf{h}_{\mathrm{AR}}P_s + \sigma^2}. \tag{12}$$

Thus, the instantaneous SNRs of the main and the eavesdropper's channels with ZF/MRC are given respectively by

$$\begin{aligned} \gamma_{\mathrm{B_{ZF}}} &= \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}}^{\mathrm{ZF}} \\ &= \frac{P_s|h_{\mathrm{AB}}|^2}{\sigma^2} + \frac{\frac{P_s}{\sigma^2}\left\|\mathbf{h}_{\mathrm{AR}}\right\|_F^2 \frac{P_r}{\sigma^2}\left\|\boldsymbol{\Xi}^{\perp}\mathbf{h}_{\mathrm{RB}}\right\|_F^2}{\frac{P_s}{\sigma^2}\left\|\mathbf{h}_{\mathrm{AR}}\right\|_F^2 + \frac{P_r}{\sigma^2}\left\|\boldsymbol{\Xi}^{\perp}\mathbf{h}_{\mathrm{RB}}\right\|_F^2 + 1} \end{aligned} \tag{13}$$

and

$$\gamma_{\mathrm{E_{ZF}}} = \frac{P_s}{\sigma^2}|h_{\mathrm{AE}}|^2. \tag{14}$$

B. MRT/MRC

For the MRT scheme, we set $\mathbf{w}_2$ to match the second hop of the main channel, i.e., $\mathbf{w}_2 = \frac{\mathbf{h}_{\mathrm{RB}}^{\dagger}}{\left\|\mathbf{h}_{\mathrm{RB}}\right\|_F}$. Therefore, the instantaneous SNRs of the main channel and the eavesdropper's channel with the MRT/MRC scheme are expressed respectively as

$$\begin{aligned} \gamma_{\mathrm{B_{MRT}}} &= \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}}^{\mathrm{MRT}} \\ &= \frac{P_s}{\sigma^2}|h_{\mathrm{AB}}|^2 + \frac{\frac{P_s}{\sigma^2}\left\|\mathbf{h}_{\mathrm{AR}}\right\|_F^2 \frac{P_r}{\sigma^2}\left\|\mathbf{h}_{\mathrm{RB}}\right\|_F^2}{\frac{P_s}{\sigma^2}\left\|\mathbf{h}_{\mathrm{AR}}\right\|_F^2 + \frac{P_r}{\sigma^2}\left\|\mathbf{h}_{\mathrm{RB}}\right\|_F^2 + 1} \end{aligned} \tag{15}$$

and

$$\begin{aligned} \gamma_{\mathrm{E_{MRT}}} &= \gamma_{\mathrm{AE}} + \gamma_{\mathrm{RE}}^{\mathrm{MRT}} \\ &= \frac{P_s|h_{\mathrm{AE}}|^2}{\sigma^2} + \frac{\frac{P_s}{\sigma^2}\left\|\mathbf{h}_{\mathrm{AR}}\right\|_F^2 \frac{P_r}{\sigma^2}\frac{\left|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{h}_{\mathrm{RE}}\right|^2}{\left\|\mathbf{h}_{\mathrm{RB}}\right\|_F^2}}{\frac{P_s}{\sigma^2}\left\|\mathbf{h}_{\mathrm{AR}}\right\|_F^2 + \frac{P_r}{\sigma^2}\frac{\left|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{h}_{\mathrm{RE}}\right|^2}{\left\|\mathbf{h}_{\mathrm{RB}}\right\|_F^2} + 1}. \end{aligned} \tag{16}$$

III. Secrecy Performance

A. Preliminaries

In this subsection, we first discuss the statistics of the SNRs of the main and the eavesdropper's channels, which will facilitate the secrecy analysis.

1) ZF/MRC: Although the distributions of γ_{AR} and $\gamma_{\mathrm{RB}}^{\mathrm{ZF}}$ are known, deriving the exact distribution of $\gamma_{\mathrm{B_{ZF}}}$ is not trivial. Hence, we seek tight upper bound which has been widely adopted in prior works such as [15], i.e.,

$$\gamma_{\mathrm{B_{ZF}}} \le \gamma_{\mathrm{AB}} + \min\left(\gamma_1, \gamma_2\right), \tag{17}$$

where $\gamma_1 = \frac{P_s}{\sigma^2}\left\|\mathbf{h}_{\mathrm{AR}}\right\|_F^2$ and $\gamma_2 = \frac{P_r}{\sigma^2}\left\|\boldsymbol{\Xi}^{\perp}\mathbf{h}_{\mathrm{RB}}\right\|_F^2$. Now, we present the PDF of $\gamma_{\mathrm{B_{ZF}}}$ in the following lemma.

Lemma 1. *The PDF of* $\gamma_{\mathrm{B_{ZF}}}$ *can be approximated by*

$$\begin{aligned} f_{\gamma_{\mathrm{B_{ZF}}}}(x) \approx \frac{1}{\overline{\gamma}_0}e^{-\frac{x}{\overline{\gamma}_0}}\Bigg[&\frac{1}{\overline{\gamma}_1^M\Gamma(M)}\sum_{k=0}^{M-2}\frac{\Upsilon\left(\eta_k, \mu_2 x\right)}{k!\mu_2^{\eta_k}\overline{\gamma}_2^k} \\ &+\frac{1}{\overline{\gamma}_2^{M-1}\Gamma(M-1)}\sum_{k=0}^{M-1}\frac{\Upsilon\left(\theta_k, \mu_2 x\right)}{k!\mu_2^{\theta_k}\overline{\gamma}_1^k}\Bigg], \end{aligned} \tag{18}$$

where $\mu_2 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_2} - \frac{1}{\overline{\gamma}_0}$, $\eta_k = M + k$, $\theta_k = M + k - 1$, $\overline{\gamma}_0 = \mathrm{E}\left[\gamma_{\mathrm{AB}}\right]$, $\overline{\gamma}_1 = \mathrm{E}\left[\gamma_1\right]$, $\overline{\gamma}_2 = \mathrm{E}\left[\gamma_2\right]$, *and* $\Upsilon(\cdot,\cdot)$ *is the lower incomplete Gamma function [16, Eq. (8.350.1)].*

Proof: See Appendix A. ■

2) MRT/MRC: Similarly, $\gamma_{\mathrm{B_{MRT}}}$ and $\gamma_{\mathrm{E_{MRT}}}$ can be upper bounded by

$$\gamma_{\mathrm{B_{MRT}}} \le \gamma_{\mathrm{AB}} + \min\left(\gamma_1, \gamma_3\right) \tag{19}$$

and

$$\gamma_{\mathrm{E_{MRT}}} \le \gamma_{\mathrm{AE}} + \min\left(\gamma_1, \gamma_4\right), \tag{20}$$

respectively, where $\gamma_3 = \frac{P_r}{\sigma^2}\left\|\mathbf{h}_{\mathrm{RB}}\right\|_F^2$ and $\gamma_4 = \frac{P_r}{\sigma^2}\frac{\left|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{h}_{\mathrm{RE}}\right|^2}{\left\|\mathbf{h}_{\mathrm{RB}}\right\|_F^2}$. Now, we present the PDFs of $\gamma_{\mathrm{B_{MRT}}}$ and $\gamma_{\mathrm{E_{MRT}}}$ in the following lemmas.

Lemma 2. *The PDF of* $\gamma_{\mathrm{B_{MRC}}}$ *can be approximated by*

$$\begin{aligned} &f_{\gamma_{\mathrm{B_{MRT}}}}(x) \approx \\ &\frac{1}{\Gamma(M)\overline{\gamma}_0}e^{-\frac{x}{\overline{\gamma}_0}}\sum_{k=0}^{M-1}\frac{\Upsilon\left(\eta_k, \mu_2 x\right)}{\Gamma(k+1)\mu_2^{\eta_k}}\left(\frac{1}{\overline{\gamma}_1^M\overline{\gamma}_2^k} + \frac{1}{\overline{\gamma}_1^k\overline{\gamma}_2^M}\right). \end{aligned} \tag{21}$$

Proof: By following similar procedure as in the proof of Lemma 1, the desired PDF of $\gamma_{\mathrm{B_{MRT}}}$ can be easily obtained. ■

Lemma 3. *The PDF of* $\gamma_{\mathrm{E_{MRT}}}$ *can be approximated by*

$$f_{\gamma_{\mathrm{E_{MRT}}}}(x) \approx \frac{e^{-\frac{x}{\overline{\gamma}_4}}}{\overline{\gamma}_4}\left[\frac{\Upsilon\left(M, \mu_4 x\right)}{\overline{\gamma}_1^M\Gamma(M)\mu_4^M} + \sum_{k=0}^{M-1}\frac{\Upsilon\left(\phi_k, \mu_4 x\right)}{k!\mu_4^{\phi_k}\overline{\gamma}_1^k\overline{\gamma}_3}\right], \tag{22}$$

where $\phi_k = k + 1$ *and* $\mu_4 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_3} - \frac{1}{\overline{\gamma}_4}$.

Proof: By following similar steps of Lemma 1, the above equation can be reached. ■

$$
\begin{aligned}
P_{\mathrm{out,ZF/MRC}}\left(R_s\right) \approx{}& \frac{1}{\overline{\gamma}_1^M \Gamma\left(M\right)} \sum_{k=0}^{M-2} \frac{\Gamma\left(\eta_k\right)}{k! \mu_2^{\eta_k} \overline{\gamma}_2^k} \left[1 - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\eta_k - 1} \frac{\mu_2^m}{\mu_1^{m+1}} - e^{-\frac{2^{2R}-1}{\overline{\gamma}_0}} \left(1 + \frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} \right.\\
&\left. + \frac{1}{\overline{\gamma}_4 \overline{\gamma}_0} e^{-\mu_1\left(2^{2R_s}-1\right)} \sum_{m=0}^{\eta_k - 1} \frac{\mu_2^m}{\mu_1^{m+1}} \sum_{v=0}^{m} \frac{\mu_1^v}{v!} \sum_{p=0}^{v} \binom{v}{p} \left(2^{2R_s} - 1\right)^{v-p} 2^{2pR_s} p! \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-p-1} \right]\\
&+ \frac{1}{\overline{\gamma}_2^{M-1} \Gamma\left(M-1\right)} \sum_{k=0}^{M-1} \frac{\Gamma\left(\theta_k\right)}{k! \mu_2^{\theta_k} \overline{\gamma}_1^k} \left[1 - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\theta_k - 1} \frac{\mu_2^m}{\mu_1^{m+1}} - e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \left(1 + \frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} \right.\\
&\left. + \frac{1}{\overline{\gamma}_4 \overline{\gamma}_0} e^{-\mu_1\left(2^{2R_s}-1\right)} \sum_{m=0}^{\theta_k - 1} \frac{\mu_2^m}{\mu_1^{m+1}} \sum_{v=0}^{m} \frac{\mu_1^v}{v!} \sum_{p=0}^{v} \binom{v}{p} \left(2^{2R_s} - 1\right)^{v-p} 2^{2pR_s} p! \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-p-1} \right]
\end{aligned} \tag{24}
$$

B. Secrecy Outage Probability

The secrecy outage probability is defined as the probability of the secrecy capacity C_{S} being lower than a predetermined threshold R_s. That is,

$$
\begin{aligned}
P_{\mathrm{out}}\left(R_s\right) &= \Pr\left(C_{\mathrm{S}} < R_s\right)\\
&= \int_0^\infty \int_0^{2^{2R_s}(1+y)-1} f_{\gamma_{\mathrm{B}}}\left(x\right) f_{\gamma_{\mathrm{E}}}\left(y\right) dx dy.
\end{aligned} \tag{23}
$$

In the following, we pursue a detailed analysis of the secrecy outage probability for the proposed schemes.

1) ZF/MRC: The secrecy outage probability of dual-hop AF relaying systems with the ZF/MRC scheme is lower bounded by (24), where $\mu_1 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_2}$.

Proof: The proof is provided in the journal version of this work [17]. ■

Having obtained the lower bound on the secrecy outage probability of the ZF/MRC scheme, now, we turn our attention to the asymptotic analysis in the high SNR regime. Without loss of generality, we assume that $\overline{\gamma}_1 \to \infty$, $\overline{\gamma}_2 = \kappa\overline{\gamma}_1$, and $\overline{\gamma}_0 = \mu\overline{\gamma}_1$.

Corollary 1. *In the high SNR regime, the secrecy outage probability of the dual-hop AF relaying with ZF/MRC is given by*

$$
\begin{aligned}
&P_{\mathrm{out,ZF/MRC}}^{\infty}\left(R_s\right)\\
&= \left(\Psi_{\mathrm{ZF/MRC}}\overline{\gamma}_1\right)^{-\Phi_{\mathrm{ZF/MRC}}} + o\left(\overline{\gamma}_1^{-\Phi_{\mathrm{ZF/MRC}}}\right),
\end{aligned} \tag{25}
$$

where $o\left(\cdot\right)$ denotes higher order terms, the achievable secrecy diversity order is $\Phi_{\mathrm{ZF/MRC}} = M$, and the the secrecy coding gain is

$$
\Psi_{\mathrm{ZF/MRC}} = \left[\sum_{n=0}^{M} \binom{M}{n} \frac{\left(2^{2R_s} - 1\right)^{M-n} \left(2^{2R_s}\overline{\gamma}_4\right)^n n!}{\mu\kappa^{M-1}\Gamma\left(M+1\right)}\right]^{-\frac{1}{M}}. \tag{26}
$$

Proof: The proof is provided in the journal version of this work [17]. ■

2) MRT/MRC: The secrecy outage probability of dual-hop AF relaying system with the MRT/MRC scheme can be approximated as (27), where $\eta_v = M + v$ and $\mu_3 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_3}$.

Proof: By inserting (21) and (22) into (23), and utilizing [16, Eq. (8.352.1)] and [16, Eq. (3.351.3)], the desired result can be obtained after some simple mathematical manipulations. ■

Corollary 2. *In the high SNR regime, the asymptotic secrecy outage probability of dual-hop AF relaying systems with MRT/MRC is expressed as*

$$
\begin{aligned}
&P_{\mathrm{out,MRT/MRC}}^{\infty}\left(R_s\right)\\
&= \left(\Psi_{\mathrm{MRT/MRC}}\overline{\gamma}_1\right)^{-\Phi_{\mathrm{MRT/MRC}}} + o\left(\overline{\gamma}_1^{-\Phi_{\mathrm{MRT/MRC}}}\right),
\end{aligned} \tag{28}
$$

where the secrecy diversity order is $\Phi_{\mathrm{MRT/MRC}} = 1$, and the secrecy coding gain is given as (29)*.*

Proof: Due to the space limit, we omit the proof here and kindly ask the readers to refer to the journal version of this paper for the details [17]. ■

IV. Numerical Results

In this section, representative numerical results are provided to verify our analysis in the previous sections. Unless otherwise specify, the following parameters are set: $\overline{\gamma}_0 = 0.4\overline{\gamma}_1$, $\overline{\gamma}_2 = 1.2\overline{\gamma}_1$, and $R_s = 2$.

Figs. 2 and 3 show the secrecy outage probability of the dual-hop AF relaying wiretap channel with the ZF/MRC and MRT/MRC schemes for different M. As illustrated, the analytical results keep sufficiently tight across the entire SNR range of interest, which demonstrates the correctness of the derived approximative results. Moreover, we observe that increasing M can significantly reduce the secrecy outage probability of the considered system for both schemes. This is intuitive since increasing M provides additional secrecy diversity, as manifested through the asymptotic curves.

Fig. 4 investigates the impact of the quality of the eavesdropper channel on the secrecy outage probability of the dual-hop AF relaying system with the proposed schemes. As expected, the secrecy outage performance of all the proposed schemes improves when the quality of eavesdropper's channel is degraded, i.e., small $\overline{\gamma}_3$ or $\overline{\gamma}_4$. However, higher secrecy diversity order of MRT scheme does not necessarily implies superior outage performance in the finite SNR regime. As shown in the figure, the ZF/MRC scheme outperforms the MRT/MRC scheme at the low SNR regime, while the opposite holds in the high SNR regime. In addition, when the quality

$$\begin{aligned} P_{\mathrm{out,MRT/MRC}}\left(R_s\right) \approx{}& \frac{1}{\Gamma\left(M\right)} \sum_{v=0}^{M-1} \frac{\Gamma\left(\eta_v\right)}{\Gamma\left(v+1\right)} \left(\frac{1}{\overline{\gamma}_1^{v}\overline{\gamma}_2^{M}} + \frac{1}{\overline{\gamma}_1^{M}\overline{\gamma}_2^{v}}\right) \Bigg\{ \frac{1}{\mu_1^{\eta_v}} - \frac{1}{\mu_2^{\eta_v}} e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \Bigg[\left(\frac{1}{\mu_4^{M}\overline{\gamma}_1^{M}} + \frac{1}{\overline{\gamma}_3} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k}\overline{\gamma}_1^{k}} \right) \\ & \times \left(1+\frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} - \frac{1}{\mu_4^{M}\overline{\gamma}_1^{M}\overline{\gamma}_4} \sum_{m=0}^{M-1} \mu_4^{m} \left(\mu_3 + \frac{2^{2R_s}}{\overline{\gamma}_0}\right)^{-m-1} - \frac{1}{\overline{\gamma}_3\overline{\gamma}_4} \sum_{k=0}^{M-1} \sum_{m=0}^{\phi_k-1} \frac{\mu_4^{m}}{\mu_4^{\phi_k}\overline{\gamma}_1^{k}} \left(\mu_3 + \frac{2^{2R_s}}{\overline{\gamma}_0}\right)^{-m-1} \Bigg] \\ & - \frac{1}{\overline{\gamma}_4} e^{-\mu_1\left(2^{2R_s}-1\right)} \sum_{p=0}^{\eta_v-1} \frac{\left(\mu_1^{p-\eta_v} - \mu_2^{p-\eta_v}\right)}{\Gamma\left(p+1\right)} \sum_{n=0}^{p} \binom{p}{n} \left(2^{2R_s}-1\right)^{p-n} 2^{2nR_s} \Bigg[n! \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-n-1} \Bigg(\frac{1}{\mu_4^{M}\overline{\gamma}_1^{M}} \\ & + \frac{1}{\overline{\gamma}_3} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k}\overline{\gamma}_1^{k}} \Bigg) - \frac{1}{\mu_4^{M}\overline{\gamma}_1^{M}} \sum_{m=0}^{M-1} \frac{(m+n)!\mu_4^{m}}{m!(\mu_1 2^{2R_s}+\mu_3)^{m+n+1}} - \frac{1}{\overline{\gamma}_3} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k}\overline{\gamma}_1^{k}} \sum_{m=0}^{\phi_k-1} \frac{(m+n)!\mu_4^{m}}{m!(\mu_1 2^{2R_s}+\mu_3)^{m+n+1}} \Bigg] \Bigg\} \end{aligned} \tag{27}$$

$$\Psi_{\mathrm{MRT/MRC}} = \begin{cases} \left[\frac{1}{\mu}\left(1+\frac{1}{\kappa^M}\right) \sum\limits_{n=0}^{M+1} \binom{M+1}{n} \frac{(n+1)!}{(M+1)!} \left(2^{2R_s}-1\right)^{M+1-n} \left(2^{2R_s}\overline{\gamma}_4\right)^{n}\right]^{-\frac{1}{M+1}}, & \overline{\gamma}_3 = \overline{\gamma}_4 \\ \left[\frac{1}{\mu}\left(1+\frac{1}{\kappa^M}\right) \sum\limits_{n=0}^{M+1} \binom{M+1}{n} \frac{n!2^{2nR_s}\overline{\gamma}_3}{(M+1)!(\overline{\gamma}_3-\overline{\gamma}_4)} \left(2^{2R_s}-1\right)^{M+1-n} \left(\overline{\gamma}_3^{n+1} - \overline{\gamma}_4^{n+1}\right)\right]^{-\frac{1}{M+1}}, & \overline{\gamma}_3 \neq \overline{\gamma}_4 \end{cases} \tag{29}$$

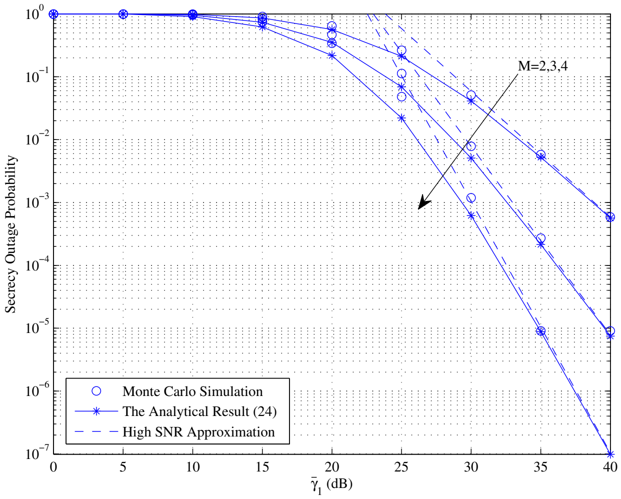

Fig. 2. Secrecy outage probability of the ZF/MRC relaying system with $\overline{\gamma}_4 = 10\mathrm{dB}$ and different relay antennas M.

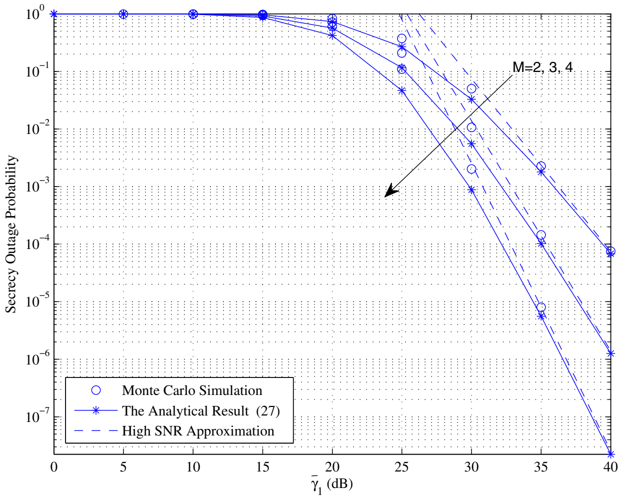

Fig. 3. Secrecy outage probability of the MRT/MRC relaying system with $\overline{\gamma}_3 = \overline{\gamma}_4 = 10\mathrm{dB}$ and different relay antennas M.

of eavesdropper's channel becomes good, i.e., large $\overline{\gamma}_3$ or $\overline{\gamma}_4$, the difference performance gap between the ZF/MRC scheme and the MRT/MRC scheme is reduced.

V. Conclusions

In this paper, we have investigated the secrecy performance of dual-hop AF relaying systems by taking into account the availability of direct link over Rayleigh fading channels. Specifically, two linear processing schemes at relay, i.e., ZF and MRT, were proposed to enhance the security of the considered system. For the two proposed schemes, we have derived the approximate secrecy outage probability, and presented an asymptotic secrecy outage analysis in the high SNR regime. Moreover, our finding suggests that the ZF/MRC scheme outperforms the MRT/MRC scheme in the low SNR regime, while the opposite holds in the high SNR regime.

Appendix A
Proof of Lemma 1

Define $\gamma_{\mathrm{z}} = \min\left(\gamma_1, \gamma_2\right)$, then, using the fact that γ_1 and γ_2 are independent random variables, we have

$$F_{\gamma_{\mathrm{z}}}\left(x\right) = F_{\gamma_1}\left(x\right) + F_{\gamma_2}\left(x\right) - F_{\gamma_1}\left(x\right) F_{\gamma_2}\left(x\right). \tag{30}$$

Noticing that γ_1 is a chi squared RV with $2M$ degrees of freedom (d.o.f.), its CDF is given by

$$F_{\gamma_1}\left(x\right) = 1 - e^{-\frac{x}{\overline{\gamma}_1}} \sum_{k=0}^{M-1} \frac{1}{k!} \left(\frac{x}{\overline{\gamma}_1}\right)^{k}. \tag{31}$$

In addition, based on [18], γ_2 is also a chi squared RV with $2\left(M-1\right)$ d.o.f. with CDF given by

$$F_{\gamma_2}\left(x\right) = 1 - e^{-\frac{x}{\overline{\gamma}_2}} \sum_{k=0}^{M-2} \frac{1}{k!} \left(\frac{x}{\overline{\gamma}_2}\right)^{k}. \tag{32}$$

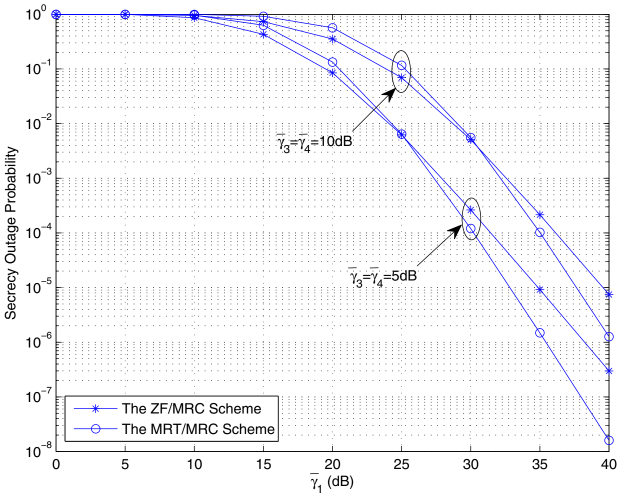

Fig. 4. Secrecy outage probability of ZF/MRC and MRT/MRC schemes with $M = 3$ and different $\overline{\gamma}_3$ and $\overline{\gamma}_4$.

Then, substituting (31) and (32) into (30) and performing some simple mathematical manipulations, the CDF of γ_z is given by

$$F_{\gamma_z}(x) = \frac{1}{\overline{\gamma}_1^M \Gamma(M)} \sum_{k=0}^{M-2} \frac{\Upsilon(\eta_k, \mu_1 x)}{k! \mu_1^{\eta_k} \overline{\gamma}_2^k} + \frac{1}{\overline{\gamma}_2^{M-1} \Gamma(M-1)} \sum_{k=0}^{M-1} \frac{\Upsilon(\theta_k, \mu_1 x)}{k! \mu_1^{\theta_k} \overline{\gamma}_1^k}. \qquad (33)$$

Taking the derivative of (33) with respect to x, the PDF of γ_z is derived as

$$f_{\gamma_z}(x) = \frac{1}{\overline{\gamma}_1^M} \frac{x^{M-1} e^{-\frac{x}{\overline{\gamma}_1}}}{\Gamma(M-1)\Gamma(M)} \Gamma\left(M-1, \frac{x}{\overline{\gamma}_2}\right) + \frac{1}{\overline{\gamma}_2^{M-1}} \frac{x^{M-2} e^{-\frac{x}{\overline{\gamma}_2}}}{\Gamma(M-1)\Gamma(M)} \Gamma\left(M, \frac{x}{\overline{\gamma}_1}\right). \qquad (34)$$

Due to the fact that γ_{AB} is an exponential RV, then according to (17), the Laplace transform of the PDF of $\gamma_{B_{ZF}}$ can be represented as

$$\mathcal{L}\left\{f_{\gamma_{B_{ZF}}}(x)\right\} \approx \frac{\mathcal{L}\{f_{\gamma_z}(x)\}}{\left(s + \frac{1}{\overline{\gamma}_0}\right)\overline{\gamma}_0}. \qquad (35)$$

By utilizing [19, Eq. (1.1.1.13)] to compute the inverse Laplace transform of (35), and solving the resultant integral by using [16, Eq. (3.351.1)], the desired PDF of $\gamma_{B_{ZF}}$ can be derived as (18).

Acknowledgment

This work was supported by the National Science Foundation of China (No. 61501507 and No. 61201229), Jiangsu Provincial Natural Science Foundation of China (No. BK20150719), Zhejiang Provincial Natural Science Foundation of China (No. LR15F010001), the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2013D06), by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, by the European Social Fund-ESF and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF)-Research Funding Program: THALES-NTUA MIMOSA.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, Oct. 1949.

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

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

[4] I. Csiszár and J. Körner, "Broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-part II: the MIMOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[6] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[7] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in correlated channel with maximal ratio combining diversity," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6745-6751, Dec. 2012.

[8] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959-2971, Aug. 2015.

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

[10] 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.

[11] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[12] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[13] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299-3310, Sep. 2014.

[14] F. S. Al-Qahtani, C. Zhong, and H. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756-1770, May 2015.

[15] Y. Huang, F. Al-Qahtani, C. Zhong, Q. Wu, J. Wang, and H. Alnuweiri, "Performance analysis of multiuser multiple antenna relaying networks with co-channel interference and feedback delay," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 59-73, Jan. 2014.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.

[17] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, Q. Wu, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," submitted for *IEEE Trans. Wireless Commun.*

[18] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359-368, Feb. 2012.

[19] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series*. New York: Gordon and Breach, 1992, vol. 5, Inverse Laplace Transforms.