Secure Transmission in Cooperative Relaying Networks with Multiple Antennas

Huang, Y., Wang, J., Zhong, C., Duong, T. Q., & Karagiannidis, G. K. (2016). Secure Transmission in Cooperative Relaying Networks with Multiple Antennas. IEEE Transactions on Wireless Communications. DOI: 10.1109/TWC.2016.2591940

Published in:
IEEE Transactions on Wireless Communications

Document Version:
Peer reviewed version

Secure Transmission in Cooperative Relaying Networks with Multiple Antennas

Yuzhen Huang, *Member*, *IEEE*, Jinlong Wang, *Senior Member*, *IEEE*, Caijun Zhong, *Senior Member*, *IEEE*, Trung Q. Duong, *Senior Member*, *IEEE*, and George K. Karagiannidis, *Fellow*, *IEEE*

***Abstract*—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. In order to exploit the available direct link and the multiple antennas for secrecy improvement, different linear processing schemes at the relay and different diversity combining techniques at the destination are proposed, namely, 1) Zero-forcing/Maximal ratio combining (ZF/MRC), 2) ZF/Selection combining (ZF/SC), 3) Maximal ratio transmission/MRC (MRT/MRC) and 4) MRT/Selection combining (MRT/SC). For all these schemes, we present new closed-form approximations for the secrecy outage probability. Moreover, we investigate a benchmark scheme, i.e., cooperative jamming/ZF (CJ/ZF), where the secrecy outage probability is obtained in exact closed-form. In addition, we present asymptotic secrecy outage expressions for all the proposed schemes in the high signal-to-noise ratio (SNR) regime, in order to characterize key design parameters, such as secrecy diversity order and secrecy array gain. The outcomes of this paper can be summarized as follows: a) MRT/MRC and MRT/SC achieve a full diversity order of $M+1$, ZF/MRC and ZF/SC achieve a diversity order of M, while CJ/ZF only achieves unit diversity order, where M is the number of antennas at the relay. b) ZF/MRC (ZF/SC) outperforms the corresponding MRT/MRC (MRT/SC) in the low SNR regime, while becomes inferior to the corresponding MRT/MRC (MRT/SC) in the high SNR. c) All of the proposed schemes tend to outperform the CJ/ZF with moderate number of antennas, and linear processing schemes with MRC attain better performance than those with SC.**

***Index Terms*—Relaying networks, amplify-and-forward, physical layer security, multiple antennas, secrecy performance.**

This work was supported by the National Science Foundation of China (No. 61501507, No. 61201229 and No. 61571463). 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). The work of T. Q. Duong was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22. The work of G. K. Karagiannidis was supported in part by 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: THALESNTUA MIMOSA. This paper was presented in part at the IEEE 83rd Vehicular Technology Conference (VTC2016-Spring), Nanjing, China, May 2016.

Y. Huang and J. Wang are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China (e-mail: yzh_huang@sina.com; wjl543@sina.com).

C. Zhong is with the Institute of Information and Communication Engineering, Zhejiang University, Hangzhou 310027, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210018, China (e-mail: caijunzhong@zju.edu.cn).

Trung Q. Duong is with Queen's University Belfast, Belfast BT7 1NN, UK (e-mail: trung.q.duong@qub.ac.uk).

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54 124, Thessaloniki, Greece (e-mail: geokarag@auth.gr).

I. Introduction

DUE to the broadcast nature of wireless transmission, wireless communications are inherently vulnerable to eavesdropping. The traditional ways of combating eavesdropping is to employ cryptographic schemes in the upper layers, which nevertheless has to deal with the problem of secret key distribution and management, in addition to the high complexity of data encryption and decryption processing [1]. Recently, the concept of physical layer security, first proposed in Shannon's pioneering work [2], has gained rekindled interests. In [3], the concept of wiretap channel was introduced, and the secrecy rate of a degraded wiretap channel was analyzed from the information-theoretic perspective. Since then, physical layer security has been widely investigated in various communication scenarios, for example, Gaussian wiretap channel [4] and relay-eavesdropper channel [5].

Recently, multiple antenna techniques, which provide extra spatial degrees of freedom, have been exploited to enhance the secrecy performance of wireless networks [6]–[11]. For example, in [6], the secrecy capacity of the Gaussian wiretap channel with multiple antennas was analyzed, by using generalized singular value decomposition and independent coding across the resultant parallel channels. In [7], transmit antenna selection (TAS) was proposed for secrecy enhancement for multiple-input multiple-output (MIMO) wiretap channels, with different receiver combining schemes. In [8] and [9], the impact of antenna correlation on the secrecy performance of multi-antenna wiretap channels was quantified. Furthermore, in [10], the authors mainly investigated the secrecy performance of the MIMO wiretap channel, by using TAS with receive generalized selection combining, over Nakagami-m fading channels. In [11], the ergodic secrecy sum-rate of a multiuser downlink system was analyzed, by using the regularized zero-forcing precoding based on imperfect channel estimation. Later, the authors in [12] and [13] investigated the secure transmission in multicell massive MIMO systems. In addition, in [14] and [15], the physical layer security of multi-antenna wiretap channels with wireless information and power transfer was investigated, respectively.

On the other hand, cooperative relaying techniques, which can improve the secrecy performance of wireless communications, have also received substantial interest [16]. In general, the relay node can either act as a conventional cooperative node to assist the transmission of the source or as a jammer by sending the interference signal, to confuse the eavesdroppers [17]–[19]. Specifically, in [20] and [21], the

authors proposed a cooperative jamming scheme to improve the security level against eavesdroppers. Later in [22]–[25], different cooperative schemes, such as decode-and-forward (DF) and amplify-and-forward (AF), were designed to enhance the security of dual-hop relaying networks. In [26] and [27], the authors investigated the secrecy performance of multiuser relaying networks, respectively. Specifically, in [26], three criteria to select the best relay and user pair were designed to improve the secure transmission, while in [27], a cooperative jamming was proposed to improve the security. Finally, a joint cooperative beamforming, jamming and power allocation scheme to enhance the security of AF relaying networks was proposed in [28].

Although these prior works have significantly improved the understanding of the secrecy performance of dual-hop relaying networks, the key limitation is that in all of them, the direct link between the transmitter and destination node was neglected, which may result in an underestimation of the secrecy performance. Only in a recent work [29], a single antenna DF relaying network with 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 this paper, we consider a more general multi-antenna dual-hop AF relaying system, taking into account the direct link between the source and destination node.

In order to exploit the extra degrees of freedom, provided by multiple antennas at the relay, we propose a heuristic two-stage relay processing scheme to enhance the security of a dual-hop relaying network. According to this scheme, the relay first uses maximal ratio combining (MRC) to maximize the signal to noise ratio (SNR) of the source-relay link, and then forwards the transformed signal to destination with simple linear processing methods, in an attempt to further improve the quality of main channel. To this end, two popular linear processing methods, i.e., 1) zero-forcing (ZF), and 2) maximal ratio transmission (MRT), will be investigated. Furthermore, since both the destination and eavesdropper receive two independent versions of the source message, diversity combining schemes can be applied. In this paper, we consider both MRC and selection combining (SC) at the destination, while, for the eavesdropper, we only consider the MRC scheme. Therefore, depending on the linear processing schemes adopted at the relay and destination, four secure transmission schemes will be investigated, namely, 1) ZF/MRC scheme, 2) ZF/SC scheme, 3) MRT/MRC scheme, and 4) MRT/SC scheme. In addition, as a benchmark, cooperative jamming with ZF scheme (CJ/ZF) is also analyzed, where the role of relay node is to send jamming signals to degrade the quality of the eavesdropper's channel.

The main contributions of this paper can be summarized as follows:

- For ZF/MRC and ZF/SC, we present novel closed-form lower and upper bounds for the secrecy outage probability and the probability of non-zero secrecy capacity, respectively, as well as a simple high SNR secrecy outage analysis. Furthermore, we show that ZF/MRC and ZF/SC achieve the same diversity order of M, where M is the number of antennas at the relay.

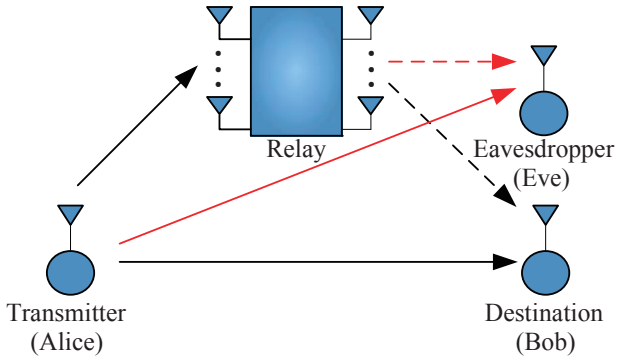


Fig. 1. System model for the relaying scheme.

- For MRT/MRC and MRT/SC, closed-form approximations for the secrecy outage probability and the probability of non-zero secrecy capacity are provided, respectively. In addition, we characterize the high SNR secrecy outage behavior, and show that both MRT/MRC and MRT/SC achieve a full diversity order of $M+1$.
- For the CJ/ZF scheme, new exact closed-form expressions for the secrecy outage probability and the probability of non-zero secrecy capacity are derived. Moreover, we characterize the high SNR secrecy outage behavior of the CJ/ZF scheme, which reveals that it achieves secrecy diversity order of one.
- The analytical results suggest that the ZF/MRC (MRT/MRC) scheme always achieves better performance than that of the corresponding ZF/SC (MRT/SC) scheme. In addition, the ZF/MRC (ZF/SC) scheme outperforms the corresponding MRT/MRC (MRT/SC) scheme in the low SNR regime, while in the high SNR regime, the MRT/MRC (MRT/SC) scheme attains better secrecy performance than the corresponding ZF/MRC (ZF/SC) scheme.
- The results demonstrate that all the proposed schemes tend to outperform the CJ/ZF scheme with moderate number of antennas, especially when the quality of eavesdropper's channel is bad. Moreover, increasing the number of antennas at the relay provides marginal performance gains for the CJ/ZF scheme, while it significantly enhances the secrecy performance of the proposed diversity schemes.

The rest of the paper is organized as follows. The system model is introduced in Section II. Section III formulates the problem and presents a set of new analytical expressions for the key secrecy performance. In Section IV, we provide numerical results and discussions. Finally, Section VI concludes the paper and summarizes our findings.

Notations: We use bold lower case letters to denote vectors and lower case letters to denote scalars, respectively. The probability density function (PDF) and the cumulative distribution function (CDF) of a random variable (RV) X are denoted as $f_X(\cdot)$ and $F_X(\cdot)$, respectively. The symbol $\|\cdot\|_F$ denotes the Frobenius norm, $\dagger$ denotes the conjugate transpose operator, $\mathrm{E}[\cdot]$ stands for the expectation operator, $n!$ denotes the factorial of integer n, and $\Gamma(x)$ is the Gamma function.

II. System Model

We consider a dual-hop multiple antenna AF relaying network as illustrated in Fig. 1, where both Alice (A), Bob (B), and Eve (E) are equipped with a single antenna, while the relay (R) is equipped with M antennas. We consider the realistic scenario where a direct link exists between A and B. Throughout this paper, the following assumptions are adopted: 1) A, R and B have perfect knowledge of the main channel fading information and E also has perfect knowledge of the eavesdropper's channel fading information[1], 2) The main channel and eavesdropper's channel are assumed to be quasi-static block fading channel with independent but non-identically distributed Rayleigh fading, such that the channel coefficients remain unchanged during the coherence time of the channel, 3) As in [29], [32], [33], we assume that the CSI of $\mathrm{R} \rightarrow \mathrm{E}$ link is available at R.

We assume a half-duplex relaying operation, as such, the entire communication between A and B consists of two phases. 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 $\frac{1}{n}\sum_{i=1}^{n} \mathrm{E}\left[|x(i)|^2\right] \leq P_s$, 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 $\mathrm{A} \rightarrow \mathrm{R}$ link with entries following identical and independently distributed (i.i.d.) Rayleigh fading with parameter λ_1, h_{AB} and h_{AE} denote the Rayleigh channel coefficients for the $\mathrm{A} \rightarrow \mathrm{B}$ and $\mathrm{A} \rightarrow \mathrm{E}$ 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. Thus, the instantaneous SNRs of $\mathrm{A} \rightarrow \mathrm{B}$ and $\mathrm{A} \rightarrow \mathrm{E}$ links are given, respectively, by

$$\gamma_{\mathrm{AB}} = \frac{P_s}{\sigma^2}|h_{\mathrm{AB}}|^2 \tag{4}$$

and

$$\gamma_{\mathrm{AE}} = \frac{P_s}{\sigma^2}|h_{\mathrm{AE}}|^2. \tag{5}$$

In the second phase[2], R retransmits a transformed version of $\mathbf{y}_{\mathrm{R}}(i)$ to B, and the signal at B is given by

$$y_{\mathrm{B},2}(i) = \mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{W}\mathbf{y}_{\mathrm{R}}(i) + n_{\mathrm{B},2}, \tag{6}$$

where $\mathbf{h}_{\mathrm{RB}}$ is an $M \times 1$ channel vector for the $\mathrm{R} \rightarrow \mathrm{B}$ link, and its entries follow i.i.d. Rayleigh fading with parameter λ_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. Hence, substituting (1) into (6) and performing some mathematical manipulations, the instantaneous SNR of $\mathrm{A} \rightarrow \mathrm{R} \rightarrow \mathrm{B}$ link is given by

$$\gamma_{\mathrm{ARB}} = \frac{P_s}{\sigma^2}\frac{\left|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{W}\mathbf{h}_{\mathrm{AR}}\right|^2}{1 + \left\|\mathbf{h}_{\mathrm{RB}}^{\dagger}\mathbf{W}\right\|_F^2}. \tag{7}$$

On the other hand, the received signal at E during the second phase can be expressed as

$$y_{\mathrm{E},2}(i) = \mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{W}\mathbf{y}_{\mathrm{R}}(i) + n_{\mathrm{E},2}, \tag{8}$$

where $\mathbf{h}_{\mathrm{RE}}$ is an $M \times 1$ channel vector for the $\mathrm{R} \rightarrow \mathrm{E}$ link, and its entries follow i.i.d. Rayleigh fading with parameter λ_3, and $n_{\mathrm{E},2}$ is the AWGN with variance σ^2. Similarly, the instantaneous SNR of $\mathrm{A} \rightarrow \mathrm{R} \rightarrow \mathrm{E}$ link can be derived as

$$\gamma_{\mathrm{ARE}} = \frac{P_s}{\sigma^2}\frac{\left|\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{W}\mathbf{h}_{\mathrm{AR}}\right|^2}{1 + \left\|\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{W}\right\|_F^2}. \tag{9}$$

Since both B and E have access to two independent copies of the source signal, several diversity combining schemes can be applied to strengthen the signal detection. Without loss of generality, we assume that two popular diversity combining schemes, i.e., MRC and SC, are adopted at B, while Eve always adopts MRC scheme[3]. Therefore, according to (4) and (7), the instantaneous SNRs of the main channel under MRC and SC schemes are given by

$$\gamma_{\mathrm{B}_{\mathrm{MRC}}} = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{ARB}} \tag{10}$$

and

$$\gamma_{\mathrm{B}_{\mathrm{SC}}} = \max\left(\gamma_{\mathrm{AB}}, \gamma_{\mathrm{ARB}}\right). \tag{11}$$

Similarly, the instantaneous SNR of the eavesdropper's channel under MRC scheme is represented as

$$\gamma_{\mathrm{E}_{\mathrm{MRC}}} = \gamma_{\mathrm{AE}} + \gamma_{\mathrm{ARE}}. \tag{12}$$

Now, according to [29], [32], [33], the achievable secrecy capacity of the relaying wiretap channels is defined as

$$C_{\mathrm{S}} \triangleq \frac{1}{2}[\log_2(1 + \gamma_{\mathrm{B}_i}) - \log(1 + \gamma_{\mathrm{E}_{\mathrm{MRC}}})]^+, \tag{13}$$

where $i \in \{\mathrm{MRC}, \mathrm{SC}\}$, the factor 1/2 accounts for the fact that the total communication consists of two time slots, and

$$[x]^+ = \max(x, 0) = \begin{cases} x, & x \geq 0 \\ 0, & x < 0 \end{cases} \tag{14}$$

Note that, due to the non-convex nature of the problem, the optimal transform matrix $\mathbf{W}$, which maximizes the achievable secrecy capacity of relaying wiretap channels, does not seem to be analytically tractable. To tackle with this problem, we

[1]In practice, the channel state information (CSI) of the main link can be obtained at A, R and B by the classic channel training, estimation, and feedback mechanisms as in [30], [31]. Similarly, the CSI of eavesdropper's link can also be achieved at Eve by traditional channel estimations.

[2]To capture the effect of linear processing schemes on the secrecy performance, in this paper, we assume that Alice remains silent in the second phase. However, it is worth mentioning that, with proper design, the secrecy performance could be further improved if Alice acts as a jammer in the second phase as shown in [18], [19].

[3]Here, we only assume that the MRC scheme is adopted at Eve. However, for the case of SC, similar analysis can be applied.

propose a heuristic two-stage relay processing strategy, i.e., the relay first uses the MRC scheme to maximize the SNR of the A $\rightarrow$ R link, and then delivers the transformed signal to B with linear processing methods to enhance the quality of the main channel. Hence, the heuristic relay precoder $\mathbf{W}$ is a rank-one 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 $\rightarrow$ R link, and $\mathbf{w}_2$ is an $M \times 1$ linear processing vector, which depends on the linear processing scheme employed by the relay. Specifically, here we consider two different linear processing schemes, namely, the ZF scheme and the MRT scheme as detailed below.

A. Zero Forcing (ZF)

The objective of ZF scheme is to maximize the received SNR at B, while avoiding the leakage of confidential information to E. According to the ZF principle, the optimal $\mathbf{w}_2$ is the solution of the following optimization problem:

$$\begin{aligned} &\max_{\mathbf{w}_2} \left| \mathbf{h}_{\mathrm{RB}}^{\dagger} \mathbf{w}_2 \right| \\ &s.t. \ \left| \mathbf{h}_{\mathrm{RE}}^{\dagger} \mathbf{w}_2 \right| = 0, \ \& \ \|\mathbf{w}_2\|_F = 1. \end{aligned} \tag{15}$$

By using projection matrix theory [34], the weight vector $\mathbf{w}_2$ is given by

$$\mathbf{w}_2 = \frac{\mathbf{\Xi}^{\perp} \mathbf{h}_{\mathrm{RB}}}{\|\mathbf{\Xi}^{\perp} \mathbf{h}_{\mathrm{RB}}\|_F}, \tag{16}$$

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

$$\alpha^2 = \frac{P_r}{\mathbf{h}_{\mathrm{AR}}^{\dagger} \mathbf{h}_{\mathrm{AR}} P_s + \sigma^2}. \tag{17}$$

Thus, the instantaneous SNRs of the main channel with MRC and SC schemes can be expressed as

$$\gamma_{\mathrm{B}_{\mathrm{MRC}}}^{\mathrm{ZF}} = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{ARB}}^{\mathrm{ZF}} \tag{18}$$

and

$$\gamma_{\mathrm{B}_{\mathrm{SC}}}^{\mathrm{ZF}} = \max\left(\gamma_{\mathrm{AB}}, \gamma_{\mathrm{ARB}}^{\mathrm{ZF}}\right), \tag{19}$$

where

$$\gamma_{\mathrm{ARB}}^{\mathrm{ZF}} = \frac{\frac{P_s}{\sigma^2} \|\mathbf{h}_{\mathrm{AR}}\|_F^2 \frac{P_r}{\sigma^2} \left\|\mathbf{\Xi}^{\perp} \mathbf{h}_{\mathrm{RB}}\right\|_F^2}{\frac{P_s}{\sigma^2} \|\mathbf{h}_{\mathrm{AR}}\|_F^2 + \frac{P_r}{\sigma^2} \|\mathbf{\Xi}^{\perp} \mathbf{h}_{\mathrm{RB}}\|_F^2 + 1}. \tag{20}$$

As a result, the instantaneous SNR of the eavesdropper's channel reduces to

$$\gamma_{\mathrm{E}_{\mathrm{MRC}}}^{\mathrm{ZF}} = \gamma_{\mathrm{AE}}. \tag{21}$$

B. Maximal ratio transmission (MRT)

According to MRT scheme, $\mathbf{w}_2$ is set to match the second hop of the main channel, i.e., $\mathbf{w}_2 = \frac{\mathbf{h}_{\mathrm{RB}}^{\dagger}}{\|\mathbf{h}_{\mathrm{RB}}\|_F}$. Therefore, the instantaneous SNRs of the main channel with MRC and SC schemes are expressed respectively as

$$\gamma_{\mathrm{B}_{\mathrm{MRC}}}^{\mathrm{MRT}} = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{ARB}}^{\mathrm{MRT}} \tag{22}$$

and

$$\gamma_{\mathrm{B}_{\mathrm{SC}}}^{\mathrm{MRT}} = \max\left(\gamma_{\mathrm{AB}}, \gamma_{\mathrm{ARB}}^{\mathrm{MRT}}\right), \tag{23}$$

where

$$\gamma_{\mathrm{ARB}}^{\mathrm{MRT}} = \frac{\frac{P_s}{\sigma^2} \|\mathbf{h}_{\mathrm{AR}}\|_F^2 \frac{P_r}{\sigma^2} \|\mathbf{h}_{\mathrm{RB}}\|_F^2}{\frac{P_s}{\sigma^2} \|\mathbf{h}_{\mathrm{AR}}\|_F^2 + \frac{P_r}{\sigma^2} \|\mathbf{h}_{\mathrm{RB}}\|_F^2 + 1}. \tag{24}$$

Similarly, the instantaneous SNR of the eavesdropper's channel with MRC scheme is given by

$$\gamma_{\mathrm{E}_{\mathrm{MRC}}}^{\mathrm{MRT}} = \gamma_{\mathrm{AE}} + \gamma_{\mathrm{ARE}}^{\mathrm{MRT}}, \tag{25}$$

where

$$\gamma_{\mathrm{ARE}}^{\mathrm{MRT}} = \frac{\frac{P_s}{\sigma^2} \|\mathbf{h}_{\mathrm{AR}}\|_F^2 \frac{P_r}{\sigma^2} \frac{\left|\mathbf{h}_{\mathrm{RB}}^{\dagger} \mathbf{h}_{\mathrm{RE}}\right|}{\|\mathbf{h}_{\mathrm{RB}}\|_F^2}}{\frac{P_s}{\sigma^2} \|\mathbf{h}_{\mathrm{AR}}\|_F^2 + \frac{P_r}{\sigma^2} \frac{\left|\mathbf{h}_{\mathrm{RB}}^{\dagger} \mathbf{h}_{\mathrm{RE}}\right|}{\|\mathbf{h}_{\mathrm{RB}}\|_F^2} + 1}. \tag{26}$$

III. Secrecy Performance Analysis

In this section, we investigate the secrecy performance of dual-hop AF multi-antenna relaying systems in terms of secrecy outage probability and probability of non-zero secrecy capacity. The derived results will enable us to examine the benefits of the proposed schemes.

A. Preliminaries

We start by presenting the probability density function (PDF) and cumulative distribution function (CDF) of the SNRs of the main and the eavesdropper's channels, which will facilitate the ensuing secrecy analysis.

1) ZF/MRC: Although the statistics of γ_{AB} and $\gamma_{\mathrm{ARB}}^{\mathrm{ZF}}$ are known [35], deriving the exact distribution of $\gamma_{\mathrm{B}_{\mathrm{MRC}}}^{\mathrm{ZF}}$ is intractable. Hence, according to [36]–[38], we first seek the tight upper bound on $\gamma_{\mathrm{ARB}}^{\mathrm{ZF}}$, i.e., $\gamma_{\mathrm{ARB}}^{\mathrm{ZF}} \leq \min\left(\gamma_1, \gamma_{2z}\right)$, where $\gamma_1 = \frac{P_s}{\sigma^2} \|\mathbf{h}_{\mathrm{AR}}\|_F^2$ and $\gamma_{2z} = \frac{P_r}{\sigma^2} \left\|\mathbf{\Xi}^{\perp} \mathbf{h}_{\mathrm{RB}}\right\|_F^2$. Thus, we have

$$\gamma_{\mathrm{B}_{\mathrm{MRC}}}^{\mathrm{ZF}} \leq \gamma_{\mathrm{B}_{\mathrm{MRC}}}^{\mathrm{ZFU}} = \gamma_{\mathrm{AB}} + \min\left(\gamma_1, \gamma_{2z}\right). \tag{27}$$

Next, we present the CDF of $\gamma_{\mathrm{B}_{\mathrm{MRC}}}^{\mathrm{ZFU}}$ in the following lemma[4].

[4]Let us remark that the CDF of $\gamma_{\mathrm{B}_{\mathrm{MRC}}}^{\mathrm{ZFU}}$ is derived with the assumption of $\mu_2 \neq 0$ in Lemma 1. Due to the space limitation, we neglect the detail analysis of the special case $\mu_2 = 0$, however, which can be easily obtained in a similar manner as in the case of $\mu_2 \neq 0$.

Lemma 1. *The CDF of* $\gamma_{\mathrm{B_{MRC}}}^{\mathrm{ZFU}}$ *is given by*

$$F_{\gamma_{\mathrm{B_{MRC}}}^{\mathrm{ZFU}}}(x) = \frac{1}{\overline{\gamma}_1^M \Gamma(M)} \sum_{k=0}^{M-2} \frac{\Gamma(\eta_k)}{k! \mu_2^{\eta_k} \overline{\gamma}_2^k} \times \left[1 - e^{-\frac{x}{\overline{\gamma}_0}} - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\eta_k - 1} \frac{\Upsilon(m+1, \mu_1 x)}{m! \mu_2^{-m} \mu_1^{m+1}}\right] + \frac{1}{\overline{\gamma}_2^{M-1} \Gamma(M-1)} \sum_{k=0}^{M-1} \frac{\Gamma(\theta_k)}{k! \mu_2^{\theta_k} \overline{\gamma}_1^k} \times \left[1 - e^{-\frac{x}{\overline{\gamma}_0}} - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\theta_k - 1} \frac{\Upsilon(m+1, \mu_1 x)}{m! \mu_2^{-m} \mu_1^{m+1}}\right], \quad (28)$$

where $\mu_1 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_2}$, $\mu_2 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_2} - \frac{1}{\overline{\gamma}_0}$, $\eta_k = M + k$, $\theta_k = M + k - 1$, $\overline{\gamma}_0 = \mathrm{E}[\gamma_{\mathrm{AB}}]$, $\overline{\gamma}_1 = \mathrm{E}[\gamma_1]$, $\overline{\gamma}_2 = \mathrm{E}[\gamma_{2z}]$, *and* $\Upsilon(\cdot,\cdot)$ *is the lower incomplete Gamma function [39, Eq. (8.350.1)].*

Proof: See Appendix A. ∎

2) ZF/SC: For the ZF/SC scheme, the exact distribution of $\gamma_{\mathrm{B_{SC}}}^{\mathrm{ZF}}$ can actually be obtained. However, to simplify the analysis, we also resort to the upper bound approach, i.e.,

$$\gamma_{\mathrm{B_{SC}}}^{\mathrm{ZF}} \le \gamma_{\mathrm{B_{SC}}}^{\mathrm{ZFU}} = \max(\gamma_{\mathrm{AB}}, \min(\gamma_1, \gamma_{2z})). \quad (29)$$

As such, we have the following key lemma:

Lemma 2. *The CDF of* $\gamma_{\mathrm{B_{SC}}}^{\mathrm{ZFU}}$ *can be expressed as*

$$F_{\gamma_{\mathrm{B_{SC}}}^{\mathrm{ZFU}}}(x) = \frac{1}{\overline{\gamma}_1^M \Gamma(M)} \left(1 - e^{-\frac{x}{\overline{\gamma}_0}}\right) \sum_{k=0}^{M-2} \frac{\Upsilon(\eta_k, \mu_1 x)}{k! \mu_1^{\eta_k} \overline{\gamma}_2^k} + \frac{1}{\overline{\gamma}_2^{M-1} \Gamma(M-1)} \left(1 - e^{-\frac{x}{\overline{\gamma}_0}}\right) \sum_{k=0}^{M-1} \frac{\Upsilon(\theta_k, \mu_1 x)}{k! \mu_1^{\theta_k} \overline{\gamma}_1^k}. \quad (30)$$

Proof: Due to the independence of γ_{AB}, γ_1 and γ_{2z}, the CDF of $\gamma_{\mathrm{B_{SC}}}^{\mathrm{ZFU}}$ can be derived as

$$F_{\gamma_{\mathrm{B_{SC}}}^{\mathrm{ZFU}}}(x) = F_{\gamma_{\mathrm{AB}}}(x) F_{\gamma_{\mathrm{Z}}}(x), \quad (31)$$

where $\gamma_{\mathrm{Z}} = \min(\gamma_1, \gamma_{2z})$. Then, substituting the CDFs of γ_{AB} and γ_{Z} (refer to (69) in Appendix A) into (31) yields the desired result. ∎

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

$$\gamma_{\mathrm{B_{MRC}}}^{\mathrm{MRT}} \le \gamma_{\mathrm{B_{MRC}}}^{\mathrm{MRTU}} = \gamma_{\mathrm{AB}} + \min(\gamma_1, \gamma_{2m}) \quad (32)$$

and

$$\gamma_{\mathrm{E_{MRC}}}^{\mathrm{MRT}} \le \gamma_{\mathrm{E_{MRC}}}^{\mathrm{MRTU}} = \gamma_{\mathrm{AE}} + \min(\gamma_1, \gamma_3), \quad (33)$$

where $\gamma_{2m} = \frac{P_r}{\sigma^2} \|\mathbf{h}_{\mathrm{RB}}\|_F^2$ and $\gamma_3 = \frac{P_r}{\sigma^2} \frac{|\mathbf{h}_{\mathrm{RB}}^\dagger \mathbf{h}_{\mathrm{RE}}|^2}{\|\mathbf{h}_{\mathrm{RB}}\|_F^2}$.

Now, we present the CDF of $\gamma_{\mathrm{B_{MRC}}}^{\mathrm{MRTU}}$ and the PDF of $\gamma_{\mathrm{E_{MRC}}}^{\mathrm{MRTU}}$ in the following lemmas.

Lemma 3. *The CDF of* $\gamma_{\mathrm{B_{MRC}}}^{\mathrm{MRTU}}$ *is given by*

$$F_{\gamma_{\mathrm{B_{MRC}}}^{\mathrm{MRTU}}}(x) = \frac{1}{\overline{\gamma}_1^M \Gamma(M)} \sum_{k=0}^{M-1} \frac{\Gamma(\eta_k)}{k! \mu_2^{\eta_k} \overline{\gamma}_2^k} \times \left[1 - e^{-\frac{x}{\overline{\gamma}_0}} - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\eta_k - 1} \frac{\mu_2^m \Upsilon(m+1, \mu_1 x)}{m! \mu_1^{m+1}}\right] + \frac{1}{\overline{\gamma}_2^M \Gamma(M)} \sum_{k=0}^{M-1} \frac{\Gamma(\eta_k)}{k! \mu_2^{\eta_k} \overline{\gamma}_1^k} \times \left[1 - e^{-\frac{x}{\overline{\gamma}_0}} - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\eta_k - 1} \frac{\mu_2^m \Upsilon(m+1, \mu_1 x)}{m! \mu_1^{m+1}}\right]. \quad (34)$$

Proof: Noticing that γ_{2m} follows the Chi-square distribution with $2M$ degrees of freedom, the desired CDF of $\gamma_{\mathrm{B_{MRC}}}^{\mathrm{MRTU}}$ can be obtained by following similar procedure as in the proof of Lemma 1. ∎

Lemma 4. *The PDF of* $\gamma_{\mathrm{E_{MRC}}}^{\mathrm{MRTU}}$ *can be expressed as*

$$f_{\gamma_{\mathrm{E_{MRC}}}^{\mathrm{MRTU}}}(x) = \frac{e^{-\frac{x}{\overline{\gamma}_4}}}{\overline{\gamma}_4} \left[\frac{\Upsilon(M, \mu_4 x)}{\overline{\gamma}_1^M \Gamma(M) \mu_4^M} + \sum_{k=0}^{M-1} \frac{\Upsilon(\phi_k, \mu_4 x)}{k! \mu_4^{\phi_k} \overline{\gamma}_1^k \overline{\gamma}_3}\right], \quad (35)$$

where $\phi_k = k + 1$, $\mu_4 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_3} - \frac{1}{\overline{\gamma}_4}$, $\overline{\gamma}_3 = \mathrm{E}[\gamma_3]$, *and* $\overline{\gamma}_4 = \mathrm{E}[\gamma_{\mathrm{AE}}]$.

Proof: Since γ_3 follows the exponential distribution [38], thus, by following the similar analysis as in Lemma 1, the desired expression can be easily obtained after some mathematical manipulations[5]. ∎

4) MRT/SC: Similarly, $\gamma_{\mathrm{B_{SC}}}^{\mathrm{MRT}}$ can be upper bounded by

$$\gamma_{\mathrm{B_{SC}}}^{\mathrm{MRT}} \le \gamma_{\mathrm{B_{SC}}}^{\mathrm{MRTU}} = \max(\gamma_{\mathrm{AB}}, \min(\gamma_1, \gamma_{2m})). \quad (36)$$

As such, we have the following result.

Lemma 5. *The CDF of* $\gamma_{\mathrm{B_{SC}}}^{\mathrm{MRTU}}$ *can be expressed as*

$$F_{\gamma_{\mathrm{B_{SC}}}^{\mathrm{MRTU}}}(x) = \frac{1}{\overline{\gamma}_1^M \Gamma(M)} \left(1 - e^{-\frac{x}{\overline{\gamma}_0}}\right) \sum_{k=0}^{M-1} \frac{\Upsilon(\eta_k, \mu_1 x)}{k! \mu_1^{\eta_k} \overline{\gamma}_2^k} + \frac{1}{\overline{\gamma}_2^M \Gamma(M)} \left(1 - e^{-\frac{x}{\overline{\gamma}_0}}\right) \sum_{k=0}^{M-1} \frac{\Upsilon(\eta_k, \mu_1 x)}{k! \mu_1^{\eta_k} \overline{\gamma}_1^k}. \quad (37)$$

Proof: Similarly, as in the proof of Lemma 2, the above result can be easily obtained after some simple mathematical manipulations. ∎

B. Secrecy Outage Probability

The secrecy outage probability is defined as the probability of the achievable secrecy capacity, C_{S}, being lower than a predetermined secrecy rate, R_s. Mathematically, it can be represented as [1]

$$P_{\mathrm{out}}(R_s) = \Pr(C_{\mathrm{S}} < R_s) = \int_0^\infty F_{\gamma_{\mathrm{B}_i}}\left(2^{2R_s}(1+x) - 1\right) f_{\gamma_{\mathrm{E_{MRC}}}}(x)\, dx. \quad (38)$$

[5]In Lemma 4, we assume $\mu_4 \neq 0$ to derive the PDF of $\gamma_{\mathrm{E_{MRC}}}^{\mathrm{MRTU}}$. The special case $\mu_4 = 0$ is not considered in this paper, however, the PDF of which can be easily achieved by following similar steps of $\mu_4 \neq 0$.

$$P_{\text{out,ZF/MRC}}\left(R_s\right) \geq \frac{1}{\overline{\gamma}_1^M \Gamma\left(M\right)} \sum_{k=0}^{M-2} \frac{\Gamma\left(\eta_k\right)}{k! \mu_2^{\eta_k} \overline{\gamma}_2^k} \left[1 - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\eta_k-1} \frac{\mu_2^m}{\mu_1^{m+1}} - e^{-\frac{2^{2R}-1}{\overline{\gamma}_0}} \left(1 + \frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} \right.$$
$$\left. + \frac{1}{\overline{\gamma}_4 \overline{\gamma}_0} e^{-\mu_1\left(2^{2R_s}-1\right)} \sum_{m=0}^{\eta_k-1} \frac{\mu_2^m}{\mu_1^{m+1}} \sum_{v=0}^{m} \frac{\mu_1^v}{v!} \sum_{p=0}^{v} \binom{v}{p} \left(2^{2R_s}-1\right)^{v-p} 2^{2pR_s} p! \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-p-1} \right]$$
$$+ \frac{1}{\overline{\gamma}_2^{M-1} \Gamma\left(M-1\right)} \sum_{k=0}^{M-1} \frac{\Gamma\left(\theta_k\right)}{k! \mu_2^{\theta_k} \overline{\gamma}_1^k} \left[1 - \frac{1}{\overline{\gamma}_0} \sum_{m=0}^{\theta_k-1} \frac{\mu_2^m}{\mu_1^{m+1}} - e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \left(1 + \frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} \right.$$
$$\left. + \frac{1}{\overline{\gamma}_4 \overline{\gamma}_0} e^{-\mu_1\left(2^{2R_s}-1\right)} \sum_{m=0}^{\theta_k-1} \frac{\mu_2^m}{\mu_1^{m+1}} \sum_{v=0}^{m} \frac{\mu_1^v}{v!} \sum_{p=0}^{v} \binom{v}{p} \left(2^{2R_s}-1\right)^{v-p} 2^{2pR_s} p! \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-p-1} \right] \quad (39)$$

In the following, we present 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 (39) at the top of the page.

Proof: Using the following series representation of the incomplete Gamma function

$$\Upsilon\left(n, x\right) = \Gamma\left(n\right)\left(1 - e^{-x} \sum_{m=0}^{n-1} \frac{x^m}{m!}\right), \quad (40)$$

and noticing that $\gamma_{\text{E}_{\text{MRC}}}^{\text{ZF}}$ is an exponential RV, the lower bound of the secrecy outage probability for the ZF/MRC scheme can be obtained by substituting (28) into (38) and with the help of [39, Eq. (3.351.3)]. ■

While Eq. (39) provides an efficient way to evaluate the secrecy outage performance of dual-hop AF relaying systems with the ZF/MRC scheme, it cannot provide additional insights into the impact of system parameters on the network performance. Motivated by this, we turn our attention to the asymptotic secrecy outage probability 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 dual-hop AF relaying systems with the ZF/MRC scheme is given by*

$$P_{\text{out,ZF/MRC}}^{\infty}\left(R_s\right) = \left(\Psi_{\text{ZF/MRC}}\overline{\gamma}_1\right)^{-\Phi_{\text{ZF/MRC}}}, \quad (41)$$

where the secrecy coding gain is given by

$$\Psi_{\text{ZF/MRC}} = \left[\sum_{n=0}^{M} \binom{M}{n} \frac{\left(2^{2R_s}-1\right)^{M-n}\left(2^{2R_s}\overline{\gamma}_4\right)^n n!}{\mu\kappa^{M-1}\Gamma\left(M+1\right)}\right]^{-\frac{1}{M}}, \quad (42)$$

and the secrecy diversity gain is $\Phi_{\text{ZF/MRC}} = M$.

Proof: See Appendix B. ■

Remark: For the ZF/MRC scheme, the achievable secrecy diversity order of dual-hop AF relaying systems is M, which is independent of the parameters of the eavesdropper's channel. However, the parameters of the eavesdropper's channel affect the secrecy outage performance of dual-hop AF relaying systems through the secrecy coding gain $\Psi_{\text{ZF/MRC}}$.

2) ZF/SC: Following the same steps as in the ZF/MRC scheme, the secrecy outage probability of dual-hop AF relaying systems with the ZF/SC scheme is lower bounded by (43), where $\mu_5 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_2} + \frac{1}{\overline{\gamma}_0}$.

Next, we turn our attention to the asymptotic outage probability $P_{\text{out,ZF/SC}}^{\infty}\left(R_s\right)$, and we have the following corollary.

Corollary 2. *In the high SNR regime, the secrecy outage probability of dual-hop AF relaying systems with the ZF/SC scheme can be expressed as*

$$P_{\text{out,ZF/SC}}^{\infty}\left(R_s\right) = \left(\Psi_{\text{ZF/SC}}\overline{\gamma}_1\right)^{-\Phi_{\text{ZF/SC}}}, \quad (44)$$

where the secrecy coding gain is

$$\Psi_{\text{ZF/SC}} = \left[\sum_{n=0}^{M} \binom{M}{n} \frac{\left(2^{2R_s}-1\right)^{M-n}\left(2^{2R_s}\overline{\gamma}_4\right)^n n!}{\mu\kappa^{M-1}\Gamma\left(M\right)}\right]^{-\frac{1}{M}}, \quad (45)$$

and the secrecy diversity gain is $\Phi_{\text{ZF/SC}} = M$.

Proof: Following similar procedures as in Appendix B, the asymptotic CDF of $\gamma_{\text{B}_{\text{SC}}}^{\text{ZF}}$ is given by

$$F_{\gamma_{\text{B}_{\text{SC}}}^{\text{ZF}}}\left(x\right) \approx \left(\frac{1}{\overline{\gamma}_1}\right)^M \frac{x^M}{\mu\kappa^{M-1}\left(M-1\right)!}. \quad (46)$$

Substituting (46) into (38), and utilizing the equation [39, Eq. (3.351.3)], the desired result can be obtained. ■

Now, comparing with the asymptotic results of the ZF/MRC and ZF/SC schemes, we have the following remark:

Remark: The ZF/MRC and ZF/SC schemes achieve the same secrecy diversity order of M, which is independent of the eavesdropper's channel. However, the ZF/MRC scheme outperforms the ZF/SC scheme by achieving a higher coding gain, i.e.,

$$\frac{\Psi_{\text{ZF/MRC}}}{\Psi_{\text{ZF/SC}}} = M^{\frac{1}{M}}, \quad (47)$$

which suggests that to achieve the same secrecy outage probability, the required transmit power of the ZF/MRC scheme is $\frac{1}{M}10\log\left(M\right)\text{dB}$ less.

3) MRT/MRC: The secrecy outage probability of dual-hop AF relaying systems with the MRT/MRC scheme can be approximated as (48), where $\eta_v = M + v$ and $\mu_3 = \frac{1}{\overline{\gamma}_1} + \frac{1}{\overline{\gamma}_3}$.

Proof: By inserting (34) and (35) into (38), and utilizing [39, Eq. (8.352.1)] and [39, Eq. (3.351.3)], the desired result

$$P_{\text{out,ZF/SC}}\left(R_s\right) \geq \frac{1}{\overline{\gamma}_1^M \Gamma\left(M\right)} \sum_{k=0}^{M-2} \frac{\Gamma\left(\eta_k\right)}{k! \mu_1^{\eta_k} \overline{\gamma}_2^k} \left\{ 1 - e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \left(1 + \frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} - \frac{1}{\overline{\gamma}_4} \sum_{m=0}^{\eta_k - 1} \frac{\mu_1^m}{m!} \sum_{n=0}^{m} \binom{m}{n} \right.$$
$$\left. \times 2^{2nR_s} n! \left(2^{2R_s} - 1\right)^{m-n} \left[e^{-\mu_1\left(2^{2R_s}-1\right)} \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-n-1} - e^{-\mu_5\left(2^{2R_s}-1\right)} \left(\mu_5 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-n-1} \right] \right\}$$
$$+ \frac{1}{\overline{\gamma}_2^{M-1} \Gamma\left(M-1\right)} \sum_{k=0}^{M-1} \frac{\Gamma\left(\theta_k\right)}{k! \mu_1^{\theta_k} \overline{\gamma}_1^k} \left\{ 1 - e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \left(1 + \frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} - \frac{1}{\overline{\gamma}_4} \sum_{m=0}^{\theta_k - 1} \frac{\mu_1^m}{m!} \sum_{n=0}^{m} \binom{m}{n} 2^{2nR_s} n! \right.$$
$$\left. \times \left(2^{2R_s} - 1\right)^{m-n} \left[e^{-\mu_1\left(2^{2R_s}-1\right)} \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-n-1} - e^{-\mu_5\left(2^{2R_s}-1\right)} \left(\mu_5 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-n-1} \right] \right\} \tag{43}$$

can be obtained after some simple mathematical manipulations. ∎

To achieve more insights, we now proceed to find the asymptotic secrecy outage probability of the MRT/MRC scheme in the high SNR regime.

Corollary 3. *In the high SNR regime, the asymptotic secrecy outage probability of dual-hop AF relaying systems with the MRT/MRC scheme is expressed as*

$$P^{\infty}_{\text{out,MRT/MRC}}\left(R_s\right) = \left(\Psi_{\text{MRT/MRC}} \overline{\gamma}_1\right)^{-\Phi_{\text{MRT/MRC}}}, \tag{49}$$

where the secrecy coding gain is given as (50)*, and the secrecy diversity gain is* $\Phi_{\text{MRT/MRC}} = M + 1$.

Proof: See Appendix C. ∎

Remark: The MRT/MRC scheme achieves a secrecy diversity order of $M + 1$, which is higher than that of the ZF/MRC scheme. However, it is worth pointing out that secrecy diversity order is an asymptotic performance measure, a higher diversity order does not necessarily implies that the MRT/MRC scheme outperforms the ZF/MRC scheme in the entire SNR range of interest. In fact, it depends on both the SNRs of the main channel and the eavesdropper channel.

4) MRT/SC: Following similar analysis as in the ZF/SC scheme, the closed-form approximation of the secrecy outage probability under the MRT/SC scheme can be expressed as (51) at the top of the next page.

Proof: By inserting (35) and (37) into (38), and utilizing [39, Eq. (8.352.1)] and [39, Eq. (3.351.3)], the final result can be derived after some simple mathematical manipulations. ∎

Next, we evaluate the asymptotic outage probability for the MRT/SC scheme.

Corollary 4. *In the high SNR regime, the asymptotic secrecy outage probability of dual-hop AF relaying systems with the MRT/SC scheme is given by*

$$P^{\infty}_{\text{out,MRT/SC}}\left(R_s\right) = \left(\Psi_{\text{MRT/SC}} \overline{\gamma}_1\right)^{-\Phi_{\text{MRT/SC}}}, \tag{52}$$

where the secrecy coding gain is expressed as (53)*, and the secrecy diversity gain is* $\Phi_{\text{MRT/SC}} = M + 1$.

Proof: From (73) and (76), the asymptotic secrecy outage probability for the MRT/SC scheme is given by

$$F_{\gamma^{\text{MRT}}_{\text{B}_{\text{SC}}}}\left(x\right) \approx \left(\frac{1}{\overline{\gamma}_1}\right)^{M+1} \frac{x^{M+1}}{M! \mu} \left(1 + \frac{1}{\kappa^M}\right). \tag{54}$$

By substituting (54) and (79) into (38), and with the help of [39, Eq. (3.351.3)], the desired result can be obtained. ∎

Now, according to Corollary 3 and Corollary 4, we proceed to the following remark.

Remark: The MRT/MRC scheme attains better secrecy outage performance than the MRT/SC scheme, and the performance gap between these two schemes can be characterized as a simple ratio of secrecy coding gain, i.e.,

$$\frac{\Psi_{\text{MRT/MRC}}}{\Psi_{\text{MRT/SC}}} = \left(M + 1\right)^{\frac{1}{M+1}}, \tag{55}$$

which suggests that for the same secrecy outage probability, the MRT/MRC scheme outperforms the MRT/SC scheme by an SNR gap of $\frac{1}{M+1} 10 \log\left(M + 1\right)$ dB less.

C. Probability of Non-Zero Secrecy Capacity

In this subsection, we check the condition for the existence of non-zero secrecy capacity. According to (13), the probability of non-zero secrecy capacity is formulated as

$$\Pr\left(C_{\text{S}} > 0\right) = \Pr\left(\gamma_{\text{B}_i} > \gamma_{\text{E}_{\text{MRC}}}\right) = 1 - P_{\text{out}}\left(0\right). \tag{56}$$

Hence, by setting $R_s = 0$ into the expressions of (39), (43), (48), and (51), closed-form approximation of the probability of positive secrecy for dual-hop AF relaying systems with each scheme can be easily evaluated after some mathematical manipulations.

D. CJ/ZF Scheme

Cooperative jamming has been demonstrated as a promising solution to improve the security of wireless communication networks [41]. As a benchmark scheme, we consider the scenario where the relay node R acts as a pure jammer as illustrated in Fig. 2. As such, the relay tries its best to degrade the quality of the eavesdropper's signal while at the same time avoiding interference at B. Therefore, the optimum beamforming vector $\mathbf{w}_3$ can be obtained by

$$\max_{\mathbf{w}_3} \left| \mathbf{h}^{\dagger}_{\text{RE}} \mathbf{w}_3 \right|$$
$$s.t. \ \left| \mathbf{h}^{\dagger}_{\text{RB}} \mathbf{w}_3 \right| = 0, \ \& \ \left\| \mathbf{w}_3 \right\|_F = 1. \tag{57}$$

$$P_{\text{out,MRT/MRC}}\left(R_s\right) \approx \frac{1}{\Gamma\left(M\right)} \sum_{v=0}^{M-1} \frac{\Gamma\left(\eta_v\right)}{v!} \left(\frac{1}{\overline{\gamma}_1^v \overline{\gamma}_2^M} + \frac{1}{\overline{\gamma}_1^M \overline{\gamma}_2^v}\right) \Bigg\{ \frac{1}{\mu_1^{\eta_v}} - \frac{1}{\mu_2^{\eta_v}} e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \Bigg[\left(\frac{1}{\mu_4^M \overline{\gamma}_1^M} + \frac{1}{\overline{\gamma}_3} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k} \overline{\gamma}_1^k} \right) \times \left(1 + \frac{2^{2R_s}\overline{\gamma}_4}{\overline{\gamma}_0}\right)^{-1} - \frac{1}{\mu_4^M \overline{\gamma}_1^M \overline{\gamma}_4} \sum_{m=0}^{M-1} \mu_4^m \left(\mu_3 + \frac{2^{2R_s}}{\overline{\gamma}_0}\right)^{-m-1} - \frac{1}{\overline{\gamma}_3 \overline{\gamma}_4} \sum_{k=0}^{M-1} \sum_{m=0}^{\phi_k - 1} \frac{\mu_4^m}{\mu_4^{\phi_k} \overline{\gamma}_1^k} \left(\mu_3 + \frac{2^{2R_s}}{\overline{\gamma}_0}\right)^{-m-1} \Bigg] - \frac{1}{\overline{\gamma}_4} e^{-\mu_1\left(2^{2R_s}-1\right)} \sum_{p=0}^{\eta_v - 1} \frac{\left(\mu_1^{p-\eta_v} - \mu_2^{p-\eta_v}\right)}{\Gamma\left(p+1\right)} \sum_{n=0}^{p} \binom{p}{n} \left(2^{2R_s}-1\right)^{p-n} 2^{2nR_s} \Bigg[n! \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-n-1} \left(\frac{1}{\mu_4^M \overline{\gamma}_1^M} + \frac{1}{\overline{\gamma}_3} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k} \overline{\gamma}_1^k} \right) - \frac{1}{\mu_4^M \overline{\gamma}_1^M} \sum_{m=0}^{M-1} \frac{(m+n)! \mu_4^m}{m! \left(\mu_1 2^{2R_s} + \mu_3\right)^{m+n+1}} - \frac{1}{\overline{\gamma}_3} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k} \overline{\gamma}_1^k} \sum_{m=0}^{\phi_k - 1} \frac{(m+n)! \mu_4^m}{m! \left(\mu_1 2^{2R_s} + \mu_3\right)^{m+n+1}} \Bigg] \Bigg\} \tag{48}$$

$$\Psi_{\text{MRT/MRC}} = \begin{cases} \left[\frac{1}{\mu} \left(1 + \frac{1}{\kappa^M}\right) \sum_{n=0}^{M+1} \binom{M+1}{n} \frac{(n+1)!}{(M+1)!} \left(2^{2R_s} - 1\right)^{M+1-n} \left(2^{2R_s} \overline{\gamma}_4\right)^n \right]^{-\frac{1}{M+1}}, & \overline{\gamma}_3 = \overline{\gamma}_4 \\ \left[\frac{1}{\mu} \left(1 + \frac{1}{\kappa^M}\right) \sum_{n=0}^{M+1} \binom{M+1}{n} \frac{n! 2^{2nR_s} \overline{\gamma}_3}{(M+1)! (\overline{\gamma}_3 - \overline{\gamma}_4)} \left(2^{2R_s} - 1\right)^{M+1-n} \left(\overline{\gamma}_3^{n+1} - \overline{\gamma}_4^{n+1}\right) \right]^{-\frac{1}{M+1}}, & \overline{\gamma}_3 \neq \overline{\gamma}_4 \end{cases} \tag{50}$$

$$P_{\text{out,MRT/SC}}\left(R_s\right) \approx \frac{1}{\Gamma\left(M\right)} \sum_{v=0}^{M-1} \frac{\Gamma\left(\eta_v\right)}{v! \mu_1^{\eta_v}} \left(\frac{1}{\overline{\gamma}_1^M \overline{\gamma}_2^v} + \frac{1}{\overline{\gamma}_1^v \overline{\gamma}_2^M}\right) \Bigg\{ 1 - e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \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} e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \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} e^{-\frac{2^{2R_s}-1}{\overline{\gamma}_0}} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k} \overline{\gamma}_1^k} \sum_{m=0}^{\phi_k - 1} \mu_4^m \times \left(\mu_3 + \frac{2^{2R_s}}{\overline{\gamma}_0}\right)^{-m-1} - \frac{1}{\overline{\gamma}_4} \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) \sum_{n=0}^{\eta_v - 1} \frac{\mu_1^n}{n!} \sum_{p=0}^{n} \binom{n}{p} \left(2^{2R_s}-1\right)^{n-p} 2^{2pR_s} p! \times \left[e^{-\mu_1\left(2^{2R_s}-1\right)} \left(\mu_1 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-p-1} - e^{-\mu_5\left(2^{2R_s}-1\right)} \left(\mu_5 2^{2R_s} + \frac{1}{\overline{\gamma}_4}\right)^{-p-1} \right] + \frac{1}{\mu_4^M \overline{\gamma}_1^M \overline{\gamma}_4} \sum_{m=0}^{M-1} \frac{\mu_4^m}{m!} \sum_{n=0}^{\eta_v - 1} \frac{\mu_1^n}{n!} \times \sum_{p=0}^{n} \binom{n}{p} \left(2^{2R_s}-1\right)^{n-p} 2^{2pR_s} (m+p)! \left[\frac{e^{-\mu_1\left(2^{2R_s}-1\right)}}{\left(\mu_1 2^{2R_s} + \mu_3\right)^{m+p+1}} - \frac{e^{-\mu_5\left(2^{2R_s}-1\right)}}{\left(\mu_5 2^{2R_s} + \mu_3\right)^{m+p+1}} \right] + \frac{1}{\overline{\gamma}_3 \overline{\gamma}_4} \sum_{k=0}^{M-1} \frac{1}{\mu_4^{\phi_k} \overline{\gamma}_1^k} \times \sum_{m=0}^{\phi_k - 1} \frac{\mu_4^m}{m!} \sum_{n=0}^{\eta_v - 1} \frac{\mu_1^n}{n!} \sum_{p=0}^{n} \binom{n}{p} \left(2^{2R_s}-1\right)^{n-p} 2^{2pR_s} (m+p)! \left[\frac{e^{-\mu_1\left(2^{2R_s}-1\right)}}{\left(\mu_1 2^{2R_s} + \mu_3\right)^{m+p+1}} - \frac{e^{-\mu_5\left(2^{2R_s}-1\right)}}{\left(\mu_5 2^{2R_s} + \mu_3\right)^{m+p+1}} \right] \Bigg\} \tag{51}$$

$$\Psi_{\text{MRT/SC}} = \begin{cases} \left[\frac{1}{\mu} \left(1 + \frac{1}{\kappa^M}\right) \sum_{n=0}^{M+1} \binom{M+1}{n} \frac{(n+1)!}{M!} \left(2^{2R_s} - 1\right)^{M+1-n} \left(2^{2R_s} \overline{\gamma}_4\right)^n \right]^{-\frac{1}{M+1}}, & \overline{\gamma}_3 = \overline{\gamma}_4 \\ \left[\frac{1}{\mu} \left(1 + \frac{1}{\kappa^M}\right) \sum_{n=0}^{M+1} \binom{M+1}{n} \frac{n! 2^{2nR_s} \overline{\gamma}_3}{M! (\overline{\gamma}_3 - \overline{\gamma}_4)} \left(2^{2R_s} - 1\right)^{M+1-n} \left(\overline{\gamma}_3^{n+1} - \overline{\gamma}_4^{n+1}\right) \right]^{-\frac{1}{M+1}}, & \overline{\gamma}_3 \neq \overline{\gamma}_4 \end{cases} \tag{53}$$

Now, according to [42, Proposition 1], the desired result is given by

$$\mathbf{w}_3 = \frac{\Pi^{\perp} \mathbf{h}_{\text{RE}}}{\left\| \Pi^{\perp} \mathbf{h}_{\text{RE}} \right\|_F}, \tag{58}$$

where $\Pi^{\perp} = \left(\mathbf{I} - \mathbf{h}_{\text{RB}} \left(\mathbf{h}_{\text{RB}}^{\dagger} \mathbf{h}_{\text{RB}}\right)^{-1} \mathbf{h}_{\text{RB}}^{\dagger}\right)$. Hence, the instantaneous SNRs of the main channel and the eavesdropper's channel are respectively expressed as

$$\gamma_{\text{B}_{\text{CJ}}} = \frac{P_s}{\sigma^2} |h_{\text{AB}}|^2 \tag{59}$$

and

$$\gamma_{\text{E}_{\text{CJ}}} = \frac{\frac{P_s}{\sigma^2} |h_{\text{AE}}|^2}{\frac{P_r}{\sigma^2} \left\| \Pi^{\perp} \mathbf{h}_{\text{RE}} \right\|_F^2 + 1}. \tag{60}$$

Now, we proceed to investigate the secrecy performance for the CJ/ZF scheme. To start with, we give the PDF of $\gamma_{\text{E}_{\text{CJ}}}$ in the following lemma.

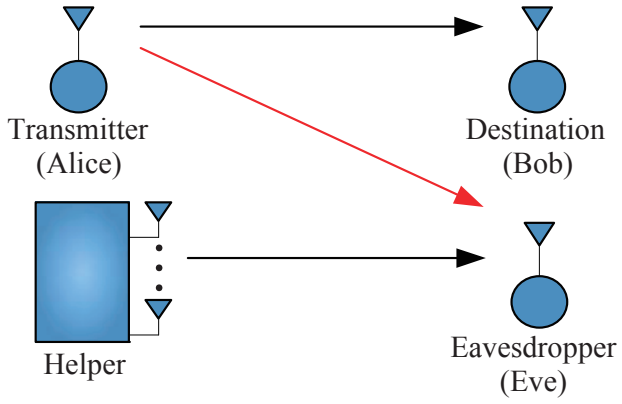


Fig. 2. System model for the cooperative jamming scheme.

Lemma 6. *The PDF of* $\gamma_{\mathrm{E_{CJ}}}$ *is given by*

$$f_{\gamma_{\mathrm{E_{CJ}}}}(x) = \frac{1}{\overline{\gamma}_4 \overline{\gamma}_3^{M-1}} \left(\frac{1}{\overline{\gamma}_3} + \frac{x}{\overline{\gamma}_4}\right)^{-(M-1)} e^{-\frac{x}{\overline{\gamma}_4}} \times \left[(M-1)\left(\frac{1}{\overline{\gamma}_3} + \frac{x}{\overline{\gamma}_4}\right)^{-1} + 1\right]. \quad (61)$$

Proof: See Appendix D. ∎

Armed with Lemma 6, a detailed analysis of the secrecy performance for the CJ/ZF scheme is provided in the following section.

1) Secrecy Outage Probability: From (59), we have

$$F_{\gamma_{\mathrm{B_{CJ}}}}(x) = 1 - e^{-\frac{x}{\overline{\gamma}_0}}. \quad (62)$$

Then, substituting (62) and (61) into (38), and performing some simple mathematical manipulations, the secrecy outage probability for the CJ/ZF scheme can be easily derived as follows:

$$P_{\mathrm{out,CJ}}(R_s) = 1 - e^{-\frac{2^{R_s}-1}{\overline{\gamma}_0}} \left[(M-1)\,\Psi\left(1, 2-M; \frac{1}{\overline{\gamma}_3} + \frac{2^{R_s}\overline{\gamma}_4}{\overline{\gamma}_0\overline{\gamma}_3}\right) + \frac{1}{\overline{\gamma}_3}\Psi\left(1, 3-M; \frac{1}{\overline{\gamma}_3} + \frac{2^{R_s}\overline{\gamma}_4}{\overline{\gamma}_0\overline{\gamma}_3}\right)\right], \quad (63)$$

where $\Psi(\alpha, \beta; z)$ is the confluent hypergeometric function of the second kind [39, Eq. (9.211.4)].

To achieve more insights, the asymptotic secrecy outage probability for the CJ/ZF scheme can be easily derived as

$$P^{\infty}_{\mathrm{out,CJ}}(R_s) = \frac{1}{\overline{\gamma}_0}\left[2^{R_s}(M-1)\frac{\overline{\gamma}_4}{\overline{\gamma}_3}\Psi\left(2, 3-M; \frac{1}{\overline{\gamma}_3}\right) + \left(2^{R_s}-1\right) + 2^{R_s}\frac{\overline{\gamma}_4}{\overline{\gamma}_3^2}\Psi\left(2, 4-M; \frac{1}{\overline{\gamma}_3}\right)\right]. \quad (64)$$

Remark: From (64), we find that the CJ/ZF scheme only achieves secrecy diversity order of one, which is independent of the number of antennas at the jammer.

2) Probability of Non-Zero Secrecy Capacity: By substituting $R_s = 0$ into (63), the exact closed-form expression of the probability of non-zero secrecy capacity for the CJ/ZF scheme is given by

$$P_{\mathrm{non,CJ}} = 1 - \frac{1}{\overline{\gamma}_3}\Psi\left(1, 3-M; \frac{1}{\overline{\gamma}_3} + \frac{\overline{\gamma}_4}{\overline{\gamma}_0\overline{\gamma}_3}\right) - (M-1)\,\Psi\left(1, 2-M; \frac{1}{\overline{\gamma}_3} + \frac{\overline{\gamma}_4}{\overline{\gamma}_0\overline{\gamma}_3}\right). \quad (65)$$

Please note, the CJ/ZF is adopted as a conventional scheme for comparison, however, the secrecy performance analysis of the CJ/ZF scheme for secure communications is also a part of the contribution of this work.

E. Comparison of the Proposed Schemes

We now provide a comparison between the four different schemes studied and the benchmark scheme. In the previous analysis, the CSI requirement to perform relay precoding or jamming was not explicitly revealed. In practice, the acquisition of CSI involves additional feedback overhead, which must be considered in the design of wireless systems. On the other hand, if a large amount of CSI is available at the transmitting node, more sophisticated transmission schemes could be designed to improve the transmission efficiency and to achieve a better secrecy performance. Hence, in order to make a fair comparison among different schemes, the CSI requirement of each scheme must be characterized. Table I gives a comparison of the ZF/MRC, ZF/SC, MRT/MRC, MRT/SC and CJ/ZF schemes in terms of CSI requirement at relay, antenna number M requirement, diversity order, and impact of antenna number M on diversity order and coding gain.

IV. Numerical Results

In this section, representative numerical results are provided to verify our analysis in the previous sections. Unless otherwise specified, the following set of parameters is used: $\overline{\gamma}_0 = 0.4\overline{\gamma}_1$, $\overline{\gamma}_2 = 1.2\overline{\gamma}_1$, $R_s = 2$, $\overline{\gamma}_3 = 10$dB, and $\overline{\gamma}_4 = 10$dB. In addition, to make a fair comparison, we assume that the transmit power of the CJ/ZF scheme at Alice is half of the sum power of the relay and Alice in the proposed schemes.

Fig. 3 illustrates the secrecy outage probability of the dual-hop AF relaying system with the ZF/MRC and ZF/SC schemes for different M. As shown in the figure, we can see that the analytical results of the ZF/MRC and ZF/SC schemes from (39) and (43) remain sufficiently tight across the entire SNR range of interest, which demonstrates the usefulness of the analytical expressions. 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. Another intuitive observation is that the ZF/MRC outperforms the ZF/SC scheme, which is consistent with the conventional relay networks with no secrecy constraint.

Fig. 4 shows the secrecy outage probability of the multi-antenna relaying-eavesdropper channel with the MRT/MRC and MRT/SC schemes for different M. It is observed that, for the two proposed schemes, the analytical approximations given in (48) and (51) are sufficiently accurate, and become

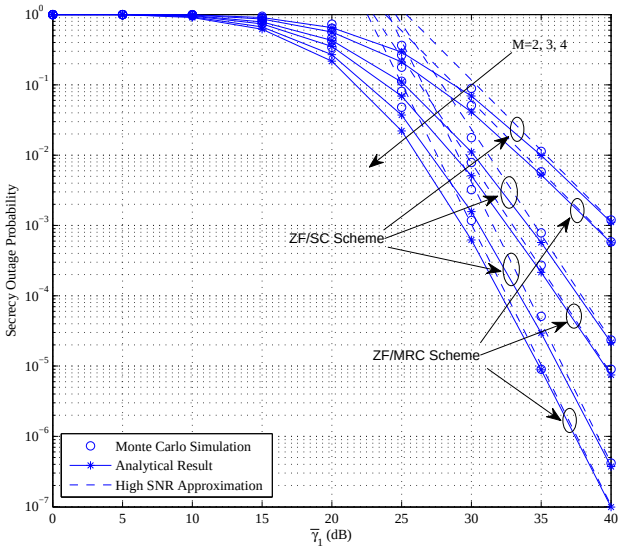


Fig. 3. Secrecy outage probability of the ZF/MRC and ZF/SC relaying systems with different relay antenna number M.

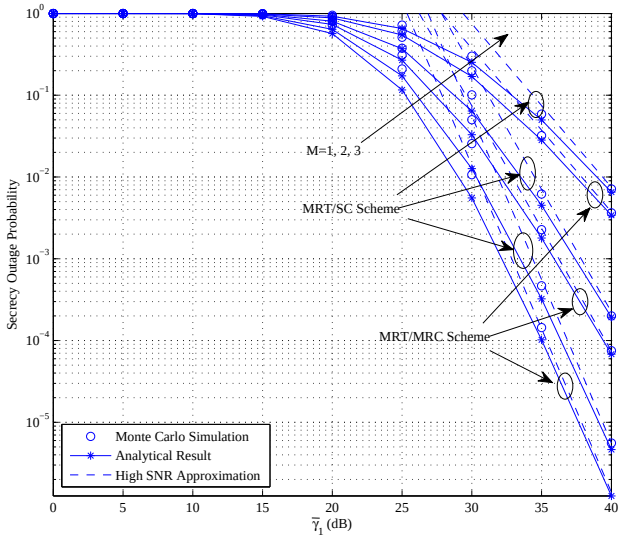


Fig. 4. Secrecy outage probability of the MRT/MRC and MRT/SC relaying systems with different relay antenna number M.

almost exact in the high SNR regime. Furthermore, we can see that the MRT/MRC scheme always attains better performance than the MRT/SC scheme, and all the slopes of the asymptotes keep parallel for each M, which indicates that the two schemes achieve the same secrecy diversity order.

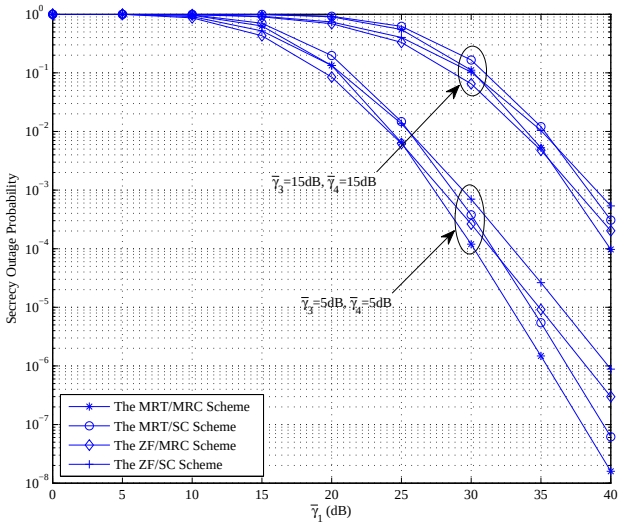


Fig. 5. Secrecy outage probability of the ZF/MRC, ZF/SC, MRT/MRC and MRT/SC schemes with $M = 3$, different $\overline{\gamma}_3$, and different $\overline{\gamma}_4$.

Fig. 5 investigates the impact of the quality of the eavesdropper's channel on the secrecy outage probability of the dual-hop AF relaying system with the proposed four 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 $\overline{\gamma}_4$. As mentioned earlier, higher secrecy diversity order of MRT schemes do not necessarily imply superior outage performance in the finite SNR regime. As shown in the figure, the ZF/MRC (ZF/SC) scheme outperforms the MRT/MRC (MRT/SC) scheme at the low SNR regime, while the opposite holds in the high SNR regime. The reason is that the ZF scheme can completely avoid information leakage to E in the second phase, as such, E has only access to a single copy of the source signal. Hence, the achievable rate of the eavesdropper's channel is reduced. On the other hand, compared to the MRT scheme, the use of ZF scheme also degrades the capacity of the main channel. In the low SNR regime, the reduction of the wiretap channel rate tends to outweigh the reduction of the main channel rate. Therefore, ZF/MRC is better than MRT/MRC in the low SNR regime. In addition, when the quality of eavesdropper's channel becomes good, i.e., large $\overline{\gamma}_3$ or $\overline{\gamma}_4$, the difference gap between the ZF/MRC scheme and the MRT/MRC scheme is reduced, and a similar phenomenon is observed between the ZF/SC scheme and the MRT/SC scheme.

Fig. 6 examines the secrecy outage probability of the CJ/ZF

TABLE I
COMPARISON OF THE ZF/MRC, ZF/SC, MRT/MRC, MRT/SC AND CJ/ZF SCHEMES

	ZF/MRC	ZF/SC	MRT/MRC	MRT/SC	CJ/ZF
CSI requirement at Relay	$\mathbf{h}_{\mathrm{AR}}$, $\mathbf{h}_{\mathrm{RB}}$, and $\mathbf{h}_{\mathrm{RE}}$	$\mathbf{h}_{\mathrm{AR}}$, $\mathbf{h}_{\mathrm{RB}}$, and $\mathbf{h}_{\mathrm{RE}}$	$\mathbf{h}_{\mathrm{AR}}$ and $\mathbf{h}_{\mathrm{RB}}$	$\mathbf{h}_{\mathrm{AR}}$ and $\mathbf{h}_{\mathrm{RB}}$	$\mathbf{h}_{\mathrm{RB}}$ and $\mathbf{h}_{\mathrm{RE}}$
Antenna number M requirement	$M > 1$	$M > 1$	None	None	$M > 1$
Diversity order	M	M	$M + 1$	$M + 1$	1
Impact of antenna number M	M provides both diversity order and coding gain.	M provides both diversity order and coding gain.	M provides both diversity order and coding gain.	M provides both diversity order and coding gain.	M provides coding gain, not diversity order.

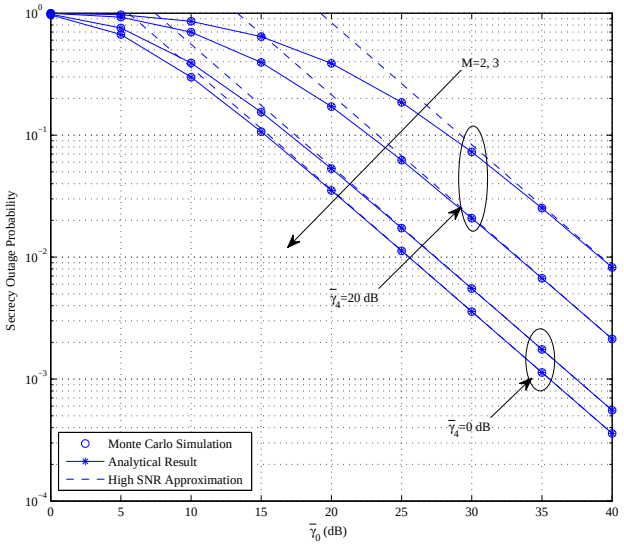


Fig. 6. Secrecy outage probability of the CJ/ZF scheme with different relay antenna number M and different $\overline{\gamma}_4$.

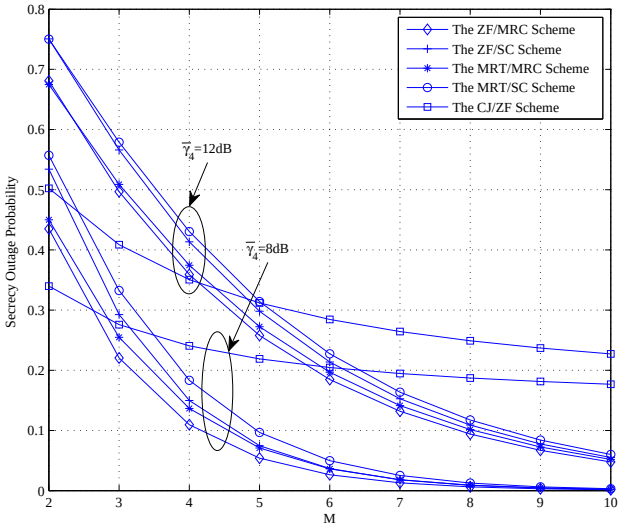


Fig. 7. Secrecy Outage comparison of the proposed schemes and the CJ/ZF scheme with $\overline{\gamma}_1 = 20$dB, $\overline{\gamma}_3 = 5$dB, different $\overline{\gamma}_4$.

scheme for different M and different $\overline{\gamma}_4$. As can be readily observed, the analytical results are in exact agreement with the Monte Carlo simulations, while the high SNR curves work quite well even at moderate SNRs. Moreover, different from the other schemes, we can see that only diversity order of one is achieved for the CJ/ZF scheme regardless of the number of antennas M. However, increasing M does improve the secrecy outage performance of the system by offering extra secrecy coding gain. In addition, we find that the quality of the eavesdropper's channel has a negative impact on the secrecy performance of the CJ/ZF scheme.

Fig. 7 illustrates the impact of the number of antennas at the relay on the secrecy outage performance of the proposed schemes and the CJ/ZF scheme with different $\overline{\gamma}_4$. It is noted that the gain of the proposed schemes relative to the CJ/ZF scheme increases with the number of antennas. This can be explained by the fact that the secrecy diversity order achieved by the proposed schemes increases with the number of antennas, while the secrecy diversity order of the CJ/ZF scheme is irrelevant to the number of antennas. It is also worth noting that the CJ/ZF may outperform the proposed schemes in certain regime, i.e., when the antenna number is small, especially when the quality of the eavesdropper's channel is relatively good, which needs to be taken into consideration for practical system design.

V. Conclusions

In this paper, we have investigated the secrecy outage performance of dual-hop AF relaying systems over Rayleigh fading channels. To exploit the available direct link for secrecy enhancement, we have proposed two linear precoding schemes with different receiving diversity combining at destination. Specifically, approximate closed-form expressions for the secrecy outage probability of all the proposed schemes were derived, based on which the probability of non-zero secrecy capacity was also evaluated. Moreover, simple and informative high SNR secrecy outage approximations were presented, which enable us to gain further insights into the impact of key parameters on the secrecy performance. In addition, to show the advantages of the proposed schemes, the benchmark CJ/ZF scheme was also analyzed. Our findings suggest that both the MRT/MRC and MRT/SC schemes achieve a full secrecy diversity order of $M+1$, while the ZF/MRC and ZF/SC schemes achieve a secrecy diversity order of M. Moreover, the ZF/MRC (ZF/SC) scheme outperforms the corresponding MRT/MRC (MRT/SC) scheme in the low SNR regime, while the opposite holds in the high SNR regime. Finally, we have shown that, the proposed schemes significantly perform better secrecy performance than the CJ/ZF scheme especially when the quality of eavesdropper's channel is bad.

Appendix A
Proof of Lemma 1

Without loss of generality, we first define $\gamma_{\mathrm{Z}} = \min(\gamma_1, \gamma_{2z})$. Then, using the fact that γ_1 and γ_2 are independent random variables, we have

$$F_{\gamma_{\mathrm{Z}}}(x) = F_{\gamma_1}(x) + F_{\gamma_{2z}}(x) - F_{\gamma_1}(x) F_{\gamma_{2z}}(x). \quad (66)$$

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

$$F_{\gamma_1}(x) = 1 - e^{-\frac{x}{\overline{\gamma}_1}} \sum_{k=0}^{M-1} \frac{1}{k!} \left(\frac{x}{\overline{\gamma}_1}\right)^k. \quad (67)$$

On the other hand, according to [42], the γ_{2z} is also a chi squared RV with $2(M-1)$ d.o.f. with CDF given by

$$F_{\gamma_{2z}}(x) = 1 - e^{-\frac{x}{\overline{\gamma}_2}} \sum_{k=0}^{M-2} \frac{1}{k!} \left(\frac{x}{\overline{\gamma}_2}\right)^k. \quad (68)$$

Then, substituting (67) and (68) into (66) and performing some simple mathematical manipulations, the CDF of Z can

be derived as

$$F_{\gamma_{\rm Z}}(x)=\frac{1}{\overline{\gamma}_1^M\Gamma(M)}\sum_{k=0}^{M-2}\frac{\Upsilon(\eta_k,\mu_1 x)}{k!\mu_1^{\eta_k}\overline{\gamma}_2^k}+\frac{1}{\overline{\gamma}_2^{M-1}\Gamma(M-1)}\sum_{k=0}^{M-1}\frac{\Upsilon(\theta_k,\mu_1 x)}{k!\mu_1^{\theta_k}\overline{\gamma}_1^k}. \quad (69)$$

Taking the derivative of (69) with respect to x, the PDF of $\gamma_{\rm Z}$ is derived as

$$f_{\gamma_{\rm Z}}(x)=\frac{1}{\overline{\gamma}_1^M}\frac{x^{M-1}e^{-\frac{x}{\overline{\gamma}_1}}}{\Gamma(M-1)\Gamma(M)}\Gamma\left(M-1,\frac{x}{\overline{\gamma}_2}\right)+\frac{1}{\overline{\gamma}_2^{M-1}}\frac{x^{M-2}e^{-\frac{x}{\overline{\gamma}_2}}}{\Gamma(M-1)\Gamma(M)}\Gamma\left(M,\frac{x}{\overline{\gamma}_1}\right), \quad (70)$$

where $\Gamma(a,b)$ is the incomplete Gamma function [39, Eq. (8.350.2)].

Due to the fact that $\gamma_{\rm AB}$ is an exponential RV, then according to (27), the Laplace transform of the PDF of $\gamma_{\rm B_{MRC}}^{\rm ZFU}$ can be represented as

$$\mathcal{L}\left\{f_{\gamma_{\rm B_{MRC}}^{\rm ZFU}}(x)\right\}=\frac{\mathcal{L}\{f_{\gamma_{\rm Z}}(x)\}}{\left(s+\frac{1}{\overline{\gamma}_0}\right)\overline{\gamma}_0}. \quad (71)$$

In order to compute the inverse Laplace transform of (71), we first utilize the formula [43, Eq. (1.1.1.13)]. Then, with the help of [39, Eq. (3.351.1)], the PDF of $\gamma_{\rm B_{MRC}}^{\rm ZFU}$ can be derived as

$$f_{\gamma_{\rm B_{MRC}}^{\rm ZFU}}(x)=\frac{1}{\overline{\gamma}_0\overline{\gamma}_1^M\Gamma(M)}e^{-\frac{x}{\overline{\gamma}_0}}\sum_{k=0}^{M-2}\frac{\Upsilon(\eta_k,\mu_2 x)}{k!\mu_2^{\eta_k}\overline{\gamma}_2^k}+\frac{1}{\overline{\gamma}_0\overline{\gamma}_2^{M-1}\Gamma(M-1)}e^{-\frac{x}{\overline{\gamma}_0}}\sum_{k=0}^{M-1}\frac{\Upsilon(\theta_k,\mu_2 x)}{k!\mu_2^{\theta_k}\overline{\gamma}_1^k}. \quad (72)$$

To obtain the CDF of $\gamma_{\rm B_{MRC}}^{\rm ZFU}$, we can directly integrate (72) by expanding $\Upsilon(\alpha,\beta)$ according to [39, Eq. (8.352.1)].

Appendix B
Proof of Corollary 1

In the high SNR regime, we assume that $\overline{\gamma}_1\to\infty$, $\overline{\gamma}_2=\kappa\overline{\gamma}_1$, and $\overline{\gamma}_0=\mu\overline{\gamma}_1$. The asymptotic CDF of $\gamma_{\rm AB}$ can be expressed as

$$F_{\gamma_{\rm AB}}(x)\approx\frac{x}{\mu\overline{\gamma}_1}. \quad (73)$$

Similarly, in the high SNR regime, the CDF of $\gamma_{\rm Z}$ can be approximated as

$$F_{\gamma_{\rm Z}}(x)\approx\frac{1}{(M-1)!}\left(\frac{x}{\kappa\overline{\gamma}_1}\right)^{M-1}. \quad (74)$$

Note that $\gamma_{\rm B_{MRC}}^{\rm ZF}\approx\gamma_{\rm AB}+\gamma_{\rm Z}$, hence, by invoking [44, Propositions 4 and 5], the asymptotic CDF of $\gamma_{\rm B_{MRC}}^{\rm ZF}$ can be expressed as

$$F_{\gamma_{\rm B_{MRC}}^{\rm ZF}}(x)\approx\frac{1}{\mu\kappa^{M-1}M!}\left(\frac{x}{\overline{\gamma}_1}\right)^{M}. \quad (75)$$

To this end, substituting (75) into (38) and utilizing [39, Eq. (3.351.3)], the asymptotic secrecy outage probability result for the ZF/MRC scheme is derived as (41) after some simple manipulations.

Appendix C
Proof of Corollary 3

Assuming $\gamma_{\rm m}=\min(\gamma_1,\gamma_{2m})$, the asymptotic CDF of $\gamma_{\rm m}$ in high SNR is given by

$$F_{\gamma_{\rm m}}(x)\approx\frac{1}{M!}\left(1+\frac{1}{\kappa^M}\right)\left(\frac{x}{\overline{\gamma}_1}\right)^M. \quad (76)$$

Furthermore, note that $\gamma_{\rm B_{MRC}}^{\rm MRT}\approx\gamma_{\rm AB}+\gamma_{\rm m}$, hence, by invoking [44, Propositions 4 and 5], the asymptotic CDF of $\gamma_{\rm B_{MRC}}^{\rm MRT}$ is given by

$$F_{\gamma_{\rm B_{MRC}}^{\rm MRT}}(x)\approx\frac{1}{\mu(M+1)!}\left(1+\frac{1}{\kappa^M}\right)\left(\frac{x}{\overline{\gamma}_1}\right)^{M+1} \quad (77)$$

On the other hand, when $\overline{\gamma}_1\to\infty$, the instantaneous SNR of the eavesdropper's channel under the MRT/MRC scheme can be approximated as

$$\gamma_{\rm E_{MRC}}^{\rm MRT}\approx\gamma_{\rm AE}+\gamma_3. \quad (78)$$

Considering that both $\gamma_{\rm AE}$ and γ_3 are the exponential RV, thus, the CDF of $\gamma_{\rm E_{MRC}}^{\rm MRT}$ is expressed as

$$f_{\gamma_{\rm E_{MRC}}^{\rm MRT}}(x)\approx\begin{cases}\frac{\overline{\gamma}_3}{\overline{\gamma}_3-\overline{\gamma}_4}\left(e^{-\frac{x}{\overline{\gamma}_3}}-e^{-\frac{x}{\overline{\gamma}_4}}\right), & \overline{\gamma}_3\neq\overline{\gamma}_4\\ \frac{x}{\overline{\gamma}_4^2}e^{-\frac{x}{\overline{\gamma}_4}}, & \overline{\gamma}_3=\overline{\gamma}_4\end{cases} \quad (79)$$

To this end, substituting (77) and (79) into (38) and utilizing [39, Eq. (3.351.3)], the asymptotic secrecy outage probability result for the MRC/MRT scheme can be obtained as (49) after some simple manipulations.

Appendix D
Proof of Lemma 4

To avoid confusion, we first define $X=\frac{P_s}{\sigma^2}|h_{\rm AE}|^2$ and $Y=\frac{P_r}{\sigma^2}\left\|\Pi^{\perp}\mathbf{h}_{\rm RE}\right\|_F^2$ in (57). According to [42], the PDF of Y is given by

$$f_Y(y)=\frac{y^{M-2}}{\Gamma(M-1)\overline{\gamma}_3^{M-1}}e^{-\frac{y}{\overline{\gamma}_3}}. \quad (80)$$

Then, by utilizing order statistic, the CDF of $\gamma_{\rm E_{CJ}}$ is expressed as

$$\begin{aligned}F_{\gamma_{\rm E_{CJ}}}(z)&=\Pr\left\{\frac{X}{Y+1}<z\right\}\\&=\int_0^\infty F_X(z(y+1))f_Y(y)\,dy\\&=1-\frac{1}{\overline{\gamma}_3^{M-1}}e^{-\frac{z}{\overline{\gamma}_4}}\left(\frac{1}{\overline{\gamma}_3}+\frac{z}{\overline{\gamma}_4}\right)^{-(M-1)},\end{aligned} \quad (81)$$

where we have used [39, Eq. (3.351.3)] to solve the corresponding integral. Thus, taking derivative of (81), the PDF of $\gamma_{\rm E_{CJ}}$ can be derived as (61).

REFERENCES

[1] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008.

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

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254-259, Jan. 2013.

[9] 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.

[10] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054-6067, Nov. 2014.

[11] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, and X. Gao, "Ergodic secrecy sum-rate for multiuser downlink transmission via regularized channel inversion: Large system analysis," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1627-1630, Sep. 2014.

[12] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766-4781, Sep. 2014.

[13] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245-2261, Mar. 2016.

[14] S. Leng, D. W. K. Ng, and R. Schober, "Power efficient and secure multiuser communication systems with wireless information and power transfer," in *IEEE International Conference on Communications Workshops (ICC)*, 2014, pp. 800-806.

[15] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K.-K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 74-85, Jan. 2016.

[16] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40-46, Dec. 2015.

[17] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293-307, Feb. 2015.

[18] 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," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007-2020, Dec. 2013.

[19] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589-605, Feb. 2015.

[20] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

[21] 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.

[22] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135-5146, Sep. 2015.

[23] 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.

[24] 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.

[25] V. N. Q. Bao, N. L. Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076-6085, Dec. 2013.

[26] 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.

[27] S.-I. Kim, I.-M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724-3737, July 2015.

[28] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893-4898, Oct. 2015.

[29] 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.

[30] L. Tong, B. Sadler, and M. Dong, "Pilot-assisted wireless transmissions: General model, design criteria, and signal processing," *IEEE Signal Process. Mag.*, vol. 21, no. 6, pp. 12-25, Nov. 2004.

[31] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453-2469, June 2008.

[32] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE J. Select. Areas Commun.*, vol. 31, no. 10. pp. 2099-2111, Oct. 2013.

[33] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 90-103, Jan. 2015.

[34] A. Basilevsky, *Applied Matrix Algebra in the Statistical Sciences*. New York: North-Holland, 1983.

[35] G. Zhu, C. Zhong, H. Suraweera, Z. Zhang, and C. Yuen, "Outage probability of dual-hop multiple antenna AF systems with linear processing in the presence of co-channel interference," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2308–2321, Apr. 2014.

[36] P. Anghel and M. Kaveh, "Exact symbol error probability of a cooperative network in a Rayleigh-fading environment," *IEEE Trans. Wireless Commun.*, vol. 3, no. 5, pp. 1416-1421, Sep. 2004.

[37] C. Zhong, H. Suraweera, A. Huang, Z. Zhang, and C. Yuen, "Outage probability of dual-hop multiple antenna AF relaying systems with interference," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 108-119, Jan. 2013.

[38] 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.

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

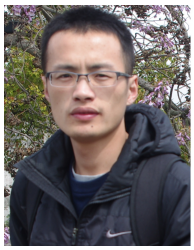
[40] J. Pérez, J. Ibánez, L. Vielva, and I. Santamaria, "Closed-form approximation for the outage capacity of orthogonal STBC," *IEEE Commun. Lett.*, vol. 9, no. 11, pp. 961-963, Nov. 2005.

[41] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[42] 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.

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

[44] Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," *IEEE Trans. Commun.*, vol. 51, no. 8, pp. 1389-1398, Aug. 2003.



Yuzhen Huang (S'12-M'16) received his B.S. degree in Communications Engineering, and Ph.D. degree in Communications and Information Systems from College of Communications Engineering, PLA University of Science and Technology, in 2008 and 2013 respectively. He has been with College of Communications Engineering, PLA University of Science and Technology since 2013, and currently as an Assistant Professor. His research interests focus on channel coding, MIMO communications systems, cooperative communications, physical layer security, and cognitive radio systems. He has published nearly 30 research papers in international journals and conferences such as IEEE TCOM, IEEE TVT, IEEE CL, WCNC, etc. He and his coauthors have been awarded a Best Paper Award at the WCSP 2013. He received an IEEE COMMUNICATIONS LETTERS exemplary reviewer certificate for 2014.

Jinlong Wang (SM'13) received the B.S. degree in mobile communications, M.S. degree and Ph.D. degree in communications engineering and information systems from Institute of Communications Engineering, Nanjing, China, in 1983, 1986 and 1992, respectively. Since 1979, Dr. Wang has been with the Institute of Communications Engineering, PLA University of Science and Technology, where he is currently a Full Professor and the Head of Institute of Communications Engineering. He has published over 100 papers in refereed mainstream journals and reputed international conferences and has been granted over 20 patents in his research areas. His current research interests are the broad area of digital communications systems with emphasis on cooperative communication, adaptive modulation, multiple-input-multiple-output systems, soft defined radio, cognitive radio, green wireless communications, and game theory.

Dr. Wang also has served as the Founding Chair and Publication Chair of International Conference on Wireless Communications and Signal Processing (WCSP) 2009, a member of the Steering Committees of WCSP2010-2012, a TPC member for several international conferences and a reviewer for many famous journals. He currently is the vice-chair of the IEEE Communications Society Nanjing Chapter and is an IEEE Senior Member.

Caijun Zhong (S'07-M'10-SM'14) received the B.S. degree in information engineering from Xi'an Jiaotong University, Xi'an, China, in 2004, and the M.S. degree in information security and the Ph.D. degree in telecommunications from the University College London, London, U.K., in 2006 and 2010, respectively. From September 2009 to September 2011, he was a Research Fellow with the Institute for Electronics, Communications and Information Technologies (ECIT), Queen's University Belfast, Belfast, U.K. Since September 2011, he has been with Zhejiang University, Hangzhou, China, where he is currently an Associate Professor. His research interests include massive MIMO systems, full-duplex communications, wireless power transfer, and physical layer security. He is an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS, EURASIP JOURNAL OF WIRELESS COMMUNICATIONS AND NETWORKING, and JOURNAL OF COMMUNICATIONS AND NETWORKS. He was an Exemplary Reviewer for the IEEE TRANSACTIONS ON COMMUNICATIONS in 2014. He and his coauthors have been awarded a Best Paper Award at the WCSP 2013. He was the recipient of the 2013 IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award.

Trung Q. Duong (S'05-M'12-SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include physical layer security, energy-harvesting communications, cognitive relay networks. He is the author or co-author of 190 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, and ELECTRONICS LETTERS. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020).

George K. Karagiannidis (M'96-SM'03-F'14) was born in Pithagorion, Samos Island, Greece. He received the University Diploma (5 years) and PhD degree, both in electrical and computer engineering from the University of Patras, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher at the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In June 2004, he joined the faculty of Aristotle University of Thessaloniki, Greece where he is currently Professor in the Electrical & Computer Engineering Dept. and Director of Digital Telecommunications Systems and Networks Laboratory. He is also Honorary Professor at South West Jiaotong University, Chengdu, China. His research interests are in the broad area of Digital Communications Systems with emphasis on Wireless Communications, Optical Wireless Communications, Wireless Power Transfer and Applications, Molecular Communications, Communications and Robotics and Wireless Security. He is the author or co-author of more than 400 technical papers published in scientific journals and presented at international conferences. He is also author of the Greek edition of a book on "Telecommunications Systems" and co-author of the book "Advanced Optical Wireless Communications Systems", Cambridge Publications, 2012. Dr. Karagiannidis has been involved as General Chair, Technical Program Chair and member of Technical Program Committees in several IEEE and non-IEEE conferences. In the past he was Editor in IEEE TRANSACTIONS ON COMMUNICATIONS, Senior Editor of IEEE COMMUNICATIONS LETTERS, Editor of the EURASIP JOURNAL OF WIRELESS COMMUNICATIONS AND NETWORKS and several times Guest Editor in IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS. From 2012 to 2015 he was the Editor-in Chief of IEEE COMMUNICATIONS LETTERS. Dr. Karagiannidis has been selected as a 2015 Thomson Reuters Highly Cited Researcher and he Listed in Thomson Reuters 2015 World's Most Influential Scientific Minds.