TẠP CHÍ KHOA HỌC
TRƯỜNG ĐẠI HỌC QUY NHƠN

Bảo mật lớp vật lý cho các kỹ thuật truyền dẫn đa người dùng của mạng chuyển tiếp MIMO lớn với xử lý tuyến tính

Nguyễn Đỗ Dũng[1,*], Đào Minh Hưng[1], Võ Nguyễn Quốc Bảo[2]

[1]*Khoa Kỹ thuật và Công nghệ, Trường Đại học Quy Nhơn, Việt Nam*
[2]*Học viện Công nghệ Bưu chính Viễn thông, Việt Nam*

Ngày nhận bài: 08/05/2021; Ngày nhận đăng:13/07/2021

TÓM TẮT

Trong bài báo này, chúng tôi xem xét vấn đề truyền dẫn đa người dùng trong hệ thống chuyển tiếp nhiều đầu vào nhiều đầu ra (MIMO). Trong đó, một trạm gốc được trang bị nhiều ăng ten truyền đồng thời thông tin đến nhiều người dùng thông qua sự trợ giúp của bộ chuyển tiếp được trang bị mảng ăng ten lớn. Giao thức giải mã và chuyển tiếp (DF) được xem xét bằng cách sử dụng kỹ thuật tổ hợp tỷ lệ cực đại/ truyền tỷ lệ cực đại (MRC/MRT) hoặc kỹ thuật tiếp nhận ép về không/ truyền ép về không (ZFR/ZFT), để xử lý tín hiệu tại bộ chuyển tiếp trong điều kiện thông tin trạng thái kênh không hoàn hảo. Kết quả, các biểu thức chính xác và biểu thức xấp xỉ đạt được về tốc độ kênh người sử dụng và tốc độ an toàn rớt kênh đối với một xác suất rớt kênh an toàn cho trước. Ngoài ra, chúng tôi đã đề xuất phân tích tiệm cận trong các trường hợp đặc biệt khác nhau. Nó đã tiết lộ rằng, phần lớn tỷ lệ nghe trộm được loại bỏ khi một số lượng ăng ten bộ chuyển tiếp tiến đến vô cùng và đồng thời năng lượng truyền tại trạm gốc và bộ chuyển tiếp có thể được giảm nhỏ xuống đáng kể theo yếu tố tỉ lệ $1/\sqrt{N}$, trong khi đó vẫn duy trì được hiệu suất hệ thống an toàn. Cuối cùng, kết quả mô phỏng thể hiện tính hợp lệ trong phân tích của bài báo.

Từ khoá: *Truyền thông an toàn, MIMO đa người dùng, chuyển tiếp MIMO lớn, mạng chuyển tiếp.*

**Tác giả liên hệ chính.*
Email: nguyendodung@qnu.edu.vn

https://doi.org/10.52111/qnjs.2022.16307

JOURNAL OF SCIENCE
QUY NHON UNIVERSITY

Physical layer security for multiuser transmission techniques of massive MIMO relay networks with linear processing

Nguyen Do Dung[1,*], **Dao Minh Hung**[1], **Vo Nguyen Quoc Bao**[2]

[1]*Faculty of Engineering and Technology, Quy Nhon University, Vietnam*
[2]*Posts and Telecommunications Institute of Technology, Vietnam*

Received: 08/05/2021; Accepted: 13/07/2021

ABSTRACT

In this paper, we consider the problem of secure multiuser transmission in a massive multiple input multiple output (MIMO) relaying system, wherein a base station equipped with many antennas transmits simultaneously its message to multiuser at the destination via help of a relay equipped with massive antenna arrays. Decode and forward (DF) protocol is considered by using the maximum ratio combining/maximum ratio transmission (MRC/MRT) or zero-forcing reception/zero-forcing transmission (ZFR/ZFT) to process signals at the relay under imperfect channel state information (CSI). As a result, exact and asymptotic expressions for user rate and outage secrecy rate for a given secure outage probability of eavesdropper links are derived. Furthermore, we have proposed the asymptotic analysis in various special cases. It is disclosed that the majority of eavesdropper rates is eliminated when a number of relay antennas go to infinity, and simultaneously the transmit power at the base station and the relay can be scaled down significantly by factor $1/\sqrt{N}$ while maintaining secure system performance. Finally, numerical results confirm the validity of our analysis.

Keywords: *Secure communication, multiuser MIMO, massive MIMO relaying, relay networks.*

1. INTRODUCTION

Recently, massive MIMO system can considerably enhance the data rate and serve many users in the same time-frequency resource by utilizing hundreds of antennas simultaneously.[1,2] Massive MIMO inherits all the advantage of traditional multiuser MIMO such as improved spectral efficiency, reliability, and reduced interference. Owing to the efficient use of the very large antenna arrays, transceiver is simplified even with just simple linear processing, e.g., maximum ratio transmission (MRC) or zero forcing (ZF).[3–6] Therefore, multiple transmit antennas techniques can also be exploited for enhancement of secrecy performance. In literatures,[7,8] it was found that,
the information leakage to an eavesdropper can be fairly small and insignificant as the number of antennas goes to infinity. As discussed in the article,[9] with standard time division duplexing (TDD) mode the legitimate user obtains several orders of magnitude much larger than the received signal power at the eavesdropper. This generates a state where the secrecy rate is quite high rate to the legitimate user. Altogether, massive MIMO enables excellent physical layer security without any extra effort.

In order to assess on the physical layer security performance, the gap between the legitimate channel capacity and the wiretap channel capacity is usually determined, namely secrecy rate.[10–12] Several excellent studies have investigated relay networks into physical layer security derived the considerable improvement of the legitimate channel capacity through cooperative diversity, hence enhances secure transmission.[13,14] However, presences of eavesdroppers in wireless networks are usually typical passive in order to hide their existence. Therefore, the transmitter cannot obtain eavesdropper CSI. Besides, the quality of legitimate CSI is also a challenge due to the fact

**Corresponding author.*
Email: nguyendodung@qnu.edu.vn

https://doi.org/10.52111/qnjs.2021.16307

that there exists legitimate channel estimation error or a feedback delay.[14–16] As in the article,[17] when the CSI is obtained by using property of reciprocity in TDD model systems, it may be imperfect because of delay or pilot contamination. In this context, the concept of secrecy outage rate was also considered to evaluate the secure communication with a given probability[18,19] due to unavailability of the eavesdropper CSI. Additionally, combining multiple relay cooperative beamforming with artificial noise (AN) was adopted to enhance the legitimate signal, and simultaneously degrade the eavesdropper signal.[20–22] Topics of secure communications on physical layer security including node authentication, message integrity, and secrecy have also been considered.[23]

In general, unlike the corresponding classical cryptographic approaches which are all based on computational security, the added strength of physical layer security is that it is based on information theoretic security, in which no limitation with respect to the opponent's computational capacity is assumed and is therefore inherently quantum resistant. Physical layer security solutions emerge as competitive candidates for low complexity, low-delay and low-footprint, adaptive, flexible and context aware security schemes, leveraging the physical layer of the communications.

Note that, secrecy performance of massive MIMO relaying system under the amplify-and-forward for multiuser transmission was discussed in the article.[24] In this paper, we continue surveying the relay-assisted massive MIMO system under DF to enhance the secrecy performance which is the paper's main motivation. Specifically, we focus on considering relay schemes, including MRC/MRT and ZFR/ZFT, and taking into account the effects of second hop channel estimation for physical layer security in a massive MIMO relaying network. The main contributions of this paper are summarized as follows:

i) Based on two linear processing methods, the secure multiuser MIMO downlink transmission techniques are considered to solve the challenging issue of the short-distance between the relay and eavesdroppers, and CSI imperfect channels. As a result, novel closed-form expressions of data rate and secrecy outage rate for MRC/MRT and ZFR/ZFT, which help us employ secure performance comparison of different network and system settings and provide significant insights for system design and optimization. It is noteworthy that secure transmission performance on short-distance eavesdroppers is addressed.

ii) The multiple-antenna MIMO technique at the relay is utilized by exploiting the large-scale antenna array gain. When the number of relay antennas approaches infinity, eavesdroppers of rate have less effects on secrecy performance, and simultaneously the transmit power at the BS and the relay can be scaled by factor $1/\sqrt{N}$.

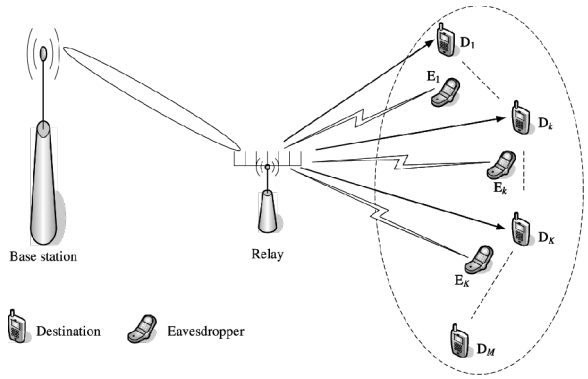

Figure 1. Relay-aided massive MIMO network.

The remainder of this chapter is organized in the following manner. In Section 2, the system model of the massive MIMO DF relaying system employing physical layer security under imperfect CSI is presented. In Section 3, we derive explicit expressions of the secrecy outage rate for both MRC/MRT and ZFR/ZFT methods, from which their secure performances in diffident cases are compared. In Section 4, we analyze asymptotic behavior of secrecy outage rate functions for typical power scaling laws in various scenarios. Numerical results are verified according to proposed schemes in Section 5. Finally, Section 6 concludes the paper.

Notation: Throughout the paper, we use upper (lower) case boldface to denote matrices (vectors). The superscripts $*$, T, and H stand for the complex conjugate, transpose, and conjugate-transpose, respectively. $\mathbf{A}_{ij}$ denotes the (i,j)-th entry of matrix $\mathbf{A}$, and $\mathbf{I}_N$ is the $N \times N$ identity matrix. We use $\mathbb{E}\{.\}$, $\|.\|$ and $\mathrm{Tr}(.)$ to denote the statistical expectation, the Euclidean norm and the trace of a matrix, respectively.

2. SYSTEM MODEL

In this section, the system model of secure multiuser downlink transmission based on relaying is introduced. Wherein, performance metrics are considered

https://doi.org/10.52111/qnjs.2022.16307

to evaluate on the secrecy characteristics of the system.

2.1. General description

In this paper, the relay strategy assisting secure multi-user downlink transmission is in Figure 1, wherein the base station (BS) is equipped with M antennas to serve corresponding single-antenna mobile destinations, M, via help of a relay (R) with N antennas. Because the system model is assumed that there is no direct path between BS and all D nodes due to a long propagation or shadowing.[25,26] Specifically, we will consider that a secure transmission downlink when K antennas at BS simultaneously send messages to desired K mobile destinations $(\mathsf{D}_1, \ldots, \mathsf{D}_K)$ with $(1 \leq K \leq M)$ in presence of K passive eavesdropper $(\mathsf{E}_1, \ldots, \mathsf{E}_K)$ either pretending to be legitimate destinations or to be idle mobile destinations.[27] We also assume that all E nodes are out of the coverage area the BS,[28,29] i.e., they are far from the BS and close to the R and D nodes. Therefore, all E nodes can only receive directly from the emitting R.

In the first phase, having K antennas transmit simultaneously their signal vector, $\mathbf{x} = [x_1, x_2, \ldots, x_K]^T$. Here, we assume that $\mathbb{E}\{|x_k|^2\} = 1$ so that P_{S} is the average transmit power per antenna at BS. The received signal at R is given by

$$\mathbf{y}_{\mathsf{R}} = \sqrt{P_{\mathsf{S}}}\mathbf{G}_{\mathsf{BR}}\mathbf{x} + \mathbf{n}_{\mathsf{R}}, \tag{1}$$

where $\mathbf{G}_{\mathsf{BR}} \in \mathbb{C}^{N\times K}$ denotes the channel matrix from BS to R. It notes that the channel matrices account for independent and identically distributed (i.i.d.) Rayleigh fading and time division duplex. More precisely, $\mathbf{G}_{\mathsf{BR}}$ can be expressed as $\mathbf{G}_{\mathsf{BR}} \triangleq \sqrt{\eta_{\mathsf{BR}}}\mathbf{H}_{\mathsf{BR}}$, where the small-scaled fading matrix $\mathsf{H}_{\mathsf{BR}} \in \mathbb{C}^{N\times K}$ has i.i.d. $\mathcal{CN}(0,1)$ elements, while factor η_{BR} is the distance-dependent path-loss random variable with variance $E\{|\eta_{\mathsf{BR}}|^2\} = \sigma^2_{\mathsf{BR}}$.

By using the linear receiver, the received signal $\mathbf{y}_{\mathsf{R}}$ at the relay is separated into K streams by multiplying it with a linear detector matrix $\mathbf{A}^T$ as

$$\mathbf{r} = \mathbf{A}^T\mathbf{y}_{\mathsf{R}}, \tag{2}$$

$$= \sqrt{P_{\mathsf{S}}}\mathbf{A}^T\mathbf{G}_{\mathsf{BR}}\mathbf{x} + \mathbf{A}^T\mathbf{n}_{\mathsf{R}}. \tag{3}$$

In particular, the k-th signal stream processed at R can be written as

$$\mathbf{r}_k = \sqrt{P_{\mathsf{S}}}\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}x_k + \sqrt{P_{\mathsf{S}}}\sum_{i\neq k}^{K}\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},i}x_i + \mathbf{a}_k^T\mathsf{n}_{\mathsf{R}}. \tag{4}$$

In the second phase, the relay performs linear precoding to all decoded signals, $\mathbf{x}$, in the first phase by multiplying it with a beamforming matrix $\mathbf{B}$, i.e., $\mathbf{s} = \mathbf{B}\mathbf{x}$. These signals are then broadcasted to destinations. Hence, the received $K \times 1$ signals at all D will be

$$\mathbf{y}_{\mathsf{D}} = \mathbf{G}_{\mathsf{RD}}^T\mathbf{s} + \mathbf{n}_{\mathsf{D}},$$

$$= \mathbf{G}_{\mathsf{RD}}^T\mathbf{B}\mathbf{x} + \mathbf{n}_{\mathsf{D}}. \tag{5}$$

In particular, we can write the received signal at D_k under the form of

$$y_{\mathsf{D}_k} = \mathbf{g}_{\mathsf{RD},k}^T\mathbf{b}_k x_k + \sum_{i\neq k}^{K}\mathbf{g}_{\mathsf{RD},k}^T\mathbf{b}_i x_i + n_{\mathsf{D}_k}, \tag{6}$$

where the channel matrix between the K destinations and the relay is denoted by $\mathbf{G}_{\mathsf{RD}} = [\mathbf{g}_{\mathsf{RD},1}, \mathbf{g}_{\mathsf{RD},2}, ..., \mathbf{g}_{\mathsf{RD},K}] \in \mathbb{C}^{N\times K}$. $\mathbf{G}_{\mathsf{RD}}$ can be further written as $\mathbf{G}_{\mathsf{RD}} = \mathbf{H}_{\mathsf{RD}}\mathbf{D}_{\mathsf{RD}}^{1/2}$, in which $\mathbf{H}_{\mathsf{RD}} \in \mathbb{C}^{N\times K}$ includes the i.i.d. $\mathcal{CN}(0,1)$ small-scale fading coefficients, and $\mathbf{D}_{\mathsf{RD}}$ is the large-scale fading diagonal matrix depended on distance path-loss, and i-th diagonal element of the diagonal matrix is denoted by $[\mathbf{D}_{\mathsf{RD}}]_{ii} = \sigma^2_{\mathsf{RD},i}, (i = 1, 2, \ldots, K)$. Moreover, $\mathbf{n}_{\mathsf{D}}$ and $\mathbf{n}_{\mathsf{R}}$ are the AWGN vectors at R and K destinations, respectively, with i.i.d. components following $\mathcal{CN}(0,1)$. From (4) and (6), the instantaneous received signal-to-interference-plus-noise ratio (SINR) at R with k-th stream and D_k is given by, respectively,

$$\gamma_{\mathsf{BR}_k} = \frac{P_{\mathsf{S}}\left|\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right|^2}{P_{\mathsf{S}}\sum_{i\neq k}^{K}\left|\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},i}\right|^2 + P_{\mathsf{S}}\left|\mathbf{a}_k^T\mathbf{n}_{\mathsf{R}}\right|^2}, \tag{7}$$

and

$$\gamma_{\mathsf{RD}_k} = \frac{\left|\mathbf{g}_{\mathsf{RD},k}^T\mathbf{b}_k\right|^2}{\sum_{i\neq k}^{K}\left|\mathbf{g}_{\mathsf{RD},k}\mathbf{b}_i\right|^2 + 1}. \tag{8}$$

As a result, we can obtain an achievable rate of the transmission links BS $\rightarrow$ R and R $\rightarrow$ D_k respectively as

$$\mathscr{R}_{\mathsf{BR}_k} = \log_2\left(1 + \gamma_{\mathsf{BR}_k}\right), \tag{9}$$

and

$$\mathscr{R}_{\mathsf{RD}_k} = \log_2\left(1 + \gamma_{\mathsf{RD}_k}\right). \tag{10}$$

At the same time, E_k tries to intercept information from R to D_k. Therefore, the received signal at E_k can be obtained as

https://doi.org/10.52111/qnjs.2021.16307

$$y_{\mathsf{E}_k} = \mathbf{g}_{\mathsf{RE},k}^T \mathbf{b}_k x_k + \sum_{i \neq k}^{K} \mathbf{g}_{\mathsf{RE},k}^T \mathbf{b}_i x_i + n_{\mathsf{E}_k}, \quad (11)$$

where $\mathbf{g}_{\mathsf{RE},k}$ is the channel vector between E_k and R, n_{E_k} is the AWGN with zero mean and unit covariance at E_k.

Similar to (8), we assume that the channel $\mathbf{g}_{\mathsf{RE},k}$ is obtained at k-th corresponding eavesdropper is perfect CSI. Therefore, the achievable SINR at E_k is

$$\gamma_{\mathsf{RE}_k} = \frac{\left|\mathbf{g}_{\mathsf{RE},k}^T \mathbf{b}_k\right|^2}{\sum_{i \neq k}^{K} \left|\mathbf{g}_{\mathsf{RE},k} \mathbf{b}_i\right|^2 + 1}. \quad (12)$$

From (12), the corresponding eavesdropper rate of transmission link $\mathsf{R} \to \mathsf{E}_k$ derived as

$$\mathscr{R}_{\mathsf{RE}_k} = \log_2 \left(1 + \gamma_{\mathsf{RE}_k}\right). \quad (13)$$

For secure multiuser massive MIMO relaying system, we assume that the achievable total legitimate channel rate and the achievable total eavesdropper channel rate are $\mathscr{R}_{\mathsf{D}}$ and $\mathscr{R}_{\mathsf{E}}$, respectively. From the perspective of information theory, the achievable secrecy rate region for decode-and-forward dualhop relay wiretap channel is expressed as [11,30]

$$\mathscr{R}_{\mathsf{SE}} = \left[\mathscr{R}_{\mathsf{D}} - \mathscr{R}_{\mathsf{E}}\right]^+ = \sum_{k=1}^{K} \mathscr{R}_{\mathsf{SE}_k}, \quad (14)$$

where $\mathscr{R}_{\mathsf{SE}_k}$ is the achievable secrecy rate at D_k,[31] given by

$$\mathscr{R}_{\mathsf{SE}_k} = \left[\mathscr{R}_{\mathsf{D}_k} - \mathscr{R}_{\mathsf{E}_k}\right]^+, \quad (15)$$

with $[x]^+ = \max(x, 0)$. In (15), $\mathscr{R}_{\mathsf{D}_k}$ and $\mathscr{R}_{\mathsf{E}_k}$ represent the achievable channel rate of the transmission link $\mathsf{BR}_k \to \mathsf{R} \to \mathsf{D}_k$ and $\mathsf{BR}_k \to \mathsf{R} \to \mathsf{E}_k$, respectively. Thus, we have

$$\mathscr{R}_{\mathsf{D}_k} = \frac{1}{2} \min \left(\mathscr{R}_{\mathsf{BR}_k}, \mathscr{R}_{\mathsf{RD}_k}\right), \quad (16)$$

and

$$\mathscr{R}_{\mathsf{E}_k} = \frac{1}{2} \min \left(\mathscr{R}_{\mathsf{BR}_k}, \mathscr{R}_{\mathsf{RE}_k}\right). \quad (17)$$

2.2. Performance metrics

In this paper, we assume that there is no knowledge of eavesdropper links at BS and R. Maintaining a steady secrecy rate over all realizations of fading channels is difficult since CSI eavesdroppers is unavailable. Based on the given secrecy outage probability, ζ, we take the maximum rate which is defined as secrecy outage rate, $\mathscr{R}_{\mathtt{OSE}_k}$, at D_k. Hence, we have[7]

$$\zeta = \Pr\left(\mathscr{R}_{\mathtt{OSE}_k} > \mathscr{R}_{\mathsf{D}_k} - \mathscr{R}_{\mathsf{E}_k}\right). \quad (18)$$

From (17), we can rewrite (18) as

$$\zeta = \Pr\left[\mathscr{R}_{\mathtt{OSE}_k} > \mathscr{R}_{\mathsf{D}_k} - \frac{1}{2}\log_2\left(1 + \gamma_{\mathsf{E}_k}\right)\right], \quad (19)$$

$$= 1 - F_{\gamma_{\mathsf{E}_k}}\left[2^{2\left(\mathscr{R}_{\mathsf{D}_k} - \mathscr{R}_{\mathtt{OSE}_k}\right)-1}\right]. \quad (20)$$

where $\gamma_{\mathsf{E}_k} \triangleq \min\left(\gamma_{\mathsf{BR}_k}, \gamma_{\mathsf{RE}_k}\right)$ and $F_{\gamma_{\mathsf{E}_k}}(.)$ is the cumulative distribution function (CDF) of γ_{E_k}. After we simply manipulate the expression (20), the system secrecy outage rate as a function of ζ can be derived as

$$\mathscr{R}_{\mathtt{OSE}_k} = \mathscr{R}_{\mathsf{D}_k} - \frac{1}{2}\log_2\left[1 + F_{\gamma_{\mathsf{E}_k}}^{-1}(1-\zeta)\right], \quad (21)$$

where ${F\gamma_{\mathsf{E}_k}}^{-1}(.)$ is the inverse CDF of $F_{\gamma_{\mathsf{E}_k}}(.)$.

We consider both MRC/MRT and ZFR/ZFT schemes under practical wireless network scenarios. Specifically, the BS and R locations are fixed while all destinations serve as mobile terminals as the case considered in this paper. Therefore, the first-hop channel, $\mathbf{G}_{\mathsf{BR}}$, is considered as perfect CSI by accurately estimating. Whereas, the achieved second-hop channel, $\mathbf{G}_{\mathsf{RD}}$, is imperfect due to applying due to channel reciprocity in TDD systems and the mobility of destination nodes,[25] which leads to the channel estimation error matrix, $\hat{\mathbf{G}}_{\mathsf{RD}}$, of the actual channel matrix $\mathbf{G}_{\mathsf{RD}}$, we can write[32]

$$\mathbf{G}_{\mathsf{RD}} = \hat{\mathbf{G}}_{\mathsf{RD}} + \boldsymbol{\mathcal{E}}_{\mathsf{RD}}, \quad (22)$$

where $\hat{\mathbf{G}}_{\mathsf{RD}} = [\hat{\mathbf{g}}_{\mathsf{RD},1}, \ldots, \hat{\mathbf{g}}_{\mathsf{RD},K}] \in \mathbb{C}^{(N \times K)}$, $\boldsymbol{\mathcal{E}}_{\mathsf{RD}} = [\mathbf{e}_{\mathsf{RD},1}, \ldots, \mathbf{e}_{\mathsf{RD},K}] \in \mathbb{C}^{(N \times K)}$ is the estimation error matrix, which is independent of $\hat{\mathbf{G}}_{\mathsf{RD}}$, i.e., $\boldsymbol{\mathcal{E}}_{\mathsf{RD}} \sim \mathcal{CN}(0, \mathbf{E}_{\mathsf{RD}})$ with $\mathbf{E}_{\mathsf{RD}} = \text{diag}\left[\sigma_{e,1}^2, \ldots, \sigma_{e,K}^2\right]$, and $\hat{\mathbf{G}}_{\mathsf{RD}} \sim \mathcal{CN}(0, \mathbf{D}_{\mathsf{RD}} - \mathbf{E}_{\mathsf{RD}})$ with $\mathbf{D}_{\mathsf{RD}} - \mathbf{E}_{\mathsf{RD}} \triangleq \hat{\mathbf{D}}_{\mathsf{RD}} = \text{diag}\left[\hat{\sigma}_{\mathsf{RD},1}^2, \ldots, \hat{\sigma}_{\mathsf{RD},K}^2\right]$, whose element is $\hat{\sigma}_{\mathsf{RD},i}^2 \triangleq \sigma_{\mathsf{RD},i}^2 - \sigma_{e,i}^2$ for $i = 1, 2, \ldots, K$.

2.2.1. *MRC/MRT processing*

With low complexity, MRC/MRT scheme is widely applied in massive MIMO techniques.[4,33] Hence, the

MRC receiver and MRT beamforming matrices at the relay are respectively given by[5,6]

$$\mathbf{A}^T = \mathbf{A}_{\mathtt{MRC}}^T \triangleq \mathbf{G}_{\mathsf{BR}}^H, \tag{23}$$

and

$$\mathbf{B} = \mathbf{B}_{\mathtt{MRC}} \triangleq \rho_{\mathtt{MRC}} \hat{\mathbf{G}}_{\mathsf{RU}}^*. \tag{24}$$

Here, $\mathbf{A}_{\mathtt{MRC}}^T$ is chosen for facilitating signal processing in the first phase. In the second phase, $\mathbf{B}_{\mathtt{MRT}}$ is chosen under the practical CSI, i.e. $\hat{\mathbf{G}}_{\mathsf{RD}}$ based on the MRT criterion. Note that $\rho_{\mathtt{MRC}}$ is the power-normalization factor to meet the long-term total transmit power at the relay[6], namely,

$$\rho_{\mathtt{MRC}} \approx \sqrt{\frac{P_{\mathsf{R}}}{N\sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2}}. \tag{25}$$

2.2.2. ZFR/ZFT *processing*

Similar to MRC/MRT scheme, when using ZFR/ZFT scheme for the receivers and precoders at R can be respectively given by[6]

$$\mathbf{A}^T = \mathbf{A}_{\mathtt{ZF}}^T \triangleq \left(\mathbf{G}_{\mathsf{BR}}^H \mathbf{G}_{\mathsf{BR}}\right)^{-1} \mathbf{G}_{\mathsf{BR}}^H, \tag{26}$$

and

$$\mathbf{B} = \mathbf{B}_{\mathtt{ZF}} \triangleq \rho_{\mathtt{ZF}} \hat{\mathbf{G}}_{\mathsf{RD}}^* \left(\hat{\mathbf{G}}_{\mathsf{RD}}^T \hat{\mathbf{G}}_{\mathsf{RD}}^*\right)^{-1} \tag{27}$$

where $\rho_{\mathtt{ZF}}$ is also the power normalization factor for ZFR/ZFT, in which we use the property of $\mathrm{Tr}(\mathbf{AB}) = \mathrm{Tr}(\mathbf{BA})$ and then applying[34] Lemma 2.9 to obtain

$$\rho_{\mathtt{ZF}} \approx \sqrt{\frac{(N-K)\,P_{\mathsf{R}}}{\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}}. \tag{28}$$

3. ACHIEVABLE RATE ANALYSIS AND SECRECY PERFORMANCE

In this section, we will consider the achievable secrecy rate of the $\mathsf{BS} \to \mathsf{R} \to \mathsf{D}_k$ link based on the approach in the article,[35] where the received signal is analyzed as a known mean times the desired symbol plus an uncorrelated effective noise. This is widely utilized in analysis of MIMO technique since it can be obtained an explicit rate expression and no requirement of instantaneous CSI at destination. Therefore, we may analyze received signal streams at R and D as follows:

From (4), the k-th received signal stream at R is rewritten as

$$\mathbf{r}_k = \sqrt{P_{\mathsf{S}}}\mathbf{a}_k^T \mathbf{g}_{\mathsf{BR},k} x_k + \tilde{n}_{\mathsf{R}_k}, \tag{29}$$

where $\tilde{n}_{\mathsf{R}_k}$ is the effective noise at R, given by

$$\tilde{n}_{\mathsf{R}_k} \triangleq \sqrt{P_{\mathsf{S}}}\sum_{i\neq k}^{K}\mathbf{a}_k^T \mathbf{g}_{\mathsf{BR},i} x_i + \mathbf{a}_k^T n_{\mathsf{R}}. \tag{30}$$

From above analyses, the k-th received SINR at R for both cases of MRC/MRT and ZFR/ZFT is express as below

$$\gamma_{\mathsf{BR}_k}^{\mathtt{MRC/ZF}} \triangleq \frac{P_{\mathsf{S}}\left|\mathbb{E}\left\{\mathbf{a}_k^T \mathbf{g}_{\mathsf{BR},k}\right\}\right|^2}{P_{\mathsf{S}}\mathrm{Var}\left(\mathbf{a}_k^T \mathbf{g}_{\mathsf{BR},k}\right) + P_{\mathsf{S}}\mathsf{IS}_k + \mathsf{NR}_k}, \tag{31}$$

where IS_k and NR_k represent the interference between streams transmitted from $\mathsf{BS} \to \mathsf{R}$, and the noise at the relay, respectively. In particular, we have

$$\mathsf{IS}_k \triangleq \sum_{i\neq k}^{K}\mathbb{E}\left\{\left|\mathbf{a}_k^T \mathbf{g}_{\mathsf{BR},i}\right|^2\right\}, \tag{32}$$

$$\mathsf{NR}_k \triangleq \mathbb{E}\left\{\left|\mathbf{a}_k^T n_{\mathsf{R}}\right|^2\right\}. \tag{33}$$

Similar to signal analysis way as in the first phase, the corresponding received SINR at D_k in the second phase is derived from (6) as follows:

$$\gamma_{\mathsf{RD}_k}^{\mathtt{MRC/ZF}} \triangleq \frac{\left|\mathbb{E}\left\{\mathbf{g}_{\mathsf{RD},k}^T \mathbf{b}_k\right\}\right|^2}{\mathrm{Var}\left(\mathbf{g}_{\mathsf{RD},k}^T \mathbf{b}_k\right) + \sum_{i\neq k}^{K}\mathbb{E}\left\{\left|\mathbf{g}_{\mathsf{RD},k}^T \mathbf{b}_i\right|^2\right\} + 1}. \tag{34}$$

Next, the legitimate channel rate and the secrecy outage rate will be considered in detail by using the above technique.

3.1. MRC/MRT at R

When MRC receiver and MRT beamforming are performed, we have the following theorem.

Theorem 1. *For* MRC/MRT *processing, the achievable rate of the transmission link* $\mathsf{BS} \to \mathsf{R} \to \mathsf{D}_k$ *in the massive MIMO DF relaying system is tightly approximated as*

$$\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}} = \frac{1}{2}\log_2\left(1 + \min\left\{\frac{NP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2 + 1}, \frac{NP_{\mathsf{R}}\hat{\sigma}_{\mathsf{RD},k}^4}{\left[P_{\mathsf{R}}\left(\hat{\sigma}_{\mathsf{RD},k}^2 + \sigma_{e,k}^2\right) + 1\right]\sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2}\right\}\right). \tag{35}$$

Proof. See Appendix A. □

For eavesdroppers, we assume that each eavesdropper has perfect CSI by the channel estimates. Therefore, the corresponding eavesdropper rate at E_k can be obtained as

$$\begin{aligned}\mathscr{R}_{\mathsf{E}_k}^{\mathtt{MRC}} &= \frac{1}{2}\log_2\left(1+\min\left(\gamma_{\mathsf{BR}_k}^{\mathtt{MRC}},\gamma_{\mathsf{RE}_k}^{\mathtt{MRC}}\right)\right),\\ &= \frac{1}{2}\log_2\left(1+\min\left(\frac{NP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1},\right.\right.\\ &\left.\left.\frac{\rho_{\mathtt{MRC}}^2\left|\mathbf{g}_{\mathsf{RE},k}^T\hat{\mathbf{g}}_{\mathsf{RD},k}^*\right|^2}{\rho_{\mathtt{MRC}}^2\sum_{i\neq k}^K\left|\mathbf{g}_{\mathsf{RE},k}^T\hat{\mathbf{g}}_{\mathsf{RD},i}^*\right|^2+1}\right)\right).\end{aligned} \tag{36}$$

Thus, the achievable secrecy rate at D_k can be given by

$$\mathscr{R}_{\mathsf{SE}_k}^{\mathtt{MRC}} = \frac{1}{2}\log_2\left(\frac{1+\min\left(\gamma_{\mathsf{BR}_k}^{\mathtt{MRC}},\gamma_{\mathsf{RD}_k}^{\mathtt{MRC}}\right)}{1+\min\left(\gamma_{\mathsf{BR}_k}^{\mathtt{MRC}},\gamma_{\mathsf{RE}_k}^{\mathtt{MRC}}\right)}\right). \tag{37}$$

Based on (37), the asymptotic form for the secrecy outage rate at D_k is derived in the following Theorem 2.

Theorem 2. *Subject to a predefined outage secrecy probability, ζ, the secrecy outage rate of D_k in* MRC/MRT *of massive MIMO DF relay network under $N > \max\left(K, \frac{(KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1)\hat{\sigma}_{\mathsf{RD},k}^2}{P_{\mathsf{S}}\sigma_{\mathsf{BR}}^2\sum_{i\neq k}^K\hat{\sigma}_{\mathsf{RD},i}^2}\right)$, is given by*

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC}} = \mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}} - \mathscr{R}_{\mathtt{OE}_k}^{\mathtt{MRC}}(\zeta), \tag{38}$$

where $\mathscr{R}_{\mathtt{OE}_k}^{\mathtt{MRC}}(\zeta)$ is obtained as shown in (39) *at the top of the next page.*

Proof. See Appendix B. □

3.2. ZFR/ZFT at R

For ZFR/ZFT, we can also obtain the rate and secrecy
outage rate of D_k, which are similar to the consideration way in MRC/MRT. As a result, we have a closed-form expression for the achievable rate in the following Theorem 3.

Theorem 3. *For* ZFR/ZFT *processing, the achievable rate of the transmission link $\mathsf{BS}\rightarrow\mathsf{R}\rightarrow\mathsf{D}_k$ in the massive MIMO DF relaying system is given as in* (40) *shown at the top of the next page.* □

Next, the acquired rate at corresponding E_k for ZFR/ZFT is

$$\begin{aligned}y_{\mathsf{RE}_k} &= \rho_{\mathtt{ZF}}\mathbf{g}_{\mathsf{RE},k}^T\left[\hat{\mathbf{G}}_{\mathsf{RD}}^*\left(\hat{\mathbf{G}}_{\mathsf{RD}}^T\hat{\mathbf{G}}_{\mathsf{RD}}^*\right)^{-1}\right]_k x_k+\\ &\quad\rho_{\mathtt{ZF}}\sum_{i\neq k}^K\mathbf{g}_{\mathsf{RE},k}^T\left[\hat{\mathbf{G}}_{\mathsf{RD}}^*\left(\hat{\mathbf{G}}_{\mathsf{RD}}^T\hat{\mathbf{G}}_{\mathsf{RD}}^*\right)^{-1}\right]_i x_i+n_{\mathsf{E}_k},\\ &= \mathbf{g}_{\mathsf{RE},k}^T\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_k x_k+\sum_{i\neq k/}^K\mathbf{g}_{\mathsf{RE},k}^T\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_i x_i+n_{\mathsf{E}_k},\end{aligned} \tag{41}$$

where $\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_k \triangleq \left[\hat{\mathbf{G}}_{\mathsf{RD}}^*\left(\hat{\mathbf{G}}_{\mathsf{RD}}^T\hat{\mathbf{G}}_{\mathsf{RD}}^*\right)^{-1}\right]_k$. Note that the received signal at E_k is presented to be similar to one at D_k in the proof of Theorem 3. Therefore, the acquired eavesdropper rate at E_k is given by

$$\begin{aligned}\mathscr{R}_{\mathsf{E}_k}^{\mathtt{ZF}} = \frac{1}{2}\log_2\left(1+\min\left\{(N-K)P_{\mathsf{S}}\sigma_{\mathsf{BR}}^2,\right.\right.\\ \left.\left.\frac{\rho_{\mathtt{ZF}}^2\left|\mathbf{g}_{\mathsf{RE},k}^T\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_k\right|^2}{\rho_{\mathtt{ZF}}^2\left|\sum_{i\neq k}^K\mathbf{g}_{\mathsf{RE},k}^T\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_i\right|^2+1}\right\}\right).\end{aligned} \tag{42}$$

The secrecy outage rate at D_k is derived in Theorem 4 by using the approach like MRC/MRT.

Theorem 4. *Subject to a predefined outage secrecy probability, ζ, the secrecy outage rate of D_k in* ZFR/ZFT *of the massive MIMO DF relay network under $N > \left(K+\frac{1}{P_{\mathsf{S}}\sigma_{\mathsf{BR}}^2\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i\neq k}^K\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}\right)$, can be given by*

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{ZF}} = \mathscr{R}_{\mathsf{D}_k}^{\mathtt{ZF}} - \mathscr{R}_{\mathtt{OE}_k}^{\mathtt{ZF}}(\zeta), \tag{43}$$

where $\mathscr{R}_{\mathtt{OE}_k}^{\mathtt{ZF}}(\zeta)$ is obtained as in (44) *shown at the top of the next page.*

Proof. See Appendix D. □

Remark 1. *It is found that the achievable rates in Theorem 1 and 3 are also valid for traditional MIMO systems. However, achieved their bounds in massive MIMO systems are tighter than that in traditional MIMO systems since the central theorem is performed to approximate the effective noise in both phases.*

$$\mathscr{R}_{\mathtt{OE}_k}^{\mathtt{MRC}}(\zeta) \triangleq \frac{1}{2}\log_2\left(\frac{N\sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2 - \left(P_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\hat{\sigma}_{\mathsf{RD},k}^2 + P_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\sum_{i\neq k}^{K}\hat{\sigma}_{\mathsf{RD},i}^2\right)\log\zeta}{N\sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2 - P_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\sum_{i\neq k}^{K}\hat{\sigma}_{\mathsf{RD},i}^2\log\zeta}\right). \tag{39}$$

$$\mathscr{R}_{\mathsf{D}_k}^{\mathtt{ZF}} = \frac{1}{2}\log_2\left(1+\min\left\{(N-K)P_{\mathsf{S}}\sigma_{\mathsf{BR}}^2, \frac{(N-K)P_{\mathsf{R}}\hat{\sigma}_{\mathsf{RD},k}^2}{P_{\mathsf{R}}\sum_{i=1}^{K}\sigma_{e,i}^2 + \hat{\sigma}_{\mathsf{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}\right\}\right). \tag{40}$$

Remark 2. *Based on the effective multiuser interference suppressing capability of* ZFR/ZFT *technique in relaying systems, the achievable rate on the* $\mathsf{BS}\to\mathsf{R}\to\mathsf{D}_k$ *transmission link is better than that for* MRC/MRT.

Remark 3. *Satisfying constraint conditions in Theorem 2 and 4 is easy by more increasing a number of* N *antennas at* R. *It implies that the signal processing systems are proposed with low-complexity, and concurrently the secrecy outage rate can be improved due to the very large number of relay antennas.*

Therefore, the secrecy outage rate should be considered in the regime of very large N to enhance the spectral efficiency, namely to improve the secure downlink transmission in multi-antenna MIMO relaying systems in the presence of eavesdroppers. In addition, the joint utilization of massive MIMO and relay can fully exploit another benefit as cutting down transmit power at the BS and relay without compromising the system performance, which is shown by the following section.

4. ASYMPTOTIC ANALYSIS WITH MASSIVE ARRAYS

With the advantage of increasing a number of N antennas at R, this section will investigate in the asymptotic analysis scenarios to provide insights into the system characteristics. Specifically, when $N\to\infty$ with fixed total transmit power of E_{S} and E_{R}, i.e., $P_{\mathsf{S}}=\frac{E_{\mathsf{S}}}{N^{\alpha}}$, $P_{\mathsf{R}}=\frac{E_{\mathsf{R}}}{N^{\beta}}$ with $\alpha,\beta\in[0,1]$. $\mathscr{R}_{\mathtt{OSE}_k}^{\mathcal{A}}$ with $\mathcal{A}\in\{\mathtt{MRC},\mathtt{ZF}\}$ can be re-expressed, respectively, as

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathcal{A},\infty} = \mathscr{R}_{\mathsf{D}_k}^{\mathcal{A},\infty} - \mathscr{R}_{\mathtt{OE}_k}^{\mathcal{A},\infty}(\zeta), \tag{45}$$

where $\mathscr{R}_{\mathsf{D}_k}^{\mathcal{A},\infty}$ and $\mathscr{R}_{\mathtt{OE}_k}^{\mathcal{A},\infty}(\zeta)$ are given in (46) and (47) for MRC and (48) and (49) for ZF, respectively, with $e_{\mathtt{M}}=\sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2$, $f_{\mathtt{M}}=-E_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\hat{\sigma}_{\mathsf{RD},k}^2\log\zeta$, $h_{\mathtt{M}}=-E_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\sum_{i\neq k}^{K}\hat{\sigma}_{\mathsf{RD},i}^2\log\zeta$, $e_{\mathtt{Z}}=\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}$, $f_{\mathtt{Z}}=-E_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\log\zeta$, and $e_{\mathtt{Z}}=-E_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i\neq k}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}\log\zeta$.

$$\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}} = \frac{1}{2}\log_2\left(1+\min\left(\frac{NE_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KE_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+N^{\alpha}}, \frac{NE_{\mathsf{R}}\hat{\sigma}_{\mathsf{RD},k}^4}{\left[E_{\mathsf{R}}\left(\hat{\sigma}_{\mathsf{RD},k}^2+\sigma_{e,k}^2\right)+N^{\beta}\right]\sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2}\right)\right), \tag{46}$$

$$\mathscr{R}_{\mathtt{OE}_k}^{\mathtt{MRC}}(\zeta) = \frac{1}{2}\log_2\left(\frac{N^{(1-\beta)}e_{\mathtt{M}}+f_{\mathtt{M}}+h_{\mathtt{M}}}{N^{(1-\beta)}e_{\mathtt{M}}+h_{\mathtt{M}}}\right), \tag{47}$$

and

$$\mathscr{R}_{\mathsf{D}_k}^{\mathtt{ZF}} = \frac{1}{2}\log_2\left(1+\min\left(\frac{(N-K)E_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{N^{\alpha}}, \frac{(N-K)E_{\mathsf{R}}\hat{\sigma}_{\mathsf{RD},k}^2}{E_{\mathsf{R}}\sum_{i=1}^{K}\sigma_{e,i}^2+N^{\beta}\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}\right)\right), \tag{48}$$

$$\mathscr{R}_{\mathtt{OE}_k}^{\mathtt{ZF}}(\zeta) = \frac{1}{2}\log_2\left(\frac{N^{\beta}e_{\mathtt{Z}}+f_{\mathtt{Z}}+h_{\mathtt{Z}}}{N^{\beta}e_{\mathtt{Z}}+h_{\mathtt{Z}}}\right), \tag{49}$$

From (46) and (48), it shows that α and β should be chosen in the interval $[0,1]$ for non-vanishing $\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC/ZF}}$ as $N\to\infty$. Because, if we choose α and/or $\beta>1$, $\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC/ZF}}$ may be zero. Therefore, we now consider the asymptotic achievable rate and secrecy outage rate of the transmission link $\mathsf{BS}\to\mathsf{R}\to\mathsf{D}_k$ as $N\to\infty$ in some following special cases. More explicitly, selected factor pairs, (α,β), are at high bound of $[0,1]$, i.e., $\alpha=1$ and/or $\beta=1$, and in the interval $(0,1)$, i.e., $\alpha=1/2$ and/or $\beta=1/2$.

https://doi.org/10.52111/qnjs.2021.16307

$$\mathbf{R}_{\mathtt{OE}_k}^{\mathtt{ZF}}(\zeta) \triangleq \frac{1}{2}\log_2\left(\frac{\hat{\sigma}_{\mathtt{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2} - \left(P_{\mathsf{R}}\sigma_{\mathtt{RE},k}^2 + P_{\mathsf{R}}\sigma_{\mathtt{RE},k}^2\hat{\sigma}_{\mathtt{RD},k}^2\sum_{i\neq k}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2}\right)\log\zeta}{\hat{\sigma}_{\mathtt{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2} - P_{\mathsf{R}}\sigma_{\mathtt{RE},k}^2\hat{\sigma}_{\mathtt{RD},k}^2\sum_{i\neq k}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2}\log\zeta}\right). \quad (44)$$

Proposition 1. *When the number of N antennas at the relay approaches infinity, the secrecy outage rate of the transmission link $\mathsf{BS}\to\mathsf{R}\to\mathsf{D}_k$ for $\mathtt{MRC}/\mathtt{MRT}$ and $\mathtt{ZFT}/\mathtt{ZFR}$ in some cases can be asymptotically approximated, respectively, as follows:*

- *Case 1: α and β are chosen at bound to be equal to one in several cases as follows:*

- *Case 1.1:* $(\alpha,\beta)=(1,1)$ *i.e.,* $(P_{\mathsf{S}}=\frac{E_{\mathsf{S}}}{N}, P_{\mathsf{R}}=\frac{E_{\mathsf{R}}}{N})$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC},\infty} = \frac{1}{2}\log_2\left(1+\min\left(E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2, \frac{E_{\mathsf{R}}\hat{\sigma}_{\mathtt{RD},k}^4}{\sum_{i=1}^{K}\hat{\sigma}_{\mathtt{RD},i}^2}\right)\right) - \frac{1}{2}\log_2\left(\frac{e_{\mathtt{M}}+f_{\mathtt{M}}+h_{\mathtt{M}}}{e_{\mathtt{M}}+h_{\mathtt{M}}}\right), \quad (50)$$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{ZF},\infty} = \frac{1}{2}\log_2\left(1+\min\left(E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2, \frac{E_{\mathsf{R}}}{\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2}}\right)\right). \quad (51)$$

- *Case 1.2:* $(\alpha,\beta)=(0,1)$ *i.e.,* $(P_{\mathsf{S}}=E_{\mathsf{S}}, P_{\mathsf{R}}=\frac{E_{\mathsf{R}}}{N})$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC},\infty} = \frac{1}{2}\log_2\left(1+\frac{E_{\mathsf{R}}\hat{\sigma}_{\mathtt{RD},k}^4}{\sum_{i=1}^{K}\hat{\sigma}_{\mathtt{RD},i}^2}\right) - \frac{1}{2}\log_2\left(\frac{e_{\mathtt{M}}+f_{\mathtt{M}}+h_{\mathtt{M}}}{e_{\mathtt{M}}+h_{\mathtt{M}}}\right), \quad (52)$$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{ZF},\infty} = \frac{1}{2}\log_2\left(1+\frac{E_{\mathsf{R}}}{\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2}}\right). \quad (53)$$

- *Case 1.3:* $(\alpha,\beta)=(1,0)$ *i.e.,* $(P_{\mathsf{S}}=\frac{E_{\mathsf{S}}}{N}, P_{\mathsf{R}}=E_{\mathsf{R}})$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC},\infty} = \frac{1}{2}\log_2\left(1+E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2\right), \quad (54)$$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{ZF},\infty} = \frac{1}{2}\log_2\left(1+E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2\right) - \frac{1}{2}\log_2\left(\frac{e_{\mathtt{Z}}+f_{\mathtt{Z}}+h_{\mathtt{Z}}}{e_{\mathtt{Z}}+h_{\mathtt{Z}}}\right). \quad (55)$$

- *Case 2: α and β are chosen in the interval $(0,1)$. We choose $\alpha=1/2$ and/or $\beta=1/2$ in several cases as follows:*

- *Case 2.1:* $(\alpha,\beta)=(1/2,1/2)$ *i.e.,* $(P_{\mathsf{S}}=\frac{E_{\mathsf{S}}}{\sqrt{N}}, P_{\mathsf{R}}=\frac{E_{\mathsf{R}}}{\sqrt{N}})$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC},\infty} = \frac{1}{2}\log_2\left(1+\min\left(\sqrt{N}E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2, \frac{\sqrt{N}E_{\mathsf{R}}\hat{\sigma}_{\mathtt{RD},k}^4}{\sum_{i=1}^{K}\hat{\sigma}_{\mathtt{RD},i}^2}\right)\right), \quad (56)$$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{ZF},\infty} = \frac{1}{2}\log_2\left(1+\min\left(\sqrt{N}E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2, \frac{\sqrt{N}E_{\mathsf{R}}}{\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2}}\right)\right). \quad (57)$$

- *Case 2.2:* $(\alpha,\beta)=(0,1/2)$ *i.e.,* $(P_{\mathsf{S}}=E_{\mathsf{S}}, P_{\mathsf{R}}=\frac{E_{\mathsf{R}}}{\sqrt{N}})$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC},\infty} = \frac{1}{2}\log_2\left(1+\frac{\sqrt{N}E_{\mathsf{R}}\hat{\sigma}_{\mathtt{RD},k}^4}{\sum_{i=1}^{K}\hat{\sigma}_{\mathtt{RD},i}^2}\right), \quad (58)$$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{ZF},\infty} = \frac{1}{2}\log_2\left(1+\frac{\sqrt{N}E_{\mathsf{R}}}{\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathtt{RD},i}^2}}\right). \quad (59)$$

- *Case 2.3:* $(\alpha,\beta)=(1,0)$ *i.e.,* $(P_{\mathsf{S}}=\frac{E_{\mathsf{S}}}{\sqrt{N}}, P_{\mathsf{R}}=E_{\mathsf{R}})$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC},\infty} = \frac{1}{2}\log_2\left(1+\sqrt{N}E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2\right), \quad (60)$$

$$\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{ZF},\infty} = \frac{1}{2}\log_2\left(1+\sqrt{N}E_{\mathsf{S}}\sigma_{\mathtt{BR}}^2\right) - \frac{1}{2}\log_2\left(\frac{e_{\mathtt{Z}}+f_{\mathtt{Z}}+h_{\mathtt{Z}}}{e_{\mathtt{Z}}+h_{\mathtt{Z}}}\right). \quad (61)$$

$$\mathscr{R}_{\mathrm{D}_k}^{\mathrm{ZF}} = \frac{1}{2}\log_2\left(1+\min\left(\frac{(N-K)E_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{N}, \frac{(N-K)E_{\mathsf{R}}\hat{\sigma}_{\mathsf{RD},k}^2}{E_{\mathsf{R}}\sum_{i=1}^{K}\sigma_{e,i}^2 + N\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}\right)\right), \tag{62}$$

$$\mathscr{R}_{\mathrm{OE}_k}^{\mathrm{ZF}}(\zeta) = \frac{1}{2}\log_2\left(\frac{N\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2} - \left(\sigma_{\mathsf{RE},k}^2 + \sigma_{\mathsf{RE},k}^2\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i\neq k}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}\right)E_{\mathsf{R}}\log\zeta}{N\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2} - E_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\hat{\sigma}_{\mathsf{RD},k}^2\sum_{i\neq k}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}\log\zeta}\right). \tag{63}$$

Proof. We first consider Case 1.1 by rewriting (48) and (49) with $P_{\mathsf{S}} = E_{\mathsf{S}}/N, P_{\mathsf{R}} = E_{\mathsf{S}}/N$, as in (62) and (63) shown at the top of the next page. The desired result as in (50) and (51) can be readily obtained by the property of $\log_2(1) = 0$ as $N \to \infty$. Other cases are omitted due to having the similar proof way. □

Remark 4. *Proposition 1 shows that, in the regime of very large relay antennas associating with either* MRC/MRT *or* ZFR/ZFT *technique at the relay, the transmit powers at both the* BS *and* R *in Case 1 and Case 2 will be scaled by factor* $1/N$ *and* $1/\sqrt{N}$*, respectively. As a result, the deterministic asymptotic expression of* $\mathscr{R}_{\mathrm{OSE}_k}^{\mathrm{MRC/ZF}}$ *is derived as* $N \to \infty$ *in all cases. In addition, the acquired rate of the* k*-th eavesdropper in almost cases is average out due to the law of large numbers, i.e.,* $\mathscr{R}_{\mathrm{OE}_k}^{\mathrm{MRC/ZF}} \to 0$*, except some cases as Case 1.1 and 1.2 for* MRC/MRT*, Case 1.3 and 2.3 for* ZFR/ZFT *go to a constant value as* $N \to \infty$*. Thus, to obtain the effectiveness against eavesdropper, Case 2 should be adopted into the massive MIMO DF relaying system.*

5. NUMERICAL RESULTS

In this section, we will assess the secure performance under different consideration by employing Monte-Carlo simulations. Most of the simulation cases, we set $\zeta = 0, 1$, $\sigma_{e,i}^2 = 0.1$, $K = 10$, and $P_{\mathsf{S}} = P_{\mathsf{R}} = 10$ dB, where the signal-to-noise ratio (SNR) is defined by either $\mathrm{SNR}_{\mathsf{S}} = 10\log_{10} P_{\mathsf{S}}$ or $\mathrm{SNR}_{\mathsf{R}} = 10\log_{10} P_{\mathsf{R}}$ to represent different transmit SNRs in dB at either BS or R, respectively. Moreover, we will take the path-loss effect of $\sigma_{\mathsf{RE},k}$ when its value is adjusted, and of σ_{BR} is normalized, i.e., $\sigma_{\mathsf{BR}} = 1$.

Figures 2 and 3 illustrate secure performance of both MRC/MRT and ZFR/ZFT processing techniques at the

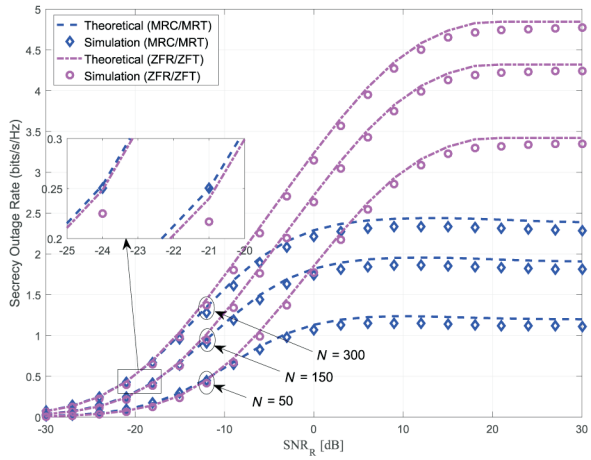

Figure 2. Secrecy outage rate versus P_{R} with $\sigma_{RE,k} = 1$ and $P_{\mathsf{S}} = 10$ dB.

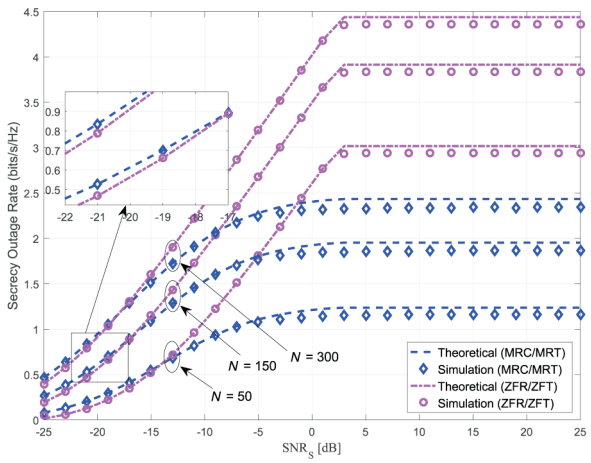

Figure 3. Secrecy outage rate versus P_{S} with $\sigma_{RE,k} = 1$ and $P_{\mathsf{R}} = 10$ dB.

https://doi.org/10.52111/qnjs.2021.16307

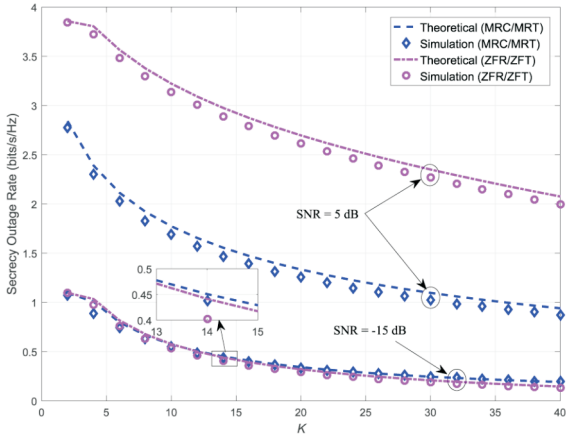

Figure 4. Secrecy outage rate versus number of destinations with $\sigma_{\mathsf{E},k} = 1, \text{SNR} = P_{\mathsf{S}} = P_{\mathsf{R}}$ and $N = 120$.

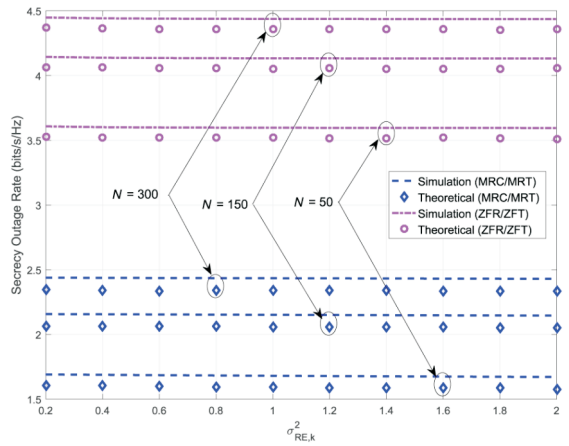

Figure 5. Effect of N on secrecy outage rate with $P_{\mathsf{S}} = P_{\mathsf{R}} = 10$ dB and $\zeta = 0.1$

relay, for the same target secure outage probability ζ by varying different transmit SNR_{R} with fixed P_{S} corresponding Figure 2 and different transmit SNR_{S} with fixed P_{R} corresponding Figure 3. In Figures 2 and 3, the secrecy outage rate will be improved by increasing either P_{R} or P_{S} increases at low SNR regime but it rapidly approaches to a saturated level, which is determined by network settings. However, when the secrecy outage rate is considered in three cases of N, i.e., $N = 50, N = 150$ and $N = 300$, it can see that increasing a number of N relay antennas can enhance the system outage rate for all range of SNRs and processing technique used at the relay. As a result, there are the following two distinguished regions. The secrecy outage rate for MRC/MRT outferforms that for ZFR/ZFT at low SNR regime. Whereas, the achieved secrecy outage rate for ZFR/ZFT within high SNR regime is better. It is due to the fact that, at high regime, the effect of multiuser interference for the MRC/MRT scheme is larger than that for ZFR/ZFT, while the system for ZFR/ZFT is able to null multiuser interference signals,[6] i.e., multiuser interference is not completely canceled out in MRC/MRT but nulled by projecting each stream onto the orthogonal complement in ZFR/ZFT scheme.

In Figure 4, the secrecy outage rate is investigated under two typical network settings, i.e., Case 1: $\text{SNR} = P_{\mathsf{S}} = P_{\mathsf{R}} = -15$ dB and Case 2: $\text{SNR} = P_{\mathsf{S}} = P_{\mathsf{R}} = 5$ dB, when we adjust a number of destinations, K. It can see that MRC/MRT outperforms ZFR/ZFT in Case 1 but not the same in Case 2, which is consistent with the numerical results in Figure 2 and 3. Because the multiuser interference of the transmission link $\mathsf{BS} \to \mathsf{R} \to \mathsf{D}_k$ within low SNR is very small, due to being inversely proportional to the number of antennas. However, within high regimes of SNR, the multiuser interference is large enough, resulting in secrecy outage rate for MRC/MRT is inferior.

In Figure 5, the transmit power at the source and the relay are fixed by 10 dB, i.e., $P_{\mathsf{S}} = P_{\mathsf{R}} = 10$ dB and $\zeta = 0.1$. The effect of eavesdropper links is investigated by comparing the secrecy outage rate with different values of $\sigma_{\mathsf{RE},k}$. It can be seen in Figure 5 that, for a given outage probability bound ζ, ZFR/ZFT can derive better secrecy outage rate than MRC/MRT, which confirms the advantage of the ZFR/ZFT scheme over the MRC/MRT within moderate to high SNR region. Moreover, the secrecy outage rate is considered in three cases of N, i.e., $N = 100$, $N = 200$, and $N = 300$, with the same effect of $\sigma_{\mathsf{RE},k}$. Results shows that increasing the number of antennas's N at R provides us an effective method to improve the achieved secrecy outage rate. On the other hand, the MRC/MRT and ZFR/ZFT are not so sensitive to short-distance eavesdropper, which shows us that the capability of both linear processing techniques against passive eavesdropper at short-distance is fairly good.

In the two figures of Figures 6 and 7, we illustrate the system secure performance when N approaches infinity in some power-scaling laws of Case 1, and 2, as addressed in Proposition 1. As expected, all asymptotic secrecy outage rates are in good agreements with the upper bound in Case 1 and the enhancement of rate of OSE_K $\left(\mathscr{R}_{\text{OSE}_k}^{\text{MRC/ZF}}\right)$ in Case 2 at high regime

https://doi.org/10.52111/qnjs.2022.16307

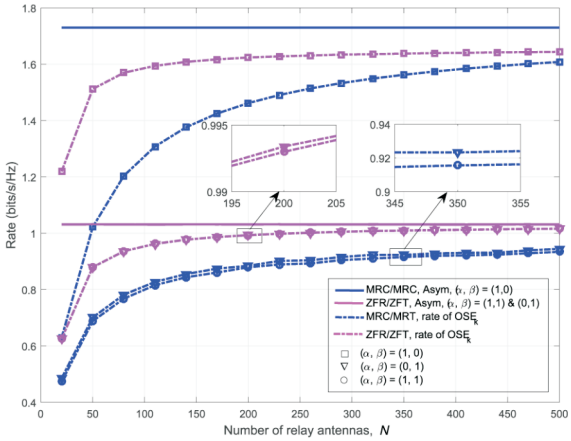

Figure 6. Secrecy rate comparison of MRC/MRT and ZFR/ZFT relaying schemes versus N in Case 1 of power scaling law with $E = E_{\mathsf{S}} = E_{\mathsf{R}} = 10$ dB and $\zeta = 0.1$.

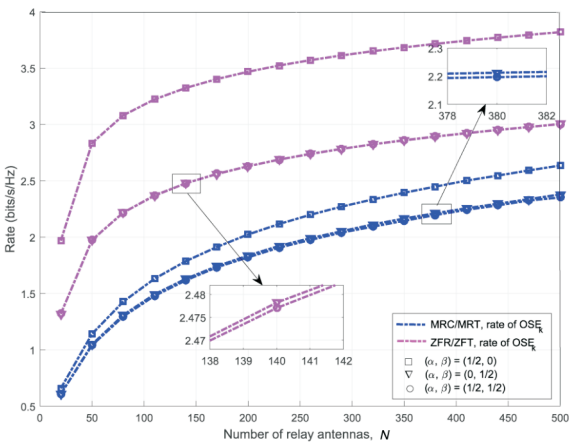

Figure 7. Secrecy outage rate comparison of MRC/MRT and ZFR/ZFT relaying schemes versus N in Case 2 of power scaling law with $E = E_{\mathsf{S}} = E_{\mathsf{R}} = 10$ dB and $\zeta = 0.1$.

of N. The advantage of ZFR/ZFT over MRC/MRT is also verified. For example, ZFR/ZFT can provide secrecy outage rate of 1.4 bits/s/Hz with $N = 40$ while $N = 150$ is required for MRC/MRT in Figure 6. Moreover, it can be seen in Figures 6 and 7 that, using both linear processing methods in Cases 1.3 and 2.3, i.e., $(\alpha, \beta) = (1, 0)$ and $(\alpha, \beta) = (1/2, 0)$ respectively, there is the best $\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC/ZF}}$ compared to other cases of Case 1, i.e., $\left[(\alpha, \beta) = (1, 1); (\alpha, \beta) = (1, 0)\right]$ and

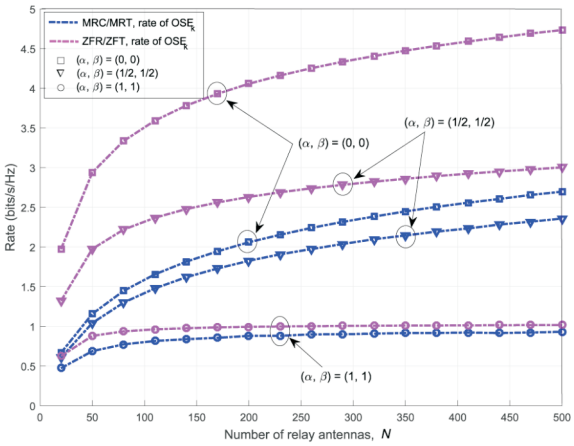

Figure 8. Secrecy outage rate of MRC/MRT and ZFR/ZFT relaying schemes versus N in Theorem 2, Theorem 4, Case 1.1 and Case 2.1 of power scaling law with $E = E_{\mathsf{S}} = E_{\mathsf{R}} = 10$ dB and $\zeta = 0.1$.

that of Case 2, i.e., $\left[(\alpha, \beta) = (1/2, 1/2); (\alpha, \beta) = (1/2, 0)\right]$ respectively, which proves that allocating transmit power at R also has significantly effect on the secrecy outage rate. Meanwhile, there is a gap of $\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC/ZF}}$ between Case 1.1 and Case 1.2 or Case 2.1 and Case 2.2 being very small in Figure 6 or 7, respectively.

Furthermore, we can see that, the effective improvement of $\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC/ZF}}$ according to Theorems 2 and 4, i.e., $(\alpha, \beta) = (0, 0)$, is the best when comparing to Cases 1.1 and 2.1 i.e., $(\alpha, \beta) = (1/2, 1/2)$ and $(\alpha, \beta) = (1, 1)$ respectively, as illustrated in Figure 8. However, reductive capability of transmit power at BS and R in case of $(\alpha, \beta) = (0, 0)$ hasn't ability. In Case 1.1 with $(\alpha, \beta) = (1, 1)$, the transmit power cutdown at BS and R is the best by inversely proportional to the number of antennas, $1/N$, but $\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC/ZF}}$ in this case is small since it rapidly approaches to a saturated level in spite of increasing $N \to \infty$. Fortunately, Case 2.1 with $(\alpha, \beta) = (1/2, 1/2)$ shows that the transmit power at BS and R can be scaled by factor $1/\sqrt{N}$ and concurrently improving the effective $\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC/ZF}}$ as more increasing N in Figure 8. From above analyses, it allows us chose effective relaying schemes based on given secure requirement of system performance.

https://doi.org/10.52111/qnjs.2021.16307

6. CONCLUSION

In this paper, we have introduced a secure multiuser transmission downlink based on massive MIMO DF relaying strategy, in which both MRC/MRT and ZFR/ZFT techniques are adopted into physical layer security. As a result, the exact and asymptotic expressions for user rate and outage secrecy rate for a predetermined secure outage probability of eavesdropper links with CSI imperfection are derived. We then have focused on the analysis and comparison of secrecy outage rate expressions in terms of SNRs, different number of users, number of antennas and eavesdropper distance. It is shown that, ZFR/ZFT processing technique at relay provides a better choice than the MRC/MRT based one in terms of the achieved secrecy performance. It is noteworthy that, information leakage prevention in all cases is quite good regardless of passive eavesdroppers located a short-distance from the relay. Since we can observe that passive eavesdroppers have less effect on secrecy rate when multiple-antenna MIMO relaying techniques are adopted. Specifically, the acquired rate of an eavesdropper diminishes to zero when asymptotic analysis is considered in various scenarios. In particular, the MIMO DF relaying system based on the large antenna array gain can balance between the achievable secrecy outage rate and effective decreased transmit power at the relay and BS. These results provide some useful insights to assist the design of massive MIMO relaying schemes for secure information transmission.

7. APPENDIX

A. Proof of Theorem 1

In this appendix, Theorem 1 is proved to achieve the rate of the transmission link $\mathsf{BS} \to \mathsf{R} \to \mathsf{D}_k$. Based on MRC/MRT, the expression (16) is rewritten as

$$\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}} = \frac{1}{2}\log_2\left(1+\min\left(\gamma_{\mathsf{RB}_k}^{\mathtt{MRC}}, \gamma_{\mathsf{RD}_k}^{\mathtt{MRC}}\right)\right), \quad (64)$$

From (64), we first need to calculate $\gamma_{\mathsf{RB}_k}^{\mathtt{MRC}}$, including four terms, i.e., $\mathbb{E}\left\{\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right\}$, $\mathrm{Var}\left(\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right)$, IS_k, and NR_k, as follows:
We derive $\mathbb{E}\left\{\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right\}$ by using MRC with $\mathbf{A}^T = \mathbf{G}_{\mathsf{BR}}^H$ as

$$\mathbb{E}\left\{\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right\} = \mathbb{E}\left\{\left\|\mathbf{g}_{\mathsf{BR},k}\right\|^2\right\} \approx N\sigma_{\mathsf{BR}}^2. \quad (65)$$

We are now to achieve $\mathrm{Var}\left(\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right)$, which is rewritten after using (65) as

$$\begin{aligned}\mathrm{Var}\left(\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right) &= \mathbb{E}\left\{\left|\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right|^2\right\} - N^2\sigma_{\mathsf{BR}}^4,\\ &= \mathbb{E}\left\{\left\|\mathbf{g}_{\mathsf{BR},k}\right\|^4\right\} - N^2\sigma_{\mathsf{BR}}^4. \quad (66)\end{aligned}$$

By applying [34, Lemma 2.9], we have

$$\begin{aligned}\mathrm{Var}\left(\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},k}\right) &= N(N+1)\sigma_{\mathsf{BR}}^4 - N^2\sigma_{\mathsf{BR}}^4,\\ &= N\sigma_{\mathsf{BR}}^4. \quad (67)\end{aligned}$$

We derive the third term, i.e., IS_k, by re-expressing it as follows:

$$\begin{aligned}\mathbb{E}\left\{\left|\mathbf{a}_k^T\mathbf{g}_{\mathsf{BR},i}\right|^2\right\} &= \sum_{i\neq k}^{K}\mathbb{E}\left\{\left|\mathbf{g}_{\mathsf{BR},k}^H\mathbf{g}_{\mathsf{BR},i}\right|^2\right\},\\ &= N(K-1)\sigma_{\mathsf{BR}}^4. \quad (68)\end{aligned}$$

In a similar way, we obtain NR_k as

$$\begin{aligned}\mathsf{NR}_k &= \mathbb{E}\left\{\left|\mathbf{g}_{\mathsf{BR},k}^T\mathbf{n}_{\mathsf{R}}\right|^2\right\},\\ &= N\sigma_{\mathsf{BR}}^2. \quad (69)\end{aligned}$$

Substituting (65), (67), (68), and (69) into (29), we obtain the result of $\gamma_{\mathsf{BR}_k}^{\mathtt{MRC}}$ as

$$\gamma_{\mathsf{BR}_k}^{\mathtt{MRC}} = \frac{NP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1}. \quad (70)$$

Next, we derive a approximated expression SINR of the transmission link $\mathsf{R} \to \mathsf{D}_k$, by following the same calculative way in the first phase above. As a result, we have

$$\gamma_{\mathsf{RD}_k}^{\mathtt{MRC}} = \frac{NP_{\mathsf{R}}\hat{\sigma}_{\mathsf{RD},k}^4}{\left[P_{\mathsf{R}}\left(\hat{\sigma}_{\mathsf{RD},k}^2+\sigma_{e,k}^2\right)+1\right]\sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2}. \quad (71)$$

From (70) and (71), we finally obtain (35) in Theorem 1.

B. Proof of Theorem 2

We will prove Theorem 2 from starting (19), hence, the inverse CDF of γ_{E_k} is needed. We first need to calculate the SINR expression of $\gamma_{\mathsf{RE}_k}^{\mathtt{MRC}}$ (36) in terms of $\left|\mathbf{g}_{\mathsf{RE},k}^T\hat{\mathbf{g}}_{\mathsf{RD},k}^*\right|^2$ and $\sum_{i\neq k}^{K}\left|\mathbf{g}_{\mathsf{RE},k}^T\hat{\mathbf{g}}_{\mathsf{RD},i}^*\right|^2$ with MRT beamforming, $\mathbf{B} = \mathbf{B}_{\mathtt{MRC}} \triangleq \rho_{\mathtt{MRC}}\hat{\mathbf{G}}_{\mathsf{RD}}^*$.

For $\left|\mathbf{g}_{\mathsf{RE},k}^T\hat{\mathbf{g}}_{\mathsf{RD},k}^*\right|^2$, we have

$$\begin{aligned}\left|\mathbf{g}_{\mathsf{RE},k}^T\mathbf{b}_k\right|^2 &= \left|\mathbf{g}_{\mathsf{RE},k}^T\hat{\mathbf{g}}_{\mathsf{RD},k}^*\right|^2,\\ &= \left\|\mathbf{g}_{\mathsf{RE},k}\right\|^2\rho_{\mathtt{MRC}}^2\hat{\sigma}_{\mathsf{RE},k}^2. \end{aligned} \quad (72)$$

Similarly, we also have

$$\begin{aligned}\sum_{i\neq k}^{K}\left|\mathbf{g}_{\mathsf{RE},k}^T\mathbf{b}_i\right|^2 &= \sum_{i\neq k}^{K}\left|\mathbf{g}_{\mathsf{RE},k}^T\hat{\mathbf{g}}_{\mathsf{RD},i}^*\right|^2,\\ &= \left\|\mathbf{g}_{\mathsf{RE},k}\right\|^2\rho_{\mathtt{MRC}}^2\sum_{i\neq k}^{K}\hat{\sigma}_{\mathsf{RD},i}^2. \end{aligned} \quad (73)$$

Substituting (72) and (73) and into (36), the achievable rate of the eavesdropper channel $\mathsf{BS}\rightarrow\mathsf{R}\rightarrow\mathsf{E}_k$ is

$$\mathscr{R}_{\mathsf{E}_k}^{\mathtt{MRC}} = \log_2\left(1+\min\left(\frac{NP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1}, \frac{\left\|\mathbf{h}_{\mathsf{RE},k}\right\|^2 b}{\left\|\mathbf{h}_{\mathsf{RE},k}\right\|^2 c+Nd}\right)\right), \quad (74)$$

where $\mathbf{g}_{\mathsf{RE},k} = \sqrt{\eta_{\mathsf{RE},k}}\mathbf{h}_{\mathsf{RE},k}$ with $\eta_{\mathsf{RE},k}$ being distance-dependent path-loss attenuation with the value of one denoted by $\sigma_{\mathsf{RE},k}^2$, $b = P_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\hat{\sigma}_{\mathsf{RD},k}^2$, $c = P_{\mathsf{R}}\sigma_{\mathsf{RE},k}^2\sum_{i\neq k}^{K}\hat{\sigma}_{\mathsf{RD},i}^2$, and $d = \sum_{i=1}^{K}\hat{\sigma}_{\mathsf{RD},i}^2$.
From (74), we can rewrite the expression (19) as in (75) shown at the top of the next page. Next, it notes that we can simplify the expression (75) based on the characteristic of network setting by using advantage of large antenna arrays at R. Specifically, making $\gamma_{\mathsf{BR},k}^{\mathtt{MRC}}$ is always greater than $\gamma_{\mathsf{RE},k}^{\mathtt{MRC}}$ if $C1: N > \frac{\left(KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1\right)\hat{\sigma}_{\mathsf{RD},k}^2}{P_{\mathsf{S}}\sigma_{\mathsf{BR}}^2\sum_{i\neq k}^{K}\hat{\sigma}_{\mathsf{RD},i}^2}$. Consequently, we have

$$\zeta = \Pr\left(\frac{\left\|\mathbf{h}_{\mathsf{RE},k}\right\|^2 b}{\left\|\mathbf{h}_{\mathsf{RE},k}\right\|^2 c+Nd} > 2^{2\left(\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}}-\mathscr{R}_{\mathtt{OSE}_k}^{\mathtt{MRC}}\right)}-1\right). \quad (76)$$

Having (76) at hands allows us to derive the the CDF of $\gamma_{\mathsf{E}_k}^{\mathtt{MRC}}$. Mathematically, we can write

$$F_{\gamma_{\mathsf{E}_k}}(\gamma) = \Pr\left(\frac{\left\|\mathbf{h}_{\mathsf{RE},k}\right\|^2 b}{\left\|\mathbf{h}_{\mathsf{RE},k}\right\|^2 c+Nd} < \gamma\right) \quad (77)$$

Over Rayleigh fading channels, $\left\|\mathbf{h}_{\mathsf{RE},k}\right\|^2$ is χ^2 distributed with 2 degrees of freedom, it is straightforward to arrive at

$$\begin{aligned}F_{\gamma_{\mathsf{E}_k}}(\gamma) &= \Pr\left(\left\|\mathbf{h}_{\mathsf{E},k}\right\|^2 < \frac{Nd\gamma}{b-c\gamma}\right),\\ &= 1-\exp\left(-\frac{Nd\gamma}{b-c\gamma}\right). \end{aligned} \quad (78)$$

resulting in $F_{\gamma_{\mathsf{E}_k}}^{-1}(\gamma)$ as

$$F_{\gamma_{\mathsf{E}_k}}^{-1}(\gamma) = \frac{Nd-(b+c)\log(1-\gamma)}{Nd-c\log(1-\gamma)}. \quad (79)$$

Combining (21) and (79), Theorem 2 is derive.

C. Proof of Theorem 3

Proof of Theorem 3 is starting from (16), in which the definition of the achievable rate of the transmission link $\mathsf{BR}\rightarrow\mathsf{R}\rightarrow\mathsf{D}_k$ is derived by using ZFR/ZFT. Hence, we need to calculate both $\gamma_{\mathsf{BR}_k}^{\mathtt{ZF}}$ and $\gamma_{\mathsf{RD}_k}^{\mathtt{ZF}}$ in two phases as follows:
Firstly, the k-th signal stream processed at R can be rewritten by recalling $\mathbf{A}_{\mathtt{ZF}}$ in (26) as in (80) shown at the top of the next page. where $\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k \triangleq \left[\left(\mathbf{G}_{\mathsf{BR}}^H\mathbf{G}_{\mathsf{BR}}\right)^{-1}\mathbf{G}_{\mathsf{BR}}^H\right]_k$.

The SINR at r_k due to no multiple signal stream interference, i.e., $\mathtt{IS}_k = 0$, can be rewritten as

$$\gamma_{\mathsf{D}_k}^{\mathtt{ZF}} \triangleq \frac{P_{\mathsf{S}}\left|\mathbb{E}\left\{\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k\mathbf{g}_{\mathsf{BR},k}\right\}\right|^2}{P_{\mathsf{S}}\mathrm{Var}\left(\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k\mathbf{g}_{\mathsf{BR},k}\right)+\mathtt{NR}_k}, \quad (81)$$

With property of ZF , we have $\mathbf{A}_{ZF}^T\mathbf{G}_{\mathsf{BR}} = \mathbf{I}_K$[5] resulting in $\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k\mathbf{g}_{\mathsf{BR},i} = \delta_{ki}$, where $\delta_{1,ki} = 1$ when $k = i$ and 0 otherwise. Therefore, we have

$$\mathbb{E}\left\{\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k\mathbf{g}_{\mathsf{BR},k}\right\} = 1. \quad (82)$$

From (82), the variance of $\left(\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k\mathbf{g}_{\mathsf{BR},k}\right)$ is given by

$$\mathrm{Var}\left(\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k\mathbf{g}_{\mathsf{BR},k}\right) = \mathbb{E}\left\{\left|\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k\mathbf{g}_{\mathsf{BR},k}\right|^2\right\}-1 = 0. \quad (83)$$

For $\mathtt{NR}_k$, we have

$$\begin{aligned}\mathtt{NR}_k &= \mathbb{E}\left\{\left|\mathbf{a}_k^T\mathsf{n}_{\mathsf{R}_k}\right|^2\right\},\\ &= \mathbb{E}\left\{\left|\left[\left(\mathbf{G}_{\mathsf{BR}}^H\mathbf{G}_{\mathsf{BR}}\right)^{-1}\mathbf{G}_{\mathsf{BR}}^H\right]_k\mathsf{n}_{R,k}\right|^2\right\},\\ &= \mathbb{E}\left\{\mathrm{Tr}\left(\left[\left(\mathbf{G}_{\mathsf{BR}}^H\mathbf{G}_{\mathsf{BR}}\right)^{-1}\right]_{kk}\right)\right\}. \end{aligned} \quad (84)$$

By using the identity of the book,[34] Lemma 2.10, we have

$$\mathtt{NR}_k = \frac{1}{(N-K)\sigma_{\mathsf{BR}}^2}. \quad (85)$$

$$\begin{aligned}\zeta &= \Pr\left(\mathscr{R}_{\mathsf{OSE}_k}^{\mathtt{MRC}} > \mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}} - \frac{1}{2}\log_2\left(1+\min\left(\gamma_{\mathsf{BR}_k}^{\mathtt{MRC}}, \gamma_{\mathsf{RE}_k}^{\mathtt{MRC}}\right)\right)\right),\\ &= \Pr\left(\frac{NP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1} \le \frac{\|\mathbf{h}_{\mathsf{RE},k}\|^2 b}{\|\mathbf{h}_{\mathsf{RE},k}\|^2 b + Nc}\right)\Pr\left(\frac{NP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1} > 2^{2\left(\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}} - \mathscr{R}_{\mathsf{OSE}_k}^{\mathtt{MRC}}\right)} - 1\right)\right.\\ &\left. + \Pr\left(\frac{NP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2}{KP_{\mathsf{S}}\sigma_{\mathsf{BR}}^2+1} > \frac{\|\mathbf{h}_{\mathsf{RE},k}\|^2 b}{\|\mathbf{h}_{\mathsf{RE},k}\|^2 c + Nd}\right)\Pr\left(\frac{\|\mathbf{h}_{\mathsf{RE},k}\|^2 b}{\|\mathbf{h}_{\mathsf{RE},k}\|^2 c + Nd} > 2^{2\left(\mathscr{R}_{\mathsf{D}_k}^{\mathtt{MRC}} - \mathscr{R}_{\mathsf{OSE}_k}^{\mathtt{MRC}}\right)} - 1\right)\right. . \qquad (75)\end{aligned}$$

$$\begin{aligned}\mathbf{r}_k &= \sqrt{P_{\mathsf{S}}}\left[\left(\mathbf{G}_{\mathsf{BR}}^H\mathbf{G}_{\mathsf{BR}}\right)^{-1}\mathbf{G}_{\mathsf{BR}}^H\right]_k \mathbf{g}_{\mathsf{BR},k}x_k\\ &+ \sqrt{P_{\mathsf{S}}}\sum_{i\neq k}^{K}\left[\left(\mathbf{G}_{\mathsf{BR}}^H\mathbf{G}_{\mathsf{BR}}\right)^{-1}\mathbf{G}_{\mathsf{BR}}^H\right]_k \mathbf{g}_{\mathsf{BR},i}x_i + \left[\left(\mathbf{G}_{\mathsf{BR}}^H\mathbf{G}_{\mathsf{BR}}\right)^{-1}\mathbf{G}_{\mathsf{BR}}^H\right]_k \mathsf{n}_{\mathsf{R}},\\ &= \sqrt{P_{\mathsf{S}}}\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k \mathbf{g}_{\mathsf{BR},k}x_k + \sqrt{P_{\mathsf{S}}}\sum_{i\neq k}^{K}\left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k \mathbf{g}_{\mathsf{BR},i}x_i + \left[\tilde{\mathbf{A}}_{\mathtt{ZF}}\right]_k \mathsf{n}_{\mathsf{R}}, \qquad (80)\end{aligned}$$

Substituting (82), (83), and (85) into (81), the achieved close-expression SINR of the k-th signal stream at R is obtained as

$$\gamma_{\mathsf{BR},k}^{\mathtt{ZF}} = (N-K)P_{\mathsf{S}}\sigma_{\mathsf{BR}}^2. \qquad (86)$$

Secondly, we derive a close-form expression SINR of the transmission link $\mathsf{R}\to\mathsf{D}_k$ by the above same way, namely,

$$\gamma_{\mathsf{RD}_k}^{\mathtt{ZF}} = \frac{(N-K)P_{\mathsf{R}}\hat{\sigma}_{\mathsf{RD},k}^2}{P_{\mathsf{R}}\sum_{i=1}^{K}\sigma_{e,i}^2 + \hat{\sigma}_{\mathsf{RD},k}^2\sum_{i=1}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}. \qquad (87)$$

From (86) and (87), we finally obtain (40), i.e., the proof of Theorem 3 is completed.

D. Proof of Theorem 4

To prove Theorem 4, we first compute $\gamma_{\mathsf{RE}_k}^{\mathtt{ZF}}$ from (42). With the help of the book,[34] Lemma 2.10, we obtain items as follows:
The received signal at E_k is

$$\begin{aligned}\left|\mathbf{g}_{\mathsf{RE},k}^T\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_k\right|^2 &= \rho_{\mathtt{ZF}}^2\mathbb{E}\left\{\left|\mathbf{g}_{\mathsf{RE},k}^T\left[\hat{\mathbf{G}}_{\mathsf{RD}}^*\left(\hat{\mathbf{G}}_{\mathsf{RD}}^T\hat{\mathbf{G}}_{\mathsf{RD}}^*\right)^{-1}\right]_k\right|^2\right\},\\ &= \|\mathbf{g}_{\mathsf{RE},k}\|^2\rho_{\mathtt{ZF}}^2\mathbb{E}\left\{\left[\left(\hat{\mathbf{G}}_{\mathsf{RD}}^T\hat{\mathbf{G}}_{\mathsf{RD}}^*\right)^{-1}\right]_{kk}\right\},\\ &\approx \frac{\|\mathbf{g}_{\mathsf{RE},k}\|^2\rho_{\mathtt{ZF}}^2}{\hat{\sigma}_{\mathsf{RD},k}^2}\frac{1}{N-K}. \qquad (88)\end{aligned}$$

For $\sum_{i\neq k}^{K}\mathbb{E}\left\{\left|\mathbf{g}_{\mathsf{RE},k}^T\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_i\right|^2\right\}$, we have

$$\begin{aligned}&\sum_{i\neq k}^{K}\mathbb{E}\left\{\left|\mathbf{g}_{\mathsf{RE},k}^T\left[\tilde{\mathbf{B}}_{\mathtt{ZF}}\right]_i\right|^2\right\}\\ &= \rho_{\mathtt{ZF}}^2\sum_{i\neq k}^{K}\mathbb{E}\left\{\left|\mathbf{g}_{\mathsf{RE},k}^T\left[\hat{\mathbf{G}}_{\mathsf{RD}}^*\left(\hat{\mathbf{G}}_{\mathsf{RD}}^T\hat{\mathbf{G}}_{\mathsf{RD}}^*\right)^{-1}\right]_i\right|^2\right\},\\ &\approx \frac{\|\mathbf{g}_{\mathsf{RE},k}\|^2\rho_{\mathtt{ZF}}^2\sum_{i\neq k}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}{N-K}. \qquad (89)\end{aligned}$$

Substituting (88) and (89) into (42), we have

$$\mathscr{R}_{\mathsf{E}_k}^{\mathtt{ZF}} = \frac{1}{2}\log_2\left(1+\min\left((N-K)P_{\mathsf{S}}\sigma_{\mathsf{BR}}^2, \frac{\frac{\|\mathbf{g}_{\mathsf{RE},k}\|^2\rho_{\mathtt{ZF}}^2}{\hat{\sigma}_{\mathsf{RD},k}^2}\frac{1}{N-K}}{\frac{\|\mathbf{g}_{\mathsf{RE},k}\|^2\rho_{\mathtt{ZF}}^2\sum_{i\neq k}^{K}\frac{1}{\hat{\sigma}_{\mathsf{RD},i}^2}}{N-K}+1}\right)\right). \qquad (90)$$

Next, we perform the same approach as for Theorem 2. Finally, we easily obtain the result as in Theorem 4.

Acknowledgments

This research is conducted within the framework of science and technology projects at institutional level of Quy Nhon University under the project code T2022.760.16.

REFERENCES

1. J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, J. C. Zhang. What will 5G be?, *IEEE Journal on Selected Areas in Communications*, **2014**, *32*(6), 1065– 1082.

2. C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. Aggoune, H. Haas, S. Fletcher, E. Hepsaydir. Cellular architecture and key technologies for 5G wireless communication networks, *IEEE Communications Magazine,* **2014**, *52*(2), 122–130.

3. T. L. Marzetta. Noncooperative cellular wireless with unlimited numbers of base station antennas, *IEEE Transactions on Wireless Communications*, **2010**, *9*(11), 3590–3600.

4. E. G. Larsson, O. Edfors, F. Tufvesson, T. L. Marzetta. Massive mimo for next generation wireless systems, *IEEE Communications Magazine*, **2014**, *52*(2), 186–195.

5. H. Q. Ngo, E. G. Larsson, T. L. Marzetta. Energy and spectral efficiency of very large multiuser mimo systems, *IEEE Transactions on Communications*, **2013**, *61*(4), 1436–1449.

6. H. Yang, T. L. Marzetta. Performance of conjugate and zero-forcing beamforming in large-scale antenna systems, *IEEE Journal on Selected Areas in Communications*, **2013**, *31*(2), 172–179.

7. X. Chen, L. Lei, H. Zhang, C. Yuen. *On the secrecy outage capacity of physical layer security in large-scale mimo relaying systems with imperfect CSI,* the 50th IEEE International Conference on Communications University of Sydney Australia, June 2014.

8. J. Zhu, R. Schober, V. K. Bhargava. Linear precoding of data and artificial noise in secure massive mimo systems, *IEEE Transactions on Wireless Communications*, **2016**, *15*(3), 2245–2261.

9. D. Kapetanovic, G. Zheng, F. Rusek. Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks, *IEEE Communications Magazine,* **2015**, *53*(6), 21–27.

10. T. Liu, S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel, *IEEE Transactions on Information Theory*, **2009**, *55*(6), 2547–2553.

11. F. Oggier, B. Hassibi. The secrecy capacity of the mimo wiretap channel, *IEEE Transactions on Information Theory,* **2011**, *57*(8), 4961–4972.

12. X. Chen, H. - H. Chen. Physical layer security in multi-cell miso downlinks with incomplete CSI—a unified secrecy performance analysis, *IEEE Transactions on Signal Processing,* **2014**, *62*(23), 6286–6297.

13. L. Dong, Z. Han, A. P. Petropulu, H. V. Poor. Improving wireless physical layer security via cooperating relays, *IEEE transactions on signal processing*, **2010**, *58*(3), 1875–1888.

14. X. Chen, C. Zhong, C. Yuen, H. - H. Chen. Multi-antenna relay aided wireless physical layer security, *IEEE Communications Magazine*, **2015**, *53*(12), 40–46.

15. M. Pei, J. Wei, K.-K. Wong, X. Wang. Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI, *IEEE Transactions on Wireless Communications*, **2012**, *11*(2), 544–549.

16. X. Wang, K. Wang, X.-D. Zhang. Secure relay beamforming with imperfect channel side information, *IEEE Transactions on Vehicular Technology,* **2013**, *62*(4), 2140–2155.

17. J. Jose, A. Ashikhmin, T. L. Marzetta, S. Vishwanath. Pilot contamination and precoding in multi-cell tdd systems, *IEEE Transactions on Wireless Communications*, **2011**, *10*(8), 2640–2651.

18. N. Yang, H. A. Suraweera, I. B. Collings, C. Yuen. Physical layer security of TAS/MRC with antenna correlation, *IEEE Transactions on Information Forensics and Security*, **2013**, *8*(1), 254–259.

19. X. Chen, Y. Zhang. Mode selection in MU - MIMO downlink networks: A physical-layer security perspective, *IEEE Systems Journal*, **2017**, *11*(2), 1128–1136.

https://doi.org/10.52111/qnjs.2021.16307

20. H.-M. Wang, Q. Yin, X.-G. Xia. Distributed beamforming for physical-layer security of two-way relay networks, *IEEE Transactions on Signal Processing,* **2012**, *60*(7), 3532–3545.

21. G. Zheng, L.-C. Choo, K.-K. Wong. Optimal cooperative jamming to enhance physical layer security using relays, *IEEE Transactions on Signal Processing,* **2011**, *59*(3), 1317–1322.

22. J. Huang, A. L. Swindlehurst. Cooperative jamming for secure communications in mimo relay networks, *IEEE Transactions on Signal Processing*, **2011**, *59*(10), 4871–4884.

23. M. Shakiba-Herfeh, A. Chorti, H. V. Poor. *Physical layer security: Authentication, integrity, and confidentiality,* in Physical Layer Security, Springer, 2021.

24. N. D. Dung, V. N. Q. Bao *et al.* Secrecy performance of massive mimo relay-aided downlink with multiuser transmission, *IET Communications*, **2019**, *13*(9), 1207–1217.

25. Y. Fu, W. P. Zhu, C. Liu. *Rate optimization for relay precoding design with imperfect CSI in two-hop mimo relay networks,* the 73rd Vehicular Technology Conference, Budapest, Hungary, May 2011.

26. C. B. Chae, T. Tang, R. W. Heath, S. Cho. Mimo relaying with linear processing for multiuser transmission in fixed relay networks, *IEEE Transactions on Signal Processing*, **2008**, *56*(2), 727–738.

27. D. W. K. Ng, E. S. Lo, R. Schober. Robust beamforming for secure communication in systems with wireless information and power transfer, *IEEE Transactions Wireless Communications,* **2014**, *13*(2), 544–549.

28. X. Wang, K. Wang, X. D. Zhang. Secure relay beamforming with imperfect channel side information, *IEEE Transactions on Vehicular Technology*, **2013**, *62*(5), 2140–2155.

29. Y. Zou, X. Wang, W. Shen. Optimal relay selection for physical-layer security in cooperative wireless networks, *IEEE Journal on Selected Areas in Communications*, **2013**, *31*(10), 2099–2111.

30. T. Liu, S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel, *IEEE Transactions on Information Theory*, **2009**, *55*(6), 2547–2553.

31. J. Huang, A. L. Swindlehurst. Cooperative jamming for secure communications in mimo relay networks, *IEEE Transactions on Signal Processing*, **2011**, *59*(10), 4871–4884.

32. H. Yin, D. Gesbert, M. Filippou, Y. Liu. A coordinated approach to channel estimation in large-scale multiple-antenna systems, *IEEE Journal on Selected Areas in Communications*, **2013**, *31*(2), 264–273.

33. T. L. Marzetta. Noncooperative cellular wireless with unlimited numbers of base station antennas, *IEEE Transactions on Wireless Communications*, **2010**, *9*(11), 3590–3600.

34. A. M. Tulino, S. Verdú. Random matrix theory and wireless communications, *Foundations and Trends ® in Communications and Information Theory,* **2004**, *1*(1), 1–182.

35. B. Hassibi, B. M. Hochwald. How much training is needed in multiple-antenna wireless links?, *IEEE Transactions on Information Theory,* **2003**, *49*(4), 951–963.

https://doi.org/10.52111/qnjs.2022.16307