Cooperative Beamforming and User Selection for Improving the Security of Relay-aided Systems

Hoang, T. M., Duong, T. Q., A. Suraweera, H., Tellambura, C., & Poor, H. V. (2015). Cooperative Beamforming and User Selection for Improving the Security of Relay-aided Systems. IEEE Transactions on Communications, 63(12), 5039 - 5051. DOI: 10.1109/TCOMM.2015.2494012

Published in:
IEEE Transactions on Communications

Document Version:
Peer reviewed version

Cooperative Beamforming and User Selection for Improving the Security of Relay-aided Systems

Tiep M. Hoang, Trung Q. Duong, *Senior Member, IEEE*, Himal A. Suraweera, *Senior Member, IEEE*, Chintha Tellambura, *Fellow, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—A relay network in which a source wishes to convey a confidential message to a legitimate destination with the assistance of trusted relays is considered. In particular, cooperative beamforming and user selection techniques are applied to protect the confidential message. The secrecy rate (SR) and secrecy outage probability (SOP) of the network are investigated first, and a tight upper bound for the SR and an exact formula for the SOP are derived. Next, asymptotic approximations for the SR and SOP in the high signal-to-noise ratio (SNR) regime are derived for two different schemes: i) cooperative beamforming and ii) multi-user selection. Further, a new concept of cooperative diversity gain, namely, adapted cooperative diversity gain (ACDG), which can be used to evaluate security level of a cooperative relaying network, is investigated. It is shown that the ACDG of cooperative beamforming is equal to the conventional cooperative diversity gain of traditional multiple-input single-output networks, while the ACDG of the multiuser scenario is equal to that of traditional single-input multiple-output networks.**

***Index terms*—**Physical layer security, decode-and-forward relays, cooperative diversity, cooperative beamforming, large scale relaying.

I. Introduction

The broadcasting aspect of wireless networks makes them vulnerable to malicious attacks of adversaries. In order to thwart such attacks, wireless security has traditionally relied on data encryption and decryption algorithms at many layers of the open systems interconnection (OSI) reference model, e.g., [1], [2]. Alternatively, an information-theoretic approach to physical layer security (PLS) exploits the random fading of wireless channels. Although PLS was first introduced by Wyner in his seminal work [3] many years ago, only recently that it has attracted the wide attention of the academic and industrial research community in wireless communications. The emergence of PLS has certainly created the need for new signal processing methods, channel modeling, and communication designs. From the information-theoretic perspective, the secrecy guarantee of wireless networks in the presence of eavesdroppers mainly relies on a metric called the secrecy rate (SR), which is the capacity difference between the legitimate channel, i.e., that of intended user, and malicious channel, i.e., that of eavesdropper [4].

To deal with the vulnerability of malicious attacks from eavesdroppers, numerous studies have been conducted, e.g., [5]–[7] and references therein. These studies cover many different system models of wireless networks such as cooperative wiretap channels (e.g., [7]–[24]), wiretap channels without cooperative nodes (e.g., [6], [25]), and cognitive radio networks (e.g., [5]). However, relays allow the benefits of range extension and distributed diversity, and thus there is also a great deal of interest in the exploitation of cooperative nodes for PLS. Node cooperation in cooperative wireless networks (CWNs) is thus an effective way to improve PLS [7]–[11]. It allows single antenna nodes to enjoy the benefits of multiple-antenna systems and is an attractive low cost solution. So far, a variety of techniques have been offered to guarantee reliable transmission via CWNs; for instance, relay selection techniques [9]–[15] and jamming methods [9], [10], [16]–[18]. Meanwhile, the design of beamforming techniques for communication reliability via CWNs has been also considered in [9]–[11] and [15]–[22]. In addition, there are attempts to propose hybrid schemes combining different techniques, for instance, there is the combination between relaying for retransmission and jamming for eavesdropping attacks in [22] and [23]. Furthermore, it is interesting that in [20], the security issue is also discussed for a large scale multiple-input multiple-output (MIMO) relaying system to get insight into the limitations of PLS when the number of relays approaches infinity. In short, the proposed schemes for improving the security level in CWNs are relatively diverse. Among the above-mentioned works on PLS in CWNs, closely related to our work are the contributions in [19]–[22]. We use cooperative beamforming or user selection techniques for security enhancement, whereas [19]–[21] do not account for multiple users. It is also noted that there are other system models in [24]–[26] similar to our work. However, [24] does not discuss multiple users, while [25] does not use cooperative nodes, and [26] does not take security issue into account. Moreover, [22] and [25] consider

Manuscript received April 22, 2015; revised July 27, 2015; accepted October 6, 2015. The editor coordinating the review of this paper and approving it for publication was Dr. Jinhong Yuan.

This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22 and by the Newton Institutional Link under Grant ID 172719890. The work of H. V. Poor was supported in part by the U.S. National Science Foundation under Grant CMMI-1435778. This paper has been presented in part at the IEEE Global Communications Conference, San Diego, CA, December 2015.

T. M. Hoang is with Duy Tan University, Da Nang 550000, Vietnam (e-mail: hmt1803@gmail.com).

T. Q. Duong is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, UK (e-mail: trung.q.duong@qub.ac.uk).

H. A. Suraweera is with the Department of Electrical and Electronic Engineering, University of Peradeniya, Peradeniya 20400, Sri Lanka (e-mail: himal@ee.pdn.ac.lk).

C. Tellambura is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta T6G 2V4, Canada (e-mail: chintha@ece.ualberta.ca).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (e-mail: poor@princeton.edu).

either cooperative beamforming or user selection only. To the best of the authors' knowledge, previous works have not investigated the impact of both cooperative beamforming and user selection on the security level of multiuser cooperative relaying networks. We are therefore motivated to examine the security level of such networks when cooperative beamforming is applied in parallel with user selection.

To evaluate the secure performance of a CWN, typical metrics such as secrecy rate (SR) [8]–[10] and secrecy outage probability (SOP) [11], [13]–[15], [20] are usually considered. Besides these two metrics, there is also another metric used to qualify the secure performance in the literature [12], which is defined in a similar way to traditional diversity gain. It is well known that traditional space/time/frequency diversity techniques are not concerned with security issues [27]. As such, the concept of traditional diversity gain seems inappropriate for studying security aspects of wireless networks. To help quantify the secure performance, [12] first introduced the notion of *intercept event* (i.e., when SR is negative), and then presented a new concept of cooperative diversity gain (we shall call it adapted cooperative diversity gain (ACDG)), which relies on the *intercept probability* of the intercept event. To be more precise, the ACDG defines the rate of decrease of the intercept probability with the increase of relative channel power gain of destination on a log-log scale. This new concept reveals that the secure performance increases with the ACDG. Due to the similarity of the ACDG to the conventional notion of diversity as well as the relevance of the ACDG to secure networks, we are motivated to examine it thoroughly.

In this paper, we evaluate the secure performance of a CWN in the presence of an eavesdropper. We divide our system model into two scenarios, namely, i) a system model with a single relay and multiple users, and ii) a system model with multiple relays and a single user. In both cases, the presence of an eavesdropper, which is another known user but not a desired destination, is assumed. The first case corresponds to a virtual SIMOSE (i.e., single-input multiple-output channel in the presence of a single eavesdropper), then the second scenario is seen as virtual MISOSE (i.e., multiple-input single-output in the presence of a single eavesdropper). Finding exact expressions for the ergodic SRs for the general case of multiple relays and multiple destinations is difficult. To circumvent this difficulty, we derive upper bounds on the quantities and asymptotic expressions at high transmit power. In addition, we analyze the ergodic SR of the proposed network for the case of large numbers of relays. We then derive the SOPs for the SIMOSE and the MISOSE cases. Finally, we borrow the concept of [12] to introduce the ACDG, and thereby quantify the secure performance of the proposed system. Furthermore, we show that the ACDG of a virtual SIMOSE (or MISOSE) system is equal to the diversity gain of a SIMO (or MISO) system. In particular, the ACDG reveals it is more compatible with secure networks than conventional diversity gain because security is taken into account.

The remainder of this paper is organized as follows. Section II describes a CWN with multiple relays, multiple destinations, and a single eavesdropper. In Section III, we present upper bounds on the ergodic SR and its approximation at high transmit power. Moreover, we analyze the ergodic SR of the proposed system with very large numbers of relays. In Sections IV and V, the SOPs and the ACDGs are respectively derived. Some numerical examples are presented in Section VI, and conclusions are drawn in VII.

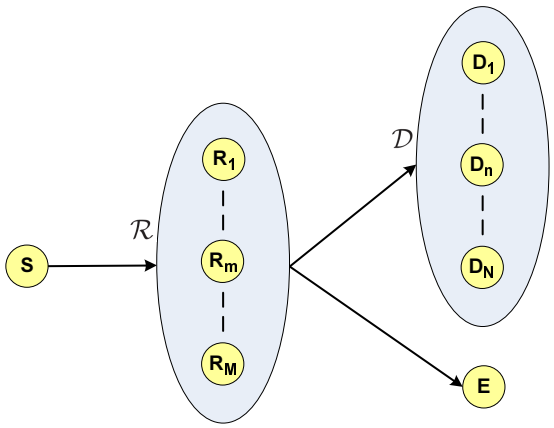

Fig. 1. System model of a relay network consisting of a source, a set $\mathcal{R}$ of M relays, a set $\mathcal{D}$ of N users, and an eavesdropper. Each terminal is equipped with a single-antenna. $\mathcal{R}$ performs cooperative beamforming, while $\mathcal{D}$ exploits user selection.

Notation: $[\cdot]^T$ and $[\cdot]^\dagger$ denote the transpose operator and Hermitian operator, respectively. $\|\cdot\|$ denotes the Euclidean norm. $\mathbb{E}\{\cdot\}$ denotes expectation. $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ denotes the complex Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$. $\mathsf{Exp}(r)$ denotes the exponential distribution with rate r. $\mathsf{Erl}(k, r)$ denotes the Erlang distribution with shape k and rate r. The functions $E_n(z)$ and ${}_2F_1(a, b; c; z)$ denote the exponential integral function of order n [28, Eq. (5.1.4)] and the hypergeometric function [29, Eq. (9.14.2)], respectively.

II. System Model

As shown in Fig. 1, we consider a cooperative relay network consisting of a single source, a set of M trusted relays, a set of N destinations, and one eavesdropper. All the nodes are single-antenna devices operating in the half-duplex mode. For notational simplicity, let S represent the source, R_m represent the mth relay $(m = 1, \ldots, M)$, D_n represent the nth destination $(n = 1, \ldots, N)$, and E represent the eavesdropper. Also, let $\mathcal{R} = \{\mathrm{R}_1, \ldots, \mathrm{R}_M\}$ represent the set of all relays preselected for forwarding the source signal, and $\mathcal{D} = \{\mathrm{D}_1, \ldots, \mathrm{D}_N\}$ represent the set of all destinations. We assume that both $\mathcal{D}$ and E are far enough from S but close enough to $\mathcal{R}$ so that they are only capable of receiving the signal retransmitted from $\mathcal{R}$. Additionally, the channel state information of the $\mathcal{R}$-D_n link as well as the $\mathcal{R}$-E link is assumed to be available at $\mathcal{R}$ (e.g., [9]–[11]). Next, we assume that each relay $\mathrm{R}_m \in \mathcal{R}$ is successful in demodulating and decoding the signal received during the first time slot (i.e., the DF protocol [30]), and all relays (i.e., the set $\mathcal{R}$) perform collaborative beamforming (e.g., see [19], [22], [24] and [31]). $\mathcal{R}$ then forwards a weighted version of the retransmitted signal to $\mathcal{D}$ during the second time slot. The retransmitted signal is also intercepted by the malicious node

E. Thus, the signals received at a certain D_n and E during the second time slot are, respectively, given by

$$y_{D_n} = \sqrt{P_R}\mathbf{w}\mathbf{h}_{\mathcal{R}D_n}x + n_{D_n}, \tag{1}$$

$$y_E = \sqrt{P_R}\mathbf{w}\mathbf{h}_{\mathcal{R}E}x + n_E, \tag{2}$$

where x is the signal retransmitted by $\mathcal{R}$ (assuming that $\mathbb{E}\{x\} = 0$ and $\mathbb{E}\left\{|x|^2\right\} = 1$), $\mathbf{w} = [w_1, \ldots, w_M]$ is the beamforming vector, $\mathbf{h}_{\mathcal{R}D_n} = [h_{R_1D_n}, \ldots, h_{R_MD_n}]^T$ is the $\mathcal{R}$-D_n channel gain vector, and $\mathbf{h}_{\mathcal{R}E} = [h_{R_1E}, \ldots, h_{R_ME}]^T$ is the $\mathcal{R}$-E channel gain vector, n_{D_n} is additive white Gaussian noise (AWGN) at D_n, and n_E is AWGN at E. Note that $h_{R_mD_n} \sim \mathcal{CN}(0, \Omega_{RD})$, $h_{R_mE} \sim \mathcal{CN}(0, \Omega_{RE})$, $n_D \sim \mathcal{CN}(0, N_0)$, and $n_E \sim \mathcal{CN}(0, N_0)$.

To proceed, we assume that all relays in $\mathcal{R}$ collaborate with each other to design the beamforming vector $\mathbf{w}$. Meanwhile, all destinations in $\mathcal{D}$ also collaborate to select a certain D_n as a representative of $\mathcal{D}$ in order to receive the signal from $\mathcal{R}$. Admittedly, the integration of these two cooperative techniques will help improve significantly the security level of the proposed system thanks to the increase in diversity at $\mathcal{R}$ and $\mathcal{D}$. Regarding the use of the beamforming scheme, the beamforming vector $\mathbf{w}$ is designed according to the channel between $\mathcal{R}$ and D^*, in which D^* is the selected D that has the strongest link between $\mathcal{R}$ and itself. Mathematically, we have

$$\mathrm{D}^* = \arg\max_{D_n \in \mathcal{D}} \|\mathbf{h}_{\mathcal{R}D_n}\|^2, \tag{3}$$

$$\|\mathbf{h}_{\mathcal{R}D^*}\|^2 = \max_{D_n \in \mathcal{D}} \|\mathbf{h}_{\mathcal{R}D_n}\|^2, \tag{4}$$

$$\mathbf{w} = \mathbf{h}_{\mathcal{R}D*}^{\dagger}/\|\mathbf{h}_{\mathcal{R}D*}\|. \tag{5}$$

Let Θ be the instantaneously received SNR at D^* for the signal retransmitted by $\mathcal{R}$ in the second time slot. We obtain from (1) that

$$\Theta = \gamma_R|\mathbf{w}\mathbf{h}_{\mathcal{R}D^*}|^2 = \gamma_R\|\mathbf{h}_{\mathcal{R}D^*}\|^2 \tag{6}$$

where $\gamma_R = P_R/N_0$. Let $X_n = \gamma_R\|\mathbf{h}_{\mathcal{R}D_n}\|^2 = \sum_{m=1}^{M}\gamma_R|h_{R_mD_n}|^2$ be a sum of independent and identically distributed (i.i.d.) exponential variables, then $X_n \sim \mathsf{Erl}\left(M, \frac{1}{\gamma_R\Omega_{RD}}\right)$. By definition of Θ, we have $\Theta = \max_{n=1,\ldots,N} X_n$. Thus, the cumulative distribution function (CDF) and the probability density function (PDF) of Θ can be readily deduced from [32] as follows:

$$F_\Theta(\theta) = \left[1 - \sum_{m=0}^{M-1}\frac{e^{-\frac{\theta}{\gamma_R\Omega_{RD}}}}{m!}\left(\frac{\theta}{\gamma_R\Omega_{RD}}\right)^m\right]^N, \tag{7}$$

and

$$f_\Theta(\theta) = N\left[1 - \sum_{m=0}^{M-1}\frac{e^{-\frac{\theta}{\gamma_R\Omega_{RD}}}}{m!}\left(\frac{\theta}{\gamma_R\Omega_{RD}}\right)^m\right]^{N-1} \times \left[\sum_{m=0}^{M-1}\left(\frac{\theta}{\gamma_R\Omega_{RD}} - m\right)\frac{e^{-\frac{\theta}{\gamma_R\Omega_{RD}}}}{m!}\frac{\theta^{m-1}}{(\gamma_R\Omega_{RD})^m}\right]. \tag{8}$$

Similarly, let Φ be the instantaneously received SNR at the eavesdropper for the signal retransmitted by $\mathcal{R}$ in the second time slot. We obtain from (2) that

$$\Phi = \left(\frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}E}^{\dagger}\mathbf{h}_{\mathcal{R}D^*}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\right)\underbrace{\left(\frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}D^*}^{\dagger}\mathbf{h}_{\mathcal{R}E}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\right)}_{\mathcal{Z}} = |\mathcal{Z}|^2. \tag{9}$$

It is apparent that SNR appears in (9) as a function of two random vectors $\mathbf{h}_{\mathcal{R}D^*}$ and $\mathbf{h}_{\mathcal{R}E}$. Conditioning on $\mathbf{h}_{\mathcal{R}D^*}$, we have

$$\begin{aligned}\mathcal{Z}\,|\mathbf{h}_{\mathcal{R}D^*} &\sim \mathcal{CN}\left(0, \frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}D^*}^{\dagger}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\Omega_{RE}\mathbf{I}\frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}D^*}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\right)\\ \Leftrightarrow \mathcal{Z}\,|\mathbf{h}_{\mathcal{R}D^*} &\sim \mathcal{CN}(0, \gamma_R\Omega_{RE})\end{aligned} \tag{10}$$

leading to $\Phi\,|\mathbf{h}_{\mathcal{R}D^*} \sim \mathsf{Exp}\left(\frac{1}{\gamma_R\Omega_{RE}}\right)$ as a result. [1] Note that $\Phi\,|\mathbf{h}_{\mathcal{R}D^*}$ is equivalent to $\Phi\,|\Theta$ and Θ is a function of $\mathbf{h}_{\mathcal{R}D^*}$ only. Thus, we shall use $\Phi\,|\Theta$ in place of $\Phi\,|\mathbf{h}_{\mathcal{R}D^*}$.

III. Ergodic Secrecy Rate

In this section, we will study the ergodic SR for the system proposed in Section II. However, analyzing the general case with $M \geq 2$ and $N \geq 2$ is difficult. In order to simplify our analysis, we shall mainly examine the following three scenarios:

- SIMOSE: $M = 1$ and $N \geq 2$.
- MISOSE: $M \geq 2$ and $N = 1$.
- Large scale MIMOSE: $M \to \infty$ and finite N.

For the first two cases, we derive tight upper bounds as well as asymptotic expressions for the ergodic SR. Moreover, exact expression for the ergodic SR is found in the third case.

In order to proceed, we first recall that the channel capacities of the links $\mathcal{R}$-D^* and $\mathcal{R}$-E in nat/s/Hz are, respectively, given by

$$C_{D^*} = \ln(1 + \Theta), \tag{11}$$

$$C_E = \ln(1 + \Phi). \tag{12}$$

Thus, the achievable SR in nat/s/Hz can be defined as [4]

$$C_\Delta(\Theta, \Phi) = [C_{D^*} - C_E]^+ = \left[\ln\left(\frac{1+\Theta}{1+\Phi}\right)\right]^+ \tag{13}$$

where $[x]^+ = \max\{0, x\}$.

The ergodic SR of the proposed system in the general case (i.e., for a MIMOSE system) is given by

$$\begin{aligned}\langle C_\Delta\rangle &= \mathbb{E}_\Theta\left\{\mathbb{E}_{\Phi|\Theta}\left\{C_\Delta(\Theta, \Phi)\,|\Theta = \theta\right\}\right\}\\ &= \mathbb{E}_\Theta\left\{\int_0^\theta \ln\left(\frac{1+\theta}{1+\phi}\right) f_{\Phi|\Theta}(\phi)\, d\phi\right\}\\ &= \mathcal{A} - \mathcal{B},\end{aligned} \tag{14}$$

[1] Let $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$. If $\mathbf{A}$ is a non-random matrix and $\mathbf{b}$ is a non-random vector, then $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{b}$ yields a circularly symmetric complex $\mathbf{y} \sim \mathcal{CN}\left(\mathbf{A}\boldsymbol{\mu} + \mathbf{b}, \mathbf{A}\boldsymbol{\Sigma}\mathbf{A}^{\dagger}\right)$ [27, Appendix A].

where the term $\mathcal{A}$ can be expressed as

$$\begin{aligned}\mathcal{A} &\triangleq \mathbb{E}_\Theta\left\{\ln(1+\theta)F_{\Phi|\Theta}\left(\theta\right)\right\}\\ &= \mathbb{E}_\Theta\left\{\ln(1+\theta)\left(1-e^{-\theta/(\gamma_R\Omega_{RE})}\right)\right\}\\ &= \mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} - \mathbb{E}_\Theta\left\{\ln(1+\theta)e^{-\theta/(\gamma_R\Omega_{RE})}\right\}, \quad (15)\end{aligned}$$

and the term $\mathcal{B}$ can be expressed as

$$\begin{aligned}\mathcal{B} &\triangleq \mathbb{E}_\Theta\left\{\int_0^\theta \ln\left(1+\phi\right) f_{\Phi|\Theta}\left(\phi\right) d\phi\right\}\\ &= \mathbb{E}_\Theta\left\{\int_0^\theta \ln\left(1+\phi\right) \frac{e^{-\phi/(\gamma_R\Omega_{RE})}}{\gamma_R\Omega_{RE}} d\phi\right\}\\ &= e^{1/(\gamma_R\Omega_{RE})}\left[E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right) - \mathbb{E}_\Theta\left\{E_1\left(\frac{1+\theta}{\gamma_R\Omega_{RE}}\right)\right\}\right]\\ &\quad - \mathbb{E}_\Theta\left\{\ln(1+\theta)e^{-\theta/(\gamma_R\Omega_{RE})}\right\} \quad (16)\end{aligned}$$

where the last equality is obtained with the help of [29, Eq. (4.331.2)].

Substituting (15) and (16) into (14), we obtain

$$\begin{aligned}\langle C_\Delta\rangle = \mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} - e^{1/(\gamma_R\Omega_{RE})}E_1\left(1/(\gamma_R\Omega_{RE})\right)\\ + e^{1/(\gamma_R\Omega_{RE})}\,\mathbb{E}_\Theta\left\{E_1\left((1+\theta)/(\gamma_R\Omega_{RE})\right)\right\}. \quad (17)\end{aligned}$$

Unfortunately the expectation $\mathbb{E}_\Theta\left\{E_1\left(\frac{1+\theta}{\gamma_R\Omega_{RE}}\right)\right\}$ in (17) cannot be found in a closed-form. We therefore aim at finding an upper bound on the ergodic SR as follows:

$$\begin{aligned}\langle C_\Delta\rangle &\le \mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} - e^{1/(\gamma_R\Omega_{RE})}E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right)\\ &\quad + e^{1/(\gamma_R\Omega_{RE})}\,\mathbb{E}_\Theta\left\{E_1\left(\theta/(\gamma_R\Omega_{RE})\right)\right\}\\ &\triangleq \langle C_\Delta\rangle^{\text{upper}} \quad (18)\end{aligned}$$

where the inequality follows from the fact that $E_1\left(x\right) = \int_x^\infty \frac{e^{-u}}{u}du$ is a decreasing function.

Lemma 1. *At high γ_R, the asymptotic expression for the ergodic SR, defined as $\langle C_\Delta\rangle^\infty$, is also that of the upper bound. In other words, we have*

$$\langle C_\Delta\rangle^\infty \triangleq \lim_{\gamma_R\to\infty}\langle C_\Delta\rangle = \lim_{\gamma_R\to\infty}\langle C_\Delta\rangle^{\text{upper}}. \quad (19)$$

Proof. See Appendix A. □

A. SIMOSE Wiretap Channel

In this subsection, we present an upper bound on and an asymptotic expression for the ergodic SR for the SIMOSE case. These results are given in Theorem 1 and Corollary 1.

Theorem 1. *In the case of SIMOSE, an upper bound on the ergodic SR is given by*

$$\begin{aligned}&\langle C_\Delta\rangle^{upper}\\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1}\left\{e^{\frac{1}{\gamma_R\Omega_{RE}}}\ln\left(1+n\frac{\Omega_{RE}}{\Omega_{RD}}\right)\right.\\ &\quad \left. + e^{\frac{n}{\gamma_R\Omega_{RD}}}E_1\left(\frac{n}{\gamma_R\Omega_{RD}}\right) - e^{\frac{1}{\gamma_R\Omega_{RE}}}E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right)\right\}. \quad (20)\end{aligned}$$

Proof. When $M=1$, the PDF of Θ in (8) reduces to

$$f_\Theta(\theta) = \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n}{\gamma_R\Omega_{RD}}e^{-\frac{n\theta}{\gamma_R\Omega_{RD}}}. \quad (21)$$

Then, the expected values in (18) can be, respectively, calculated as follows:

$$\begin{aligned}&\mathbb{E}_\Theta\left\{\ln(1+\theta)\right\}\\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\int_0^\infty \ln(1+\theta)\frac{ne^{-\frac{n\theta}{\gamma_R\Omega_{RD}}}}{\gamma_R\Omega_{RD}}d\theta\\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}e^{\frac{n}{\gamma_R\Omega_{RD}}}E_1\left(\frac{n}{\gamma_R\Omega_{RD}}\right), \quad (22)\end{aligned}$$

and

$$\begin{aligned}&\mathbb{E}_\Theta\left\{E_1\left(\theta/\left(\gamma_R\Omega_{RE}\right)\right)\right\}\\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\int_0^\infty E_1\left(\frac{\theta}{\gamma_R\Omega_{RE}}\right)\frac{ne^{-\frac{n\theta}{\gamma_R\Omega_{RD}}}}{\gamma_R\Omega_{RD}}d\theta\\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\ln\left(1+n\frac{\Omega_{RE}}{\Omega_{RD}}\right). \quad (23)\end{aligned}$$

Finally, substituting (22) and (23) into (18) yields (20). □

To facilitate the analysis of the asymptotic expression for the ergodic SR, we now state Proposition 1, which will be applied to the proof of Corollary 1.

Proposition 1. *If a and b are finite numbers, then*

$$\mathcal{L}(a,b) \triangleq \lim_{\gamma\to\infty}\left[E_1\left(a/\gamma\right) - E_1\left(b/\gamma\right)\right] = \ln(b/a). \quad (24)$$

Proof. Using the Taylor series expansion for the function $E_1(x)$ [29, Eq.(8.214.2)] (note that $E_1(x) = -Ei(-x)$), we rewrite $E_1\left(x\right) = -\mathcal{E} - \ln x - \sum_{k=1}^{\infty}\frac{(-x)^k}{k!k}$ where $\mathcal{E}$ is Euler's constant [29, Eq. (8.367.1)]. Then we have the resulting limit

$$\begin{aligned}\mathcal{L}(a,b) &= \lim_{\frac{1}{\gamma}\to 0}\left[\ln\left(b/\gamma\right) - \ln\left(a/\gamma\right) + \sum_{k=1}^{\infty}\frac{(-1)^k}{k!k}\frac{\left(b^k-a^k\right)}{\gamma^k}\right]\\ &= \lim_{\frac{1}{\gamma}\to 0}\left[\ln\left(b/\gamma\right) - \ln\left(a/\gamma\right)\right] = \ln(b/a). \quad (25)\end{aligned}$$

□

Corollary 1. *In the case of SIMOSE, an asymptotic expression for the ergodic SR is given by*

$$\langle C_\Delta\rangle^\infty = \sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1}\ln\left(1+\frac{\Omega_{RD}}{n\Omega_{RE}}\right). \quad (26)$$

Proof. Following Lemma 1, at high γ_R, the asymptotic expression for the ergodic SR is given by

$$\begin{aligned}\langle C_\Delta\rangle^\infty &= \lim_{\gamma_R\to\infty}\langle C_\Delta\rangle^{\text{upper}}\\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1}\left\{\ln\left(1+n\frac{\Omega_{RD}}{\Omega_{RE}}\right)\right.\\ &\quad \left. + \underbrace{\lim_{\gamma_R\to\infty}\left[E_1\left(\frac{n}{\gamma_R\Omega_{RD}}\right) - E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right)\right]}_{\mathcal{L}\left(\frac{n}{\Omega_{RD}},\frac{n}{\Omega_{RE}}\right)}\right\}. \quad (27)\end{aligned}$$

Finally, applying Proposition 1 to the limit on the RHS of (27), we arrive at (26) and complete the proof. □

B. MISOSE Wiretap Channel

Similar to the previous subsection, we now present an upper bound on and an asymptotic expression for the ergodic SR for the MISOSE case through Theorem 2 and Corollary 2.

Theorem 2. *In the case of MISOSE, an upper bound on the ergodic SR is given by*

$$\begin{aligned}
&\langle C_\Delta \rangle^{upper} \\
&= e^{\frac{1}{\gamma_R \Omega_{RE}}} \ln\left(1+\frac{\Omega_{RE}}{\Omega_{RD}}\right) + \mathcal{C}_1(\gamma_R) + \sum_{m=1}^{M-1} \frac{1}{m!}\mathcal{C}_2(\gamma_R) \\
&+ e^{\frac{1}{\gamma_R \Omega_{RE}}} \sum_{m=1}^{M-1} \left(\frac{\Omega_{RE}}{\Omega_{RD}+\Omega_{RE}}\right)^m \\
&\quad \times \left[\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}} \frac{1}{m+1}\ {}_2F_1\left(1, m+1; m+2; \frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right. \\
&\quad \left. - \frac{1}{m}\ {}_2F_1\left(1, m; m+1; \frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right] \qquad (28)
\end{aligned}$$

where

$$\mathcal{C}_1(\gamma_R) \triangleq e^{\frac{1}{\gamma_R \Omega_{RD}}} E_1\left(\frac{1}{\gamma_R \Omega_{RD}}\right) - e^{\frac{1}{\gamma_R \Omega_{RE}}} E_1\left(\frac{1}{\gamma_R \Omega_{RE}}\right) \qquad (29)$$

and

$$\begin{aligned}
\mathcal{C}_2(\gamma_R) \triangleq \frac{1}{(\gamma_R \Omega_{RD})^m} &\left[\frac{1}{\gamma_R \Omega_{RD}} \mathcal{I}\left(\frac{1}{\gamma_R \Omega_{RD}}, m\right)\right. \\
&\left. - m\mathcal{I}\left(\frac{1}{\gamma_R \Omega_{RD}}, m-1\right)\right] \qquad (30)
\end{aligned}$$

where the function $\mathcal{I}(\alpha, m) \triangleq \int_0^\infty \theta^m \ln(1+\theta) e^{-\alpha\theta} d\theta,\ m \in \mathbb{N}$ is calculated in Appendix B.

Proof. When $N = 1$, the PDF of Θ in (8) reduces to

$$f_\Theta(\theta) = \sum_{m=0}^{M-1} \frac{e^{-\frac{\theta}{\gamma_R \Omega_{RD}}}}{m! (\gamma_R \Omega_{RD})^m} \left(\frac{\theta^m}{\gamma_R \Omega_{RD}} - m\theta^{m-1}\right). \qquad (31)$$

Thus, the expected values in (18) can be, respectively, calculated as follows:

$$\begin{aligned}
&\mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} \\
&= \frac{1}{\gamma_R \Omega_{RD}} \int_0^\infty \ln(1+\theta) e^{-\frac{\theta}{\gamma_R \Omega_{RD}}} d\theta \\
&+ \sum_{m=1}^{M-1} \frac{1}{m! (\gamma_R \Omega_{RD})^m} \int_0^\infty \left(\frac{\theta^m}{\gamma_R \Omega_{RD}} - m\theta^{m-1}\right) \\
&\qquad \times \ln(1+\theta) e^{-\frac{\theta}{\gamma_R \Omega_{RD}}} d\theta \\
&\overset{(a)}{=} e^{\frac{1}{\gamma_R \Omega_{RD}}} E_1\left(\frac{1}{\gamma_R \Omega_{RD}}\right) + \sum_{m=1}^{M-1} \frac{1}{m! (\gamma_R \Omega_{RD})^m} \\
&\times \left[\frac{1}{\gamma_R \Omega_{RD}} \mathcal{I}\left(\frac{1}{\gamma_R \Omega_{RD}}, m\right) - m\mathcal{I}\left(\frac{1}{\gamma_R \Omega_{RD}}, m-1\right)\right], \qquad (32)
\end{aligned}$$

and

$$\begin{aligned}
&\mathbb{E}_\Theta\left\{E_1\left(\theta/\left(\gamma_R \Omega_{RE}\right)\right)\right\} \\
&= \sum_{m=0}^{M-1} \frac{1}{m! (\gamma_R \Omega_{RD})^m} \int_0^\infty E_1\left(\frac{\theta}{\gamma_R \Omega_{RE}}\right) \\
&\qquad \times \left(\frac{\theta^m}{\gamma_R \Omega_{RD}} - m\theta^{m-1}\right) e^{-\frac{\theta}{\gamma_R \Omega_{RD}}} d\theta \\
&\overset{(b)}{=} \ln\left(1+\frac{\Omega_{RE}}{\Omega_{RD}}\right) + \sum_{m=1}^{M-1} \left(\frac{\Omega_{RE}}{\Omega_{RD}+\Omega_{RE}}\right)^m \\
&\times \left[\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}} \frac{1}{m+1}\ {}_2F_1\left(1, m+1; m+2; \frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right. \\
&\qquad \left. - \frac{1}{m}\ {}_2F_1\left(1, m; m+1; \frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right] \qquad (33)
\end{aligned}$$

where (a) follows from Proposition 2 (see Appendix B); and (b) is obtained by using [29, Eq. (6.228.2)]. Finally, substituting (32) and (33) into (18) yields (28). □

Corollary 2. *In the case of MISOSE, an asymptotic expression for the ergodic SR is given by*

$$\begin{aligned}
&\langle C_\Delta \rangle^{\infty} \\
&= \ln\left(1+\frac{\Omega_{RD}}{\Omega_{RE}}\right) + \sum_{m=1}^{M-1} \frac{1}{m} \\
&+ \sum_{m=1}^{M-1} \left(\frac{\Omega_{RE}}{\Omega_{RD}+\Omega_{RE}}\right)^m \\
&\quad \times \left[\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}} \frac{1}{m+1}\ {}_2F_1\left(1, m+1; m+2; \frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right. \\
&\quad \left. - \frac{1}{m}\ {}_2F_1\left(1, m; m+1; \frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right] \qquad (34)
\end{aligned}$$

Proof. Again following Lemma 1, at high γ_R, we have $\langle C_\Delta \rangle^{\infty} = \lim_{\gamma_R \to \infty} \langle C_\Delta \rangle^{\text{upper}}$. Upon examining (28), we can see that taking the limit of $\langle C_\Delta \rangle^{\text{upper}}$ relies only on taking the limits of the expressions $\mathcal{C}_1(\gamma_R)$ and $\mathcal{C}_2(\gamma_R)$. These limits are calculated as follows:

$$\begin{aligned}
&\lim_{\gamma_R \to \infty} \mathcal{C}_1(\gamma_R) \\
&= \lim_{\gamma_R \to \infty} \left[e^{\frac{1}{\gamma_R \Omega_{RD}}} E_1\left(\frac{1}{\gamma_R \Omega_{RD}}\right) - e^{\frac{1}{\gamma_R \Omega_{RE}}} E_1\left(\frac{1}{\gamma_R \Omega_{RE}}\right)\right] \\
&= \lim_{\gamma_R \to \infty} \left[E_1\left(\frac{1}{\gamma_R \Omega_{RD}}\right) - E_1\left(\frac{1}{\gamma_R \Omega_{RE}}\right)\right] \\
&= \mathcal{L}\left(\frac{1}{\Omega_{RD}}, \frac{1}{\Omega_{RE}}\right) \\
&\overset{(a)}{=} \ln\left(\Omega_{RD}/\Omega_{RE}\right) \qquad (35)
\end{aligned}$$

where (a) follows Proposition 1. And

$$\begin{aligned}
&\lim_{\gamma_R\to\infty}\mathcal{C}_2(\gamma_R)\\
&\overset{(b)}{=}\lim_{\gamma_R\to\infty}\left\{\sum_{k=0}^{m}\frac{m!}{(m-k)!}\sum_{h=1}^{m-k}\frac{(h-1)!}{(-\gamma_R\Omega_{RD})^{m-k-h}}\right.\\
&\quad\left.-m\sum_{k=0}^{m-1}\frac{(m-1)!}{(m-k-1)!}\sum_{h=1}^{m-k-1}\frac{(h-1)!}{(-\gamma_R\Omega_R)^{m-k-h-1}}\right\}\\
&=m!+\sum_{k=0}^{m-2}\frac{m!(m-k-1)!}{(m-k)!}+\sum_{k=0}^{m-2}\frac{m!}{(m-k-1)!}\\
&\times\lim_{\gamma_R\to\infty}\left[(m-k-2)!\left(\frac{-1}{(m-k)\gamma_R\Omega_{RD}}-1\right)\right.\\
&\left.+\sum_{h=1}^{m-k-2}\frac{(h-1)!}{(-\gamma_R\Omega_{RD})^{m-k-h-1}}\left(\frac{-1}{(m-k)\gamma_R\Omega_{RD}}-1\right)\right]\\
&=m!+\sum_{k=0}^{m-2}\frac{m!(m-k-1)!}{(m-k)!}+\sum_{k=0}^{m-2}\frac{m!(m-k-2)!(-1)}{(m-k-1)!}\\
&=m!+m!\left(-1+\sum_{k=1}^{m}\frac{1}{k}\right)-m!\sum_{k=1}^{m-1}\frac{1}{k}\\
&=(m-1)! \qquad (36)
\end{aligned}$$

where (b) is obtained by first substituting (70) from Appendix B into (29) and then simplifying the expression. Finally, taking the limit of (28) with the aid of (35)–(36), we readily obtain the desired result (34). □

C. Analysis for Large Scale MIMOSE Relaying Systems

Unlike both SIMOSE and MISOSE scenarios discussed above, in this subsection we consider a limiting scenario with a very large number of relays (i.e., $M\to\infty$) and a moderate number of users (i.e., finite N) to get insight into the ergodic SR of the proposed system [20].

Based on this large-scale MIMO relaying system in the presence of eavesdropper, we now derive the ergodic SR and state the following theorem:

Theorem 3. *For the proposed system, when the number of relays is very large, i.e. $M\to\infty$, the ergodic SR converges to*

$$\begin{aligned}
\langle C\rangle^{lar}&=\ln(1+M\gamma_R\Omega_{RD})-e^{\frac{1}{\gamma_R\Omega_{RE}}}E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right)\\
&\quad+e^{\frac{1}{\gamma_R\Omega_{RE}}}E_1\left(\frac{1+M\gamma_R\Omega_{RD}}{\gamma_R\Omega_{RE}}\right). \qquad (37)
\end{aligned}$$

Proof. Similarly as in [33], we apply the law of large numbers [34] to (4) so as to reach the limit $\frac{1}{M}\|\mathbf{h}_{\mathcal{R}D_n}\|^2\overset{asym}{\to}\mathbb{E}\left\{|h_{R_mD_n}|^2\right\}=\Omega_{RD}$ where $\overset{asym}{\to}$ denotes the convergence as $M\to\infty$. As a result, D^* can be selected arbitrarily from the set $\mathcal{D}$ of finite N users because the fact that $D^*=\arg\max_{D_n\in\mathcal{D}}\|\mathbf{h}_{\mathcal{R}D_n}\|^2\overset{asym}{\to}\arg\max_{D_n\in\mathcal{D}}\Omega_{RD}$ for all $n=1,\ldots,N$. Therefore, we obtain the convergence of Θ as

$$\Theta=\gamma_R\|\mathbf{h}_{\mathcal{R}D^*}\|^2\overset{asym}{\to}\gamma_RM\Omega_{RD}. \qquad (38)$$

Applying the Lindeberg-Levy central limit theorem, we have

$$\frac{\mathbf{h}^\dagger_{\mathcal{R}D^*}\mathbf{h}_{\mathcal{R}E}}{\sqrt{M}}\overset{dist}{\to}\mathcal{CN}\left(0,\Omega_{RD}\Omega_{RE}\right) \qquad (39)$$

where $\overset{dist}{\to}$ denotes convergence in distribution as $M\to\infty$. Employing two convergence properties (38)–(39), we obtain the convergence of Φ as

$$\Phi=\gamma_R\frac{|\mathbf{h}^\dagger_{\mathcal{R}D^*}\mathbf{h}_{\mathcal{R}E}|^2}{\|\mathbf{h}_{\mathcal{R}D^*}\|^2}\overset{dist}{\to}\Psi\sim\mathsf{Exp}\left(\frac{1}{\gamma_R\Omega_{RE}}\right). \qquad (40)$$

Finally, the ergodic SR of the proposed system with very large M is derived as

$$\begin{aligned}
\langle C\rangle^{lar}&=\lim_{M\to\infty}\mathbb{E}_{\Theta,\Phi}\left\{\left[\ln\left(\frac{1+\Theta}{1+\Phi}\right)\right]^+\right\}\\
&=\mathbb{E}_{\Psi}\left\{\left[\ln\left(\frac{1+\gamma_RM\Omega_{RD}}{1+\Psi}\right)\right]^+\right\}\\
&=\ln(1+M\gamma_R\Omega_{RD})\left(1-e^{-M\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\\
&\quad-\frac{1}{\gamma_R\Omega_{RE}}\int_0^{M\gamma_R\Omega_{RD}}\ln(1+\psi)e^{-\frac{\psi}{\gamma_R\Omega_{RE}}}d\psi. \qquad (41)
\end{aligned}$$

Applying integration by parts to the integral in the last equality and then manipulating the RHS, we easily arrive at (37) and complete the proof. □

Observation: It is clear that Corollaries 1 and 2 provide better insight into the influence of the ratio Ω_{RD}/Ω_{RE} on the ergodic SR. Of course, the asymptotic expressions for the ergodic SR strictly depend on this ratio when γ_R is very large. Meanwhile, Theorem 3 gives us a relatively compact expression of the ergodic SR in the MIMOSE case with large M and moderate N.

IV. Secrecy Outage Probability

In this section, we present the SOP, which is defined as the probability that the instantaneous SR is below a threshold value ϵ. The SOP will be derived for two cases: SIMOSE systems and MISOSE systems.

The SOP of the proposed system in the general case (i.e., for a MIMOSE system) is given by

$$\begin{aligned}
\mathcal{P}_{\text{out}}&=\mathbb{P}\left\{C_\Delta(\Theta,\Phi)<\epsilon\right\}=\mathbb{P}\left\{\frac{1+\Theta}{1+\Phi}<e^\epsilon\right\}\\
&=1-\mathbb{P}\left\{\Phi\le e^{-\epsilon}(1+\Theta)-1\right\}\\
&=1-\int_{e^\epsilon-1}^{\infty}F_{\Phi|\Theta}\left(e^{-\epsilon}(1+\theta)-1\right)f_\Theta(\theta)d\theta \qquad (42)
\end{aligned}$$

where the last equality follows from the fact that $F_{\Phi|\Theta}\left(e^{-\epsilon}(1+\theta)-1\right)=0$ where $\theta\le e^\epsilon-1$. On recalling

that $\Phi|\mathbf{h}_{\mathcal{R}D^*} \leftrightarrow \Phi|\Theta$ leads to $\Phi|\Theta \sim \mathsf{Exp}\left(\frac{1}{\gamma_R\Omega_{RE}}\right)$, we can proceed to formulate (42) as

$$\begin{aligned}\mathcal{P}_{\text{out}} &= 1 - \int_{e^\epsilon-1}^{\infty} \left[1 - e^{-\left(e^{-\epsilon}(1+\theta)-1\right)/(\gamma_R\Omega_{RE})}\right] f_\Theta(\theta)d\theta \\ &= 1 - \int_{e^\epsilon-1}^{\infty} f_\Theta(\theta)d\theta \\ &\quad + \int_{e^\epsilon-1}^{\infty} e^{-\left(e^{-\epsilon}(1+\theta)-1\right)/(\gamma_R\Omega_{RE})} f_\Theta(\theta)d\theta \\ &= F_\Theta\left(e^\epsilon-1\right) + e^{\left(1-e^{-\epsilon}\right)/(\gamma_R\Omega_{RE})}\mathcal{G}(\epsilon) \end{aligned} \tag{43}$$

where the integral $\mathcal{G}(\epsilon)$ is defined as

$$\mathcal{G}(\epsilon) \triangleq \int_{e^\epsilon-1}^{\infty} e^{-\theta e^{-\epsilon}/(\gamma_R\Omega_{RE})} f_\Theta(\theta)d\theta. \tag{44}$$

A. SIMOSE Wiretap Channel

Theorem 4. *In the case of SIMOSE, the SOP can be written as*

$$\begin{aligned}\mathcal{P}_{\text{out}} = \left(1 - e^{\frac{1-e^\epsilon}{\gamma_R\Omega_{RD}}}\right)^N + \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n}{\gamma_R\Omega_{RD}} \\ \times \left(\frac{e^{-\epsilon}}{\gamma_R\Omega_{RE}} + \frac{n}{\gamma_R\Omega_{RD}}\right)^{-1} e^{\frac{(1-e^\epsilon)n}{\gamma_R\Omega_{RD}}}.\end{aligned} \tag{45}$$

Proof. When $M = 1$, the CDF of Θ in (7) reduces to

$$F_\Theta(\theta) = \left[1 - e^{-\frac{\theta}{\gamma_R\Omega_{RD}}}\right]^N. \tag{46}$$

Moreover, by substituting (21) into (44), $\mathcal{G}(\epsilon)$ can be calculated as follows:

$$\begin{aligned}\mathcal{G}(\epsilon) &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n}{\gamma_R\Omega_{RD}} \\ &\quad \times \int_{e^\epsilon-1}^{\infty} e^{-\theta\left(\frac{e^{-\epsilon}}{\gamma_R\Omega_{RE}} + \frac{n}{\gamma_R\Omega_{RD}}\right)}d\theta \\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n}{\gamma_R\Omega_{RD}} \\ &\quad \times \left(\frac{e^{-\epsilon}}{\gamma_R\Omega_{RE}} + \frac{n}{\gamma_R\Omega_{RD}}\right)^{-1} e^{-(e^\epsilon-1)\left(\frac{e^{-\epsilon}}{\gamma_R\Omega_{RE}} + \frac{n}{\gamma_R\Omega_{RD}}\right)}.\end{aligned} \tag{47}$$

Finally, using (46) and substituting (47) into (43), we arrive at the SOP shown in (45). □

Corollary 3. *In the case of SIMOSE, an asymptotic expression for $\mathcal{P}_{\text{out}}$ at high γ_R ($\gamma_R \to \infty$) is obtained by taking the limit of* (45)*, i.e.,*

$$\begin{aligned}\mathcal{P}_{\text{out}}^{\text{asym}} &= \lim_{\gamma_R\to\infty} \mathcal{P}_{\text{out}} \\ &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\left(\frac{\Omega_{RD}}{\Omega_{RE}}\frac{e^{-\epsilon}}{n} + 1\right)^{-1}.\end{aligned} \tag{48}$$

B. MISOSE Wiretap Channel

Theorem 5. *In the case of MISOSE, the SOP can be written as*

$$\begin{aligned}\mathcal{P}_{\text{out}} &= 1 - e^{\frac{(1-e^\epsilon)}{\gamma_R\Omega_{RD}}}\sum_{m=0}^{M-1}\frac{1}{m!}\left(\frac{e^\epsilon-1}{\gamma_R\Omega_{RD}}\right)^m \\ &\quad + e^{\frac{\left(1-e^{-\epsilon}\right)}{\gamma_R\Omega_{RE}}}\sum_{m=0}^{M-1}\left(1 + e^{-\epsilon}\frac{\Omega_{RD}}{\Omega_{RE}}\right)^{-m} e^{-(e^\epsilon-1)\beta} \\ &\quad \times \left\{\sum_{i=0}^{m-1}\left[\left(1 + e^{-\epsilon}\frac{\Omega_{RD}}{\Omega_{RE}}\right)^{-1} - 1\right]\frac{[(e^\epsilon-1)\beta]^i}{i!}\right. \\ &\quad \left. + \left(1 + e^{-\epsilon}\frac{\Omega_{RD}}{\Omega_{RE}}\right)^{-1}\frac{[(e^\epsilon-1)\beta]^m}{m!}\right\}.\end{aligned} \tag{49}$$

Proof. When $N = 1$, the CDF of Θ in (7) reduces to

$$F_\Theta(\theta) = 1 - \sum_{m=0}^{M-1}\frac{e^{-\frac{\theta}{\gamma_R\Omega_{RD}}}}{m!}\left(\frac{\theta}{\gamma_R\Omega_{RD}}\right)^m. \tag{50}$$

Moreover, by substituting (31) into (44), $\mathcal{G}(\epsilon)$ can be calculated as follows:

$$\begin{aligned}&\mathcal{G}(\epsilon) \\ &= \sum_{m=0}^{M-1}\frac{1}{m!\left(\gamma_R\Omega_{RD}\right)^m}\int_{e^\epsilon-1}^{\infty}\left(\frac{\theta^m}{\gamma_R\Omega_{RD}} - m\theta^{m-1}\right)e^{-\theta\beta}d\theta \\ &= \sum_{m=0}^{M-1}\left(1 + e^{-\epsilon}\frac{\Omega_{RD}}{\Omega_{RE}}\right)^{-m} e^{-(e^\epsilon-1)\beta} \\ &\quad \times \left\{\sum_{i=0}^{m-1}\left[\left(1 + e^{-\epsilon}\frac{\Omega_{RD}}{\Omega_{RE}}\right)^{-1} - 1\right]\frac{[(e^\epsilon-1)\beta]^i}{i!}\right. \\ &\quad \left. + \left(1 + e^{-\epsilon}\frac{\Omega_{RD}}{\Omega_{RE}}\right)^{-1}\frac{[(e^\epsilon-1)\beta]^m}{m!}\right\}\end{aligned} \tag{51}$$

where $\beta \triangleq \left(\frac{e^{-\epsilon}}{\gamma_R\Omega_{RE}} + \frac{1}{\gamma_R\Omega_{RD}}\right)$. The second equality is obtained by applying [29, Eq. (2.33.10)] to the integral and then using the definition of the incomplete gamma function [29, Eq. (8.352.4)]. Finally, using (50) and substituting (51) into (43), we arrive at the SOP shown in (49). □

Corollary 4. *In the case of MISOSE, an asymptotic expression for $\mathcal{P}_{\text{out}}$ at high γ_R ($\gamma_R \to \infty$) is obtained by taking the limit of* (49)*, i.e.,*

$$\begin{aligned}\mathcal{P}_{\text{out}}^{\text{asym}} &= \lim_{\gamma_R\to\infty} \mathcal{P}_{\text{out}} \\ &= 1 - \sum_{m=0}^{M-1}\frac{1}{\Omega_{RD}^m}\left(\frac{e^{-\epsilon}}{\Omega_{RE}} + \frac{1}{\Omega_{RD}}\right)^{-m} \\ &\quad \times \left[1 - \frac{1}{\Omega_{RD}}\left(\frac{e^{-\epsilon}}{\Omega_{RE}} + \frac{1}{\Omega_{RD}}\right)^{-1}\right].\end{aligned} \tag{52}$$

Observation: To evaluate the SOP at high γ_R, we can use the simple expressions shown in Corollaries 3 and 4 rather than the exact expressions shown in Theorems 4 and 5.

V. Adapted Cooperative Diversity Gain

Inspired by the work in [12], in this section, we present the ACDG for two scenarios: SIMOSE systems and MISOSE systems. According to [12], the conventional concept of cooperative diversity gain is inappropriate to study security issues in CWNs. Instead, a new concept of cooperative diversity gain, namely, the *ACDG*, is defined in a manner similar to the conventional one.

Before defining the ACDG, we first state that an intercept event occurs when the channel capacity of the link $\mathcal{R}$-D* becomes less than of the link $\mathcal{R}$-E, i.e., $C_{D^*} < C_E$. The intercept probability is then given by

$$\begin{aligned}\mathcal{P}_{\rm int} &\triangleq \mathbb{P}\left\{C_{D^*} < C_E\right\} = \mathbb{P}\left\{\Theta < \Phi\right\}\\ &= 1 - \int_0^\infty F_{\Phi|\Theta}(\theta) f_\Theta(\theta) d\theta\\ &= \int_0^\infty e^{-\frac{\theta}{\gamma_R \Omega_{RE}}} f_\Theta(\theta) d\theta. \end{aligned} \tag{53}$$

We next define λ as the ratio of the average channel gain of the link $\mathcal{R}$-D* to that of the link $\mathcal{R}$-E, i.e.,

$$\lambda \triangleq \frac{\mathbb{E}\left\{\|\mathbf{h}_{\mathcal{R}D^*}\|^2\right\}}{\mathbb{E}\left\{\|\mathbf{h}_{\mathcal{R}E}\|^2\right\}} = \frac{\sum_{m=1}^M \mathbb{E}\left\{|h_{R_m D^*}|^2\right\}}{\sum_{m=1}^M \mathbb{E}\left\{|h_{R_m E}|^2\right\}} = \frac{\Omega_{RD}}{\Omega_{RE}}. \tag{54}$$

Based on the intercept probability $\mathcal{P}_{\rm int}$ and the ratio λ, we finally define the ACDG as

$$d = -\lim_{\lambda \to \infty} \frac{\log \mathcal{P}_{\rm int}}{\log \lambda}. \tag{55}$$

Herein, the similarity between the concept of the ACDG and the conventional definition of diversity can be easily recognized. From the intercept probability point of view, the correlation between the secure metric $\mathcal{P}_{\rm int}$ and the ratio λ can be examined. In this way, the ACDG d is viewed as the key factor that affects the slope of the $\mathcal{P}_{\rm int}$ curve to enhance communication reliability. In the following, we will examine the ACDG for two cases: i) SIMOSE and ii) MISOSE wiretap channels.

A. SIMOSE Wiretap Channel

Theorem 6. *When $M = 1$ and $N \geq 1$, the ACDG of the proposed system is equal to $d = N$.*

Proof. Substituting (21) into (53) and then introducing $t \triangleq \theta/\left(\gamma_R \Omega_{RD}\right)$, we can rewrite (53) as

$$\begin{aligned}\mathcal{P}_{\rm int} &= \int_0^\infty e^{-\lambda t} \left[\sum_{n=1}^N \binom{N}{n} (-1)^{n-1} n e^{-nt}\right] dt\\ &= \int_0^\infty e^{-\lambda t} d\left[(1-e^{-t})^N\right]\\ &= \int_0^\infty e^{-\lambda t} \underbrace{N e^{-t}\left(1-e^{-t}\right)^{N-1}}_{\triangleq \Upsilon_1(t)} dt. \end{aligned} \tag{56}$$

Moreover, $\Upsilon_1(t)$ can be expanded as

$$\begin{aligned}\Upsilon_1(t) &= N\left[1 + \sum_{k=1}^\infty \frac{(-t)^k}{k!}\right]\left[-\sum_{k=1}^\infty \frac{(-t)^k}{k!}\right]^{N-1}\\ &= N t^{N-1} + o(t^N), \end{aligned} \tag{57}$$

in some neighbourhood of $t = 0^+$. Note that the symbol $o(\cdot)$ in (57) is the little-o notation.

Now, in order to investigate the asymptotic behavior of the integral in (56) we apply Watson's lemma [35, Lemma 1.2] and write

$$\begin{aligned}\mathcal{P}_{\rm int} &= N \frac{\Gamma((N-1)+1)}{\lambda^{(N-1)+1}} + o\left(\frac{1}{\lambda^{N+1}}\right)\\ &= \frac{N!}{\lambda^N} + o\left(\frac{1}{\lambda^{N+1}}\right) \text{ as } \lambda \to \infty. \end{aligned} \tag{58}$$

Finally, the ACDG of the proposed system with $M = 1$ and $N \geq 1$ can be derived as

$$d = -\lim_{\lambda \to \infty} \frac{\left[\log(N!) - \log\left(\lambda^N\right)\right]}{\log \lambda} = N. \tag{59}$$

This result reveals that $\mathcal{P}_{\rm int}$ decreases inversely with N, and therefore the security performance is improved by increasing N. This completes the proof. □

B. MISOSE Wiretap Channel

Theorem 7. *When $N = 1$ and $M \geq 1$, the ACDG of the proposed system is equal to $d = M$.*

Proof. Substituting (31) into (53) and then introducing $t \triangleq \theta/\left(\gamma_R \Omega_{RD}\right)$, we can rewrite (53) as

$$\begin{aligned}\mathcal{P}_{\rm int} &= \int_0^\infty e^{-\lambda t}\left[e^{-t}\sum_{m=0}^{M-1}\frac{1}{m!}\left(t^m - m t^{m-1}\right)\right] dt\\ &= \int_0^\infty e^{-\lambda t} \underbrace{\left[e^{-t}\frac{t^{M-1}}{(M-1)!}\right]}_{\triangleq \Upsilon_2(t)} dt. \end{aligned} \tag{60}$$

Moreover, $\Upsilon_2(t)$ can be expanded as

$$\Upsilon_2(t) = \left[1 + \sum_{k=1}^\infty \frac{(-t)^k}{k!}\right]\frac{t^{M-1}}{(M-1)!} = \frac{t^{M-1}}{(M-1)!} + o\left(t^M\right), \tag{61}$$

in some neighbourhood of $t = 0^+$.

Therefore, Watson's lemma is applicable to (60) and we can express

$$\begin{aligned}\mathcal{P}_{\rm int} &= \frac{1}{(M-1)!}\frac{\Gamma((M-1)+1)}{\lambda^{(M-1)+1}} + o\left(\frac{1}{\lambda^{M+1}}\right)\\ &= \frac{M}{\lambda^M} + o\left(\frac{1}{\lambda^{M+1}}\right) \text{ as } \lambda \to \infty. \end{aligned} \tag{62}$$

Finally, the ACDG of the proposed system with $N = 1$ and $M \geq 1$ can be written as

$$d = -\lim_{\lambda \to \infty} \frac{\left[\log M - \log \lambda^M\right]}{\log \lambda} = M. \tag{63}$$

This result reveals that $\mathcal{P}_{\rm int}$ decreases inversely with M, therefore the security performance is improved by increasing M. This completes the proof. □

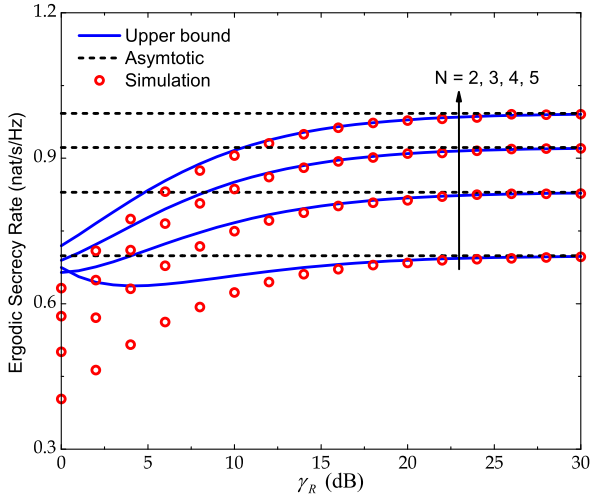

Fig. 2. Ergodic secrecy rate and its upper bound versus γ_R. System parameters: $M = 1$, $N = \{2, \ldots, 6\}$, $\Omega_{RD} = 2.5$, and $\Omega_{RE} = 4$.

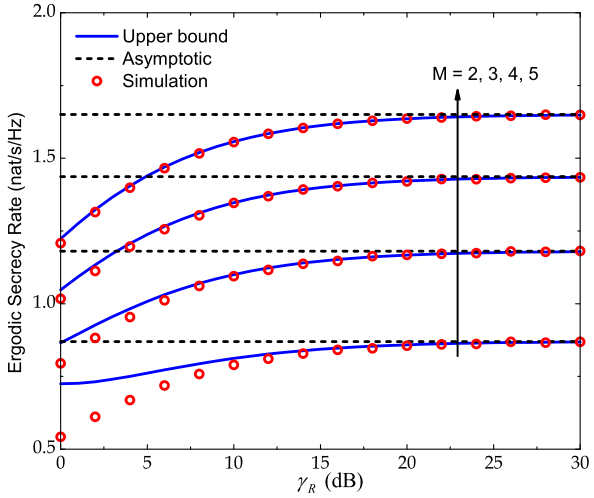

Fig. 3. Ergodic secrecy rate and its upper bound versus γ_R. System parameters: $M = \{2, \ldots, 6\}$, $N = 1$, $\Omega_{RD} = 2.5$, and $\Omega_{RE} = 4$.

VI. Numerical Results and Discussion

This section gives some numerical examples to verify the analysis presented in Sections III–V, and illustrate the key behaviors of the system when different network parameters are varied. Without loss of generality, N_0 is set to 0 dB, and so γ_R is referred to as P_R.

In Figs. 2 and 3, the mean channel powers of the links R_m-D_n and R_m-E are set to $\Omega_{RD} = 2.5$ and $\Omega_{RE} = 4$ respectively. Fig. 2 considers the proposed system with $M = 1$ and $N = \{2, 3, 4, 5, 6\}$, whereas Fig. 3 considers the proposed system with $M = \{2, 3, 4, 5, 6\}$ and $N = 1$. For each figure, we observe that the upper bound gets closer to the ergodic SR as γ_R (or P_R) increases from 0 dB to 30 dB. This can be easily explained by assessing that $E_1\left(\frac{1+\theta}{\gamma_R \Omega_{RE}}\right) \approx E_1\left(\frac{\theta}{\gamma_R \Omega_{RE}}\right)$ with large enough θ due to the fact that $\theta = \gamma_R \|\mathbf{h}_{RD^*}\|^2$. On this observation, the upper bound can be referred to as an approximation to the ergodic SR at high γ_R. Moreover, the asymptotic line agrees exactly with both the simulation and the upper bound at high γ_R, which confirms again the correctness of our analyses.

In Fig. 4, we show the ergodic SR for the case of a very large MIMO relaying system. Although M is assumed to approach to infinity, we illustrate a more practical scenario with $M = \{50, 100, 150\}$. For each given M, we consider $N = \{1, 2, 3\}$ for comparison. Likewise, we choose $\Omega_{RD} = 2.5$ and $\Omega_{RE} = 4$. The figure shows the convergence of the ergodic SR (as stated in Theorem 3) in the case that M is much greater than N. When the ratio $\frac{M}{N}$ becomes larger, the agreement between the simulation and the analysis becomes closer. As expected, when $N = 1$ and $M = 50$, the simulated points lie slightly lower than the analytical curve because the analysis is intended for $M \to \infty$. However, they nearly coincide with each other when $N = 1$ and $M = 150$. This suggests that exact agreement is achievable when $N = 1$ and M takes very large number.

Figs. 5 and 6 show the secrecy outage probabilities in two scenarios of interest, the proposed system with $M = 1$ (i.e., the SIMOSE scenario), and the proposed system with $N = 1$ (i.e., the MISOSE scenario). We also choose $\Omega_{RD} = 2.5$, and $\Omega_{RE} = 4$. The outage threshold is chosen to be $\epsilon = 0.5 \ln 2$ (in nat/s/Hz). As we can see from these figures, when γ_R increases from 0 dB to 40 dB, the secrecy outage probabilities decrease slightly, while increasing N (the SIMOSE scenario) or M (the MISOSE scenario) improves the system performance more significantly. These observations suggest that increasing the number of relaying/destination nodes is a much more effective strategy than increasing the transmit power at the relays.

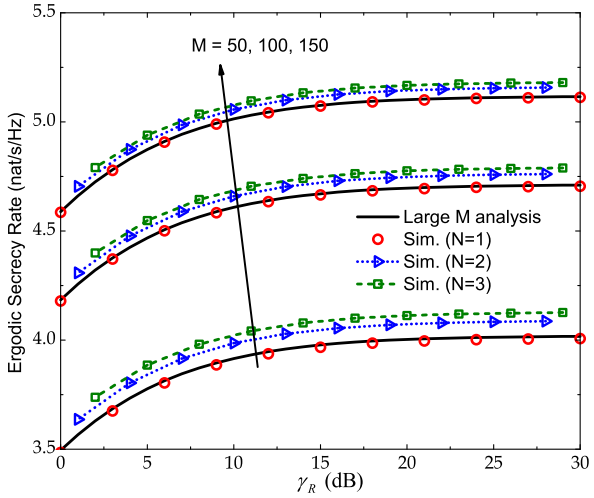

Fig. 4. Ergodic secrecy rate versus γ_R. System parameters: $M = \{50, 100, 150\}$, $N = \{1, 2, 3\}$, $\Omega_{RD} = 2.5$, and $\Omega_{RE} = 4$.

Figs. 7 and 8 show the intercept probabilities versus the ratio $\lambda = \frac{\Omega_{RD}}{\Omega_{RE}}$ in two scenarios of interest, namely, SIMOSE and MISOSE. For each of these figures, we can see that the worst case occurs when $M = 1$ and $N = 1$, while the intercept probability decreases strongly with the number of nodes and λ. As proved in Theorems 6 and 7, the number of nodes is equal to the ACDG, which serves to shift the intercept probability

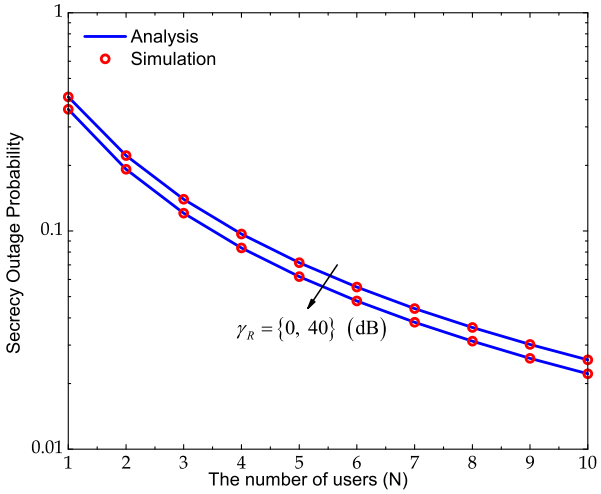

Fig. 5. Secrecy outage probability versus N. System parameters: $M = 1$, $\Omega_{RD} = 5$, $\Omega_{RE} = 2$, $\epsilon = 0.5 \ln 2$ nat/s/Hz, and $\gamma_R = \{0, 40\}$ dB.

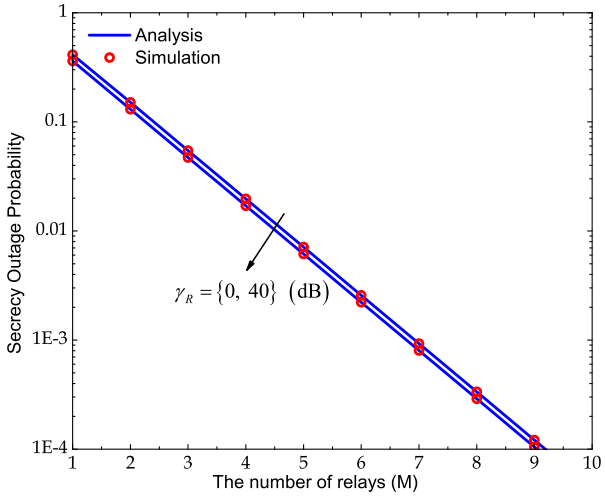

Fig. 6. Secrecy outage probability versus M. System parameters: $N = 1$, $\Omega_{RD} = 5$, $\Omega_{RE} = 2$, $\epsilon = 0.5 \ln 2$ nat/s/Hz, and $\gamma_R = \{0, 40\}$ dB.

curves to the left and therefore improves the reliability of the proposed system from the security point of view. Furthermore, these figures reveal striking similarities of the ACDG to the conventional cooperative diversity gain. As such, the concept of the ACDG seems to be more compatible with security issue of wireless networks than the concept of traditional diversity gain.

VII. Conclusions

We have considered the use of cooperative beamforming and user selection for relay network security. First, we have analyzed the ergodic SRs for three cases: SIMOSE systems ($M = 1$, $N \geq 2$), MISOSE systems ($M \geq 2$, $N = 1$), and very large scale MIMOSE systems ($M \to \infty$, finite N). Bounds on and asymptotic expressions for the ergodic SR for the first two cases, and an exact expression for the ergodic SR at very large M for the third case have been derived. Secondly, we have evaluated the security performance for SIMOSE and MISOSE systems in terms of outage probability. We have quantified the ACDG, similar to conventional cooperative diversity gain, for SIMOSE and MISOSE systems. The validity of our expressions have been verified through simulation results. For future work, we plan to investigate the more generic case of the proposed network and the effects of other factors, e.g. imperfect channel state information.

Appendix

A. Proof of Lemma 1

Proof. It is clear from (18) that proving Lemma 1 is equivalent to proving

$$\lim_{\gamma_R \to \infty} \mathbb{E}_\Theta \left\{ E_1 \left(\frac{1+\theta}{\gamma_R \Omega_{RE}} \right) \right\} = \lim_{\gamma_R \to \infty} \mathbb{E}_\Theta \left\{ E_1 \left(\frac{\theta}{\gamma_R \Omega_{RE}} \right) \right\}. \quad (64)$$

First, we rewrite the left hand side (LHS) of (64) as

$$\begin{aligned} \text{LHS}_{(64)} &= \lim_{\gamma_R \to \infty} \int_0^\infty E_1 \left(\frac{1+\theta}{\gamma_R \Omega_{RE}} \right) f_\Theta(\theta) d\theta \\ &= \lim_{\gamma_R \to \infty} \int_0^\infty \underbrace{E_1 \left(\frac{1+\gamma_R z}{\gamma_R \Omega_{RE}} \right) f_{\|\mathbf{h}_{\mathcal{R}D^*}\|^2}(z)}_{\hbar_{\gamma_R}(z)} dz \end{aligned} \quad (65)$$

where $f_\Theta(\theta)$ is given in (8) and $f_{\|\mathbf{h}_{\mathcal{R}D^*}\|^2}(z) = \gamma_R f_\Theta(\gamma_R z)$ due to the relation in (6). Additionally, it is easy to confirm that $f_{\|\mathbf{h}_{\mathcal{R}D^*}\|^2}(z)$ is no longer dependent on γ_R, while $E_1 \left(\frac{1+\gamma_R z}{\gamma_R \Omega_{RE}} \right)$ is an increasing function of γ_R.

We therefore come to the conclusion that $\hbar_{\gamma_R}(z)$ is increasing in $\gamma_R \geq 0$, is bounded above and has the limit

$$\lim_{\gamma_R \to \infty} \hbar_{\gamma_R}(z) = E_1 \left(\frac{z}{\Omega_{RE}} \right) f_{\|\mathbf{h}_{\mathcal{R}D^*}\|^2}(z). \quad (66)$$

Following these observations, we have

$$\begin{aligned} \text{LHS}_{(64)} &= \lim_{\gamma_R \to \infty} \int_0^\infty \hbar_{\gamma_R}(z) dz \\ &= \int_0^\infty E_1 \left(\frac{z}{\Omega_{RE}} \right) f_{\|\mathbf{h}_{\mathcal{R}D^*}\|^2}(z) dz. \end{aligned} \quad (67)$$

Because the right hand side (RHS) of (67) is independent of γ_R, we can also rewrite it as the limit of a constant, i.e., (67) becomes

$$\begin{aligned} \text{LHS}_{(64)} &= \lim_{\gamma_R \to \infty} \int_0^\infty E_1 \left(\frac{z}{\Omega_{RE}} \right) f_{\|\mathbf{h}_{\mathcal{R}D^*}\|^2}(z) dz \\ &= \lim_{\gamma_R \to \infty} \mathbb{E}_\Theta \left\{ E_1 \left(\frac{\theta}{\gamma_R \Omega_{RE}} \right) \right\} \equiv \text{RHS}_{(64)} \end{aligned} \quad (68)$$

and the proof is complete. □

B. Integral

Proposition 2. *Let us define*

$$\mathcal{I}(\alpha, m) \triangleq \int_0^\infty \theta^m \ln(1+\theta) e^{-\alpha\theta} d\theta, \ m \in \mathbb{N}. \quad (69)$$

Then $\mathcal{I}(\alpha, m)$ can be expressed in two ways:

- *Either [29, Eq.(4.222.8)]*

$$\mathcal{I}(\alpha,m) = \alpha^{-(m+1)} \sum_{k=0}^{m} \frac{m!}{(m-k)!} \left[\frac{(-1)^{m-k} e^{\alpha} E_1(\alpha)}{\alpha^{m-k}} + \sum_{h=1}^{m-k} \frac{(h-1)!}{(-1/\alpha)^{m-k-h}} \right] \tag{70}$$

- *or*

$$\mathcal{I}(\alpha,m) = \alpha^{-(m+1)} G_{3,2}^{1,3}\left(\alpha^{-1} \left| \begin{matrix} -m, 1, 1 \\ 1, 0 \end{matrix} \right. \right) \tag{71}$$

where $G_{p,q}^{m,n}\left(z \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right)$ is Meijer G-function [36, Eq.(1.122)].

If $m = 0$, then both (70) *and* (71) *reduce to*

$$\mathcal{I}(\alpha, 0) = \alpha^{-1} e^{\alpha} E_1(\alpha). \tag{72}$$

Proof. Rewriting $\ln(1+\theta)$ in terms of Meijer G-function [37, Eq.(8.4.6.5)], we have

$$\ln(1+\theta) = G_{2,2}^{1,2}\left(\theta \left| \begin{matrix} 1, 1 \\ 1, 0 \end{matrix} \right. \right).$$

Then $\mathcal{I}(\alpha, m)$ can be evaluated as follows:

$$\begin{aligned} \mathcal{I}(\alpha,m) &= \int_0^{\infty} \theta^m G_{2,2}^{1,2}\left(\theta \left| \begin{matrix} 1, 1 \\ 1, 0 \end{matrix} \right. \right) e^{-\alpha\theta} d\theta \\ &= L\left\{ \theta^m G_{2,2}^{1,2}\left(\theta \left| \begin{matrix} 1, 1 \\ 1, 0 \end{matrix} \right. \right); \alpha \right\} \\ &= \alpha^{-(m+1)} H_{3,2}^{1,3}\left[\alpha^{-1} \left| \begin{matrix} (-m, 1), (1, 1), (1, 1) \\ (1, 1), (0, 1) \end{matrix} \right. \right] \end{aligned} \tag{73}$$

where $L\{f(\theta); \alpha\}$ denotes the Laplace transform [36, Eq. (2.11)] and $H_{p,q}^{m,n}\left[z \left| \begin{matrix} (a_p, A_p) \\ (b_q, B_q) \end{matrix} \right. \right]$ is the H-function [36, Eq. (1.2)]. The last equality is obtained by using the Laplace transform of the Meijer G-function [36, Eq. (2.29)]. Evaluating the RHS of (73) again with the help of [37, Eq. (8.3.2.21)], i.e. $H_{p,q}^{m,n}\left[z \left| \begin{matrix} (a_p, 1) \\ (b_q, 1) \end{matrix} \right. \right] = G_{p,q}^{m,n}\left(z \left| \begin{matrix} (a_p) \\ (b_q) \end{matrix} \right. \right)$, we arrive at (71). In addition, if $m = 0$, we can apply directly [29, Eq. (4.337.2)] to (69) in order to obtain (72). We thus complete the proof. □

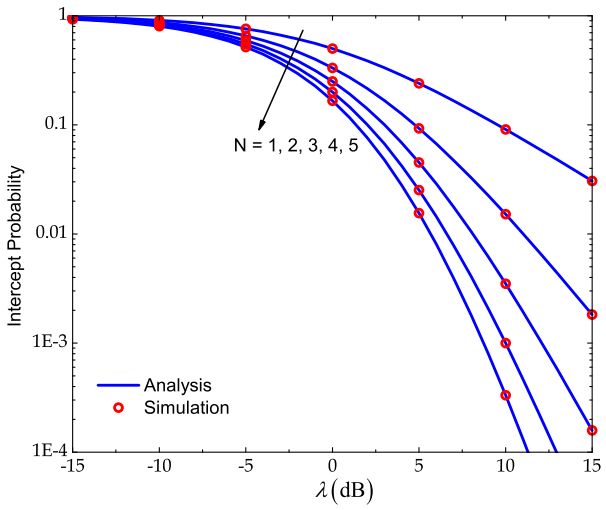

Fig. 7. Intercept probability versus $\lambda = \Omega_{RD}/\Omega_{RE}$. The proposed system has a single relay, and a group of $N = \{1, 2, 3, 4, 5\}$ users.

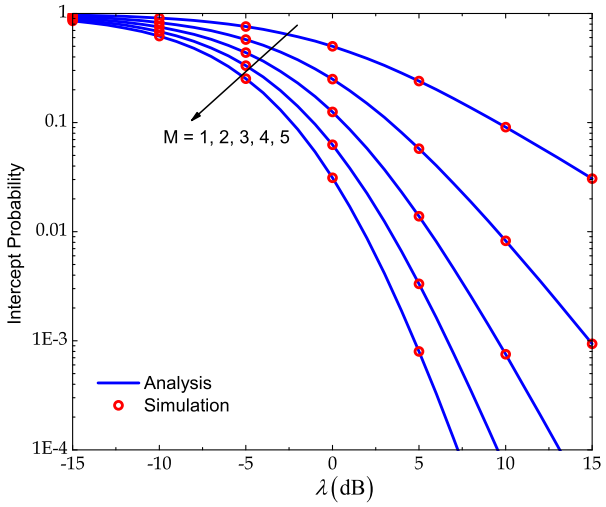

Fig. 8. Intercept probability versus $\lambda = \Omega_{RD}/\Omega_{RE}$. The proposed system has a single user, and a group of $M = \{1, 2, 3, 4, 5\}$ relays.

REFERENCES

[1] K. C. Chan and S. H. G. Chan, "Key management approaches to offer data confidentiality for secure multicast," *IEEE Network Mag.*, vol. 17, no. 5, pp. 30–39, Sep. 2003.

[2] J. Yang, L. Gao, and Y. Zhang, "Improving memory encryption performance in secure processors," *IEEE Trans. Computers*, vol. 54, no. 5, pp. 630–640, May 2005.

[3] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2006, pp. 356–360.

[5] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys and Tutorials*, vol. 15, no. 1, pp. 428–445, Jan. 2013.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

[7] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[13] A. Jindal, C. Kundu, and R. Bose, "Secrecy outage of dual-hop AF relay system with relay selection without eavesdropper's CSI," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1759–1762, Oct. 2014.

[14] E. R. Alotaibi and K. A. Hamdi, "Relay selection for multi-destination in cooperative networks with secrecy constraints," in *Proc. IEEE Vehicular Tech. Conf. (VTC Fall)*, Vancouver, Canada, Sep. 2014, pp. 14–17.

[15] L. Wang, S. Xu, W. Yang, W. Yang, and Y. Cai, "Security performance of multiple antennas multiple relaying networks with outdated relay selection," in *Proc. IEEE Wireless Commun. and Signal Process. (WCSP)*, Hefei, China, Oct. 2014, pp. 1–6.

[16] J. Yang, I. M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[17] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Info. Foren. Sec.*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[18] T. T. Tran and H. Y. Kong, "CSI-secured orthogonal jamming method for wireless physical layer security," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 841–844, May 2014.

[19] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *IEEE Journal of Commun. and Networks*, vol. 14, no. 4, pp. 364–373, Aug. 2012.

[20] X. Chen, L. Lei, H. Zhang, and C. Yuen, "On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, Australia, Jun. 2014, pp. 2052–2057.

[21] M. Qian, C. Liu, and Y. Fu, "Distributed beamforming designs to improve physical layer security in wireless relay networks," *EURASIP J. Advances in Signal Process.*, vol. 1, no. 56, pp. 1687–6180, Apr. 2014.

[22] 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. Info. Foren. Sec.*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[23] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Info. Foren. Sec.*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[24] Z. Liu, X. Zhang, C. Chen, and H. Xiang, "Combined relay selection and secure beamforming for decode-and-forward networks with multiple eavesdroppers," in *Proc. IEEE Wireless Commun. and Signal Process. (WXSP)*, Hangzhou, China, Oct. 2013, pp. 1–6.

[25] X. Liu, F. Gao, G. Wang, and X. Wang, "Joint beamforming and user selection in multicast downlink channel under secrecy-outage constraint," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 82–85, Jan. 2014.

[26] S. S. Ikki and M. H. Ahmed, "Performance analysis of adaptive decode-and-forward cooperative diversity networks with best-relay selection," *IEEE Trans. Commun.*, vol. 58, no. 1, pp. 68–72, Jan. 2010.

[27] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, 1st ed. New York: Cambridge Univ. Press, 2005.

[28] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. USA: Govt. Print. Off., 1970.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. USA: Academic Press, 2007.

[30] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[31] Y. Yang, Q. Li, W. K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[32] V. A. Aalo, "Performance of maximal-ratio diversity systems in a correlated Nakagami-fading environment," *IEEE Trans. Commun.*, vol. 43, no. 8, pp. 2360–2369, Aug. 1995.

[33] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser mimo systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[34] H. Cramer, *Random Variables and Probability Distributions*. Cambridge, UK: Cambridge University Press, 1970.

[35] R. B. Paris and D. Kaminski, *Asymptotics and Mellin-Barnes Integrals*. Cambridge, UK: Cambridge University Press, 2001.

[36] A. M. Mathai, R. K. Saxena, and H. J. Haubold, *The H-Function: Theory and Applications*. New York: Springer, 2010.

[37] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series, Volume 3: More Special Functions*. New York: Gordon and Breach Science, 1990.

Tiep M. Hoang was born in Daklak, Vietnam, in 1989. He received the B.S. degree in Electrical Engineering from Ho Chi Minh City University of Technology, Vietnam, in 2012, and the M.S. degree in Electrical Engineering from Kyung Hee University, Yongin, Korea, in 2014. He is now with Duy Tan University, Vietnam, as a Research Assistant. His current research interests include cooperative networks and wireless security.

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 cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-waves communications, and localization for radios and networks. He is the author or co-author of 170 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 ON SELECTED AREAS IN 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.

Himal A. Suraweera (S'04, M'07, SM'15) received the B.Sc. degree (first class honors) in Electrical and Electronic Engineering, Peradeniya University, Sri Lanka, in 2001 and the Ph.D. degree from Monash University, Melbourne, Australia, in 2007. He was also awarded the 2007 Mollie Holman Doctoral and 2007 Kenneth Hunt Medals for his doctoral thesis upon graduating from Monash University.

From October 2006 to January 2007 he was at Monash University as a Research Associate. From February 2007 to June 2009, he was at the center for Telecommunications and Microelectronics, Victoria University, Melbourne, Australia as a Research Fellow. From July 2009 to January 2011, he was with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore as a Research Fellow. From January 2011 to May 2013, he was a Post-Doctoral Research Associate at the Singapore University of Technology and Design, Singapore. Currently he is a Senior Lecturer at the Department of Electrical and Electronic Engineering, University of Peradeniya. His main research interests include cooperative communications, energy harvesting and Green communications, full-duplex communications, massive MIMO, cognitive radio and wireless security.

Dr. Suraweera serves as an editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS and the Green Communications and Networking Series of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received an IEEE Communications Letters exemplary reviewer certificate in 2009, two IEEE Wireless Communications Letters exemplary certificates in 2012 and 2013 and an IEEE Transactions on Vehicular Technology Top Reviewer Award in 2013. He received an IEEE Communications Society Asia-Pacific Outstanding Young Researcher Award in 2011 and the Best Paper Award at the WCSP 2013 Conference.

Chintha Tellambura (F'11) received the B.Sc. degree (with first-class honor) from the University of Moratuwa, Sri Lanka, in 1986, the M.Sc. degree in Electronics from the University of London, United Kingdom, in 1988, and the Ph.D. degree in Electrical Engineering from the University of Victoria, Canada, in 1993. He was a Postdoctoral Research Fellow with the University of Victoria (1993-1994) and the University of Bradford (1995-1996). He was with Monash University, Australia, from 1997 to 2002. Presently, he is a Professor with the Department of Electrical and Computer Engineering, University of Alberta. His current research interests include the design, modelling and analysis of cognitive radio networks, heterogeneous cellular networks and multiple-antenna wireless networks.

Prof. Tellambura served as an editor for both IEEE Transactions on Communications (1999-2011) and IEEE Transactions on Wireless Communications (2001-2007) and was the Area Editor for Wireless Communications Systems and Theory in the IEEE Transactions on Wireless Communications during 2007-2012. Prof. Tellambura and co-authors received the Communication Theory Symposium best paper award in the 2012 IEEE International Conference on Communications, Ottawa, Canada. He is the winner of the prestigious McCalla Professorship and the Killam Annual Professorship from the University of Alberta. Prof. Tellambura has authored or coauthored over 480 journal and conference publications with total citations more than 10,000 and an h-index of 52 (Google Scholar).

H. Vincent Poor (S'72, M'77, SM'82, F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. His research interests are in the areas of information theory, statistical signal processing and stochastic analysis, and their applications in wireless networks and related fields. Among his publications in these areas are the recent books *Principles of Cognitive Radio* (Cambridge University Press, 2013) and *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge University Press, 2014).

Dr. Poor is a member of the National Academy of Engineering, the National Academy of Sciences, and is a foreign member of Academia Europaea and the Royal Society. He is also a fellow of the American Academy of Arts and Sciences, the Royal Academy of Engineering (U. K), and the Royal Society of Edinburgh. He received the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, the 2015 EURASIP Athanasios Papoulis Award, and honorary doctorates from Aalborg University, Aalto University, the Hong Kong University of Science and Technology, and the University of Edinburgh.