Cooperative Beamforming and User Selection for Physical Layer Security in Relay Systems

Tiep M. Hoang[†], Trung Q. Duong[♯], Himal A. Suraweera[§], Chintha Tellambura[¶], and H. Vincent Poor[‡]
[†]Duy Tan University, Vietnam (e-mail: hmt1803@gmail.com)
[♯]Queen's University Belfast, UK (e-mail: trung.q.duong@qub.ac.uk)
[§]University of Peradeniya, Sri Lanka (e-mail: himal@ee.pdn.ac.lk)
[¶]University of Alberta, Canada (e-mail: chintha@ece.ualberta.ca)
[‡] Princeton University, Princeton, NJ, USA (e-mail: poor@princeton.edu)

***Abstract*—A cooperative network in which confidential messages are conveyed from a source to a legitimate destination with the help of decode-and-forward relays in the presence of a malicious eavesdropper is considered. Tight upper bounds on the ergodic secrecy rate are derived in the cases of i) cooperative beamforming and ii) multi-user selection. Further, a new concept of cooperative diversity gain, namely, adapted cooperative diversity gain (ACDG), is investigated. It is shown that the ACDG can be seen as an effective metric to evaluate the security level of a cooperative wireless network in the presence of eavesdroppers. Also, the ACDG obtained in the cooperative beamforming scenario is equal to the traditional cooperative diversity gain of traditional multiple-input single-output networks, while the ACDG obtained in the multiuser scenario is equal to that of traditional single-input multiple-output networks.**

I. Introduction

Due to the popularity of various wireless devices and applications in recent years, security of communication systems has become an important issue of research. The broadcast nature of the wireless channel is a key factor in making it vulnerable to eavesdropping. To this end, while most security solutions focus on methods from an upper layer perspective such as data encryption, secret key-generation, etc. Recent solutions have focused also on providing enhanced security using physical layer techniques [1]. Initial information and communication theoretic studies of physical layer security (PLS) date back to the seminal work of Wyner [2] and it remains a challenging yet promising field of study [3].

In order to deal with the security vulnerability, various PLS techniques such as the use of multiple antennas/relaying/jamming and user selection have been advocated [4]–[8]. Among the current set of solutions toward the design of secured wireless networks, node cooperation in a cooperative wireless network (CWN) is a noticeable option. Node cooperation, for instance relay selection techniques [4]–[6], [9]–[12] and jamming methods [9], [10], [13]–[15], allow systems with single antenna nodes to exploit the benefits of multiple antenna systems. In addition, the design of cooperative beamforming techniques for PLS in CWNs where nodes can collaboratively work to build a virtual beam towards the receiver have been discussed in [6], [9]–[11] and [13]–[19].

There is a rich body of literature that has investigated PLS of dual-hop transmission with single/multiple relays and single/-multiple eavesdropper/s; see for example [8] and [16]–[20]. However, the authors in [8] did not take beamforming into account while the authors in [16]–[20] assumed cooperative beamforming at the relays but did not consider multiple users. In contrast, in this paper, we consider the use of cooperative beamforming and user selection in order to enjoy the benefits of spatial diversity from the exploitation of node cooperation.

Traditionally, cooperative diversity gain is used to evaluate the performance of a CWN at high signal-to-noise ratio (SNR). This approach, however, is not suitable for a secured CWN. Alternatively, [4] introduced a new metric to evaluate the secure performance of secured CWNs considering the ratio of the legitimate channel gain to the eavesdropping channel gain instead of the SNR. Motivated by the work in [4], we also evaluate the secure performance of our proposed system through the new metric, which we shall call the *adapted cooperative diversity gain* (ACDG).

In this work, we consider two system models i) a WCN with one relay and multiple users, i.e., the single-input multiple-output in the presence of single eavesdropper (SIMOSE) wiretap channel, and ii) a WCN with multiple relays and a single user, i.e., the multiple-input single-output in the presence of single eavesdropper (MISOSE) wiretap channel. We derive upper bounds on the ergodic secrecy rate for both scenarios. Based on the concept of the ACDG, we quantify the secure performance of the proposed WCNs and show that the ACDG of a virtual SIMOSE (or MISOSE) system is equal to the diversity gain of a single-input multiple-output (SIMO) (or multiple-input single output, MISO) system. Thus, the ACDG is seen as the counterpart of cooperative diversity gain in secured WCNs because of the involvement of the security aspect.

Throughout the paper, we use the following 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 [21, Eq. (5.1.4)] and the hypergeometric function [22, Eq. (9.14.2)], respectively.

II. System Model

We consider a cooperative relay network in which there is a single source, a set of M trusted relays, a set of N destinations, and one eavesdropper (cf. Fig. 1). All the nodes are single-antenna devices and operate 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. Additionally, it is noted that there are no direct links S-$\mathcal{D}$ and S-E. 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 [23]), and all relays (i.e., the set $\mathcal{R}$) perform collaborative beamforming (e.g., see [16], [17], [20] and [24]). $\mathcal{R}$ 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 $n_E \sim \mathcal{CN}(0, N_0)$.

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

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

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

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

Let Θ be the instantaneous 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 $\gamma_R = P_R/N_0$. The cumulative distribution function (cdf) and the probability density function (pdf) of Θ are presented in Appendix A.

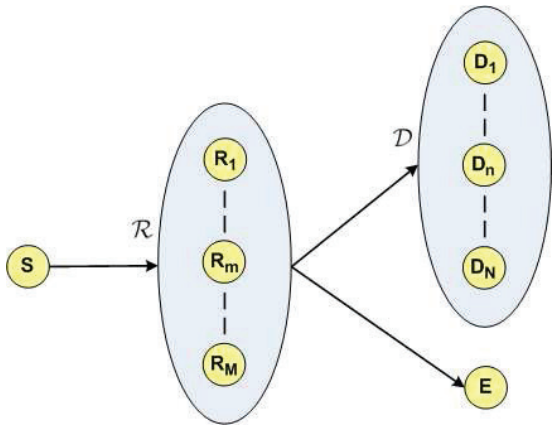

Fig. 1. A wireless relay system that consists of a source, a set of M relays, a set of N users, and an eavesdropper.

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

$$\Phi = \left(\frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}E}^{\dagger}\mathbf{h}_{\mathcal{R}D^*}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\right)\underbrace{\left(\frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}D^*}^{\dagger}\mathbf{h}_{\mathcal{R}E}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\right)}_{\mathcal{Z}} = |\mathcal{Z}|^2. \tag{7}$$

It is apparent that SNR appears in (7) 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 get

$$\begin{aligned}\mathcal{Z}\,|\mathbf{h}_{\mathcal{R}D^*} &\sim \mathcal{CN}\left(0, \frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}D^*}^{\dagger}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\Omega_{RE}\mathbf{I}\frac{\sqrt{\gamma_R}\mathbf{h}_{\mathcal{R}D^*}}{\|\mathbf{h}_{\mathcal{R}D^*}\|}\right)\\ \Leftrightarrow \mathcal{Z}\,|\mathbf{h}_{\mathcal{R}D^*} &\sim \mathcal{CN}(0, \gamma_R\Omega_{RE})\end{aligned} \tag{8}$$

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 $\Phi\,|\Theta$ because the fact that 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

The achievable secrecy rate in nat/s/Hz can be defined as

$$C_\Delta(\Theta, \Phi) = \left[\ln\left(\frac{1+\Theta}{1+\Phi}\right)\right]^+ \tag{9}$$

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

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

$$\begin{aligned}\overline{C}_\Delta &= \mathbb{E}_\Theta\left\{\mathbb{E}_{\Phi|\Theta}\left\{C_\Delta(\Theta, \Phi)\,|\Theta = \theta\right\}\right\}\\ &= \mathbb{E}_\Theta\left\{\int_0^\theta \ln\left(\frac{1+\theta}{1+\phi}\right) f_{\Phi|\Theta}(\phi)\, d\phi\right\}\\ &= \mathcal{A} - \mathcal{B}.\end{aligned} \tag{10}$$

[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 $\mathbf{y} \sim \mathcal{CN}\left(\mathbf{A}\boldsymbol{\mu} + \mathbf{b}, \mathbf{A}\boldsymbol{\Sigma}\mathbf{A}^{\dagger}\right)$ [25, Appendix A].

where the terms $\mathcal{A}$ and $\mathcal{B}$ can be expressed as

$$\begin{aligned}\mathcal{A} &= \mathbb{E}_\Theta\left\{\ln(1+\theta)F_{\Phi|\Theta}\left(\theta\right)\right\}\\ &= \mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} - \mathbb{E}_\Theta\left\{\ln(1+\theta)e^{-\theta/(\gamma_R\Omega_{RE})}\right\}, \quad (11)\\ \mathcal{B} &= \mathbb{E}_\Theta\left\{\int_0^\theta \ln\left(1+\phi\right) f_{\Phi|\Theta}\left(\phi\right) d\phi\right\}\\ &= e^{1/(\gamma_R\Omega_{RE})}\left[E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right) - \mathbb{E}_\Theta\left\{E_1\left(\frac{1+\theta}{\gamma_R\Omega_{RE}}\right)\right\}\right]\\ &\quad - \mathbb{E}_\Theta\left\{\ln(1+\theta)e^{-\theta/(\gamma_R\Omega_{RE})}\right\}. \quad (12)\end{aligned}$$

Substituting both (11) and (12) into (10), we obtain

$$\begin{aligned}\langle C_\Delta\rangle &= \mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} - e^{1/(\gamma_R\Omega_{RE})}E_1\left(1/(\gamma_R\Omega_{RE})\right)\\ &\quad + e^{1/(\gamma_R\Omega_{RE})}\,\mathbb{E}_\Theta\left\{E_1\left(\frac{1+\theta}{\gamma_R\Omega_{RE}}\right)\right\}\\ &\le \mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} - e^{1/(\gamma_R\Omega_{RE})}E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right)\\ &\quad + e^{1/(\gamma_R\Omega_{RE})}\,\mathbb{E}_\Theta\left\{E_1\left(\theta/(\gamma_R\Omega_{RE})\right)\right\}\\ &\triangleq \langle C_\Delta\rangle^{\text{upper}} \quad (13)\end{aligned}$$

where the inequality follows from the fact that $E_1(x) = \int_x^\infty \frac{e^{-u}}{u}du$ is a decreasing function. Eq. (13) shows that the ergodic secrecy rate $\langle C_\Delta\rangle$ has an upper bound $\langle C_\Delta\rangle^{\text{upper}}$. Further, at high SNR, we can show that $\langle C_\Delta\rangle^{\infty} \triangleq \lim_{\gamma_R\to\infty}\langle C_\Delta\rangle = \lim_{\gamma_R\to\infty}\langle C_\Delta\rangle^{\text{upper}}$ which reveals that $\langle C_\Delta\rangle^{\text{upper}}$ is also exact in the asymptotic sense. However, due to limited space we opted not to report the detailed proof of this result.

A. SIMOSE Wiretap Channel

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

$$\begin{aligned}\langle C_\Delta\rangle^{\textit{upper}} &= \sum_{n=1}^{N}\binom{N}{n}(-1)^{n-1}\left\{e^{\frac{1}{\gamma_R\Omega_{RE}}}\ln\left(1+n\frac{\Omega_{RE}}{\Omega_{RD}}\right)\right.\\ &\left. + e^{\frac{n}{\gamma_R\Omega_{RD}}}E_1\left(\frac{n}{\gamma_R\Omega_{RD}}\right) - e^{\frac{1}{\gamma_R\Omega_{RE}}}E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right)\right\}. \quad (14)\end{aligned}$$

Proof. When $M=1$, the pdf of Θ in (41) reduces to

$$f_\Theta(\theta) = \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{n}{\gamma_R\Omega_{RD}}e^{-\frac{n\theta}{\gamma_R\Omega_{RD}}}. \quad (15)$$

Using the above pdf expression to calculate the expected values in (13), we obtain

$$\mathbb{E}_\Theta\left\{\ln(1+\theta)\right\} = \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}e^{\frac{n}{\gamma_R\Omega_{RD}}}E_1\left(\frac{n}{\gamma_R\Omega_{RD}}\right), \quad (16)$$

$$\mathbb{E}_\Theta\left\{E_1\left(\frac{\theta}{(\gamma_R\Omega_{RE})}\right)\right\} = \sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\ln\left(1+n\frac{\Omega_{RE}}{\Omega_{RD}}\right) \quad (17)$$

after simple manipulations. Finally, substituting (16) and (17) into (13) yields (14). □

B. MISOSE Wiretap Channel

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

$$\begin{aligned}&\langle C_\Delta\rangle^{\textit{upper}}\\ &= e^{\frac{1}{\gamma_R\Omega_{RE}}}\ln\left(1+\frac{\Omega_{RE}}{\Omega_{RD}}\right) + \mathcal{C}_1(\gamma_R) + \sum_{m=1}^{M-1}\frac{1}{m!}\mathcal{C}_2(\gamma_R)\\ &+ e^{\frac{1}{\gamma_R\Omega_{RE}}}\sum_{m=1}^{M-1}\left(\frac{\Omega_{RE}}{\Omega_{RD}+\Omega_{RE}}\right)^m\\ &\quad\times\left[\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\frac{1}{m+1}\,{}_2F_1\left(1,m+1;m+2;\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right.\\ &\quad\left. - \frac{1}{m}\,{}_2F_1\left(1,m;m+1;\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right] \quad (18)\end{aligned}$$

where

$$\mathcal{C}_1(\gamma_R) \triangleq e^{\frac{1}{\gamma_R\Omega_{RD}}}E_1\left(\frac{1}{\gamma_R\Omega_{RD}}\right) - e^{\frac{1}{\gamma_R\Omega_{RE}}}E_1\left(\frac{1}{\gamma_R\Omega_{RE}}\right), \quad (19)$$

$$\begin{aligned}\mathcal{C}_2(\gamma_R) \triangleq \frac{1}{(\gamma_R\Omega_{RD})^m}&\left[\frac{1}{\gamma_R\Omega_{RD}}\mathcal{I}\left(\frac{1}{\gamma_R\Omega_{RD}},m\right)\right.\\ &\left. - m\mathcal{I}\left(\frac{1}{\gamma_R\Omega_{RD}},m-1\right)\right] \quad (20)\end{aligned}$$

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 [22, Eq. (4.222.8)].*

Proof. When $N=1$, the pdf of Θ in (41) reduces to

$$f_\Theta(\theta) = \sum_{m=0}^{M-1}\frac{e^{-\frac{\theta}{\gamma_R\Omega_{RD}}}}{m!\left(\gamma_R\Omega_{RD}\right)^m}\left(\frac{\theta^m}{\gamma_R\Omega_{RD}} - m\theta^{m-1}\right). \quad (21)$$

Using the above pdf expression to calculate the expected values in (13), we obtain

$$\begin{aligned}&\mathbb{E}_\Theta\left\{\ln(1+\theta)\right\}\\ &= e^{\frac{1}{\gamma_R\Omega_{RD}}}E_1\left(\frac{1}{\gamma_R\Omega_{RD}}\right) + \sum_{m=1}^{M-1}\frac{1}{m!\left(\gamma_R\Omega_{RD}\right)^m}\\ &\quad\times\left[\frac{1}{\gamma_R\Omega_{RD}}\mathcal{I}\left(\frac{1}{\gamma_R\Omega_{RD}},m\right) - m\mathcal{I}\left(\frac{1}{\gamma_R\Omega_{RD}},m-1\right)\right], \quad (22)\end{aligned}$$

and

$$\begin{aligned}&\mathbb{E}_\Theta\left\{E_1\left(\theta/\left(\gamma_R\Omega_{RE}\right)\right)\right\}\\ &= \ln\left(1+\frac{\Omega_{RE}}{\Omega_{RD}}\right) + \sum_{m=1}^{M-1}\left(\frac{\Omega_{RE}}{\Omega_{RD}+\Omega_{RE}}\right)^m\\ &\quad\times\left[\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\frac{1}{m+1}\,{}_2F_1\left(1,m+1;m+2;\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right.\\ &\quad\left. - \frac{1}{m}\,{}_2F_1\left(1,m;m+1;\frac{1}{1+\frac{\Omega_{RD}}{\Omega_{RE}}}\right)\right] \quad (23)\end{aligned}$$

after simple manipulations. Finally, substituting (22) and (23) into (13) yields (18). □

IV. Adapted Cooperative Diversity Gain

We state that an intercept event occurs when the channel capacity of the link $\mathcal{R}$-D* becomes less than that of the link $\mathcal{R}$-E. Thus the intercept probability is then given by

$$\mathcal{P}_{\text{int}} = \mathbb{P}\left\{\Theta < \Phi\right\} = \int_0^\infty e^{-\frac{\theta}{\gamma_R \Omega_{RE}}} f_\Theta(\theta) d\theta. \tag{24}$$

According to [4], the traditional diversity gain definition is not appropriate for security issue in secured CWNs. Instead, a different concept of diversity gain, which we call the ACDG, is defined as

$$d = -\lim_{\lambda \to \infty} \frac{\log \mathcal{P}_{\text{int}}}{\log \lambda} \tag{25}$$

where λ is the ratio of average channel gain between $\mathcal{R}$ and D* to that between $\mathcal{R}$ and E, i.e.,

$$\lambda = \frac{\mathbb{E}\left\{\|\mathbf{h}_{\mathcal{R}D^*}\|^2\right\}}{\mathbb{E}\left\{\|\mathbf{h}_{\mathcal{R}E}\|^2\right\}} = \frac{\Omega_{RD}}{\Omega_{RE}}. \tag{26}$$

We now derive the ACDG for SIMOSE and MISOSE systems as follows:

A. SIMOSE Wiretap Channel

Theorem 3. *When $M = 1$ and $N \geq 1$, the ACDG of the SIMOSE system is equal to $d = N$.*

Proof. Substituting (15) into (24) and then evaluating the integral in (24) we have

$$\begin{aligned}\mathcal{P}_{\text{int}} &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^{n-1} n}{\gamma_R \Omega_{RD}} \left(\frac{n}{\gamma_R \Omega_{RD}} + \frac{1}{\gamma_R \Omega_{RE}}\right)^{-1} \\ &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^{n-1} n}{n + \lambda}.\end{aligned} \tag{27}$$

By evaluating the term

$$\begin{aligned}&\binom{N}{n}(-1)^{n-1} n = N! \left[\frac{(-1)^{n-1}}{(n-1)!}\right]\left[\frac{1}{(N-n)!}\right] \\ &= N! \left[(1-n)(2-n)\ldots((n-1)-n)\right]^{-1} \\ &\quad \times \left[((n+1)-n)((n+2)-n)\ldots(N-n)\right]^{-1} \\ &= N! \prod_{\substack{k=1 \\ k \neq n}}^{N} (k-n)^{-1},\end{aligned} \tag{28}$$

we can rewrite (27) as

$$\mathcal{P}_{\text{int}} = N! \sum_{n=1}^{N} \frac{1}{n+\lambda} \prod_{\substack{k=1 \\ k \neq n}}^{N} (k-n)^{-1} = N! \sum_{n=1}^{N} \frac{r_n}{n+\lambda} \tag{29}$$

where

$$r_n = \lim_{\lambda \to -n} \left\{(n+\lambda) \prod_{k=1}^{N} (k+\lambda)^{-1}\right\}, \; n \in \{1, \ldots, N\}. \tag{30}$$

According to the Cauchy residue theorem [26], we can see that r_n appears as the residue of the function $u(\lambda) = \left[\prod_{k=1}^{N}(k+\lambda)\right]^{-1}$ at simple pole $\lambda = -n$. Thus, applying the Cauchy residue theorem to (29), we have

$$\mathcal{P}_{\text{int}} = N! u(\lambda) = N! \prod_{k=1}^{N} (k+\lambda)^{-1}. \tag{31}$$

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

$$d = -\lim_{\lambda \to \infty} \frac{\left[\log(N!) - \log\left(\prod_{k=1}^{N}(k+\lambda)\right)\right]}{\log \lambda} = N. \tag{32}$$

□

B. MISOSE Wiretap Channel

Theorem 4. *When $N = 1$ and $M \geq 1$, the ACDG of the MISOSE system is equal to $d = M$.*

Proof. Substituting (21) into (24) and then evaluating the integral in (24) we have

$$\begin{aligned}\mathcal{P}_{\text{int}} &= \frac{1}{\gamma_R \Omega_{RD}} \left(\frac{1}{\gamma_R \Omega_{RD}} + \frac{1}{\gamma_R \Omega_{RE}}\right)^{-1} \\ &\quad + \sum_{m=1}^{M-1} \left(1 + \frac{\gamma_R \Omega_{RD}}{\gamma_R \Omega_{RE}}\right)^{-m} \left[\left(1 + \frac{\gamma_R \Omega_{RD}}{\gamma_R \Omega_{RE}}\right)^{-1} - 1\right] \\ &= (1+\lambda)^{-M} \underbrace{\left[(1+\lambda)^{M-1} - \lambda \sum_{m=1}^{M-1} (1+\lambda)^{m-1}\right]}_{v(\lambda)}.\end{aligned} \tag{33}$$

Using the binomial theorem, we can express $v(\lambda)$ as

$$v(\lambda) = 1 + \sum_{m=1}^{M-1} \binom{M-1}{m} \lambda^m - \sum_{m=1}^{M-1} \sum_{k=0}^{m-1} \binom{m-1}{k} \lambda^{k+1}. \tag{34}$$

The third term of (34) can be successively analyzed into

$$\begin{aligned}&\sum_{m=1}^{M-1} \sum_{k=0}^{m-1} \binom{m-1}{k} \lambda^{k+1} \\ &= \sum_{l=1}^{M-1} \sum_{m=l}^{M-1} \binom{m-1}{l-1} \lambda^l \overset{(a)}{=} \sum_{l=1}^{M-1} \sum_{m=l}^{M-1} \binom{m-1}{m-l} \lambda^l \\ &= \sum_{l=1}^{M-1} \left[\binom{l-1}{0} + \binom{l}{1} + \ldots \binom{M-2}{M-l-1}\right] \lambda^l \\ &\overset{(b)}{=} \sum_{l=1}^{M-1} \binom{M-1}{M-l-1} \lambda^l \overset{(c)}{=} \sum_{l=1}^{M-1} \binom{M-1}{l} \lambda^l\end{aligned} \tag{35}$$

where the equalities (a) and (c) follow from [21, Eq. (3.1.3)]; the equality (b) is obtained by using [21, Eq. (24.1.1.II.A)]. We then substitute (35) into (34) to get a surprisingly simple expression

$$v(\lambda) = 1. \tag{36}$$

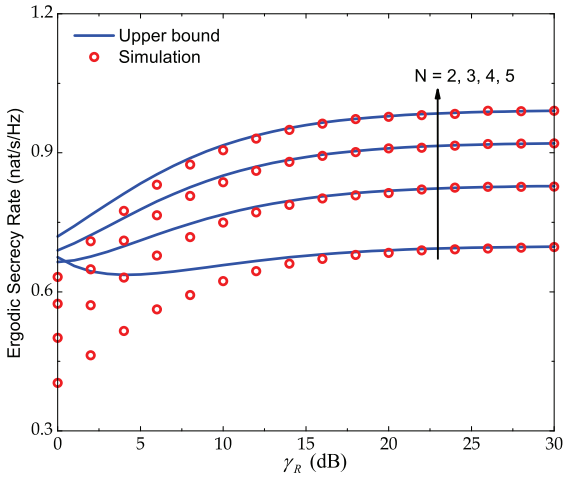

Fig. 2. Ergodic secrecy rate and its upper bound versus γ_R. System parameters: $M = 1$, $N = \{2, \ldots, 6\}$, $\Omega_{RD} = 2.5$, and $\Omega_{RE} = 4$.

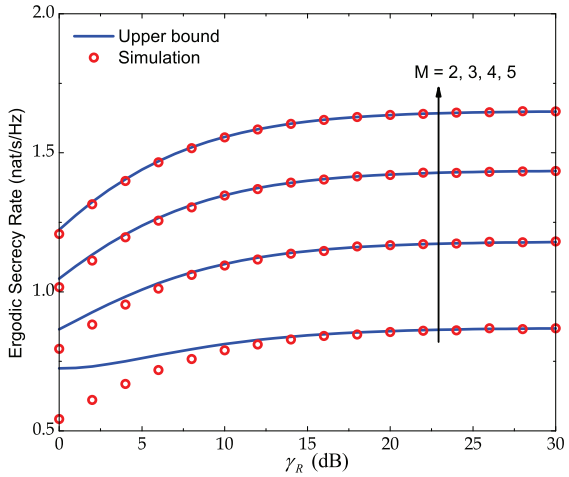

Fig. 3. Ergodic secrecy rate and its upper bound versus γ_R. System parameters: $M = \{2, \ldots, 6\}$, $N = 1$, $\Omega_{RD} = 2.5$, and $\Omega_{RE} = 4$.

As a result, (33) reduces to

$$\mathcal{P}_{\text{int}} = (1+\lambda)^{-M}. \tag{37}$$

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

$$d = -\lim_{\lambda \to \infty} \frac{\log\left[(1+\lambda)^{-M}\right]}{\log \lambda} = M. \tag{38}$$

□

V. Numerical Results and Discussion

In this section, we present some representative numerical examples to verify the analysis presented in previous sections, and illustrate the key behaviors of the system when different network parameters are varied. 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 secrecy rate as γ_R (or P_R when N_0 is set to 0 dB) 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 secrecy rate at high γ_R.

Figs. 4 and 5 show the intercept probability versus the ratio $\lambda = \frac{\Omega_{RD}}{\Omega_{RE}}$ for SIMOSE and MISOSE systems, respectively. In each of these figures, we see that the worst case occurs when $M = 1$ and $N = 1$, while the intercept probability decreases strictly with the number of nodes and λ. As proved in Theorems 3 and 4, the ACDG equals the number of nodes and serves to shift the intercept probability curves to the left and therefore improves the reliability of the SIMOSE and MISOSE systems from a security point of view. Furthermore, these figures reveal striking similarities of the ACDG to the traditional 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.

VI. Conclusions

We have considered the use of cooperative beamforming and user selection for secured WCNs. In particular, our analysis has focused on two cases, namely, SIMOSE systems ($M = 1$, $N \geq 2$) and MISOSE systems ($M \geq 2$, $N = 1$). For each case, we have derived a tight upper bound (and exact in an asymptotic sense) on the ergodic secrecy rate. We have also evaluated the security level in terms of the ACDG, similar to conventional cooperative diversity gain, for SIMOSE and MISOSE systems. We have shown that the ACDGs of SIMOSE and MISOSE systems are respectively equal to the number of users and the number of relays. The validity of our expressions have been verified through extensive simulations results.

Acknowledgement

This research was supported in part by the U.S. National Science Foundation under Grant CMMI-1435778.

Appendix

A. Distribution of Θ

Since $X_n = \gamma_R \|\mathbf{h}_{\mathcal{R}D_n}\|^2 = \sum_{m=1}^{M} \gamma_R |h_{R_m D_n}|^2$ is a sum of independent and identically distributed (i.i.d.) exponential variables, then $X_n \sim \text{Erl}\left(M, \frac{1}{\gamma_R \Omega_{RD}}\right)$. By definition of Θ, we have

$$\Theta = \gamma_R \|\mathbf{h}_{\mathcal{R}D^*}\|^2 = \max_{n=1,\ldots,N} X_n. \tag{39}$$

The CDF of Θ is given by

$$F_\Theta(\theta) = F_{X_n}^N(\theta) = \left[1 - \sum_{m=0}^{M-1} \frac{e^{-\frac{\theta}{\gamma_R \Omega_{RD}}}}{m!} \left(\frac{\theta}{\gamma_R \Omega_{RD}}\right)^m\right]^N \tag{40}$$

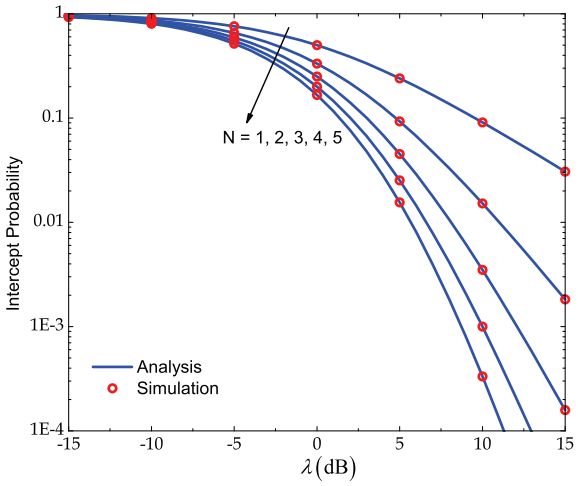

Fig. 4. Intercept probability versus $\lambda = \Omega_{RD}/\Omega_{RE}$. The SIMOSE system has a single relay, and a group of $N = \{1, 2, 3, 4, 5\}$ users.

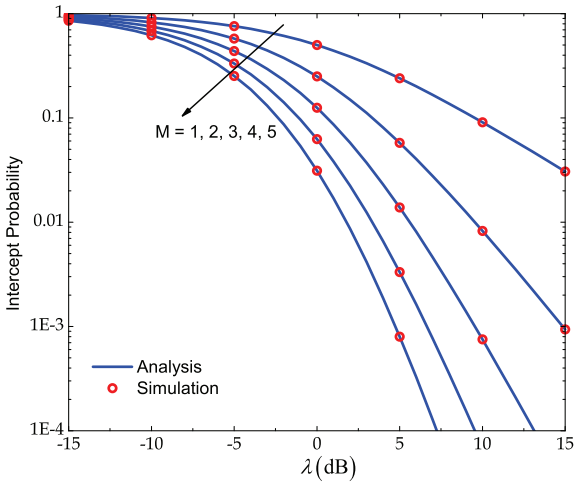

Fig. 5. Intercept probability versus $\lambda = \Omega_{RD}/\Omega_{RE}$. The MISOSE system has a single user, and a group of $M = \{1, 2, 3, 4, 5\}$ relays.

and hence the pdf of Θ is given by

$$f_\Theta(\theta) = dF_\Theta(\theta)/d\theta$$
$$= N\left[1 - \sum_{m=0}^{M-1} \frac{e^{-\frac{\theta}{\gamma_R \Omega_{RD}}}}{m!}\left(\frac{\theta}{\gamma_R \Omega_{RD}}\right)^m\right]^{N-1}$$
$$\times \left[\sum_{m=0}^{M-1}\left(\frac{\theta}{\gamma_R \Omega_{RD}} - m\right)\frac{e^{-\frac{\theta}{\gamma_R \Omega_{RD}}}}{m!}\frac{\theta^{m-1}}{(\gamma_R \Omega_{RD})^m}\right]. \quad (41)$$

REFERENCES

[1] X. Zhou, L. Song, and Y. Zhang, Eds., *Physical Layer Security in Wireless Communications*. Boca Raton, FL: CRC Press, 2013.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.

[8] 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.

[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] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

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

[23] 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.

[24] 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.

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

[26] R. P. Agarwal, K. Perera, and S. Pinelas, *An Introduction to Complex Analysis*. USA: Springer, 2010.