MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

On the Security of Cooperative Single Carrier Systems

Wang, L.; Kim, K.J.; Duong, T.Q.; Elkashlan, M.; Poor, H.V.

TR2014-128 December 2014

Abstract

In this paper, the impact of multiple eavesdroppers on cooperative single carrier systems with multiple relays and multiple destinations is examined. To achieve the secrecy diversity gains in the form of opportunistic selection, a two-stage scheme is proposed for joint relay and destination selection, in which, after the selection of the relay with the minimum effective maximum signal-to-noise ratio (SNR) to a cluster of eavesdroppers, the destination that has the maximum SNR from the chosen relay is selected. In order to accurately assess the secrecy performance, the exact and asymptotic expressions are obtained in closed-form for the ergodic secrecy rate in frequency selective fading. Based on the asymptotic analysis, key design parameters such as multiplexing gain, and power cost are characterized, from which new insights are drawn. Moreover, it is concluded that capacity ceiling occurs when the average received power at the eavesdropper is proportional to the counterpart at the destination.

IEEE Global Communications Conference (GLOBECOM)

On the Security of Cooperative Single Carrier Systems

Lifeng Wang*, Kyeong Jin Kim†, Trung Q. Duong‡, Maged Elkashlan*, and H. Vincent Poor§
*School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK
†Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA
‡School of Electronics, Electrical Engineering, and Computer Science, Queen's University Belfast, Belfast, UK
§Department of Electrical Engineering, Princeton University, Princeton, NJ, USA

***Abstract*—In this paper, the impact of multiple eavesdroppers on cooperative single carrier systems with multiple relays and multiple destinations is examined. To achieve the secrecy diversity gains in the form of opportunistic selection, a two-stage scheme is proposed for joint relay and destination selection, in which, after the selection of the relay with the minimum effective maximum signal-to-noise ratio (SNR) to a cluster of eavesdroppers, the destination that has the maximum SNR from the chosen relay is selected. In order to accurately assess the secrecy performance, the exact and asymptotic expressions are obtained in closed-form for the ergodic secrecy rate in frequency selective fading. Based on the asymptotic analysis, key design parameters such as multiplexing gain, and power cost are characterized, from which new insights are drawn. Moreover, it is concluded that capacity ceiling occurs when the average received power at the eavesdropper is proportional to the counterpart at the destination.**

I. Introduction

Recently, the concept of physical (PHY) layer security has attracted considerable interest amongst wireless network designers. In wireless PHY layer security, the breakthrough idea is to exploit the characteristics of wireless channels such as fading or noise to transmit a message from a source to an intended destination while keeping the message confidential from passive eavesdroppers [1]. Driven by this and with the aid of multiple-input multiple-output (MIMO) technology, PHY layer security in MIMO wiretap channels that employ multiple co-located antennas at the transmitter, the legitimate receiver, and/or the eavesdropper has attracted considerable attention (e.g., [2–4], and the references therein). Unfortunately, exploiting multiple co-located antennas to secure the wireless transmission would often face the practical constraints of size and power, especially in small mobile and sensor terminals. One way around this is cooperative relaying to achieve spatial diversity using distributed terminals [5–8].

It is important to note that although PHY layer security has been extensively studied in the open literature for both MIMO and cooperative communication networks, all previous works have assumed flat fading channels. In practice, multipath components are frequently present in wireless communication systems due to multiple reflectors, in which reflectors cause a time dispersion and frequency selective fading. If the signal bandwidth is larger than the frequency coherence bandwidth or the delay spread is larger than the symbol duration, the signal is distorted due to intersymbol interference (ISI). To avoid the use of equalizers in dealing with ISI, single carrier (SC) transmission is an alternative attractive solution [9]. There are several existing works and on-going activities in the context of CP-SC transmission in several different domains [10–12].

While the aforementioned literature laid a solid foundation for the study of CP-SC systems, the PHY layer security issues with secrecy constraints in CP-SC transmission remain unknown. In this paper, to harness the aforementioned characteristics of multipath components in practice within the framework of PHY layer security, we focus on secure CP-SC transmission in DF relay networks. In contrast to the rich body of literature on PHY layer security, we consider the multiple relays and multiple destinations coexist with a cluster of eavesdroppers in frequency selective fading environment. A two-stage relay and destination selection is proposed to minimize the eavesdropping and maximize the signal power of the link between the relay and the destination. Analytical results for ergodic secrecy rate are derived in closed-form. The multiplexing gain and the power cost are calculated based on simplified expressions for the ergodic secrecy rate in the high-SNR regime. Furthermore, we reach an interesting conclusion that secrecy performance limits exist when the average received power at the eavesdropper is proportional to the counterpart at the destination.

Notation: The superscript $(\cdot)^H$ denotes complex conjugate transposition; $\boldsymbol{I}_N$ is an $N\times N$ identity matrix; $\mathbf{0}$ denotes an all-zeros matrix of appropriate dimensions; $\mathcal{CN}\left(\mu,\sigma^2\right)$ denotes the complex Gaussian distribution with the mean μ and the variance σ^2; $\mathbb{C}^{m\times n}$ denotes the vector space of all $m\times n$ complex matrices; $F_{\varphi}(\cdot)$ denotes the cumulative distribution function (CDF) of the random variable (RV) φ; $E_a\{\cdot\}$ denotes expectation with respect to a. The probability density function (PDF) of φ is denoted by $f_{\varphi}(\cdot)$; $[x]^+ = \max(x,0)$; $\sum_{l_1,\ldots,l_a}^{i}$ denotes a set of nonnegative integers $\{l_1,\ldots,l_a\}$ satisfying $\sum_{t=1}^{a} l_t = i$.

II. System and Channel Model

In the considered system, the source transmits the signal to the destinations via relay link, which is intercepted by the eavesdroppers. The direct link between source and destinations

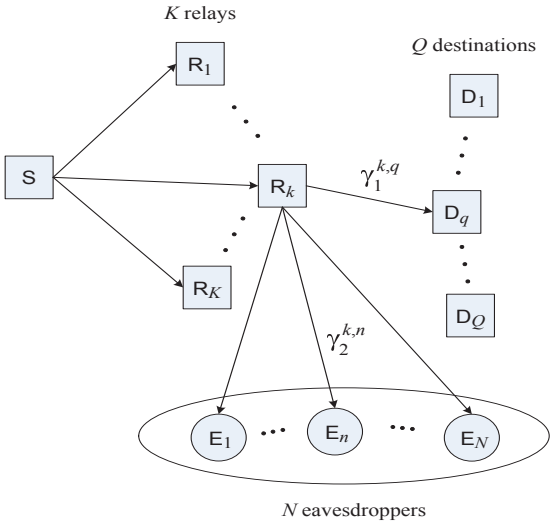

Fig. 1. PHY layer security for cooperative single carrier systems.

is assumed to be non-existent, due to the deep fading. Each node has only one antenna and there are K relays and Q destinations. We assume the following set of instantaneous impulse channel responses.

- A set of channels $\{\boldsymbol{g}^{k,q}, \forall k,q\}$ between a particular kth relay and the qth destination undergo a frequency selective fading. They are assumed to have the same N_1 multipath components, i.e., $\boldsymbol{g}^{k,q} \triangleq [g_1^{k,q}, \ldots, g_{N_1}^{k,q}]^T \in \mathbb{C}^{N_1 \times 1}$, each of which is distributed by the complex white Gaussian distribution with the zero mean and the unit variance. The path losses over these channels are denoted by $\{\alpha_1^{k,q}, \forall k,q\}$.
- A set of channels $\{\boldsymbol{h}^{k,1}, \ldots, \boldsymbol{h}^{k,n}, \ldots, \boldsymbol{h}^{k,N}\}$ between the kth relay and N eavesdroppers undergo a frequency selective fading. They are assumed to have the same N_2 multipath components, i.e., $\boldsymbol{h}^{k,n} \triangleq [h_1^{k,n}, \ldots, h_{N_2}^{k,n}]^T \in \mathbb{C}^{N_2 \times 1}$, each of which is distributed by the complex white Gaussian distribution with the zero mean and the unit variance. The path losses over these channels are denoted by $\{\alpha_2^{k,n}, \forall k,n\}$.
- The maximum channel length in the considered system is assumed to be $N_g = \max(N_1, N_2)$.

For single-carrier cooperative transmission, we assume that

- Binary phase shift keying (BPSK) modulation is applied such that P modulated data symbols transmitted by the source form a transmit symbol block $\boldsymbol{x} \in \mathbb{C}^{P\times 1} \in \{-1,1\}^P$ satisfying $E_{\boldsymbol{x}}\{\boldsymbol{x}\} = \boldsymbol{0}$ and $E_{\boldsymbol{x}}\{\boldsymbol{x}\boldsymbol{x}^H\} = \boldsymbol{I}_P$.
- To prevent inter-block symbol interference (IBSI) [10], the CP comprising of P_g symbols is appended to the front of $\boldsymbol{x}$. It is also assume that $P_g \geq N_g$.
- We employ the selective-DF relaying protocol, which selects one relay and destination among their groups. This selection is accomplished via the proposed two-step selection scheme.
- We assume perfect decoding at each relay, so that error propagation does not exist in the considered system.

The signal received at the nth eavesdropper from the kth relay is given by

$$\boldsymbol{r}^{k,n} = \sqrt{P_s \alpha_2^{k,n}} \boldsymbol{H}^{k,n} \boldsymbol{x} + \boldsymbol{n}_2^{k,n} \tag{1}$$

where P_s is the transmit power and $\boldsymbol{H}^{k,n}$ is the right circulant matrix [10] defined by $\boldsymbol{h}^{k,n}$. Also, we assume that $\boldsymbol{n}_2^{k,n} \sim \mathcal{C}N(\boldsymbol{0}, \sigma_n^2 \boldsymbol{I}_P)$. Since we assume perfect decoding at the all relays and perfect knowledge of CSI, channels between the source and relays are not taken into considered in (1) [7, 13].

Definition 1: Applying the properties of the right circulant channel matrix [10, 14], the instantaneous signal-to-noise ratio (SNR) between the kth relay and the nth eavesdropper is defined as

$$\gamma_2^{k,n} = \frac{P_s \alpha_2^{k,n} \|\boldsymbol{h}^{k,n}\|^2}{\sigma_n^2} = \tilde{\alpha}_2^{k,n} \|\boldsymbol{h}^{k,n}\|^2 \sim \chi^2(2N_2, \tilde{\alpha}_2^{k,n}) \tag{2}$$

where $\tilde{\alpha}_2^{k,n} \triangleq \frac{P_s \alpha_2^{k,n}}{\sigma_n^2}$, and the CDF of $\gamma_2^{k,n}$ is

$$F_{\gamma_2^{k,n}}(x) = 1 - e^{-x/\tilde{\alpha}_2^{k,n}} \sum_{l=0}^{N_2-1} \frac{1}{l!} \Big(\frac{x}{\tilde{\alpha}_2^{k,n}}\Big)^l \mathrm{U}(x), \tag{3}$$

where $\mathrm{U}(x)$ denotes the discrete unit function.

Now the received signal at the qth destination from the kth relay is given by

$$\boldsymbol{z}^{k,q} = \sqrt{P_s \alpha_1^{k,q}} \boldsymbol{G}^{k,q} \boldsymbol{x} + \boldsymbol{n}_1^{k,q} \tag{4}$$

where $\boldsymbol{G}^{k,q}$ is the right circulant matrix defined by $\boldsymbol{g}^{k,q}$. Also, we assume that $\boldsymbol{n}_1^{k,q} \sim \mathcal{C}N(\boldsymbol{0}, \sigma_n^2 \boldsymbol{I}_Q)$. According to Definition 1, the instantaneous SNR of the link between the kth relay and the qth destination is $\gamma_1^{k,q} = \frac{P_s \alpha_1^{k,q} \|\boldsymbol{g}^{k,q}\|^2}{\sigma_n^2} = \tilde{\alpha}_1^{k,q} \|\boldsymbol{g}^{k,q}\|^2 \sim \chi^2(2N_1, \tilde{\alpha}_1^{k,q})$, where $\tilde{\alpha}_1^{k,q} \triangleq \frac{P_s \alpha_1^{k,q}}{\sigma_n^2}$, and the CDF of $\gamma_1^{k,q}$ is

$$F_{\gamma_1^{k,q}}(x) = 1 - e^{-x/\tilde{\alpha}_1^{k,q}} \sum_{l=0}^{N_1-1} \frac{1}{l!} \Big(\frac{x}{\tilde{\alpha}_1^{k,q}}\Big)^l \mathrm{U}(x). \tag{5}$$

In the sequel, we assume that pathloss components $\alpha_2^{k,n}$ and $\alpha_1^{k,q}$ are independent of the indices of the relay, eavesdropper, and destination, so that we have $\alpha_2 = \{\alpha_2^{k,n}, \forall k,n\}$ and $\alpha_1 = \{\alpha_1^{k,q}, \forall k,q\}$. The corresponding normalized quantities are defined as $\tilde{\alpha}_1 \triangleq \frac{P_s \alpha_1}{\sigma_n^2}$ and $\tilde{\alpha}_2 \triangleq \frac{P_s \alpha_2}{\sigma_n^2}$.

III. RELAY AND DESTINATION SELECTION UNDER A GROUP OF EAVESDROPPERS

In this section, we shall first propose the two-stage relay and destination selection procedure, in which a relay is selected to minimize the worst-case eavesdropping in the eavesdropper group. And then, the desired destination is selected from the chosen relay to have the maximum instantaneous SNR between them. That is, the relay and destination are chosen according to the following selection criteria:

$$\begin{aligned} \text{stage1} \quad &: \quad k^* = \min \arg_{k\in[1,K]} (\gamma_2^{k,\max}) \text{ and} \\ \text{stage2} \quad &: \quad q^* = \max \arg_{q\in[1,Q]} (\gamma_1^{k^*,q}) \end{aligned} \tag{6}$$

where $\gamma_2^{k,\max}$ denotes the maximum instantaneous SNR among those of between the kth relay and N eavesdroppers. In addition, $\gamma_1^{k^*,q}$ denotes the maximum instantaneous SNR between the selected relay and the qth destination. When $Q = 1$, the proposed relay and destination selection scheme becomes somewhat similar to that of [7]. However, due to an achievable multiuser diversity, the proposed selection scheme will result in better secrecy outage probabilities, non-zero achievable secrecy rates, and ergodic secrecy rates. For this selection, we use a training symbol which has the same statistical properties as $\boldsymbol{x}$, and assume a quasi-stationary channel during its operation.

Next, the corresponding CDF and PDF for a link from a particular relay to a group of eavesdroppers will be derived. We start the derivation for the CDF of $\gamma_2^{k,\max}$, which is given by

$$F_{\gamma_2^{k,\max}}(x) = \Big[1 - e^{-x/\tilde{\alpha}_2} \sum_{l=0}^{N_2-1} \frac{1}{l!}\Big(\frac{x}{\tilde{\alpha}_2}\Big)^l\Big]^N \mathrm{U}(x) \quad (7)$$

where we assume that channels between a particular relay and N eavesdroppers are independent and identically distributed (i.i.d.).

Since $\{\gamma_2^{1,\max}, \cdots, \gamma_2^{K,\max}\}$ is a set of i.i.d. continuous random variables, the PDF of $\gamma_2^{\min,\max} \triangleq \gamma_2^{k^*,\max} \triangleq \min(\gamma_2^{1,\max}, \cdots, \gamma_2^{K,\max})$ is derived in (8) at the top of the next page. Due to limited space, we do not include a detailed derivation of (8). If we use the order statistics, and binomial and multinomial formulas, we can readily derive (8).

For the i.i.d. frequency selective fading channels between a particular relay and a group of Q destinations, the CDF of $\gamma_1^{k^*,q^*} \triangleq \max(\gamma_1^{k^*,1}, ..., \gamma_1^{k^*,Q})$ is given by

$$F_{\gamma_1^{k^*,q^*}}(x) = \Big[1 - e^{-x/\tilde{\alpha}_1} \sum_{l=0}^{N_1-1} \frac{1}{l!}\big(\frac{x}{\tilde{\alpha}_1}\big)^l\Big]^Q \mathrm{U}(x). \quad (10)$$

IV. Ergodic Secrecy Rate

The instantaneous secrecy rate is expressed as [4, 15]

$$C_s = \frac{1}{2}[\log_2(1+\gamma_1^{k^*,q^*}) - \log_2(1+\gamma_2^{\min,\max})]^+ \quad (11)$$

where $\log_2(1+\gamma_1^{k^*,q^*})$ is the instantaneous capacity of the channel between the chosen relay and the selected destination, whereas $\log_2(1+\gamma_2^{\min,\max})$ is the instantaneous capacity of the wiretap channel between the selected relay and the eavesdropper group. Having obtained PDFs and CDFs of SNRs achieved by the two-stage relay and destination selection scheme, the exact ergodic secrecy rate will be derived. Then, an asymptotic analysis of the ergodic secrecy rate will be developed to see the asymptotic behavior of the system.

The ergodic secrecy rate is defined as the instantaneous secrecy rate C_s averaged over $\gamma_1^{j^*,q^*}$ and $\gamma_2^{\min,\max}$. As such, we formulate the ergodic secrecy rate as

$$\bar{C}_s = \int_0^\infty \int_0^\infty C_s f_{\gamma_1^{k^*,q^*}}(x_1)\, f_{\gamma_2^{\min,\max}}(x_2) dx_1 dx_2. \quad (12)$$

Substituting (11) into (12), and applying some algebraic manipulations, we obtain

$$\bar{C}_s = \frac{1}{2\log(2)} \int_0^\infty \frac{F_{\gamma_2^{\min,\max}}(x_2)}{1+x_2} \Big(1 - F_{\gamma_1^{k^*,q^*}}(x_2)\Big) dx_2. \quad (13)$$

Based on the PDF of $\gamma_2^{\min,\max}$ given in (8), the CDF of $\gamma_2^{\min,\max}$ is given by

$$F_{\gamma_2^{\min,\max}}(x) = A\widetilde{\sum}\Big[\frac{(\tilde{N}_2-1)!}{(\beta_2)^{\tilde{N}_2}} - e^{-\beta_2 x} \sum_{n_1=0}^{\tilde{N}_2-1} \frac{(\tilde{N}_2-1)!}{n_1!} \frac{x^{n_1}}{(\beta_2)^{\tilde{N}_2-n_1}}\Big]. \quad (14)$$

In addition, by employing binomial and multinomial formulas, the CDF of $\gamma_1^{k^*,q^*}$ in (10) can be re-expressed as

$$F_{\gamma_1^{k^*,q^*}}(x) = 1 + \sum_{q=1}^{Q} \binom{Q}{q} (-1)^q e^{-qx/\tilde{\alpha}_1} \sum_{w_1,\ldots,w_{N_1}}^{q} \frac{q!}{w_1! \ldots w_{N_1}!} \frac{x^{\tilde{L}_1}}{\prod_{t=0}^{N_1-1} \Big(t!(\tilde{\alpha}_1)^t\Big)^{w_{t+1}}}, \quad (15)$$

where $\tilde{L}_1 \triangleq \sum_{t=0}^{N_1-1} t w_{t+1}$. Substituting (14) and (15) into (13), and using the confluent hypergeometric function [16, eq. (9.211.4)], we obtain the ergodic secrecy rate expressed in (16) at the top of the next page.

In order to gather further insight, we present the asymptotic ergodic secrecy rate. We first consider the case of $\tilde{\alpha}_1 \to \infty$ and a fixed $\tilde{\alpha}_2$, and provide the following corollary.

Corollary 1: The asymptotic ergodic secrecy rate at $\tilde{\alpha}_1 \to \infty$ and a fixed $\tilde{\alpha}_2$ is given by (17) at the next page. In (17), $\psi(\cdot)$ is the digamma function [17].

Proof: A proof of this corollary is given in Appendix A. In this Appendix, we have defined $A_1 \triangleq \sum_{t=0}^{N_2-1} t v_{t+1} + 1$ and $A_2 \triangleq m/\tilde{\alpha}_2$. ■

With the help of (17), we confirm that the multiplexing gain [18] is 1/2 in bits/sec/Hz/(3 dB), which is given by

$$S^\infty = \lim_{\tilde{\alpha}_1 \to \infty} \frac{\bar{C}_1^\infty}{\log_2(\tilde{\alpha}_1)} = \frac{1}{2}. \quad (18)$$

It is indicated from (18) that under there circumstances, secure communication achieves the same spectral efficiency as communication without eavesdropping. Moreover, using (17), we can easily calculate the additional power cost for different network parameters while maintaining a specified target ergodic secrecy rate. For example, we consider different numbers of relays K_1 and K_2 with $K_1 > K_2$. Compared to the K_1 case, the additional power cost in achieving the specified target ergodic secrecy rate in the K_2 scenario is calculated as

$$\Delta P \ (\mathrm{dB}) = \frac{10}{\log 10} [\eta(K_1) - \eta(K_2)] \quad (19)$$

$$f_{\gamma_2^{\min,\max}}(x) = \frac{KN}{(\tilde{\alpha}_2)^{N_2}(N_2-1)!}\sum_{k=0}^{K-1}\sum_{m=0}^{Nk}\sum_{j=0}^{N-1}\binom{K-1}{k}\binom{Nk}{m}\binom{N-1}{j}(-1)^{k+m+j}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\sum_{u_1,\ldots,u_{N_2}}^{j}\frac{m!}{v_1!\ldots v_{N_2}!}\frac{j!}{u_1!\ldots u_{N_2}!}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{u_{t+1}}}$$
$$e^{-\frac{x(m+j+1)}{\tilde{\alpha}_2}}x^{N_2+(\sum_{t=0}^{N_2-1}tv_{t+1})+(\sum_{t=0}^{N_2-1}tu_{t+1})-1}$$
$$= A\widetilde{\sum}e^{-\beta_2 x}x^{\tilde{N}_2-1}\mathrm{U}(x) \tag{8}$$

where $A\triangleq\frac{KN}{(\tilde{\alpha}_2)^{N_2}(N_2-1)!}$, $\beta_2\triangleq\frac{(m+j+1)}{\tilde{\alpha}_2}$, $\tilde{N}_2\triangleq N_2+(\sum_{t=0}^{N_2-1}tv_{t+1})+(\sum_{t=0}^{N_2-1}tu_{t+1})$, and

$$\widetilde{\sum}\triangleq\sum_{k=0}^{K-1}\sum_{m=0}^{Nk}\sum_{j=0}^{N-1}\binom{K-1}{k}\binom{Nk}{m}\binom{N-1}{j}(-1)^{k+m+j}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\sum_{u_1,\ldots,u_{N_2}}^{j}\frac{m!}{v_1!\ldots v_{N_2}!}\frac{j!}{u_1!\ldots u_{N_2}!}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{u_{t+1}}}. \tag{9}$$

$$\bar{C}_s = -\frac{A}{2\log(2)}\widetilde{\sum}\sum_{q=1}^{Q}\binom{Q}{q}(-1)^q\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}\left(t!(\tilde{\alpha}_1)^t\right)^{w_{t+1}}}$$
$$\Big(\frac{\Gamma(\tilde{N}_2)\Gamma(\tilde{L}_1+1)}{(\beta_2)^{\tilde{N}_2}}\Psi(\tilde{L}_1+1,\tilde{L}_1+1;q/\tilde{\alpha}_1)-\sum_{n_1=0}^{\tilde{N}_2-1}\frac{\Gamma(\tilde{N}_2)\Gamma(\tilde{L}_1+n_1+1)}{n_1!(\beta_2)^{\tilde{N}_2-n_1}}$$
$$\Psi(\tilde{L}_1+n_1+1,\tilde{L}_1+n_1+1;\beta_2+q/\tilde{\alpha}_1)\Big). \tag{16}$$

$$\bar{C}_1^{\infty} = \frac{1}{2}\log_2(\tilde{\alpha}_1)+\frac{1}{2\log(2)}\Big[\frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q\sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}}$$
$$\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}[\psi(N_1+\tilde{L}_1)-\log(q+1)]+\sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}(\frac{m!}{v_1!\ldots v_{N_2}!})\frac{\Gamma(\sum_{t=0}^{N_2-1}tv_{t+1}+1)}{\prod_{t=0}^{N_2-1}\left(t!(\tilde{\alpha}_2)^t\right)^{v_{t+1}}}\Psi(A_1,A_1;A_2)\Big]. \tag{17}$$

---

where

$$\eta(K) = \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}(\frac{m!}{v_1!\ldots v_{N_2}!})\frac{\Gamma(\sum_{t=0}^{N_2-1}tv_{t+1}+1)}{\prod_{t=0}^{N_2-1}\left(t!(\tilde{\alpha}_2)^t\right)^{v_{t+1}}}\Psi(A_1,A_1;A_2).$$

Similarly, the additional power cost in achieving the specified target ergodic secrecy rate under different numbers of destinations or eavesdroppers can be accordingly obtained.

We next consider the case of $\tilde{\alpha}_1\to\infty$ and $\tilde{\alpha}_2\to\infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2}=\kappa$. Using the similar way as the proof of Corollary 1, we provide the following corollary.

Corollary 2: The asymptotic ergodic secrecy rate at $\tilde{\alpha}_1\to\infty$ and $\tilde{\alpha}_2\to\infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2}=\kappa$ is given by (20) at the top of the next page, where $\hat{\beta}\triangleq m+j+1$, $\widehat{\sum}\triangleq\widetilde{\sum}(\tilde{\alpha}_2)^{\tilde{N}_2-N_2}$. It is indicated from (20) that a capacity ceiling exists in this case.

V. Simulation Results

For the simulations, we use BPSK modulation. The transmission block size is formed by 64 BPSK symbols. The CP length is given by 16 BPSK symbols. Every channel vectors are generated by $\boldsymbol{h}^{k,n}\sim\mathcal{CN}(\mathbf{0},\boldsymbol{I}_{N_2}),\forall k,n$ and $\boldsymbol{g}^{k,q}\sim\mathcal{CN}(\mathbf{0},\boldsymbol{I}_{N_1}),\forall k,q$. The curves obtained via actual link

$$\bar{C}_2^{\infty} = \frac{1}{2}\log_2(\kappa) + \frac{1}{2\log(2)}\Big[\frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q \sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}}$$
$$\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}[\psi(N_1+\tilde{L}_1)-\log(q+1)] - \frac{KN}{(N_2-1)!}\widehat{\sum}\frac{\Gamma(\tilde{N}_2)}{(\hat{\beta})^{\tilde{N}_2}}[\psi(\tilde{N}_2)-\log(\hat{\beta})]\Big]. \quad (20)$$

simulations are denoted by **Ex**, whereas analytically derived curves are denoted by **An**. Asymptotically obtained curves are denoted by **As** in the following figures.

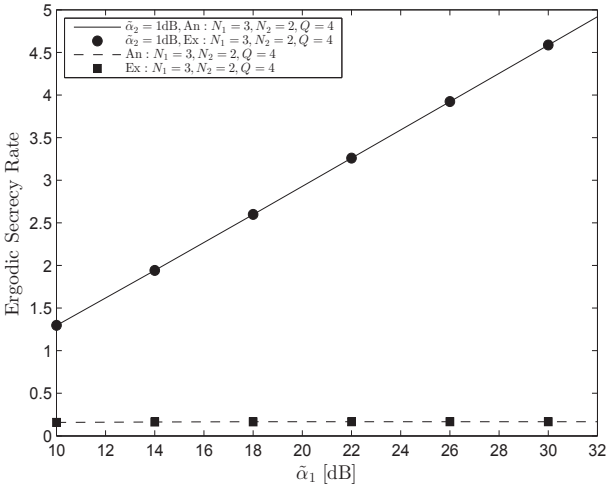

Fig. 2. Ergodic secrecy rate for various values of (N_1, N_2, Q).

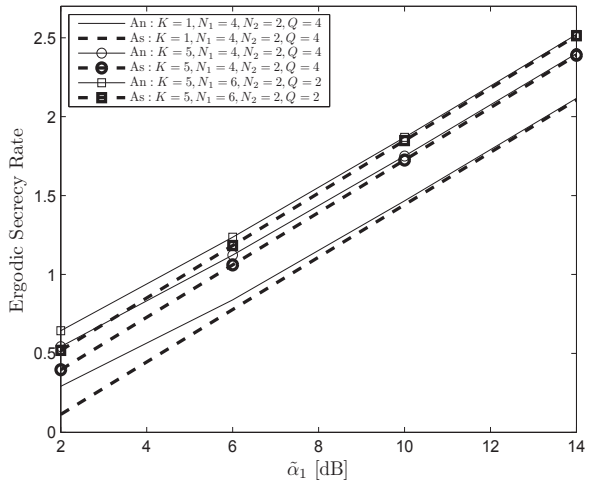

Fig. 3. Ergodic secrecy rate for various values of N_1 and Q at fixed values of $N = 3$ and $\tilde{\alpha}_2 = 1$ dB.

In Fig. 2, we first compare the derived ergodic secrecy rate with the exactly obtained ergodic secrecy rate for the case of

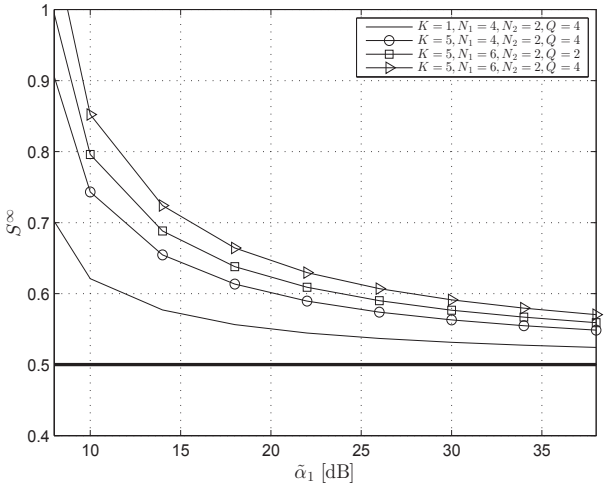

Fig. 4. Multiplexing gain S^{∞}.

$(N_1 = 3, N_2 = 2, Q = 4)$. We assume a fixed number of eavesdroppers $(N = 3)$ and a single relay $(K = 1)$. Perfect matchings between them can be observed. From this figure, we can see that in contrast to the fixed $\tilde{\alpha}_2$ case, capacity ceiling is intrinsic when $\tilde{\alpha}_2$ and $\tilde{\alpha}_1$ are proportional, as verified in Corollary 2. In Fig. 3, we show the asymptotic ergodic secrecy rate for various values of (K, N_1, N_2, Q) at a fixed number of eavesdroppers $N = 3$ and $\tilde{\alpha}_2 = 1$ dB. This plot shows the corresponding asymptotic ergodic secrecy rate obtained from Corollary 1. As $\tilde{\alpha}_1$ increases, the differences between the exact ergodic secrecy rates and the asymptotic ergodic secrecy rates are negligible. We can also easily see that the multipath diversity and the multiuser diversity are two key factors in determining the ergodic secrecy rates. According to (19), a total of five relays can reduce 0.8 dB power than a single relay in achieving 2.0 secrecy rate. Fig. 4 shows the multiplexing gain S^{∞} as a function of (K, N_1, Q), which are the key system and channel parameters in determining the diversity gain. As $\tilde{\alpha}_1$ increases, the multiplexing gain S^{∞} approaches 1/2. Since a larger diversity has a more influence from the second term in the right hand side of (17), the convergence speed to 1/2 becomes slower as the diversity gain increases.

VI. Conclusions

In this paper, we have proposed cooperative single carrier systems with multiple relays and destinations. A coexisting group of eavesdroppers have been assumed to eavesdrop the

relays. For this challenging environment, we have proposed a two-stage relay and destination selection scheme. We have analyzed the secrecy performance in terms of the ergodic secrecy rate. Having derived the asymptotic ergodic secrecy rate, the multiplexing gain has been shown to be equal to the number of hops.

APPENDIX A: A DETAILED DERIVATION OF COROLLARY 1

We first rewrite the CDF of $\gamma_2^{\min,\max}$ as

$$F_{\gamma_2^{\min,\max}}(x) = 1 + \tilde{F}_{\gamma_2^{\min,\max}}(x), \tag{A.1}$$

where

$$\tilde{F}_{\gamma_2^{\min,\max}}(x) = \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}e^{-mx/\tilde{\alpha}_2} \sum_{v_1,\ldots,v_{N_2}}^{m}\Big(\frac{m!}{v_1!\ldots v_{N_2}!}\Big)\frac{x^{\sum_{t=0}^{N_2-1}tv_{t+1}}}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}.$$

Then, the ergodic secrecy rate is derived as (A.2)

$$\bar{C}_s = \frac{1}{2\log(2)}\Big[\underbrace{\int_0^\infty \log(1+x_1)f_{\gamma_1^{k^*,q^*}}(x_1)dx_1}_{\Theta_1} + \underbrace{\int_0^\infty\int_0^{x_1}\frac{\tilde{F}_{\gamma_2^{\min,\max}}(x_2)}{1+x_2}f_{\gamma_1^{k^*,q^*}}(x_1)dx_2dx_1}_{\Theta_2}\Big]. \tag{A.2}$$

As $\tilde{\alpha}_1 \to \infty$, Θ_1 asymptotically becomes

$$\Theta_1^\infty = \log(\tilde{\alpha}_1) + \int_0^\infty \log\left(\frac{x_1}{\tilde{\alpha}_1}\right)f_{\gamma_1^{k^*,q^*}}(x_1)\,dx_1. \tag{A.3}$$

The PDF of $\gamma_1^{k^*,q^*}$ can be obtained by taking the derivative of (10). Substituting the PDF of $\gamma_1^{k^*,q^*}$ into (A.3), and employing [16, eq. 4.352.1], we compute (A.3) as

$$\Theta_1^\infty = \log(\tilde{\alpha}_1) + \frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q \sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}} \frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}\big[\psi(N_1+\tilde{L}_1)-\log(q+1)\big]. \tag{A.4}$$

Changing the order of integration in Θ_2, we have

$$\Theta_2 = \int_0^\infty \frac{\tilde{F}_{\gamma_2^{\min,\max}}(x_2)}{1+x_2}(1-F_{\gamma_1^{k^*,q^*}}(x_2))dx_2. \tag{A.5}$$

Applying the Taylor series expansion truncated to the N_1th order given by $e^x = \sum_{l=0}^{N_1}\frac{x^l}{l!} + O(x^{N_1})$, we derive the first order expansion of $F_{\gamma_1^{k^*,q^*}}(x)$, which is specified in (10), at high $\tilde{\alpha}_1$ as

$$F_{\gamma_1^{k^*,q^*}}(x) = \frac{1}{(N_1!)^Q}\left(\frac{x}{\tilde{\alpha}_1}\right)^{QN_1} + O((\tilde{\alpha}_1)^{-QN_1}). \tag{A.6}$$

From (A.6), we see that as $\tilde{\alpha}_1 \to \infty$, $F_{\gamma_1^{k^*,q^*}}(x_2) \approx 0$. Hence, the asymptotic expression for Θ_2 is given by

$$\Theta_2^\infty = \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}\sum_{v_1,\ldots,v_{N_2}}^{m}(\frac{m!}{v_1!\ldots v_{N_2}!}) \frac{\Gamma(\sum_{t=0}^{N_2-1}tv_{t+1}+1)}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\Psi(A_1,A_1;A_2). \tag{A.7}$$

Substituting (A.7) and (A.4) into (A.2), we derive the asymptotic expression for the ergodic secrecy capacity as (17).

REFERENCES

[1] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[2] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with *M*-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

[3] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–357, 2012.

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

[5] 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.

[6] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, Jun. 2011.

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

[8] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[9] S. Kato, H. Harada, R. Funada, T. Baykas, C. S. Sum, J. Wang, and M. A. Rahman, "Single carrier transmission for multi-gigabit 60-GHz WPAN systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 8, pp. 1466–1478, Oct. 2009.

[10] K. J. Kim, T. A. Tsiftsis, and H. V. Poor, "Power allocation in cyclic prefixed single-carrier relaying systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2297–2305, Jul. 2011.

[11] T.-H. Pham, Y.-C. Liang, A. Nallanathan, and H. Garg, "Optimal training sequences for channel estimation in bi-directional relay networks with multiple antennas," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 474–479, Feb. 2010.

[12] K. J. Kim, T. Q. Duong, M. Elkashlan, P. L. Yeoh, H. V. Poor, and M. H. Lee, "Spectrum sharing single-carrier in the presence of multiple licensed receivers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5223–5235, Oct. 2013.

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

[14] P. R. Davis, *Circulant Matrices*. New York: John Wiley, 1979.

[15] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

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

[17] M. Abramovitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. New York: Dover, 1972.

[18] A. Lozano, A. M. Tulino, and S. Verdú, "High-SNR power offset in multiantenna communication," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, IL, Jun. 2004, p. 287.