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

Security Enhancement of Cooperative Single Carrier Systems

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

TR2014-129 September 2014

Abstract

In this paper, the impact of multiple active 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. To accurately assess the secrecy performance, exact and asymptotic expressions are obtained in closed form for several security metrics, including the secrecy outage probability, probability of nonzero secrecy rate, and ergodic secrecy rate in frequency selective fading. Based on the asymptotic analysis, key design parameters, such as secrecy diversity gain, secrecy array gain, secrecy multiplexing gain, and power cost, are characterized, from which new insights are drawn. In addition, it is concluded that secrecy performance limits occur when the average received power at the eavesdropper is proportional to the counterpart at the destination. In particular, for the secrecy outage probability, it is confirmed that the secrecy diversity gain collapses to zero with outage floor, whereas for the ergodic secrecy rate, it is confirmed that its slope collapses to zero with capacity ceiling.

IEEE Transactions on Information Forensics and Security

Security Enhancement of Cooperative Single Carrier Systems

Lifeng Wang, *Student Member, IEEE,* Kyeong Jin Kim, *Senior Member, IEEE,* Trung Q. Duong, *Senior Member, IEEE,* Maged Elkashlan, *Member, IEEE,* and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—In this paper, the impact of multiple active 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 several security metrics including the secrecy outage probability, the probability of non-zero secrecy rate, and the ergodic secrecy rate in frequency selective fading. Based on the asymptotic analysis, key design parameters such as secrecy diversity gain, secrecy array gain, secrecy multiplexing gain, and power cost are characterized, from which new insights are drawn. Moreover, it is concluded that secrecy performance limits occur when the average received power at the eavesdropper is proportional to the counterpart at the destination. Specifically, for the secrecy outage probability, it is confirmed that the secrecy diversity gain collapses to zero with outage floor, whereas for the ergodic secrecy rate, it is confirmed confirm that its slope collapses to zero with capacity ceiling.**

***Index Terms*—Cooperative transmission, frequency selective fading, physical layer security, secrecy ergodic rate, secrecy outage probability, single carrier transmission.**

I. Introduction

DUE to the broadcast nature of radio channels, wireless transmissions are vulnerable to eavesdropping that may potentially intercept or interrupt communication between legitimate terminals. As such, security and privacy are of utmost concern for wireless technologies. Security is conventionally treated as a high-layer problem to be solved using cryptographic methods. However, in some network architectures, such cryptographic security is practically infeasible due to high complexity in data encryption and decryption and the distributed nature of the infrastructure. Alternatively, in wireless physical (PHY) layer security, the characteristics of wireless channels such as fading or noise are exploited to transmit a message from a source to an intended destination while keeping the message confidential from passive eavesdroppers [1].

In recent years, the concept of PHY layer security has attracted considerable interest amongst wireless network designers. One approach to PHY security is to degrade the signal-to-noise ratio (SNR) of the eavesdropper relative to the legitimate receiver. This will guarantee perfect secrecy in wiretap channels. This approach can be aided by multiple-input multiple-output (MIMO) technology, and consequently PHY layer security in MIMO wiretap channels that employ multiple colocated antennas at the transmitter, the legitimate receiver, and/or the eavesdropper has attracted considerable attention (e.g., [2]–[7], and the references therein). For example, maximal ratio combining (MRC) for security enhancement was proposed in [2] and the corresponding secrecy outage probability was derived. A general observation in that work was that increasing the diversity gain of the main channel can effectively reduce the secrecy outage probability. The single-input single-output multi-eavesdropper (SISOME) system was considered in [3], in which a single antenna transmitter communicates with a single antenna legitimate receiver in the presence of multiple eavesdroppers equipped with multiple antennas. In [4], transmit antenna selection (TAS) was proposed to provide secure communication. The proposed scheme consisted of a multiple antenna transmitter with a single radio frequency (RF) chain, a single antenna legitimate receiver, and a multiple antenna eavesdropper. In [5], cooperative jamming was introduced to confuse the eavesdropper in a multiple-input single-output (MISO) wiretap channel. By taking into account multiple antennas at the transmitter, the legitimate receiver, and the eavesdropper, the secrecy performance of several diversity combining schemes over independent and correlated fading channels was investigated in [6] and [7], respectively.

Unfortunately, exploiting multiple colocated antennas to secure wireless transmissions against eavesdropping and security attacks will often face the practical constraints of size and

Manuscript received March 4, 2014; revised June 22, 2014; accepted September 14, 2014. The editor coordinating the review of this paper and approving it for publication was Prof. T. Charles Clancy.

This paper will be presented in part at the Global Communications Conferences (Globecom), Austin, TX, December 2014.

L. Wang and M. Elkashlan are with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK (email:{lifeng.wang, maged.elkashlan}@qmul.ac.uk).

K. J. Kim is with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA (e-mail: Kyeong.j.kim@hotmail.com).

T. Q. Duong is with Queen's University Belfast, Belfast, UK (e-mail: trung.q.duong@qub.ac.uk).

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

This research was supported in part by the U. S. National Science Foundation under Grants CMMI-1435778 and ECCS-1343210 and the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant 102.04-2013.13.

power, especially in small mobile and sensor terminals. One way around this is cooperative relaying to achieve spatial diversity using distributed terminals. Several dual-hop cooperative security schemes have been proposed and the impact of terminal cooperation on the secrecy rate was considered [8]–[16]. In particular, the performance of secure relay networks with different relaying protocols such as decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming was reported in [8], taking into account relay weights and power allocation. In [9] and [10], several secure selection schemes for opportunistic relaying were proposed. Relay selection and cooperative jamming was proposed in [11] and [12] for one-way relaying, and in [13] and [14] for two-way relaying. A new secrecy transmission protocol was proposed in [15], where the concept of interference alignment was combined with cooperative jamming to ensure that the artificial noise from the transmitters can be aligned at the destination, but not at the eavesdropper. The impact of cooperative jamming on MIMO wiretap channels was studied in [16].

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 which uses an increased symbol duration by forming a transmission block symbol [17], [18], with additional cyclic prefix (CP) symbols in front of the transmission block symbol. Thus, compared to orthogonal frequency-division multiplexing (OFDM) transmission, a block-wise processing is necessary for CP-SC transmission. There are several existing works and on-going activities in the context of CP-SC transmission in several different domains, including non-cooperative systems, cooperative relaying systems, and spectrum sharing systems, as follows.

- *Non-cooperative systems:* Opportunistic scheduling was proposed in [19] to achieve multiuser diversity. In [20] and [21], cyclic delay diversity (CDD) was employed for the frequency-domain equalizer (FDE), whereas distributed space-frequency block coding was employed with CP-SC systems [22] to achieve transmit diversity gain. Several channel estimators for CP-SC systems were investigated in [23]–[25].
- *Cooperative relaying systems:* For several relaying protocols such as DF and AF, as well as project and forward relaying [26], optimal power allocation [27], new receiver design [28], optimal training sequences for channel estimation [29], and best terminal selection [30] were proposed to enhance the performance.
- *Spectrum sharing systems:* For cooperative spectrum sharing [31], [32], and non-cooperative spectrum sharing [33], CP-SC transmission was proposed considering the impact of multipath diversity on the system performance, taking into account several performance indicators such as outage probability, symbol error rate, and ergodic capacity.

While the above noted 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, our main contributions are summarized as follows.

- Frequency selective fading is considered with constraints of PHY layer security, in which multiple relays and multiple destinations coexist with a cluster of eavesdroppers. 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 the secrecy outage probability, the probability of non-zero achievable secrecy rate, and the ergodic secrecy rate are derived in closed-form. The secrecy diversity gain and the secrecy array gain are calculated based on simplified expressions for the secrecy outage probability in the high SNR regime. Likewise, the multiplexing gain and the power cost are calculated based on simplified expressions for the ergodic secrecy rate in the high SNR regime.
- It is confirmed that the secrecy diversity gain is directly determined by the multipath diversity and the multiuser diversity between the relays and the destinations. The multiplexing gain is independent of the system and channel parameters including the number of multipaths, relays, eavesdroppers, and destinations. Our high SNR analysis shows that when the average received power at the eavesdropper is proportional to the counterpart at the destination, both the secrecy diversity gain and the secrecy capacity slope collapse to zero, thereby creating a secrecy outage floor and a secrecy capacity ceiling.

The rest of the paper is organized as follows. In Section II, we first detail the system and channel model of the proposed single carrier systems. In Section III, two-stage relay and destination selection is proposed under a group of eavesdroppers. Performance analysis of the considered physical system is presented in Section IV. Simulation results are presented in Section V and conclusions are drawn in Section VI.

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; and $E_a\{\cdot\}$ denotes expectation with respect to a. The probability density function (PDF) of φ is denoted by $f_{\varphi}(\cdot)$; $[x]^+ = \max(x, 0)$

and $\sum_{l_1,\ldots,l_a}^{i}$ denotes a set of nonnegative integers $\{l_1,\ldots,l_a\}$ satisfying $\sum_{t=1}^{a} l_t = i$.

II. System and Channel Model

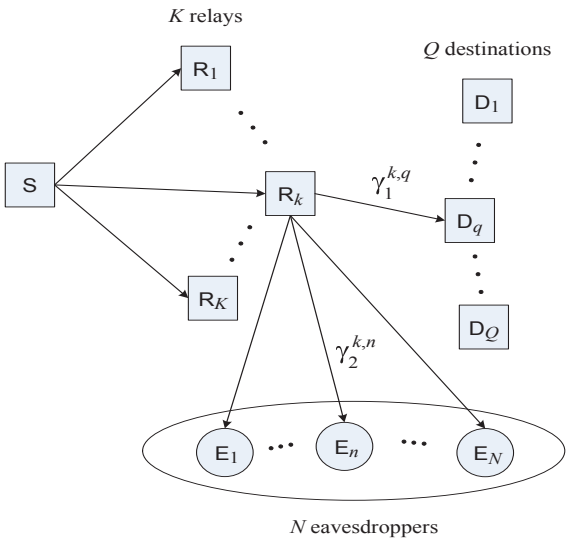

Fig. 1. PHY layer security for cooperative single carrier systems.

In the considered system, which is shown in Fig. 1, 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 the 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 $N_g = \max(N_1, N_2, N_3)$, where N_3 denotes the multipath channel length between the source and relays.

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) [17], [27], [29], 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 [1].

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 [27], [34] defined by $\boldsymbol{h}^{k,n}$. Also, we assume that $\boldsymbol{n}_2^{k,n} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_P)$. Since we assume perfect decoding at all the relays and perfect knowledge of CSI[2], channels between the source and the relays are not taken into account in (1) [10], [11].

Definition 1: Applying the properties of the right circulant channel matrix [27], [34], the instantaneous 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 and PDF of $\gamma_2^{k,n}$ are, respectively, given by

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

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

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 $\boldsymbol{n}_1^{k,q} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_Q)$. According to Definition 1, the instantaneous SNR of the link between the kth relay and the qth destination is given by $\gamma_1^{k,q} = \frac{P_s\alpha_1^{k,q}\|\boldsymbol{g}^{k,q}\|^2}{\sigma_n^2} = \tilde{\alpha}_1^{k,q}\|\boldsymbol{g}^{k,q}\|^2 \sim \chi^2(2N_1, \tilde{\alpha}_1^{k,q})$, so that the CDF of $\gamma_1^{k,q}$ is given by

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

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 $\alpha_1 = \{\alpha_1^{k,q}, \forall k,q\}$.

[1]Practically, the source and the relays are located in the same cluster yielding high received SNRs at the DF relays to successfully decode the messages.

[2]This assumption is commonly seen in the prior literature [8], [10]. The CSI of the eavesdropper channels can be obtained in the scenario where eavesdroppers are active.

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, to decrease the amount of information that eavesdroppers wiretap. 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 [10]. (Note that the relay selection based on maximal secrecy rate was analyzed in the prior literature such as [10], which brings large system overhead compared with our proposed scheme.) 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 that 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

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

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 $\gamma_2^{\min,\max} \triangleq \gamma_2^{k^*,\max} \triangleq \min(\gamma_2^{1,\max}, \cdots, \gamma_2^{K,\max})$ can be derived in the following lemma.

Lemma 1: For the i.i.d. frequency selective fading channels between a particular relay and a group of eavesdroppers, the PDF of $\gamma_2^{\min,\max}$ is given by (8) at the top of the next page.

Proof: A proof of this lemma is provided in Appendix A. ∎

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

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

IV. PERFORMANCE ANALYSIS OF THE PHYSICAL SECRECY SYSTEM

The instantaneous secrecy rate is expressed as [6], [35]

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

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 secrecy outage probability, the probability of non-zero achievable secrecy rate, and the ergodic secrecy rate will be derived. Then, an asymptotic analysis of the secrecy outage probability will be developed to see the asymptotic behavior of the system.

A. Secrecy Outage Probability

According to [7], the secrecy outage probability for a given secure rate, R, is given by

$$\begin{aligned} P_{\text{out}} &= Pr(C_s < R) \\ &= \int_0^\infty F_{\gamma_1^{k^*,q^*}}(2^{2R}(1+\gamma)-1) f_{\gamma_2^{\min,\max}}(\gamma) d\gamma. \end{aligned} \tag{12}$$

A closed-form expression of (12) is provided by the following theorem.

Theorem 1: The secrecy outage probability of the single carrier system employing the proposed relay selection scheme in frequency selective fading is given by

$$\begin{aligned} P_{\text{out}} = C\widetilde{\sum}\sum_{q=0}^{Q} \binom{Q}{q} (-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}} \\ \sum_{w_1,\ldots,w_{N_1}}^{q} \frac{q!}{w_1!\ldots w_{N_1}!} \frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} \\ \sum_{p=0}^{\tilde{L}_1} \binom{\tilde{L}_1}{p} (J_R-1)^{\tilde{L}_1-p} (J_R)^p \Big(\frac{qJ_R}{\tilde{\alpha}_1} + \beta_2\Big)^{-(p+\tilde{N}_2)} \\ (p+\tilde{N}_2-1)! \end{aligned} \tag{13}$$

where $J_R \triangleq 2^{2R}$ and $\tilde{L}_1 \triangleq \sum_{t=0}^{N_1-1} t w_{t+1}$.

Proof: A detailed derivation is provided in Appendix B. ∎

To explicitly see the secrecy diversity gain, we provide an asymptotic expression for (13) in the following theorem.

Theorem 2: The asymptotic secrecy outage probability at a fixed $\tilde{\alpha}_2$ is given by

$$P_{\text{out}}^{\infty} \triangleq \lim_{\tilde{\alpha}_1\to\infty} P_{\text{out}} = (G_a\tilde{\alpha}_1)^{-QN_1} + O\big((\tilde{\alpha}_1)^{-QN_1}\big) \tag{14}$$

where the secrecy array gain is given by

$$\begin{aligned} G_a = \Big[\frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}\sum_{l=0}^{QN_1} \binom{QN_1}{l} (J_R-1)^{QN_1-l} \\ (J_R)^l (\tilde{\alpha}_2)^l \frac{(l+\tilde{N}_2-1)!}{(\hat{\beta})^{l+\tilde{N}_2}}\Big]^{-\frac{1}{QN_1}} \end{aligned} \tag{15}$$

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

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

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

with $\hat{C}\triangleq\frac{KN}{(N_2-1)!}$, $\hat{\beta}\triangleq m+j+1$, and $\widehat{\sum}$, which is given by

$$\widehat{\sum}\triangleq\sum_{k=0}^{K-1}\sum_{m=0}^{Nk}\sum_{j=0}^{N-1}\binom{K-1}{k}\binom{Nk}{m}\binom{N-1}{j}(-1)^{k+m+j}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\sum_{u_1,\ldots,u_{N_2}}^{j}\frac{m!}{v_1!\ldots v_{N_2}!}\frac{j!}{u_1!\ldots u_{N_2}!}$$
$$\frac{1}{\prod_{t=0}^{N_2-1}(t!)^{v_{t+1}}}\frac{1}{\prod_{t=0}^{N_2-1}(t!)^{u_{t+1}}}. \tag{16}$$

Proof: A detailed proof of this theorem is provided in Appendix C. ∎

This theorem shows that the secrecy diversity gain is QN_1, which is the product of the multipath diversity gain and the multiuser diversity gain achievable between the selected relay and the Q destinations.

Corollary 1: When $\tilde{\alpha}_1\to\infty, \tilde{\alpha}_2\to\infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2}=\kappa$, then the asymptotic secrecy outage probability is given by

$$P_{\text{out}}^{\infty} = \frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}(\kappa)^{QN_1}(J_R)^{QN_1}\frac{(QN_1+\tilde{N}_2-1)!}{(\hat{\beta})^{QN_1+\tilde{N}_2}} \tag{17}$$

which shows that the secrecy diversity gain is not achievable for this particular case.

B. The probability of non-zero achievable secrecy rate

In the following, we shall derive the probability of non-zero achievable secrecy rate.

Corollary 2: The probability of non-zero achievable secrecy rate is provided by (18) at the top of the next page. In (18), we have defined $\tilde{N}_1\triangleq N_1+(\sum_{t=0}^{N_1-1}tw_{t+1})+(\sum_{t=0}^{N_2-1}tv_{t+1})$.

Proof: A proof of this corollary is provided in Appendix D. ∎

To investigate the effect of the diversity gain on the convergence behavior of the probability of non-zero achievable secrecy rate to $Pr(C_s>0)=1$, we derive an asymptotic probability of non-zero achievable secrecy rate. According to (D.3), the probability of non-zero achievable secrecy rate can be rewritten as

$$Pr(C_s>0) = 1-\int_0^{\infty}F_{\gamma_1^{k^*,q^*}}(x)f_{\gamma_2^{\min,\max}}(x)dx. \tag{19}$$

Substituting (C.1) and (8) into (19), we get the following asymptotic probability of non-zero achievable secrecy rate

$$Pr(C_s^{\infty}>0) = 1-\frac{C}{(N_1!)^Q}\left(\frac{1}{\tilde{\alpha}_1}\right)^{N_1Q}\widetilde{\sum}\frac{(N_1Q+\tilde{N}_2-1)!}{(\beta_2)^{N_1Q+\tilde{N}_2}} \tag{20}$$

which shows that the multipath diversity gain and the multiuser diversity gain simultaneously affect the convergence speed of the non-zero achievable secrecy rate to $Pr(C_s>0)=1$. In the following, we shall derive the ergodic secrecy rate for the proposed system.

C. Ergodic Secrecy Rate

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

$$\bar{C}_s = \int_0^{\infty}\int_0^{\infty}C_s f_{\gamma_1^{k^*,q^*}}(x_1)\, f_{\gamma_2^{\min,\max}}(x_2)dx_1dx_2. \tag{21}$$

Substituting (11) into (21), and applying some algebraic manipulations, we obtain [36]

$$\bar{C}_s = \frac{1}{2\log(2)}\int_0^{\infty}\frac{F_{\gamma_2^{\min,\max}}(x_2)}{1+x_2}\left(1-F_{\gamma_1^{k^*,q^*}}(x_2)\right)dx_2. \tag{22}$$

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

$$F_{\gamma_2^{\min,\max}}(x) = \int_0^x f_{\gamma_2^{\min,\max}}(t)\,dt$$
$$= C\widetilde{\sum}\Big[\frac{(\tilde{N}_2-1)!}{(\beta_2)^{\tilde{N}_2}} - e^{-\beta_2 x}\sum_{n_1=0}^{\tilde{N}_2-1}\frac{(\tilde{N}_2-1)!}{n_1!}\frac{x^{n_1}}{(\beta_2)^{\tilde{N}_2-n_1}}\Big]. \tag{23}$$

$$Pr(C_s>0)=1-\frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!}\sum_{k=0}^{K}\sum_{m=0}^{Nk}\sum_{q=0}^{Q-1}\binom{Q-1}{q}\binom{K}{k}\binom{Nk}{m}(-1)^{q+k+m}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}\Big(\frac{m!}{v_1!\ldots v_{N_2}!}\Big)\sum_{w_1,\ldots,w_{N_1}}^{q}\Big(\frac{q!}{w_1!\ldots w_{N_1}!}\Big)\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}$$
$$\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}\Big(\frac{m}{\tilde{\alpha}_2}+\frac{q+1}{\tilde{\alpha}_1}\Big)^{-\tilde{N}_1}(\tilde{N}_1-1)!. \tag{18}$$

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

$$F_{\gamma_1^{k^*,q^*}}(x)=1+\sum_{q=1}^{Q}\binom{Q}{q}(-1)^q e^{-qx/\tilde{\alpha}_1}$$
$$\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{x^{\tilde{L}_1}}{\prod_{t=0}^{N_1-1}\Big(t!(\tilde{\alpha}_1)^t\Big)^{w_{t+1}}}. \tag{24}$$

Substituting (23) and (24) into (22), and using the confluent hypergeometric function [37, eq. (9.211.4)] given by $\Psi(\alpha,\gamma;z)=\frac{1}{\Gamma(\alpha)}\int_0^\infty e^{-zt}t^{\alpha-1}(1+t)^{\gamma-\alpha-1}dt$, we obtain the ergodic secrecy rate expressed in (25) 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 3: The asymptotic ergodic secrecy rate at $\tilde{\alpha}_1\to\infty$ and a fixed $\tilde{\alpha}_2$ is given by (26) at the top of the next page. In (26), $\psi(\cdot)$ is the digamma function [38].

Proof: A proof of this corollary is provided in Appendix E. ∎

With the help of (26), we confirm that the multiplexing gain [39] is 1/2 in bits/sec/Hz/(3 dB), which is given by

$$S^{\infty}=\lim_{\tilde{\alpha}_1\to\infty}\frac{\bar{C}_1^{\infty}}{\log_2(\tilde{\alpha}_1)}=\frac{1}{2}. \tag{27}$$

It is indicated from (27) that under these circumstances, secure communication achieves the same spectral efficiency as communication without eavesdropping. Moreover, using (26), 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

$$\Delta P\ (\mathrm{dB})=\frac{10}{\log 10}\left[\eta(K_1)-\eta(K_2)\right] \tag{28}$$

where

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

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 $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2}=\kappa$, and provide the following corollary.

Corollary 4: 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 (29) at the top of the next page.

Proof: A proof of this corollary is provided in Appendix F. ∎

It is indicated from (29) that a capacity ceiling exists in this case.

D. The Effects of Multiple Antennas at the Eavesdroppers

We shall investigate the effect of multiple antennas at the eavesdroppers. Using MRC at each eavesdropper, the received signal expressed in (1) becomes

$$\boldsymbol{r}^{k,n}=\sqrt{P_s\alpha_2^{k,n}}\sum_{r=1}^{M}(\tilde{\boldsymbol{H}}_r^{k,n})^H\boldsymbol{H}_r^{k,n}\boldsymbol{x}+\sum_{r=1}^{M}(\tilde{\boldsymbol{H}}_r^{k,n})^H\boldsymbol{n}_1^{k,n} \tag{30}$$

where $\boldsymbol{H}_r^{k,n}$ is the right circulant matrix formed for a link from the kth relay to the rth receive antenna branch at the nth eavesdropper. In the formulation of (30), we assume M antennas at the each eavesdropper, and $\alpha_2^{k,n}$ is independent of the antenna branches. In addition, $\tilde{\boldsymbol{H}}_r^{k,n}$ is the receive matrix for the rth receive antenna branch at the nth eavesdropper. The maximum instantaneous post-processing SNR due to MRC, which is imposes $\tilde{\boldsymbol{H}}_r^{k,n}=\boldsymbol{H}_r^{k,n}$, becomes [33]

$$\gamma_2^{k,n,\mathrm{eMRC}}=\frac{P_s\alpha_2^{k,n}\sum_{r=1}^{M}\|\boldsymbol{h}_r^{k,n}\|^2}{\sigma_n^2}. \tag{31}$$

Comparing to the expression in (2), we can easily see that

$$\gamma_2^{k,n,\mathrm{eMRC}}=\tilde{\alpha}_2^{k,n}\sum_{r=1}^{M}\|\boldsymbol{h}_r^{k,n}\|^2\ \sim\chi^2(2N_2M,\tilde{\alpha}_2^{k,n}). \tag{32}$$

$$\bar{C}_s = -\frac{C}{2\log(2)}\widetilde{\sum}\sum_{q=1}^{Q}\binom{Q}{q}(-1)^q \sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}\left(t!(\tilde{\alpha}_1)^t\right)^{w_{t+1}}}$$
$$\Big(\frac{\Gamma(\tilde{N}_2)\Gamma(\tilde{L}_1+1)}{(\beta_2)^{\tilde{N}_2}}\Psi(\tilde{L}_1+1,\tilde{L}_1+1;q/\tilde{\alpha}_1) - \sum_{n_1=0}^{\tilde{N}_2-1}\frac{\Gamma(\tilde{N}_2)\Gamma(\tilde{L}_1+n_1+1)}{n_1!(\beta_2)^{\tilde{N}_2-n_1}}$$
$$\Psi(\tilde{L}_1+n_1+1,\tilde{L}_1+n_1+1;\beta_2+q/\tilde{\alpha}_1)\Big). \tag{25}$$

$$\bar{C}_1^{\infty} = \frac{1}{2}\log_2(\tilde{\alpha}_1) + \frac{1}{2\log(2)}\Big[\frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q\sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}}$$
$$\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}[\psi(N_1+\tilde{L}_1)-\log(q+1)] + \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}$$
$$\sum_{v_1,\ldots,v_{N_2}}^{m}(\frac{m!}{v_1!\ldots v_{N_2}!})\frac{\Gamma(\sum_{t=0}^{N_2-1}tv_{t+1}+1)}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\Psi(\sum_{t=0}^{N_2-1}tv_{t+1}+1,\sum_{t=0}^{N_2-1}tv_{t+1}+1;m/\tilde{\alpha}_2)\Big]. \tag{26}$$

$$\bar{C}_2^{\infty} = \frac{1}{2}\log_2(\kappa) + \frac{1}{2\log(2)}\Big[\frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q\sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}}$$
$$\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}[\psi(N_1+\tilde{L}_1)-\log(q+1)] - \hat{C}\widehat{\sum}\frac{\Gamma(\tilde{N}_2)}{(\hat{\beta})^{\tilde{N}_2}}[\psi(\tilde{N}_2)-\log(\hat{\beta})]\Big]. \tag{29}$$

$$P_{\text{out}}^{\text{eMRC}} = C^{\text{eMRC}}\widetilde{\sum}^{\text{eMRC}}\sum_{q=0}^{Q}\binom{Q}{q}(-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}}\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}$$
$$\sum_{p=0}^{\tilde{L}_1}\binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p\big(\frac{qJ_R}{\tilde{\alpha}_1}+\beta_2\big)^{-(p+\tilde{N}_2^{\text{eMRC}})}(p+\tilde{N}_2^{\text{eMRC}}-1)!,$$

$$Pr(C_s^{\text{eMRC}}>0) = 1 - \frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!}\sum_{k=0}^{K}\sum_{m=0}^{Nk}\sum_{q=0}^{Q-1}\binom{Q-1}{q}\binom{K}{k}\binom{Nk}{m}(-1)^{q+k+m}$$
$$\sum_{v_1,\ldots,v_{MN_2}}^{m}(\frac{m!}{v_1!\ldots v_{MN_2}!})\sum_{w_1,\ldots,w_{N_1}}^{q}(\frac{q!}{w_1!\ldots w_{N_1}!})\frac{1}{\prod_{t=0}^{MN_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}$$
$$\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}(\frac{m}{\tilde{\alpha}_2}+\frac{q+1}{\tilde{\alpha}_1})^{-\tilde{N}_1}(\tilde{N}_1-1)!, \text{ and}$$

$$\bar{C}_s^{\text{eMRC}} = -\frac{1}{2\log(2)}C^{\text{eMRC}}\widetilde{\sum}^{\text{eMRC}}\sum_{q=1}^{Q}\binom{Q}{q}(-1)^q\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}\left(t!(\tilde{\alpha}_1)^t\right)^{w_{t+1}}}$$
$$\Big[\frac{\Gamma(\tilde{N}_2^{\text{eMRC}})\Gamma(\tilde{L}_1+1)}{(\beta_2)^{\tilde{N}_2^{\text{eMRC}}}}\Psi(\tilde{L}_1+1,\tilde{L}_1+1;q/\tilde{\alpha}_1) - \sum_{n_1=0}^{\tilde{N}_2^{\text{eMRC}}-1}\frac{\Gamma(\tilde{N}_2^{\text{eMRC}})\Gamma(\tilde{L}_1+n_1+1)}{n_1!(\beta_2)^{\tilde{N}_2^{\text{eMRC}}-n_1}}$$
$$\Psi(\tilde{L}_1+n_1+1,\tilde{L}_1+n_1+1;\beta_2+q/\tilde{\alpha}_1)\Big]. \tag{33}$$

Using the statistical properties of $\gamma_2^{k,n,\mathrm{eMRC}}$, the performance metrics, such as the secrecy outage probability, the probability of non-zero achievable secrecy rate, and the ergodic secrecy rate can be derived. Their corresponding expressions are given by (33) at the bottom of the previous page. In (33), we have defined $C^{\mathrm{eMRC}} \triangleq C\big|_{N_2 \to MN_2}$, $\widetilde{\sum}^{\mathrm{eMRC}} \triangleq \widetilde{\sum}\Big|_{N_2 \to MN_2}$, and $\tilde{N}_2^{\mathrm{eMRC}} \triangleq MN_2 + (\sum_{t=0}^{MN_2-1} tv_{t+1}) + (\sum_{t=0}^{MN_2-1} tu_{t+1})$.

Corollary 5: The multiple antennas employed in the form of MRC at each eavesdropper do not influence the secrecy diversity gain. They can only change the secrecy array gain.

Proof: According to Theorem 2, the asymptotic secrecy outage probability at a fixed $\tilde{\alpha}_2$ is given by

$$P_{\mathrm{out}}^{\infty,\mathrm{eMRC}} = (G_a^{\mathrm{eMRC}} \tilde{\alpha}_1)^{-QN_1} + O((\tilde{\alpha}_1)^{-QN_1}) \quad (34)$$

where

$$G_a^{\mathrm{eMRC}} = \Big[\frac{\hat{C}^{\mathrm{eMRC}}}{(N_1!)^Q} \widehat{\sum}^{\mathrm{eMRC}} \sum_{l=0}^{QN_1} \binom{QN_1}{l} (J_R - 1)^{QN_1 - l} (J_R)^l (\tilde{\alpha}_2)^l \frac{(l + \tilde{N}_2^{\mathrm{eMRC}} - 1)!}{(\hat{\beta})^{l + \tilde{N}_2^{\mathrm{eMRC}}}}\Big]^{-\frac{1}{QN_1}} \quad (35)$$

with $\hat{C}^{\mathrm{eMRC}} \triangleq \hat{C}\big|_{N_2 \to MN_2}$ and $\widehat{\sum}^{\mathrm{eMRC}} \triangleq \widehat{\sum}\Big|_{N_2 \to MN_2}$, where $\hat{C}$ and $\widehat{\sum}$ are specified in (16). From (34), we can readily see that MRC at the each eavesdropper does not affect the secrecy diversity gain. ■

Corollary 6: The multiple antennas employed in the form of MRC at the eavesdroppers do not influence the multiplexing gain. They can only change the additional power cost for a specified target ergodic secrecy rate.

Proof: According to Corollary 3, the asymptotic ergodic secrecy rate at a fixed $\tilde{\alpha}_2$ is given by only interchanging the parameter $N_2 \to MN_2$. From (27), we see that the multiplexing gain is still 1/2, and MRC at the eavesdroppers impacts the additional power cost as shown in (28). ■

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 $\boldsymbol{h}^{k,n} \sim CN(\mathbf{0}, \boldsymbol{I}_{N_2}), \forall k, n$ and $\boldsymbol{g}^{k,q} \sim CN(\mathbf{0}, \boldsymbol{I}_{N_1}), \forall k, q$. The curves obtained via actual link simulations are denoted by **Ex**, whereas analytically derived curves are denoted by **An**. Asymptotically obtained curves are denoted by **As** in the following figures.

A. Secrecy Outage Probability

Figs. 2-4 show the secrecy outage probability for various scenarios. Fig. 2 shows the secrecy outage probability for various values of N_1 at fixed values of $(K = 4, N = 2, N_2 = 3, Q = 1, M = 1, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB. As Theorem 2 proves, a lower secrecy outage probability is achieved by a bigger value of N_1. In this particular scenario, the secrecy diversity gain becomes N_1. We can see exact matches between the analytically derived curves and the simulation obtained curves for the outage probability. Fig. 3 shows the secrecy outage probability for various values of Q and M at fixed value of $(K = 4, N = 2, N_1 = 3, N_2 = 2, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB. We can observe the effect of the multiuser diversity gain on the secrecy outage probability. As Q increases, a lower secrecy outage probability is obtained due to the multiuser diversity. We can also observe the effect of multiple antennas at the eavesdroppers. For the same channel length and the number of destinations, for example, $(N_1 = 3, N_2 = 2, Q = 1, M = 1)$ has a 3 dB gain over $(N_1 = 3, N_2 = 2, Q = 1, M = 2)$ at 1×10^{-3} outage probability. Similar behavior can be observed as M becomes larger. Moreover, it can be seen that N, the number of eavesdroppers, does not change the secrecy diversity gain. Fig. 4 verifies the derived asymptotic secrecy outage probability at a fixed $\tilde{\alpha}_2$. As $\tilde{\alpha}_1$ increases, the asymptotic curves approaches the simulation obtained curves for various values of N_1, Q, and M. From these curves, we can see that the secrecy diversity gain is $N_1 Q$, which is determined by the multipath diversity gain, N_1, and the multiuser diversity gain, Q. It is irrespective of M. A similar overall diversity gain is obtained in [27], which does not consider eavesdroppers.

B. The Non-Zero achievable Secrecy Rate

Fig. 5 illustrates the non-zero achievable secrecy rate for various values of N_1, M, and Q. At fixed $(K = 4, N = 2)$ and $\tilde{\alpha}_2 = 5$ dB, this figure shows that $(N_1 = 2, M = 2, Q = 1)$ has the slowest convergence speed arriving at $Pr(C_{\min} > 0) = 0.999$ due to the smallest achievable diversity gain and the value of M. Although $(N_1 = 2, M = 2, Q = 1)$ has the same diversity gain as $(N_1 = 2, M = 1, Q = 1)$, its convergence speed is slowest due to greater eavesdropping capability of eavesdroppers. If we compare two particular scenarios, such as $(N_1 = 2, M = 2, Q = 1)$ and $(N_1 = 3, M = 2, Q = 1)$, then the multipath diversity is seen to be one of the key factor in determining the convergence speed, whereas by comparing $(N_1 = 2, M = 2, Q = 1)$ with $(N_1 = 2, M = 2, Q = 2)$, we can see that the multiuser diversity is another key factor in

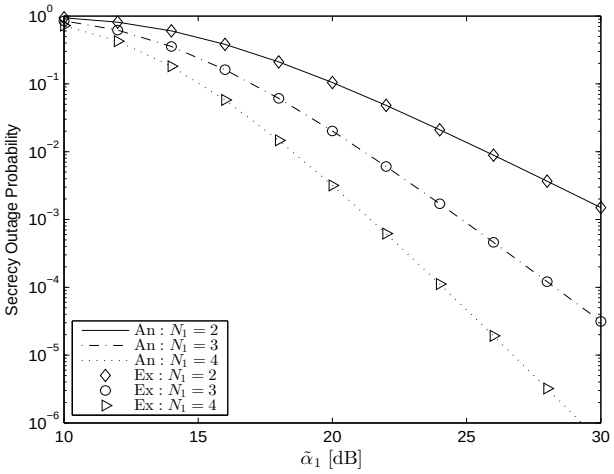

Fig. 2. Secrecy outage probability for various values of N_1 at fixed values of $(N_2 = 3, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB.

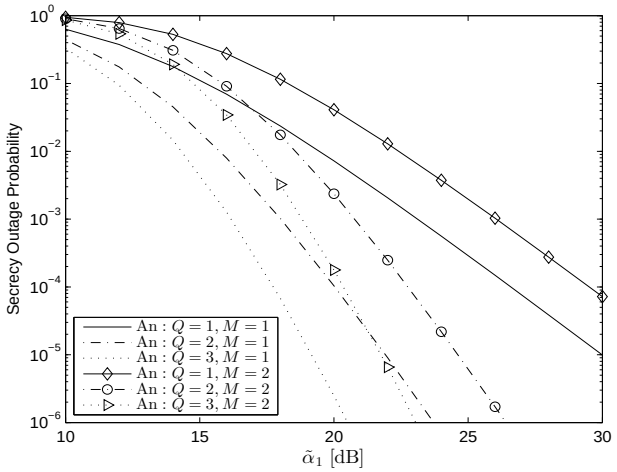

Fig. 3. Secrecy outage probability for various values of Q and M at fixed values of $(N_1 = 3, N_2 = 2, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB.

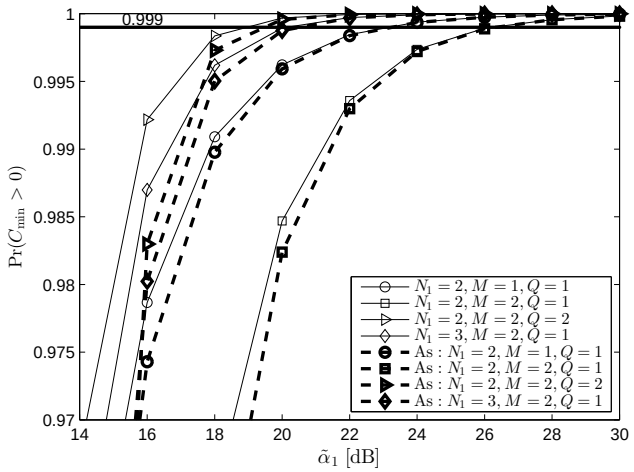

Fig. 5. Non-zero achievable secrecy rate for various values of N_1, M, and Q at fixed values of $N_2 = 2$ and $\tilde{\alpha}_2 = 5$ dB.

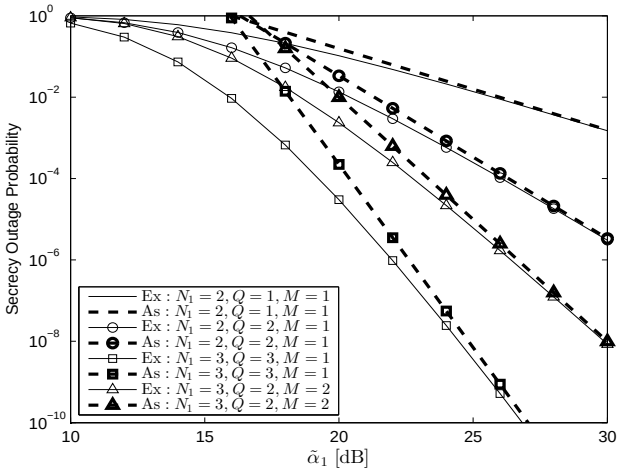

Fig. 4. Asymptotic secrecy outage probability for various values of N_1, Q, and M at fixed values of $(N_2 = 3, R = 1)$ and $\tilde{\alpha}_2 = 5$ dB.

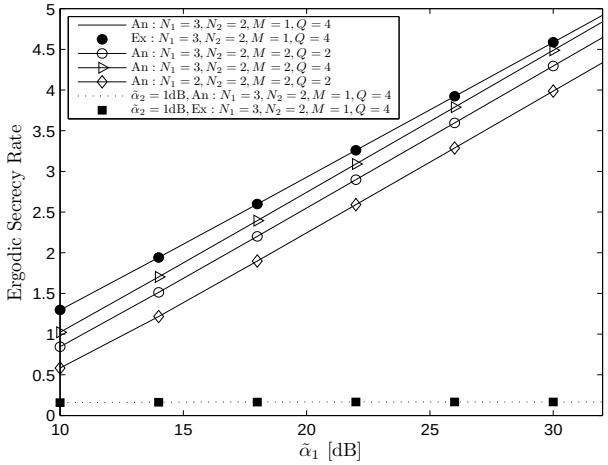

Fig. 6. Ergodic secrecy rate for various values of (K, N_1, N_2, M, Q).

determining the convergence speed of the non-zero achievable secrecy rate.

C. The Ergodic Secrecy Rate

In Fig. 6, we first compare the derived ergodic secrecy rate with the simulation obtained ergodic secrecy rate for the case of $(N_1 = 3, N_2 = 2, M = 1, Q = 4)$. 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 compare several scenarios to investigate the effects from the system configurations and channels.

- The effect of eavesdropping: More eavesdropping reduces the ergodic secrecy rate. For example, $(N_1 = 3, N_2 = 2, M = 2, Q = 4)$ vs. $(N_1 = 3, N_2 = 2, M = 1, Q = 4)$.
- The effect of multipath diversity which is achievable between the relay and the destination: Higher multipath diversity gain results in a higher ergodic secrecy rate. For example, $(N_1 = 3, N_2 = 2, M = 2, Q = 2)$ vs. $(N_1 = 2, N_2 = 2, M = 2, Q = 2)$.
- The effect of number of destinations: With more destinations, a higher ergodic secrecy rate can be obtained due to a larger multiuser diversity gain. For example, $(N_1 = 2, N_2 = 2, M = 2, Q = 4)$ vs. $(N_1 = 2, N_2 = 2, M = 2, Q = 2)$.
- The effect of fixed $\tilde{\alpha}_2$: As Corollary 4 verified, capacity ceilings are intrinsic for this case.

In Fig. 7, we show the asymptotic ergodic secrecy rate for various values of (K, N_1, N_2, M, Q) at a fixed number of eavesdroppers $N = 3$ and $\tilde{\alpha}_2$. This plot shows the corresponding asymptotic ergodic secrecy rate obtained from Corollary 3. As $\tilde{\alpha}_1$ increases, the differences between the analytical 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 (28), a total of five

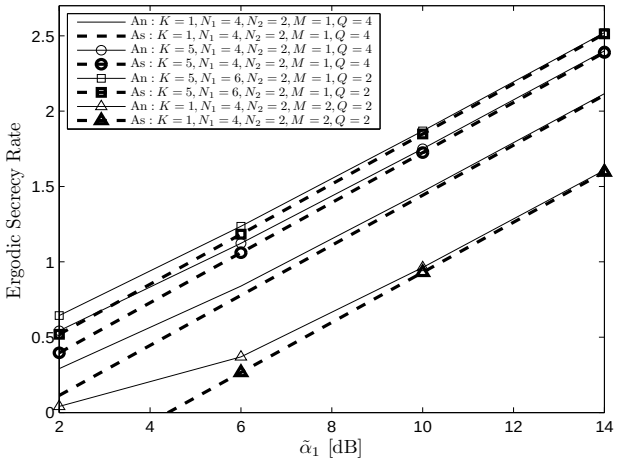

Fig. 7. Ergodic secrecy rate for various values of N_1 and Q at fixed values of $(K=4,N=2)$ and $\tilde{\alpha}_2=1$ dB.

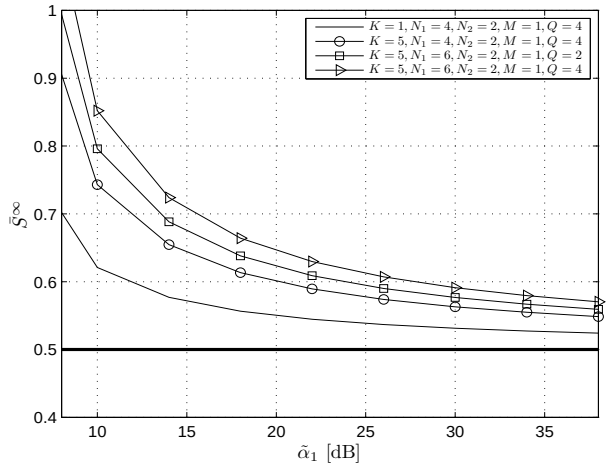

Fig. 8. Multiplexing gain S^{∞}.

relays can reduce 0.8 dB power than a single relay in achieving 2.0 secrecy rate. Fig. 8 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 (26), 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: 1) relay is selected to minimize the worst-case eavesdropping, and 2) the desired destination is selected to achieve the multiuser diversity gain. We have derived the secrecy outage probability, the non-zero secrecy rate, and the ergodic secrecy rate. From the derivations and the link simulations, the diversity gain has been shown to be determined by the multipath diversity gain and the multiuser diversity gain. 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 Lemma 1

According to the order statistics, the PDF of $\gamma_2^{\min,\max}$ is given by

$$f_{\gamma_2^{\min,\max}}(x)=K(1-F_{\gamma_2^{k,\max}}(x))^{K-1}f_{\gamma_2^{k,\max}}(x). \quad \text{(A.1)}$$

Binomial and multinomial formulas provide the following expression for $f_{\gamma_2^{k,\max}}(x)$:

$$f_{\gamma_2^{k,\max}}(x)=\frac{N}{(\tilde{\alpha}_2)^{N_2}(N_2-1)!}\sum_{j=0}^{N-1}\binom{N-1}{j}(-1)^j e^{-\frac{x(j+1)}{\tilde{\alpha}_2}} \sum_{u_1,\ldots,u_{N_2}}^{j}\Big(\frac{j!}{u_1!\ldots u_{N_2}!}\Big)\frac{x^{N_2+\sum_{t=0}^{N_2-1}tu_{t+1}-1}}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{u_{t+1}}}. \quad \text{(A.2)}$$

Again binomial and multinomial formulas lead us to get the following expression for $(1-F_{\gamma_2^{k,\max}}(x))^{K-1}$:

$$\begin{aligned}
&(1-F_{\gamma_2^{k,\max}}(x))^{K-1}\\
&=\Big[1-\Big(1-e^{-x/\tilde{\alpha}_2}\sum_{l=0}^{N_2-1}\frac{1}{l!}\Big(\frac{x}{\tilde{\alpha}_2}\Big)^l\Big)^N\Big]^{K-1}\\
&=\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k\Big(1-e^{-x/\tilde{\alpha}_2}\sum_{l=0}^{N_2-1}\frac{1}{l!}\Big(\frac{x}{\tilde{\alpha}_2}\Big)^l\Big)^{kN}\\
&=\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k\sum_{m=0}^{Nk}\binom{Nk}{m}(-1)^m e^{-mx/\tilde{\alpha}_2}\\
&\quad\Big(\sum_{l=0}^{N_2-1}\frac{1}{l!}(\frac{x}{\tilde{\alpha}_2})^l\Big)^m\\
&=\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k\sum_{m=0}^{Nk}\binom{Nk}{m}(-1)^m e^{-mx/\tilde{\alpha}_2}\\
&\quad\sum_{v_1,\ldots,v_{N_2}}^{m}\Big(\frac{m!}{v_1!\ldots v_{N_2}!}\Big)\frac{x^{\sum_{t=0}^{N_2-1}tv_{t+1}}}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}. \qquad \text{(A.3)}
\end{aligned}$$

Multiplying (A.2) and (A.3) and after some manipulations, yields (8).

Appendix B: A detailed derivation of Theorem 1

Now substituting $f_{\gamma_2^{\min,\max}}(\gamma)$, which is derived in (8) and $F_{\gamma_1^{k^*,q^*}}(\gamma)$, which is derived in (5) into (12), we have (B.1) at the top of the next page. Using multinomial and binomial formulas, J_1 becomes

$$J_1=\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} \sum_{p=0}^{\tilde{L}_1}\binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p\gamma^p. \quad \text{(B.2)}$$

$$P_{out} = \int_0^\infty \Big[1 - e^{-(J_R-1+J_R\gamma)/\tilde{\alpha}_1} \sum_{l=0}^{N_1-1} \frac{1}{l!}\Big(\frac{(J_R-1+J_R\gamma)}{\tilde{\alpha}_1}\Big)^l\Big]^Q f_{\gamma_2^{\min,\max}}(\gamma)d\gamma$$
$$= \sum_{q=0}^{Q}\binom{Q}{q}(-1)^q \int_0^\infty e^{-q(J_R-1+J_R\gamma)/\tilde{\alpha}_1} \underbrace{\Big[\sum_{l=0}^{N_1-1} \frac{1}{l!}\Big(\frac{(J_R-1+J_R\gamma)}{\tilde{\alpha}_1}\Big)^l\Big]^q}_{J_1} f_{\gamma_2^{\min,\max}}(\gamma)d\gamma. \quad \text{(B.1)}$$

Substituting (B.2) into (B.1), yields

$$P_{out} = \sum_{q=0}^{Q}\binom{Q}{q}(-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}} \sum_{w_1,\ldots,w_{N_1}}^{q} \frac{q!}{w_1!\ldots w_{N_1}!} \frac{\sum_{p=0}^{\tilde{L}_1}\binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} \int_0^\infty e^{-qJ_R\gamma/\tilde{\alpha}_1}\gamma^p f_{\gamma_2^{\min,\max}}(\gamma)d\gamma. \quad \text{(B.3)}$$

Again using (8) into (B.3), we have (B.4) at the top of the next page which proves (13).

APPENDIX C: A DETAILED DERIVATION OF THEOREM 2

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 (5), at high $\tilde{\alpha}_1$ as

$$F_{\gamma_1^{k^*,q^*}}(x) = \Big[1 - e^{-x/\tilde{\alpha}_1}\Big(e^{x/\tilde{\alpha}_1} - \frac{1}{N_1!}\Big(\frac{x}{\tilde{\alpha}_1}\Big)^{N_1} - O((\frac{x}{\tilde{\alpha}_1})^{N_1})\Big)\Big]^Q = \frac{1}{(N_1!)^Q}\left(\frac{x}{\tilde{\alpha}_1}\right)^{QN_1} + O((\tilde{\alpha}_1)^{-QN_1}). \quad \text{(C.1)}$$

In addition, the PDF expression $f_{\gamma_2^{\min,\max}}(x)$ in (8) needs to be written as

$$f_{\gamma_2^{\min,\max}}(x) = \hat{C}\widehat{\sum}\frac{x^{\tilde{N}_2-1}}{(\tilde{\alpha}_2)^{\tilde{N}_2}}e^{-\frac{\hat{\beta}x}{\tilde{\alpha}_2}}\mathrm{U}(x). \quad \text{(C.2)}$$

Substituting (C.1) and (C.2) into (12), the asymptotic secrecy outage probability is calculated as (C.3) at the top of the next page which proves (15).

APPENDIX D: A DETAILED DERIVATION OF COROLLARY 1

The CDF of $\gamma_2^{\min,\max}$ is given by

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

In addition, the PDF of $\gamma_1^{k^*,q^*}$ is given by

$$f_{\gamma_1^{k^*,q^*}}(x) = \frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q \sum_{w_1,\ldots,w_{N_1}}^{q}\Big(\frac{q!}{w_1!\ldots w_{N_1}!}\Big)\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} x^{N_1+\sum_{t=0}^{N_1-1}tw_{t+1}-1}e^{-\frac{x(q+1)}{\tilde{\alpha}_1}}\mathrm{U}(x). \quad \text{(D.2)}$$

The probability of non-zero achievable secrecy rate is given by

$$Pr(C_s>0) = \int_0^\infty F_{\gamma_2^{\min,\max}}(x)f_{\gamma_1^{k^*,q^*}}(x)dx = 1 - \frac{Q}{(\tilde{\alpha}_1)^{N_1}(N_1-1)!}\sum_{k=0}^{K}\sum_{m=0}^{Nk}\sum_{q=0}^{Q-1}\binom{Q-1}{q}\binom{K}{k}\binom{Nk}{m} (-1)^{q+k+m}\sum_{v_1,\ldots,v_{N_2}}^{m}\Big(\frac{m!}{v_1!\ldots v_{N_2}!}\Big)\sum_{w_1,\ldots,w_{N_1}}^{q}\Big(\frac{q!}{w_1!\ldots w_{N_1}!}\Big) \frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}} \int_0^\infty e^{-x(\frac{m}{\tilde{\alpha}_2}+\frac{q+1}{\tilde{\alpha}_1})}x^{\tilde{N}_1-1}dx \quad \text{(D.3)}$$

which becomes (18).

APPENDIX E: A DETAILED DERIVATION OF COROLLARY 3

Based on (D.1), we first rewrite the CDF of $\gamma_2^{\min,\max}$ as

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

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 (E.2) at the top of the next page. As $\tilde{\alpha}_1 \to \infty$, Θ_1 asymptotically becomes

$$\Theta_1^\infty = \int_0^\infty \Big[\log(\tilde{\alpha}_1) + \log\left(\frac{x_1}{\tilde{\alpha}_1}\right)\Big]f_{\gamma_1^{k^*,q^*}}(x_1)\,dx_1 = \log(\tilde{\alpha}_1) + \int_0^\infty \log\left(\frac{x_1}{\tilde{\alpha}_1}\right)f_{\gamma_1^{k^*,q^*}}(x_1)\,dx_1. \quad \text{(E.3)}$$

Substituting the PDF of $\gamma_1^{k^*,q^*}$ given in (D.2) into (E.3), and employing [37, eq. 4.352.1] given by

$$
\begin{aligned}
P_{out} &= C\widetilde{\sum}\sum_{q=0}^{Q}\binom{Q}{q}(-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}}\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{\sum_{p=0}^{\tilde{L}_1}\binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}\\
&\quad\int_0^\infty e^{-\gamma\left(\frac{qJ_R}{\tilde{\alpha}_1}+\beta_2\right)}\gamma^{p+\tilde{N}_2-1}d\gamma\\
&= C\widetilde{\sum}\sum_{q=0}^{Q}\binom{Q}{q}(-1)^q e^{-\frac{q(J_R-1)}{\tilde{\alpha}_1}}\sum_{w_1,\ldots,w_{N_1}}^{q}\frac{q!}{w_1!\ldots w_{N_1}!}\frac{1}{\prod_{t=0}^{N_1-1}(t!(\tilde{\alpha}_1)^t)^{w_{t+1}}}\\
&\quad\sum_{p=0}^{\tilde{L}_1}\binom{\tilde{L}_1}{p}(J_R-1)^{\tilde{L}_1-p}(J_R)^p\Big(\frac{qJ_R}{\tilde{\alpha}_1}+\beta_2\Big)^{-(p+\tilde{N}_2)}(p+\tilde{N}_2-1)!. \qquad \text{(B.4)}
\end{aligned}
$$

$$
\begin{aligned}
P_{out}^{\infty} &= \frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}\int_0^\infty\Big(\frac{J_R\gamma+J_R-1}{\tilde{\alpha}_1}\Big)^{QN_1}\frac{\gamma^{\tilde{N}_2-1}}{(\tilde{\alpha}_2)^{\tilde{N}_2}}e^{-\frac{\hat{\beta}\gamma}{\tilde{\alpha}_2}}d\gamma+O((\tilde{\alpha}_1)^{-QN_1})\\
&= \frac{\hat{C}}{(N_1!)^Q}\widehat{\sum}\sum_{l=0}^{QN_1}\binom{N_1}{l}\Big(\frac{1}{\tilde{\alpha}_1}\Big)^{QN_1}(J_R-1)^{QN_1-l}(J_R)^l\int_0^\infty\gamma^l\frac{\gamma^{\tilde{N}_2-1}}{\big(\tilde{\alpha}_1\big)^{\tilde{N}_2}}e^{-\frac{\hat{\beta}\gamma}{\tilde{\alpha}_2}}d\gamma+\\
&\quad O((\tilde{\alpha}_1)^{-QN_1})\\
&= \frac{C}{(N_1!)^Q}\widehat{\sum}\sum_{l=0}^{QN_1}\binom{QN_1}{l}\Big(\frac{1}{\tilde{\alpha}_1}\Big)^{QN_1}(J_R-1)^{QN_1-l}(J_R)^l(\tilde{\alpha}_2)^l\frac{(l+\tilde{N}_2-1)!}{(\hat{\beta})^{l+\tilde{N}_2}}+O\big((\tilde{\alpha}_1)^{-QN_1}\big)\\
&= (G_a\tilde{\alpha}_1)^{-QN_1}+O((\tilde{\alpha}_1)^{-QN_1}). \qquad \text{(C.3)}
\end{aligned}
$$

$$
\begin{aligned}
\bar{C}_s &= \frac{1}{2\log(2)}\int_0^\infty\left[\int_0^{x_1}\frac{F_{\gamma_2^{\min,\max}}(x_2)}{1+x_2}dx_2\right]f_{\gamma_1^{k^*,q^*}}(x_1)\,dx_1\\
&= \frac{1}{2\log(2)}\Big[\underbrace{\int_0^\infty\log(1+x_1)f_{\gamma_1^{k^*,q^*}}(x_1)dx_1}_{\Theta_1}+\underbrace{\int_0^\infty\int_0^{x_1}\frac{\tilde{F}_{\gamma_2^{\min,\max}}(x_2)}{1+x_2}f_{\gamma_1^{k^*,q^*}}(x_1)dx_2dx_1}_{\Theta_2}\Big]. \qquad \text{(E.2)}
\end{aligned}
$$

$\int_0^\infty x^{\nu-1}e^{-\mu x}\log(x)\,dx = \frac{1}{\mu^\nu}\Gamma(\nu)\big[\psi(\nu)-\log(\mu)\big]$, asymptotic expression for Θ_2 is given by we compute (E.3) as

$$
\begin{aligned}
\Theta_1^{\infty} &= \log(\tilde{\alpha}_1)+\frac{Q}{(N_1-1)!}\sum_{q=0}^{Q-1}\binom{Q-1}{q}(-1)^q\\
&\quad\sum_{w_1,\ldots,w_{N_1}}^{q}\Big(\frac{q!}{w_1!\ldots w_{N_1}!}\Big)\frac{1}{\prod_{t=0}^{N_1-1}(t!)^{w_{t+1}}}\\
&\quad\frac{\Gamma(N_1+\tilde{L}_1)}{(q+1)^{N_1+\tilde{L}_1}}\big[\psi(N_1+\tilde{L}_1)-\log(q+1)\big]. \qquad \text{(E.4)}
\end{aligned}
$$

Changing the order of integration in Θ_2, we have

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

According to the first order expansion of the CDF of $\gamma_1^{k^*,q^*}$ shown in (C.1), as $\tilde{\alpha}_1\to\infty$, $F_{\gamma_1^{k^*,q^*}}(x_2)\approx 0$. Hence, the

$$
\begin{aligned}
\Theta_2^{\infty} &= \int_0^\infty\frac{\tilde{F}_{\gamma_2^{\min,\max}}(x_2)}{1+x_2}dx_2\\
&= \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}\sum_{v_1,\ldots,v_{N_2}}^{m}\Big(\frac{m!}{v_1!\ldots v_{N_2}!}\Big)\\
&\quad\frac{1}{\prod_{t=0}^{N_2-1}(t!(\tilde{\alpha}_2)^t)^{v_{t+1}}}\int_0^\infty\frac{e^{-mx_2/\tilde{\alpha}_2}x_2^{\sum_{t=0}^{N_2-1}tv_{t+1}}}{1+x_2}dx_2\\
&= \sum_{k=1}^{K}\sum_{m=1}^{Nk}\binom{K}{k}\binom{Nk}{m}(-1)^{k+m+1}\sum_{v_1,\ldots,v_{N_2}}^{m}\Big(\frac{m!}{v_1!\ldots v_{N_2}!}\Big)\\
&\quad\frac{\Gamma(\sum_{t=0}^{N_2-1}tv_{t+1}+1)}{\prod_{t=0}^{N_2-1}\big(t!(\tilde{\alpha}_2)^t\big)^{v_{t+1}}}\\
&\quad\Psi(\sum_{t=0}^{N_2-1}tv_{t+1}+1,\ \sum_{t=0}^{N_2-1}tv_{t+1}+1;m/\tilde{\alpha}_2). \qquad \text{(E.6)}
\end{aligned}
$$

Substituting (E.6) and (E.4) into (E.2), we derive the asymptotic expression for the ergodic secrecy capacity as (26).

APPENDIX F: A DETAILED DERIVATION OF COROLLARY 4

In the case of $\tilde{\alpha}_1 \to \infty$ and $\tilde{\alpha}_2 \to \infty$ with $\frac{\tilde{\alpha}_1}{\tilde{\alpha}_2} = \kappa$, the asymptotic ergodic secrecy rate can be easily obtained based on the proof of Corollary 3 in Appendix E. We only need to further provide an asymptotic expression for Θ_2^{∞} with $\tilde{\alpha}_2 \to \infty$. Observing Θ_1^{∞} in (E.3), an asymptotic expression for Θ_2^{∞} can be derived as

$$\Theta_{21}^{\infty} = -\log\left(\tilde{\alpha}_2\right) - \int_0^{\infty} \log\left(\frac{x_2}{\tilde{\alpha}_2}\right) f_{\gamma_2^{\min,\max}}\left(x_2\right) dx_2. \quad \text{(F.1)}$$

Substituting the PDF of $\gamma_2^{\min,\max}$ in (8) into (F.1), we obtain

$$\begin{aligned}\Theta_{21}^{\infty} &= -\log\left(\tilde{\alpha}_2\right) - \hat{C}\widehat{\sum} \int_0^{\infty} e^{-\hat{\beta}x} x^{\tilde{N}_2 - 1} \log(x_2) dx_2 \\ &= -\log(\tilde{\alpha}_2) - \hat{C}\widehat{\sum} \frac{\Gamma(\tilde{N}_2)}{(\hat{\beta})^{\tilde{N}_2}} [\psi(\tilde{N}_2) - \log(\hat{\beta})]. \quad \text{(F.2)}\end{aligned}$$

Substituting the new asymptotic expression for Θ_2^{∞} in (F.2) and (E.4) into (E.2), we get (29).

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] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.

[3] 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.

[4] 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.

[5] J. Huang and A. L. Swindlehurst, "Robust secure transmission in miso channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] J. Ding, M. Xu, J. Lu, and F. Liu, "Improving wireless security for bidirectional communication scenarios," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2842–2848, 2012.

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

[15] J. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, 2012.

[16] 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.

[17] 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.

[18] IEEE P802.11ad/D0.1, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Enhancements for very high throughput in the 60GHz band," Jun. 2010.

[19] K. J. Kim and T. A. Tsiftsis, "Performance analysis of QRD-based cyclically prefixed single-carrier transmissions with opportunistic scheduling," *IEEE Trans. Veh. Technol.*, vol. 60, pp. 328–333, Jan. 2011.

[20] Y.-C. Liang, W. S. Leon, Y. Zeng, and C. Xu, "Design of cyclic delay diversity for single carrier cyclic prefix (SCCP) transmissions with block-iterative GDFE(BI-GDFE) receiver," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 677–684, Feb. 2008.

[21] A. Mehana and A. Nosratinia, "Single-carrier frequency-domain equalizer with multi-antenna transmit diversity," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 388–397, Jan. 2013.

[22] D.-Y. Seol, U.-K. Kwon, and G.-H. Im, "Performance of single carrier transmission with cooperative diversity over fast fading channels," *IEEE Trans. Commun.*, vol. 57, pp. 2799–2807, Sep. 2009.

[23] F. Gao, A. Nallanathan, and C. Tellambura, "Blind channel estimation for cyclic-prefixed single-carrier systems by exploiting real symbol characteristics," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 2487–2498, Sep. 2007.

[24] Y. Zeng and T. S. Ng, "Pilot cyclic prefixed single carrier transmission communication: Channel estimation and equalization," *IEEE Signal Process. Lett.*, vol. 12, pp. 56–59, Jan. 2005.

[25] Y. Wang and X. Dong, "Frequency-domain channel estimation for SC-FDE in UWB communications," *IEEE Trans. Commun.*, vol. 54, pp. 2155–2163, Dec. 2006.

[26] H. Chergui, T. Ait-Idir, M. Benjillali, and S. Saoudi, "Joint-over-transmissions project and forward relaying for single carrier broadband MIMO ARQ systems," in *Proc. IEEE Veh. Techol. Conf.*, Yokohama, Japan, May 2011, pp. 1–5.

[27] 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.

[28] H. Eghbali, S. Muhaidat, and N. Al-Dhahir, "A novel receiver design for single-carrier frequency domain equalization in broadband wireless networks with amplify-and-forward relaying," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 721–727, Mar. 2011.

[29] 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.

[30] K. J. Kim and T. A. Tsiftsis, "On the performance of cyclic prefix-based single-carrier cooperative diversity systems with best relay selection," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1269–1279, Apr. 2011.

[31] K. J. Kim, T. Q. Duong, H. V. Poor, and L. Shu, "Performance analysis of cyclic prefixed single-carrier spectrum sharing relay systems in primary user interference," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6729–6734, Dec. 2012.

[32] K. J. Kim, T. Q. Duong, and X.-N. Tran, "Performance analysis of cognitive spectrum-sharing single-carrier systems with relay selection," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6435–6449, Dec. 2012.

[33] 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.

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

[35] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[36] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

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

[38] M. Abramovitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed. New York: Dover, 1972.
[39] 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.

Lifeng Wang (S'12) is working towards his Ph.D. degree in Electronic Engineering at Queen Mary University of London. Before that, he received the M.S. degree in Electronic Engineering from the University of Electronic Science and Technology of China, in 2012.

His research interests include millimeter-wave communications, physical layer security and 5G HetNets.

Kyeong Jin Kim (SM'11) received the M.S. degree from the Korea Advanced Institute of Science and Technology (KAIST) in 1991 and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of California, Santa Barbara in 2000. During 1991-1995, he was a research engineer at the video research center of Daewoo Electronics, Ltd., Korea. In 1997, he joined the data transmission and networking laboratory, University of California, Santa Barbara. After receiving his degrees, he joined the Nokia research center (NRC) and Nokia Inc., Dallas, TX, as a senior research engineer, where he was, from 2005 to 2009, an L1 specialist. During 2010-2011, he was an Invited Professor at Inha University, Korea. Since 2012, he has worked as a senior principal research staff in the Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA. His research has been focused on the transceiver design, resource management, scheduling in the cooperative wireless communications systems, cooperative spectrum sharing system, device-to-device communications, and GPS systems.

Dr. Kim currently serves as an editor for the IEEE COMMUNICATIONS LETTERS and INTERNATIONAL JOURNAL OF ANTENNAS AND PROPAGATION. He also serves as guest editors for the EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING: Special Issue on "Cooperative Cognitive Networks" and IET COMMUNICATIONS: Special Issue on "Secure Physical Layer Communications". He served as a TPC chair for the IEEE GLOBECOM 2013 and 2014 Workshop on Trusted Communications with Physical Layer Security. He received the Best Paper Award at the International Conference on Communications and Networking in China (CHINACOM) in 2014.

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, and then continued working at BTH as a project manager. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). He held a visiting position at Polytechnic Institute of New York University and Singapore University of Technology and Design in 2009 and 2011, respectively. 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.

Dr. Duong has been a TPC chair for several IEEE international conferences and workshops including the most recently IEEE GLOBECOM13 Workshop on Trusted Communications with Physical Layer Security. He currently serves as an Editor for the IEEE COMMUNICATIONS LETTERS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. Dr. Duong has served as the Lead Guest Editor of the special issue on "Location Awareness for Radios and Networks" of the IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, the Lead Guest Editor of the special issue on "Secure Physical Layer Communications" of the IET COMMUNICATIONS, Guest Editor of the special issue on "Green Media: Toward Bringing the Gap between Wireless and Visual Networks" of the IEEE WIRELESS COMMUNICATIONS MAGAZINE, Guest Editor of the special issue on "Millimeter Wave Communications for 5G" and "Energy Harvesting Communications" of the IEEE COMMUNICATIONS MAGAZINE, Guest Editor of the special issue on "Cooperative Cognitive Networks" of the EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, Guest Editor of special issue on "Security Challenges and Issues in Cognitive Radio Networks" of the EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He is awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013 and the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012.

Maged Elkashlan (M'06) received the Ph.D. degree in Electrical Engineering from the University of British Columbia, Canada, 2006. From 2006 to 2007, he was with the Laboratory for Advanced Networking at University of British Columbia. From 2007 to 2011, he was with the Wireless and Networking Technologies Laboratory at Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. During this time, he held an adjunct appointment at University of Technology Sydney, Australia. In 2011, he joined the School of Electronic Engineering and Computer Science at Queen Mary University of London, UK, as an Assistant Professor. He also holds visiting faculty appointments at the University of New South Wales, Australia, and Beijing University of Posts and Telecommunications, China. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing for distributed data processing, millimeter wave communications, cognitive radio, and physical layer security.

Dr. Elkashlan currently serves as an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the IEEE COMMUNICATIONS LETTERS. He also serves as the Lead Guest Editor for the special issue on "Green Media: The Future of Wireless Multimedia Networks" of the IEEE WIRELESS COMMUNICATIONS MAGAZINE, Lead Guest Editor for the special issue on "Millimeter Wave Communications for 5G" of the IEEE COMMUNICATIONS MAGAZINE, Guest Editor for the special issue on "Energy Harvesting Communications" of the IEEE COMMUNICATIONS MAGAZINE, and Guest Editor for the special issue on "Location Awareness for Radios and Networks" of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received the Best Paper Award at the IEEE International Conference on Communications (ICC) in 2014, the International Conference on Communications and Networking in China (CHINACOM) in 2014, and the IEEE Vehicular Technology Conference (VTC-Spring) in 2013. He received the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012.

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. Dr. Poor's research interests are in the areas of stochastic analysis, statistical signal processing, and information theory, and their applications in wireless networks and related fields such as social networks and smart grid. Among his publications in these areas are the recent books *Principles of Cognitive Radio* (Cambridge, 2013) and *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge University Press, 2014).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and 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. In 1990, he served as President of the IEEE Information Theory Society, and in 2004-07 he served as the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, and honorary doctorates from Aalborg University, Aalto University, the Hong Kong University of Science and Technology and the University of Edinburgh.