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

Secrecy Performance of Finite-Sized Cooperative Single Carrier Systems with Unreliable Backhaul Connections

Kim, K.J.; Yeoh, P.L.; Orlik, P.V.; Poor, H.V.

TR2016-106 July 2016

Abstract

In this paper, the secrecy performance of finitesized cooperative cyclic prefixed single carrier systems with multiple eavesdroppers and unreliable wireless backhaul connections across multiple transmitters is investigated. For nonidentical frequency selective fading channels between the relay and destination nodes, secrecy performance metrics including the secrecy outage probability, ergodic secrecy rate, and probability of non-zero achievable secrecy rate are derived. Furthermore, the existence of performance limits on the secrecy outage probability and probability of non-zero achievable secrecy rate are verified for various backhaul scenarios. These limits are found to be exclusively determined by the backhaul reliability. For imperfect backhaul connections, it is found that the diversity gain promised by cooperative cyclic prefixed single carrier systems cannot be achieved in the conventional asymptotic high signal-to-noise ratio region. Link-level simulations are conducted to verify the derived impact of backhaul reliability on the secrecy performance.

IEEE Transactions on Signal Processing

This work may not be copied or reproduced in whole or in part for any commercial purpose. Permission to copy in whole or in part without payment of fee is granted for nonprofit educational and research purposes provided that all such whole or partial copies include the following: a notice that such copying is by permission of Mitsubishi Electric Research Laboratories, Inc.; an acknowledgment of the authors and individual contributions to the work; and all applicable portions of the copyright notice. Copying, reproduction, or republishing for any other purpose shall require a license with payment of fee to Mitsubishi Electric Research Laboratories, Inc. All rights reserved.

Copyright © Mitsubishi Electric Research Laboratories, Inc., 2016
201 Broadway, Cambridge, Massachusetts 02139

Secrecy Performance of Finite-Sized Cooperative Single Carrier Systems with Unreliable Backhaul Connections

Kyeong Jin Kim, *Senior Member, IEEE*, Phee Lep Yeoh, *Member, IEEE*,
Philip V. Orlik, *Senior Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—In this paper, the secrecy performance of finite-sized cooperative cyclic prefixed single carrier systems with multiple eavesdroppers and unreliable wireless backhaul connections across multiple transmitters is investigated. For non-identical frequency selective fading channels between the relay and destination nodes, secrecy performance metrics including the secrecy outage probability, ergodic secrecy rate, and probability of non-zero achievable secrecy rate are derived. Furthermore, the existence of performance limits on the secrecy outage probability and probability of non-zero achievable secrecy rate are verified for various backhaul scenarios. These limits are found to be exclusively determined by the backhaul reliability. For imperfect backhaul connections, it is found that the diversity gain promised by cooperative cyclic prefixed single carrier systems cannot be achieved in the conventional asymptotic high signal-to-noise ratio region. Link-level simulations are conducted to verify the derived impact of backhaul reliability on the secrecy performance.**

***Index Terms*—Wireless backhaul, single carrier transmission, frequency selective fading, two-hop relaying protocol, eavesdroppers, secrecy outage probability, ergodic secrecy rate.**

I. Introduction

COMPLEX technological innovations such as Internet-connected smart cities and the Internet of Things, together with the unrelenting proliferation of tablets and smartphones, point to future wireless networks that will be highly dense and heterogeneous [1]. The accompanying backhaul connections between the control unit (CU) (for example, the access point) and the backbone will also be dense [2]. Thus, a large-scale wired backhaul deployment to support such future networks would lead to excessive costs to maintain all the connections. For this reason, wireless backhaul is emerging as an attractive alternative to wired backhaul for future dense heterogeneous networks [3]. While wireless backhaul can relax the requirement for the availability of wired connections [4], the associated information exchange is intrinsically unreliable due to the stochastic nature of wireless channels.

Manuscript received October 1, 2015; revised February 1, 2016; accepted March 30, 2016. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. S. Cui.

K. J. Kim and P. V. Orlik are with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA.

P. L. Yeoh is with the University of Melbourne, Parkville, Victoria, Austalia.

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA.

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

The reliability of wireless backhaul connections has been recently investigated for coordinated multi-point (CoMP) cooperation in [5]–[9]. In [5], the impact of unreliable backhauls on the delay performance of a heterogeneous cellular network was studied, whereas the average sum rate for cooperative cloud radio access networks was analyzed in [6]. In [7], a game-theoretic approach is employed to study the impact of heterogeneous backhaul on the coherent downlink CoMP cooperation assuming highly available and reliable wired and wireless backhauls. For a finite backhaul capacity, uplink limited cooperation based on data sharing is proposed in [8]. From a secrecy perspective, cooperative scheduling is proposed in [9] to create intentional interference to eavesdroppers in the cellular system where base stations are connected via finite-capacity backhaul links.

Finite-capacity and unreliable backhauls have also been considered in non-cellular networks with distributed relays. In [10], the authors establish the rate-distortion region in the context of source reconstruction, and in [11] the average achievable rate of data transmission over a cooperative relaying network was investigated. For two source nodes connected by orthogonal limited-rate error free backhauls, the outer bound on the capacity region for multicast relaying is derived in [12]. In [13], the authors examine cooperative network coding for relay-assisted two sources and two destinations with an ideal backhaul connection between the source nodes. For uplink joint processing, several schemes such as the distributed compression [14], distributed decoding by exchanging decoded data bits [15], and decentralized decoding [16] are proposed. In [17] and [18], a wireless backhaul is designed to connect multiple wireless access points to a wired gateway.

To circumvent the frequency selective fading nature of wireless channels, we consider cyclic prefixed single carrier (CP-SC) transmission which has a practical deployment with a simple transmitter structure that can avoid the high peak-to-average power ratio exhibited by orthogonal frequency division multiplexing (OFDM) [19]. Several advanced cooperative relaying schemes [20]–[23] have been proposed for CP-SC transmission. In frequency selective fading, it has been shown that an overall diversity gain promised by the multi-user and multi-path diversity gains can be achieved by cooperative CP-SC transmission. The advantages of CP-SC transmission has also been applied to cooperative spectrum sharing systems in [24].

Due to the broadcast nature of wireless transmission, wire-

less physical layer security is an important consideration to ensure the confidentiality of information exchange from eavesdroppers. Several approaches have been proposed to degrade the signal-to-noise ratio (SNR) of the eavesdropper relative to the legitimate receiver by employing multiple antennas at the transmitter and/or the legitimate receiver [25]–[29]. The use of CP-SC transmission for physical layer security has been investigated recently in [30], which proposed a two-stage relay and destination selection procedure. A relay node is first chosen to minimize the amount of information that can be inferred by the eavesdroppers, then a desired destination is selected from the chosen relay node to maximize the instantaneous received SNR.

While the above mentioned literature provides a foundation for the study of CP-SC systems in different applications, the effect of unreliable backhaul on the physical layer security of CP-SC transmission remains unknown. As such, in contrast to the open literature on physical layer security which assume perfect backhaul connections [25]–[33], the main contributions of this paper are summarized as follows.

Contributions:

- We evaluate the overall secrecy performance of a finite-sized cooperative CP-SC system in terms of the number of transmitters while accounting for the backhaul reliability[1] and multiple eavesdroppers that can infer useful information from the main channels. We consider realistic frequency selective fading links that have different fading channel conditions.
- Based on the statistics of the end-to-end SNR (e-SNR) of the main channel, we derive new closed-form expressions for the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate. Moreover, we derive their closed-form expressions in the asymptotic regime that show the existence of an intrinsic outage probability floor and a ceiling on the probability of non-zero achievable secrecy rate. The asymptotic limits are exclusively determined by the backhaul reliability independent of transmitter cooperation and multipath diversity gain.
- Based on the link-level simulations, it is found that the convergence time to approach the asymptotic limits are determined by the number of transmitters and the multipath diversity gain of the main channel. Notably, the existence of any unreliable backhaul connection will result in a loss of diversity gain.

The main challenge of this work is to derive accurate closed-form expressions for the CDF and PDF of the received SNRs of a cooperative CP-SC system with multiple eavesdroppers. To do so, we apply properties of the right circulant channel matrix to note that the received SNRs are distributed according to the chi-squared distribution with different degrees of freedom (DoF) determined by the number of multipaths in the channels. Our closed-form expressions clearly identify separable contributions of the unreliable wireless backhaul and the cooperative CP-SC which allows us to accurately analyze the asymptotic secrecy performance for identical and non-identical backhaul reliability.

[1]The term *backhaul reliability* can be used to model operating conditions that cause a radio link failure [7], [11], [34] due to network congestion, delay, and radio synchronization lost due to bad radio condition. In [35], the backhaul link failure probability (LFP) is defined in terms of the outage probability of the backhaul link.

Notation: $\mathcal{CN}\left(\mu, \sigma^2\right)$ denotes the complex Gaussian distribution with the mean μ and the variance σ^2; $F_{\varphi}(\cdot)$ and $f_{\varphi}(\cdot)$ respectively denote the cumulative distribution function (CDF) and the probability density function (PDF) of the random variable (RV) φ. A length of a vector $\boldsymbol{a}$ is denoted by $\mathbb{L}(\boldsymbol{a})$.

Organization: The rest of the paper is organized as follows. In Section II, we first detail the system and channel model of the proposed system. The e-SNR and its distributions are derived in Section III. Performance analysis of the considered a finite-sized cooperative system is presented in Section IV. Simulation results are presented in Section V and conclusions are drawn in Section VI.

II. System and Channel Model

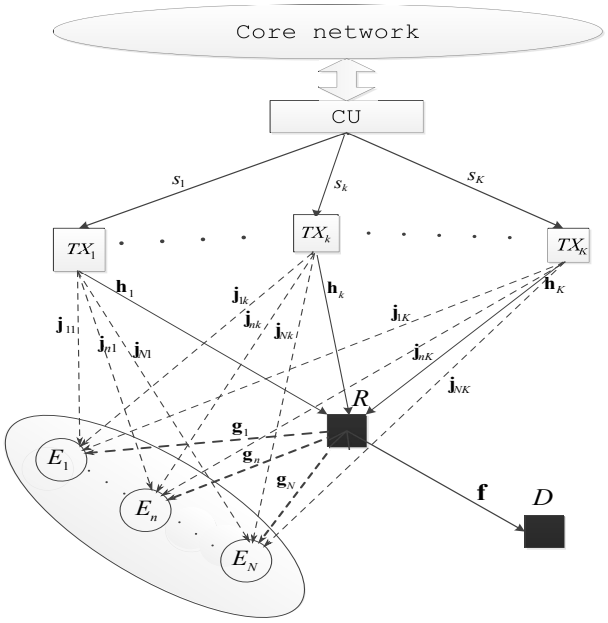

Fig. 1. Block diagram of a finite-sized cooperative CP-SC system with multiple eavesdroppers and multiple transmitters connected to the CU via unreliable wireless backhauls. Reliability of the kth backhaul is denoted by s_k. The set of N eavesdropping channels and main relaying channels are denoted by $\{\boldsymbol{j}_{nk}, \boldsymbol{g}_n, \forall n, k\}$ and $\{\boldsymbol{f}, \boldsymbol{h}_k, \forall k\}$, respectively.

Fig. 1 shows the block diagram of the considered system consisting of a control unit (CU) providing unreliable wireless backhaul to K transmitters $(TX_1, \ldots, TX_K)$ communicating with a destination D via an intermediate relay R in the presence of N eavesdroppers $(E_1, \ldots, E_N)$. A motivating example for such a system model is in future dense heterogeneous networks where the transmitters are small cell base stations providing wireless coverage to an indoor destination user via an intermediate outdoor relay station. The eavesdroppers are nearby receivers attempting to access information sent to the destination by listening to transmissions from the transmitters and the relay. All the transmitters, eavesdroppers, relay node,

and destination node are assumed to be equipped with a single antenna. Similar to [28], we adopt transmit antenna selection (TAS) across the K transmitters such that the transmitter with the highest received SNR at the relay is selected to transmit. Due to the stochastic nature of the channels, the best transmit antenna for the relay is equivalent to a random transmit antenna for the eavesdroppers. By increasing the diversity gain of the main relaying channel with TAS, the secrecy outage probability can be effectively reduced. To minimize the signalling overhead, we consider selection combining (SC) across the N eavesdroppers to select the maximum received SNR across all the received signals from the transmitters and the relay node. In this secrecy system, we employ the following channel models.

- The CSI requirements are detailed as follows: The relay needs CSI of the transmitters-to-relay links, the destination needs CSI of the relay-to-destination link, and the eavesdroppers need CSI of both the transmitters-to-eavesdroppers and the relay-to-eavesdroppers links [27], [30], [31], [33].
- Channel gains are independent and identically distributed (i.i.d.) complex Gaussian random variables with zero means and unit variances.
- A channel from the kth transmitter to the relay node is denoted by $\boldsymbol{h}_k$ with $\mathbb{L}(\boldsymbol{h}_k) = L_{h,k}$. A path loss component over this channel is denoted by $\alpha_{h,k}$.
- A channel from the relay node to the destination is denoted by $\boldsymbol{f}$ with $\mathbb{L}(\boldsymbol{f}) = L_f$. A path loss component over this channel is denoted by α_f.
- A channel from the kth transmitter to the nth eavesdroppers is denoted by $\boldsymbol{j}_{nk}$ with $\mathbb{L}(\boldsymbol{j}_{nk}) = L_{j,n,k}$ and $\alpha_{j,n,k}$ for a path loss component over this channel.
- A channel from the relay node to the nth eavesdroppers is denoted by $\boldsymbol{g}_n$ with $\mathbb{L}(\boldsymbol{g}_n) = L_{g,n}$ and $\alpha_{g,n}$ for a path loss component over this channel.
- The maximum number of multipaths in the system is defined by $L_{\max} = \max\{\{L_{h,k}, \forall k\}, L_f, \{L_{j,n,k}, \forall k, n\}, \{L_{g,n}, \forall n\}\}$.
- Perfect synchronization is assumed between the CU and all the transmitters.
- Backhaul reliability for transmitter TX_k is given by s_k, which is the probability that the transmitter successfully decodes the source message sent over its dedicated backhaul, whereas it is erased with probability $1 - s_k$ due to unreliable backhaul. These erasures are assumed to be independent across messages and follow a Bernoulli process $\mathrm{Bernoulli}(1-s_k)$ [34], with $\mathbb{I}_k$ being an indicator function to model reliability of the kth backhaul link such that $Pr(\mathbb{I}_k = 1) = s_k$ and $Pr(\mathbb{I}_k = 0) = 1 - s_k$.

For cooperative CP-SC transmission, we also use the following schemes:

- M-ary phase-shift keying (MPSK) modulation is applied at the transmitters. The transmission symbol block $\boldsymbol{x} \in \mathbb{C}^{B\times 1}$ is transmitted from the transmitters simultaneously due to exact synchronization between them. The size of the symbol block is denoted by B. We assume that $E[\boldsymbol{x}] = \boldsymbol{0}$ and $E[\|\boldsymbol{x}\|^2] = \boldsymbol{I}_B$.
- A two-hop decode-and-forward (DF) relaying protocol [33], [36], [37] is employed at the relay node. All eavesdroppers can infer transmissions from the transmitters and the relay node in the first and second hops, respectively.
- Coexisting N eavesdroppers also employ CP-SC transmission.
- To prevent inter-block symbol interference (IBSI), an additional CP comprising of P_g symbols from $\boldsymbol{x}$ is appended to the front of $\boldsymbol{x}$ with $P_g \geq L_{\max}$.

After the removal of the CP-related signal, the received signal at the relay node is given by

$$\boldsymbol{y}^{\mathrm{R}} = \sqrt{\bar{P}\alpha_{h,k^*}}\boldsymbol{H}^*\mathbb{I}_{k^*}\boldsymbol{x} + \boldsymbol{z}^{\mathrm{R}} \tag{1}$$

where

$$k^* = \arg\max_{1\leq k\leq K} ||\boldsymbol{h}_k|| \tag{2}$$

is the index of the selected transmitter, $\bar{P}$ denotes the maximum transmission power at the transmitters, and $\boldsymbol{z}^{\mathrm{R}} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$ is the additive noise vector. Due to CP-SC transmission, $\boldsymbol{H}^*$ is represented by the right circulant matrix [24], [38]; that is, $\boldsymbol{H}^*$ is specified by the corresponding channel vector $\boldsymbol{h}_{k^*}$ with additional zeros to have the same size as $\boldsymbol{x}$ [24]. Assuming perfect decoding at the relay node [33], [36], the received signal at the destination is given by

$$\boldsymbol{y}^{\mathrm{D}} = \sqrt{P_R\alpha_f}\boldsymbol{F}\boldsymbol{x} + \boldsymbol{z}^{\mathrm{D}} \tag{3}$$

where $\boldsymbol{F}$ is a right circulant matrix determined by the channel vector $\boldsymbol{f}$ with additional zeros, and $\boldsymbol{z}^{\mathrm{D}} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$. The transmission power at the relay node is denoted by P_R.

In the eavesdroppers' channel, the signal received from the selected k^* transmitter to the nth eavesdropper is given by

$$\boldsymbol{y}^{\mathrm{E},n,1} = \sqrt{\bar{P}\alpha_{j,n,k^*}}\mathbb{I}_{k^*}\boldsymbol{J}_{nk^*}\boldsymbol{x} + \boldsymbol{z}^{\mathrm{E},n,1} \tag{4}$$

where $\boldsymbol{J}_{nk^*}$ is a right circulant matrix determined by $\boldsymbol{j}_{nk^*}$ with additional zeros, and $\boldsymbol{z}^{\mathrm{E},n,1} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$. The signal received from the relay node to the nth eavesdropper, in the second time slot is given by

$$\boldsymbol{y}^{\mathrm{E},n,2} = \sqrt{P_R\alpha_{g,n}}\boldsymbol{G}_n\boldsymbol{x} + \boldsymbol{z}^{\mathrm{E},n,2} \tag{5}$$

where $\boldsymbol{G}_n$ is a right circulant matrix determined by $\boldsymbol{g}_n$ with additional zeros, and $\boldsymbol{z}^{\mathrm{E},n,2} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$. Note that in the representation of Eqs. (3), (4), and (5), the CP-related signal parts are removed.

III. Derivation of the e-SNR

According to Eqs. (1)-(3), and using the properties of the right circulant matrix [24], the normalized SNRs in the main relaying channels are defined as follows:

$$\lambda^{\mathrm{R}} \triangleq \max_{k=1,\ldots,K}\Big(\frac{\bar{P}\alpha_{h,k}\mathbb{I}_k\|\boldsymbol{h}_k\|^2}{\sigma_n^2}\Big) \stackrel{\triangle}{=} \bar{P}\tilde{\alpha}_{h,k^*}\mathbb{I}_{k^*}\|\boldsymbol{h}_{k^*}\|^2 \text{ and}$$
$$\lambda^{\mathrm{D}} \triangleq \frac{P_R\alpha_f\|\boldsymbol{f}\|^2}{\sigma_n^2} \stackrel{\triangle}{=} P_R\tilde{\alpha}_f\|\boldsymbol{f}\|^2 \tag{6}$$

where $\tilde{\alpha}_{h,k} \stackrel{\triangle}{=} \alpha_{h,k}/\sigma_n^2$ and $\tilde{\alpha}_f \stackrel{\triangle}{=} \alpha_f/\sigma_n^2$. For the DF relaying protocol, the e-SNR of the system is given by [36]

$$\lambda^{\mathrm{DF}} = \min(\lambda^{\mathrm{R}}, \lambda^{\mathrm{D}}). \tag{7}$$

Similarly from (4)-(5), the normalized SNRs for a particular eavesdropping channel is given by

$$\lambda^{\mathrm{E},n,1} \triangleq \frac{\bar{P}\alpha_{j,n,k^*}\mathbb{I}_{k^*}\|\boldsymbol{j}_{nk^*}\|^2}{\sigma_n^2} \triangleq \bar{P}\tilde{\alpha}_{j,n,k^*}\mathbb{I}_{k^*}\|\boldsymbol{j}_{nk^*}\|^2 \text{ and}$$
$$\lambda^{\mathrm{E},n,2} \triangleq \frac{P_R\alpha_{g,n}\|\boldsymbol{g}_n\|^2}{\sigma_n^2} \triangleq P_R\tilde{\alpha}_{g,n}\|\boldsymbol{g}_n\|^2 \quad (8)$$

where $\tilde{\alpha}_{j,n,k^*} \triangleq \alpha_{j,n,k^*}/\sigma_n^2$ and $\tilde{\alpha}_{g,n} \triangleq \alpha_{g,n}/\sigma_n^2$. Applying the SC protocol, the achievable SNR out of a cluster of eavesdropping channels is given by

$$\lambda^{\mathrm{E,max}} \triangleq \max_{n=1\ldots N}(\lambda^{\mathrm{E},n,1}, \lambda^{\mathrm{E},n,2}). \quad (9)$$

A. Statistical Properties of the SNRs of the System

Using the properties of the right circulant channel matrix, we can see that λ^{D} and $\lambda^{\mathrm{E},n,2}$ are distributed according to the chi-squared distribution with different DoF [24] mainly determined by the number of multipaths. Since different fading and pathloss between two nodes are more realistic in the wireless system, non-identical frequency selective channels are accounted in the following formulation. We denote the distributions of λ^{D} and $\lambda^{\mathrm{E},n,2}$, respectively, as follows:

$$\lambda^{\mathrm{D}} \sim \chi^2(2L_f, P_R\tilde{\alpha}_f) \text{ and } \lambda^{\mathrm{E},n,2} \sim \chi^2(2L_{g,n}, P_R\tilde{\alpha}_{g,n}) \quad (10)$$

where the DoFs are denoted by $2L_f$ and $2L_{g,n}$, respectively. Their corresponding power normalizing constants are denoted by $P_R\tilde{\alpha}_f$ and $P_R\tilde{\alpha}_{g,n}$.

The CDF and PDF of the random variable $\lambda \sim \chi^2(2L_a, C_a)$ are, respectively, given by

$$f_\lambda(x) = \frac{1}{\Gamma(L_a)(C_a)^{L_a}}x^{L_a-1}e^{-x/Ca} \text{ and}$$
$$F_\lambda(x) = 1 - e^{-x/C_a}\sum_{l=0}^{L_a-1}\frac{1}{l!}\Big(\frac{x}{C_a}\Big)^l. \quad (11)$$

According to the theory of order statistics, the random variable λ^{R} is the largest of K products of Bernoulli random variables and chi-squared random variables. We provide the following proposition for the CDF and PDF of the SNR λ^{R}.

Proposition 1: The CDF of the SNR λ^{R} is given by

$$F_{\lambda^{\mathrm{R}}}(x) = 1 + \sum_{k=1}^{K}(-1)^k\Upsilon\prod_{t=1}^{k}\Big(\frac{s_{q_t}}{\ell_t!(\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}}\Big)e^{-\beta x}x^{\bar{l}} \quad (12)$$

where we define $\beta \triangleq \sum_{t=1}^{k}\frac{1}{\bar{P}\tilde{\alpha}_{h,q_t}}$, $\bar{l} \triangleq \sum_{t=1}^{k}\ell_t$, and

$$\Upsilon \triangleq \sum_{q_1=1}^{K-k+1}\cdots\sum_{q_k=q_{k-1}+1}^{K}\sum_{\ell_1=0}^{L_{h,q_1}-1}\cdots\sum_{\ell_k=0}^{L_{h,q_k}-1}. \quad (13)$$

Proof: See Appendix A. ∎

Note that this proposition is of particular interest since it is applicable to a wide range of scenarios with non-identical frequency selective fading channels, non-identical backhaul reliability, and any degrees of transmitter cooperation.

Based on Proposition 1, the distribution of the e-SNR of the main relaying channel is derived in the following theorem.

Theorem 1: For non-identical frequency selective fading, the distribution of the e-SNR of the main relaying channel in the considered finite-sized cooperative CP-SC system connected via unreliable backhauls is given by (14) at the top of the next page.

Proof: See Appendix B. ∎

Note that the derived closed-form expression is different from related results in [39] and [40] due to the fact that we have taken into account transmitter cooperation connected to the CU via dedicated backhauls with non-identical backhaul reliability and fairly general channel fading conditions in the distribution of the main relaying channel.

Proposition 2: The CDF and PDF of the received SNR by the eavesdropping channel with non-identical frequency fading is derived as

$$F_{\lambda^{\mathrm{E,max}}}(x) = 1 + \Phi e^{-\tilde{\beta}x}x^{\tilde{l}} \text{ and}$$
$$f_{\lambda^{\mathrm{E,max}}}(x) = \Phi\Big[\tilde{l}x^{\tilde{l}-1}e^{-\tilde{\beta}x} - \tilde{\beta}x^{\tilde{l}}e^{-\tilde{\beta}x}\Big] \quad (15)$$

where we define $\tilde{\beta} \triangleq \sum_{t=1}^{n}\frac{1}{\tilde{P}_{q_t}}$, $\tilde{l} \triangleq \sum_{t=1}^{n}r_t$, and

$$\Phi \triangleq \sum_{n=1}^{2N}(-1)^n\sum_{q_1=1}^{2N-n+1}\cdots\sum_{q_n=q_{n-1}+1}^{2N}\sum_{r_1=0}^{L_{3,q_1}-1}\cdots\sum_{r_n=0}^{L_{3,q_n}-1}\prod_{t=1}^{n}\Big(\frac{\tilde{s}_{q_t}}{r_t!(\tilde{P}_{q_t})^{r_t}}\Big) \quad (16)$$

with

$$\tilde{s}_n = \begin{cases} s_{k^*} & \text{for } n = 1,\ldots,N \\ 1 & \text{for } n = N+1,\ldots,2N \end{cases}, \quad (17)$$

$$\tilde{P}_n = \begin{cases} \bar{P}\tilde{\alpha}_{j,n,k^*} & \text{for } n = 1,\ldots,N \\ P_R\tilde{\alpha}_{g,n} & \text{for } n = N+1,\ldots,2N \end{cases}, \quad (18)$$

and

$$L_{3,n} = \begin{cases} L_{j,n,k^*} & \text{for } n = 1,\ldots,N \\ L_{g,n} & \text{for } n = N+1,\ldots,2N \end{cases}. \quad (19)$$

Proof: See Appendix C. ∎

IV. Performance Analysis

In this section, based on the above closed-form statistical expressions, we compute the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy capacity in non-identical frequency selective fading. Note that since k^* obtained by the transmitter selection protocol described by Eq. (2) is random over a particular set of transmitters, the evaluation of the performance metrics is only feasible by considering identical backhaul reliability and identical fading channels for the K transmitter links but non-identical frequency selective fading channels for the relay-to-destination and relay-to-eavesdropper links. This assumption is generalized to non-identical backhaul reliability and non-identical frequency selective fading channels across all the links when we analyze the asymptotic limits of the secrecy performance in the high SNR region.

$$
\begin{aligned}
F_{\lambda^{\mathrm{DF}}}(x) &= 1-(1-F_{\lambda^{\mathrm{R}}}(x))(1-F_{\lambda^{\mathrm{D}}}(x)) \\
&= 1-\sum_{k=1}^{K}\Upsilon(-1)^{k+1}\prod_{t=1}^{k}\left(\frac{s_{q_t}}{\ell_t!(\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}}\right)\sum_{l=0}^{L_f-1}\frac{1}{l!(P_R\tilde{\alpha}_f)^l}e^{-x\left(\beta+\frac{1}{P_R\tilde{\alpha}_f}\right)}x^{\bar{l}+l} \\
&= 1-\tilde{F}_{\lambda^{\mathrm{DF}}}(x). \qquad (14)
\end{aligned}
$$

A. Identical Backhaul Reliability

From Eqs. (14) and (15), we present the following secrecy performance analysis for cooperative CP-SC with identical backhaul reliability.

1) Secrecy Outage Probability: The secrecy outage occurs when a cluster of eavesdroppers can infer data transmission, so that perfect secrecy is compromised [29]. At a given secure rate R, the secrecy outage probability is given by [29]

$$
\begin{aligned}
P_{out} &= Pr(C_s < R) \\
&= \int_0^{\infty} F_{\lambda^{\mathrm{DF}}}(2^{2R}(1+x)-1)f_{\lambda^{\mathrm{E,max}}}(x)dx \qquad (20)
\end{aligned}
$$

where an instantaneous secrecy rate is denoted by C_s. The instantaneous capacity of the main relaying channel is given by $\log_2(1+\lambda^{\mathrm{DF}})$, whereas an instantaneous capacity of the channels between the relay node and a cluster of eavesdroppers is given by $\log_2(1+\lambda^{\mathrm{E,max}})$. According to these two instantaneous capacities, the instantaneous secrecy rate is defined as [27]–[30]

$$
C_s = \frac{1}{2}\Big[\log_2(1+\lambda^{\mathrm{DF}}) - \log_2(1+\lambda^{\mathrm{E,max}})\Big]^{+} \qquad (21)
$$

where $[x]^{+}$ denotes $\max\{0,x\}$. Now using (14) and (15), a closed-form expression for (20) is provided in the following theorem.

Theorem 2: The secrecy outage probability of a finite-sized cooperative CP-SC system with an identical backhaul reliability but non-identical frequency selective fading is given by (22) at the top the next page. In (22), we define $J_R \triangleq 2^{2R}$.

Proof: With the help of (14) and (15), (22) can be readily derived. ∎

Note that this theorem provides an analytical framework to aid the outage probability evaluation/design of a finite-sized cooperative CP-SC system in terms of key design parameters such as transmitter cooperation, number of eavesdroppers, frequency selectivity, and backhaul reliability.

2) The Probability of Non-Zero Achievable Secrecy Rate: The probability of non-zero achievable secrecy rate is given by [27], [30]

$$
Pr(C_s>0) = \int_0^{\infty}\tilde{F}_{\lambda^{\mathrm{DF}}}(x)f_{\lambda^{\mathrm{E,max}}}(x)dx \qquad (23)
$$

which is evaluated as (24) at the top of the next page. Note that $\tilde{F}_{\lambda^{\mathrm{DF}}}(x)$ in (23) is easily extracted from (14).

3) Ergodic Secrecy Rate: The ergodic secrecy rate is given by [27]

$$
\bar{C}_s = \frac{1}{2\log(2)}\int_0^{\infty}\frac{F_{\lambda^{\mathrm{E,max}}}(x)}{1+x}(\tilde{F}_{\lambda^{\mathrm{DF}}}(x))dx. \qquad (25)
$$

Note that (25) can be obtained by averaging an instantaneous secrecy capacity over SNRs λ^{DF} and $\lambda^{\mathrm{E,max}}$. Upon applying the expressions for $F_{\lambda^{\mathrm{E,max}}}(x)$ and $\tilde{F}_{\lambda^{\mathrm{DF}}}(x)$ into (25), we can derive the corresponding closed-form expression in the following theorem.

Theorem 3: The ergodic secrecy rate of a finite-sized cooperative CP-SC system connected to the CU via unreliable backhauls and non-identical frequency selective fading channels at the relay and eavesdroppers is given by (26) at the middle of the next page. In (26), $\Psi(a,b;z) = \frac{1}{\Gamma(a)}\int_0^{\infty}e^{-zt}t^{a-1}(1+t)^{b-a-1}dt$ denotes the confluent hypergeometric function [41, eq. (9.211/4)].

Proof: Since a proof of this theorem can be readily derived via [30], a detailed proof is not provided. ∎

To obtain further insights, we derive asymptotic secrecy outage probability, probability of non-zero achievable secrecy rate, and secrecy ergodic rate when the backhauls are completely perfect in their connections.

4) Asymptotic Performance of the System with Completely Perfect Backhauls: Asymptotic secrecy outage probability, probability of non-zero achievable secrecy rate, and secrecy ergodic rate with completely perfect backhauls are given by the following theorem.

Theorem 4: For non-identical frequency selective fading channels and completely perfect backhaul connections, asymptotic secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate are given by (27), (28), and (29), respectively. In (27), (28), and (29), we define

$$
\tilde{\beta} \triangleq \sum_{t=1}^{n}\frac{1}{\tilde{P}_{q_t}}, \tilde{l} \triangleq \sum_{t=1}^{n} r_t,
$$

and

$$
\begin{aligned}
\Xi \triangleq & \sum_{n=1}^{2N}(-1)^n \sum_{q_1=1}^{2N-n+1}\cdots\sum_{q_n=q_{n-1}+1}^{2N}\sum_{r_1=0}^{L_{3,q_1}-1}\cdots\sum_{r_n=0}^{L_{3,q_n}-1} \\
& \prod_{t=1}^{n}\Big(\frac{1}{r_t!(\tilde{P}_{q_t})^{r_t}}\Big). \qquad (30)
\end{aligned}
$$

Proof: See Appendix D. ∎

From this theorem, the secrecy diversity gain can be seen as:

$$
G_d = \min\Big(\sum_{k=1}^{K}L_{h,k}, L_f\Big). \qquad (31)
$$

Thus, only the multipath diversity gain can be achievable by the employed SC protocol; that is, transmitter cooperation has no effect on the diversity gain. In addition, this multipath gain

$$P_{out} = 1 - \sum_{k=1}^{K} \Upsilon(-1)^{k+1} \prod_{t=1}^{k} \left(\frac{s_{q_t}}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \sum_{l=0}^{L_f-1} \frac{1}{l!(P_R\tilde{\alpha}_f)^l} \sum_{v=0}^{\bar{l}+l} \binom{\bar{l}+l}{v} (J_R-1)^{\bar{l}+l-v} J_R^v e^{-(J_R-1)\left(\beta + \frac{1}{P_R\tilde{\alpha}_f}\right)}$$
$$\Phi\Big[\tilde{l}\Gamma(v+\tilde{l}) \left(\tilde{\beta} + J_R\beta + \frac{J_R}{P_R\tilde{\alpha}_f} \right)^{-v-\tilde{l}} - \tilde{\beta}\Gamma(v+\tilde{l}+1) \left(\tilde{\beta} + J_R\beta + \frac{J_R}{P_R\tilde{\alpha}_f} \right)^{-v-\tilde{l}-1} \Big]. \tag{22}$$

$$Pr(C_s > 0) = \sum_{k=1}^{K} \Upsilon(-1)^{k+1} \prod_{t=1}^{k} \left(\frac{s_{q_t}}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \sum_{l=0}^{L_f-1} \frac{1}{l!(P_R\tilde{\alpha}_f)^l}$$
$$\Phi\Big[\tilde{l}\Gamma(\bar{l}+l+\tilde{l}) \left(\tilde{\beta} + \beta + \frac{1}{P_R\tilde{\alpha}_f} \right)^{-\bar{l}-l-\tilde{l}} - \tilde{\beta}\Gamma(\bar{l}+l+\tilde{l}+1) \left(\tilde{\beta} + \beta + \frac{1}{P_R\tilde{\alpha}_f} \right)^{-\bar{l}-l-\tilde{l}-1} \Big]. \tag{24}$$

$$\bar{C}_s = \frac{1}{2\log(2)} \sum_{k=1}^{K} \Upsilon(-1)^{k+1} \prod_{t=1}^{k} \left(\frac{s_{q_t}}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \sum_{l=0}^{L_f-1} \frac{1}{l!(P_R\tilde{\alpha}_f)^l} \left[\Gamma(\bar{l}+l+1)\Psi\left(\bar{l}+l+1, \bar{l}+l+1; \beta + \frac{1}{P_R\tilde{\alpha}_f} \right) \right.$$
$$\left. -\Phi\Gamma(\bar{l}+l+\tilde{l}+1)\Psi\left(\bar{l}+l+\tilde{l}+1, \bar{l}+l+\tilde{l}+1; \tilde{\beta}+\beta + \frac{1}{P_R\tilde{\alpha}_f} \right) \right]. \tag{26}$$

$$P_{\text{out}}^{\text{as}} = \begin{cases} \frac{\Xi \sum_{u=0}^{\tilde{L}_{h,k}} \binom{\tilde{L}_{h,k}}{u} (J_R-1)^{\tilde{L}_{h,k}-u} J_R^u}{(\bar{P}\tilde{\alpha}_{h,k})^{\tilde{L}_{h,k}} \prod_{k=1}^{K} (L_{h,k})!} \left(\frac{\tilde{l}\Gamma(u+\tilde{l})}{\tilde{\beta}^{u+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(u+\tilde{l}+1)}{\tilde{\beta}^{u+\tilde{l}+1}} \right) & \text{when } L_f > \tilde{L}_{h,k}, \\ \frac{\Xi \sum_{v=0}^{L_f} \binom{L_f}{v} (J_R-1)^{L_f-v} J_R^v}{(P_R\tilde{\alpha}_f)^{L_f} (L_f)!} \left(\frac{\tilde{l}\Gamma(v+\tilde{l})}{\tilde{\beta}^{v+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(v+\tilde{l}+1)}{\tilde{\beta}^{v+\tilde{l}+1}} \right) & \text{when } L_f < \tilde{L}_{h,k}, \\ \frac{\Xi \sum_{u=0}^{\tilde{L}_{h,k}} \binom{\tilde{L}_{h,k}}{u} (J_R-1)^{\tilde{L}_{h,k}-u} J_R^u}{(\bar{P}\tilde{\alpha}_{h,k})^{\tilde{L}_{h,k}} \prod_{k=1}^{K} (L_{h,k})!} \left(\frac{\tilde{l}\Gamma(u+\tilde{l})}{\tilde{\beta}^{u+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(u+\tilde{l}+1)}{\tilde{\beta}^{u+\tilde{l}+1}} \right) & \\ + \frac{\Xi \sum_{v=0}^{L_f} \binom{L_f}{v} (J_R-1)^{L_f-v} J_R^v}{(P_R\tilde{\alpha}_f)^{L_f} (L_f)!} \left(\frac{\tilde{l}\Gamma(v+\tilde{l})}{\tilde{\beta}^{v+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(v+\tilde{l}+1)}{\tilde{\beta}^{v+\tilde{l}+1}} \right) & \text{when } L_f = \tilde{L}_{h,k}. \end{cases} \tag{27}$$

$$Pr^{\text{as}}(C_s > 0) = \begin{cases} 1 - \frac{\Xi}{(\bar{P}\tilde{\alpha}_{h,k})^{\tilde{L}_{h,k}} \prod_{k=1}^{K} (L_{h,k})!} \left(\frac{\tilde{l}\Gamma(\tilde{L}_{h,k}+\tilde{l})}{\tilde{\beta}^{\tilde{L}_{h,k}+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(\tilde{L}_{h,k}+\tilde{l}+1)}{\tilde{\beta}^{\tilde{L}_{h,k}+\tilde{l}+1}} \right) & \text{when } L_f > \tilde{L}_{h,k}, \\ 1 - \frac{\Xi}{(P_R\tilde{\alpha}_f)^{L_f} (L_f)!} \left(\frac{\tilde{l}\Gamma(L_f+\tilde{l})}{\tilde{\beta}^{L_f+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(L_f+\tilde{l}+1)}{\tilde{\beta}^{L_f+\tilde{l}+1}} \right) & \text{when } L_f < \tilde{L}_{h,k}, \\ 1 - \frac{\Xi}{(\bar{P}\tilde{\alpha}_{h,k})^{\tilde{L}_{h,k}} \prod_{k=1}^{K} (L_{h,k})!} \left(\frac{\tilde{l}\Gamma(\tilde{L}_{h,k}+\tilde{l})}{\tilde{\beta}^{\tilde{L}_{h,k}+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(\tilde{L}_{h,k}+\tilde{l}+1)}{\tilde{\beta}^{\tilde{L}_{h,k}+\tilde{l}+1}} \right) & \\ \quad - \frac{\Xi}{(P_R\tilde{\alpha}_f)^{L_f} (L_f)!} \left(\frac{\tilde{l}\Gamma(L_f+\tilde{l})}{\tilde{\beta}^{L_f+\tilde{l}}} - \frac{\tilde{\beta}\Gamma(L_f+\tilde{l}+1)}{\tilde{\beta}^{L_f+\tilde{l}+1}} \right) & \text{when } L_f = \tilde{L}_{h,k}. \end{cases} \tag{28}$$

$$\bar{C}_s^{as} = \frac{1}{2\log(2)} \sum_{k=1}^{K} \Upsilon(-1)^{k} \prod_{t=1}^{k} \left(\frac{1}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \sum_{l=0}^{L_f-1} \frac{1}{l!(P_R\tilde{\alpha}_f)^l} \left(\beta + \frac{1}{P_R\tilde{\alpha}_f} \right)^{-(\bar{l}+l)} \Gamma(\bar{l}+l+1)$$
$$[\psi(\bar{l}+l) - \psi(\bar{l}+l+1)] + \frac{1}{2\log(2)} \Xi\Gamma(\tilde{l}+1)\Psi(\tilde{l}+1, \tilde{l}+1; \tilde{\beta}). \tag{29}$$

also affects the convergence speed of the non-zero achievable secrecy rate to $Pr(C_s > 0) = 1$ [30]. In the following, we relax the identical backhaul reliability condition in the asymptotic performance analysis to investigate an exclusive effect of backhaul reliability on the secrecy performance.

B. Asymptotic Secrecy Performance Analysis for Non-identical Backhaul Reliability and Frequency Selective Fading Channel

At a fixed received SNR of the eavesdropping channels, the existence of limits on the secrecy outage probability and probability of non-zero achievable secrecy rate is inevitable with unreliable backhauls, which is given by the following theorem.

Theorem 5: For frequency selective fading channels and at a fixed received SNR of the eavesdropping links, an asymptotic secrecy outage probability limit and an asymptotic limit on the probability of non-zero achievable secrecy rate are, respectively, given by

$$P_{\text{out}}^{\text{as},L} = \prod_{k=1}^{K}(1 - s_k) \text{ and} \tag{32}$$

$$Pr^{\text{as},L}(C_s > 0) = 1 - \prod_{k=1}^{K}(1 - s_k). \tag{33}$$

In addition, the asymptotic ergodic secrecy rate is given by (34) at the top of the next page.

Proof: See Appendix E. ∎

Note that from this theorem we can see that only a set of backhaul reliability levels, $\{s_k\}$, exclusively determines asymptotic limits on the secrecy outage probability and probability of non-zero achievable secrecy rate. As a special case, for an identical backhaul reliability s, asymptotic performance limits are given by $P_{\text{out}}^{\text{as},L} = (1-s)^K$ and $Pr^{\text{as},L}(C_s > 0) = 1-(1-s)^K$. As $s_k \to 1, \forall k$, we can see $P_{\text{out}}^{\text{as},L} \to 0$ and $Pr^{\text{as},L}(C_s > 0) \to 1$, which corresponds to the conventional system with transmitter cooperation and completely perfect backhauls in their connections. This theorem shows that a lower secrecy outage occurs as the backhaul reliability increases, and $Pr(C_s > 0) = 1$ is not achievable when the backhaul connections are not completely perfect in transporting data. In contrast with existing results for perfect backhauls in [24] and [30], we see that the asymptotic diversity gain promised by cooperative CP-SC transmission is not attainable in frequency selective fading channels with imperfect backhauls. However, from the link simulations, we find that a faster convergence speed arriving at these limits can be obtained in proportional to the achievable diversity gain by the CP-SC transmission. Note that compared with the secrecy outage probability and probability of non-zero achievable secrecy rate, there is no limit on the asymptotic secrecy ergodic rate in (34) due to the presence of s_{k^*} in Φ as defined in (16).

V. Simulation Results

In the following link simulations, we apply quadrature phase-shift keying (QPSK) modulation to the data symbols. The curves obtained via link-level simulations are denoted by **Ex** whereas analytically derived curves are denoted by **An**. For notational purpose, limits on asymptotic secrecy performance metrics under unreliable backhauls are denoted by $P_{\text{out}}^{\text{as},L}$ and $P_r^{\text{as},L}(C_s > 0)$, whereas analytic secrecy performance metrics under completely perfect backhauls are denoted by P_{out}^{∞}, $P_r^{\infty}(C_s > 0)$, and $\bar{C}_s^{\infty}$. The block size is $B = 64$, $\bar{P} = 1$, and $P_R = \chi_R \bar{P}$ with $0 < \chi_R < 1$. We consider the following scenarios to highlight the impacts of key design parameters of a finite-sized CP-SC system on the secrecy performance.

- S_1: $s_k = 0.99$, $L_{h,k} = \{2,3\}$, $L_f = 2$, $L_{j,n,k} = \{1,2\}$, $L_{g,n} = \{2,3\}$, $\chi_R = 0.1$.
- S_2: $s_k = 0.80$, $L_{h,k} = \{1,3\}$, $L_f = 2$, $L_{j,n,k} = \{1,2\}$, $L_{g,n} = \{2,3\}$, $\chi_R = 0.1$.
- S_3: $s_k = 0.90$, $L_{h,k} = \{1,3,1\}$, $L_{j,n,k} = \{1,2,1\}$, $L_{g,n} = \{2,3,2\}$, $\chi_R = 0.1$.
- S_4: $s_k = 0.90$, $L_{h,k} = \{3,5,3\}$, $\chi_R = 0.1$.
- S_5: $s_k = \{0.9, 0.95, 0.97\}$, $L_{h,k} = \{1,3,3\}$, $L_f = 2$, $L_{j,n,k} = \{1,2,1\}$, $L_{g,n} = \{2,3,2\}$, $\chi_R = 0.1$.
- S_6: $s_k = \{0.8, 0.85, 0.87\}$, $L_{h,k} = \{1,3,3\}$, $L_f = 2$, $L_{j,n,k} = \{1,2,1\}$, $L_{g,n} = \{2,3,2\}$, $\chi_R = 0.1$.
- S_7: $K = 3$, $L_{h,k} = \{1,3,3\}$, $L_{j,n,k} = \{1,2,1\}$, $L_{g,n} = \{2,3,2\}$, $\chi_R = 0.1$.

A. Identical Backhaul Reliability but Non-Identical Frequency Selective Fading Channel

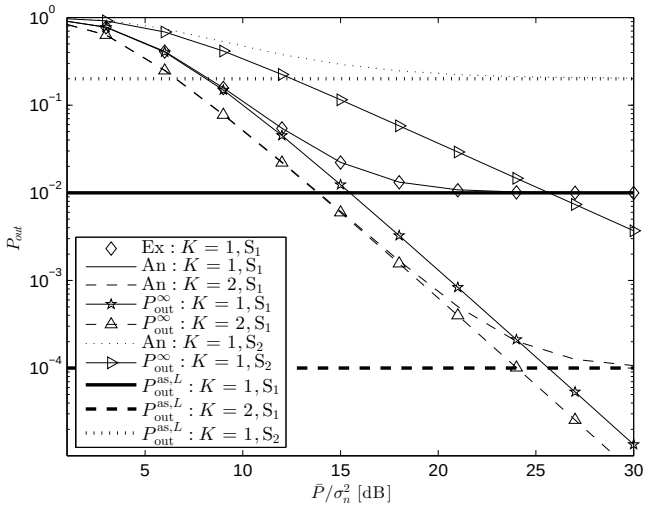

Fig. 2. Secrecy outage probability for various scenarios for $N = 2$ at a fixed value of $P_R \alpha_{g,n}$.

We first verify the accuracy of the analytically derived secrecy outage probability in scenario S_1. We can see good agreement between the analytical curves and the link-level simulations. For scenarios S_1, and S_2, Fig. 2 shows the secrecy outage probability in terms of transmitter cooperation and backhaul reliability. We can see that increasing the transmitter cooperation results in less frequent secrecy outages due to a higher received signal power at the destination. For non-identical frequency selective fading, we can also evaluate the

$$\bar{C}_s^{\mathrm{as},L} = \frac{1}{2\log(2)} \sum_{k=1}^{K} \Upsilon(-1)^k \prod_{t=1}^{k} \left(\frac{s_{q_t}}{\ell_t!(\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \sum_{l=0}^{L_f-1} \frac{1}{l!(P_R\tilde{\alpha}_f)^l} \left(\beta + \frac{1}{P_R\tilde{\alpha}_f} \right)^{-(\bar{l}+l)} \Gamma(\bar{l}+l+1)$$
$$[\psi(\bar{l}+l) - \psi(\bar{l}+l+1)] + \frac{1}{2\log(2)} \left(1 - \prod_{k=1}^{K} (1-s_k) \right) \Phi\Gamma(\tilde{l}+1)\Psi(\tilde{l}+1, \tilde{l}+1; \tilde{\beta}). \quad (34)$$

secrecy outage probability limits as $\tilde{\alpha}_{h,k} \to \infty$ and $\tilde{\alpha}_f \to \infty$. For scenario S_1, they are, respectively, given by $P_{\mathrm{out}}^{\mathrm{as},L} = 0.01$ and $P_{\mathrm{out}}^{\mathrm{as},L} = 0.0001$ for $K = 1$ and $K = 2$, which are exclusively determined by backhaul reliability $s_k = 0.99$ independent of other parameters. For a lower backhaul reliability, $s_k = 0.8$, we observe the existence of a higher limit on the secrecy outage probability, $P_{\mathrm{out}}^{\mathrm{as},L} = 0.2$. We can verify that under completely perfect backhaul connections, the outage diversity gain is $G_d = \min\left(\sum_{k=1}^{K} L_{h,k}, L_f\right)$ by measuring the slope on a $\log - \log$ plot. For example, for scenario S_1, the diversity gain is $G_d = 2$ for $K = 1$ and $K = 2$, since L_f dominates $\min\left(\sum_{k=1}^{K} L_{h,k}, L_f\right)$. Since $\min\left(L_{h,1}, L_f\right) = 1$ for scenario S_2, only $G_d = 1$ can be achieved by the system. Interestingly, we observe that the secrecy outage probability under unreliable backhauls approaches the asymptotic limit with perfect backhaul connections when σ_n^2 is large, whereas the secrecy outage probability approaches the asymptotic limit with imperfect backhaul when σ_n^2 is small. As such, we can classify the operating region into two sub-regions based on the magnitude of σ_n^2. In the imperfect backhaul sub-region, the multipath diversity gain is not achievable, whereas in the perfect backhaul sub-region, the multipath diversity gain is achievable. The boundary between the two sub-regions depends on the multipath diversity gain and backhaul reliability.

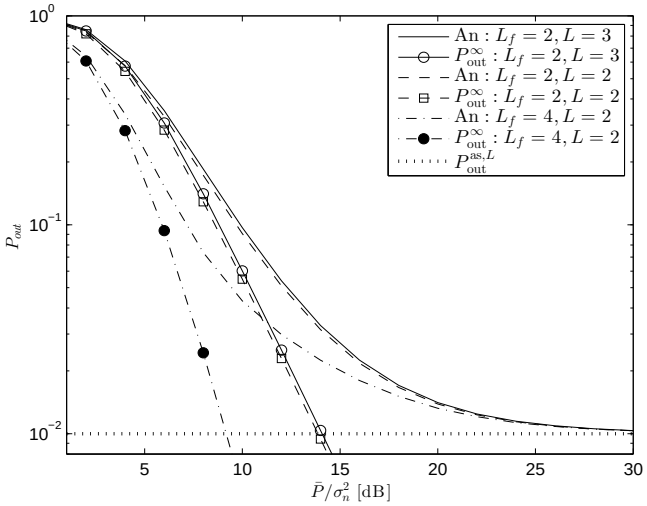

Fig. 3. Secrecy outage probability for various scenarios for $K = 2$ at a fixed value of $P_R\alpha_{g,n}$.

In Fig. 3, for a fixed transmitter cooperation ($K = 2$) and scenario S_3, we investigate the effects of L_f and N on the secrecy outage probability. For the same value of L_f, a larger N results in a higher secrecy outage probability due to more severe eavesdropping. From the asymptotic curves, we note that a different value of N has no effect on the slope of the curves since the diversity gain is independent of N. We can also observe that if we increase L_f, then a lower secrecy outage probability is obtained. However, as σ_n decreases, multipath diversity effect decreases due to detrimental effect from unreliable backhauls.

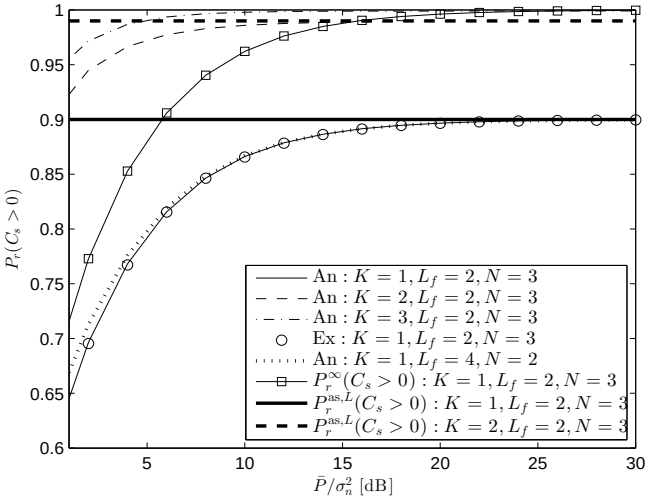

Fig. 4. Probability of non-zero achievable secrecy rate for various scenarios at a fixed value of $P_R\alpha_{g,n}$.

In Fig. 4, we illustrate the probability of non-zero achievable secrecy rate for scenario S_3. We can see the joint effect of the number of eavesdroppers, number of transmitters, frequency selectivity over the channels between the transmitters and the relay, and backhaul reliability. In Fig. 5, we investigate the effects of frequency selectivity on the convergence time of the probability of non-zero achievable secrecy rate at fixed $N = 3$ and $s_k = 0.9$ for scenario S_4. From Figs. 4 and 5, we can observe the following facts:

- The probability of non-zero achievable secrecy rate increases with increasing number of transmitters due to the increased power at the destination.
- The probability of non-zero achievable secrecy rate decreases with increasing number of eavesdroppers. However, as σ_n^2 decreases (or $\tilde{\alpha}_{h,k}$ and $\tilde{\alpha}_{g,n}$ increases), difference between them becomes unnoticeable and independent of the parameters except backhaul reliability and transmitter cooperation.
- If backhauls are not perfect in transporting data, $Pr(C_s >$

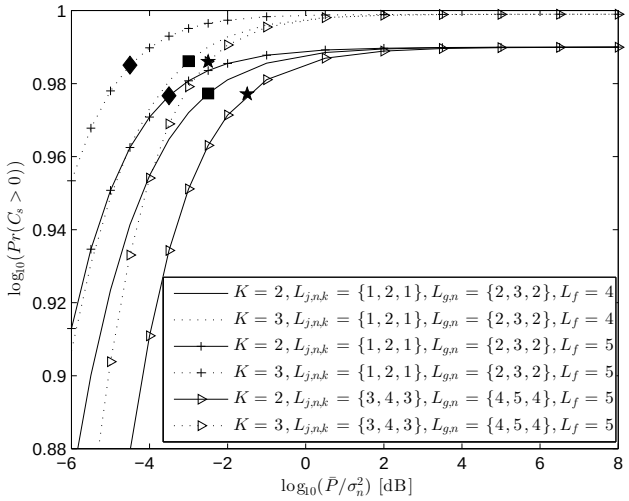

Fig. 5. Convergence time analysis of the probability of non-zero achievable secrecy rate arriving at 99% of asymptotic limits $P_{\text{out}}^{\text{as},L}$ for various scenarios at a fixed $P_R\alpha_{g,n}$. In this figure, ★, ■, and ♦ denote boundary points starting $P_{\text{out}} \geq 0.99 P_{\text{out}}^{\text{as},L}$.

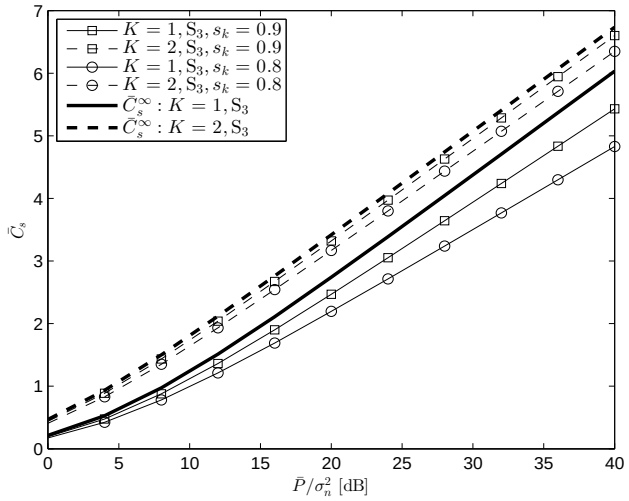

Fig. 6. Ergodic secrecy rate for various scenarios at a fixed $P_R\alpha_{g,n}$.

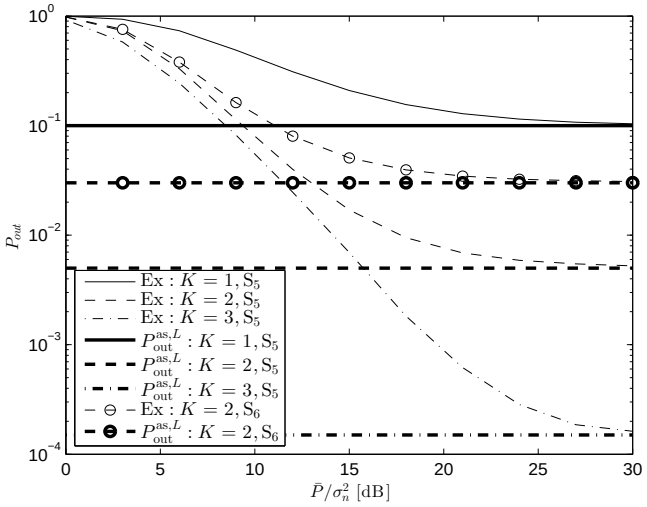

Fig. 7. Secrecy outage probability for various scenarios at fixed $P_R\alpha_g$ and $N=2$ with $L_g=1$.

$0) = 1$ is not achievable. Asymptotically, it approaches the secrecy limit on the probability of non-zero achievable secrecy rate. This limit is mainly determined by backhaul reliability. For instance, for scenarios S_3 and S_4, we have $Pr^{\text{as},L}(C_s > 0) = 1 - (1 - s_k)^K$ for transmitter cooperation K and backhaul reliability s_k.

- As $\min(\sum_{k=1}^{K} L_{h,k}, L_f)$ increases, a faster convergence time is obtained in arriving at the 99% of the asymptotic limit on the non-zero achievable secrecy rate. For example, $\min(\sum_{k=1}^{2} L_{h,k}, L_f = 5)$ has a slower convergence time than $\min(\sum_{k=1}^{2} L_{h,k}, L_f = 4)$. Also, as transmitter cooperation increases, a slower convergence time can be observed. Thus, the conventional diversity gains promised by CP-SC transmission is shown to affect the convergence time for arriving at the performance limits.

In Fig. 6, we first verify the accuracy of the derived ergodic secrecy rate for a particular scenario S_3. In addition, this figure shows the ergodic secrecy rate for various values of backhaul reliability comparing with that of the system having completely perfect backhaul connections. As σ_n^2 decreases, a bigger gap can be observed since backhaul reliability influences the performance. We also observe that the gap between the curves decreases as backhaul reliability increases. That is, a more reliable backhaul results in a higher ergodic secrecy rate.

B. Non-Identical Backhaul Reliability

Fig. 7 shows the empirical secrecy outage probability and its asymptotic limit for non-identical backhaul reliability in scenarios S_5 and S_6. Based on the asymptotic limit of the secrecy outage probability derived in Theorem 5, we see that the empirical secrecy outage probability approaches its limit specified by $P_{\text{out}}^{\text{as},L} = \prod_{k=1}^{K}(1 - s_k)$. We can see that for scenario S_5, $P_{\text{out}}^{\text{as},L}$ is 5×10^{-3} and 1.4×10^{-4}, respectively, for $K = 2$ and $K = 3$.

In Fig. 8, we use the same scenarios as in Fig. 7. It can be readily seen that the derived asymptotic limit on the probability of non-zero achievable secrecy rate is correct and exclusively determined by backhaul reliability. That is, $Pr^{\text{as},L}(C_s > 0) = 1 - \prod_{k=1}^{K}(1 - s_k)^K$.

In Fig. 9, we plot the ergodic secrecy rate with its asymptotic ergodic secrecy rate for scenario S_7 with non-identical backhaul reliability and different values of L_f. We can see that as σ_n^2 decreases, the difference between the ergodic secrecy rate and its asymptotic ergodic secrecy rate becomes negligible. As in Fig. 6, a higher diversity gain, which is mainly determined by the multipath gain, a higher ergodic secrecy rate can be achieved. Moreover, a higher backhaul reliability can result in a higher diversity gain. It is also

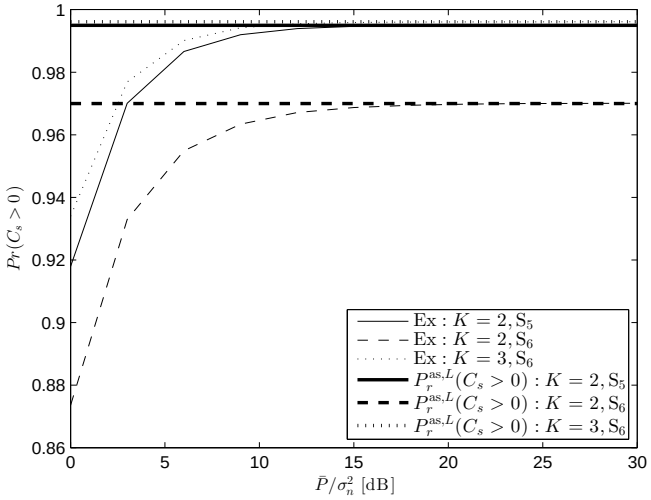

Fig. 8. Probability of non-zero achievable secrecy rate for various scenarios at a fixed $P_R\alpha_g$.

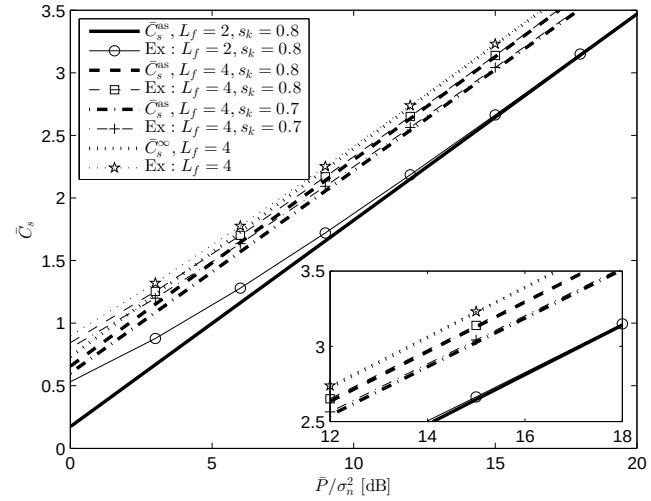

Fig. 9. Ergodic secrecy rate for various scenarios at a fixed $P_R\alpha_g$.

observed that perfect backhaul connections result in a higher ergodic secrecy rate over the system with unreliable backhaul connections.

VI. Conclusions

In this paper, the impact of unreliable backhauls has been examined for finite-sized cooperative single carrier systems coexisting with multiple passive eavesdroppers. Taking into account backhaul reliability, we have derived the distributions of the end-to-end SNR of the main relaying channel under non-identical frequency selective fading channel across the relay and destination nodes in the system. Based on this derivation, we have derived secrecy performance metrics such as the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate. For these derivations, we have first verified their accuracy. We have also derived the corresponding asymtotic performance metrics. Specifically, we have shown that irrespective of the system configuration parameters and frequency selective fading, single carrier systems display a secrecy outage probability limit which is exclusively determined by the backhaul reliability. It has been seen that the conventional promised diversity gain by single carrier system only affects the convergence time arriving at these asymptotic secrecy performance limits.

Appendix A: Derivation of Proposition 1

From the definition of the random variable λ^{R}, we can recall that

$$\lambda^{\mathrm{R}} = \max_{k=1,\ldots,K} \left(\mathbb{I}_k \bar{P}\tilde{\alpha}_{h,k} \|\boldsymbol{h}_k\|^2 \right) \tag{A.1}$$

where $\bar{P}\tilde{\alpha}_{h,k}\|\boldsymbol{h}_k\|^2 \sim \chi^2(2L_{h,k}, \bar{P}\tilde{\alpha}_{h,k})$. In (A.1), one particular random variable $\mathbb{I}_k\bar{P}\tilde{\alpha}_{h,k}\|\boldsymbol{h}_k\|^2$ has the following PDF

$$f_{\mathbb{I}_k\bar{P}\tilde{\alpha}_{h,k}\|\boldsymbol{h}_k\|^2}(x) = (1-s_k)\delta(x) + \frac{s_k}{\Gamma(L_{h,k})(\bar{P}\tilde{\alpha}_{h,k})^{L_{h,k}}} x^{L_{h,k}-1} e^{-x/\bar{P}\tilde{\alpha}_{h,k}} \tag{A.2}$$

where $\delta(\cdot)$ denotes the Dirac delta function and CDF

$$\begin{aligned} F_{\mathbb{I}_k\bar{P}\tilde{\alpha}_{h,k}\|\boldsymbol{h}_k\|^2}(x) &= \int_0^x f_{\mathbb{I}_k\bar{P}\tilde{\alpha}_{h,k}\|\boldsymbol{h}_k\|^2}(y)dy \\ &= 1 - \frac{s_k\Gamma(L_{h,k}, x/\bar{P}\tilde{\alpha}_{h,k})}{\Gamma(L_{h,k})}. \end{aligned} \tag{A.3}$$

With some manipulations, we can have the (CDF) of $\lambda^{\mathrm{R}} = \max_{k=1,\ldots,K}\left(\mathbb{I}_k\bar{P}\tilde{\alpha}_{h,k}\|\boldsymbol{h}_k\|^2\right)$ as follows:

$$\begin{aligned} F_{\lambda^{\mathrm{R}}}(x) &= \prod_{k=1}^{K} F_{\mathbb{I}_k\bar{P}\tilde{\alpha}_{h,k}\|\boldsymbol{h}_k\|^2}(x) \\ &= \prod_{k=1}^{K}\left(1 - \frac{s_k\Gamma(L_{h,k}, x/\bar{P}\tilde{\alpha}_{h,k})}{\Gamma(L_{h,k})}\right) \\ &= 1 + \sum_{k=1}^{K}\sum_{q_1=1}^{K-k+1}\sum_{q_2=q_1+1}^{K-k+2}\cdots\sum_{q_k=q_{k-1}+1}^{K}(-1)^k \\ &\quad \prod_{t=1}^{k}\left(\frac{s_{q_t}\Gamma(L_{h,q_t}, x/\bar{P}\tilde{\alpha}_{h,q_t})}{\Gamma(L_{h,q_t})}\right). \end{aligned} \tag{A.4}$$

Substituting the series expansion of the upper incomplete gamma function [41, eq. 8.352/2] results in

$$\begin{aligned} F_{\lambda^{\mathrm{R}}}(x) &= 1 + \sum_{k=1}^{K}\sum_{q_1=1}^{K-k+1}\sum_{q_2=q_1+1}^{K-k+2}\cdots\sum_{q_k=q_{k-1}+1}^{K}(-1)^k \\ &\quad \Big(\prod_{t=1}^{k}s_{q_t}\Big)e^{-\sum_{t=1}^{k}\frac{x}{\bar{P}\tilde{\alpha}_{h,q_t}}}\prod_{t=1}^{k}\Big(\sum_{\ell=0}^{L_{h,q_t}-1}\frac{x^\ell}{\ell!(\bar{P}\tilde{\alpha}_{h,q_t})^\ell}\Big) \\ &= 1 + \sum_{k=1}^{K}\Upsilon(-1)^k\prod_{t=1}^{k}\left(\frac{s_{q_t}}{\ell_t!(\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}}\right) \\ &\quad e^{-\sum_{t=1}^{k}\frac{x}{\bar{P}\tilde{\alpha}_{h,q_t}}}x^{\sum_{t=1}^{k}\ell_t} \end{aligned} \tag{A.5}$$

where we define the summation over all combinations of links and channel lengths between the transmitters and the relay node as

$$\Upsilon = \sum_{q_1=1}^{K-k+1} \sum_{q_2=q_1+1}^{K-k+2} \cdots \sum_{q_k=q_{k-1}+1}^{K} \sum_{\ell_1=0}^{L_{h,q_1}-1} \sum_{\ell_2=0}^{L_{h,q_2}-1} \cdots \sum_{\ell_k=0}^{L_{h,q_k}-1} \tag{A.6}$$

following the same steps as in [37].

Appendix B: Derivation of Theorem 1

We first express $F_{\lambda^{\mathrm{R}}}(x)$ alternatively as

$$\begin{aligned} F_{\lambda^{\mathrm{R}}}(x) &= 1 - \sum_{k=1}^{K} \Upsilon (-1)^{k+1} \prod_{t=1}^{k} \left(\frac{s_{q_t}}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) e^{-\beta x} x^{\bar{l}} \\ &= 1 - J_1 \end{aligned} \tag{B.1}$$

where

$$J_1 \triangleq \sum_{k=1}^{K} \Upsilon (-1)^{k+1} \prod_{t=1}^{k} \left(\frac{s_{q_t}}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) e^{-\beta x} x^{\bar{l}}. \tag{B.2}$$

Since $\lambda^{\mathrm{D}} \sim \chi^2(2L_f, P_R\tilde{\alpha}_f)$, $1 - F_{\lambda^{\mathrm{D}}}(x)$ is given by

$$1 - F_{\lambda^{\mathrm{D}}}(x) = e^{-x/P_R\tilde{\alpha}_f} \sum_{l=0}^{L_f-1} \frac{1}{l!} \big(\frac{x}{P_R\tilde{\alpha}_f} \big)^{l}. \tag{B.3}$$

Now using (B.1) and (B.3), we can yield (14).

Appendix C: Derivation of Proposition 2

The CDF of $\lambda^{\mathrm{E,max}}$ in (10) is given by

$$F_{\lambda^{\mathrm{E,max}}}(x) \quad = \quad \prod_{n=1}^{N} F_{\lambda^{\mathrm{E},n,1}}(x) F_{\lambda^{\mathrm{E},n,2}}(x) \tag{C.1}$$

where

$$F_{\lambda^{\mathrm{E,n,1}}}(x) = 1 - s_{k^*} e^{-\frac{x}{\bar{P}\tilde{\alpha}_{j,n,k^*}}} \sum_{r=0}^{L_{j,n,k^*}-1} \frac{1}{r!} \Big(\frac{x}{\bar{P}\tilde{\alpha}_{j,n,k^*}} \Big)^{r} \tag{C.2}$$

is the CDF of the received SNR from the transmitters to the eavesdroppers and

$$F_{\lambda^{\mathrm{E,n,2}}}(x) = \quad 1 - e^{-\frac{x}{P_R\tilde{\alpha}_{g,n}}} \sum_{\tilde{r}=0}^{L_{g,n}-1} \frac{1}{\tilde{r}!} \Big(\frac{x}{P_R\tilde{\alpha}_{g,n}} \Big)^{\tilde{r}} \tag{C.3}$$

is the CDF of the received SNR from the relay to the eavesdroppers. We can re-express (C.1) according to

$$F_{\lambda^{\mathrm{E,max}}}(x) \quad \triangleq \quad \prod_{n=1}^{2N} F_{\lambda^{\mathrm{E},n,3}}(x) \tag{C.4}$$

where we have combined $F_{\lambda^{\mathrm{E,n,1}}}(x)$ and $F_{\lambda^{\mathrm{E,n,2}}}(x)$ as

$$F_{\lambda^{\mathrm{E,n,3}}}(x) = 1 - \tilde{s}_n e^{-\frac{x}{\tilde{P}_n}} \sum_{r=0}^{L_{3,n}-1} \frac{1}{r!} \Big(\frac{x}{\tilde{P}_n} \Big)^{r} \tag{C.5}$$

with $\tilde{s}_n$,$\tilde{P}_n$, and $L_{3,n}$ defined in (17), (18), and (19), respectively. We can expand the product term in (C.4) according to similar steps shown in Appendix A which results in the CDF expression in (15), from which the PDF follows directly.

Appendix D: Derivation of Theorem 4

The asymptotic CDFs of λ^{R} as $\tilde{\alpha}_{h,k} \to \infty$ with perfect backhaul is given by

$$\begin{aligned} F_{\lambda^{\mathrm{R}}}(x) &= \prod_{k=1}^{K} \left(1 - \frac{\Gamma(L_{h,k}, x/\bar{P}\tilde{\alpha}_{h,k})}{\Gamma(L_{h,k})} \right) \\ &= \prod_{k=1}^{K} \left(1 - e^{-\frac{x}{\bar{P}\tilde{\alpha}_{h,k}}} \sum_{\ell=0}^{L_{h,k}-1} \frac{1}{\ell!} \left(\frac{x}{\bar{P}\tilde{\alpha}_{h,k}} \right)^{\ell} \right) \\ &\approx \prod_{k=1}^{K} \frac{1}{(L_{h,k})!} \left(\frac{x}{\bar{P}\tilde{\alpha}_{h,k}} \right)^{L_{h,k}} \end{aligned} \tag{D.1}$$

where we have used the definition of $F_{\lambda^{\mathrm{R}}}(x)$ in (A.4) with $s_k = 1$. As such, the asymptotic expression for (14) as $\tilde{\alpha}_{h,k}, \tilde{\alpha}_f \to \infty$ with (D.1) and $F_{\lambda^{\mathrm{D}}}(x)$ as $F_{\lambda^{\mathrm{D}}}(x) \approx \frac{1}{(L_f)!} \Big(\frac{x}{P_R\tilde{\alpha}_f} \Big)^{L_f}$ is given by (D.2) at the top of the following page where $\tilde{L}_{h,k} \triangleq \sum_{k=1}^{K} (L_{h,k})$.

Similar to [30], we derive the asymptotic limits for a fixed received SNR of the eavesdropper links since the eavesdropper links do not affect the system diversity gain. As such, the CDF and PDF of $\lambda^{\mathrm{E,max}}$ with perfect backhaul, i.e., $s_k = 1\ \forall k$, is given by

$$\begin{aligned} &F_{\lambda^{\mathrm{E,max}}}(x) \triangleq 1 + \Xi e^{-\tilde{\beta}x} x^{\tilde{l}} \text{ and} \\ &f_{\lambda^{\mathrm{E,max}}}(x) \triangleq \Xi \Big[\tilde{l} x^{\tilde{l}-1} e^{-\tilde{\beta}x} - \tilde{\beta} x^{\tilde{l}} e^{-\tilde{\beta}x} \Big]. \end{aligned} \tag{D.3}$$

Applying (D.2) and (D.3) to (20), we can derive the asymptotic secrecy outage probability as in (27). Likewise, the asymptotic probability of non-zero secrecy rate is derived by substituting (D.2) and (D.3) into (23) and solving the resulting integral which results in (28).

To derive the asymptotic ergodic secrecy capacity, we re-express (25) with a change of integration order as [30]

$$\begin{aligned} \bar{C}_s &= \frac{1}{2\log(2)} \int_0^{\infty} \Big[\int_0^{x_1} \frac{1 + F^*_{\lambda^{\mathrm{E,max}}}(x_2)}{1 + x_2} dx_2 \Big] f_{\lambda^{\mathrm{DF}}}(x_1) dx_1 \\ &= \frac{1}{2\log(2)} \Big[\underbrace{\int_0^{\infty} \log(1 + x_1) f_{\lambda^{\mathrm{DF}}}(x_1) dx_1}_{\Omega_1} + \\ &\quad \underbrace{\int_0^{\infty} \int_0^{x_1} \frac{F^*_{\lambda^{\mathrm{E,max}}}(x_2)}{1 + x_2} f_{\lambda^{\mathrm{DF}}}(x_1) dx_2 dx_1}_{\Omega_2} \Big] \end{aligned} \tag{D.4}$$

where $f_{\lambda^{\mathrm{DF}}}(x)$ is the PDF of the SNR λ^{DF} which is the derivative of (14) given by

$$\begin{aligned} f_{\lambda^{\mathrm{DF}}}(x) = &\sum_{k=1}^{K} \Upsilon (-1)^{k} \prod_{t=1}^{k} \left(\frac{1}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \\ &\sum_{l=0}^{L_f-1} \frac{1}{l! (P_R\tilde{\alpha}_f)^{l}} \Big((\bar{l} + l) e^{-x\left(\beta + \frac{1}{P_R\tilde{\alpha}_f}\right)} x^{\bar{l}+l-1} - \\ &\big(\beta + \frac{1}{P_R\tilde{\alpha}_f} \big) e^{-x(\beta + \frac{1}{P_R\tilde{\alpha}_f})} x^{\bar{l}+l} \Big) \end{aligned} \tag{D.5}$$

and

$$F^*_{\lambda^{\mathrm{E,max}}}(x) \triangleq F_{\lambda^{\mathrm{E,max}}}(x) - 1 = \Xi e^{-\tilde{\beta}x} x^{\tilde{l}}. \tag{D.6}$$

$$F_{\lambda^{\mathrm{DF}}}(x) \approx \begin{cases} \prod_{k=1}^{K} \frac{1}{(L_{h,k})!}\Big(\frac{x}{\bar{P}\tilde{\alpha}_{h,k}}\Big)^{L_{h,k}} & \text{when } L_f > \tilde{L}_{h,k}, \\ \frac{1}{(L_f)!}\Big(\frac{x}{P_R\tilde{\alpha}_f}\Big)^{L_f} & \text{when } L_f < \tilde{L}_{h,k}, \\ \frac{1}{(L_f)!}\Big(\frac{x}{P_R\tilde{\alpha}_f}\Big)^{L_f} + \prod_{k=1}^{K} \frac{1}{(L_{h,k})!}\Big(\frac{x}{\bar{P}\tilde{\alpha}_{h,k}}\Big)^{L_{h,k}} & \text{when } L_f = \tilde{L}_{h,k}. \end{cases} \tag{D.2}$$

Based on (D.2), the asymptotic limit of the first integral can be evaluated for $\tilde{\alpha}_{h,k}, \tilde{\alpha}_f \to \infty$ as

$$\begin{aligned} \Omega_1 &= \int_0^\infty \log(x_1) f_{\lambda^{\mathrm{DF}}}(x_1) dx_1 \\ &= \sum_{k=1}^{K} \Upsilon (-1)^k \prod_{t=1}^{k} \left(\frac{1}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \sum_{l=0}^{L_f-1} \frac{1}{l! (P_R\tilde{\alpha}_f)^l} \\ &\quad \int_0^\infty \log(x_1) \Bigg((\bar{l}+l) e^{-x_1\left(\beta + \frac{1}{P_R\tilde{\alpha}_f}\right)} x_1^{\bar{l}+l-1} - \\ &\quad \Big(\beta + \frac{1}{P_R\tilde{\alpha}_f}\Big) e^{-x_1\left(\beta + \frac{1}{P_R\tilde{\alpha}_f}\right)} x_1^{\bar{l}+l} \Bigg) dx_1 \\ &= \sum_{k=1}^{K} \Upsilon (-1)^k \prod_{t=1}^{k} \left(\frac{1}{\ell_t! (\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}} \right) \sum_{l=0}^{L_f-1} \frac{\Gamma(\bar{l}+l+1)}{l! (P_R\tilde{\alpha}_f)^l} \\ &\quad \Big(\beta + \frac{1}{P_R\tilde{\alpha}_f}\Big)^{-(\bar{l}+l)} \Big[\psi(\bar{l}+l) - \psi(\bar{l}+l+1) \Big] \end{aligned} \tag{D.7}$$

where we solve the integral using [41, eq. 4.352.1] $\int_0^\infty x^{\nu-1} e^{-\mu x} \log x dx = \frac{1}{\mu^\nu}\Gamma(\nu)[\psi(\nu) - \log\mu]$.

Applying a change of integration order, the second integral is solved for $\tilde{\alpha}_{h,k}, \tilde{\alpha}_f \to \infty$ as

$$\begin{aligned} \Omega_2 &= \int_0^\infty \frac{F^*_{\lambda^{\mathrm{E,max}}}(x_2)}{1+x_2} (1 - F_{\lambda^{\mathrm{DF}}}(x_2)) dx_2 \\ &\approx \int_0^\infty \frac{F^*_{\lambda^{\mathrm{E,max}}}(x_2)}{1+x_2} dx_2 \\ &= \Xi \int_0^\infty \frac{e^{-\tilde{\beta}x} x^{\tilde{l}}}{1+x_2} dx_2 = \Xi \Gamma(\tilde{l}+1) \Psi(\tilde{l}+1, \tilde{l}+1; \tilde{\beta}) \end{aligned} \tag{D.8}$$

where $\Psi(a,b;z) = \frac{1}{\Gamma(a)} \int_0^\infty e^{-zt} t^{a-1} (1+t)^{b-a-1} dt$ is the confluent hypergeometric function [41, eq. (9.211/4)]. Substituting (D.7) and (D.8) into (D.4) results in the asymptotic ergodic secrecy capacity in (29).

Appendix E: Derivation of Theorem 5

For the asymptotic limit of the CDF of λ^{DF}, we can first derive the asymptotic CDF of λ^{R} in (12) as $\tilde{\alpha}_{h,k} \to \infty$

$$\begin{aligned} F_{\lambda^{\mathrm{R}}}(x) &= \prod_{k=1}^{K} \left(1 - \frac{s_k \Gamma(L_{h,k}, x/\bar{P}\tilde{\alpha}_{h,k})}{\Gamma(L_{h,k})} \right) \\ &\approx \prod_{k=1}^{K} (1 - s_k) \end{aligned} \tag{E.1}$$

since $\Gamma(L_{h,k}, x/\bar{P}\tilde{\alpha}_{h,k}) \approx \Gamma(L_{h,k})$ as $\tilde{\alpha}_{h,k} \to \infty$. Thus, the asymptotic CDF of λ^{D} as $\tilde{\alpha}_f \to \infty$ is given by

$$\begin{aligned} F_{\lambda^{\mathrm{D}}}(x) &= 1 - e^{-x/P_R\tilde{\alpha}_f} \sum_{l=0}^{L_f-1} \frac{1}{l!} \Big(\frac{x}{P_R\tilde{\alpha}_f}\Big)^l \\ &\approx \frac{1}{(L_f)!} \Big(\frac{x}{P_R\tilde{\alpha}_f}\Big)^{L_f}. \end{aligned} \tag{E.2}$$

As such, the asymptotic limit for (14) is given by

$$\begin{aligned} F_{\lambda^{\mathrm{DF}}}(x) &= F_{\lambda^{\mathrm{R}}}(x) + F_{\lambda^{\mathrm{D}}}(x) - F_{\lambda^{\mathrm{R}}}(x) F_{\lambda^{\mathrm{D}}}(x) \\ &\approx \prod_{k=1}^{K} (1 - s_k) \end{aligned} \tag{E.3}$$

since $F_{\lambda^{\mathrm{D}}}(x)$ decays faster than $F_{\lambda^{\mathrm{R}}}(x)$ as $\tilde{\alpha}_{h,k}, \tilde{\alpha}_f \to \infty$.

Similarly, as $\tilde{\alpha}_{j,n,k^*} \to \infty$, the CDF of $\lambda^{\mathrm{E,n,1}}$ in (C.5) can be approximated as

$$F_{\lambda^{\mathrm{E,n,1}}}(x) \approx 1 - s_{k^*} \tag{E.4}$$

since the series expansion of $e^{-\frac{x}{\bar{P}\tilde{\alpha}_{j,n,k^*}}} = \sum_{k=0}^{\infty} (-x)^k / k! (\bar{P}\tilde{\alpha}_{j,n,k^*})^k$ and the summation of $\sum_{r=0}^{L_{j,n,k^*}-1} \frac{1}{r!} \Big(\frac{x}{\bar{P}\tilde{\alpha}_{j,n,k^*}}\Big)^r$ are both dominated by their first terms which is equal to 1. As $\tilde{\alpha}_{g,n} \to \infty$, the CDF of $\lambda^{\mathrm{E,n,2}}$ in (C.3) can be approximated as

$$\begin{aligned} F_{\lambda^{\mathrm{E,n,2}}}(x) &= 1 - e^{-\frac{x}{P_R\tilde{\alpha}_{g,n}}} \sum_{\tilde{r}=0}^{L_{g,n}-1} \frac{1}{\tilde{r}!} \Big(\frac{x}{P_R\tilde{\alpha}_{g,n}}\Big)^{\tilde{r}} \\ &\approx \frac{1}{(L_{g,n})!} \Big(\frac{x}{P_R\tilde{\alpha}_{g,n}}\Big)^{L_{g,n}} \end{aligned} \tag{E.5}$$

As such, the asymptotic limit of the CDF of $\lambda^{\mathrm{E,max}}$ in (17) is given by

$$\begin{aligned} F_{\lambda^{\mathrm{E,max}}}(x) &= \prod_{n=1}^{N} F_{\lambda^{\mathrm{E,n,1}}}(x) F_{\lambda^{\mathrm{E,n,2}}}(x) \\ &\approx \frac{(1 - s_{k^*})^N}{((L_{g,n})!)^N \prod_{n=1}^{N} \tilde{\alpha}_{g,n}^{L_{g,n}}} \Big(\frac{x}{P_R}\Big)^{N(L_{g,n})} \end{aligned} \tag{E.6}$$

as $\tilde{\alpha}_{j,n,k^*}, \tilde{\alpha}_{g,n} \to \infty$.

Applying (E.6) and (E.3) to the derivations of the secrecy outage probability results in

$$\begin{aligned} P_{\mathrm{out}}^{\mathrm{as}} &= \int_0^\infty F_{\lambda^{\mathrm{DF}}}(2^{2R}(1+x) - 1) f_{\lambda^{\mathrm{E,max}}}(x) dx \\ &= \prod_{k=1}^{K} (1 - s_k) \end{aligned} \tag{E.7}$$

since $f_{\lambda^{\mathrm{E,max}}}(x)$ decays faster than $F_{\lambda^{\mathrm{DF}}}(x)$.

Likewise, the asymptotic probability of non-zero secrecy rate is derived as

$$\begin{aligned} Pr(C_s > 0) &= 1 - \int_0^\infty F_{\lambda^{\mathrm{DF}}}(x) f_{\lambda^{\mathrm{E,max}}}(x) dx \\ &= 1 - \prod_{k=1}^{K} (1 - s_k). \end{aligned} \tag{E.8}$$

The asymptotic ergodic secrecy capacity is evaluated as

$$\bar{C}_s = \frac{1}{2\log(2)}\Big[\underbrace{\int_0^\infty \log(x_1) f_{\lambda^{\mathrm{DF}}}(x_1)dx_1}_{\Omega_3} + \underbrace{\int_0^\infty \frac{F^*_{\lambda^{\mathrm{E,max}}}(x_2)}{1+x_2}(1-F_{\lambda^{\mathrm{DF}}}(x_2))dx_2}_{\Omega_4}\Big] \quad \text{(E.9)}$$

where

$$\begin{aligned}\Omega_3 &= \sum_{k=1}^{K}\Upsilon(-1)^k \prod_{t=1}^{k}\Big(\frac{s_{q_t}}{\ell_t!(\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}}\Big)\sum_{l=0}^{L_f-1}\frac{1}{l!(P_R\tilde{\alpha}_f)^l} \\ &\int_0^\infty \log(x_1)\Big((\bar{l}+l)e^{-x\left(\beta+\frac{1}{P_R\tilde{\alpha}_f}\right)}x^{\bar{l}+l-1} - \\ &\big(\beta+\frac{1}{P_R\tilde{\alpha}_f}\big)e^{-x\left(\beta+\frac{1}{P_R\tilde{\alpha}_f}\right)}x^{\bar{l}+l}\Big)dx_1 \\ &= \sum_{k=1}^{K}\Upsilon(-1)^k \prod_{t=1}^{k}\big(\frac{s_{q_t}}{\ell_t!(\bar{P}\tilde{\alpha}_{h,q_t})^{\ell_t}}\big)\sum_{l=0}^{L_f-1}\frac{\Gamma(\bar{l}+l+1)}{l!(P_R\tilde{\alpha}_f)^l} \\ &\big(\beta+\frac{1}{P_R\tilde{\alpha}_f}\big)^{-(\bar{l}+l)}[\psi(\bar{l}+l)-\psi(\bar{l}+l+1)] \quad \text{(E.10)}\end{aligned}$$

and

$$\begin{aligned}\Omega_4 &= \int_0^\infty \frac{F^*_{\lambda^{\mathrm{E,max}}}(x_2)}{1+x_2}\Big(1-\prod_{k=1}^{K}(1-s_k)\Big)dx_2 \\ &= \Big(1-\prod_{k=1}^{K}(1-s_k)\Big)\Phi\Gamma(\tilde{l}+1)\Psi(\tilde{l}+1,\tilde{l}+1;\tilde{\beta}). \quad \text{(E.11)}\end{aligned}$$

REFERENCES

[1] J. Andrews, S. Buzzi, W. Choi, S. Hanly, A. Lozano, A. Soong, and J. Zhang, "What will 5G be ?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, p. 10651082, Jun. 2014.

[2] J. Andrews, "Seven ways that hetnets are a cellular paradigm shift," *IEEE Commun. Mag.*, vol. 51, no. 3, pp. 136–144, Mar. 2013.

[3] Z. Mayer, J. Li, A. Papadogiannis, and T. Svensson, "On the impact of control channel reliability on coordinated multi-point transmission," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014:28, pp. 1–16, 2014.

[4] O. Tipmongkolsilp, S. Zaghloul, and A. Jukan, "The evolution of cellular backhaul technologies: Current issues and future trends," *IEEE Commun. Surveys Tuts.*, vol. 13, pp. 97–113, 2012.

[5] P. Xia, C.-H. Liu, and J. G. Andrews, "Downlink coordinated multi-point with overhead modeling in heterogeneous cellular networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, pp. 4025–4037, Aug. 2013.

[6] S.-H. Park, O. Simeone, O. Sahin, and S. Shamai, "Robust and efficient distributed compression for cloud radio access networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 692–703, Feb. 2013.

[7] F. Pantisano, M. Bennis, W. Saad, M. Debbah, and M. Latva-aho, "On the impact of heterogeneous backhauls on coordinated multipoint transmission in femtocell networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, Jun. 2012, pp. 5064–5069.

[8] Y. Li, X. Wang, S. Zhou, and S. Alshomrani, "Uplink coordinated multi-point reception with limited backhaul via cooperative group decoding," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3017–3030, Jun. 2014.

[9] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 2, pp. 242–256, Jun. 2009.

[10] P. Ishwar, R. Puri, K. Ramchandran, and S. S. Pradhan, "On rate-constrained distributed estimation in unreliable sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, pp. 765–775, 2006.

[11] S. Simeone, O. Somekh, E. Erkip, H. V. Poor, and S. Shamai, "Robust communication via decentralized processing with unreliable backhaul links," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4187–4201, Jul. 2011.

[12] J. Du, M. Xiao, M. Skoglund, and M. Medard, "Wireless multicast relay networks with limited-rate source-conferencing," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1390–1401, Aug. 2013.

[13] J. Du, M. Xiao, and M. Skoglund, "Cooperative network coding strategies for wireless relay networks with backhaul," *IEEE Trans. Commun.*, vol. 60, pp. 2502–2514, Sep. 2011.

[14] A. D. Coso and S. Simoens, "Distributed compression for MIMO coordinated networks with a backhaul constraint," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4698–4709, Sep. 2011.

[15] O. Simeone, O. Somekh, H. Poor, and S. Shamai, "Enhancing uplink throughput via local base station cooperation," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, Nov. 2008, pp. 116–120.

[16] E. Aktas, J. Evans, and S. Hanly, "Distributed decoding in a cellular multiple-access channel," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 241–250, Jun. 2008.

[17] V. Gambiroza, B. Sadeghi, and E. W. Knightly, "End-to-end performance and fairness in multihop wireless backhaul networks," in *International conference on Mobile Computing and Networking*, Philadelphia, PA, USA, Spt.-Oct. 2004, pp. 289–301.

[18] G. Narlikar, G. Wilfong, and L. Zhang, "Designing multihop wireless backhaul networks with delay gurantees," *Wireless Netw.*, vol. 16, no. 1, pp. 237 –254, Jan. 2010.

[19] 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.

[20] 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.

[21] D.-Y. Seol, U.-K. Kwon, G.-H. Im, and E.-S. Kim, "Relay-based single carrier transmission with SFBC in uplink fast fading channels," *IEEE Commun. Lett.*, vol. 12, no. 12, pp. 928–930, Dec. 2007.

[22] 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.

[23] P. Wu and R. Schober, "Cooperative beamforming for single-carrier frequency-domain equalization systems with multiple relays," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2276–2286, Jun. 2012.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90–103, 2015.

[31] 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.

[32] 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.

[33] 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.

[34] T. A. Khan, P. Orlik, K. J. Kim, and R. W. Heath, "Performance analysis of cooperative wireless networks with unreliable backhaul links," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1386–1389, Aug. 2015.

[35] Z. Mayer, J. Li, A. Papadogiannis, and T. Svensson, "On the impact of control channel reliability on coordinated multi-point transmission," *EURASIP Journal on Wireless Communications and Networking*, no. 2014:28, 2014.
[36] T. Wang, A. Cano, G. B. Giannakis, and J. N. Laneman, "High-performance cooperative demodulation with decode-and-forward relays," *IEEE Trans. Commun.*, vol. 55, no. 7, pp. 1427–1438, 2007.
[37] H. Yu, I.-H. Lee, and G. L. Stuber, "Outage probability of decode-and-forward cooperative relaying systems with co-channel interference," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 266–274, Jan. 2012.
[38] P. R. Davis, *Circulant Matrices*. N. Y.: John Wiley, 1979.
[39] D. Torrieri and M. C. Valenti, "The outage probability of a finite Ad Hoc network in Nakagami fading," *IEEE Trans. Commun.*, vol. 60, pp. 2960–2970, Dec. 2012.
[40] J. Guo, S. Durrani, and X. Zhou, "Outage probability in arbitrarily-shaped finite wireless networks," *IEEE Trans. Commun.*, vol. 62, pp. 699–712, Feb. 2014.
[41] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York: Academic Press, 2007.

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 works 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, physical layer secrecy system, and device-to-device communications.

Dr. Kim currently serves as an editor for the IEEE COMMUNICATIONS LETTERS and INTERNATIONAL JOURNAL OF ANTENNAS AND PROPAGATION. He also served 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". Since 2013, he has served as a TPC chair for the IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security.

Phee Lep Yeoh (M'12) received the B.E. degree with University Medal from the University of Sydney, Australia, in 2004, and the Ph.D. degree from the University of Sydney, Australia, in 2012. From 2005 to 2008, he worked at Telstra Australia as a wireless network engineer. From 2008 to 2012, he was with the Telecommunications Laboratory at the University of Sydney and the Wireless and Networking Technologies Laboratory at the Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia.

In 2012, he joined the Department of Electrical and Electronic Engineering at the University of Melbourne, Australia. He is a recipient of the 2014 Australian Research Council Discovery Early Career Researcher Award. He has served as the TPC chair for the 2016 Australian Communications Theory Workshop (AusCTW) and TPC member for IEEE GLOBECOM, ICC, and VTC conferences. He has received best paper awards at IEEE ICC 2014 and IEEE VTC-Spring 2013, and the best student paper award at AusCTW 2013. His current research interests include heterogeneous wireless networks, large-scale MIMO networks, cognitive cooperative communications, and multiscale molecular communications.

Philip V. Orlik (SM'97) was born in New York, NY in 1972. He received the B.E. degree in 1994 and the M.S. degree in 1997 both from the State University of New York at Stony Brook. In 1999 he earned his Ph. D. in electrical engineering also from SUNY Stony Brook.

In 2000 he joined Mitsubishi Electric Research Laboratories Inc. located in Cambridge, MA where he is currently the Team Leader of the Mobile Systems Group. His primary research focus is on advanced wireless and mobile communications, sensor networks, ad hoc networking and UWB. Other research interests include vehicular/car-to-car communications, mobility modeling, performance analysis, and queuing theory.

H. Vincent Poor (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 statistical signal processing, stochastic analysis and information theory, and their applications in wireless networks and related fields. Among his publications in these areas is the recent book *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 and the National Academy of Inventors, and of other national and international academies. He received the Technical Achievement and Society Awards of the IEEE Signal Processing Society in 2007 and 2011, respectively. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, the 2015 EURASIP Athanasios Papoulis Award, the 2016 John Fritz Medal, and honorary doctorates from Aalborg University, Aalto University, HKUST and the University of Edinburgh.