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

Secrecy Performance of Finite-Sized In-Band Selective Relaying Systems with Unreliable Backhaul and Cooperative Eavesdroppers

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

TR2018-110 August 17, 2018

Abstract

This paper investigates the secrecy performance of a finite-sized in-band selective relaying system with M transmitters connected via unreliable backhaul links, N decode-and-forward relays, and K collaborative eavesdroppers. To send the source message to the destination, a transmitter-relay pair that achieves the highest end-to-end signal-to-noise ratio is selected for transmissions, while the K eavesdroppers combine all the received signals from the selected transmitter and relay using maximum ratio combining. The proposed model introduces backhaul reliability and eavesdropping probability parameters to investigate practical constraints on the transmitter-relay cooperation and eavesdropper collaboration, respectively. Closed-form expressions are derived for the secrecy outage probability, probability of nonzero achievable secrecy rate, and ergodic secrecy rate for nonidentical frequency-selective fading channels with robust cyclicprefixed single carrier transmissions. These results show that the asymptotic secrecy outage probability and probability of non-zero achievable secrecy rate are exclusively determined by the number of transmitters M and their corresponding set of backhaul reliability levels. Under unreliable backhaul connections, it is found that the secrecy diversity gain is determined by M, N, and the number of multipath components in the frequency selective fading channels. Link-level simulations are conducted to verify the derived impacts of backhaul reliability and collaborative eavesdropping on the secrecy performance.

IEEE Journal on Selected Areas in Communications

Secrecy Performance of Finite-Sized In-Band Selective Relaying Systems with Unreliable Backhaul and Cooperative Eavesdroppers

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

***Abstract*—This paper investigates the secrecy performance of a finite-sized in-band selective relaying system with M transmitters connected via unreliable backhaul links, N decode-and-forward relays, and K collaborative eavesdroppers. To send the source message to the destination, a transmitter-relay pair that achieves the highest end-to-end signal-to-noise ratio is selected for transmissions, while the K eavesdroppers combine all the received signals from the selected transmitter and relay using maximum ratio combining. The proposed model introduces backhaul reliability and eavesdropping probability parameters to investigate practical constraints on the transmitter-relay cooperation and eavesdropper collaboration, respectively. Closed-form expressions are derived for the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate for non-identical frequency-selective fading channels with robust cyclic-prefixed single carrier transmissions. These results show that the asymptotic secrecy outage probability and probability of non-zero achievable secrecy rate are exclusively determined by the number of transmitters M and their corresponding set of backhaul reliability levels. Under unreliable backhaul connections, it is found that the secrecy diversity gain is determined by M, N, and the number of multipath components in the frequency selective fading channels. Link-level simulations are conducted to verify the derived impacts of backhaul reliability and collaborative eavesdropping on the secrecy performance.**

***Index Terms*—Wireless backhaul, in-band selective relaying, eavesdropping probability, secrecy outage probability.**

I. Introduction

With unprecedented demands for wireless data traffic, it is envisioned that ultra dense heterogeneous networks will be a key feature of future wireless cellular networks. Specifically, it is anticipated that large numbers of small cells could be deployed in high-traffic areas to satisfy the data demands of large numbers of wireless devices [1], [2]. A key challenge in ultra-dense deployments is the provision of large-scale, ultra-reliable, and highly-secure backhaul links for the small cell base stations [3]–[5]. Recently, wireless backhaul has gained considerable interest due to its flexibility and scalability in providing large-scale backhaul connections between the control unit (CU) e.g., a nearby macro base station or internet gateway and the small cell transmitters [6]–[8]. It has been shown that wireless technologies such as millimeter wave (mmWave) communications [9] and massive multiple input multiple output (MIMO) antennas [10] could be used to provide backhaul connections supporting hundreds of gigabits backhaul traffic in 5G ultra dense heterogeneous small cell networks. However, wireless backhauling for 5G small cells is sometimes unreliable and insecure due to wireless channel impairments such as non-line-of-sight (nLoS) propagation, severe fading, network congestion, and synchronization [11], [12].

The impacts of wireless backhaul reliability and capacity constraints on system performance have been investigated for various heterogeneous networks including finite-sized systems [13], cloud radio networks [14], and coordinated multi-point transmissions [15], which represent different 5G network topologies. In [16], the authors analyzed the impact of nLoS propagation on the outage performance of 5G mmWave backhaul links. Wireless backhauls have also been widely applied in cooperative relay networks for uplink connections [17]–[19]. In [20], the outage performance was investigated for cooperative systems with unreliable backhauls over Rayleigh fading channels.

A promising 5G waveform solution to improve the reliability and security of wireless backhauls is cyclic-prefixed single-carrier (CP-SC) transmissions. It has been shown that CP-SC transmission with either null cyclic-prefix (CP) [21] or block-wise data CP [22] are suitable for deploying massive MIMO in mmWave communications with robustness to phase noise and carrier frequency offset. In advanced cooperative relaying systems, CP-SC is a practical transmission scheme for achieving multi-user and multi-path diversity [23], [24]. In [25], the secrecy performance of finite-sized CP-SC relay systems with unreliable backhauls and a single relay was investigated. To improve the end-to-end system performance, several relay selection schemes have been proposed for CP-SC-based cooperative relay systems in [26], [27].

Given the broadcast nature of wireless channels, the physical layer transmission of legitimate signals are vulnerable to be

Manuscript received August 18, 2017; revised January 30, 2018; accepted February 16, 2018. *(Corresponding author: Kyeong Jin Kim.)*

H. Liu is with the School of Information Science and Electric Engineering, Shandong Jiaotong University, Jinan 250357, China. He is also with the Department of Information and Communication Engineering, Inha University, Incheon 22212, South Korea (e-mail: hong.w.liu@hotmail.com).

P. L. Yeoh is with the School of Electrical and Information Engineering, University of Sydney, Australia (e-mail: phee.yeoh@sydney.edu.au).

K. J. Kim and P. V. Orlik are with Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA 02139 USA (e-mail: kkim@merl.com; porlik@merl.com).

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

This work was supported in part by the U.S. National Science Foundation under Grants ECCS-1549881 and ECCS-1647198, and in part by the Australian Research Council grant DE140100420.

intercepted by potential external eavesdroppers [28]–[30]. As an important means of securing wireless transmissions against eavesdropping, physical layer security strategies have been investigated based on exploiting physical characteristics of the wireless medium from a channel coding perspective [31]–[33]. In the presence of multiple eavesdroppers, cooperative relay systems have been proposed to further enhance physical layer security using relay selection [34], [35], joint relay-user selection [36], and beamforming [37], [38]. When multiple antennas are deployed at a single transmitter, it has been shown that transmit antenna selection (TAS) can enhance secrecy performance [39]–[41]. In [42], TAS has been applied to achieve diversity with the aid of incremental relaying for a cooperative relay system with a single relay. Different from [42], we consider the impact of multiple relays with relay selection and TAS at the transmitters. Similarly, when multiple transmitters are connected to a CU via wireless backhauls, transmitter selection can be used to achieve diversity for secure communications [25]. Since the proposed system uses the CU for transmitter cooperation, the challenging synchronization between transmitters can be reduced in the transmitter selection.

In [43], the physical layer security performance of finite-sized cooperative relay systems with unreliable backhaul links was analyzed for a single eavesdropper attempting to intercept tranmissions from multiple transmitters and a single relay. The more general scenario of multiple colluding eavesdroppers was considered in [25] where the intercepted signal with the highest signal-to-noise ratio (SNR) among the eavesdroppers was selected for decryption. Previous results have shown that the secrecy performance of finite-sized cooperative relay systems with multiple colluding eavesdroppers can be improved by either transmitter selection [25] or relay selection [44]. To enhance the intercept capability, maximum SNR-based selection [25] or maximum ratio combining (MRC) [44] may be applied across all the eavesdroppers, which makes achieving secure communications very challenging with escalating wiretapping and decrypting capabilities [28]–[30]. In practice, it has been shown that multiple eavesdroppers may not always be capable of intercepting legitimate wireless transmissions due to imperfect synchronization and inner-information exchange among the eavesdroppers [44]. As a further countermeasure against eavesdropper collaboration, the effect of joint transmitter-relay cooperation on the physical layer security of finite-sized cooperative systems with unreliable backhauls remains unknown.

In this paper, we present a general analytical framework for the secrecy performance of a finite-sized in-band selective relaying system consisting of M transmitters and N relays in the presence of K eavesdroppers. Several potential 5G characters have been considered in this paper, including wireless backhaul, frequency-selective fading, CP-SC transmission, transmitter-relay cooperation, and eavesdropper cooperation. Different from the incremental relay system in which TAS is applied for enhancing physical layer security [42], multiple transmitters are connected to a CU with unreliable wireless backhaul in this paper. Intuitively, the considered transmitter cooperation can be recognized as a CU with a distributed TAS if perfect wireless backhaul connections are available. In the main channel, M transmitters are connected to a CU via unreliable backhauls, while a transmitter-relay pair associated with the highest end-to-end SNR is selected out of the MN transmitter-relay pairs to transmit the source message to the destination. In the eavesdropping channel, K eavesdroppers collaborate to share information obtained from the active transmitter-relay pair. Since the benefits of eavesdropper collaboration is achieved at the expense of synchronization to the legitimate transmissions and inner-information exchange, we introduce an eavesdropping probability parameter to model the cost of the eavesdropper collaboration [44]. To quantitatively assess the joint impact of the unreliable backhauls and eavesdropping probability on the secrecy performance of the considered system, we derive new exact and asymptotic closed-form expressions for the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate under quasi-static frequency-selective fading channels with CP-SC transmissions. Since these secrecy performance metrics are tightly coupled with respect to the secrecy rate of the main channels under quasi-static fading channels, the obtained results for these metrics are practically useful for designing secret key exchange protocols and coding algorithms [28], [29]. In contrast to previous results on physical layer security in the presence of multiple eavesdroppers, the main contributions of this paper are summarized as follows.

- For finite-sized in-band selective relaying systems, we derive the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate with multiple transmitter-relay cooperation, backhaul reliability, and eavesdropping probability. Note that an investigation of the joint impact of transmitter-relay cooperation, backhaul reliability, and eavesdropping probability in finite-sized in-band selective relay systems has not been investigated previously. Thus, its accompanying secrecy performance analysis is novel from this work. Moreover, we consider frequency-selective fading channels which are fairly general for practical applications.
- A new closed-form expression for the cumulative distribution function (CDF) of the end-to-end SNR is derived for the main channel of the finite-sized in-band selective relaying system. Compared to previous idealized linear models of selective relaying [45] in which an identical number of nodes and identical flat fading links are assumed for each hop, we consider a finite-sized in-band selective relaying system with general M, N, and non-identical frequency-selective fading channels.
- The secrecy performance is investigated under unreliable backhauls and non-ideal eavesdropper collaboration. The joint impacts of unreliable backhauls and non-ideal eavesdropper collaboration are comprehensively characterized in terms of the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate. Different from most existing works considering multiple eavesdroppers, collaborative detection using MRC across multiple eavesdroppers is considered in this paper.
- Asymptotic limits of the secrecy outage probability and

TABLE I
NOTATION USED IN THIS PAPER

Notation	Description
$[x]^+$	$[x]^+ \triangleq \max(x, 0)$.
$\delta(\cdot)$	$\delta(\cdot)$ denotes the delta function.
$\mathbb{E}\{\cdot\}$	$\mathbb{E}\{\cdot\}$ is the expectation operation.
$\mathbb{L}(\boldsymbol{a})$	$\mathbb{L}(\boldsymbol{a})$ denotes the length of a vector $\boldsymbol{a}$.
$\{\boldsymbol{a}\}$	$\{\boldsymbol{a}\}$ is the set containing all the elements of a vector $\boldsymbol{a}$.
$\boldsymbol{I}_B$	$\boldsymbol{I}_B$ is the $B \times B$ identity matrix.
$\boldsymbol{A}(i,j)$	$\boldsymbol{A}(i,j)$ is the (i,j)-th element of a matrix $\boldsymbol{A}$.
$\boldsymbol{A}(i,:)$	$\boldsymbol{A}(i,:)$ is the ith row of a matrix $\boldsymbol{A}$.
$\boldsymbol{C}_k^n$	$\boldsymbol{C}_k^n$ is an $\binom{n}{k} \times k$ integer matrix, whose ith row contains the ith result of the combinations of $\{1, 2, \ldots, n\}$ taking k elements for each combination.
$\bar{\boldsymbol{C}}_k^n$	$\bar{\boldsymbol{C}}_k^n$ is an $\binom{n}{k} \times (n-k)$ integer matrix such that the union of $\boldsymbol{C}_k^n(i,:)$ and $\bar{\boldsymbol{C}}_k^n(i,:)$ contains all the elements of the set $\{1, 2, \ldots, n\}$.
$\mu(\varphi)$	$\mu(\varphi) \triangleq \lceil \frac{\varphi}{N} \rceil$
$\nu(\varphi)$	$\nu(\varphi) \triangleq \varphi - \lceil \frac{\varphi}{N} - 1 \rceil N$
$\widetilde{\alpha}_\ell$	$\widetilde{\alpha}_\ell \triangleq \sum_{\varepsilon=1}^{\ell} \frac{1}{P_R \widetilde{\rho}_{f,r_\varepsilon}}$
$\widetilde{\alpha}_\ell$	$\widetilde{\alpha}_\ell \triangleq \sum_{\varepsilon=1}^{\ell} \frac{1}{P_R \widetilde{\rho}_{f,r_\varepsilon}}$
$\widehat{\alpha}_\varphi$	$\widehat{\alpha}_\varphi \triangleq \sum_{\varepsilon=1}^{\varphi} \frac{1}{P \widetilde{\rho}_{h,\nu(\hat{r}_\varepsilon),\mu(\hat{r}_\varepsilon)}}$
$\widetilde{\beta}_\ell$	$\widetilde{\beta}_\ell \triangleq \sum_{\varepsilon=1}^{\ell} t_\varepsilon$
$\widehat{\beta}_\varphi$	$\widehat{\beta}_\varphi \triangleq \sum_{\varepsilon=1}^{\varphi} s_\varepsilon$
$\widetilde{\Upsilon}_\ell$	$\widetilde{\Upsilon}_\ell \triangleq \prod_{\varepsilon=1}^{\ell} \frac{1}{t_\varepsilon! (P_R \widetilde{\rho}_{f,\tilde{r}_\varepsilon})^{t_\varepsilon}}$
$\widehat{\Upsilon}_\varphi$	$\widehat{\Upsilon}_\varphi \triangleq \prod_{\varepsilon=1}^{\varphi} \frac{1}{s_\varepsilon! (P \widetilde{\rho}_{h,\nu(\hat{r}_\varepsilon),\mu(\hat{r}_\varepsilon)})^{s_\varepsilon}}$
$\widetilde{\sum}$	$\widetilde{\sum} \triangleq \sum_{\ell=1}^{N} \sum_{\tilde{r}_1=1}^{N-\ell+1} \sum_{\tilde{r}_2=r_1+1}^{N-\ell+2} \cdots \sum_{\tilde{r}_\ell=\tilde{r}_{\ell-1}+1}^{N} \sum_{t_1=0}^{L_{f,\tilde{r}_1}-1} \sum_{t_2=0}^{L_{f,\tilde{r}_2}-1} \cdots \sum_{t_\ell=0}^{L_{f,\tilde{r}_\ell}-1}$
$\widehat{\sum}$	$\widehat{\sum} \triangleq \sum_{\varphi=1}^{MN} \sum_{\hat{r}_1=1}^{MN-\varphi+1} \sum_{\hat{r}_2=\hat{r}_1+1}^{MN-\varphi+2} \cdots \sum_{\hat{r}_\varphi=\hat{r}_{\varphi-1}+1}^{MN} \sum_{s_1=0}^{L_{h,\nu(\hat{r}_1),\mu(\hat{r}_1)}-1} \sum_{s_2=0}^{L_{h,\nu(\hat{r}_2),\mu(\hat{r}_2)}-1} \cdots \sum_{s_\varphi=0}^{L_{h,\nu(\hat{r}_\varphi),\mu(\hat{r}_\varphi)}-1}$

probability of non-zero achievable secrecy rate are presented for finite-sized in-band selective relaying systems. It is shown that an intrinsic outage probability floor and a ceiling on the probability of non-zero achievable secrecy rate are exclusively determined by the backhaul reliability and transmitter cooperation. It is also shown that the secrecy diversity gain is jointly determined by M, N, and the summation of the multi-path components in the frequency-selective fading channels.

The rest of this paper is organized as follows: Section II presents the system and channel model; Section III derives the statistical properties of the end-to-end SNRs; Section IV analyzes the secrecy performance of the considered system; Section V gives simulation results to verify the analysis, and Section VI summarizes the paper.

Notation: $f_x(\cdot)$ and $F_x(\cdot)$ denote the probability density function (PDF) and CDF of the random variable (RV) x, respectively. $\mathcal{CN}(\mu, \sigma^2)$ denotes the complex Gaussian distribution with the mean μ and the variance σ^2. $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ denote the floor and ceil functions, respectively. Additional notation used in this paper is summarized in Table I.

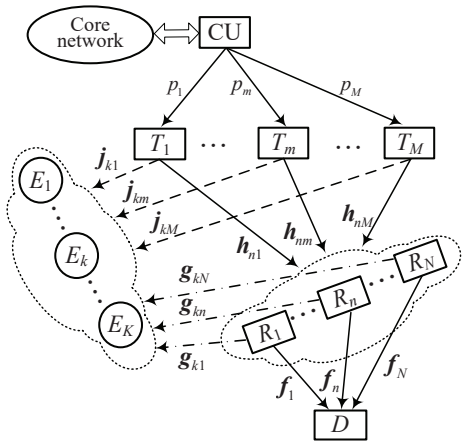

Fig. 1. Block diagram of a finite-sized in-band selective relaying system with unreliable backhauls in the presence of multiple eavesdroppers.

II. SYSTEM AND CHANNEL MODEL

Fig. 1 shows a block diagram of the considered finite-sized in-band selective relaying system, in which M transmitters $(T_1, \ldots, T_M)$ are connected to a CU via unreliable wireless backhauls. Different from a finite-sized cooperative relaying system with a single relay and a single eavesdropper [46], the considered system includes N intermediate relay nodes $(R_1, \ldots, R_N)$ and K colluding eavesdroppers $(E_1, \ldots, E_K)$. We consider that M transmitters and N relays are operated in-band, whereas massive MIMO and mmWave communications are employed for wireless backhaul connections [9], [10], [12], [16]. With the aid of analog beamforming [47] or a hybrid of analog beamforming and digital MIMO processing [48] for wireless backhaul connections, we assume that the nearby users can hardly intercept wireless backhaul transmissions unless the users are located within the narrow beams. Therefore, in this paper, we only consider that multiple eavesdroppers wiretap the legitimate transmissions from multiple transmitters and relays. Due to large path-loss or obstacles, we assume that the direct links between T_m, $\forall m$ and D are unavailable. The details of the channel model are described as follows:

- The channel vectors of the $T_m \to R_n$, $R_n \to D$, $T_m \to E_k$, and $R_n \to E_k$ links are respectively denoted by $\boldsymbol{h}_{nm}$, $\boldsymbol{f}_n$, $\boldsymbol{j}_{km}$, and $\boldsymbol{g}_{kn}$ for $m = 1, \ldots, M$, $n = 1, \ldots, N$, and $k = 1, \ldots, K$, respectively.
- The elements of the channel vectors are independent and identically distributed (i.i.d.) complex Gaussian random variables with zero means and unit variances. All the channels are assumed to be block fading, i.e., the elements of channel vectors remain constant, but independently vary from one transmission block to another.
- We consider non-identical frequency selective fading channels to model realistic systems with different channel vector lengths and path loss. As such, we denote the lengths of $\boldsymbol{h}_{nm}$, $\boldsymbol{f}_n$, $\boldsymbol{j}_{km}$, and $\boldsymbol{g}_{kn}$ by $L_{h,n,m} \triangleq \mathbb{L}(\boldsymbol{h}_{nm})$, $L_{f,n} \triangleq \mathbb{L}(\boldsymbol{f}_n)$, $L_{j,k,m} \triangleq \mathbb{L}(\boldsymbol{j}_{km})$,

and $L_{g,k,n} \triangleq \mathbb{L}(\boldsymbol{g}_{kn})$, respectively, and $L_{\max} = \max\{L_{h,n,m}, L_{f,n}, L_{j,k,m}, L_{g,k,n}\}$ over $\forall m, n, k$ is the maximum number of multipath components in the system. The path-loss components over $\boldsymbol{h}_{nm}$, $\boldsymbol{f}_n$, $\boldsymbol{j}_{km}$, and $\boldsymbol{g}_{kn}$ are denoted by $\rho_{h,n,m}$, $\rho_{f,n}$, $\rho_{j,k,m}$, and $\rho_{g,k,n}$, respectively.

- Based on channel state information (CSI) of the main channel, selective relaying is implemented using a centralized approach [34], [45], i.e., a single $T_m \rightarrow R_n \rightarrow D$ link with the highest end-to-end SNR is selected to transmit the source message to the destination. For the centralized mechanism, we assume that the CU uses CSI knowledge of all the links in the main channel to select the best transmitter-relay pair [34], while the relay R_n has CSI of the links $T_m \rightarrow R_n$, $\forall m$ and the destination has CSI of the links $R_n \rightarrow D$, $\forall n$ [25], [34], [45].
- The backhaul reliability for the link CU $\rightarrow T_m$ is denoted by p_m, which represents the probability that T_m can successfully decode the source message via its backhaul transmission. The backhaul reliability follows a Bernoulli process and is independent across source messages [25], so that $\Pr(\mathbb{B}_m = 1) = p_m$ and $\Pr(\mathbb{B}_m = 0) = 1 - p_m$, where $\mathbb{B}_m$ is a binary indicator function.
- The eavesdropping probability for E_k is denoted by q_k, which is the probability that E_k can successfully obtain information from the legitimate transmission and collaborate with the colluding eavesdroppers. A Bernoulli random variable $\mathbb{I}_k$ is applied to represent q_k. Due to constraints on signalling synchronization, transmission bandwidth, and channel capacity of the eavesdropping links, the eavesdropping probability that E_k successfully intercepts the transmitter/relay transmissions and exchanges information amongst the colluding eavesdroppers is given by $\Pr(\mathbb{I}_k = 1) = q_k$; otherwise $\Pr(\mathbb{I}_k = 0) = 1 - q_k$ [44].

When a backhaul transmission fails, we do not consider additional coding, automatic repeat request (ARQ), and power control to focus on the impact of backhaul reliability on the secrecy performance. For each transmission block, the selective relaying is conducted within two consecutive time phases. In the first time phase, the selected transmitter sends the source message to the selected relay. In the second time phase, the selected relay transmits its signal to the destination. We assume that the relays work in decode-and-forward (DF) relaying mode, such that the re-transmitted signal by the selected relay is accurately decoded from the source message. In the main channel, we adopt CP-SC transmission with M-ary phase-shift keying (MPSK) modulation. We assume perfect synchronization between the CU and all the transmitters by a timestamp provided by a global navigation satellite system (GNSS), such that all the transmitters simultaneously transmit a symbol block $\boldsymbol{x} \in \mathbb{C}^{B\times 1}$, where B is the size of the symbol block, $\mathbb{E}\{\boldsymbol{x}\} = \boldsymbol{0}$, and $\mathbb{E}\{||\boldsymbol{x}||^2\} = \boldsymbol{I}_B$. To prevent inter-block symbol interference (IBSI), an additional cyclic-prefix (CP) comprising of L_c symbols from $\boldsymbol{x}$ is appended to the front of $\boldsymbol{x}$ with $L_c \geq L_{\max}$.

In the first and second time phase, the selected relay and destination removes the CP-related signals to obtain their effective received signals, respectively. The received signals at the selected relay and destination can be expressed as

$$\boldsymbol{y}^{\mathrm{R}} = \sqrt{\bar{P}\rho_{h,\widetilde{n},\widetilde{m}}}\mathbb{B}_{\widetilde{m}}\boldsymbol{H}_{\widetilde{n},\widetilde{m}}\boldsymbol{x} + \boldsymbol{z}^{\mathrm{R}} \tag{1}$$

and

$$\boldsymbol{y}^{\mathrm{D}} = \sqrt{P_R\rho_{f,\widetilde{n}}}\boldsymbol{F}_{\widetilde{n}}\boldsymbol{x} + \boldsymbol{z}^{\mathrm{D}}, \tag{2}$$

respectively, where $\bar{P}$ is the maximum transmission power at the transmitters, P_R is the transmission power at each relay, $\widetilde{m}$ and $\widetilde{n}$ are the indices of the selected transmitter and relay, respectively, and $\boldsymbol{z}^{\mathrm{R}} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$ and $\boldsymbol{z}^{\mathrm{D}} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$ are the additive noise vectors at the selected relay and destination, respectively. Due to CP-SC transmission, $\boldsymbol{H}_{\widetilde{n},\widetilde{m}}$ ($\boldsymbol{F}_{\widetilde{n}}$) is the right circulant matrix specified by the corresponding channel vectors $\boldsymbol{h}_{\widetilde{n},\widetilde{m}}$ ($\boldsymbol{f}_{\widetilde{n}}$) with zero padding to match the length of $\boldsymbol{x}$ [27].

In the considered finite-sized in-band selective relaying system, a transmitter-relay pair with the highest end-to-end SNR is selected to transmit in the main channel, such that the selected node indices are given by

$$(\widetilde{m}, \widetilde{n}) = \arg\max_{\forall m,\forall n} \lambda^{T_mR_nD}, \tag{3}$$

where $\lambda^{T_mR_nD}$ is the end-to-end SNR of the main channel transmission associated with the link $T_m \rightarrow R_n \rightarrow D$ which will be defined in the following section.

For the eavesdropping channel, we assume that the eavesdroppers are aware of CP-SC transmissions used in the main channel and apply the corresponding demodulation scheme in the interception. After removal of the CP-related signal parts, the effective received signals at E_k in the first and second time phases are given by

$$\boldsymbol{y}^{\mathrm{E},k,1} = \sqrt{\bar{P}\rho_{j,k,\widetilde{m}}}\mathbb{I}_k\mathbb{B}_{\widetilde{m}}\boldsymbol{J}_{k,\widetilde{m}}\boldsymbol{x} + \boldsymbol{z}^{\mathrm{E},k,1} \tag{4}$$

and

$$\boldsymbol{y}^{\mathrm{E},k,2} = \sqrt{P_R\rho_{g,k,\widetilde{n}}}\mathbb{I}_k\boldsymbol{G}_{k,\widetilde{n}}\boldsymbol{x} + \boldsymbol{z}^{\mathrm{E},k,2}, \tag{5}$$

respectively, where $\boldsymbol{J}_{k,\widetilde{m}}$ ($\boldsymbol{G}_{k,\widetilde{n}}$) is the right circulant matrix determined by $\boldsymbol{j}_{k,\widetilde{m}}$ ($\boldsymbol{g}_{k,\widetilde{n}}$) with additional zeros, and the additive noise vectors are $\boldsymbol{z}^{\mathrm{E},k,1} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$ and $\boldsymbol{z}^{\mathrm{E},k,2} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2\boldsymbol{I}_B)$. Note that (4) and (5) indicate that the intercept capability of E_k is constrained by its eavesdropping probability that specifies $\mathbb{I}_k$ in the first and second time phases, respectively.

III. Derivation of the SNRs

In the main channel, considering an arbitrary end-to-end link $T_m \rightarrow R_n \rightarrow D$, $\forall m$, $\forall n$, the corresponding end-to-end SNR with DF relaying is given by

$$\lambda^{T_mR_nD} \triangleq \min(\lambda^{T_mR_n}, \lambda^{R_nD}), \tag{6}$$

where $\lambda_{T_mR_n}$ and λ_{R_nD} are the SNRs of the $T_m \rightarrow R_n$ and $R_n \rightarrow D$ links, respectively, which can be derived from (1) and (2) as

$$\lambda^{T_mR_n} \triangleq \frac{\bar{P}\rho_{h,n,m}\mathbb{B}_m||\boldsymbol{h}_{n,m}||^2}{\sigma_n^2} \triangleq \bar{P}\widetilde{\rho}_{h,n,m}\mathbb{B}_m||\boldsymbol{h}_{n,m}||^2 \tag{7}$$

and

$$\lambda^{R_nD} \triangleq \frac{P_R\rho_{f,n}||\boldsymbol{f}_n||^2}{\sigma_n^2} \triangleq P_R\widetilde{\rho}_{f,n}||\boldsymbol{f}_n||^2, \tag{8}$$

where $\widetilde{\rho}_{h,n,m} \triangleq \rho_{h,n,m}/\sigma_n^2$ and $\widetilde{\rho}_{f,n} \triangleq \rho_{f,n}/\sigma_n^2$. Based on the joint transmitter-relay pair selection in (3), the end-to-end SNR of the main channel with DF relaying can be written as

$$\begin{aligned}\lambda^{\mathrm{DF}} &= \max_{\forall m,\forall n}\left(\lambda^{T_mR_nD}\right)\\ &= \max_{\forall m,\forall n}\left(\min\left(\lambda^{T_mR_n},\lambda^{R_nD}\right)\right).\end{aligned} \tag{9}$$

In the eavesdropper channel, based on (4)-(5), the received SNRs at E_k in the first and second time phases can be respectively expressed as

$$\lambda^{\mathrm{E},k,1} \triangleq \bar{P}\widetilde{\rho}_{j,k,\widetilde{m}}\mathbb{I}_k\mathbb{B}_{\widetilde{m}}||\boldsymbol{j}_{k,\widetilde{m}}||^2 \tag{10}$$

and

$$\lambda^{\mathrm{E},k,2} \triangleq P_R\widetilde{\rho}_{g,k,\widetilde{n}}\mathbb{I}_k||\boldsymbol{g}_{k,\widetilde{n}}||^2, \tag{11}$$

where $\widetilde{\rho}_{j,k,\widetilde{m}} \triangleq \rho_{j,k,\widetilde{m}}/\sigma_n^2$ and $\widetilde{\rho}_{g,k,\widetilde{n}} \triangleq \rho_{g,k,\widetilde{n}}/\sigma_n^2$. To maximize the total received SNR, the eavesdroppers collaboratively detect their receptions by applying MRC across all the received signals from the transmitter $T_{\widetilde{m}}$ and relay $R_{\widetilde{n}}$ over two consecutive time phases. Thus, the received SNR with MRC across all the K eavesdroppers can be expressed as

$$\begin{aligned}\lambda^{\mathrm{E}} &= \sum_{k=1}^{K}\left(\lambda^{\mathrm{E},k,1}+\lambda^{\mathrm{E},k,2}\right)\\ &\triangleq \sum_{k=1}^{2K}\widetilde{\mathbb{I}}_k\widetilde{\lambda}^{\mathrm{E},k},\end{aligned} \tag{12}$$

where

$$\widetilde{\mathbb{I}}_k \triangleq \begin{cases}\mathbb{I}_k\mathbb{B}_{\widetilde{m}}, & k=1,2,\ldots,K\\ \mathbb{I}_{k-K}, & k=K+1,K+2,\ldots,2K\end{cases} \tag{13}$$

and

$$\widetilde{\lambda}^{\mathrm{E},k} \triangleq \begin{cases}\bar{P}\widetilde{\rho}_{j,k,\widetilde{m}}||\boldsymbol{j}_{k,\widetilde{m}}||^2, & k=1,2,\ldots,K\\ P_R\widetilde{\rho}_{g,k-K,\widetilde{n}}||\boldsymbol{g}_{k,\widetilde{n}}||^2, & k=K+1,K+2,\ldots,2K.\end{cases} \tag{14}$$

It is interesting to point out that previous works on the security of two-hop relaying have considered the following two simpler interception schemes: 1) the eavesdroppers only intercept the transmissions from the selected relay and ignore the source transmitter in [35]–[37]; 2) only a single eavesdropper with the highest receive SNR is adopted for selection combining (SC) in [35]–[38] and the signals intercepted by all the other eavesdroppers are ignored. Compared to the SC schemes that only intercept the relay transmission, the considered eavesdropping scheme applies MRC to combine the signals intercepted by all the eavesdroppers from both the source transmitter and relay, which provides a significant advance in the literature representing a worse case scenario for secure communications in two-hop relaying systems. Note that a DF relay can enhance the secrecy performance by sending independent codewords with respect to source messages, which prohibits the eavesdropping MRC from combining both the source and relay transmissions [49]. The considered eavesdropping MRC model in (12) can be also applied to the scenarios of [49] by setting $\widetilde{\mathbb{I}}_k = 0$ for $k = 1,2,\ldots,K$ or $\widetilde{\mathbb{I}}_k = 0$ for $k = K+1,K+2,\ldots,2K$ for wiretapping only the source or relay transmissions.

A. Statistical Properties of the SNRs

In this subsection, we derive the statistical distributions of λ^{DF} and λ^{E}, respectively. Applying the properties of the right circulant channel matrix for CP-SC transmissions, it can be shown that the SNR λ^{R_nD} follows a chi-squared distribution with degrees of freedom (DoF) determined by the number of multipath components [27], given by

$$\lambda^{R_nD} \sim \chi^2(2L_{f,n}, P_R\widetilde{\rho}_{f,n}), \tag{15}$$

where the DoF is denoted by $2L_{f,n}$ and the power normalization constant is denoted by $P_R\widetilde{\rho}_{f,n}$. For a RV $\lambda \sim \chi^2(2L_a,\eta_a)$, its PDF and CDF are respectively given by

$$f_\lambda(x;L_a,\eta_a) = \frac{1}{\Gamma(L_a)(\eta_a)^{L_a}}x^{L_a-1}e^{-\frac{x}{\eta_a}} \tag{16}$$

and

$$F_\lambda(x;L_a,\eta_a) = 1-e^{-\frac{x}{\eta_a}}\sum_{t=0}^{L_a-1}\frac{1}{t!}\left(\frac{x}{\eta_a}\right)^t. \tag{17}$$

Proposition 1. *An exact closed-form expression for the CDF of the end-to-end SNR of the main channel, λ^{DF} in* (9)*, is given by*

$$\begin{aligned}F_{\lambda^{\mathrm{DF}}}(x) = 1+\left(1-\prod_{m=1}^{M}(1-p_m)\right)\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi+1}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi\\ \times e^{-(\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi)x}x^{\widetilde{\beta}_\ell+\widehat{\beta}_\varphi}.\end{aligned} \tag{18}$$

Proof: See Appendix A. ∎

For finite-sized in-band selective relaying with unreliable backhauls, the expression in (18) is a new closed-form expression for the CDF of the end-to-end SNR, which is valid for a wide range of scenarios with non-identical backhaul reliabilities, non-identical frequency-selective fading channels, and arbitrary number of transmitters and relays.

To derive the distribution of the eavesdropper channel SNR λ^E in (12), we first note that $\widetilde{\mathbb{I}}_k$ in (13) is a Bernoulli RV satisfying $\Pr\left(\widetilde{\mathbb{I}}_k=1\right)=\widetilde{q}_k$ and $\Pr\left(\widetilde{\mathbb{I}}_k=0\right)=1-\widetilde{q}_k$ with

$$\widetilde{q}_k \triangleq \begin{cases}p_{\widetilde{m}}q_k, & k=1,2,\ldots,K\\ q_{k-K}, & k=K+1,K+2,\ldots,2K.\end{cases} \tag{19}$$

For $k=1,\ldots,K$, $\widetilde{\mathbb{I}}_k$ is a product of two independent Bernoulli processes specified by the probability $\widetilde{q}_k$, which is the product of the backhaul reliability, $p_{\widetilde{m}}$, and the eavesdropping probability, q_k. Moreover, it can be shown that $\widetilde{\lambda}^{\mathrm{E},k}$ in (14) is distributed according to $\widetilde{\lambda}^{\mathrm{E},k} \sim \chi^2(2L_{e,k},\eta_{e,k})$ with

$$L_{e,k} = \begin{cases}L_{j,k,\widetilde{m}}, & k=1,2,\ldots,K\\ L_{g,k-K,\widetilde{n}}, & k=K+1,K+2,\ldots,2K\end{cases} \tag{20}$$

and

$$\eta_{e,k} = \begin{cases}\bar{P}\widetilde{\rho}_{j,k,\widetilde{m}}, & k=1,2,\ldots,K\\ P_R\widetilde{\rho}_{g,k-K,\widetilde{n}}, & k=K+1,K+2,\ldots,2K.\end{cases} \tag{21}$$

Based on (20) and (21), the PDF $f_{\widetilde{\lambda}^{\mathrm{E},k}}(x)$ of $\widetilde{\lambda}^{\mathrm{E},k}$ can be obtained by substituting $\{L_a, \eta_a\} = \{L_{e,k}, \eta_{e,k}\}$ into (16).

Next, we introduce a RV

$$\widetilde{X}^{\boldsymbol{C}_k^n(\tau,:)} \triangleq \widetilde{\lambda}^{\mathrm{E},\boldsymbol{C}_k^n(\tau,1)} + \ldots, \widetilde{\lambda}^{\mathrm{E},\boldsymbol{C}_k^n(\tau,k)}, \tag{22}$$

where $2 \leq k \leq n$ and $1 \leq \tau \leq \binom{n}{k}$. Note that $\widetilde{X}^{\boldsymbol{C}_k^n(\tau,:)}$ is the summation of k independent chi-squared RVs, while each RV $\lambda^{\mathrm{E},\boldsymbol{C}_k^n(\tau,i)}$ $(i = 1, \ldots, k)$ also follows the gamma distribution with the shape factor $L_{e,\boldsymbol{C}_k^n(\tau,i)}$ and the scale factor $\eta_{e,\boldsymbol{C}_k^n(\tau,i)}$. As such, we can write the PDF and CDF of $\widetilde{X}^{\boldsymbol{C}_k^n(\tau,:)}$ as [50]

$$f_{\widetilde{X}^{\boldsymbol{C}_k^n(\tau,:)}}(x) = \sum_{i \in \boldsymbol{C}_k^n(\tau,:)} \sum_{j=1}^{L_{e,i}} \Xi_{i,j} f_\lambda(x; j, \eta_{e,i}) \tag{23}$$

and

$$F_{\widetilde{X}^{\boldsymbol{C}_k^n(\tau,:)}}(x) = \sum_{i \in \boldsymbol{C}_k^n(\tau,:)} \sum_{j=1}^{L_{e,i}} \Xi_{i,j} F_\lambda(x; j, \eta_{e,i}), \tag{24}$$

where $f_\lambda(x; j, \eta_{e,i})$ and $F_\lambda(x; j, \eta_{e,i})$ are given by (16) and (17), respectively. Denoting $\bar{L}_{e,i} \triangleq L_{e,\boldsymbol{C}_k^n(\tau,i)}$ and $\bar{\eta}_{e,i} \triangleq \eta_{e,\boldsymbol{C}_k^n(\tau,i)}$, the coefficient $\Xi_{i,j}$ in (23) and (24) can be expressed as [50]

$$\begin{aligned}
\Xi_{i,j} = \sum_{\ell_1=j}^{\bar{L}_{e,i}} \sum_{\ell_2=j}^{\ell_1} \cdots \sum_{\ell_{k-2}=j}^{\ell_{k-3}} \Bigg[& \frac{(-1)^{\bar{L}_e - \bar{L}_{e,i}} \bar{\eta}_{e,i}^j}{\bar{\eta}_e} \\
& \times \frac{(\bar{L}_{e,i} + \bar{L}_{e,1+U(1-i)} - \ell_1 - 1)!}{(\bar{L}_{e,1+U(1-i)} - 1)!(\bar{L}_{e,i} - \ell_1)!} \\
& \left(\frac{1}{\bar{\eta}_{e,i}} - \frac{1}{\bar{\eta}_{e,1+U(1-i)}}\right)^{\ell_1 - \bar{L}_{e,i} - \bar{L}_{e,1+U(1-i)}} \\
& \times \frac{(\ell_{k-2} + \bar{L}_{e,k-1+U(k-1-i)} - j - 1)!}{(\bar{L}_{e,k-1+U(k-1-i)} - 1)!(\ell_{k-2} - j)!} \\
& \times \left(\frac{1}{\bar{\eta}_{e,i}} - \frac{1}{\bar{\eta}_{k-1+U(k-1+i)}}\right)^{j - \ell_{k-2} - \bar{L}_{e,k-1+U(k-1-i)}} \\
& \times \prod_{s=1}^{k-3} \frac{(\ell_s + \bar{L}_{e,s+1+U(s+1-i)} - \ell_{s+1} - 1)!}{(\bar{L}_{e,s+1+U(s+1-i)} - 1)!(\ell_s - \ell_{s+1})!} \\
& \times \left(\frac{1}{\bar{\eta}_{e,i}} - \frac{1}{\bar{\eta}_{e,s+1+U(s+1-i)}}\right)^{\ell_{s+1} - \ell_s - \bar{L}_{e,s+1+U(s+1-i)}} \Bigg].
\end{aligned} \tag{25}$$

Since the selective relaying strategy chooses the transmitter-relay pair $(\widetilde{m}, \widetilde{n})$ according to (3), which corresponds to a random selection of the transmitter-relay pairs from the point of the view of the eavesdroppers, the evaluation of the statistics of the exact SNR of the eavesdropping channel is only tractable by considering identical backhaul reliability and identical frequency-selective fading for the channels $\boldsymbol{j}_{k,m}$ with $\forall m$ and identical frequency-selective fading for $\boldsymbol{g}_{k,n}$ with $\forall n$ but non-identical frequency-selective fading channels between the $T_m \to R_n$ and $R_n \to D$ links. This assumption will be relaxed to non-identical backhaul reliabilities and non-identical frequency-selective fading channels across all the links for the asymptotic SNR analysis in Section IV.

Proposition 2. *The PDF and CDF of the received SNR of the eavesdropping channel with MRC across K eavesdroppers and over two consecutive time phases are given by*

$$\begin{aligned}
f_{\lambda^{\mathrm{E}}}(x) = \delta(x) & \prod_{k=1}^{2K} (1 - \widetilde{q}_k) \\
& + \sum_{\tau=1}^{\binom{2K}{1}} w_{1,\tau} f_\lambda\Big(x; L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}, \eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}\Big) \\
& + \sum_{k=2}^{2K} \sum_{\tau=1}^{\binom{2K}{k}} \sum_{i \in \boldsymbol{C}_k^{2K}(\tau,:)} \sum_{j=1}^{L_{e,i}} w_{k,\tau} f_\lambda(x; j, \eta_{e,i})
\end{aligned} \tag{26}$$

and

$$\begin{aligned}
F_{\lambda^{\mathrm{E}}}(x) = & \prod_{k=1}^{2K} (1 - \widetilde{q}_k) \\
& + \sum_{\tau=1}^{\binom{2K}{1}} w_{1,\tau} F_\lambda\Big(x; L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}, \eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}\Big) \\
& + \sum_{k=2}^{2K} \sum_{\tau=1}^{\binom{2K}{k}} \sum_{i \in \boldsymbol{C}_k^{2K}(\tau,:)} \sum_{j=1}^{L_{e,i}} w_{k,\tau} F_\lambda(x; j, \eta_{e,i}),
\end{aligned} \tag{27}$$

respectively, where $w_{k,\tau}$ is given by (28) *at the next page.*

Proof: See Appendix B. ∎

The closed-form PDF and CDF of the eavesdropper channel SNR λ^{E} in Proposition 2 explicitly reflects the contributions from all K eavesdroppers with MRC and the constraints from the eavesdropping probability and backhaul reliability in $\tilde{q}_k$.

IV. Secrecy Performance Analysis

In this section, based on the statistical distributions of the end-to-end SNRs in Propositions 1 and 2, we proceed to analyze the secrecy performance of finite-sized selective relaying systems with unreliable backhauls and frequency-selective fading. Specifically, we focus on the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate. A security advantage is achieved due to the fact that the transmitter-relay pair selection based on the main channel is random with respect to the eavesdropping channels.

We first analyze the secrecy performance with identical backhaul reliability and identical frequency-selective fading for the eavesdropping channels $\boldsymbol{j}_{k,m}$, $\forall m$ and $\boldsymbol{g}_{k,n}$, $\forall n$, respectively. However, all the main channel links in the system are assumed to be non-identical frequency-selective fading. Finally, we derive the asymptotic secrecy performance limits under non-identical backhaul reliabilities and non-identical frequency-selective fading across all the links in the high SNR region.

The maximum achievable rates of the main channel and eavesdropping channel are respectively given by

$$\mathcal{C}_{\mathrm{DF}} = \frac{1}{2}\log_2(1 + \lambda^{\mathrm{DF}}) \text{ and } \mathcal{C}_{\mathrm{E}} = \frac{1}{2}\log_2(1 + \lambda^{\mathrm{E}}), \tag{29}$$

$$w_{k,\tau} \triangleq \begin{cases} \widetilde{q}_{\boldsymbol{C}_k^{2K}(\tau,1)} \cdots \widetilde{q}_{\boldsymbol{C}_k^{2K}(\tau,k)} \Big(1-\widetilde{q}_{\bar{\boldsymbol{C}}_k^{2K}(\tau,1)}\Big) \cdots \Big(1-\widetilde{q}_{\bar{\boldsymbol{C}}_k^{2K}(\tau,2K-k)}\Big), & 1 \le k < 2K \\ \widetilde{q}_{\boldsymbol{C}_{2K}^{2K}(1,1)} \cdots \widetilde{q}_{\boldsymbol{C}_{2K}^{2K}(1,2K)}, & k = 2K \end{cases} \tag{28}$$

where the pre-log factor $\frac{1}{2}$ is due to the half-duplex relaying. Substituting (29) into $\mathcal{C}_{\rm s} = \big[\mathcal{C}_{\rm DF} - \mathcal{C}_{\rm E}\big]^+$, the secrecy rate of the main channel can be expressed as [51]–[53]

$$\mathcal{C}_{\rm s} = \frac{1}{2}\bigg[\log_2\bigg(\frac{1+\lambda^{\rm DF}}{1+\lambda^{\rm E}}\bigg)\bigg]^+. \tag{30}$$

A. Identical Backhaul Reliability

Based on the closed-form expressions in (18), (26), and (27), we present the following secrecy performance analysis for finite-sized in-band selective relaying systems with identical backhaul reliability.

1) Secrecy Outage Probability: A secrecy outage event occurs when the secrecy rate of the main channel in (30) is less than a target secrecy rate $\mathcal{R} > 0$ [28], [29], [53].

$$\begin{aligned} P_{\rm out} &= \Pr(\mathcal{C}_{\rm s} < \mathcal{R}) \\ &= \int_0^\infty F_{\lambda^{\rm DF}}\big(J_R(1+x)-1\big) f_{\lambda^{\rm E}}(x){\rm d}x, \end{aligned} \tag{31}$$

where $J_R \triangleq 2^{2\mathcal{R}}$.

Theorem 1. *The secrecy outage probability of a finite-sized in-band selective relaying system wiretapped by multiple eavesdroppers under unreliable backhauls and non-identical frequency-selective fading is given by* (32) *at the next page.*

Proof: Substituting (18) and (26) into (31), we expand the term $(J_R - 1 + J_R x)^{\widetilde{\beta}_\ell + \widehat{\beta}_\varphi}$ in the integral according to

$$(J_R - 1 + J_R x)^{\widetilde{\beta}_\ell + \widehat{\beta}_\varphi} = \sum_{\upsilon=0}^{\widetilde{\beta}_\ell + \widehat{\beta}_\varphi} (J_R - 1)^{\widetilde{\beta}_\ell + \widehat{\beta}_\varphi - \upsilon} J_R^\upsilon x^\upsilon. \tag{33}$$

Applying the series expansion in (33), we solve the resulting integral using the identity $\int_0^\infty x^a e^{-cx^b} = \Gamma((a+1)/b)/(bc^{(a+1)/b})$ [54, 3.326/2] to derive the result in (32). ∎

Theorem 1 provides a general analytical framework for evaluating the secrecy outage probability of a finite-sized in-band selective relaying system. The joint impact on the secrecy outage probability of the transmitter-relay cooperation under unreliable backhauls and the eavesdropping collaboration with MRC across K eavesdroppers and over two time slots is explicitly characterized in (32). Compared to the approximate outage probability of the idealized linear system model of selective relaying with equal numbers of transmitters and relays [45], Theorem 1 provides a new closed-form secrecy outage probability expression for selective relaying with arbitrary degrees of transmitter-relay cooperation and eavesdropper collaboration under frequency-selective fading channels. Moreover, (32) shows that an increasing $\widetilde{q}_k$ corresponds to an explicit decreasing for the term $F_{\lambda^{\rm DF}}(J_R-1)\prod_{k=1}^{2K}(1-\widetilde{q}_k)$ in $P_{\rm out}$, while the joint impact of the backhaul reliability and eavesdropping probability on $P_{\rm out}$ is additionally characterized as the term $\sum_{k=1}^{2K}\sum_{\tau=1}^{\binom{2K}{k}} w_{k,\tau}$. When simultaneous perfect backhaul connections and perfect eavesdropper cooperation occur, we have $\prod_{k=1}^{2K}(1-\widetilde{q}_k)=0$ and $\prod_{m=1}^{M}(1-p_m)=0$, with which the corresponding $P_{\rm out}$ can be obtained from (32).

As a special case of the secrecy outage probability, the probability of non-zero achievable secrecy rate of a finite-sized in-band selective relaying system wiretapped by multiple eavesdroppers under unreliable backhauls and non-identical frequency-selective fading can be evaluated as [53]

$$\Pr(\mathcal{C}_{\rm s} > 0) = \int_0^\infty \bar{F}_{\lambda^{\rm DF}}(x) f_{\lambda^{\rm E}}(x){\rm d}x, \tag{34}$$

which is evaluated as (35) at the next page. In (34), $\bar{F}_{\lambda^{\rm DF}}(x) = 1 - F_{\lambda^{\rm DF}}(x)$ can be easily extracted from (18).

In (35), the term $1-\prod_{m=1}^{M}(1-p_m)$ explicitly shows that an increasing backhaul reliability results in an increasing $\Pr(\mathcal{C}_{\rm s} > 0)$, while the term $\prod_{k=1}^{2K}(1-\widetilde{q}_k)$ indicates that an increasing eavesdropping probability results in a decreasing $\Pr(\mathcal{C}_{\rm s} > 0)$. Moreover, with simultaneous perfect backhaul connections and perfect eavesdropper cooperation, the first term $\big(1-\prod_{m=1}^{M}(1-p_m)\big)\prod_{k=1}^{2K}(1-\widetilde{q}_k)$ in (35) becomes zero.

2) Ergodic Secrecy Rate: By averaging the instantaneous secrecy rate over the SNR distributions of $\lambda^{\rm DF}$ and $\lambda^{\rm E}$, the ergodic secrecy rate can be expressed as [53]

$$\bar{\mathcal{C}}_{\rm s} = \frac{1}{2\log(2)}\int_0^\infty \frac{\bar{F}_{\lambda^{\rm DF}}(x) F_{\lambda^{\rm E}}(x)}{1+x}{\rm d}x. \tag{36}$$

Theorem 2. *The ergodic secrecy rate of a finite-sized in-band selective relaying system wiretapped by multiple eavesdroppers under unreliable backhauls and non-identical frequency-selective fading channels is given by* (37) *at the next page.*

Proof: Substituting the expressions for $\bar{F}_{\lambda^{\rm DF}}(x)$ and $F_{\lambda^{\rm E}}(x)$ into (36), we solve the integral which results in (37), where $\Psi(a,b;z) = \frac{1}{\Gamma(a)}\int_0^\infty e^{-zt}t^{a-1}(1+t)^{b-a-1}{\rm d}t$ is the confluent hypergeometric function [54, 9.211/4]. ∎

The results in Theorem 2 explicitly consider the backhaul reliability, frequency-selective fading, transmitter-relay cooperation, as well as eavesdropper cooperation, so that Theorem 2 provides a general form for the ergodic secrecy rate. Moreover, (37) shows that an increasing backhaul reliability p_m results in an increasing $1-\prod_{m=1}^{M}(1-P_M)$, which has a tendency for increasing the ergodic secrecy rate as will be verified by the simulations in Section V. For a special case with simultaneous perfect backhaul connections and perfect eavesdropper cooperation, the corresponding ergodic secrecy rate can be obtained by substituting $\prod_{m=1}^{M}(1-p_m)=0$ and $\prod_{k=1}^{2K}(1-\widetilde{q}_k)=0$ into (37).

Proposition 3. *For non-identical frequency-selective fading channels and perfect backhaul connections, the secrecy diver-*

$$P_{\text{out}} = F_{\lambda^{\text{DF}}}(J_R-1)\prod_{k=1}^{2K}(1-\widetilde{q}_k) + \sum_{k=1}^{2K}\sum_{\tau=1}^{\binom{2K}{k}} w_{k,\tau} + \left(1-\prod_{m=1}^{M}(1-p_m)\right)\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi+1}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi \sum_{\upsilon=0}^{\widetilde{\beta}_\ell+\widehat{\beta}_\varphi}\sum_{\tau=1}^{\binom{2K}{1}}\binom{\widetilde{\beta}_\ell+\widehat{\beta}_\varphi}{\upsilon}$$
$$\times\frac{(J_R-1)^{\widetilde{\beta}_\ell+\widehat{\beta}_\varphi-\upsilon}J_R^{\upsilon}e^{-(\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi)(J_R-1)}w_{1,\tau}\Gamma\Big(L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}+\upsilon\Big)}{\Gamma\Big(L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}\Big)\Big(\eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}\Big)^{L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}}}\left(J_R(\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi)+\frac{1}{\eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}}\right)^{-\left(L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}+\upsilon\right)}$$
$$+\left(1-\prod_{m=1}^{M}(1-p_m)\right)\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi+1}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi\sum_{\upsilon=0}^{\widetilde{\beta}_\ell+\widehat{\beta}_\varphi}\sum_{k=2}^{2K}\sum_{\tau=1}^{\binom{2K}{k}}\sum_{i\in\boldsymbol{C}_k^{2K}(\tau,:)}\sum_{j=1}^{L_{e,i}}\binom{\widetilde{\beta}_\ell+\widehat{\beta}_\varphi}{\upsilon}(J_R-1)^{\widetilde{\beta}_\ell+\widehat{\beta}_\varphi-\upsilon}J_R^{\upsilon}$$
$$\times\frac{e^{-(\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi)(J_R-1)}w_{k,\tau}\Xi_{i,j}\Gamma(j+\upsilon)}{\Gamma(j)(\eta_{e,i})^j}\left(J_R(\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi)+\frac{1}{\eta_{e,i}}\right)^{-(j+\upsilon)}. \tag{32}$$

$$\Pr(\mathcal{C}_{\text{s}}>0) = \left(1-\prod_{m=1}^{M}(1-p_m)\right)\prod_{k=1}^{2K}(1-\widetilde{q}_k) + \left(1-\prod_{m=1}^{M}(1-p_m)\right)\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi\sum_{\tau=1}^{\binom{2K}{1}}$$
$$\frac{w_{1,\tau}\Gamma\Big(L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}+\widetilde{\beta}_\ell+\widehat{\beta}_\varphi\Big)}{\Gamma\Big(L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}\Big)\Big(\eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}\Big)^{L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}}}\left(\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi+\frac{1}{\eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}}\right)^{-\left(L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}+\widetilde{\beta}_\ell+\widehat{\beta}_\varphi\right)}+\left(1-\prod_{m=1}^{M}(1-p_m)\right)$$
$$\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi\sum_{k=2}^{2K}\sum_{\tau=1}^{\binom{2K}{k}}\sum_{i\in\boldsymbol{C}_k^{2K}(\tau,:)}\sum_{j=1}^{L_{e,i}}\frac{w_{k,\tau}\Xi_{i,j}\Gamma(j+\widetilde{\beta}_\ell+\widehat{\beta}_\varphi)}{\Gamma(j)(\eta_{e,i})^j}\left(\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi+\frac{1}{\eta_{e,i}}\right)^{-(j+\widetilde{\beta}_\ell+\widehat{\beta}_\varphi)}. \tag{35}$$

$$\bar{\mathcal{C}}_{\text{s}} = \frac{1}{2\log(2)}\left(1-\prod_{m=1}^{M}(1-p_m)\right)\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi\left(\prod_{k=1}^{2K}(1-\widetilde{q}_k)+\sum_{\tau=1}^{\binom{2K}{1}}w_{1,\tau}+\sum_{k=2}^{2K}\sum_{\tau=1}^{\binom{2K}{k}}\sum_{i\in\boldsymbol{C}_k^{2K}(\tau,:)}\sum_{j=1}^{L_{e,i}}w_{k,\tau}\Xi_{i,j}\right)$$
$$\times\Gamma(\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+1)\Psi\big(\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+1,\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+1;\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi\big)+\frac{1}{2\log(2)}\left(1-\prod_{m=1}^{M}(1-p_m)\right)\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi+1}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi$$
$$\sum_{\tau=1}^{\binom{2K}{1}}\sum_{s=0}^{L_{e,\boldsymbol{C}_1^{2K}(\tau,1)}-1}\frac{w_{1,\tau}}{s!\eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}^s}\Gamma(\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+s+1)\Psi\left(\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+s+1,\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+s+1;\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi+\frac{1}{\eta_{e,\boldsymbol{C}_1^{2K}(\tau,1)}}\right)$$
$$+\frac{1}{2\log(2)}\left(1-\prod_{m=1}^{M}(1-p_m)\right)\widetilde{\sum}\widehat{\sum}(-1)^{\ell+\varphi+1}\widetilde{\Upsilon}_\ell\widehat{\Upsilon}_\varphi\sum_{k=2}^{2K}\sum_{\tau=1}^{\binom{2K}{k}}\sum_{i\in\boldsymbol{C}_k^{2K}(\tau,:)}\sum_{j=1}^{L_{e,i}}\sum_{s=0}^{j-1}\frac{w_{k,\tau}\Xi_{i,j}}{s!\eta_{e,i}^s}\Gamma(\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+s+1)$$
$$\times\Psi\left(\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+s+1,\widetilde{\beta}_\ell+\widehat{\beta}_\varphi+s+1;\widetilde{\alpha}_\ell+\widehat{\alpha}_\varphi+\frac{1}{\eta_{e,i}}\right). \tag{37}$$

sity gain of the finite-sized in-band selective relaying system is given by

$$G_d = \min\left(\sum_{\varphi=1}^{MN}L_{h,\nu(\varphi),\mu(\varphi)},\sum_{n=1}^{N}L_{f,n}\right), \tag{38}$$

where $\mu(\varphi)=\left\lceil\frac{\varphi}{N}\right\rceil$ *and* $\nu(\varphi)=\varphi-\left\lceil\frac{\varphi}{N}-1\right\rceil N$.

Proof: See Appendix C. ∎

Proposition 3 shows that the secrecy diversity gain is jointly determined by M, N, and the number of multi-path components in the $T_m\to R_n$ and $R_n\to D$ links, denoted by $L_{h,\nu(\varphi),\mu(\varphi)}$ and $L_{f,n}$, respectively. The result in (38) shows that the considered system achieves not only transmitter-relay cooperation diversity but also multi-path diversity. We note that the secrecy diversity gain is only affected by the number of transmitters, M, when the summation of the multi-path components in the $T_m\to R_n$ links is less than the summation of the multi-path components in the $R_n\to D$ links. For comparable values of $L_{h,\nu(\varphi),\mu(\varphi)}$ and $L_{f,n}$, it can be inferred from (38) that the secrecy diversity gain is mainly determined by the number of relays, N, besides the corresponding multi-path diversity.

B. Asymptotic Analysis with Non-Identical Backhaul and Frequency Selective Fading

From the point of view of the eavesdroppers, the selected transmitter for transmission is randomly chosen. Consequently, it is hard to trace the closed-form expressions for the statistics of the received SNR λ^{E} with non-identical backhaul and frequency-selective fading. In this part, we provide asymptotic secrecy performance for the case of non-identical backhaul and frequency-selective fading.

When the average path-loss of the eavesdropping channel is much larger than that of the main channel, it has been shown that $P_{\mathrm{out}} = 1$ and $\Pr(\mathcal{C}_{\mathrm{s}} > 0) = 0$ for the conventional secrecy communications [28], [29]. For our considered system, also of interest is the asymptotic behavior of P_{out} and $\Pr(\mathcal{C}_{\mathrm{s}} > 0)$ when the average path-loss of the main channel is much larger than that of the eavesdropping channels, i.e., $\rho_x \gg \rho_y$, $\forall \rho_x \in \{\rho_{h,n,m}, \rho_{f,n}\}$ and $\forall \rho_y \in \{\rho_{j,k,m}, \rho_{g,k,n}\}$.

Theorem 3. *For a fixed SNR in the eavesdropping channels with MRC across multiple eavesdroppers, as the equivalent transmit powers $\bar{P}\rho_{h,\widetilde{n},\widetilde{m}}$ and $P_R\rho_{f,\widetilde{n}}$ approach infinity, the asymptotic limits on the secrecy outage probability and the probability of non-zero achievable secrecy rate are respectively given by*

$$P_{\mathrm{out}}^{as} = \prod_{m=1}^{M} (1 - p_m) \tag{39}$$

and

$$\Pr{}^{as}(\mathcal{C}_{\mathrm{s}} > 0) = 1 - \prod_{m=1}^{M} (1 - p_m). \tag{40}$$

Proof: See Appendix D. ∎

It can be observed from (39) and (40) that asymptotic limits on the secrecy outage probability and probability of non-zero achievable secrecy rate are exclusively determined by the number of transmitters, M, and the corresponding set of backhaul reliability levels, p_m. Conditioned on that $\rho_x \gg \rho_y$, $\forall \rho_x \in \{\rho_{h,n,m}, \rho_{f,n}\}$ and $\forall \rho_y \in \{\rho_{j,k,m}, \rho_{g,k,n}\}$, the results of Theorem 3 show that the number of eavesdroppers and relays do not impact on the asymptotic limits of our finite-sized in-band selective relaying system with unreliable backhauls. In fact, increasing M and p_m directly improves the asymptotic secrecy performance of the system. On the contrary, conditioned on that $\rho_x \ll \rho_y$, we also have $P_{\mathrm{out}} = 1$ and $\Pr(\mathcal{C}_{\mathrm{s}} > 0) = 0$, which are similar to those of the conventional secrecy communications [28], [29]. In the case of identical backhaul reliability $p_m = \bar{p}$, $\forall m$, the asymptotic limits of Theorem 3 can be expressed as $P_{\mathrm{out}}^{as} = (1 - \bar{p})^M$ and $\Pr{}^{as}(\mathcal{C}_{\mathrm{s}} > 0) = 1 - (1 - \bar{p})^M$. For perfect backhaul connections, we can directly infer that $P_{\mathrm{out}}^{as} \to 0$ and $\Pr{}^{as}(\mathcal{C}_{\mathrm{s}} > 0) \to 1$ as $p_m \to 1$. For non-perfect backhaul connections, Theorem 3 indicates that $P_{\mathrm{out}} = 0$ and $\Pr(\mathcal{C}_{\mathrm{s}} > 0) = 1$ cannot be achieved.

V. Simulation Results

In this section, we presents link-level simulation results to validate our analyzed secrecy performance metrics. In the link-level simulations, we apply quadrature phase-shift keying (QPSK) modulation for CP-SC data symbols and set $B = 64$, $\bar{P} = 1$, $P_R = \chi_r \bar{P}$ with $0 < \chi_r < 1$. In all the simulation figures, SNR denotes $\bar{P}/\sigma^2$ while the path-loss components $\rho_{h,n,n}$ and $\rho_{f,n}$ are normalized for the main channel. For the eavesdropping channel, $\lambda^{\mathrm{E},k,1}$ and $\lambda^{\mathrm{E},k,2}$ are scaled with the fixed parameters $\{\bar{P}\widetilde{\rho}_{j,1,m}, \bar{P}\widetilde{\rho}_{j,2,m}, \bar{P}\widetilde{\rho}_{j,3,m}\} = 3$ dB $\times \{1, 1.2, 1.3\}$ and $\{P_R\widetilde{\rho}_{g,1,n}, P_R\widetilde{\rho}_{g,2,n}, P_R\widetilde{\rho}_{g,3,n}\} = 3$ dB $\times \{1.1, 1.25, 1.35\}$, respectively. For notational convenience, the link-level simulation results are denoted by "Ex", while the analytical results are denoted by "An". The analytical secrecy outage probability and ergodic secrecy rate under perfect backhauls are denoted by $P_{\mathrm{out}}^{\infty}$ and $\bar{\mathcal{C}}_{\mathrm{s}}^{\infty}$, which are evaluated by substituting $p_m = 1$, $\forall m$ into (32) and (37), respectively. To highlight the impact of key design parameters of the finite-sized in-band selective relaying system on the secrecy performance, we consider 4 different scenarios, i.e., S_1, S_2, S_3,

TABLE II
Simulation Parameters

Parameter	Scenario S_1	Scenario S_2
M	2	{2, 4}
N	2	2
K	{1, 2, 3}	{1, 2, 3}
$[p_1, \ldots, p_M]$	[0.98, 0.98]	[0.92, 0.92, 0.92, 0.92]
$[q_1, \ldots, q_K]$	[0.3, 0.3, 0.5]	[0.3, 0.3, 0.5]
$[L_{f,1}, \ldots, L_{f,N}]$	[2, 3]	[2, 5]
$\begin{bmatrix} L_{h,1,1} & \cdots & L_{h,1,M} \\ \cdots & \ddots & \cdots \\ L_{h,N,1} & \cdots & L_{h,N,M} \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 2 \end{bmatrix}$
$\begin{bmatrix} L_{j,1,1} & \cdots & L_{j,1,M} \\ \cdots & \ddots & \cdots \\ L_{j,K,1} & \cdots & L_{j,K,M} \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 2 & 2 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix}$
$\begin{bmatrix} L_{g,1,1} & \cdots & L_{g,1,N} \\ \cdots & \ddots & \cdots \\ L_{g,K,1} & \cdots & L_{g,K,N} \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 2 & 2 \end{bmatrix}$
Parameter	**Scenario S_3**	**Scenario S_4**
M	4	{2, 4}
N	{2, 4}	{2, 4}
K	{1, 2, 3}	{1, 2, 3}
$[p_1, \ldots, p_M]$	[0.92, 0.92, 0.92, 0.92]	[0.9, 0.9, 0.92, 0.95]
$[q_1, \ldots, q_K]$	[0.3, 0.3, 0.5]	[0.3, 0.3, 0.5]
$[L_{f,1}, \ldots, L_{f,N}]$	[1, 3, 2, 5]	[2, 3, 1, 4]
$\begin{bmatrix} L_{h,1,1} & \cdots & L_{h,1,M} \\ \cdots & \ddots & \cdots \\ L_{h,N,1} & \cdots & L_{h,N,M} \end{bmatrix}$	$\begin{bmatrix} 2 & 2 & 1 & 3 \\ 1 & 2 & 1 & 4 \\ 1 & 5 & 2 & 1 \\ 2 & 1 & 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 & 3 & 2 \\ 1 & 2 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 2 & 2 & 3 & 2 \end{bmatrix}$
$\begin{bmatrix} L_{j,1,1} & \cdots & L_{j,1,M} \\ \cdots & \ddots & \cdots \\ L_{j,K,1} & \cdots & L_{j,K,M} \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 2 & 3 & 2 & 1 \\ 1 & 2 & 1 & 4 \end{bmatrix}$
$\begin{bmatrix} L_{g,1,1} & \cdots & L_{g,1,N} \\ \cdots & \ddots & \cdots \\ L_{g,K,1} & \cdots & L_{g,K,N} \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 & 2 & 1 \\ 3 & 2 & 2 & 1 \\ 2 & 1 & 2 & 4 \end{bmatrix}$

and S_4, and set $\chi_r = 0.1$. Additional simulation parameters are summarized in Table II.

A. Identical Backhaul Reliability and Non-Identical Frequency Selective Fading Channels

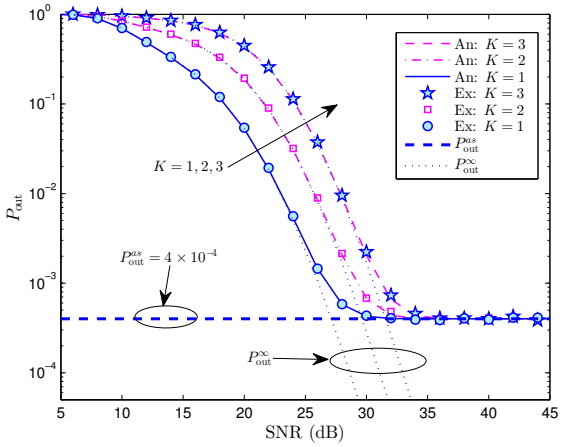

Fig. 2. Secrecy outage probability versus SNR for scenario S_1.

In Fig. 2, we verify the accuracy of the analytical secrecy outage probability and asymptotic secrecy outage probability for scenario S_1 with $M = N = 2$. We see in this figure that, throughout the considered SNR region, the analytical curves match the simulation curves. With increasing SNR, the secrecy outage probability under unreliable backhauls first decreases and then approaches the asymptotic limit P_{out}^{as} in the high SNR region. For scenario S_1, this figure verifies the accuracy of $P_{\text{out}}^{as} = \prod_{m=1}^{M}(1-p_m) = 4\times10^{-4}$ indicating that P_{out}^{as} is exclusively determined by the number of cooperative transmitters and corresponding backhaul reliability. However, under perfect backhaul connections, i.e., $p_m = 1$, $\forall m$, this figure shows that P_{out}^{∞} monotonically decreases with increasing SNR. When the number of collaborative eavesdroppers increases from $K = 1$ to $K = 3$, we find that the secrecy outage probability increases in the low and middle SNR regions, whereas P_{out} achieved by $K = 1$, 2, and 3 converge to the same asymptotic limit $P_{\text{out}}^{as} = 4\times10^{-4}$ in the high SNR region.

In Fig. 3, we plot the secrecy outage probability versus SNR for scenario S_2 with $M = 2$, 4, and $N = 2$. When the number of cooperative transmitters increases from $M = 2$ to $M = 4$, this figure shows that the asymptotic limit P_{out}^{as} decreases from $P_{\text{out}}^{as} = 6.4\times10^{-3}$ to $P_{\text{out}}^{as} = 4.1\times10^{-5}$. Thus, increasing transmitters cooperation results in a lower asymptotic secrecy outage probability as proven by Theorem 3. Moreover, we see in this figure that the secrecy outage probabilities achieved by $M = 2$ and $M = 4$ have the same slope in the low and middle SNR regions due to the sharing of the same N and the summation of multi-path components in the $R_n \to D$ links. Note that in this scenario, the secrecy diversity gain is determined by N and corresponding number of multipath components $L_{f,n}$. Thus, increasing transmitter cooperation in this scenario does not increase the diversity. Similar to Fig. 2, Fig. 3 shows that increasing eavesdroppers collaboration

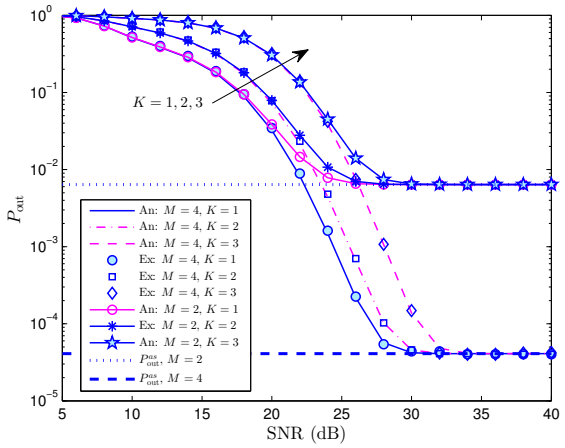

Fig. 3. Secrecy outage probability versus SNR for scenario S_2.

increases the secrecy outage probability in the low and middle SNR regions; while in the high SNR region, the secrecy outage probability is exclusively limited by the backhaul reliability, p_m, and transmitter cooperation, M.

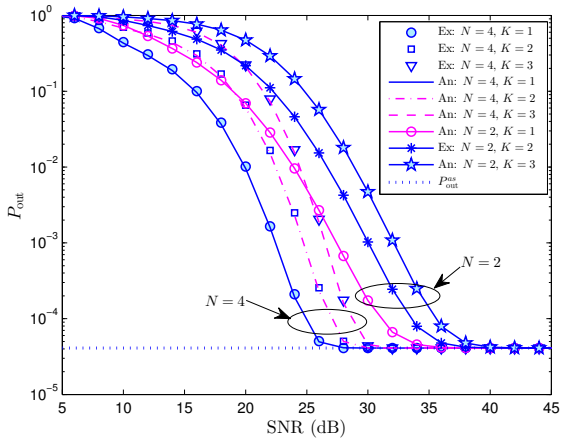

Fig. 4. Secrecy outage probability versus SNR for scenario S_3.

The secrecy outage probability versus SNR for scenario S_3 is depicted in Fig. 4, where we set $M = 2$ and $N = 2$ and 4. With increasing number of cooperative relays from $N = 2$ to $N = 4$, Fig. 4 shows that the secrecy outage probability curves achieve the increased secrecy diversity gain resulting from relay cooperation. At the P_{out} level of 10^{-4}, this figure shows that $N = 4$ achieves an approximately 6 dB SNR gain over $N = 2$. Furthermore, both $N = 2$ and $N = 4$ achieve the same asymptotic limit $P_{\text{out}}^{as} = 4.1\times10^{-5}$, which verifies that increasing relay cooperation does not change the asymptotic secrecy outage probability in the high SNR region as proven by Theorem 3. It should be pointed out that, as verified by Figs. 2-4, the eavesdropper cooperation does not affect the secrecy diversity gain and asymptotic P_{out}^{as}, which are consistent with Proposition 3 and Theorem 3.

In Fig. 5, we verify the accuracy of the analytical probability of non-zero achievable secrecy rate and corresponding asymptotic limit for scenario S_1, where we consider two

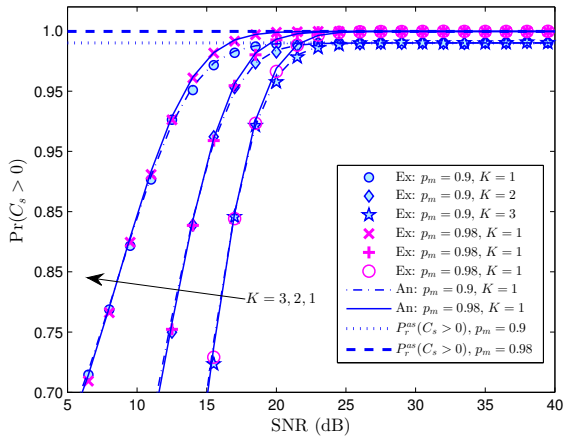

Fig. 5. $\Pr(\mathcal{C}_\mathrm{s} > 0)$ versus SNR for scenario S_1.

cases of backhaul reliability, i.e., $p_m = 0.9$ and $p_m = 0.98$, respectively. The accuracy of the analytical $\Pr(\mathcal{C}_\mathrm{s} > 0)$ has been verified by the curves in Fig. 5. With increasing SNR, we see that the probability of non-zero achievable secrecy rate under unreliable backhauls first increases and then approaches the asymptotic limits $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0)$ in the high SNR region. For scenario S_1, this figure also verifies the accuracy of $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0) = 1 - \prod_{m=1}^{M}(1 - p_m)$. For $p_m = 0.9$ and $p_m = 0.98$, this figure confirms that $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0) = 0.99$ and $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0) = 0.9996$, respectively. Thus, increasing backhaul reliability results in improved $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0)$. With increasing eavesdroppers collaboration from $K = 1$ to $K = 3$, Fig. 5 shows that $\Pr(\mathcal{C}_\mathrm{s} > 0)$ decreases in the low and middle SNR regions. However, in the high SNR region, the probabilities of non-zero achievable rate for $K = 1$, 2, and 3 converge to the same asymptotic limit, which is exclusively determined by the backhaul reliability and transmitter cooperation.

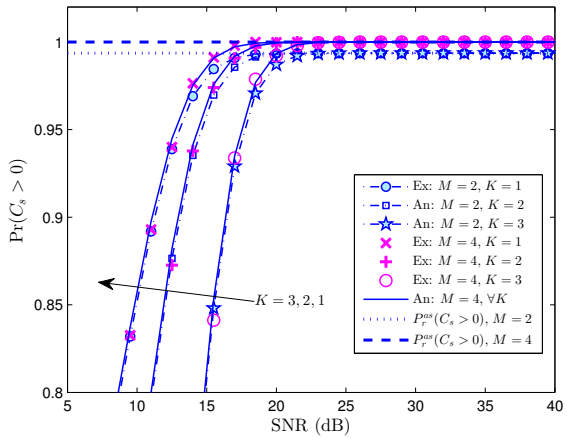

Fig. 6. $\Pr(\mathcal{C}_\mathrm{s} > 0)$ versus SNR for scenario S_2.

In Fig. 6, we investigate the probability of non-zero achievable secrecy rate versus SNR for scenario S_2 with $M = 2$, 4, and $N = 2$. By increasing transmitter cooperation $M = 2$ to $M = 4$, Fig. 6 shows that the asymptotic limits $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0)$ increases from $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0) = 0.9936$ to $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0) \approx 1$. Therefore, increasing transmitter cooperation results in a higher asymptotic probability of non-zero achievable rate. Furthermore, this figure confirms that the probabilities of non-zero achievable rate for $M = 2$ and $M = 4$ have the same slope before they approach the asymptotic limits. As a result, the secrecy diversity gain is not affected by transmitter cooperation since the secrecy diversity gain is determined by N and $L_{f,n}$ in this scenario. This figure also shows that $\Pr(\mathcal{C}_\mathrm{s} > 0)$ decreases with increasing eavesdropper collaboration from $K = 1$ to $K = 3$ in the low and middle SNR regions; while in the high SNR region, $\Pr(\mathcal{C}_\mathrm{s} > 0)$ is exclusively determined by the backhaul reliability.

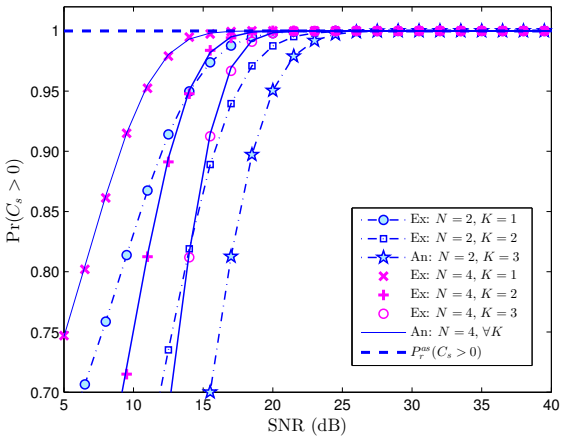

Fig. 7. $\Pr(\mathcal{C}_\mathrm{s} > 0)$ versus SNR for scenario S_3.

The probability of non-zero achievable secrecy rate versus SNR for scenario S_3 is depicted in Fig. 7, where we set $M = 2$ and $N = 2$, 4. With increasing number of cooperative relays from $N = 2$ to $N = 4$, this figure shows that the probabilities of non-zero achievable secrecy rate obtain the increased secrecy diversity gain resulting from relay cooperation, i.e., the $\Pr(\mathcal{C}_\mathrm{s} > 0)$ achieved by $N = 4$ has a more upward slope than that of $N = 2$. Moreover, this figure shows that $N = 2$ and $N = 4$ achieve the same asymptotic limit $\Pr^{as}(\mathcal{C}_\mathrm{s} > 0) \approx 1$ in the high SNR region, which verifies that increasing relay cooperation does not affect the asymptotic probability of non-zero achievable secrecy rate in the high SNR region.

In Fig. 8, we plot the ergodic secrecy rate versus SNR for scenario S_3, where we consider $p_m = 0.7$ and $p_m = 0.8$. This figure verifies the accuracy of the analytical $\bar{\mathcal{C}}_\mathrm{s}$. Compared to the case of perfect backhaul connections, this figure shows the ergodic secrecy rate for different values of backhaul connections. As SNR increases, a larger gap of the ergodic secrecy rate can be observed reflecting that the backhaul reliability influences the performance. By increasing transmitter-relay cooperation from $\{M = 2, N = 2\}$ to $\{M = 4, N = 4\}$, the ergodic secrecy rate also increases. Furthermore, it can be seen that the ergodic gap between unreliable backhaul and perfect backhaul becomes insignificant for $\{M = 4, N = 4\}$ compared to $\{M = 2, N = 2\}$. Thus, increasing transmitter-relay cooperation can effectively combat the negative effect of unreliable backhaul on the ergodic secrecy rate. Fig. 8 also shows that the ergodic secrecy rate decreases with increasing

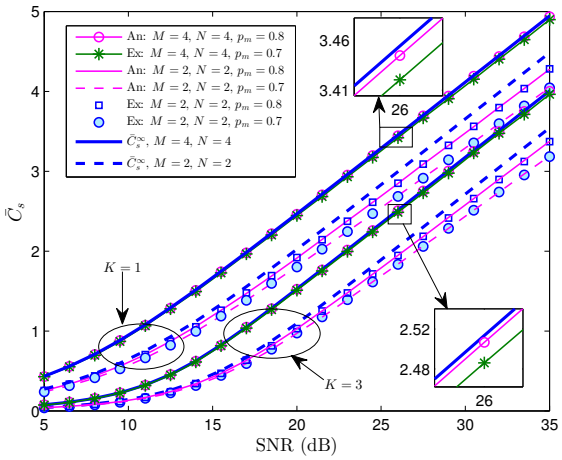

Fig. 8. Ergodic secrecy rate for scenario S_3.

eavesdropper collaboration from $K=1$ to $K=3$.

B. Non-Identical Backhaul Reliability and Frequency-Selective Fading Channels

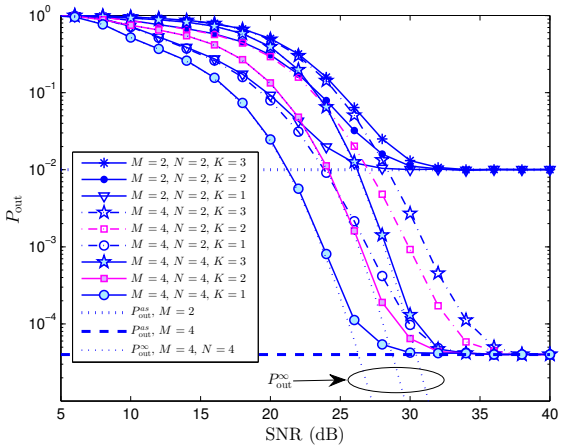

Fig. 9. Secrecy outage probability for scenario S_4.

Fig. 9 plots the secrecy outage probability versus SNR for scenario S_4. Under non-identical backhaul reliability, this figure shows that the asymptotic limit of secrecy outage probability is exclusively determined by backhaul reliability and the number of transmitters, while the secrecy diversity is determined by the number of relays and the summation of $L_{f,n}$ in this scenario. By increasing transmitter cooperation from $M=2$ to $M=4$, this figure shows that the asymptotic limit decreases from $P_{\text{out}}^{as}=1.0\times10^{-2}$ to $P_{\text{out}}^{as}=4.0\times10^{-5}$, according to our derived expression $P_{\text{out}}^{as}=\prod_{m=1}^{M}(1-p_m)$. For the achieved secrecy diversity, Fig. 9 shows that $N=4$ results in a more downward slope than that of $N=2$. As eavesdropper collaboration increases, the secrecy outage probability increases in the low and middle SNR regions, while the secrecy outage probability converges to P_{out}^{as} in the high SNR region irrespective of the number of eavesdroppers.

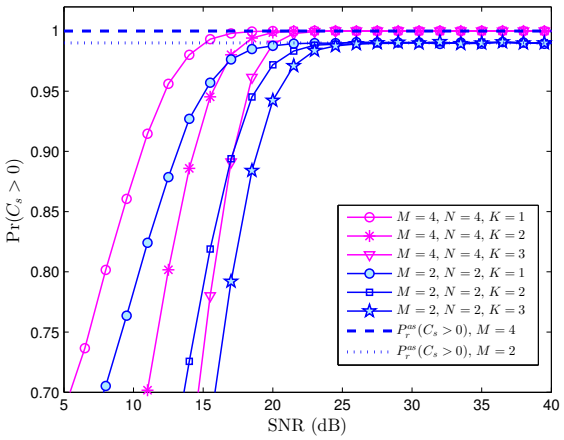

Fig. 10. Probability of non-zero achievable secrecy rate versus SNR.

In Fig. 10, the probability of non-zero achievable secrecy rate versus SNR for scenario S_4 is depicted. It can be readily seen that the diversity is influenced by the number of relays, while the asymptotic limit on the probability of non-zero achievable secrecy rate is determined by $\Pr^{as}(\mathcal{C}_{\text{s}}>0)=1-\prod_{m=1}^{M}(1-p_m)$, which is affected by both the backhaul reliability and the number of transmitters. Moreover, the probability of non-zero achievable secrecy rate decreases with increasing eavesdropper collaboration in the low and middle SNR regions; while in the high SNR region, $\Pr(\mathcal{C}_{\text{s}}>0)$ approaches the asymptotic limit $\Pr^{as}(\mathcal{C}_{\text{s}}>0)=1-\prod_{m=1}^{M}(1-p_m)$.

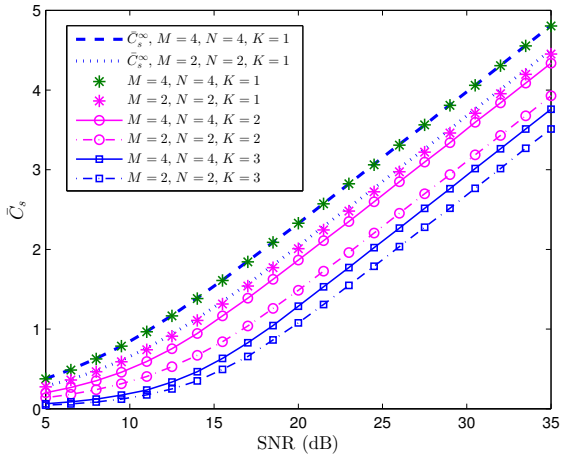

Fig. 11. Ergodic secrecy rate versus SNR.

In Fig. 11, we plot the ergodic secrecy rate versus SNR for scenario S_4 considering non-identical backhaul reliability. When the number of eavesdroppers increases from $K=1$ to $K=3$, this figure shows that the ergodic secrecy rate decreases. As $\bar{P}/\sigma^2$ increases, the gap between the ergodic secrecy rates under perfect and unreliable backhauls also increases. This figure also shows that by increasing transmitter-relay cooperation, a higher ergodic secrecy rate can be achieved. Moreover, the ergodic secrecy rate gap between unreliable and perfect backhauls becomes negligible when transmitter-cooperation increases from $\{M=2, N=2\}$ to

$\{M = 4, N = 4\}$.

VI. Conclusion

This paper has investigated the secrecy performance of a finite-sized in-band selective relaying system with M transmitters, N relays, and K eavesdroppers, which reveals several practical significances on the physical layer security of 5G ultra dense heterogeneous small cell networks. The constraints of backhaul reliability in the main channel and eavesdropping probability in the eavesdropping channel have been considered in the analysis. The exact secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate have been derived in closed-form. Our results have shown that asymptotic limits on the secrecy outage probability and probability of non-zero achievable secrecy rate are jointly determined by transmitter cooperation and backhaul reliability, whereas eavesdropper cooperation is not a factor in the asymptotic secrecy performance metrics. It has also been shown that the secrecy diversity gain promised by the system is jointly determined by M, N, and the number of multi-path components in the frequency-selective channels. It was found that when backhaul reliability is fixed, increasing transmitter-relay cooperation increases the diversity gain in the low and middle SNR regions and improves the asymptotic performance in the high SNR region. The impacts of M, N, K, backhaul reliability, and eavesdropping probability on the secrecy performance of the considered system have been verified accurately by simulation results.

Appendix A: A proof of Proposition 1

Corresponding to backhaul transmission from the CU to T_m, let $\lambda^{C_uT_m}$ denote the received SNR at the transmitter T_m. Irrespective of backhaul reliability, let $\widehat{\lambda}^{T_mR_n} \triangleq \bar{P}\widetilde{\rho}_{h,n,m}||\boldsymbol{h}_{n,m}||^2$ denote the received SNR at R_n corresponding to the transmission through the link $T_m \to R_n$. Since the transmission via the link CU $\to T_m \to R_n \to D$ can be regarded as a three-hop relay link, the corresponding end-to-end SNR can be expressed as

$$\lambda^{T_mR_nD} = \min\left(\lambda^{C_uT_m}, \widehat{\lambda}^{T_mR_n}, \lambda^{R_nD}\right). \tag{A.1}$$

Then, the end-to-end SNR of the main channel can be rewritten as

$$\lambda^{\mathrm{DF}} = \max_{\forall m,\forall n}\left(\min\left(\lambda^{C_uT_m}, \widehat{\lambda}^{T_mR_n}, \lambda^{R_nD}\right)\right). \tag{A.2}$$

The CDF of λ^{DF} can be written as

$$\begin{aligned} F_{\lambda^{\mathrm{DF}}}(x) &= \underbrace{\Pr\left(\lambda^{\mathrm{DF}} < x, \max_{\forall m}\left(\lambda^{C_uT_m}\right) < x\right)}_{\mathrm{Pr}_1(x)} \\ &\quad + \underbrace{\Pr\left(\lambda^{\mathrm{DF}} < x, \max_{\forall m}\left(\lambda^{C_uT_m}\right) > x, \max_{\forall n}\left(\lambda^{R_nD}\right) < x\right)}_{\mathrm{Pr}_2(x)} \\ &\quad + \underbrace{\Pr\left(\lambda^{\mathrm{DF}} < x, \max_{\forall m}\left(\lambda^{C_uT_m}\right) > x, \max_{\forall n}\left(\lambda^{R_nD}\right) > x\right)}_{\mathrm{Pr}_3(x)}. \end{aligned} \tag{A.3}$$

Since the backhauls are shared by all the MN end-to-end links, i.e., each backhaul connection is shared by N end-to-end links, the term $\mathrm{Pr}_1(x)$ in (A.3) can be evaluated as

$$\begin{aligned} \mathrm{Pr}_1(x) &= \Pr\left(\max_{\forall m}\left(\lambda^{C_uT_m}\right) < x\right) = \Pr\left(\mathbb{B}_m = 0, \forall m\right) \\ &= \prod_{m=1}^{M}(1 - p_m). \end{aligned} \tag{A.4}$$

In (A.4), we have applied the fact that a non-zero $\lambda^{C_uT_m}$ due to the perfectly reliable backhaul transmission ($\mathbb{B}_m = 1$) is larger than any practical $x > 0$, so that the event $\max\left(\lambda^{C_uT_m}\right) = 0$ occurs when all the backhaul connections are erased with probability $1-p_m$, $\forall m$ due to unreliable backhaul connections. Similarly, the N links at the hop $R_n \to D$ are shared by all the MN end-to-end links. Considering that the link $R_n \to D$ is independent of the backhaul connection CU $\to T_m$, the term $\mathrm{Pr}_2(x)$ in (A.3) can be evaluated as

$$\begin{aligned} \mathrm{Pr}_2(x) &= \Pr\left(\max_{\forall n}\left(\lambda^{R_nD}\right) < x\right)\Pr\left(\max_{\forall m}\left(\lambda^{C_uT_m}\right) > x\right) \\ &= \prod_{n=1}^{N}\left(1 - e^{-\frac{x}{P_R\widetilde{\rho}_{f,n}}}\sum_{t=0}^{L_{f,n}-1}\frac{1}{t!}\frac{x^t}{(P_R\widetilde{\rho}_{f,n})^t}\right) \\ &\quad \times\left(1 - \prod_{m=1}^{M}(1 - p_m)\right) \\ &= \left(1 + \sum_{\ell=1}^{N}\sum_{\widetilde{r}_1=1}^{N-\ell+1}\sum_{\widetilde{r}_2=\widetilde{r}_1+1}^{N-\ell+2}\cdots\sum_{\widetilde{r}_\ell=\widetilde{r}_{\ell-1}+1}^{N}(-1)^\ell\right. \\ &\quad \left.\times e^{-\widetilde{\alpha}_\ell x}\prod_{\varepsilon=1}^{\ell}\left(\sum_{t=0}^{L_{f,r_\varepsilon}-1}\frac{x^t}{t!(P_R\widetilde{\rho}_{f,r_\varepsilon})^t}\right)\right) \\ &\quad \times\left(1 - \prod_{m=1}^{M}(1 - p_m)\right) \\ &= \left(1 + \widetilde{\sum}(-1)^\ell\widetilde{\Upsilon}_\ell e^{-\widetilde{\alpha}_\ell x}x^{\widetilde{\beta}_\ell}\right)\left(1 - \prod_{m=1}^{M}(1 - p_m)\right), \end{aligned} \tag{A.5}$$

where $\widetilde{\alpha}_\ell \triangleq \sum_{\varepsilon=1}^{\ell}\frac{1}{P_R\widetilde{\rho}_{f,r_\varepsilon}}$, $\widetilde{\beta}_\ell \triangleq \sum_{\varepsilon=1}^{\ell}t_\varepsilon$, $\widetilde{\Upsilon}_\ell \triangleq \prod_{\varepsilon=1}^{\ell}\left(\frac{1}{t_\varepsilon!(P_R\widetilde{\rho}_{f,r_\varepsilon})^{t_\varepsilon}}\right)$, and $\widetilde{\sum} \triangleq \sum_{\ell=1}^{N}\sum_{\widetilde{r}_1=1}^{N-\ell+1}\sum_{\widetilde{r}_2=\widetilde{r}_1+1}^{N-\ell+2}\cdots\sum_{\widetilde{r}_\ell=\widetilde{r}_{\ell-1}+1}^{N}\sum_{t_1=0}^{L_{f,\widetilde{r}_1}-1}\sum_{t_2=0}^{L_{f,\widetilde{r}_2}-1}\cdots\sum_{t_\ell=0}^{L_{f,\widetilde{r}_\ell}-1}$ is the summation over all combinations of the link $R_n \to D$, $\forall n$ and channel lengths of $\boldsymbol{f}_n$, $\forall n$.

In the considered three-hop selective relay link, if there is at least one backhaul connection can provide a perfectly reliable link, we have $\mathbb{B}_m = 1$, $\exists m$ or equivalently $\max\left(\lambda^{C_uT_m}\right) > x$. Therefore, when the event $\max\left(\lambda^{C_uT_m}\right) > x$ occurs, the event $\lambda^{\mathrm{DF}} < x$ becomes

$$\max_{\forall m,\forall n}\left(\min\left(\widehat{\lambda}^{T_mR_n}, \lambda^{R_nD}\right)\right) < x. \tag{A.6}$$

Substituting (A.6) into the term $\mathrm{Pr}_3(x)$, it can be evaluated as

$$\begin{aligned} \mathrm{Pr}_3(x) = \Pr\left(\max_{\forall m}\left(\lambda^{C_uT_m}\right) > x, \max_{\forall n}\left(\lambda^{R_nD}\right) > x,\right. \\ \left.\max_{\forall m,\forall n}\left(\widehat{\lambda}^{T_mR_n}\right) < x\right). \end{aligned} \tag{A.7}$$

The CDF of $\widehat{\lambda}^{T_mR_n}$ is given by

$$F_{\widehat{\lambda}^{T_mR_n}}(x) = \Pr\left(\widehat{\lambda}^{T_mR_n} < x\right) = 1 - e^{\frac{x}{\bar{P}\widetilde{\rho}_{h,n,m}}} \sum_{s=0}^{L_{h,n,m}-1} \frac{1}{s!} \frac{x^s}{(\bar{P}\widetilde{\rho}_{h,n,m})^s}. \quad \text{(A.8)}$$

Define $\widehat{\lambda} \triangleq \max_{\forall m,\forall n}\left(\widehat{\lambda}^{T_mR_n}\right)$. According to the theory of order statistics, the CDF of $\widehat{\lambda}$ can be written as

$$F_{\widehat{\lambda}}(x) = \prod_{m=1}^{M}\prod_{n=1}^{N} F_{\widehat{\lambda}^{T_mR_n}}(x) = \prod_{\varphi=1}^{MN} F_{\lambda^{\overline{TR}_{(\varphi)}}}(x), \quad \text{(A.9)}$$

where $\lambda^{\overline{TR}_{(\varphi)}} \triangleq \widehat{\lambda}^{T_{\mu(\varphi)}R_{\nu(\varphi)}}$ with $\mu(\varphi) = \left\lceil \frac{\varphi}{N} \right\rceil$ and $\nu(\varphi) = \varphi - \left\lceil \frac{\varphi}{N} - 1 \right\rceil N$. Substituting (A.8) into (A.9), the CDF of $\widehat{\lambda}$ can be evaluated as

$$\begin{aligned} F_{\widehat{\lambda}}(x) &= 1 + \sum_{\varphi=1}^{MN} \sum_{\widehat{r}_1=1}^{MN-\ell+1} \sum_{\widehat{r}_2=\widehat{r}_1+1}^{MN-\ell+2} \cdots \sum_{\widehat{r}_\ell=\widehat{r}_{\ell-1}+1}^{MN} (-1)^{\varphi} \\ &\quad \times e^{-\widehat{\alpha}_\varphi x} \prod_{\varepsilon=1}^{\varphi} \left(\sum_{s=0}^{L_{h,\nu(\widehat{r}_\varepsilon),\mu(\widehat{r}_\varepsilon)}-1} \frac{x^s}{s!(\bar{P}\widetilde{\rho}_{h,\nu(\widehat{r}_\varepsilon),\mu(\widehat{r}_\varepsilon)})^s} \right) \\ &= 1 + \widehat{\sum}(-1)^{\varphi} \widehat{\Upsilon}_\varphi e^{-\widehat{\alpha}_\varphi x} x^{\widehat{\beta}_\varphi}, \end{aligned} \quad \text{(A.10)}$$

where $\widehat{\alpha}_\varphi \triangleq \sum_{\varepsilon=1}^{\varphi} \frac{1}{\bar{P}\widetilde{\rho}_{h,\nu(\widehat{r}_\varepsilon),\mu(\widehat{r}_\varepsilon)}}$, $\widehat{\beta}_\varphi \triangleq \sum_{\varepsilon=1}^{\varphi} s_\varepsilon$, $\widehat{\Upsilon}_\varphi \triangleq \prod_{\varepsilon=1}^{\varphi} \frac{1}{s_\varepsilon!(\bar{P}\widetilde{\rho}_{h,\nu(\widehat{r}_\varepsilon),\mu(\widehat{r}_\varepsilon)})^{s_\varepsilon}}$ and

$$\begin{aligned} \widehat{\sum} \triangleq \sum_{\varphi=1}^{MN} \sum_{\widehat{r}_1=1}^{MN-\varphi+1} \sum_{\widehat{r}_2=\widehat{r}_1+1}^{MN-\varphi+2} \cdots \sum_{\widehat{r}_\varphi=\widehat{r}_{\varphi-1}+1}^{MN} \\ \sum_{s_1=0}^{L_{h,\nu(\widehat{r}_1),\mu(\widehat{r}_1)}-1} \sum_{s_2=0}^{L_{h,\nu(\widehat{r}_2),\mu(\widehat{r}_2)}-1} \cdots \sum_{s_\varphi=0}^{L_{h,\nu(\widehat{r}_\varphi),\mu(\widehat{r}_\varphi)}-1} \end{aligned} \quad \text{(A.11)}$$

is the summation over all combinations of the $T_m \to R_n$ links and channel lengths of all the $T_m \to R_n$ links. Moreover, extracting from (A.5), we have

$$\Pr\left(\max_{\forall m}\left(\lambda^{C_uT_m}\right) > x\right) = 1 - \prod_{m=1}^{M}(1-p_m) \quad \text{(A.12)}$$

and

$$\Pr\left(\max_{\forall n}\left(\lambda^{R_nD}\right) > x\right) = \widetilde{\sum}(-1)^{\ell+1}\widetilde{\Upsilon}_\ell e^{-\widetilde{\alpha}_\ell x}(x)^{\widetilde{\beta}_\ell}. \quad \text{(A.13)}$$

Substituting (A.12), (A.13), and $\Pr\left(\max\left(\widehat{\lambda}^{T_mR_n}\right) < x\right) = F_{\widehat{\lambda}}(x)$ into (A.7), the term $\mathrm{Pr}_3(x)$ is derived as

$$\begin{aligned} \mathrm{Pr}_3 = &\left(1 - \prod_{m=1}^{M}(1-p_m)\right)\left(1 + \widehat{\sum}(-1)^{\ell}\widehat{\Upsilon}_\ell e^{-\widehat{\alpha}_\ell x}(x)^{\widehat{\beta}_\ell}\right) \\ &\times \widetilde{\sum}(-1)^{\ell+1}\widetilde{\Upsilon}_\ell e^{-\widetilde{\alpha}_\ell x}(x)^{\widetilde{\beta}_\ell}. \end{aligned} \quad \text{(A.14)}$$

With the obtained (A.4), (A.5), and (A.14), we arrive at (18).

Appendix B: A proof of Proposition 2

Since each term $Y_k \triangleq \widetilde{\mathbb{I}}_k\widetilde{\lambda}^{\mathrm{E},k}$ of λ^{E} in (12) has the form of the product of the Bernoulli RV $\widetilde{\mathbb{I}}_k$ and the chi-squared RV $\widetilde{\lambda}^{\mathrm{E},k}$, it can be shown that Y_k has the PDF of

$$\begin{aligned} f_{Y_k}(y) &= (1-\widetilde{q}_k)\delta(y) + \frac{\widetilde{q}_k}{\Gamma(L_{e,k})(\eta_{e,k})^{L_{e,k}}} y^{L_{e,k}-1} e^{-\frac{y}{\eta_{e,k}}} \\ &= (1-\widetilde{q}_k)\delta(y) + \widetilde{q}_k f_\lambda(y; L_{e,k}, \eta_{e,k}), \end{aligned} \quad \text{(B.1)}$$

where the PDF $f_\lambda(y; L_{e,k}, \eta_{e,k})$ has the form of (16). In order to derive the PDF of the SNR λ^{E} in closed-form, we present the following three steps and define $X_K \triangleq \sum_{k=1}^{K} Y_k$, so that $\lambda^{\mathrm{E}} = X_{2K}$.

1) Step 1 (K=2 Terms): For $K = 2$, the PDF of $X_2 = Y_1 + Y_2$ can be evaluated as

$$\begin{aligned} f_{X_2}(x) &= \int_0^x f_{Y_1}(y) f_{Y_2}(x-y)\mathrm{d}y \\ &= \delta(x)\prod_{k=1}^{2}(1-\widetilde{q}_k) + \widetilde{q}_1(1-\widetilde{q}_2)f_\lambda(x; L_{e,1}, \eta_{e,1}) \\ &\quad + \widetilde{q}_2(1-\widetilde{q}_1)f_\lambda(x; L_{e,2}, \eta_{e,2}) \\ &\quad + \widetilde{q}_1\widetilde{q}_2\int_0^x f_\lambda(y; L_{e,1}, \eta_{e,1}) f_\lambda(x-y; L_{e,2}, \eta_{e,2})\mathrm{d}y \\ &\triangleq \delta(x)\prod_{k=1}^{2}(1-\widetilde{q}_k) \\ &\quad + \sum_{\tau=1}^{\binom{2}{1}} \widetilde{w}_{2,1,\tau} f_\lambda\left(x; L_{e,\boldsymbol{C}_1^2(\tau,1)}, \eta_{e,\boldsymbol{C}_1^2(\tau,1)}\right) \\ &\quad + \sum_{\tau=1}^{\binom{2}{2}} \widetilde{w}_{2,2,\tau} f_{\widetilde{X}^{\boldsymbol{C}_2^2(\tau,:)}}(x), \end{aligned} \quad \text{(B.2)}$$

where

$$\widetilde{w}_{2,1,\tau} = \widetilde{q}_{\boldsymbol{C}_1^2(\tau,1)}\left(1 - \widetilde{q}_{\bar{\boldsymbol{C}}_1^2(\tau,1)}\right), \quad \text{(B.3)}$$

$$\widetilde{w}_{2,2,\tau} = \widetilde{q}_{\boldsymbol{C}_2^2(\tau,1)}\widetilde{q}_{\boldsymbol{C}_2^2(\tau,2)}, \quad \text{(B.4)}$$

the PDF $f_\lambda\left(x; L_{e,\boldsymbol{C}_1^2(\tau,1)}, \eta_{e,\boldsymbol{C}_1^2(\tau,1)}\right)$ can be obtained by substituting $\{L_a, \eta_a\} = \{L_{e,\boldsymbol{C}_1^2(\tau,1)}, \eta_{e,\boldsymbol{C}_1^2(\tau,1)}\}$ into (16), and $f_{\widetilde{X}^{\boldsymbol{C}_2^2(\tau,:)}}(x)$ is the PDF of the RV $\widetilde{X}^{\boldsymbol{C}_2^2(\tau,:)} \triangleq \widetilde{\lambda}^{\mathrm{E},\boldsymbol{C}_2^2(\tau,1)} + \lambda^{\mathrm{E},\boldsymbol{C}_2^2(\tau,2)}$, which is determined by (23).

2) Step 2 (K=3 Terms): For $K = 3$, the PDF of $X_3 = X_2 + Y_3$ can be expressed with $f_{X_2}(x)$ and $f_{Y_3}(x)$ as

$$f_{X_3}(z) = \int_0^x f_{X_2}(x) f_{Y_3}(x-y)\mathrm{d}y. \quad \text{(B.5)}$$

Following similar procedures as for the evaluation of the PDF of X_2, after some complicated but straightforward manipulations, we arrive at

$$\begin{aligned} f_{X_3}(x) &= \delta(x)\prod_{k=1}^{3}(1-\widetilde{q}_k) \\ &\quad + \sum_{\tau=1}^{\binom{3}{1}} \widetilde{w}_{3,1,\tau} f_\lambda\left(x; L_{e,\boldsymbol{C}_1^3(\tau,1)}, \eta_{e,\boldsymbol{C}_1^3(\tau,1)}\right) \\ &\quad + \sum_{k=2}^{3}\sum_{\tau=1}^{\binom{3}{k}} \widetilde{w}_{3,k,\tau} f_{\widetilde{X}^{\boldsymbol{C}_k^3(\tau,:)}}(x), \end{aligned} \quad \text{(B.6)}$$

where

$$\widetilde{w}_{3,1,\tau} = \widetilde{q}_{\boldsymbol{C}_1^3(\tau,1)}\big(1-\widetilde{q}_{\bar{\boldsymbol{C}}_1^3(\tau,1)}\big)\big(1-\widetilde{q}_{\bar{\boldsymbol{C}}_1^3(\tau,2)}\big), \tag{B.7}$$

$$\widetilde{w}_{3,2,\tau} = \widetilde{q}_{\boldsymbol{C}_2^3(\tau,1)}\widetilde{q}_{\boldsymbol{C}_2^3(\tau,2)}\big(1-\widetilde{q}_{\bar{\boldsymbol{C}}_2^3(\tau,1)}\big), \tag{B.8}$$

$$\widetilde{w}_{3,3,\tau} = \widetilde{q}_{\boldsymbol{C}_3^3(\tau,1)}\widetilde{q}_{\boldsymbol{C}_3^3(\tau,2)}\widetilde{q}_{\boldsymbol{C}_3^3(\tau,3)}. \tag{B.9}$$

In (B.6), $f_\lambda\big(x; L_{e,\boldsymbol{C}_1^3(\tau,1)}, \eta_{e,\boldsymbol{C}_1^3(\tau,1)}\big)$ and $f_{\widetilde{X}^{\boldsymbol{C}_k^{3}(\tau,:)}}(x)$ are similarly determined as those in Step 2.

3) Step 3 (2K Terms): Following the same procedures as Step 1 and 2 for the sum of $\lambda^{\mathrm{E}} = X_{2K} = \sum_{k=1}^{2K} Y_k$, (26) can be obtained, where $w_{k,\tau}$ is generated from Step 1 and 2 with respect to $\widetilde{w}_{n,k,\tau}$ as given by (28). In (26), we have expressed $f_{\widetilde{X}^{\boldsymbol{C}_k^{2K}(\tau,:)}}(x)$ with its form in (23).

By integrating (26), the CDF of λ^{E} is derived as (27), where $F_\lambda\big(x; L_{e,\boldsymbol{C}_1^3(\tau,1)}, \eta_{e,\boldsymbol{C}_1^3(\tau,1)}\big)$ is given by (17).

Appendix C: A proof of Proposition 3

It has been shown that a fixed received SNR of the eavesdropping channel does not affect the secrecy diversity gain, while the secrecy diversity gain is determined by the asymptotic limit on the end-to-end SNR of main channel [25]. We start the proof with the evaluation of asymptotic limits for $\mathrm{Pr}_1(x)$, $\mathrm{Pr}_2(x)$, and $\mathrm{Pr}_3(x)$ with respect to $F_{\lambda^{\mathrm{DF}}}(x) = \mathrm{Pr}_1(x) + \mathrm{Pr}_2(x) + \mathrm{Pr}_3(x)$ as defined in Appendix A.

With perfect backhaul, it can be easily shown that $\mathrm{Pr}_1(x) = 0$. The asymptotic expression for $\mathrm{Pr}_2(x)$ as $P_R\widetilde{\rho}_{f,n} \to \infty$ with perfect backhaul is given by

$$\begin{aligned}\mathrm{Pr}_2(x) &= \prod_{n=1}^{N}\left(1 - e^{-\frac{x}{P_R\widetilde{\rho}_{f,n}}}\sum_{t=0}^{L_{f,n}-1}\frac{1}{t!}\frac{x^t}{(P_R\widetilde{\rho}_{f,n})^t}\right)\\ &\quad\times\left(1-\prod_{m=1}^{M}(1-p_m)\right)\\ &= \prod_{n=1}^{N}\frac{1}{(L_{f,n})!}\left(\frac{x}{P_R\widetilde{\rho}_{f,n}}\right)^{L_{f,n}}.\end{aligned} \tag{C.1}$$

As such, the asymptotic CDF of $\widehat{\lambda}$ as $\bar{P}\widetilde{\rho}_{h,n,m} \to \infty$ can be evaluated as

$$F_{\widehat{\lambda}}(x) = \prod_{\varphi=1}^{MN}\frac{1}{\big(L_{h,\nu(\varphi),\mu(\varphi)}\big)!}\left(\frac{x}{\bar{P}\widetilde{\rho}_{h,\nu(\varphi),\mu(\varphi)}}\right)^{L_{h,\nu(\varphi),\mu(\varphi)}}. \tag{C.2}$$

Moreover, with perfect backhaul, we have the asymptotic limits

$$\Pr\left(\max_{\forall m}\big(\lambda^{C_u T_m}\big) > x\right) = 1 \tag{C.3}$$

and

$$\Pr\left(\max_{\forall n}\big(\lambda^{R_n D}\big) > x\right) = 1 - \prod_{n=1}^{N}\frac{1}{(L_{f,n})!}\left(\frac{x}{P_R\widetilde{\rho}_{f,n}}\right)^{L_{f,n}}. \tag{C.4}$$

Based on (C.2), (C.3), (C.4) and according to (A.7), the asymptotic limit for $\mathrm{Pr}_3(x)$ can be expressed as

$$\begin{aligned}\mathrm{Pr}_3(x) &= \left(1 - \prod_{n=1}^{N}\frac{1}{(L_{f,n})!}\left(\frac{x}{P_R\widetilde{\rho}_{f,n}}\right)^{L_{f,n}}\right)\\ &\quad\times\prod_{\varphi=1}^{MN}\frac{1}{\big(L_{h,\nu(\varphi),\mu(\varphi)}\big)!}\left(\frac{x}{\bar{P}\widetilde{\rho}_{h,\nu(\varphi),\mu(\varphi)}}\right)^{L_{h,\nu(\varphi),\mu(\varphi)}}.\end{aligned} \tag{C.5}$$

With the obtained $\mathrm{Pr}_1(x) = 0$, (C.1), and (C.5), the asymptotic limit for $F_{\lambda^{\mathrm{DF}}}(x)$ is given by

$$F_{\lambda^{\mathrm{DF}}}(x) = \begin{cases}\prod\limits_{\varphi=1}^{MN}\frac{1}{\left(L_{h,\nu(\varphi),\mu(\varphi)}\right)!}\left(\frac{x}{\bar{P}\widetilde{\rho}_{h,\nu(\varphi),\mu(\varphi)}}\right)^{L_{h,\nu(\varphi),\mu(\varphi)}}, \\ \qquad\text{when}\ \ \widetilde{L}_f > \widetilde{L}_h,\\ \prod\limits_{n=1}^{N}\frac{1}{(L_{f,n})!}\left(\frac{x}{P_R\widetilde{\rho}_{f,n}}\right)^{L_{f,n}}, \\ \qquad\text{when}\ \ \widetilde{L}_f < \widetilde{L}_h,\\ \prod\limits_{n=1}^{N}\frac{1}{(L_{f,n})!}\left(\frac{x}{P_R\widetilde{\rho}_{f,n}}\right)^{L_{f,n}} \\ \quad+\prod\limits_{\varphi=1}^{MN}\frac{1}{\left(L_{h,\nu(\varphi),\mu(\varphi)}\right)!}\left(\frac{x}{\bar{P}\widetilde{\rho}_{h,\nu(\varphi),\mu(\varphi)}}\right)^{L_{h,\nu(\varphi),\mu(\varphi)}} \\ \qquad\text{when}\ \ \widetilde{L}_f = \widetilde{L}_h,\end{cases} \tag{C.6}$$

where $\widetilde{L}_h \triangleq \sum_{\varphi=1}^{MN} L_{h,\nu(\varphi),\mu(\varphi)}$ and $\widetilde{L}_f \triangleq \sum_{n=1}^{N} L_{f,n}$. Based on (C.6), the secrecy diversity gain is clearly given by

$$G_d = \min\left(\sum_{\varphi=1}^{MN} L_{h,\nu(\varphi),\mu(\varphi)}, \sum_{n=1}^{N} L_{f,n}\right). \tag{C.7}$$

Appendix D: A proof of Theorem 3

To derive the asymptotic limit on the CDF of λ^{DF}, we need to evaluate the asymptotic limits on $\mathrm{Pr}_2(x)$ and $\mathrm{Pr}_3(x)$, respectively. As $P_R\widetilde{\rho}_{f,n} \to \infty$, the asymptotic $\mathrm{Pr}_2(x)$ can be evaluated as

$$\begin{aligned}\mathrm{Pr}_2(x) &= \prod_{n=1}^{N}\left(1 - e^{-\frac{x}{P_R\widetilde{\rho}_{f,n}}}\sum_{t=0}^{L_{f,n}-1}\frac{1}{t!}\frac{x^t}{(P_R\widetilde{\rho}_{f,n})^t}\right)\\ &\quad\times\left(1-\prod_{m=1}^{M}(1-p_m)\right)\\ &\approx \prod_{n=1}^{N}\frac{1}{(L_{f,n})!}\left(\frac{x}{P_R\widetilde{\rho}_{f,n}}\right)^{L_{f,n}}\left(1-\prod_{m=1}^{M}(1-p_m)\right)\\ &\to 0.\end{aligned} \tag{D.1}$$

As $\bar{P}\widetilde{\rho}_{h,n,m} \to \infty$, the asymptotic CDF of $\widehat{\lambda}$ can be expressed as

$$\begin{aligned}F_{\widehat{\lambda}}(x) &= \prod_{\varphi=1}^{MN}\left(1 - e^{\frac{x}{\bar{P}\widetilde{\rho}_{h,n,m}}}\sum_{s=0}^{L_{h,n,m}-1}\frac{1}{s!}\frac{x^s}{(\bar{P}\widetilde{\rho}_{h,n,m})^s}\right)\\ &\approx \prod_{\varphi=1}^{MN}\frac{1}{(L_{h,n,m})!}\left(\frac{x}{\bar{P}\widetilde{\rho}_{h,n,m}}\right)^{L_{h,n,m}}\\ &\to 0.\end{aligned} \tag{D.2}$$

Similarly, as $P_R\widetilde{\rho}_{f,n} \to \infty$, we have the asymptotic limit

$$\Pr\left(\max_{\forall n}\big(\lambda^{R_n D}\big) > x\right) \to 1. \tag{D.3}$$

Substituting (A.12), (D.2), and (D.3) into the term $\Pr_3(x)$, the asymptotic limit on $\Pr_3(x)$ as $\bar{P}\widetilde{\rho}_{h,n,m} \to \infty$ and $P_R\widetilde{\rho}_{f,n} \to \infty$ is zero. Therefore, the asymptotic limit on the CDF of λ^{DF} as $\bar{P}\widetilde{\rho}_{h,n,m} \to \infty$ and $P_R\widetilde{\rho}_{f,n} \to \infty$ is given by

$$\begin{aligned} F_{\lambda^{\mathrm{DF}}}(x) &= \Pr_1(x) + \Pr_2(x) + \Pr_3(x) \\ &= \prod_{m=1}^{M}(1-p_m). \end{aligned} \tag{D.4}$$

As $\eta_a \to \infty$, the CDF in (17) has the asymptotic limit of

$$F_{\lambda}(x; L_a, \eta_a) = \frac{1}{(L_a)!}\left(\frac{x}{\eta_a}\right)^{L_a}. \tag{D.5}$$

Substituting the asymptotic limit form of (D.5) into (27) and taking its derivative, we obtain the asymptotic limit on the PDF $f_{\lambda^{\mathrm{E}}}(x)$ including a asymptotic PDF limit of

$$f_{\lambda}(x; L_a, \eta_a) = \frac{1}{(L_a-1)!}\frac{x^{L_a-1}}{(\eta_a)^{L_a}} \tag{D.6}$$

as $\eta_a \to \infty$. Applying the asymptotic PDF $f_{\lambda^{\mathrm{E}}}(x)$ and (D.4) to the derivation of the secrecy outage probability, we obtain

$$\begin{aligned} P_{\mathrm{out}}^{as} &= \int_0^{\infty} F_{\lambda^{\mathrm{DF}}}(J_R(1+x)-1) f_{\lambda^{\mathrm{E}}}(x)\mathrm{d}x \\ &= \prod_{m=1}^{M}(1-p_m) \end{aligned} \tag{D.7}$$

since $f_{\lambda^{\mathrm{E}}}(x)$ decays faster than $F_{\lambda^{\mathrm{DF}}}(x)$ given that $\rho_x \gg \rho_y$, $\forall \rho_x \in \{\rho_{h,n,m}, \rho_{f,n}\}$ and $\forall \rho_y \in \{\rho_{j,k,m}, \rho_{g,k,n}\}$.

Similarly, the asymptotic probability of non-zero secrecy rate can be evaluated as

$$\begin{aligned} \Pr^{as}(\mathcal{C}_s > 0) &= 1 - \int_0^{\infty} F_{\lambda^{\mathrm{DF}}}(x) f_{\lambda^{\mathrm{E}}}(x)\mathrm{d}x \\ &= 1 - \prod_{m=1}^{M}(1-p_m). \end{aligned} \tag{D.8}$$

REFERENCES

[1] J. Xu, J. Wang, Y. Zhu, Y. Yang, X. Zheng, S. Wang, L. Liu, K. Horneman, and Y. Teng, "Cooperative distributed optimization for the hyperdense small cell deployment," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 61–67, May 2014.

[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

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

[4] Z. Mayer, J. Li, A. Papadogiannis, and T. Svensson, "On the impact of control channel reliability on coordinated multi-point transmission," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 28, pp. 1–16, 2014.

[5] M. Jaber, M. Imran1, R. Tafazolli1, and A. Tukmanov, "5G backhaul challenges and emerging research directions: A survey," *IEEE Access*, vol. 4, pp. 1743–1766, Apr. 2016.

[6] S. Arad and J. Hoadley, *Systems and methods optimizing backhaul transport*. U.S. Patent 2014/0 160 939 A1, Jun. 12, 2014.

[7] S. Chia, M. Gasparroni, and P. Brick, "The next challenge for cellular networks: Backhaul," *IEEE Microw. Mag.*, vol. 10, no. 5, pp. 54–66, Aug. 2009.

[8] X. Ge, S. Tu, G. Mao, C. X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Access*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

[9] Z. Pi, J. Choi, and R. Heath, "Millimeter-wave gigabit broadband evolution toward 5G: Fixed access and backhaul," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 138–144, Apr. 2016.

[10] H. Tabassum, A. H. Sakr, and E. Hossain, "Analysis of massive MIMO-enabled downlink wireless backhauling for full-duplex small cells," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2354–2369, Jun. 2016.

[11] M. Coldrey, H. Koorapaty, J. E. Berg, Z. Ghebretensa, J. Hansryd, A. Derneryd, and S. Falahati, "Small-cell wireless backhauling: A non-line-of-sight approach for point-to-point microwave links," in *Proc. IEEE Veh. Technol. Conf.*, Québec City, Canada, 3-6 Sept. 2012, pp. 1–5.

[12] U. Siddique, H. Tabassum, E. Hossain, and D. I. Kim, "Wireless backhauling of 5G small cells: Challenges and solution approaches," *IEEE Wireless Commun.*, vol. 22, no. 5, pp. 22–31, Oct. 2016.

[13] D. Torrieri and M. C. Valenti, "The outage probability of a finite Ad Hoc network in Nakagami fading," *IEEE Trans. Commun.*, vol. 60, no. 12, p. 2960C2970, Dec. 2012.

[14] S. H. Park, O. Simeone, O. Sahin, and S. Shamai, "Multihop backhaul compression for the uplink of cloud radio access networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3185–3199, May 2016.

[15] 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, 10-15 Jun. 2012, pp. 5064–5069.

[16] H. Jung and I. H. Lee, "Outage analysis of millimeter-wave wireless backhaul in the presence of blockage," *IEEE Commun. Lett.*, vol. 20, no. 11, pp. 2268–2271, Nov. 2016.

[17] H. Phan, F. Zheng, and M. Fitch, "Wireless backhaul networks with precoding complex field network coding," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 447–450, Mar. 2015.

[18] 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, Sept. 2011.

[19] O. Simeone, O. Somekh, H. V. Poor, and S. Shamai, "Enhancing uplink throughput via local base station cooperation," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, 26-29 Oct. 2008, pp. 116–120.

[20] 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.

[21] S. G. Larew, T. A. Thomas, M. Cudak, and A. Ghosh, "Air interface design and ray tracing study for 5G millimeter wave communications," in *Proc. IEEE GLOBECOM Workshops*, Atlanta, GA, USA, 9-13 Dec. 2013, pp. 117–122.

[22] H. Nikopour, W. Lee, R. Doostnejad, E. Sasoglu, C. D. Silva, H. Niu, and S. Talwar, "Single carrier waveform solution for millimeter wave air interface," in *Proc. GLOBECOM Workshops*, Washington, DC, USA, 4-8 Dec. 2016, pp. 1–6.

[23] 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, pp. 928–930, Dec. 2007.

[24] 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.

[25] K. J. Kim, P. L. Yeoh, P. Orlik, and H. V. Poor, "Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections," *IEEE Trans. Signal Process.*, vol. 64, no. 17, pp. 4403–4416, Sept. 2016.

[26] 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.

[27] 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.

[28] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. 2006 IEEE ISIT*, Seattle, WA, USA, 9-14 Jul. 2006, pp. 356–360.

[29] M. Bloch, J. Barros, M. R. D. Rodriques, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[30] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[31] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[33] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[34] 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.
[35] X. Ding, T. Song, Y. Zou, and X. Chen, "Intercept probability analysis of relay selection for wireless communications in the presence of multiple eavesdroppers," in *Proc. IEEE WCNC 2016*, Doha, Qatar, 3-6 Apr. 2016, pp. 1–6.
[36] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser multiple amplify-and-forward relay networks in presence of multiple eavesdroppers," in *Proc. IEEE GLOBECOM 2014*, Austin, TX, USA, 8-12 Dec. 2014, pp. 4120–4125.
[37] H. Shen, W. Xu, and C. Zhao, "QoS constrained optimization for multi-antenna AF relaying with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2224–2228, Dec. 2015.
[38] J. H. Lee, "Confidential multicasting assisted by multi-hop multi-antenna DF relays in the presence of multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 64, no. 10, pp. 4295–4304, Oct. 2016.
[39] H. Alves, R. D. Souza, and M. Debbah, "Enhanced physical layer security through transmit antenna selection," in *Proc. IEEE GLOBECOM Workshops*, Houston, TX, USA, 5-9 Dec. 2011, pp. 879–883.
[40] 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. 372–375, Jun. 2012.
[41] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.
[42] Y. Feng, S. Yan, Z. Yang, N. Yang, and W. Zhu, "TAS-based incremental hybrid decode-amplify-forward relaying for physical layer security enhancement," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3876–3891, Jun. 2017.
[43] P. L. Yeoh, K. J. Kim, P. Orlik, and H. V. Poor, "Secrecy performance of cooperative single carrier systems with unreliable backhaul connections," in *Proc. IEEE GLOBECOM 2016*, Washington, DC, 4-8 Dec. 2016, pp. 1–6.
[44] P. L. Yeoh, N. Yang, and K. J. Kim, "Secrecy outage probability of selective relaying wiretap channels with collaborative eavesdropping," in *Proc. IEEE GLOBECOM 2015*, San Diego, CA, 6-10 Dec. 2015, pp. 1–6.
[45] B. Gui, L. Dai, and L. J. Cimini, "Routing strategies in multihop cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 843–855, Feb. 2009.
[46] H. Liu, K. J. Kim, T. A. Tsiftsis, K. S. Kwak, and H. V. Poor, "Secrecy performance of finite-sized cooperative full-duplex relay system with unreliable backhauls," *IEEE Trans. Signal Process.*, vol. 65, no. 23, pp. 6185–6200, Dec. 2017.
[47] S. Hur, T. Kim, D. J. Love, J. V. Krogmeier, T. A. Tomas, and A. Ghosh, "Millimeter wave beamforming for wireless backhaul and access in small cell networks," *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4391–4403, Oct. 2013.
[48] O. E. Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, "Spatially sparse precoding in millimeter wave MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1499–1513, Mar. 2014.
[49] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.
[50] G. K. Karagiannidis, N. C. Sagias, and T. A. Tsiftsis, "Closed-form statistics for the sum of squared Nakagami-m variables and its applications," *IEEE Trans. Commun.*, vol. 54, no. 8, pp. 1353–1359, Aug. 2006.
[51] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory 2007*, Nice, France, 24-29 Jun. 2007, pp. 2471–2475.
[52] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[53] 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.
[54] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York: Academic Press, 2007.

Hongwu Liu received the Ph.D. degree from Southwest Jiaotong University in 2008. From 2008 to 2010, he was with Nanchang Hangkong University. From 2010 to 2011, he was a Post-Doctoral Fellow with the Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Science. From 2011 to 2013, he was a Research Fellow with the UWB Wireless Communications Research Center, Inha University, South Korea. In 2014, he joined Shandong Jiaotong University, China, as an associated professor. He is currently a Research Professor with the Department of Information and Communication Engineering, Inha University. His research interests include MIMO signal processing, cognitive radios, cooperative communications, wireless secrecy communications, and future 5G techniques.

Phee Lep Yeoh (S'08-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. From 2012 to 2016, he was with the Department of Electrical and Electronic Engineering at the University of Melbourne, Australia. In 2016, he joined the School of Electrical and Information Engineering at the University of Sydney, Australia.

Dr. Yeoh is a recipient of the 2017 Alexander von Humboldt Research Fellowship for Experienced Researchers and the 2014 Australian Research Council (ARC) Discovery Early Career Researcher Award (DECRA). 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 wireless security, ultra-reliable and low-latency communications (URLLC), ultra-dense networks, and multiscale molecular communications.

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, CA, USA, in 2000. From 1991 to 1995, he was a Research Engineer with the Video Research Center, 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 and Nokia Inc., Dallas, TX, USA, as a Senior Research Engineer, where he was an L1 Specialist, from 2005 to 2009. During 2010-2011, he was an Invited Professor at Inha University, Incheon, Korea. Since 2012, he has been a Senior Principal Research Staff with the Mitsubishi Electric Research Laboratories, Cambridge, MA, USA. His research include transceiver design, resource management, scheduling in the cooperative wireless communications system, cooperative spectrum sharing system, physical layer secrecy system, and device-to-device communications.

Dr. Kim currently serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS. He served as an Editor of the IEEE COMMUNICATIONS LETTERS and INTERNATIONAL JOURNAL OF ANTENNAS AND PROPAGATION. He also served as a Guest Editor of the EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING: SPECIAL ISSUE ON COOPERATIVE COGNITIVE NETWORKS and IET COMMUNICATIONS: SPECIAL ISSUE ON SECURE PHYSICAL LAYER COMMUNICATIONS.

Philip V. Orlik (M'99) 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 Manager of the Electronics and Communications Group. His primary research focus is on advanced wireless and wired communications, sensor/IoT networks. Other research interests include vehicular/car-to-car communications, mobility modeling, performance analysis, and queuing theory.

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 currently the Michael Henry Strater University Professor of Electrical Engineering. During 2006 to 2016, he served as Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. He received the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, Honorary Professorships at Peking University and Tsinghua University, both conferred in 2017, and a D.Sc. honoris causa from Syracuse University also awarded in 2017.