Secure Cooperative Single Carrier Systems Under Unreliable Backhaul and Dense Networks Impact

Nguyen, H. T., Zhang, J., Yang, . N., Duong, Q., & Hwang, W-J. (2017). Secure Cooperative Single Carrier Systems Under Unreliable Backhaul and Dense Networks Impact. IEEE Access, 5, 18310-18324. DOI: 10.1109/ACCESS.2017.2727399

Published in:
IEEE Access

Document Version:
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES ON RADIO ACCESS AND SECURITY METHODS IN 5G NETWORKS

Received June 28, 2017, accepted July 8, 2017, date of publication July 14, 2017, date of current version September 27, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2727399

Secure Cooperative Single Carrier Systems Under Unreliable Backhaul and Dense Networks Impact

HUY T. NGUYEN[1], JUNQING ZHANG[2], NAN YANG[3], (Member, IEEE), TRUNG Q. DUONG[2], (Senior Member, IEEE), AND WON-JOO HWANG[1], (Senior Member, IEEE)

[1]Department of Information and Communication System, Inje University, Gimhae 621-749, South Korea
[2]School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, U.K.
[3]Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia

Corresponding author: Won-Joo Hwang (ichwang@inje.ac.kr)

The work of H. T. Nguyen and W.-J. Hwang was supported by the Ministry of Science, ICT and Future Planning, South Korea, through the Grand Information Technology Research Center Program under Grant IITP-2017-2016-0-00318. The work of T. Q. Duong was supported in part by the Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22 and in part by the Engineering and Physical Sciences Research Council under Grant EP/P019374/1.

ABSTRACT In this paper, the impacts of unreliable backhaul links on the secrecy performance of cooperative single carrier heterogeneous networks in the presence of eavesdroppers are investigated. A two-phase transmitter/relay selection scheme is proposed, where the best transmitter is selected to maximize signal-to-noise ratio at the relays in the first phase and the best relay is chosen in the second phase to minimize the signal-to-interference-plus-noise ratio of the eavesdroppers with the aid of a friendly jammer. Closed-form expressions are derived for the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate. The asymptotic performance analysis is furthermore performed to explicitly reveal the impacts of unreliable backhaul links on the secrecy performance. Our results show that the diversity gain cannot be achieved in the presence of imperfect backhaul links.

INDEX TERMS Unreliable backhaul, heterogeneous networks, frequency selective fading, secrecy outage probability, ergodic secrecy rate, physical layer security, single carrier system.

I. INTRODUCTION

In recent years, the concept of physical layer security (PLS) has gained vast attention now that the presence of malicious eavesdroppers has caused bad effects on the transmission of confidential information in wireless communication systems [1]. Different from upper layer security where the message is encrypted/decrypted with specific key secretly shared between the source and destination, PLS performs the information-theoretical approach to gain the benefit from the physical characteristics in preventing eavesdropping attacks [2]. These PLS methods entail cooperative relaying and/or exploiting the aid of jamming signals such that the confidential message is securely acquired at the receiver.

To satisfy the exponential increase in the number of users and data traffic, network infrastructure has grown towards higher density and heterogeneity [3]. In such heterogeneous networks (HetNets), besides the threats of eavesdropping, one of the critical problems is unreliable backhaul links or backhaul reliability, which has attracted considerable interest in the existing literature [4]–[10]. The network performance in HetNets currently has to depend on unreliable backhaul communication since the signals transmitted via wireless backhaul links are impacted by multiple propagation fading, i.e., small and large scale fading, as well as transmission delay and synchronization among transceivers [11], [12]. Thus, the transmissions via backhaul links are not intrinsically reliable in the context of wireless communication systems. It has been shown that the presence of unreliable backhaul links strongly deteriorates the network performance since the asymptotic limitation is mainly determined by reliability levels [6], [7].

Among the recent studies on PLS, the opportunistic cooperative relay approach has been examined for both decode-and-forward (DF) [13], [14] and amplify-and-forward (AF) [2], [15] relaying schemes. These studies have attempted to minimize the overheard information by degrading the achievable signal-to-noise ratio (SNR) at the eavesdroppers. This approach demonstrates the ability of preventing the leakage of confidential information. However, such prevention cannot be guaranteed when the number of

eavesdroppers increases. To tackle this problem, a friendly jammer has been incorporated to generate interference signals towards eavesdroppers [16]–[19]. It has been shown that the secrecy rate is significantly enhanced with the help of jammers.

While PLS enables the confidential message to successfully arrive at the legitimate destination, most of the previous PLS works have assumed ideal wireless backhaul links. In the context of HetNets, this assumption, however, is impractical. The presence of unreliable backhaul has been investigated relative to the scaling of the network performance. For example, the authors in [4]–[6] developed the analytical frameworks to examine the performance of cooperative wireless systems. Additionally, the investigation on backhaul reliability was extended to spectrum sharing environments by considering the primary user interference constraints [7]–[9]. However, without considering the presence of eavesdroppers, the information between the source and destination could be left vulnerable. Very recently, the impacts of backhaul reliability have been examined in the presence of multiple eavesdroppers [10]. Nevertheless, the authors have not exploited cooperative jamming in the preventing of eavesdroppers, where a single relay is adopted.

From these observations, it can be seen that PLS in the presence of unreliable backhaul links has not been completely investigated yet. Motivated by this, in this paper we investigate the secrecy performance of single carrier systems taking into account cooperative jamming.[1] Our main contributions are summarized as follows:

- We investigate the secrecy performance of cooperative HetNets by exploiting cooperative relay and jamming signals in the presence of unreliable backhaul links between macro-cells and small-cells. Specifically, the context of cycle prefixed single carrier (CP-SC) transmission[2] is employed to avoid inter-symbol interference (ISI) [20], [22]. Moreover, we consider frequency selective fading channels in the network since multipath components in practical scenarios usually reflect the transmission signals between senders and receivers [10], [14].
- By taking into account dense networks, we apply the best relay selection in multi-relay networks. In particular, we propose a two-phase transmitter/relay selection scheme. The achievable SNR at the relays is maximized by applying the best transmitter selection in/during the first phase and the relay selection scheme is deployed in/during the second phase such that the instantaneous signal-to-interference-plus-noise ratio (SINR) at the eavesdroppers is minimized.
- The secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate are derived in closed-form to analyze the secrecy performance of the network. The asymptotic secrecy expressions are also attained to gain full insights into the impact of backhaul reliability on the network secrecy performance in the high SNR regime.
- We show that the number of multipath components and the degrees of cooperative transmission significantly impact the scaling of secrecy performance. More importantly, backhaul reliability is shown as an important factor in PLS system design, which strongly affects the achievable secrecy performance.

The rest of this paper is organized as follows. In Section II, we describe the network and channel models of the proposed cooperative single-carrier systems. Our proposed two-phase transmitter/relay selection scheme is detailed in Section III. In Section IV, the analysis is provided to obtain the closed-form expressions for secrecy performance metrics. Numerical results are presented in Section V and conclusions are drawn in Section VI.

Notation: $\mathcal{CN}(\mu, \sigma_n^2)$ denotes the complex Gaussian distribution with mean μ and variance σ_n^2; $\boldsymbol{I}_m$ is an $m \times m$ identity matrix; $\mathbb{C}^{m\times n}$ is vector space of $m \times n$ complex matrices; $X \sim \chi^2(N_X, \alpha_X)$ denotes chi-square distribution with degree of freedom (DoF) N_X and power normalizing constant α_X. $F_\lambda(\gamma)$ and $f_\lambda(\gamma)$ denote the cumulative distribution function (CDF) and probability density function (PDF) of the random variable (RV) λ, respectively; $\mathbb{E}_\lambda\{f(\gamma)\}$ denotes the expectation of $f(\gamma)$ with respect to the RV λ. In addition, $\binom{\tau_1}{\tau_2} = \frac{\tau_1!}{\tau_2!(\tau_1-\tau_2)}$ denotes the binomial coefficient.

II. NETWORK AND CHANNEL MODELS

We consider a HetNet as illustrated in Fig. 1. In this network, there is a macro-cell base station (Macro-BS) connected to the core network. Also, K small-cell transmitters T_k, $k \in \{1, 2, \cdots, K\}$, are connected to the Macro-BS via unreliable backhaul links. These K small-cell transmitters communicate with a user D via M DF relays R_m, $m \in \{1, 2, \cdots, M\}$. Furthermore, there are a single jammer J and N eavesdroppers E_n, $n \in \{1, 2, \cdots, N\}$, in the network. We assume that there is no direct link between T_k and D or between T_k and E_n due to poor channel conditions, $\forall k \in K, \forall n \in N$. All the transmitters and receivers are equipped with a single antenna[3] and operate in half-duplex mode. The eavesdroppers cooperate to overhear the transmissions between R_m and D while J generates interference directly to the eavesdroppers.[4]

For a cooperative CP-SC system, we make the following assumptions:

[1] Unlike [10], we exploit the PLS in the context of multiple relays to highlight the impact of dense networks.

[2] The ISI is generated if the coherence bandwidth is smaller than the signal bandwidth, which could lead to the distortion of the transmit signals. With the aid of CP-SC, the ISI can be prevented by attaching the additional prefixes in front of the transmit symbol block and repeating until the end [20], [21].

[3] Note that the jammer in this model is equipped with a single antenna. This assumption is common since a multiple-antenna jamming node may not be available due to the cost, power, and size limitations [19].

[4] In order to obtain the optimal relays weights, we suppose that J and D cooperate with each other. Thus, the complete nulling of jamming signal at D can be achieved [2], [18].

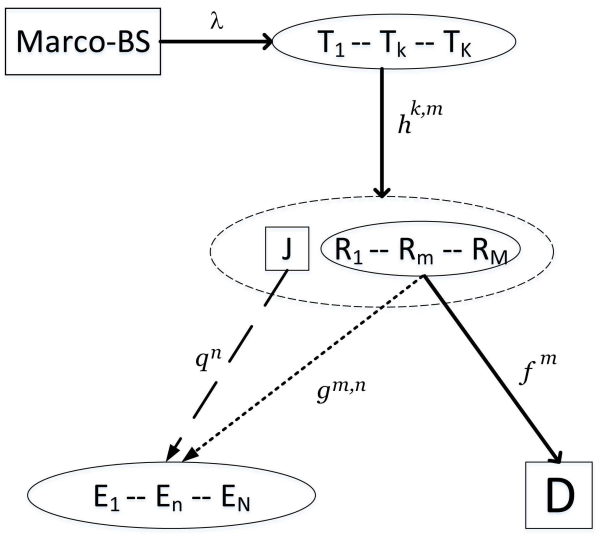

FIGURE 1. The network model of a cooperative single carrier HetNet, where small-cell transmitters connect to the macro-cell via unreliable backhaul links. The PLS exploiting the cooperative relay and the aid of jamming signals is taken into account in the presence of eavesdroppers.

- All channels in the considered network are assumed to undergo frequency selective fading. For example, the channel between T_k and R_m, $\forall k, m$, which is denoted by $\boldsymbol{h}^{k,m} \triangleq [h_1^{k,m}, \ldots, h_{N_R}^{k,m}]^T \in \mathbb{C}^{N_R \times 1}$, consists of N_R multipath components. The corresponding path loss component over $\boldsymbol{h}^{k,m}$ is denoted as $\alpha_T^{k,m}$.
- Similarly, the channel between R_m and E_n, $\forall m, n$, which is denoted by $\boldsymbol{g}^{m,n} \triangleq [g_1^{m,n}, \ldots, g_{N_E}^{m,n}]^T \in \mathbb{C}^{N_E \times 1}$, consists of N_E multipath components. The corresponding path loss component over $\boldsymbol{g}^{m,n}$ is denoted as $\alpha_E^{m,n}$.
- The channel between R_m and D, $\forall m$ and the channel between J and E_n, $\forall n$, which are denoted by $\boldsymbol{f}^m \triangleq [f_1^m, \ldots, f_{N_D}^m]^T \in \mathbb{C}^{N_D \times 1}$ and $\boldsymbol{q}^n \triangleq [q_1^n, \ldots, q_{N_J}^n]^T \in \mathbb{C}^{N_J \times 1}$, consist of N_D and N_J multipath components, respectively. The corresponding path loss component over $\boldsymbol{f}^m$ and $\boldsymbol{q}^n$ are denoted by α_D^m and α_J^n, respectively.
- The transmit symbol block $\boldsymbol{x} \in \mathbb{C}^{S \times 1}$ and interference signal $\boldsymbol{v} \in \mathbb{C}^{S \times 1}$ are transmitted from the Macro-BS and J, respectively, with a symbol block size of S. We assume that $\mathbb{E}[\boldsymbol{x}] = \mathbb{E}[\boldsymbol{v}] = 0$ and $\mathbb{E}[||\boldsymbol{x}||^2] = \mathbb{E}[||\boldsymbol{v}||^2] = \boldsymbol{I}_S$.
- The maximum multipath components in the network is denoted by $N_{max} = \max\,(N_R, N_E, N_J, N_D)$. To avoid the ISI and interblock symbol interference (IBSI) [21], [23], a CP comprised of additional N_{add} symbols is added in front of the transmit symbol $\boldsymbol{x}$, where $N_{add} \geq N_{max}$.

In the considered network, the channel state information (CSI) is assumed to be perfectly known at the relays, J, and D for all active links, since it is a common assumption for PLS literature [2], [10], [24]. Also, we assume that the information[5] from the eavesdroppers can be measured by J in the network [25]. As the transmit symbol block $\boldsymbol{x}$ is transmitted from the Macro-BS, it must pass through the dedicated wireless backhaul links. Due to the nature of wireless channels, the reception status at the K transmitters is presented by success/failure transmission. Thus, the reliability of the wireless backhaul links follows a Bernoulli process $\mathbb{I}_k$, i.e., the message is successfully received at the receivers with a successful probability of λ_k [4], [7]. The failure probability is accordingly given by $1 - \lambda_k$.

Due to multipath fading, the received signal at R_m from T_k is given by

$$\boldsymbol{y}_R^{k,m} = \sqrt{\mathcal{P}_t \alpha_T^{k,m}} \boldsymbol{H}^{k,m} \mathbb{I}_k \mathbf{x} + \boldsymbol{n}_R^{k,m}, \tag{1}$$

where $\mathcal{P}_t$ is the transmit power and $\boldsymbol{H}^{k,m}$ is the right circulant matrix [20], [26] with the corresponding channel vector $\boldsymbol{h}^{k,m}$, and $\boldsymbol{n}_R^{k,m} \sim \mathcal{CN}\left(0, \sigma_n^2 \boldsymbol{I}_S\right)$ is an additive noise vector at R_m. $\mathbb{I}_k$ recalls the backhaul reliability which is modeled as a Bernoulli process.[6] From (1), the instantaneous SNR between T_k and R_m in the first time slot can be expressed as

$$\gamma_R^{k,m} = \frac{\mathcal{P}_t \alpha_T^{k,m} ||\boldsymbol{h}^{k,m}||^2}{\sigma_n^2} \mathbb{I}_k = \widetilde{\alpha}_T^{k,m} ||\boldsymbol{h}^{k,m}||^2 \mathbb{I}_k, \tag{2}$$

where $\widetilde{\alpha}_T^{k,m} \triangleq \dfrac{\mathcal{P}_t \alpha_T^{k,m}}{\sigma_n^2}$ and $\widetilde{\alpha}_T^{k,m} ||\boldsymbol{h}^{k,m}||^2 \sim \chi^2\left(2N_R, \widetilde{\alpha}_T^{k,m}\right)$.

The received signals at E_n and D from R_m are, respectively, given by

$$\begin{aligned} \boldsymbol{y}_E^{m,n} &= \sqrt{\mathcal{P}_r \alpha_E^{m,n}} \boldsymbol{G}^{m,n} \mathbf{x} + \sqrt{\mathcal{P}_j \alpha_J^n} \boldsymbol{Q}^n \mathbf{v} + \boldsymbol{n}_E^{m,n}, \\ \boldsymbol{y}_D^m &= \sqrt{\mathcal{P}_r \alpha_D^m} \boldsymbol{F}^m \mathbf{x} + \boldsymbol{n}_D^m, \end{aligned} \tag{3}$$

where $\mathcal{P}_r$ and $\mathcal{P}_j$ are the transmit powers at the relays and J, respectively, $\boldsymbol{G}^{m,n}$, $\boldsymbol{Q}^n$, and $\boldsymbol{F}^m$ are the right circulant matrix with the corresponding channel vectors $\boldsymbol{g}^{m,n}$, $\boldsymbol{q}^n$, and $\boldsymbol{f}^m$, respectively, $\boldsymbol{n}_E^{m,n} \sim \mathcal{CN}(0, \sigma_n^2 \boldsymbol{I}_S)$ and $\boldsymbol{n}_D^m \sim \mathcal{CN}(0, \sigma_n^2 \boldsymbol{I}_S)$ denote the noise vectors at E_n and D.

Thus, the instantaneous SINR between R_m and E_n can be written as

$$\gamma_E^{m,n} = \frac{\mathcal{P}_r \alpha_E^{m,n} ||\boldsymbol{g}^{m,n}||^2}{\sigma_n^2 + \mathcal{P}_j \alpha_J^n ||\boldsymbol{q}^n||^2} = \frac{\widetilde{\alpha}_E^{m,n} ||\boldsymbol{g}^{m,n}||^2}{1 + \widetilde{\alpha}_J^n ||\boldsymbol{q}^n||^2}, \tag{4}$$

where $\widetilde{\alpha}_E^{m,n} \triangleq \dfrac{\mathcal{P}_r \alpha_E^{m,n}}{\sigma_n^2}$, $\widetilde{\alpha}_J^n \triangleq \dfrac{\mathcal{P}_j \alpha_J^n}{\sigma_n^2}$, $\widetilde{\alpha}_E^{m,n} ||\boldsymbol{g}^{m,n}||^2 \sim \chi^2\left(2N_E, \widetilde{\alpha}_E^{m,n}\right)$, and $\widetilde{\alpha}_J^n ||\boldsymbol{q}^n||^2 \sim \chi^2\left(2N_J, \widetilde{\alpha}_J^n\right)$.

In the second time slot, the instantaneous SNR between R_m and D can be expressed as

$$\gamma_D^m = \frac{\mathcal{P}_r \alpha_D^m ||\boldsymbol{f}^m||^2}{\sigma_n^2} = \widetilde{\alpha}_D^m ||\boldsymbol{f}^m||^2, \tag{5}$$

where $\widetilde{\alpha}_D^m \triangleq \dfrac{\mathcal{P}_r \alpha_D^m}{\sigma_n^2}$ and $\gamma_D^m \sim \chi^2\left(2N_D, \widetilde{\alpha}_D^m\right)$.

[5] Information here is the achievable CSI of the eavesdroppers, in which the jammer uses this information to calculate and forward the SINR to the relays for the cooperative PLS purpose.

[6] Since the transmission via backhaul link is not guaranteed, the message transmitted via backhaul link can be successfully received or dropped. Thus, it is common to model the backhaul reliability by Bernoulli process, which canonically performs success/failure transmission [4]–[8], [10].

Since all the channels are assumed to undergo frequency selective fading, they are distributed according to chi-square distribution. Thus, the CDF and PDF of the RV $X \sim \chi^2(2N_X, \widetilde{\alpha}_X)$ are given by [10], [14]

$$F_X(x) = 1 - e^{-x/\widetilde{\alpha}_X} \sum_{l=0}^{N_X-1} \frac{1}{l!} \left(\frac{x}{\widetilde{\alpha}_X}\right)^l,$$
$$f_X(x) = \frac{1}{(\widetilde{\alpha}_X)^{N_X}(N_X-1)!} x^{N_X-1} e^{-x/\widetilde{\alpha}_X}, \quad (6)$$

respectively. We assume that the unreliable backhaul links are independent from the indices of the K transmitters, i.e., $\lambda_k = \lambda, \forall k$. We also assume that the set of path loss components $\{\alpha_T^{k,m}, \alpha_E^{m,n}, \alpha_J^n, \alpha_D^m\}$ is identically varied among the K transmitters, M relays and N eavesdroppers, i.e., it can be rewritten as $\alpha_T = \alpha_T^{k,m}, \alpha_E = \alpha_E^{m,n}, \alpha_J = \alpha_J^n, \alpha_D = \alpha_D^m, \forall k, m, n$.

III. THE TWO-PHASE TRANSMITTER/RELAY SELECTION SCHEME

Our approach for achieving high PLS level is the proposed two-phase selection scheme which maximizes the achievable performance while reducing the performance at the eavesdroppers as much as possible. In the first phase, each relay chooses the best transmitter among the K small-cells to maximize their achievable SNR. The selected transmitter can be mathematically expressed as

$$\text{Phase 1:} \quad k^* = \arg \max_{k=1,\ldots,K} \gamma_R^{k,m}, \quad (7)$$

where $\gamma_R^{k,m}$ recalls the instantaneous SNR at R_m via T_k. From (7), the statistical property of the instantaneous SNR via the best transmitter T_{k^*} is given in the following theorem.

Theorem 1: Given K independent and identical unreliable backhaul connections, the CDF of the received SNR at R_m via the best transmitter is given as

$$F_{\gamma_R^{k^*,m}}(x) = 1 + \sum_{k=1}^{K} \sum_{\omega_1,\ldots,\omega_{N_R}}^{k} \binom{K}{k} \left(\frac{k!}{\omega_1!\ldots\omega_{N_R}!}\right) \times \frac{(-1)^k \lambda^k}{\prod_{t=0}^{N_R-1} (t!(\widetilde{\alpha}_T)^t)^{\omega_{t+1}}} x^{\sum_{t=0}^{N_R-1} t\omega_{t+1}} e^{-kx/\widetilde{\alpha}_T}. \quad (8)$$

Proof: The proof is given in Appendix A. □

In the second phase, one relay is selected such that the SINR between the particular relay and N eavesdroppers is minimized. It can be formulated as

$$\text{Phase 2:} \quad m^* = \arg \min_{m=1,\ldots,M} \gamma_E^{m,n^*}, \quad (9)$$

where $\gamma_E^{m,n^*} = \max(\gamma_E^{m,1}, \ldots, \gamma_E^{m,N})$ is the maximum instantaneous SINR between R_m and N eavesdroppers. The CDF of the RV γ_E^{m,n^*} is given in the following lemma.

Lemma 1: For the independent and identically distributed (i.i.d.) frequency selective fading channels, the CDF of the instantaneous SINR between R_m and N eavesdroppers is given as

$$F_{\gamma_E^{m,n^*}}(x) = \widehat{\sum_{N,n,N_E}} e^{-\varphi_1^N x} x^{\varphi_2^N} \left(\frac{1}{\widetilde{\alpha}_J} + \frac{x}{\widetilde{\alpha}_E}\right)^{-\varphi_3^N}, \quad (10)$$

where $\varphi_1^N \triangleq n/\widetilde{\alpha}_E$, $\varphi_2^N \triangleq \sum_{t=0}^{N_E-1} t\vartheta_{t+1}$, $\varphi_3^N \triangleq \sum_{\eta_1=0}^{0}(N_J+\eta_1)\mu_{1,\eta_1+1} + \sum_{\eta_2=0}^{1}(N_J+\eta_2)\mu_{2,\eta_2+1} + \ldots + \sum_{\eta_{N_E}=0}^{N_E-1}(N_J+\eta_{N_E})\mu_{N_E,\eta_{N_E}+1}$ and $\widehat{\sum_{N,n,N_E}}$ is the shorthand notation given by (11) *at the top of next page.*

Proof: The proof is given in Appendix B. □

Given M independent relays, the statistical property of the achievable SINR at the eavesdroppers via R_m is given in the following theorem.

Theorem 2: For the i.i.d. frequency selective fading channels, the PDF of the instantaneous SINR between R_m and the eavesdroppers, denoted by $\gamma_E^{m^*,n^*}$, is given by (12) *at the top of next page.*

Proof: The proof is given in Appendix C. □

Since the DF relaying protocol is adopted at the relays, the selected relay processes the received information and then directly forward to D. The instantaneous end-to-end SNR at D from the m^*-th relay, denoted by $\widetilde{\gamma}_{DF}^{m^*}$, is mathematically given by

$$\widetilde{\gamma}_{DF}^{m^*} = \min(\gamma_R^{k^*,m^*}, \gamma_D^{m^*}), \quad (14)$$

where $\gamma_D^{m^*}$ recalls the instantaneous SNR between the m^*-th relay and D in the second time slot. The CDF of the RV $\gamma_D^{m^*}$ is given as

$$F_{\gamma_D^{m^*}}(x) = 1 - e^{-x/\widetilde{\alpha}_D} \sum_{q=0}^{N_D-1} \frac{1}{q!} \left(\frac{x}{\widetilde{\alpha}_D}\right)^q. \quad (15)$$

According to (14), the statistical property of the instantaneous end-to-end SNR at D $\widetilde{\gamma}_{DF}^{m^*}$ can be obtained by the following theorem.

Theorem 3: For the proposed cooperative HetNet with unreliable backhaul links, the CDF of the instantaneous SNR at D via the m^*-th relay is given by

$$F_{\widetilde{\gamma}_{DF}^{m^*}}(x) = 1 + \widetilde{\sum_{D}} x^{\beta} e^{-\Phi x}, \quad (16)$$

where $\beta = \sum_{t=0}^{N_R-1} t\omega_{t+1} + q$, $\Phi = k/\widetilde{\alpha}_T + 1/\widetilde{\alpha}_D$ and $\widetilde{\sum_{D}}$ is the shorthand notation of

$$\widetilde{\sum_{D}} = \sum_{k=1}^{K} \sum_{q=0}^{N_D-1} \sum_{\omega_1,\ldots,\omega_{N_R}}^{k} \binom{K}{k} \left(\frac{k!}{\omega_1!\ldots\omega_{N_R}!}\right) \times (-1)^k \lambda^k \frac{1}{q! \prod_{t=0}^{N_R-1} (t!(\widetilde{\alpha}_T)^t)^{\omega_{t+1}}} \left(\frac{1}{\widetilde{\alpha}_D}\right)^q. \quad (17)$$

Proof: According to the definition of RV $\widetilde{\gamma}_{DF}^{m^*}$, which is given in (14), the CDF of $\widetilde{\gamma}_{DF}^{m^*}$ can be expressed as

$$F_{\widetilde{\gamma}_{DF}^{m^*}}(x) = 1 - [1 - F_{\gamma_R^{k^*,m^*}}(x)][1 - F_{\gamma_D^{m^*}}(x)]. \quad (18)$$

$$\widehat{\sum_{N,n,N_E}} = \sum_{n=0}^{N} \sum_{\vartheta_1,\ldots,\vartheta_{N_E}}^{n} \sum_{\mu_{1,1}}^{\vartheta_1} \sum_{\mu_{2,1},\mu_{2,2}}^{\vartheta_2} \cdots \sum_{\mu_{N_E,1},\ldots,\mu_{N_E,N_E}}^{\vartheta_{N_E}} \binom{N}{n}(-1)^n \left(\frac{n!}{\vartheta_1!\ldots\vartheta_{N_E}!}\right)\left(\frac{\vartheta_1!}{\mu_{1,1}!}\right)\left(\frac{\vartheta_2!}{\mu_{2,1}!\mu_{2,2}!}\right)\cdots$$
$$\times \left(\frac{\vartheta_{N_E}!}{\mu_{N_E,1}!\ldots\mu_{N_E,N_E}!}\right)\left(\frac{1}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\right)^n \frac{1}{\prod_{t=0}^{N_E-1}(t!(\widetilde{\alpha}_E)^t)^{\vartheta_{t+1}}} \prod_{\eta_1=0}^{0}\left[\binom{0}{\eta_1}\Gamma(N_J+\eta_1)\right]^{\mu_{1,\eta_1+1}}$$
$$\times \prod_{\eta_2=0}^{1}\left[\binom{1}{\eta_2}\Gamma(N_J+\eta_2)\right]^{\mu_{2,\eta_2+1}} \cdots \prod_{\eta_{N_E}=0}^{N_E-1}\left[\binom{N_E-1}{\eta_{N_E}}\Gamma(N_J+\eta_{N_E})\right]^{\mu_{N_E,\eta_{N_E}+1}}. \quad (11)$$

$$f_{\gamma_E^{m^*,n^*}}(x) = \mathcal{Q}\widetilde{\sum_E} e^{-\widetilde{\varphi}_1 x}\left(\mathcal{B}_1 x^{\widetilde{\varphi}_2} - \mathcal{B}_2 x^{\widetilde{\varphi}_2-1} + \mathcal{B}_3 x^{\widetilde{\varphi}_2+1}\right)\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-\widetilde{\varphi}_3}, \quad (12)$$

where $\mathcal{Q} \triangleq \frac{MN}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}$, $\mathcal{B}_1 \triangleq \frac{1/\widetilde{\alpha}_J + N_J + j - i}{\widetilde{\alpha}_E}$, $\mathcal{B}_2 \triangleq \frac{i}{\widetilde{\alpha}_J}$, $\mathcal{B}_3 \triangleq \frac{1}{(\widetilde{\alpha}_E)^2}$, $\widetilde{\varphi}_1 \triangleq 1/\widetilde{\alpha}_E + \varphi_1^{N-1} + \varphi_1^{mN}$, $\widetilde{\varphi}_2 \triangleq \varphi_2^{N-1} + \varphi_2^{mN} + i$, $\widetilde{\varphi}_3 \triangleq \varphi_3^{N-1} + \varphi_3^{mN} + N_J + j + 1$ and $\widetilde{\sum_E}$ is the shorthand notation of

$$\widetilde{\sum_E} \triangleq \widehat{\sum_{N-1,l,N_E}} \widehat{\sum_{mN,r,N_E}} \sum_{m=0}^{M-1}\sum_{i=0}^{N_E-1}\sum_{j=0}^{i}\binom{M-1}{m}\binom{i}{j}(-1)^m \frac{1}{i!(\widetilde{\alpha}_E)^i}\Gamma(N_J+j). \quad (13)$$

By substituting (8) and (15) into (18) and after some simple manipulations, the CDF of instantaneous end-to-end SNR at D is obtained as in (16). □

IV. SECRECY PERFORMANCE ANALYSIS

In this section, we investigate the secrecy performance of the proposed network based on the statistical properties derived in Section III. We first focus on the secrecy outage probability, where the eavesdroppers's CSI is assumed unavailable in the considered network. In this case, the transmitters encode and send the confidential message with the constant secrecy rate of θ. If the instantaneous secrecy capacity, denoted by $\mathcal{C}_S$ in bits/s/Hz, is greater than θ, the secrecy gain is guaranteed. Otherwise, information-theoretic security is compromised [27]. The asymptotic secrecy outage probability is then attained to study the asymptotic behavior of the proposed network.

The secrecy capacity $\mathcal{C}_S$ can be expressed as [28]

$$\mathcal{C}_S = \frac{1}{2}\left[\log_2(1+\widetilde{\gamma}_{DF}^{m^*}) - \log_2(1+\gamma_E^{m^*,n^*})\right]^+, \quad (19)$$

where $\log_2(1+\widetilde{\gamma}_{DF}^{m^*})$ is the instantaneous capacity at D respect to the m^*-th relay and $\log_2(1+\gamma_E^{m^*,n^*})$ is the instantaneous capacity of the wiretap channel between the m^*-th relay and n^*-th eavesdropper.

A. SECRECY OUTAGE PROBABILITY

The secrecy outage probability, which is defined as the probability that the secrecy capacity falls below the given rate threshold, can be expressed as [14], [29]

$$\mathcal{P}_{out}(\theta) = Pr(\mathcal{C}_S < \theta) = \int_0^\infty F_{\widetilde{\gamma}_{DF}^{m^*}}\left(2^{2\theta}(1+x)-1\right) f_{\gamma_E^{m^*,n^*}}(x)\,dx. \quad (20)$$

From (20), the closed-from expression for the secrecy outage probability is given in the following theorem.

Theorem 4: For the cooperative single-carrier HetNet with unreliable backhaul links, the secrecy outage probability with two-phase transmitter/relay selection scheme is given as in (21) *at the top of next page.*

Proof: The proof is given in Appendix D. □

To provide full insights into the impacts of unreliable backhaul connections, the asymptotic expression for the secrecy outage probability is given in the following theorem.

Theorem 5: Given the fixed set $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$, *the asymptotic expression for secrecy outage probability is given as* (22) *at the top of next page.*

Proof: Observing the CDF of RV $\gamma_D^{m^*}$ in (15), we find that $e^{-x/\widetilde{\alpha}_D} \overset{\widetilde{\alpha}_D\to\infty}{\approx} 1$ and $\sum_{q=0}^{N_D-1}$ is dominated by $q=0$ when $\widetilde{\alpha}_D \to \infty$. Thus,

$$\lim_{\widetilde{\alpha}_D\to\infty} F_{\gamma_D^{m^*}}(x) \approx 0, \quad (23)$$

which yields the CDF of the instantaneous end-to-end SNR of D as

$$F_{\widetilde{\gamma}_{DF}^{m^*}}(x) = 1 + \widetilde{\sum_{D^\infty}} x^{\tilde{\beta}} e^{-\tilde{\Phi}x}. \quad (24)$$

By substituting (12) and (24) into (20), the asymptotic outage probability is obtained as in (22). □

From (22), we observe that since the backhaul links are unreliable, the secrecy diversity gain is not achievable. Furthermore, the asymptotic secrecy outage is independent of DoF of channels between relay and D. Thus, the limitation on secrecy outage probability is determined as a constant.

$$\mathcal{P}_{out}(\theta) = 1 + \mathcal{Q}\widetilde{\sum_{D}}\widetilde{\sum_{E}}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}(\Upsilon-1)^{\beta-\alpha}(\Upsilon)^{\alpha}\widetilde{\alpha}_{E}^{\widetilde{\varphi}_3}e^{-\Phi\,(\Upsilon-1)}(\mathcal{O}_1-\mathcal{O}_2+\mathcal{O}_3), \tag{21}$$

where $\Upsilon \triangleq 2^{2\theta}$, $\epsilon \triangleq \dfrac{\widetilde{\alpha}_E}{\widetilde{\alpha}_J}$ and

$$\begin{aligned}
\mathcal{O}_1 &= \mathcal{B}_1\Gamma(\widetilde{\varphi}_2+\alpha+1)\epsilon^{\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3}\Psi\,(\widetilde{\varphi}_2+\alpha+1,\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3,\epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)),\\
\mathcal{O}_2 &= \mathcal{B}_2\Gamma(\widetilde{\varphi}_2+\alpha)\epsilon^{\widetilde{\varphi}_2+\alpha-\widetilde{\varphi}_3}\Psi\,(\widetilde{\varphi}_2+\alpha,\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3,\epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)),\\
\mathcal{O}_3 &= \mathcal{B}_3\Gamma(\widetilde{\varphi}_2+\alpha+2)\epsilon^{\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3}\Psi\,(\widetilde{\varphi}_2+\alpha+2,\widetilde{\varphi}_2+\alpha+3-\widetilde{\varphi}_3,\epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)).
\end{aligned}$$

$$\mathcal{P}_{out}^{\infty}(\theta) \overset{\widetilde{\alpha}_D\to\infty}{=} 1 + \mathcal{Q}\widetilde{\sum_{D^\infty}}\widetilde{\sum_{E}}\sum_{\alpha=0}^{\tilde{\beta}}\binom{\tilde{\beta}}{\alpha}(\Upsilon-1)^{\tilde{\beta}-\alpha}(\Upsilon)^{\alpha}\widetilde{\alpha}_{E}^{\widetilde{\varphi}_3}e^{-\tilde{\Phi}(\Upsilon-1)}(\widehat{\mathcal{O}_1}-\widehat{\mathcal{O}_2}+\widehat{\mathcal{O}_3}), \tag{22}$$

where $\tilde{\beta} = \sum_{t=0}^{N_R-1} t\omega_{t+1}$, $\tilde{\Phi} = \dfrac{k}{\widetilde{\alpha}_T}$, $\widetilde{\sum_{D^\infty}} = \sum_{k=1}^{K}\sum_{\omega_1,\ldots,\omega_{N_R}}^{k}\binom{K}{k}\left(\dfrac{k!}{\omega_1!\ldots\omega_{N_R}!}\right)\dfrac{(-1)^{k-1}\lambda^k}{\prod_{t=0}^{N_R-1}(t!(\widetilde{\alpha}_T)^t)^{\omega_{t+1}}}$, and

$$\begin{aligned}
\widehat{\mathcal{O}_1} &= \mathcal{B}_1\Gamma(\widetilde{\varphi}_2+\alpha+1)\epsilon^{\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+1,\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3,\epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right),\\
\widehat{\mathcal{O}_2} &= \mathcal{B}_2\Gamma(\widetilde{\varphi}_2+\alpha)\epsilon^{\widetilde{\varphi}_2+\alpha-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha,\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3,\epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right),\\
\widehat{\mathcal{O}_3} &= \mathcal{B}_3\Gamma(\widetilde{\varphi}_2+\alpha+2)\epsilon^{\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+2,\widetilde{\varphi}_2+\alpha+3-\widetilde{\varphi}_3,\epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right).
\end{aligned}$$

B. THE PROBABILITY OF NON-ZERO ACHIEVABLE SECRECY RATE

In wiretap channels, the probability of non-zero achievable secrecy rate is defined as the probability of the positive secrecy rate, which can be achieved if $\widetilde{\gamma}_{DF}^{m^*} > \gamma_E^{m^*,n^*}$ is satisfied. The probability of positive secrecy expression is given by [28]

$$\begin{aligned}
Pr(\mathcal{C}_S>0) &= 1-\mathcal{P}_{out}(0)\\
&= 1-\int_0^{\infty} F_{\widetilde{\gamma}_{DF}^{m^*}}(x) f_{\gamma_E^{m^*,n^*}}(x)\,dx. \qquad (25)
\end{aligned}$$

Thus, the closed-form expression for the probability of non-zero achievable secrecy rate is given in the following theorem.

Theorem 6: For the cooperative single-carrier HetNet with respect to unreliable backhaul links, the probability of non-zero achievable secrecy rate with two-phase transmitter/relay selection scheme is given as in (26) *at the top of next page.*

Proof: By applying the same process as in Theorem 4, the closed-form expression for $Pr(\mathcal{C}_S > 0)$ can be obtained with the help of [30, eq. (2.3.6.9)]. Thus, we arrive at (26). □

To investigate the asymptotic behavior of the probability of non-zero achievable secrecy rate in high SNR regime, the asymptotic expression is given in the following theorem.

Theorem 7: Given the fixed set $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$*, the asymptotic probability of non-zero achievable secrecy rate is given as in* (27) *at the top of next page.*

Proof: The proof is similarly as in Theorem 5. As $\widetilde{\alpha}_D \to \infty$, we have

$$F_{\widetilde{\gamma}_{DF}^{m^*}}(x) \overset{\widetilde{\alpha}_D\to\infty}{=} 1 + \widetilde{\sum_{D^\infty}} x^{\tilde{\beta}} e^{-\tilde{\Phi}x}. \tag{28}$$

By substituting (28) and (12) into (25), we arrive at (27). □

C. ERGODIC SECRECY RATE

The ergodic secrecy rate expression is given by [31]

$$\begin{aligned}
\mathcal{C}_{erg} &= \mathbb{E}\left\{\frac{1}{2}\log_2\left(\frac{1+\widetilde{\gamma}_{DF}^{m^*}}{1+\gamma_E^{m^*,n^*}}\right)\right\}\\
&= \frac{1}{2\ln(2)}\int_0^{\infty}\frac{F_{\gamma_E^{m^*,n^*}}(x)}{1+x}[1-F_{\widetilde{\gamma}_{DF}^{m^*}}(x)]dx, \qquad (29)
\end{aligned}$$

where

$$F_{\gamma_E^{m^*,n^*}}(x) = \int_0^x f_{\gamma_E^{m^*,n^*}}(t)\,dt. \tag{30}$$

The closed-form expression for ergodic secrecy rate is given in the following theorem.

Theorem 8: For the cooperative single-carrier HetNet with unreliable backhaul links, the ergodic secrecy rate with two-phase transmitter/relay selection scheme is given as in (31) *at the top of next page.*

Proof: The proof is given in Appendix E. □

Theorem 9: Given the fixed set $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$*, the asymptotic ergodic secrecy rate is given as* (32) *at the top of next page.*

Proof: Since $\widetilde{\alpha}_D \to \infty$, we observe that

$$F_{\widetilde{\gamma}_{DF}^{m^*}}(x) \overset{\widetilde{\alpha}_D\to\infty}{=} 1 + \widetilde{\sum_{D^\infty}} x^{\tilde{\beta}} e^{-\tilde{\Phi}x}. \tag{33}$$

$$Pr(\mathcal{C}_S > 0) = -\mathcal{Q}\widetilde{\sum_D}\widetilde{\sum_E}\widetilde{\alpha}_E^{\widetilde{\varphi}_3}(\mathcal{N}_1 - \mathcal{N}_2 + \mathcal{N}_3), \tag{26}$$

where

$$\begin{aligned}
\mathcal{N}_1 &= \mathcal{B}_1\Gamma(\widetilde{\varphi}_2+\beta+1)\epsilon^{\widetilde{\varphi}_2+\beta+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\beta+1, \widetilde{\varphi}_2+\beta+2-\widetilde{\varphi}_3, \epsilon(\Phi+\widetilde{\varphi}_1)\right),\\
\mathcal{N}_2 &= \mathcal{B}_2\Gamma(\widetilde{\varphi}_2+\beta)\epsilon^{\widetilde{\varphi}_2+\beta-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\beta, \widetilde{\varphi}_2+\beta+1-\widetilde{\varphi}_3, \epsilon(\Phi+\widetilde{\varphi}_1)\right),\\
\mathcal{N}_3 &= \mathcal{B}_3\Gamma(\widetilde{\varphi}_2+\beta+2)\epsilon^{\widetilde{\varphi}_2+\beta+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\beta+2, \widetilde{\varphi}_2+\beta+3-\widetilde{\varphi}_3, \epsilon(\Phi+\widetilde{\varphi}_1)\right).
\end{aligned}$$

$$Pr(\mathcal{C}_S^{\infty} > 0) \overset{\widetilde{\alpha}_D\to\infty}{=} -\mathcal{Q}\widetilde{\sum_{D^\infty}}\widetilde{\sum_E}\widetilde{\alpha}_E^{\widetilde{\varphi}_3}(\widehat{\mathcal{N}_1} - \widehat{\mathcal{N}_2} + \widehat{\mathcal{N}_3}), \tag{27}$$

where

$$\begin{aligned}
\widehat{\mathcal{N}_1} &= \mathcal{B}_1\Gamma(\widetilde{\varphi}_2+\tilde{\beta}+1)\epsilon^{\widetilde{\varphi}_2+\tilde{\beta}+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\tilde{\beta}+1, \widetilde{\varphi}_2+\tilde{\beta}+2-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}+\widetilde{\varphi}_1)\right),\\
\widehat{\mathcal{N}_2} &= \mathcal{B}_2\Gamma(\widetilde{\varphi}_2+\tilde{\beta})\epsilon^{\widetilde{\varphi}_2+\tilde{\beta}-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\tilde{\beta}, \widetilde{\varphi}_2+\tilde{\beta}+1-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}+\widetilde{\varphi}_1)\right),\\
\widehat{\mathcal{N}_3} &= \mathcal{B}_3\Gamma(\widetilde{\varphi}_2+\tilde{\beta}+2)\epsilon^{\widetilde{\varphi}_2+\tilde{\beta}+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\tilde{\beta}+2, \widetilde{\varphi}_2+\tilde{\beta}+3-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}+\widetilde{\varphi}_1)\right).
\end{aligned}$$

$$\begin{aligned}
\mathcal{C}_{erg} = -\frac{1}{2\ln(2)}\Bigg(&\widetilde{\sum_D}\Gamma(\beta+1)\Psi\left(\beta+1, \beta+1, \Phi\right)\\
&- \widetilde{\sum_D}\sum_{h=0}^{M}\binom{M}{h}(-1)^h\widetilde{\alpha}_J^{\varphi_3^{hN}}\widehat{\sum_{hN,v,N_E}}\frac{(\Phi+\varphi_1^{hN})^{-\varphi_2^{hN}-\beta-1}}{\Gamma(\varphi_3^{hN})}H^{1,1,1,1,1}_{1,(1:1),0,(1:1)}\left[\begin{matrix}\frac{1}{\Phi+\varphi_1^{hN}}\\ \frac{1}{\epsilon(\Phi+\varphi_1^{hN})}\end{matrix}\middle|\begin{matrix}(1+\varphi_2^{hN}+\beta,1)\\ (0,1);(1-\varphi_3^{hN},1)\\ -\\ (0,1);(0,1)\end{matrix}\right]\Bigg),
\end{aligned} \tag{31}$$

$$\begin{aligned}
\mathcal{C}_{erg}^{\infty} \overset{\widetilde{\alpha}_D\to\infty}{=} -\frac{1}{2\ln(2)}\Bigg(&\widetilde{\sum_{D^\infty}}\Gamma(\tilde{\beta}+1)\Psi\left(\tilde{\beta}+1, \tilde{\beta}+1, \tilde{\Phi}\right)\\
&- \widetilde{\sum_{D^\infty}}\sum_{h=0}^{M}\binom{M}{h}(-1)^h\widetilde{\alpha}_J^{\varphi_3^{hN}}\widehat{\sum_{hN,v,N_E}}\frac{(\tilde{\Phi}+\varphi_1^{hN})^{-\varphi_2^{hN}-\tilde{\beta}-1}}{\Gamma(\varphi_3^{hN})}H^{1,1,1,1,1}_{1,(1:1),0,(1:1)}\left[\begin{matrix}\frac{1}{\tilde{\Phi}+\varphi_1^{hN}}\\ \frac{1}{\epsilon(\tilde{\Phi}+\varphi_1^{hN})}\end{matrix}\middle|\begin{matrix}(1+\varphi_2^{hN}+\tilde{\beta},1)\\ (0,1);(1-\varphi_3^{hN},1)\\ -\\ (0,1);(0,1)\end{matrix}\right]\Bigg),
\end{aligned} \tag{32}$$

By substituting (33) and (12) into (29), the asymptotic expression for ergodic secrecy rate is thus obtained as in (32). □

V. NUMERICAL RESULTS

In this section, we provide the numerical results to validate our analysis in Section IV and investigate the secrecy outage probability, probability of non-zero achievable secrecy rate, and ergodic secrecy rate of the considered network. The binary phase-shift keying (BPSK) modulation is adopted in the simulations with transmission block size $S = 64$ symbols. The curves obtained via link-level simulations are denoted by Ex, whereas the curves for analytical results are denoted by An. In the following, we investigate the network performance with various parameters to examine the effects of the degrees of cooperative transmission, DoFs, and backhaul reliability.

A. SECRECY OUTAGE PROBABILITY

Fig. 2 illustrates the secrecy outage probability for various M and N. The network parameters are set as $K = 3, \lambda = 0.995$, $\{N_R, N_E, N_J, N_D\} = \{2, 2, 2, 3\}$, and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\} = \{10, 10, 10\}$ dB. It can be observed that the number of relays/eavesdroppers strongly affects the secrecy outage probability. For example, when $N = 1$, the secrecy outage probability becomes lower when more relays help with

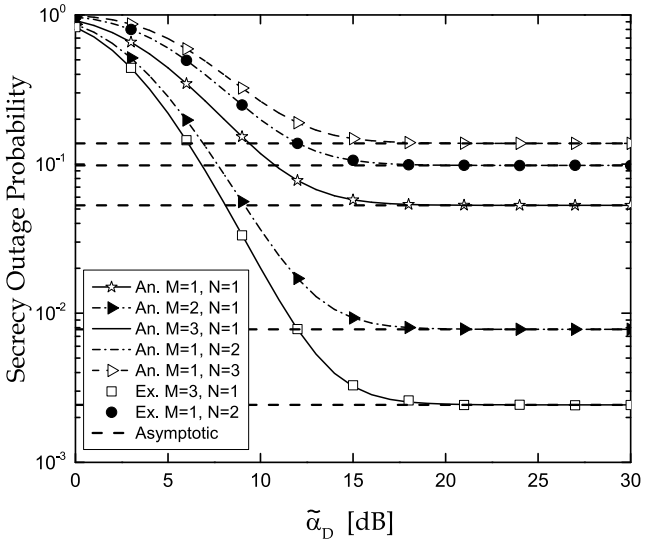

FIGURE 2. Secrecy outage probability for various M, N of the proposed network.

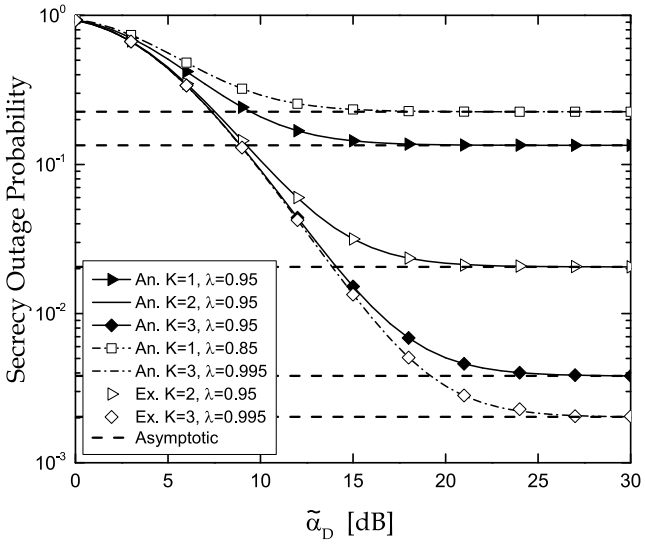

FIGURE 3. Secrecy outage probability for various K, λ of the proposed network.

the cooperative transmission. Differently, when $M = 1$, the secrecy outage probability becomes higher when the number of eavesdroppers increases. This is due to the fact that when the number of relays increases, the secrecy rate becomes higher as a result of the reduction in the wiretap channel capacity. Similarly, the secrecy rate decreases proportionally to the increase in the number of eavesdroppers. We further see that our analysis precisely matches the simulations and our analysis approaches the asymptotic results, presented in Theorem 5, in the high SNR regime.

Fig. 3 plots the secrecy outage probability with various K and λ. We set $M = 2, N = 1, \{N_R, N_E, N_J, N_D\} = \{2, 2, 3, 2\}$, and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\} = \{10, 10, 10\}$ dB. At $\lambda = 0.95$, we observe that when the number of

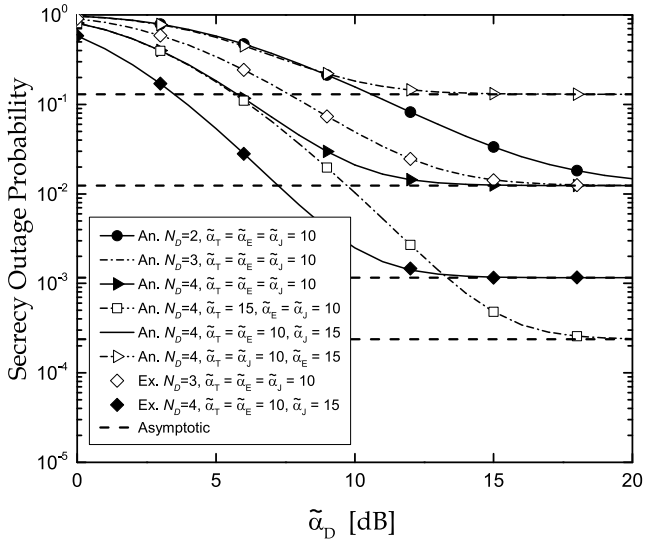

FIGURE 4. Secrecy outage probability for various DoFs and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$ of the proposed network.

transmitters increases, the secrecy outage probability profoundly decreases, due to the increased received signal power at D. When $K = 1$, the secrecy outage probability increases when the backhaul reliability reduces from 0.95 to 0.85. In contrast, the increase in the backhaul reliability, e.g., λ increases from 0.95 to 0.995, leads to a lower secrecy outage probability.

In Fig. 4, we investigate the effects of DoFs and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$ on the secrecy outage probability. In the settings, we set $K = 3, M = 1, N = 2, \lambda = 0.98$, and $\{N_R, N_E, N_J\} = \{2, 2, 4\}$. As N_D increases, we observe that the lower secrecy outage probability is achieved. We also observe that as $\widetilde{\alpha}_T$ and $\widetilde{\alpha}_J$ increase, the secrecy outage probability becomes lower while the increase in $\widetilde{\alpha}_E$ results in high achievable secrecy outage. It is clearly to see that the increase in $\widetilde{\alpha}_T$ results in a high received power at the receiver while the increase in $\widetilde{\alpha}_J$ reduces the SINR of the eavesdroppers.

B. PROBABILITY OF NON-ZERO ACHIEVABLE SECRECY RATE

Fig. 5 shows the probability of non-zero achievable secrecy rate for various M and N. The network parameters are set as $K = 3, \lambda = 0.995, \{N_R, N_E, N_J, N_D\} = \{2, 4, 2, 2\}$, and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\} = \{10, 10, 10\}$ dB. Again, we observe that the analytical results precisely match the simulation ones, and approach the asymptotic ones at high SNRs. We also see that when $N = 1$, the increasing M leads to a higher $Pr(\mathcal{C}_S > 0)$, which implies that the main channel capacity is reliably larger than the wiretap channel capacity. We further see that the increase in the number of eavesdroppers degrades the non-zero achievable secrecy probability.

In Fig. 6, the probability of non-zero achievable secrecy rate is investigated for various K and λ. In this figure, we set $M = 2, N = 1, \{N_R, N_E, N_J, N_D\} = \{2, 2, 2, 2\}$,

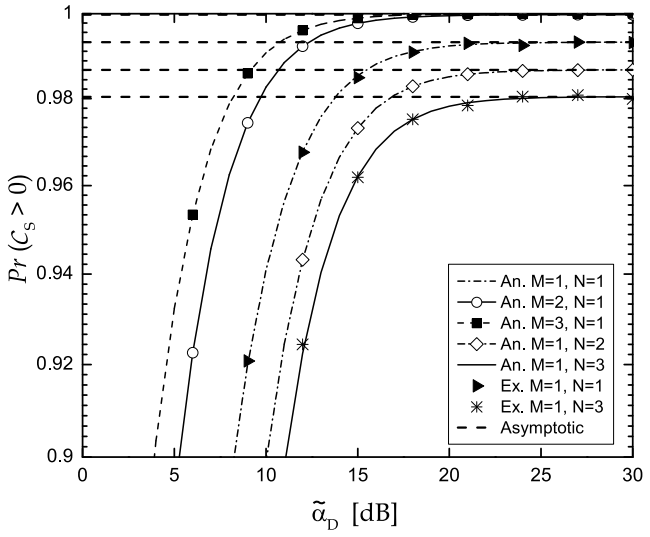

FIGURE 5. Non-zero achievable secrecy rate probability for various M, N of the proposed network.

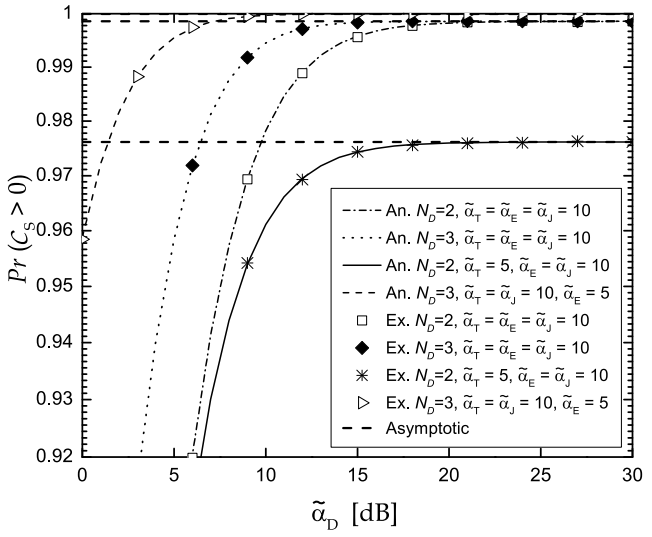

FIGURE 7. Non-zero achievable secrecy rate probability for various DoFs and $\{\tilde{\alpha}_T, \tilde{\alpha}_E, \tilde{\alpha}_J\}$ of the proposed network.

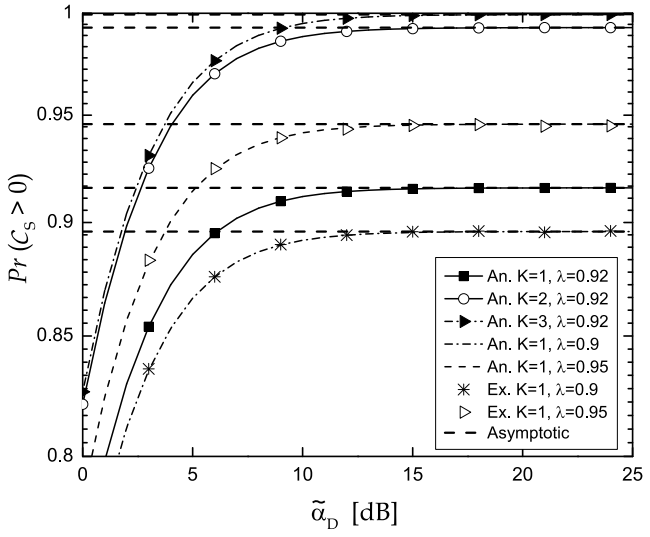

FIGURE 6. Non-zero achievable secrecy rate probability for various K, λ of the proposed network.

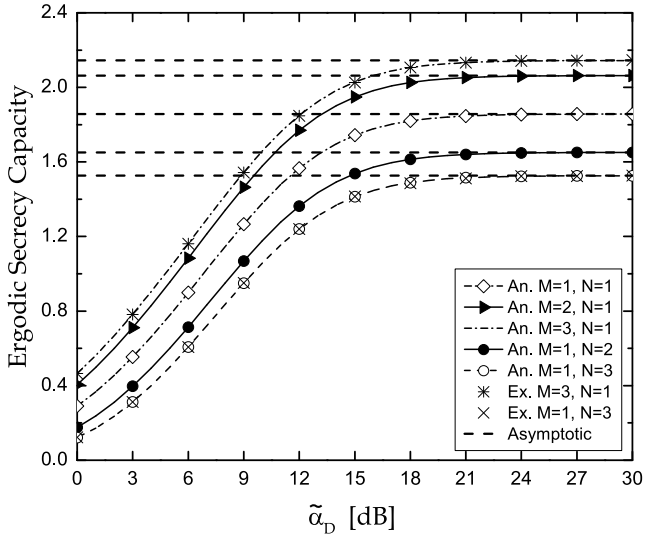

FIGURE 8. Ergodic secrecy rate for various M, N of the proposed network.

and $\{\tilde{\alpha}_T, \tilde{\alpha}_E, \tilde{\alpha}_J\} = \{10, 10, 10\}$ dB. Similar to Fig. 3, the increase in the number of transmitters leads to a higher $Pr(\mathcal{C}_S > 0)$, which is due to the increase in improved main channel capacity. It has been proved that in the case of $\lambda = 0.92$, $Pr(\mathcal{C}_S > 0)$ for $K = 3$ outperforms those for $K = 1$ and $K = 2$. Furthermore, we can observe that at the same level of cooperative transmission, the backhaul reliability gives strong impacts on $Pr(\mathcal{C}_S > 0)$. Specifically, a higher probability of non-zero achievable secrecy rate is achieved if the backhaul links are more reliable.

Fig. 7 plots the probability of non-zero achievable secrecy rate for various DoFs and $\{\tilde{\alpha}_T, \tilde{\alpha}_E, \tilde{\alpha}_J\}$ with the network parameters are set as $K = 3, M = 1, N = 1$, and $\lambda = 0.995$. We observe that when $\tilde{\alpha}_D$ is very low, increasing N_D leads to a higher $Pr(\mathcal{C}_S > 0)$. When $\tilde{\alpha}_D$ is large, the impact of N_D on $Pr(\mathcal{C}_S > 0)$ is insignificant. Moreover, it can be seen that decreasing $\tilde{\alpha}_E$ can improve the network performance due to the reduced achievable SINR at the eavesdroppers. Furthermore, decreasing $\tilde{\alpha}_T$ leads to a lower $Pr(\mathcal{C}_S > 0)$ since less received signal power is obtained at the receiver.

C. ERGODIC SECRECY RATE

Fig. 8 plots the ergodic secrecy rate for various M and N with $K = 3, \lambda = 0.92, \{N_R, N_E, N_J, N_D\} = \{2, 2, 2, 2\}$, and $\{\tilde{\alpha}_T, \tilde{\alpha}_E, \tilde{\alpha}_J\} = \{10, 10, 10\}$ dB. This figure shows, again, the accuracy of our analysis. When $N = 1$, we observe that the ergodic secrecy rate increases with M, which is due to the increasing capacity at D. Differently, the increase in N when $M = 1$ results in the decreased ergodic secrecy rate since the eavesdropping capability increases.

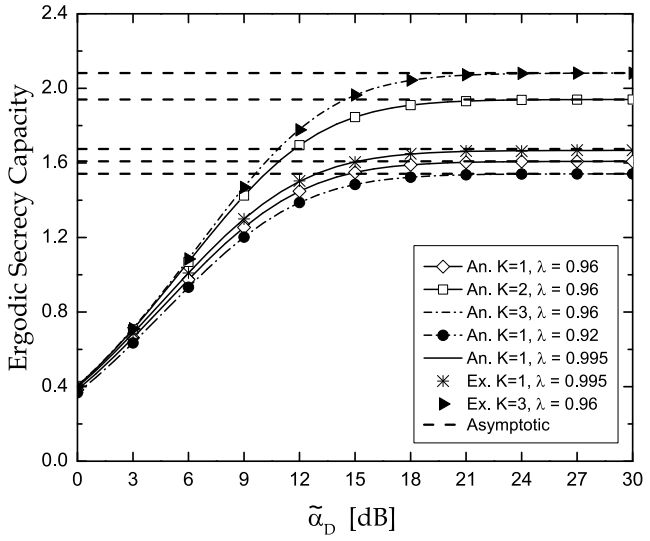

FIGURE 9. Ergodic secrecy rate for various K, λ of the proposed network.

Fig. 9 shows the ergodic capacity for various K and λ. We set $M = 2, N = 1, \{N_R, N_E, N_J, N_D\} = \{2, 2, 2, 2\}$, and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\} = \{10, 10, 10\}$ dB. From this figure, backhaul reliability and the degrees of cooperative transmission reveal their influence the network performance. We can see that $K = 3$ provides the highest ergodic secrecy rate comparing to $K = 1$ and $K = 2$ when $\lambda = 0.96$. For the non-cooperative transmission ($K = 1$), the backhaul link with the highest reliability $\lambda = 0.995$ results in the highest ergodic secrecy rate, compared to $\lambda = 0.92$ and $\lambda = 0.96$.

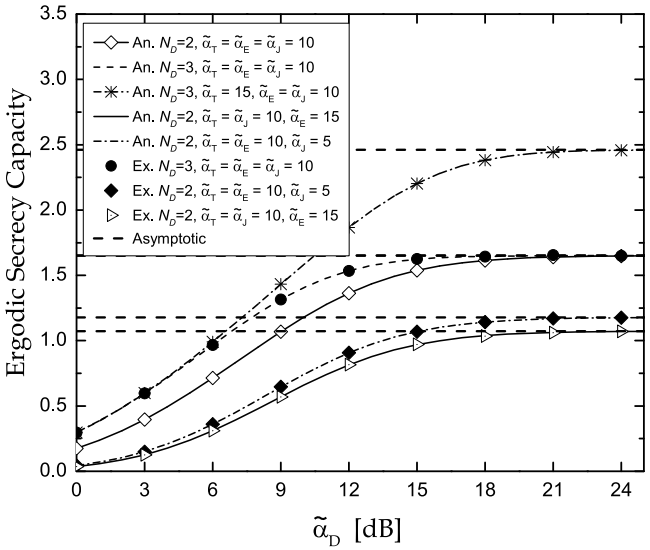

FIGURE 10. Ergodic secrecy rate for various DoFs and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$ of the proposed network.

In Fig. 10, we investigate the ergodic secrecy rate with various DoFs and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$ with $K = 3, M = 1, N = 2$, and $\lambda = 0.92$. In this figure, we observe that the increase in N_D has a positive effect on the network performance, i.e., $N_D = 3$ results a higher ergodic secrecy rate than $N_D = 2$ for $\widetilde{\alpha}_T = \widetilde{\alpha}_E = \widetilde{\alpha}_J = 10$ dB. Also, changing the set $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J\}$ has a strong impact on the ergodic secrecy rate. Specifically, the increase in $\widetilde{\alpha}_T$ and $\widetilde{\alpha}_J$ leads to an increase in the ergodic secrecy rate while the increase in $\widetilde{\alpha}_E$ results in a reduction in the ergodic secrecy capacity.

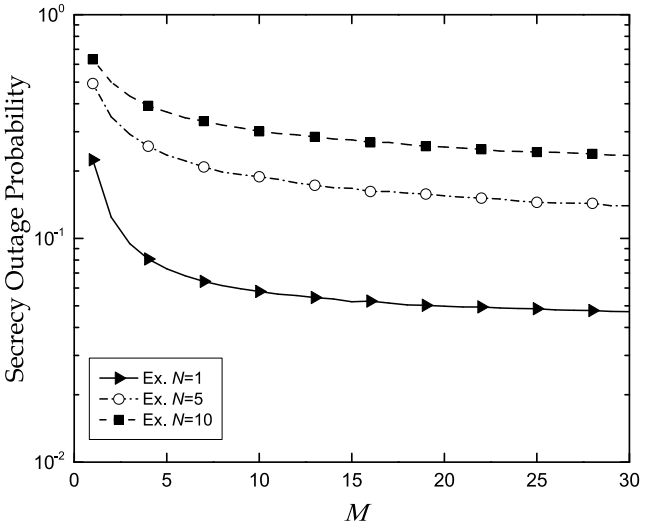

FIGURE 11. Impact of the dense networks on the secrecy outage probability.

In Fig. 11, we show the effects of dense networks on secrecy outage probability versus number of relays M with $K = 10, \lambda = 0.95, \{N_R, N_E, N_J, N_D\} = \{2, 2, 2, 2\}$, and $\{\widetilde{\alpha}_T, \widetilde{\alpha}_E, \widetilde{\alpha}_J, \widetilde{\alpha}_D\} = \{10, 10, 10, 10\}$ dB. It can be seen that the secrecy outage probability almost decreases when more relays cooperate in the network for all cases $N = \{0, 5, 10\}$. Furthermore, the increase in the number of eavesdroppers degrades the system performance since the achievable capacity in the wiretap channels gets higher.

VI. CONCLUSIONS

In this paper, the impacts of unreliable backhaul links on the secrecy performance of cooperative single carrier systems were investigated. To minimize as much information overheard by the eavesdroppers while satisfying the instantaneous SNR at the receiver, a two-phase transmitter/relay selection scheme was proposed. We then derived the exact expressions for the critical secrecy performance metrics such as secrecy outage probability, non-zero secrecy rate probability, and ergodic secrecy rate. The asymptotic expressions were also attained to investigate the network performance at high SNRs. Our results proved that backhaul reliability is determined as an important parameter relative to the scaling of the secrecy performance.

APPENDIX A
PROOF OF THEOREM 1

According to the definition of the RV $\gamma_R^{k,m}$, which is given as $\gamma_R^{k,m} = \widetilde{\alpha}_T ||\boldsymbol{h}^{k,m}||^2 \mathbb{I}_k$, the distribution of the RV $\gamma_R^{k,m}$ is

thus obtained as the product of the Bernoulli process $\mathbb{I}_k$ and the random process $\widetilde{\alpha}_T||\boldsymbol{h}^{k,m}||^2 \sim \chi^2(2N_R, \widetilde{\alpha}_T)$. From (6), the PDF and CDF of the RV $\gamma_R^{k,m}$ can be written as

$$f_{\gamma_R^{k,m}}(x) = (1-\lambda)\delta(x) + \frac{\lambda}{(\widetilde{\alpha}_T)^{N_R}(N_R-1)!}x^{N_R-1}e^{-x/\widetilde{\alpha}_T},$$
$$F_{\gamma_R^{k,m}}(x) = 1 - \lambda e^{-x/\widetilde{\alpha}_T}\sum_{l=0}^{N_R-1}\frac{1}{l!}\left(\frac{x}{\widetilde{\alpha}_T}\right)^l, \quad \text{(A.1)}$$

where $\delta(.)$ denotes the Dirac delta function. Since the best transmitter T_{k^*} is selected, the statistic of the RV $\gamma_R^{k^*,m} = \max(\gamma_R^{1,m}, \ldots, \gamma_R^{K,m})$ is given as

$$\begin{aligned}F_{\gamma_R^{k^*,m}}(x) &= \left[F_{\gamma_R^{k,m}}(x)\right]^K,\\ &= \sum_{k=0}^{K}\binom{K}{k}(-1)^k\left(\lambda e^{-x/\widetilde{\alpha}_T}\sum_{l=0}^{N_R-1}\frac{1}{l!}\left(\frac{x}{\widetilde{\alpha}_T}\right)^l\right)^k\\ &= \sum_{k=0}^{K}\binom{K}{k}(-1)^k\lambda^k e^{-kx/\widetilde{\alpha}_T}\\ &\quad\times\sum_{\omega_1,\ldots,\omega_{N_R}}^{k}\left(\frac{k!}{\omega_1!\ldots\omega_{N_R}!}\right)\frac{x^{\sum_{t=0}^{N_R-1}t\omega_{t+1}}}{\prod_{t=0}^{N_R-1}(t!(\widetilde{\alpha}_T)^t)^{\omega_{t+1}}}.\end{aligned} \quad \text{(A.2)}$$

After some simple manipulations, we arrive at (8).

APPENDIX B
PROOF OF LEMMA 1

According to (4), the distribution of the RV $\gamma_E^{m,n}$ is analytically the joint distribution of the RV $\widetilde{\alpha}_E^{m,n}||\boldsymbol{g}^{m,n}||^2 \sim \chi^2(2N_E, \widetilde{\alpha}_E)$ and RV $\widetilde{\alpha}_J^n||\boldsymbol{q}^n||^2 \sim \chi^2(2N_J, \widetilde{\alpha}_J)$, which can be obtained by

$$\begin{aligned}F_{\gamma_E^{m,n}}(x) &= \mathbb{E}\left\{F_{\widetilde{\alpha}_E^{m,n}||\boldsymbol{g}^{m,n}||^2}((1+y)x) \mid \widetilde{\alpha}_J^n||\boldsymbol{q}^n||^2 = y\right\}\\ &= \int_0^\infty\left(1 - e^{-(1+y)x/\widetilde{\alpha}_E}\sum_{i=0}^{N_E-1}\frac{1}{i!}\left(\frac{(1+y)x}{\widetilde{\alpha}_E}\right)^i\right)\\ &\quad\times\frac{1}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}y^{N_J-1}e^{-y/\widetilde{\alpha}_J}dy\\ &= 1 - \frac{1}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\sum_{i=0}^{N_E-1}\frac{1}{i!(\widetilde{\alpha}_E)^i}x^i e^{-x/\widetilde{\alpha}_E}\\ &\quad\times\sum_{j=0}^{i}\binom{i}{j}\int_0^\infty y^{N_J+j-1}e^{-y(1/\widetilde{\alpha}_J+x/\widetilde{\alpha}_E)}dy\\ &= 1 - \frac{1}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\sum_{i=0}^{N_E-1}\sum_{j=0}^{i}\binom{i}{j}\frac{\Gamma(N_J+j)}{i!(\widetilde{\alpha}_E)^i}\\ &\quad\times x^i e^{-x/\widetilde{\alpha}_E}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+j)}.\end{aligned} \quad \text{(B.1)}$$

Since the frequency selective fading channels between the particular relay to the eavesdroppers are i.i.d. RVs, the CDF of the RV γ_E^{m,n^*} is given as

$$\begin{aligned}&F_{\gamma_E^{m,n^*}}(x)\\ &= [F_{\gamma_E^{m,n}}(x)]^N\\ &= \sum_{n=0}^{N}\binom{N}{n}(-1)^n\left(\frac{e^{-x/\widetilde{\alpha}_E}}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\right)^n\\ &\quad\times\underbrace{\left(\sum_{l=0}^{N_E-1}\sum_{r=0}^{l}\binom{l}{r}\frac{\Gamma(N_J+r)}{l!(\widetilde{\alpha}_E)^l}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+r)}x^l\right)^n}_{\mathcal{J}_1}\end{aligned} \quad \text{(B.2)}$$

By applying binomial and multinomial theorems, $\mathcal{J}_1$ is obtained as (B.3) at the top of next page.

Substituting (B.3) into (B.2), the CDF of the RV γ_E^{m,n^*} is thus attained as in (10).

APPENDIX C
PROOF OF THEOREM 2

According to the definition of the RV $\gamma_E^{m^*,n^*}$ in (9), which is given by $\gamma_E^{m^*,n^*} = \min(\gamma_E^{1,n^*}, \ldots, \gamma_E^{M,n^*})$, the PDF of $\gamma_E^{m^*,n^*}$ can be mathematically expressed based on the order statistics as

$$f_{\gamma_E^{m^*,n^*}}(x) = Mf_{\gamma_E^{m,n^*}}(x)\left[1 - F_{\gamma_E^{m,n^*}}(x)\right]^{M-1}. \quad \text{(C.1)}$$

From (C.1), $f_{\gamma_E^{m,n^*}}(x)$ can be calculated by taking the first derivative of the CDF of the RV γ_E^{m,n^*}, which is derived in (10). The expression $f_{\gamma_E^{m,n^*}}(x)$ is thus obtained as in (C.2) at the top of next page, where $\mathcal{J}_2$ is derived similarly to Lemma 1 with $\{\varphi_1^{N-1}, \varphi_2^{N-1}, \varphi_3^{N-1}\}$ is the set of parameters corresponding to $\widehat{\sum_{N-1,l,N_E}}$.

Again binomial and multinomial theorems for $\left[1 - F_{\gamma_E^{m,n^*}}(x)\right]^{M-1}$, yields

$$\begin{aligned}&\left[1 - F_{\gamma_E^{m,n^*}}(x)\right]^{M-1}\\ &= \sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\left[1 - \frac{1}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\sum_{l=0}^{N_E-1}\sum_{r=0}^{l}\right.\\ &\quad\left.\times\binom{l}{r}\frac{\Gamma(N_J+r)}{l!(\widetilde{\alpha}_E)^l}x^l e^{-x/\widetilde{\alpha}_E}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+r)}\right]^{mN}\\ &= \sum_{m=0}^{M-1}\binom{M-1}{m}(-1)^m\\ &\quad\times\widehat{\sum_{mN,r,N_E}}e^{-\varphi_1^{mN}x}x^{\varphi_2^{mN}}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-\varphi_3^{mN}},\end{aligned} \quad \text{(C.3)}$$

where $[.]^{mN}$ is evaluated similarly to Lemma 1 and $\{\varphi_1^{mN}, \varphi_2^{mN}, \varphi_3^{mN}\}$ is the set of parameters corresponding to $\widehat{\sum_{mN,r,N_E}}$.

$$
\begin{aligned}
\mathcal{J}_1 &= \sum_{n=0}^{N}\binom{N}{n}(-1)^n\left(\frac{e^{-x/\widetilde{\alpha}_E}}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\right)^n \sum_{\vartheta_1,\ldots,\vartheta_{N_E}}^{n}\left(\frac{n!}{\vartheta_1!\ldots\vartheta_{N_E}!}\right)\frac{1}{\prod_{t=0}^{N_E-1}(t!(\widetilde{\alpha}_E)^t)^{\vartheta_{t+1}}}x^{\sum_{t=0}^{N_E-1}t\vartheta_{t+1}} \\
&\times\left[\sum_{r_1=0}^{0}\binom{0}{r_1}\Gamma(N_J+r_1)\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+r_1)}\right]^{\vartheta_1}\left[\sum_{r_2=0}^{1}\binom{1}{r_2}\Gamma(N_J+r_2)\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+r_2)}\right]^{\vartheta_2}\cdots \\
&\times\left[\sum_{r_{N_E}=0}^{N_E-1}\binom{N_E-1}{r_{N_E}}\Gamma(N_J+r_{N_E})\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+r_{N_E})}\right]^{\vartheta_{N_E}} \\
&= \sum_{n=0}^{N}\binom{N}{n}(-1)^n\left(\frac{e^{-x/\widetilde{\alpha}_E}}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\right)^n \sum_{\vartheta_1,\ldots,\vartheta_{N_E}}^{n}\left(\frac{n!}{\vartheta_1!\ldots\vartheta_{N_E}!}\right)\frac{1}{\prod_{t=0}^{N_E-1}(t!(\widetilde{\alpha}_E)^t)^{\vartheta_{t+1}}}x^{\sum_{t=0}^{N_E-1}t\vartheta_{t+1}} \\
&\times\sum_{\mu_{1,1}}^{\vartheta_1}\left(\frac{\vartheta_1!}{\mu_{1,1}!}\right)\prod_{\eta_1=0}^{0}\left[\binom{0}{\eta_1}\Gamma(N_J+\eta_1)\right]^{\mu_{1,\eta_1+1}}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-\sum_{\eta_1=0}^{0}(N_J+\eta_1)\mu_{1,\eta_1+1}} \\
&\times\sum_{\mu_{2,1},\mu_{2,2}}^{\vartheta_2}\left(\frac{\vartheta_2!}{\mu_{2,1}!\mu_{2,2}!}\right)\prod_{\eta_2=0}^{1}\left[\binom{1}{\eta_2}\Gamma(N_J+\eta_2)\right]^{\mu_{2,\eta_2+1}}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-\sum_{\eta_2=0}^{1}(N_J+\eta_2)\mu_{2,\eta_2+1}}\cdots \\
&\times\sum_{\mu_{N_E,1},\ldots,\mu_{N_E,N_E}}^{\vartheta_{N_E}}\left(\frac{\vartheta_{N_E}!}{\mu_{N_E,1}!\ldots\mu_{N_E,N_E}!}\right)\prod_{\eta_{N_E}=0}^{N_E-1}\left[\binom{N_E-1}{\eta_{N_E}}\Gamma(N_J+\eta_{N_E})\right]^{\mu_{N_E,\eta_{N_E}+1}}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-\sum_{\eta_{N_E}=0}^{N_E-1}(N_J+\eta_{N_E})\mu_{N_E,\eta_{N_E}+1}}
\end{aligned}
\tag{B.3}
$$

$$
\begin{aligned}
f_{\gamma_E^{m,n^*}}(x) &= \frac{\partial F_{\gamma_E^{m,n^*}}(x)}{\partial x} \\
&= \frac{N}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\sum_{i=0}^{N_E-1}\sum_{j=0}^{i}\binom{i}{j}\frac{\Gamma(N_J+j)}{i!(\widetilde{\alpha}_E)^i}\left(\frac{1/\widetilde{\alpha}_J+N_J+j-i}{\widetilde{\alpha}_E}x^i-\frac{i}{\widetilde{\alpha}_J}x^{i-1}+\frac{1}{(\widetilde{\alpha}_E)^2}x^{i+1}\right)e^{-x/\widetilde{\alpha}_E} \\
&\times\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+j+1)}\underbrace{\left[1-\frac{1}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\sum_{l=0}^{N_E-1}\sum_{r=0}^{l}\binom{l}{r}\frac{\Gamma(N_J+r)}{l!(\widetilde{\alpha}_E)^l}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+r)}x^l e^{-x/\widetilde{\alpha}_E}\right]^{N-1}}_{\mathcal{J}_2} \\
&= \frac{N}{(\widetilde{\alpha}_J)^{N_J}(N_J-1)!}\sum_{i=0}^{N_E-1}\sum_{j=0}^{i}\binom{i}{j}\frac{\Gamma(N_J+j)}{i!(\widetilde{\alpha}_E)^i}\left(\frac{1/\widetilde{\alpha}_J+N_J+j-i}{\widetilde{\alpha}_E}x^i-\frac{i}{\widetilde{\alpha}_J}x^{i-1}+\frac{1}{(\widetilde{\alpha}_E)^2}x^{i+1}\right)e^{-x/\widetilde{\alpha}_E} \\
&\times\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-(N_J+j+1)}\widehat{\sum_{N-1,l,N_E}}e^{-\varphi_1^{N-1}x}x^{\varphi_2^{N-1}}\left(\frac{1}{\widetilde{\alpha}_J}+\frac{x}{\widetilde{\alpha}_E}\right)^{-\varphi_3^{N-1}}.
\end{aligned}
\tag{C.2}
$$

By substituting (C.2), (C.3) into (C.1) and after some manipulations, the PDF of the RV $\gamma_E^{m^*,n^*}$ is thus obtained as in (12).

APPENDIX D
PROOF OF THEOREM 4

From the definition of the secrecy outage probability, by substituting (16) and (12) into (20), the secrecy outage probability expression is thus obtained as (D.1) at the top of next page, where $\mathcal{J}_3$ can be evaluated by using the help of [30, Eq. (2.3.6.9)] with $\Psi(a,b,c) = \frac{1}{\Gamma(a)}\int_0^\infty e^{-ct}t^{b-a}(1+t)^{b-a-1}dt$ denotes the confluent hypergeometric function [32, eq. (9.211.4)]. After some manipulations, we arrive at (21).

APPENDIX E
PROOF OF THEOREM 6

According to the order statistics, the CDF of the RV $\gamma_E^{m^*,n^*}$ in (30) can be expressed as

$$
\begin{aligned}
F_{\gamma_E^{m^*,n^*}}(x) &= 1-[1-F_{\gamma_E^{m,n^*}}(x)]^M \\
&= 1-\sum_{h=0}^{M}\binom{M}{h}(-1)^h[F_{\gamma_E^{m,n^*}}(x)]^h \\
&= 1-\sum_{h=0}^{M}\binom{M}{h}(-1)^h[F_{\gamma_E^{m,n}}(x)]^{hN},
\end{aligned}
\tag{E.1}
$$

$$\mathcal{P}_{out}(\theta) = \int_0^\infty \left[1 + \widetilde{\sum_D}(\Upsilon - 1 + \Upsilon x)^\beta e^{-\Phi\,(\Upsilon-1+\Upsilon x)}\right] \mathcal{Q}\widetilde{\sum_E} e^{-\widetilde{\varphi}_1\, x}\left(\mathcal{B}_1\, x^{\widetilde{\varphi}_2} - \mathcal{B}_2\, x^{\widetilde{\varphi}_2-1} + \mathcal{B}_3\, x^{\widetilde{\varphi}_2+1}\right)\left(\frac{1}{\widetilde{\alpha}_J} + \frac{x}{\widetilde{\alpha}_E}\right)^{-\widetilde{\varphi}_3} dx$$
$$= 1 + \mathcal{Q}\widetilde{\sum_D}\widetilde{\sum_E}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}(\Upsilon-1)^{\beta-\alpha}(\theta)^\alpha e^{-\Phi\,(\Upsilon-1)}$$
$$\times \underbrace{\int_0^\infty e^{-(\Phi\Upsilon+\widetilde{\varphi}_1)x}\left(\mathcal{B}_1\, x^{\widetilde{\varphi}_2+\alpha} - \mathcal{B}_2\, x^{\widetilde{\varphi}_2+\alpha-1} + \mathcal{B}_3\, x^{\widetilde{\varphi}_2+\alpha+1}\right)\left(\frac{1}{\widetilde{\alpha}_J} + \frac{x}{\widetilde{\alpha}_E}\right)^{-\widetilde{\varphi}_3} dx}_{\mathcal{J}_3}, \tag{D.1}$$

$$\mathcal{C}_{erg} = -\frac{1}{2\ln(2)}\left(\widetilde{\sum_D}\underbrace{\int_0^\infty \frac{x^\beta e^{-\Phi x}}{1+x}}_{\mathcal{J}_4} - \widetilde{\sum_D}\sum_{h=0}^{M}\binom{M}{h}(-1)^h\widetilde{\alpha}_J^{\varphi_3^{hN}}\widehat{\sum_{hN,v,N_E}}\underbrace{\int_0^\infty \frac{e^{-(\Phi+\varphi_1^{hN})x}x^{\varphi_2^{hN}+\beta}}{(1+x)\,(1+x/\epsilon)^{\varphi_3^{hN}}}}_{\mathcal{J}_5}\right), \tag{E.3}$$

where $[F_{\gamma_E^{m,n^*}}(x)]^{hN}$ can be evaluated similarly to Lemma 1, yields

$$F_{\gamma_E^{m^*,n^*}}(x) = 1 - \sum_{h=0}^{M}\binom{M}{h}(-1)^h \times \widehat{\sum_{hN,v,N_E}} e^{-\varphi_1^{hN}x}x^{\varphi_2^{hN}}\left(\frac{1}{\widetilde{\alpha}_J} + \frac{x}{\widetilde{\alpha}_E}\right)^{-\varphi_3^{hN}}, \tag{E.2}$$

where $\{\varphi_1^{hN}, \varphi_2^{hN}, \varphi_3^{hN}\}$ is the set of parameters corresponding to $\widehat{\sum_{hN,v,N_E}}$. By substituting (E.2) and (16) into (29), the ergodic secrecy rate expression can be written as (E.3) at the top of this page,

where $\mathcal{J}_4$ can be evaluated by using the help of [30, eq. (2.3.6.9)], yields

$$\mathcal{J}_4 = \Gamma(\beta+1)\Psi(\beta+1, \beta+1, \Phi), \tag{E.4}$$

In (E.3), $\mathcal{J}_5$ is in the complex integral form. To evaluate $\mathcal{J}_5$, we first express the product of elementary $(1+x)^{-1}$ and $(1+x/\epsilon)^{-\varphi_3^{hN}}$ in terms of Fox H-function with the help of [33, Appendix A7] as

$$\frac{1}{1+x} = H_{11}^{11}\left[x\,\middle|\,\begin{matrix}(0,1)\\(0,1)\end{matrix}\right],$$
$$\frac{1}{(1+x/\epsilon)^{\varphi_3^{hN}}} = \frac{1}{\Gamma(\varphi_3^{hN})}H_{11}^{11}\left[\frac{x}{\epsilon}\,\middle|\,\begin{matrix}(1-\varphi_3^{hN},1)\\(0,1)\end{matrix}\right], \tag{E.5}$$

where $H_{pq}^{mn}[.]$ denotes the Fox H-function [33, Eq. (1.1.1)]. Applying the integral transform for $\mathcal{J}_5$ with the help of [33, eq. (2.6.2)], yields

$$\mathcal{J}_5 = \frac{(\Phi+\varphi_1^{hN})^{-\varphi_2^{hN}-\beta-1}}{\Gamma(\varphi_3^{hN})} \times H_{1,(1:1),0,(1:1)}^{1,1,1,1,1}\left[\begin{matrix}\frac{1}{\Phi+\varphi_1^{hN}}\\ \frac{1}{\epsilon(\Phi+\varphi_1^{hN})}\end{matrix}\,\middle|\,\begin{matrix}(1+\varphi_2^{hN}+\beta,1)\\(0,1);(1-\varphi_3^{hN},1)\\-\\(0,1);(0,1)\end{matrix}\right], \tag{E.6}$$

where $H_{E,(A:C),F,(B:D)}^{L,N,N',M,M'}[.]$ is the generalized Fox H-function [33, eq. (2.2.1)]. Substituting (E.4) and (E.6) into (E.3), we arrive at (31).

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[2] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

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

[5] K. J. Kim, T. Khan, and P. V. Orlik, "Performance analysis of cooperative systems with unreliable backhauls and selection combining," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2448–2461, Mar. 2017.

[6] K. J. Kim, P. V. Orlik, and T. A. Khan, "Performance analysis of finite-sized co-operative systems with unreliable backhauls," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 5001–5015, Jul. 2016.

[7] H. T. Nguyen, D.-B. Ha, S. Q. Nguyen, and W.-J. Hwang, "Cognitive heterogeneous networks with unreliable backhaul connections," *J. Mobile Netw. Appl.*, to be published.

[8] H. T. Nguyen, T. Q. Duong, O. A. Dobre, and W.-J. Hwang, "Cognitive heterogeneous networks with best relay selection over unreliable backhaul connections," in *Proc. IEEE VTC-Fall*, Toronto, ON, Canada, Sep. 2017.

[9] H. T. Nguyen, T. Q. Duong, and W.-J. Hwang, "Multiuser relay networks over unreliable backhaul links under spectrum sharing environment," *IEEE Commun. Lett.*, to be published.

[10] K. J. Kim, P. L. Yeoh, P. V. 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, Sep. 2016.

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

[12] O. Simeone, O. Somekh, E. Erkip, H. V. Poor, and S. S. Shitz, "Robust communication via decentralized processing with unreliable backhaul links," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4187–4201, Jul. 2011.

[13] 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.

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

[15] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

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

[17] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[18] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Jan. 2017.

[19] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[20] 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.

[21] S. Kato *et al.*, "Single carrier transmission for multi-gigabit 60-GHz WPAN systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 8, pp. 1466–1478, Oct. 2009.

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

[23] K. J. Kim, T. A. Tsiftsis, and H. V. Poor, "Power allocation in cyclic prefixed single-carrier relaying systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2294–2305, Jul. 2011.

[24] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

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

[26] P. J. Davis, *Circulant Matrices*. New York, NY, USA: AMS, 2012.

[27] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* fading channels," *IEEE Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

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

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

[30] A. Prudnikov, Y. A. Brychkov, and O. Marichev, *Elementary Functions* (Integrals and Series), vol. 1, 4th ed. London, U.K.: Gordon and Breach, 1998.

[31] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5051, Dec. 2015.

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

[33] A. M. Mathai and R. K. Saxena, *The H-Function With Applications in Statistics and Other Disciplines*. New Delhi, India: Wiley Eastern, 1978.

HUY T. NGUYEN was born in Ben Tre, Vietnam, in 1990. He received the B.S. degree in computer science and engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2013, the M.S. degree from the Department of Information and Communication System, Inje University, South Korea, in 2016, where he is currently pursuing the Ph.D. degree. His research interests include cooperative communications, cognitive radio, energy-harvesting systems, and physical layer security.

JUNQING ZHANG received the B.Eng. and M.Eng. degrees in electrical engineering from Tianjin University, China, in 2009 and 2012, respectively, and the Ph.D. degree in electronics and electrical engineering from Queen's University Belfast, U.K., in 2016. He is currently a Post-Doctoral Research Fellow with Queen's University Belfast. His research interests include physical layer security, cryptography, and OFDM.

NAN YANG (S'09–M'11) received the B.S. degree in electronics from China Agricultural University in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology, in 2007 and 2011, respectively. He was a Post-Doctoral Research Fellow with the Commonwealth Scientific and Industrial Research Organization from 2010 to 2012 and a Post-Doctoral Research Fellow with the University of New South Wales from 2012 to 2014. He has been with the Research School of Engineering, Australian National University, since 2014, where he is currently a Future Engineering Research Leadership Fellow and a Senior Lecturer. His general research interests include communications theory and signal processing, with specific interests in massive multi-antenna systems, millimeter wave communications, cyber-physical security, and molecular communications. He received the Exemplary Reviewer Award of the IEEE Communications Letters in 2012 and 2013, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award and the Exemplary Reviewer Award of the IEEE Wireless Communications Letters in 2014, the Top Reviewer Award from the IEEE Transactions on Vehicular Technology in 2015, and the Exemplary Reviewer Award of the IEEE Transactions on Communications in 2015 and 2016, respectively. He is also a Co-Recipient of the Best Paper Awards from the IEEE GlobeCOM 2016 and the IEEE VTC 2013-Spring. He is currently serving on the Editorial Board of the IEEE Transactions on Wireless Communications, the IEEE Transactions on Vehicular Technology, and the *Transactions on Emerging Telecommunications Technologies*.

TRUNG Q. DUONG (S'05–M'12–SM'13) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology, Sweden, in 2012. Since 2013, he has joined Queen's University Belfast, U.K. as a Lecturer (Assistant Professor). He has authored or co-authored of 240 technical papers published in scientific journals and presented at international conferences. His current research interests include physical layer security, energy-harvesting communications, and cognitive relay networks. He received the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) 2013, the IEEE International Conference on Communications (ICC) 2014, and the IEEE Global Communications Conference (GLOBECOM). He was a recipient of prestigious Royal Academy of Engineering Research Fellowship from 2016 to 2021. He currently serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTION ON WIRELESS COMMUNICATIONS, the IET Communications, and a Senior Editor of the IEEE COMMUNICATIONS LETTERS. He has also served as a Guest Editor of the special issue for the IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, the IET Communications, the *IEEE Wireless Communications Magazine*, the *IEEE Communications Magazine*, the *EURASIP Journal on Wireless Communications and Networking*, the *EURASIP Journal on Advances Signal Processing*, and he was an Editor of the IEEE COMMUNICATIONS LETTERS, the *Wiley Transactions on Emerging Telecommunications Technologies*, and the *Electronics Letters*.

WON-JOO HWANG (M'03–SM'17) received the B.S. and M.S. degree in computer engineering from Pusan National University, Pusan, South Korea, in 1998 and 2000, and the Ph.D. degree in information systems engineering from Osaka University, Japan, in 2002. He is currently a Full Professor with Inje University, Gyeongnam, South Korea. His research interests are in network optimization and cross layer design. He is a member of the IEICE.