Mobile Networks and Applications
https://doi.org/10.1007/s11036-018-1159-z

Performance Analysis for Secure Cooperative Systems Under Unreliable Backhaul Over Nakagami-*m* Channels

Cheng Yin[1] · **Emiliano Garcia-Palacios**[1]

Abstract

In this paper, the secrecy performance of cooperative heterogeneous networks with unreliable backhaul over Nakagami-*m* fading channels is investigated. To secure the proposed system, a friendly jammer is considered to confuse eavesdroppers. To transmit the signals from the source to the destination, a two-phase transmitter/relay selection scheme is proposed. The best transmitter is selected when the signal-to-noise ratio at the relays is maximized. In the second phase, the best relay is chosen when the jamming signal-to-interference-plus-noise ratio of the eavesdroppers is minimized. To investigate the system performance, closed -form expressions are derived for the secrecy outage probability, ergodic capacity and non-zero achievable secrecy rate. In order to gain an insight into the system, asymptotic analysis is also provided. The results show that the degree of cooperative transmission and backhaul reliability are key parameters in the system and these parameters determine the secrecy performance.

Keywords Unreliable backhaul · Heterogeneous networks · Physical layer security · Nakagami-*m* fading channels

1 Introduction

Due to the increasing wireless data traffic demand, future networks will become more dense and heterogeneous. In heterogeneous networks (HetNets), macro cells and small cells will be used to increase the capacity needed for this rise in traffic demand and to offload traffic. A backhaul link will connect these small cells with the core network. The traditional backhaul is wired and can ensure the connection. However, the cost of the deployment and maintenance is high, especially when a large number of small cells is needed to cover dense scenarios. Moreover, small cells may not need such a highly reliable backhaul as traditional macro cells do [27]. This is because small cells serve a lower traffic capacity than macro cells. In this way, wireless backhaul has emerged as an alternative and attractive approach due to its low cost and flexibility. However, wireless backhaul is not as reliable as its wired backhaul counterpart due to wireless channel impairments such as non-line-of-sight (nLOS) propagation and channel fading [10].

The reliability of the backhaul is an important factor in HetNets and research has been undertaken to investigate how the backhaul reliability can affect the system performance [2, 10–15, 19–22, 31]. In [2], the authors considered co-channel inter-cell interference (ICI) in HetNets with unreliable backhaul and coordinated multi-point (CoMP) transmission was considered to reduce the interference. In [12–15, 22, 31], the impact of unreliable backhaul on cooperative relay systems was investigated. The outage probability of finite-sized selective relaying systems with unreliable backhaul was studied in [15]. A cognitive network with unreliable backhaul was investigated in [21], and asymptotic analysis showed that performance was mainly decided by backhaul reliability. For all the research mentioned on unreliable backhaul connections, backhaul reliability is a key factor in the system performance. Therefore, in a HetNet context it is essential for us to investigate backhaul reliability.

Another aspect that cannot be ignored is security [5]. For a complete study in HetNets system, security needs to be considered. The traditional way to enhance security is deploying cryptographic techniques across upper layers. However, it consumes significant power to encrypt and decrypt data [25]. In addition, with the development of quantum computing, key schemes can be broken and the key infrastructure become insecure [30]. In recent years,

✉ Cheng Yin
cyin01@qub.ac.uk

[1] Queen's University Belfast, Belfast, UK

Published online: 07 November 2018

physical layer security (PLS) has become increasingly popular to secure wireless communications [9, 26, 28]. The main idea of PLS is that the wireless channels are random and unpredictable, thus this can be exploited to keep the information confidential from eavesdroppers. Wyner proposed that when the main channel has better propagation conditions than the eavesdroppers', the communication between legitimate users could be secure [29]. However, when the wiretap channel is better, the secrecy rate can even drop to zero [7]. Various PLS techniques have been investigated to tackle this problem and enhance the security of the main channel; one of the main techniques is using cooperative jamming to generate artificial noise to confuse eavesdroppers [1, 4, 6, 7, 16, 17, 23, 32]. In [6, 32], the authors considered PLS and energy harvesting with a friendly jammer, and the authors in [6] also proposed joint jammer and relay selection schemes. In related work [16], a jammer is assumed to be an energy constrained node with no power of its own and can harvest power from the source node, but cooperative relaying was not considered in this work. However, all of the research above ignored the reliability of the backhaul. As discussed an unreliable wireless backhaul results in poor performance. It is essential to consider backhaul reliability when studying PLS in a small cell HetNet contexts.

Research in [13, 14, 22, 31] has taken into account PLS in relay systems with unreliable backhaul. In [31], the authors studied PLS and energy harvesting. In [14], the authors studied PLS in full-duplex cooperative relay systems. In [13], multiple eavesdroppers that can wiretap information from relay and transmitters are considered in a finite-sized cooperative system. In [22], a friendly jammer was used to confuse eavesdroppers in single carrier systems.

Cooperative jamming in the presence of wireless backhaul over Nakagami-m fading channels has not been studied yet. In this research, we investigate the cooperative jamming in a small cells HetNet context with unreliable backhaul over Nakagami-m fading channel. In our system model, an outage occurs when the system is either not reliable or not secure, hence we assess the secrecy outage probability as a performance parameter. Our main contributions are summarized as below:

- We investigate the secrecy performance of cooperative systems by exploiting cooperative relay and jamming signals in the presence of unreliable backhaul links between macro-cells and small-cells over Nakagami-m fading channels.
- A two-phase transmitter/relay selection scheme is proposed. The achievable SNR at the relays is maximized by applying the best small cell transmitter selection in the first phase. The relay selection scheme is deployed in the second phase to minimize the instantaneous signal-to-interference-plus-noise ratio (SINR) at the eavesdroppers.
- Analytical expressions to evaluate the secrecy outage probability, non-zero achievable secrecy rate, and ergodic capacity are derived in closed-form. 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.
- The effect of the number of small-cell transmitters, relays, eavesdroppers and backhaul reliability on the system performance is investigated.

The remainder of the paper is organized as follows. System and channel models are described in Section 2. Derivation of the SNR distributions in the proposed system is obtained in Section 3. The closed-form expressions for outage probability, ergodic capacity and symbol error rate as well as the asymptotic analysis are carried out in Section 4, while numerical results are presented in Section 5. Finally, the paper is concluded in Section 6.

Notation: $P[\cdot]$ is the probability of occurrence of an event. For a random variable X, $F_X(\cdot)$ denotes its cumulative distribution function (CDF) and $f_X(\cdot)$ denotes the corresponding probability density function (PDF). $\max(\cdot)$ and $\min(\cdot)$ denote the maximum and minimum of their arguments, respectively.

2 System model

We consider a HetNet system with a macro base station, S, K small cells, $T_{\{1,\cdots,K\}}$, M relays, $R_{\{1,\cdots,M\}}$, a jammer, J, N eavesdroppers, $E_{\{1,\cdots,N\}}$ and a destination, D, as shown in Fig. 1. S is connected to T_k via wireless backhaul. We assume that there is no direct link between T_k and D because of the poor channel condition. T_k sends information to D with the help of R_m. A single J transmits jamming signals in the system, and we assume that the jamming signals can be nulled out at D [6]. E_n wiretaps the information transmitted from R_m. All of the nodes are equipped with single antenna and operate in half-duplex. We assume that all the channels are Nakagami-m fading, and the channel power gains are gamma distributed. The cumulative distribution function (CDF) and probability density function (PDF) of the random variable X can be written as

$$F_X(x) = 1 - \exp\left(-\frac{x}{\theta_X}\right) \sum_{i=0}^{m_X-1} \frac{1}{i!} \left(\frac{x}{\theta_X}\right)^i. \quad (1)$$

$$f_X(x) = \frac{x^{m_X-1}}{\Gamma(m_X)\theta_X^{m_X}} \exp\left(-\frac{x}{\theta_X}\right). \quad (2)$$

Where $\Gamma(\cdot,\cdot)$ is the incomplete gamma function [8, Eq. (8.352.6)].

Backhaul reliability is modeled as a Bernoulli process $\mathbb{I}_k$ with success probability s_k where $\mathbb{P}(\mathbb{I}_{k^*} = 1) = s_k$ and $\mathbb{P}(\mathbb{I}_{k^*} = 0) = 1 - s_k$. This indicates that T_k is participating in the transmission if the message is successfully delivered over its dedicated backhaul with probability s_k whereas it defers its transmission with probability $1 - s_k$.

We assume the global channel state information (CSI) is available, which is a common assumption in PLS [22]. The CSI of the eavesdroppers can be known when eavesdroppers are active in the network and their status can be monitored [3].

In the first hop, the received signals at R_m are of the form

$$\boldsymbol{y}_R = \sqrt{\mathcal{P}_t \alpha_T^{k,m}} h_{T_k R_m} \mathbb{I}_k \mathbf{x} + z, \quad (3)$$

where $\mathcal{P}_t$ is the transmit power at T_k and $h_{T_k R_m}$ is the channel coefficient of the link $T_k - R_m$, x is the unit power transmitted symbol and z is the complex additive white Gaussian noise (AWGN) with zero mean and variance σ, i.e., $z \sim CN(0, \sigma)$. The path loss component corresponding to $h_{T_k R_m}$ is denoted as $\alpha_T^{k,m}$, respectively.

In the second hop, the received signals at D are of the form

$$\boldsymbol{y}_D = \sqrt{\mathcal{P}_r \alpha_D^m} h_{R_m D} \mathbf{x} + z, \quad (4)$$

where $\mathcal{P}_r$ is the transmit power at relays and $h_{R_m D}$ is the channel coefficient of the link $R_m - D$. The path loss component corresponding to $h_{R_m D}$ is represented by α_D^m, respectively.

Similarly, the received signals at E are of the form

$$\boldsymbol{y}_E = \sqrt{\mathcal{P}_r \alpha_E^{m,n}} h_{R_m E_n} \mathbf{x} + \sqrt{\mathcal{P}_j \alpha_J^n} h_{J E_n} + z, \quad (5)$$

where $\mathcal{P}_j$ is the transmit power at the jammer, $h_{R_m E_n}$ is the channel coefficient of the link $R_m - E_n$ and $h_{J E_n}$ is the channel coefficient of the link $J - E_n$. The path loss component corresponding to $h_{R_m E_n}$ and $h_{J E_n}$ are denoted as $\alpha_E^{m,n}$ and α_J^n, respectively.

We assume that the unreliable backhaul links are independent from the indices of the K transmitters, i.e., $s_k = s, \forall k$.

3 SNR distributions

In this section, SNR distributions are derived firstly which are necessary for system secrecy performance analysis in the next section.

From Eq. 3, the SNR from T_k and R_m can be given as

$$SNR_{T_k R_m} = \frac{\mathcal{P}_t \alpha_T^{k,m} |h_{T_k R_m}|^2}{\sigma_n^2} \mathbb{I}_k = \widetilde{\alpha}_R |h_{T_k R_m}|^2 \mathbb{I}_k = \lambda^{k,m} \mathbb{I}_k, \quad (6)$$

where $\widetilde{\alpha}_R = \frac{\mathcal{P}_t \alpha_T^{k,m}}{\sigma_n^2}$. $\lambda^{k,m} \sim \text{Ga}(m_R, \theta_R)$.

Similarly, according to Eqs. 4 and 5, the SNR between R_m and D and the SINR between R_m and E_n can be obtained as

$$SNR_{R_m D} = \frac{\mathcal{P}_r \alpha_D^m |h_{R_m D}|^2}{\sigma_n^2} = \widetilde{\alpha}_D |h_{R_m D}|^2 = \lambda_D^m, \quad (7)$$

$$SINR_{R_m E_n} = \frac{\mathcal{P}_r \alpha_E^{m,n} |h_{R_m E_n}|^2}{\sigma_n^2 + \mathcal{P}_j \alpha_J^n |h_{J E_n}|^2} = \frac{\widetilde{\alpha}_E |h_{R_m E_n}|^2}{1 + \widetilde{\alpha}_J |h_{J E_n}|^2} = \frac{\lambda^{m,n}}{1 + \lambda_J^n}, \quad (8)$$

where $\widetilde{\alpha}_D = \frac{\mathcal{P}_r \alpha_D^m}{\sigma_n^2}$, $\widetilde{\alpha}_E = \frac{\mathcal{P}_r \alpha_E^{m,n}}{\sigma_n^2}$ and $\widetilde{\alpha}_J = \frac{\mathcal{P}_j \alpha_J^n}{\sigma_n^2}$. $\lambda_D^m \sim \text{Ga}(m_D, \theta_D)$, $\lambda^{m,n} \sim \text{Ga}(m_E, \theta_E)$ and $\lambda_J^n \sim \text{Ga}(m_J, \theta_J)$.

In order to achieve a high performance of the considered system, our selection scheme is to maximize the performance at the relays and destination and minimize the performance at the eavesdroppers.

3.1 Distribution of the link $T_{k^*} - R_m$

In the first hop, each relay selects a small cell that can achieve the best performance of the link $T_k - R_m$. In this way, the best small cell is selected as

$$k^* = \arg \max_{k=1,\ldots,K} SNR_{T_k R_m}, \quad (9)$$

Corresponding CDF of $SNR_{T_{K^*} R_m}$ is given as

$$F_{SNR_{T_{k^*} R_m}}(x) = 1 + \sum_{k=1}^{K} \sum_{\omega_1,\ldots,\omega_{m_R}}^{k} \binom{K}{k} \left(\frac{k!}{\omega_1!\ldots\omega_{m_R}!}\right) \frac{(-1)^k s^k}{\prod_{t=0}^{m_R-1} (t!(\theta_R)^t)^{\omega_{t+1}}} \times x^{\sum_{t=0}^{m_R-1} t\omega_{t+1}} e^{-kx/\theta_R}. \quad (10)$$

The proof is given in Appendix A.

3.2 Distribution of the link $R_m - E_{n^*}$

In the second hop, the eavesdropper is selected when the SINR between R_m and E_n is maximum to enhance its performance,

$$n^* = \arg \max_{k=1,\ldots,K} SINR_{R_m E_n}. \quad (11)$$

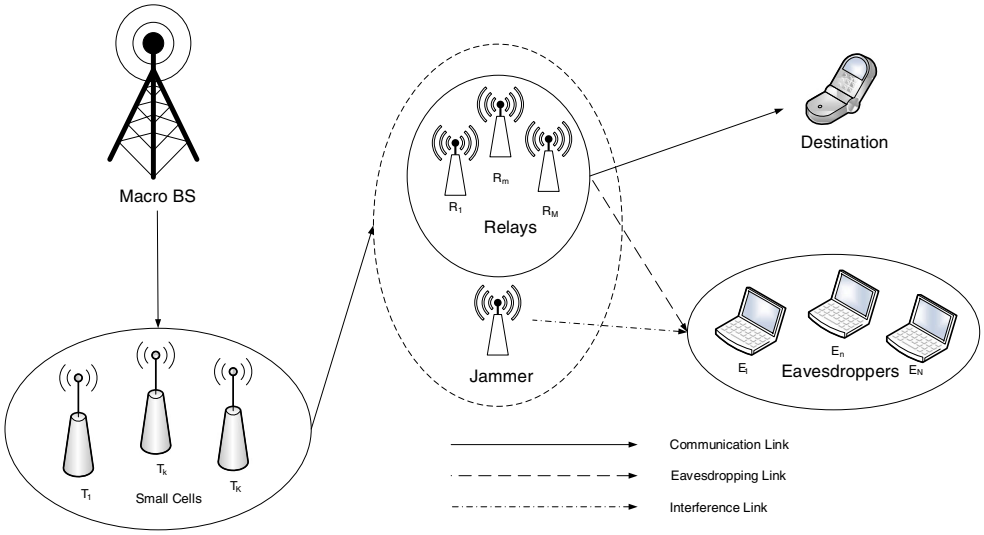

Fig. 1 A cooperative heterogeneous network with multiple small cell transmitters, relays and a friendly jammer in the presence of eavesdroppers

Corresponding CDF of $SINR_{R_m E_{n^*}}$ can be derived according to Appendix B.

3.3 Distribution of the link $R_{m^*} - E_{n^*}$

The relay is selected when the SNR of the link $R_m - E_{n^*}$ is minimized. It can be formulated as

$$m^* = \arg \min_{m=1,\ldots,M} SINR_{R_m E_{n^*}}, \tag{12}$$

corresponding PDF of $SINR_{R_{m^*} E_{n^*}}$ can be derived according to Appendix C and corresponding CDF of $SINR_{R_{m^*} E_{n^*}}$ can be obtained as

$$F_{SINR_{R_{m^*} E_{n^*}}}(x) = \int_0^x f_{SINR_{R_{m^*} E_{n^*}}}(t)\, dt. \tag{13}$$

3.4 Distribution of the end-to-end SNR

The relays use decode-and-forward (DF) protocol for its high system performance. This is because the interference is lower in DF protocol compared with amplify-and-forward (AF) protocol [31]. In this way, the end-to-end SNR of the considered system at the destination is given by

$$SNR_{DF} = \min(SNR_{T_{k^*} R_{m^*}}, SNR_{R_{m^*} D}), \tag{14}$$

where $SNR_{T_{k^*} R_{m^*}}$ is the SNR from the selected small cell transmitter to the selected relay, and $SNR_{R_{m^*} D}$ is the SNR from the selected relay to the destination.

Corresponding CDF of the end-to-end SNR_{DF} can be obtained as

$$\begin{aligned} F_{SNR_{DF}}(x) &= 1 - [1 - F_{SNR_{T_{k^*} R_{m^*}}}(x)] \\ &\quad \times [1 - F_{SNR_{R_{m^*} D}}(x)]. \end{aligned} \tag{15}$$

According to Eq. 15 and by applying binomial and multinomial theorems, the CDF of the end-to-end SNR obtained at D can be given as

$$\begin{aligned} F_{SNR_{DF}}(x) &= 1 + \sum_{k=1}^{K} \sum_{q=0}^{m_D - 1} \sum_{\omega_1,\ldots,\omega_{m_R}}^{k} \binom{K}{k} \left(\frac{k!}{\omega_1! \ldots \omega_{N_R}!} \right) \\ &\quad \times (-1)^k s^k \frac{1}{q! \prod_{t=0}^{m_R - 1} (t! (\theta_R)^t)^{\omega_{t+1}}} \left(\frac{1}{\theta_D} \right)^q \\ &\quad \times x^{\sum_{t=0}^{m_R - 1} t\omega_{t+1} + q} e^{(-k/\theta_R + 1/\theta_D)x}. \end{aligned} \tag{16}$$

4 Secrecy performance analysis

This section derives the performances of secrecy outage probability, non-zero achievable secrecy rate and ergodic capacity utilizing the SNR distributions obtained in the previous section. Towards deriving these performances, secrecy rate is required to be defined first. Secrecy capacity is equal to the difference between main channel and the wiretap channel, which is given by [31]

$$C_S = \frac{1}{2} \left[\log_2(1 + SNR_{DF}) - \log_2(1 + SINR_{R_{m^*} E_{n^*}}) \right]^+, \tag{17}$$

where $[x]^+ = \max(x, 0)$. In addition, $\log_2(1 + SNR_{DF})$ is the instantaneous capacity obtained at D from selected relay and $\log_2(1 + SNR_{R_{m^*} E_{n^*}})$ is the instantaneous capacity of the channel from selected relay to the selected eavesdropper.

4.1 Secrecy outage probability

The secrecy outage probability is introduced to evaluate the system security and it is defined as the probability that the instantaneous secrecy capacity is less than a positive target secrecy rate θ [31], i.e.,

$$\begin{aligned}\mathcal{P}_{out}(\theta) &= Pr(\mathcal{C}_S < \theta)\\ &= \int_0^{\infty} F_{SNR_{DF}}\left(2^{2\theta}(1+x)-1\right)\\ &\quad \times f_{SINR_{R_{m^*}E_{n^*}}}(x)\,dx. \end{aligned} \tag{18}$$

Substitute (15) and (32) into (18), and with the help of [24, Eq. (2.3.6.9)], [8, Eq. (9.211.4)], the expression for secrecy outage probability can be given as (19).

$$\begin{aligned}\mathcal{P}_{out}(\theta) &= 1 + J\widetilde{\sum_{D}}\widetilde{\sum_{E}}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}(\Upsilon-1)^{\beta-\alpha}\\ &\quad\times(\Upsilon)^{\alpha}\theta_E{}^{\widetilde{\varphi}_3}e^{-\Phi(\Upsilon-1)}(J_1-J_2+J_3), \end{aligned} \tag{19}$$

where

$$\begin{cases} J_1 = Q_1\Gamma(\widetilde{\varphi}_2+\alpha+1)\epsilon^{\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+1, \widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3, \epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)\right),\\ J_2 = Q_2\Gamma(\widetilde{\varphi}_2+\alpha)\epsilon^{\widetilde{\varphi}_2+\alpha-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha, \widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3, \epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)\right),\\ J_3 = Q_3\Gamma(\widetilde{\varphi}_2+\alpha+2)\epsilon^{\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+2, \widetilde{\varphi}_2+\alpha+3-\widetilde{\varphi}_3, \epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)\right). \end{cases}$$

and $\beta = \sum_{t=0}^{m_R-1} t$, $\Upsilon = 2^{2\theta}$, $\epsilon = \frac{\theta_E}{\theta_J}$ $J = \frac{MN}{(\theta_J)^{m_J}(m_J-1)!}$.

$$Q_1 = \frac{1/\theta_J + m_J + j - i}{\theta_E},\ Q_2 \triangleq \frac{i}{\theta_J},\ Q_3 = \frac{1}{(\theta_E)^2}.$$

$$\begin{aligned}\varphi_1^N &= n/\theta_E, \varphi_2^N \triangleq \sum_{t=0}^{m_E-1} t\vartheta_{t+1}, \varphi_3^N\\ &= \sum_{\eta_1=0}^{0}(m_J+\eta_1)\mu_{1,\eta_1+1} + \sum_{\eta_2=0}^{1}(m_J+\eta_2)\\ &\quad\times\mu_{2,\eta_2+1} + \ldots + \sum_{\eta_{m_E}=0}^{m_E-1}(m_J+\eta_{m_E})\mu_{m_E,\eta_{m_E}+1}.\end{aligned}$$

$$\begin{aligned}\widetilde{\varphi}_1 &= 1/\theta_E + \varphi_1^{N-1} + \varphi_1^{mN}, \widetilde{\varphi}_2 = \varphi_2^{N-1} + \varphi_2^{mN} + i, \widetilde{\varphi}_3\\ &= \varphi_3^{N-1} + \varphi_3^{mN} + m_J + j + 1.\end{aligned}$$

In addition, $\widehat{\sum_{N,n,m_E}}$, $\widetilde{\sum_{E}}$, $\widetilde{\sum_{D}}$ are the shorthand notations of

$$\begin{cases} \widetilde{\sum_{D}} = \sum_{k=1}^{K}\sum_{q=0}^{m_D-1}\sum_{\omega_1,\ldots,\omega_{m_R}}^{k}\binom{K}{k}\left(\frac{k!}{\omega_1!\ldots\omega_{m_R}!}\right)(-1)^k\lambda^k\\ \qquad \frac{1}{q!\prod_{t=0}^{m_R-1}(t!(\theta_R)^t)^{\omega_{t+1}}}\left(\frac{1}{\theta_D}\right)^q.\\ \widetilde{\sum_{E}} = \widehat{\sum_{N-1,l,m_E}}\ \widehat{\sum_{mN,r,m_E}}\ \sum_{m=0}^{M-1}\sum_{i=0}^{m_E-1}\sum_{j=0}^{i}\binom{M-1}{m}\binom{i}{j}(-1)^m\frac{1}{i!(\theta_E)^i}\Gamma(m_J+j).\\ \widehat{\sum_{N,n,m_E}} = \sum_{n=0}^{N}\sum_{\vartheta_1,\ldots,\vartheta_{m_E}}^{n}\sum_{\mu_{1,1}}^{\vartheta_1}\sum_{\mu_{2,1},\mu_{2,2}}^{\vartheta_2}\cdots\sum_{\mu_{m_E,1},\ldots,\mu_{m_E,m_E}}^{\vartheta_{m_E}}\binom{N}{n}(-1)^n\\ \qquad \left(\frac{n!}{\vartheta_1!\ldots\vartheta_{m_E}!}\right)\left(\frac{\vartheta_1!}{\mu_{1,1}!}\right)\left(\frac{\vartheta_2!}{\mu_{2,1}!\mu_{2,2}!}\right)\ldots\left(\frac{\vartheta_{m_E}!}{\mu_{m_E,1}!\ldots\mu_{m_E,m_E}!}\right)\\ \qquad \left(\frac{1}{(\theta_J)^{m_J}(m_J-1)!}\right)^n\frac{1}{\prod_{t=0}^{m_E-1}(t!(\theta_E)^t)^{\vartheta_{t+1}}}\prod_{\eta_1=0}^{0}\left[\binom{0}{\eta_1}\Gamma(m_J+\eta_1)\right]^{\mu_{1,\eta_1+1}}\\ \qquad \prod_{\eta_2=0}^{1}\left[\binom{1}{\eta_2}\Gamma(m_J+\eta_2)\right]^{\mu_{2,\eta_2+1}}\ldots\\ \qquad \prod_{\eta_{m_E}=0}^{m_E-1}\left[\binom{m_E-1}{\eta_{m_E}}\Gamma(m_J+\eta_{m_E})\right]^{\mu_{m_E,\eta_{m_E}+1}}. \end{cases}$$

To provide full insights into the impact of unreliable backhaul connections, the asymptotic expression for the secrecy outage probability can be obtained as Eq. 20.

$$\mathcal{P}_{out}^{\infty}(\theta) \overset{\theta_D\to\infty}{=} 1 + J\widetilde{\sum_{D^{\infty}}}\widetilde{\sum_{E}}\sum_{\alpha=0}^{\tilde{\beta}}\binom{\tilde{\beta}}{\alpha}(\Upsilon-1)^{\tilde{\beta}-\alpha}(\Upsilon)^{\alpha}\theta_E{}^{\widetilde{\varphi}_3}e^{-\tilde{\Phi}(\Upsilon-1)}(J_4-J_5+J_6), \tag{20}$$

where

$$\begin{cases} J_4 = Q_1\Gamma(\widetilde{\varphi}_2+\alpha+1)\epsilon^{\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+1, \widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right), \\ J_5 = Q_2\Gamma(\widetilde{\varphi}_2+\alpha)\epsilon^{\widetilde{\varphi}_2+\alpha-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha, \widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right), \\ J_6 = Q_3\Gamma(\widetilde{\varphi}_2+\alpha+2)\epsilon^{\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+2, \widetilde{\varphi}_2+\alpha+3-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right). \end{cases}$$

and $\tilde{\beta} = \sum_{t=0}^{m_R-1} t\omega_{t+1}$, $\tilde{\Phi} = \frac{k}{\theta_R}$, $\widetilde{\sum_{D^\infty}} = \sum_{k=1}^{K}\sum_{\omega_1,\ldots,\omega_{m_R}}$ $\binom{K}{k}\left(\frac{k!}{\omega_1!\ldots\omega_{m_R}!}\right)\frac{(-1)^{k-1}s^k}{\prod_{t=0}^{m_R-1}(t!(\theta_R)^t)^{\omega_{t+1}}}$

4.2 Probability of non-zero secrecy rate

The probability of non-zero secrecy rate is the probability that secrecy rate is more than zero, or another way $SNR_{T_{k^*}D}$ is higher than $SINR_{R_{m^*}E_{n^*}}$. The probability of none-zero secrecy rate can be obtained as [31]

$$\begin{aligned} Pr(C_S > 0) &= 1 - \mathcal{P}_{out}(0) \\ &= 1 - \int_0^\infty F_{SNR_{DF}}(x)\, f_{SINR_{R_{m^*}E_{n^*}}}(x)\, dx, \end{aligned} \tag{21}$$

Using Eqs. 15 and 32 and with the help of [24, Eq. (2.3.6.9)]. The closed-form expression for the probability of non-zero achievable secrecy rate is given as, Eq. 22.

$$Pr(\mathcal{C}_S > 0) = -J\widetilde{\sum_D}\widetilde{\sum_E}\theta_E^{\widetilde{\varphi}_3}(J_7 - J_8 + J_9), \tag{22}$$

where

$$\begin{cases} J_7 = Q_1\Gamma(\widetilde{\varphi}_2+\beta+1)\epsilon^{\widetilde{\varphi}_2+\beta+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\beta+1, \widetilde{\varphi}_2+\beta+2-\widetilde{\varphi}_3, \epsilon(\Phi+\widetilde{\varphi}_1)\right), \\ J_8 = Q_2\Gamma(\widetilde{\varphi}_2+\beta)\epsilon^{\widetilde{\varphi}_2+\beta-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\beta, \widetilde{\varphi}_2+\beta+1-\widetilde{\varphi}_3, \epsilon(\Phi+\widetilde{\varphi}_1)\right), \\ J_9 = Q_3\Gamma(\widetilde{\varphi}_2+\beta+2)\epsilon^{\widetilde{\varphi}_2+\beta+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\beta+2, \widetilde{\varphi}_2+\beta+3-\widetilde{\varphi}_3, \epsilon(\Phi+\widetilde{\varphi}_1)\right). \end{cases}$$

To investigate the asymptotic behavior of the probability of non-zero achievable secrecy rate in high SNR regime, the asymptotic expression is given as Eq. 23.

$$Pr(\mathcal{C}_S^\infty > 0) \overset{\theta_D\to\infty}{=} -J\widetilde{\sum_{D^\infty}}\widetilde{\sum_E}\theta_E^{\widetilde{\varphi}_3}(J_{10} - J_{11} + J_{12}), \tag{23}$$

where

$$\begin{cases} J_{10} = Q_1\Gamma(\widetilde{\varphi}_2+\tilde{\beta}+1)\epsilon^{\widetilde{\varphi}_2+\tilde{\beta}+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\tilde{\beta}+1, \widetilde{\varphi}_2+\tilde{\beta}+2-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}+\widetilde{\varphi}_1)\right), \\ J_{11} = Q_2\Gamma(\widetilde{\varphi}_2+\tilde{\beta})\epsilon^{\widetilde{\varphi}_2+\tilde{\beta}-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\tilde{\beta}, \widetilde{\varphi}_2+\tilde{\beta}+1-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}+\widetilde{\varphi}_1)\right), \\ J_{12} = Q_3\Gamma(\widetilde{\varphi}_2+\tilde{\beta}+2)\epsilon^{\widetilde{\varphi}_2+\tilde{\beta}+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\tilde{\beta}+2, \widetilde{\varphi}_2+\tilde{\beta}+3-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}+\widetilde{\varphi}_1)\right). \end{cases}$$

4.3 Ergodic capacity

The ergodic capacity is defined as the average secrecy rate averaged over all the SNR distributions.

Ergodic capacity (nat/s/Hz) is expressed as [31]

$$\mathcal{C}_{erg} = \frac{1}{2\ln(2)}\int_0^\infty \frac{F_{SINR_{E_{n^*},m^*}}(x)}{1+x}[1 - F_{SNR_{DF}}(x)]dx \tag{24}$$

Substitute (13) and (15) into (24), and with the help of [24, Eq. (2.3.6.9)], [18, Eq. (1.1.1)], [18, Eq. (2.6.2)], [18, Appendix A7], ergodic capacity can be evaluated as Eq. 25.

$$\mathcal{C}_{erg} = -\frac{1}{2\ln(2)}\left(\widetilde{\sum_{D}}\Gamma(\beta+1)\Psi\left(\beta+1,\beta+1,\Phi\widetilde{\sum_{D}}\sum_{h=0}^{M}\binom{M}{h}(-1)^h\theta_J{}^{\varphi_3^{hN}}\right)\right.$$
$$\left.-\widehat{\sum_{hN,v,N_E}}\frac{(\Phi+\varphi_1^{hN})^{-\varphi_2^{hN}-\beta-1}}{\Gamma(\varphi_3^{hN})}H^{1,1,1,1,1}_{1,(1:1),0,(1:1)}\left[\begin{array}{c|c}\frac{1}{\Phi+\varphi_1^{hN}} & (1+\varphi_2^{hN}+\beta,1)\\ \frac{1}{\epsilon(\Phi+\varphi_1^{hN})} & (0,1);(1-\varphi_3^{hN},1)\\ & -\\ & (0,1);(0,1)\end{array}\right]\right). \tag{25}$$

To gain the full insights of the system, the asymptotic ergodic capacity is given as Eq. 26.

$$\mathcal{C}_{erg}^{\infty} \overset{\theta_D\to\infty}{=} -\frac{1}{2\ln(2)}\left(\widetilde{\sum_{D^\infty}}\Gamma(\tilde{\beta}+1)\Psi\left(\tilde{\beta}+1,\tilde{\beta}+1,\tilde{\Phi}\widetilde{\sum_{D^\infty}}\sum_{h=0}^{M}\binom{M}{h}(-1)^h\theta_J{}^{\varphi_3^{hN}}\right)\right.$$
$$\left.-\widehat{\sum_{hN,v,m_E}}\frac{(\tilde{\Phi}+\varphi_1^{hN})^{-\varphi_2^{hN}-\tilde{\beta}-1}}{\Gamma(\varphi_3^{hN})}H^{1,1,1,1,1}_{1,(1:1),0,(1:1)}\left[\begin{array}{c|c}\frac{1}{\tilde{\Phi}+\varphi_1^{hN}} & (1+\varphi_2^{hN}+\tilde{\beta},1)\\ \frac{1}{\epsilon(\tilde{\Phi}+\varphi_1^{hN})} & (0,1);(1-\varphi_3^{hN},1)\\ & -\\ & (0,1);(0,1)\end{array}\right]\right). \tag{26}$$

where $H_{pq}^{mn}[.]$ denotes the Fox H-function [18, Eq. (1.1.1)].

5 Numerical results

In this section, numerical results along with simulations are shown for the analysis carried out on the proposed system. The threshold of secrecy outage probability is fixed at $\theta = 1$ bits/s/Hz. The binary phase-shift keying (BPSK) modulation is adopted in the simulations with transmission block size $S = 64$ symbols. In figures, "Sim" represents the simulation results, "Ana" represents the analytical results and "Asy" represents the asymptotic analysis results. We investigate the network performance with various parameters to examine the effects of the degrees of cooperative transmission and backhaul reliability.

5.1 Secrecy outage probability

Fig. 2 investigates the secrecy outage probability for various M and N. The network parameters are set as $K = 3, s = 0.998, \{m_R, m_E, m_J, m_D\} = \{2, 2, 2, 3\}$, and $\{\theta_R, \theta_E, \theta_J\} = \{10, 10, 10\}$ dB. We can observe that the number of relays and eavesdroppers strongly affects the secrecy outage probability. Specifically, when $N = 1$, the secrecy outage probability decreases when the number of relay increases, thus achieving a better system performance. By contrast, when $M = 1$, the secrecy outage probability increases when the number of eavesdropper increases. We can also observe that our results approach asymptotic results in the high SNR regime.

Figure 3 plots the secrecy outage probability with various K and s. We set the parameters as $M = 2, N = 1, \{m_R, m_E, m_J, m_D\} = \{2, 2, 3, 2\}$,and $\{\theta_R, \theta_E, \theta_J\} =$

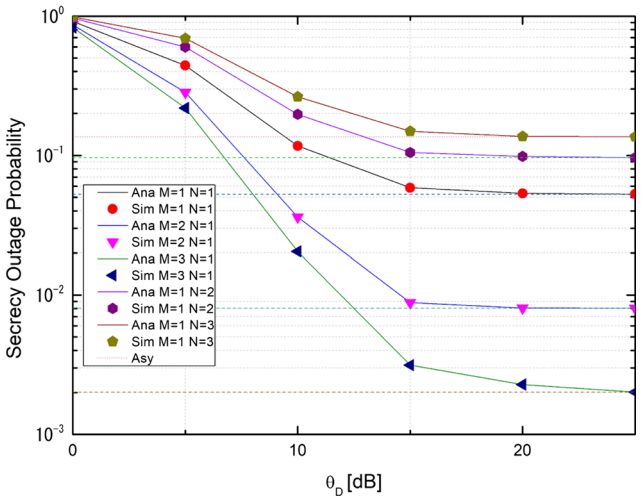

Fig. 2 Secrecy outage probability for various M, N

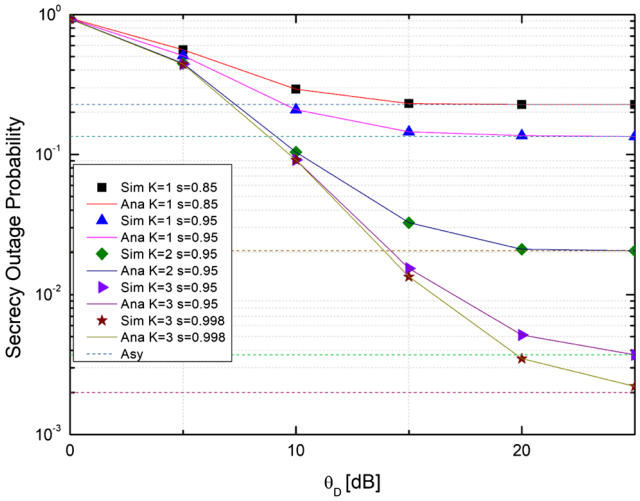

Fig. 3 Secrecy outage probability for various K, s

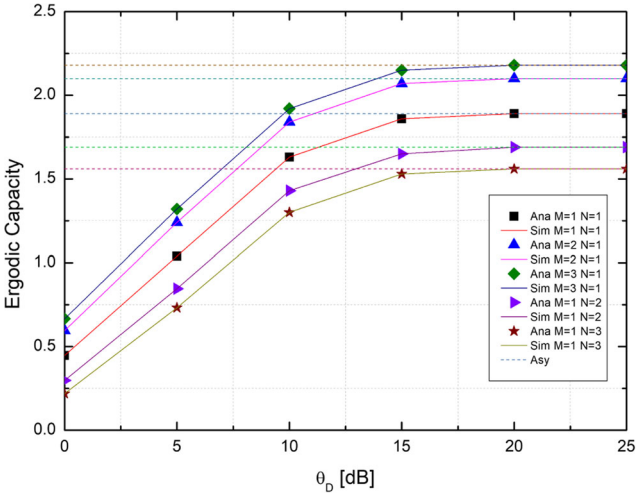

Fig. 5 Ergodic capacity for various M, N

{10, 10, 10} dB. We can observe from the figures that when $K = 1$, the secrecy outage probability decreases when the backhaul reliability gets higher. If the system has more reliable backhaul, it performs better.

In addition, when $s = 0.95$ and the number of small-cell transmitters increases from $K = 1$ to $K = 3$, the secrecy outage probability decreases due to the increased received signal power at D.

Figure 4 shows the effects of dense networks on secrecy outage probability versus number of relays M with $K = 10$, $s = 0.998$, $\{m_R, m_E, m_J, m_D\} = \{2, 2, 2, 3\}$, and $\{\theta_R, \theta_E, \theta_J, \theta_D\} = \{10, 10, 10, 10\}$ dB. We can observe that for all $N = \{1, 5, 10\}$, secrecy outage probability decreases when there are more relays due to the cooperative communication. In addition, with the increase of N from $N = 1$ to $N = 10$, the secrecy outage probability increases.

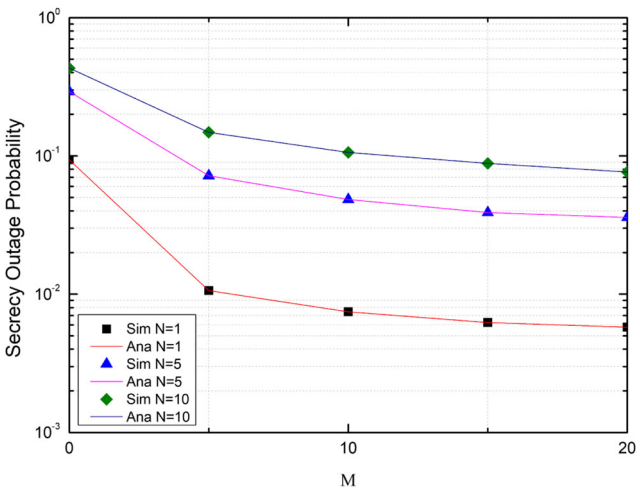

Fig. 4 Impact of the dense networks on the secrecy outage probability

This is because the achievable capacity in the wiretap channels gets higher.

5.2 Ergodic capacity

Figures 5 and 6 depict the effect of the number of small-cell transmitters, the number of relays and eavesdroppers and backhaul reliability on the ergodic capacity. Parameters are the same in the corresponding figures of the ergodic capacity and secrecy outage probability. Effects of the degree of cooperative transmission and reliability of backhaul are complementary on ergodic secrecy rate and secrecy outage probability. When secrecy outage probability decreases, the ergodic secrecy rate would increase. We can observe in the figures that when $N = 1$, the ergodic

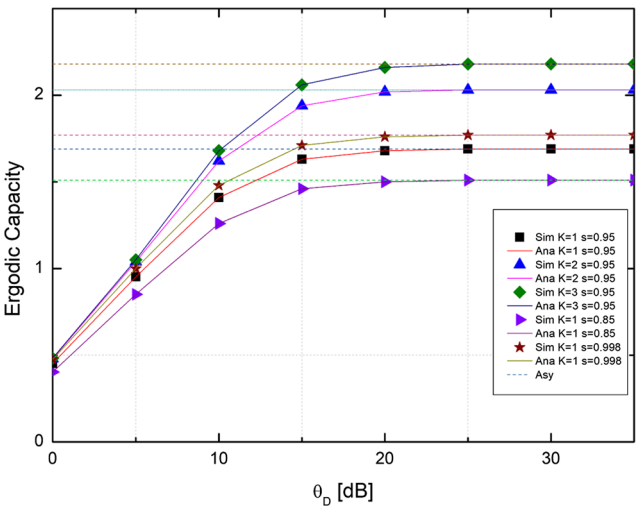

Fig. 6 Ergodic capacity for various K, s

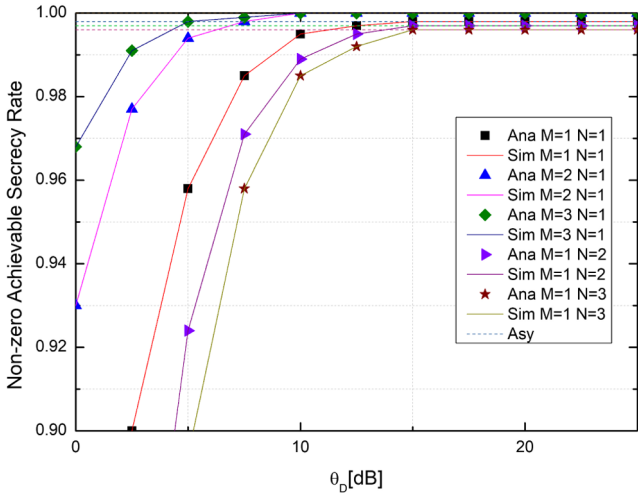

Fig. 7 Non-zero achievable secrecy rate probability for various M, N

capacity increases when the number of relay grows. Also, when $M = 1$, ergodic capacity decreases when the number of eavesdroppers increases. In addition, when $K = 1$, the ergodic capacity increases when the backhaul is more reliable, and when $s = 0.95$, the ergodic capacity increases when the number of small-cell transmitters increases.

5.3 Non-zero achievable secrecy rate

Figures 7 and 8 show the same performances as of secrecy outage probability and ergodic secrecy rate with the same parameters, correspondingly. The observations are similar in all the cases.

In the figure, simulation results match well with the numerical results, thus, validating the analysis presented in the paper.

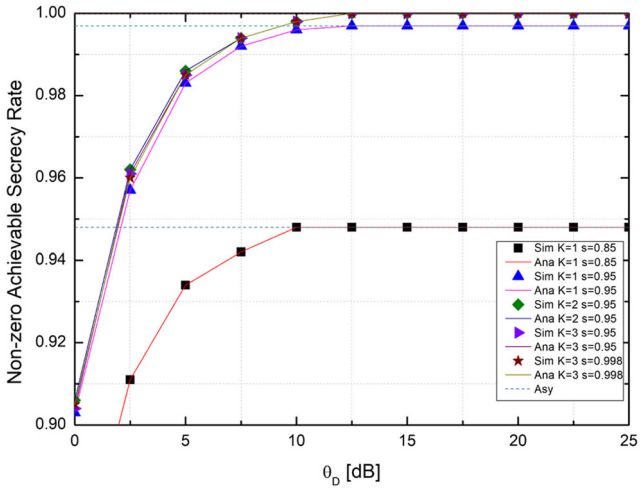

Fig. 8 Non-zero achievable secrecy rate probability for various K, s

6 Conclusions

This paper investigates the secrecy performance of cooperative heterogeneous networks with unreliable backhaul links. A two phase transmitter/relay selection scheme was proposed to maximize the SNR at the relays and minimize the SINR at the eavesdroppers. Closed-form expressions are derived and asymptotic expressions are also provided. Results show that when the number of small-cell transmitters and relays increases, the system can achieve a better performance. However, the increase of eavesdroppers can significantly degrade the system performance. Moreover, backhaul reliability is a key parameter for the improvement of secrecy performance.

Appendix A

Since all the channels follow Nakagami-m fading, and the CDF and PDF can be found in Eqs. 1 and 2. The CDF and PDF of $SNR_{T_k R_m}$ can be written as

$$f_{SNR_{T_k R_m}}(x) = (1-s)\delta(x) + \frac{s}{(\theta_R)^{m_R}(m_R-1)!} x^{m_R-1} e^{-x/\theta_R},$$

$$F_{SNR_{T_k R_m}}(x) = 1 - s e^{-x/\theta_R} \sum_{l=0}^{m_R-1} \frac{1}{l!}\left(\frac{x}{\theta_R}\right)^l, \quad (27)$$

where $\delta(.)$ denotes the Dirac delta function. Since the best transmitter T_{k^*} is selected, the CDF of $SNR_{T_{k^*} R_m}$ can be given as

$$F_{SNR_{T_{k^*} R_m}}(x) = \left[F_{SNR_{T_k R_m}}(x)\right]^K. \quad (28)$$

After some simple manipulations, we can derive (10).

Appendix B

The CDF of $SINR_{R_m E_n}$ can be obtained as

$$F_{SINR_{R_m E_n}}(x) = 1 - \frac{1}{(\theta_J)^{m_J}(m_J-1)!} \times \sum_{i=0}^{m_E-1}\sum_{j=0}^{i}\binom{i}{j}\frac{\Gamma(m_J+j)}{i!(\theta_E)^i}, \times x^i e^{-x/\theta_E}\left(\frac{1}{\theta_J}+\frac{x}{\theta_E}\right)^{-(m_J+j)}. \quad (29)$$

Since the frequency selective fading channels between the particular relay to the eavesdroppers are independent and identically distributed, the CDF of the $SINR_{E_{n^*}}$ is given as

$$F_{SINR_{R_m E_{n^*}}}(x) = [F_{SINR_{R_m E_n}}(x)]^N. \tag{30}$$

Appendix C

We first derive the PDF of $SINR_{R_m E_{n^*}}$,

$$f_{SINR_{R_m E_{n^*}}}(x) = \frac{\partial F_{SINR_{R_m E_{n^*}}}(x)}{\partial x}. \tag{31}$$

Since (12), we derive the PDF of $SINR_{R_{m^*} E_{n^*}}$,

$$f_{SINR_{R_{m^*} E_{n^*}}}(x) = M f_{SINR_{R_m E_{n^*}}} \times (x) \left[1 - F_{SINR_{R_m E_{n^*}}}(x)\right]^{M-1}. \tag{32}$$

References

1. Akitaya T, Asano S, Saba T (2014) Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in mimo-ofdm systems. In: 2014 IEEE international conference on Communications workshops (ICC). IEEE, pp 807–812
2. Ali MS, Synthia M (2015) Performance analysis of jt-comp transmission in heterogeneous network over unreliable backhaul. In: 2015 international conference on Electrical engineering and information communication technology (ICEEICT). IEEE, pp. 1–5
3. Dong L, Han Z, Petropulu AP, Poor HV (2010) Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Process 58(3):1875–1888
4. El Shafie A, Mabrouk A, Tourki K, Al-Dhahir N, Hamila R (2018) A secret-key-aided scheme to secure transmissions from single-antenna rf-eh source nodes. IEEE Wirel Commun Lett 7(2):238–241
5. Hieu TD, Duy TT, Kim BS (2018) Performance enhancement for multihop harvest-to-transmit wsns with path-selection methods in presence of eavesdroppers and hardware noises. IEEE Sensors J 18(12):5173–5186
6. Hoang TM, Duong TQ, Vo NS, Kundu C (2017) Physical layer security in cooperative energy harvesting networks with a friendly jammer. IEEE Wirel Commun Lett 6(2):174–177
7. Hui H, Swindlehurst AL, Li G, Liang J (2015) Secure relay and jammer selection for physical layer security. IEEE Signal Process Lett 22(8):1147–1151
8. Jeffrey A, Zwillinger D (2007) Table of integrals, series, and products. Academic Press, New York
9. Jiang X, Zhong C, Chen X, Duong TQ, Tsiftsis TA, Zhang Z (2016) Secrecy performance of wirelessly powered wiretap channels. IEEE Trans Commun 64(9):3858–3871
10. Khan TA, Orlik P, Kim KJ, Heath RW (2015) Performance analysis of cooperative wireless networks with unreliable backhaul links. IEEE Commun Lett 19(8):1386–1389
11. Kim KJ, Khan TA, Orlik PV (2017) Performance analysis of cooperative systems with unreliable backhauls and selection combining. IEEE Trans Veh Technol 66(3):2448–2461
12. Kim KJ, Orlik PV, Khan TA (2016) Performance analysis of finite-sized co-operative systems with unreliable backhauls. IEEE Trans Wirel Commun 15(7):5001–5015
13. Kim KJ, Yeoh PL, Orlik PV, Poor HV (2016) Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections. IEEE Trans Signal Process 64(17): 4403–4416
14. Liu H, Kim KJ, Tsiftsis TA, Kwak KS, Poor HV (2017) Secrecy performance of finite-sized cooperative full-duplex relay systems with unreliable backhauls. IEEE Trans Signal Process 65(23):6185–6200
15. Liu H, Kwak KS (2017) Outage probability of finite-sized selective relaying systems with unreliable backhauls. In: 2017 international conference on Information and communication technology convergence (ICTC). IEEE, pp 1232–1237
16. Liu W, Zhou X, Durrani S, Popovski P (2016) Secure communication with a wireless-powered friendly jammer. IEEE Trans Wirel Commun 15(1):401–415
17. Liu Y, Wang L, Duy TT, Elkashlan M, Duong TQ (2015) Relay selection for security enhancement in cognitive relay networks. IEEE Wirel Commun Lett 4(1):46–49
18. Mathai AM, Saxena RK (1978) The h function with applications in statistics and other disciplines
19. Nguyen HT, Duong TQ, Dobre OA, Hwang WJ (2017) Cognitive heterogeneous networks with best relay selection over unreliable backhaul connections. In: 2017 IEEE 86th Vehicular technology conference (VTC-fall). IEEE, pp 1–5
20. Nguyen HT, Duong TQ, Hwang WJ (2017) Multiuser relay networks over unreliable backhaul links under spectrum sharing environment. IEEE Commun Lett 21(10):2314–2317
21. Nguyen HT, Ha DB, Nguyen SQ, Hwang WJ (2017) Cognitive heterogeneous networks with unreliable backhaul connections. Mobile Networks and Applications:1–14
22. Nguyen HT, Zhang J, Yang N, Duong TQ, Hwang WJ (2017) Secure cooperative single carrier systems under unreliable backhaul and dense networks impact. IEEE Access 5:18310–18324
23. Nguyen VD, Duong TQ, Shin OS, Nallanathan A, Karagiannidis GK (2017) Enhancing phy security of cooperative cognitive radio multicast communications. IEEE Trans Cogn Commun Netw 3(4):599–613
24. Prudnikov A, Brychkov I, Marichev O (1998) Integrals and Series, vol. 1: Elementary functions. Gordon and Breach Science Publishers, New York
25. Rodríguez LJ, Tran NH, Duong TQ, Le-Ngoc T, Elkashlan M, Shetty S (2015) Physical layer security in wireless cooperative relay networks: State of the art and beyond. IEEE Commun Mag 53(12):32–39
26. Sheng Z, Tuan HD, Nasir AA, Duong TQ, Poor HV (2018) Power allocation for energy efficiency and secrecy of wireless interference networks. IEEE Transactions on Wireless Communications
27. Siddique U, Tabassum H, Hossain E, Kim DI (2015) Wireless backhauling of 5g small cells: challenges and solution approaches. IEEE Wirel Commun 22(5):22–31
28. Wang L, Kim KJ, Duong TQ, Elkashlan M, Poor HV (2015) Security enhancement of cooperative single carrier systems. IEEE Trans Inf Forensic Secur 10(1):90–103
29. Wyner AD (1975) The wire-tap channel. Bell Labs Techn J 54(8):1355–1387

30. Yang M, Guo D, Huang Y, Duong TQ, Zhang B (2016) Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks. IEEE Trans Commun 64(12):5189–5202
31. Yin C, Nguyen HT, Kundu C, Kaleem Z, Garcia-Palacios E, Duong TQ (2018) Secure energy harvesting relay networks with unreliable backhaul connections. IEEE Access 6:12074–12084
32. Zhou X, McKay MR (2010) Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. IEEE Trans Veh Technol 59(8):3831–3842