Secrecy Spectrum and Secrecy Energy Efficiency in Massive MIMO Enabled HetNets

Zhihao Zhong, Jianhua Peng, Kaizhi Huang, Lu Xia, and Xiaohui Qi
National Digital Switching System Engineering & Technological Research Center
Zhengzhou, 450002 - CHINA
[e-mail: b101180166@smail.nju.edu.cn]
*Corresponding author: Zhihao Zhong

Received August 26, 2016; revised November 28, 2016; accepted December 23, 2016; published February 28, 2017

Abstract

Security and resource-saving are both demands of the fifth generation (5G) wireless networks. In this paper, we study the secrecy spectrum efficiency (SSE) and secrecy energy efficiency (SEE) of a *K*-tier massive multiple-input multiple-output (MIMO) enabled heterogeneous cellular network (HetNet), in which artificial noise (AN) are employed for secrecy enhancement. Assuming (i) independent Poisson point process model for the locations of base stations (BSs) of each tier as well as that of eavesdroppers, (ii) zero-forcing precoding at the macrocell BSs (MBSs), and (iii) maximum average received power-based cell selection, the tractable lower bound expressions for SSE and SEE of massive MIMO enabled HetNets are derived. Then, the influences on secrecy oriented spectrum and energy efficiency performance caused by the power allocation for AN, transmit antenna number, number of users served by each MBS, and eavesdropper density are analyzed respectively. Moreover, the analysis accuracy is verified by Monte Carlo simulations.

Keywords: Heterogeneous cellular networks, physical layer security, massive MIMO, energy efficiency, artificial noise

This work has been partly supported by the National Natural Science Foundation of China under Grant No.61401510 and 61521003, and the National High Technology Research & Development Program of China (863 Program) under Grant No.2015AA01A708.

https://doi.org/10.3837/tiis.2017.02.002 **ISSN : 1976-7277**

1. Introduction

Owing to the ever-growing demand for high-quality high-rate wireless communications, the fifth generation (5G) cellular networks in the future are likely to be massive multiple-input multiple-output (MIMO) enabled heterogeneous cellular networks (HetNets) [1]. With a mixture of macrocells and larger number of smaller cells such as microcells, picocells, and femtocells, HetNets bring the network closer to end users, thereby providing higher throughput and coverage [2]. Massive MIMO, also named large-scale antenna arrays, is an emerging physical layer technology which can produce high-resolution spatial beam and significantly improve radio spectral efficiency in HetNets [3]. These benefits have put massive MIMO enabled HetNets in the spotlight of preliminary 5G discussions [4].

In the past few years, the theoretical understanding of massive MIMO enabled HetNets has progressed significantly [5]. Recently, stochastic geometry is emerging as a popular technique that supports comprehensive yet tractable analysis of massive MIMO enabled HetNets [6-7]. To improve throughput in massive MIMO enabled HetNets, inter-tier interference coordination strategies were proposed in [8]. User association and interference management in massive MIMO aided HetNets were further investigated in [9] and [10]. Spectrum and energy efficiency in massive MIMO enabled HetNets were analyzed in [7] and [11].

Since the open nature of wireless channels, ensuring security is an essential task for wireless communication systems regardless of the type of network structure utilized. Physical layer security (PLS) has drawn ever-increasing attention as it can realize secure communication without using any ciphering keys [12]. Research efforts on the PLS have been made by considering different aspects, such as artificial noise (AN) [13], beamforming [14], and cooperative jamming [15], etc. Very recently, the investigation of PLS in HetNets was pioneered by the authors of [16]. Based on stochastic geometry, secrecy outage probability and network-wide secrecy throughput for HetNets were examined in [17] and [18]. PLS for massive MIMO aided HetNets was first investigated in [19]. A very recent contribution on coordinated multipoint secrecy transmission in HetNets was made by the authors of [20].

While there is a strong desire to improve the coverage and security on the one hand, the industry is on the other hand constantly facing the increasing challenge of meeting the demand of green communications [21]. Throughput and secrecy capacity maximization leads to large spectrum and energy consumptions, which are not desirable in forthcoming communication networks. In order to promote economic and ecological sustainability, nowadays researchers have made efforts to study the energy and spectral efficiency tradeoff instead of traditional pursuit of higher capacity and coverage [22-23]. Nevertheless, secrecy oriented spectrum and energy efficiency performance has been rarely discussed in the above researches. The researches on the energy and spectral efficiency problem of massive MIMO enabled HetNets, such as [7] and [11], mainly focused on the scenario without the existence of eavesdroppers. While many security issues in HetNets have been studied in the literature [12-20], controlling the spectrum and energy consumption on securing mobile communications in massive MIMO enabled HetNets has not been actively addressed. To the best of our knowledge, no prior work has accounted for secrecy spectrum efficiency (SSE) and secrecy energy efficiency (SEE) when designing massive MIMO enabled HetNets, and a fundamental analysis framework to evaluate the secrecy oriented spectrum and energy efficiency performance in massive MIMO enabled HetNets is lacking. Motivated by the above reasons as well as the demands for security and resource-saving in the future wireless networks, we aim to propose a tractable

approach for secrecy spectrum efficiency (SSE) and secrecy energy efficiency (SEE) analysis in the downlink of a *K*-tier massive MIMO enabled HetNets.

For clarity, our main contributions are summarized below:

- The achievable ergodic rate for macrocell base station (MBS) users, small-cell base station (SBS) users, and eavesdroppers of *K*-tier massive MIMO enabled HetNets are derived respectively on the condition that each MBS transmits artificial noise (AN) in the null space of the main channel to guarantee the secrecy at the intended receiver.
- Under the same conditions, a fundamental analysis framework to evaluate the secrecy oriented spectrum and energy efficiency performance in massive MIMO enabled HetNets is proposed.
- The impacts of AN power allocation ratio, MBS's transmit antenna number, number of users served by each MBS, and eavesdropper density on SSE as well as SEE are examined.

The remainder of this paper is organized as follows: Section 2 outlines the system model and the fundamental expressions. Section 3 introduces the derivations and analyses of SSE and SEE. Section 4 presents the numerical results. Finally, Section 5 concludes this study.

Notations: $|\cdot|$, $\mathrm{P}\{\cdot\}$, and $\mathrm{E}_A\{\cdot\}$ denote absolute value, probability, and expectation with respect to A, respectively. $\Gamma\{N,\lambda\}$ stands for gamma distribution with parameters N and λ. $\exp(\lambda)$ represents exponential distribution with parameter λ. $f_A(\cdot)$ and $\mathrm{F}_A(\cdot)$ denote probability density function and cumulative distribution function (CDF) of a random variable A, respectively. $\Gamma(z)$ represents the gamma function with parameters z. $\mathrm{B}_{(x)}[p,q]$ represents the incomplete beta function [24, (8.391)] with parameters x, p, and q. ${}_2F_1[\alpha,\beta;\gamma;z]$ is the Gauss hypergeometric function [24, (9.142)] with parameters α, β, γ, and z. L_A stands for Laplace transform with respect to A. Additionally, $\{x\}^+ = \max\{x,0\}$.

2. System Model

In this study, we consider a *K*-tier HetNets consisting of macrocells and small-cells such as picocells and femtocells. As in other studies, we assume that the locations of the base stations (BSs) in the i^{th} tier and eavesdroppers are characterized by two independent homogeneous Poisson point process (PPP) Φ_i and Φ_E with densities λ_i and λ_E, respectively. The first tier represents the class of MBSs, where each *N*-antenna MBS adopting massive MIMO simultaneously communicates with S users ($N >> S \geq 1$). SBSs, legitimate users, and eavesdroppers are each equipped with a single antenna. In the i^{th} tier, total transmit power of each BS is P_i, the path loss exponent is α_i, and the biasing factor is B_i, $i \in [2,K]$. Under the assumption of co-channel deployment and perfect channel state information, each MBS uses zero-forcing beamforming to transmit S data streams with equal power assignment. Meanwhile, each MBS transmits artificial noise (AN) in the null space of the main channel to guarantee the secrecy at the intended receiver. All channels in the system are assumed to undergo independent and identically distributed quasi-static Rayleigh fading.

2.1 Legitimate Users

Without loss of generality, we analyze a typical users located at the origin o and consider a mobile association policy that associates each legitimate user with the BS providing the

maximum average received signal power. Hence, the receive signal to interference plus noise ratio (SINR) of a typical user at a random distance $\left|X_{M,o}\right|$ from its associated MBS o_M can be expressed as

$$\mathrm{SINR}_M = \frac{(1-\eta)P_1 h_{M,o}\beta\left|X_{M,o}\right|^{-\alpha_1}}{S\left(I_M+\delta^2\right)}, \tag{1}$$

where $\eta \in [0,1]$ denotes the power allocation ratio of the AN power to the total transmit power, $h_{M,o} \sim \Gamma(N-S+1,1)$ is the small-scale fading channel power gain between o_M and the typical user, β is the frequency dependent constant value, δ^2 is the additive noise power, and $I_M = I_{M,M} + I_{M,S} + I_{M,AN}$. The intra-tier interference for a MBS user is given by

$$I_{M,M} = \sum_{l\in\Phi_1\setminus o_M} \frac{(1-\eta)P_1}{S} h_{M,l}\beta\left|X_{M,l}\right|^{-\alpha_1}, \tag{2}$$

where $h_{M,l} \sim \Gamma(S,1)$ and $\left|X_{M,l}\right|$ are the equivalent small-scale fading interfering channel power gain and distance between the typical user and MBS $l \in \Phi_1 \setminus o_M$ (except the serving MBS o_M), respectively. The cross-tier interference for a MBS user can be written as

$$I_{M,S} = \sum_{i=2}^{K}\sum_{j\in\Phi_i} P_i h_{i,j}\beta\left|X_{i,j}\right|^{-\alpha_i}, \tag{3}$$

where $h_{i,j} \sim \exp(1)$ and $\left|X_{i,j}\right|$ are the small-scale fading interfering channel power gain and distance between the typical user and SBS j in the i^{th} tier, respectively. The artificial noise interference received by a MBS user is given by

$$I_{M,AN} = \sum_{l\in\Phi_1\setminus o_M} \frac{\eta P_1}{S} h_{AN,l}\beta\left|X_{M,l}\right|^{-\alpha_1}, \tag{4}$$

where $h_{AN,l} \sim \Gamma(S,1)$ is the equivalent AN interfering channel power gain between the typical user and MBS l.

The SINR of a typical user at a random distance $\left|X_{k,o}\right|$ from its associated SBS o_k in the k^{th} tier ($k \in [2,K]$) can be formulated as

$$\mathrm{SINR}_k = \frac{P_k g_{k,o}\beta\left|X_{k,o}\right|^{-\alpha_k}}{I_k+\delta^2}, \tag{5}$$

where $g_{k,o} \sim \exp(1)$ is the small-scale fading channel power gain between the typical user and its serving SBS o_k, and $I_k = I_{k,M} + I_{k,S} + I_{k,AN}$. The macrocells-tier interference for a SBS user is given by

$$I_{k,M} = \sum_{l \in \Phi_1} \frac{(1-\eta)P_1}{S} g_{M,l} \beta \left| X_{M,l} \right|^{-\alpha_1}, \tag{6}$$

where $g_{M,l} \sim \Gamma(S,1)$ is the equivalent small-scale fading interfering channel power gain between the typical user and MBS *l*. The small-cells-tier interference for a SBS user can be written as

$$I_{k,S} = \sum_{i=2}^{K} \sum_{j \in \Phi_i \setminus o_k} P_i g_{i,j} \beta \left| X_{i,j} \right|^{-\alpha_i}, \tag{7}$$

where $g_{i,j} \sim \exp(1)$ is the small-scale fading interfering channel power gain between the typical user and SBS *j* in the i^{th} tier. The artificial noise interference received by a SBS user is given by

$$I_{k,AN} = \sum_{l \in \Phi_1 \setminus o_M} \frac{\eta P_1}{S} g_{AN,l} \beta \left| X_{M,l} \right|^{-\alpha_1}, \tag{8}$$

where $g_{AN,l} \sim \Gamma(S,1)$ is the equivalent AN interfering channel power gain between the typical user and MBS *l*.

2.2 Eavesdroppers

In order to analytically characterize the secrecy performance in massive MIMO enabled HetNets, the capability of not only legitimate users but also eavesdroppers needs to be considered. In this work, we consider a worst-case wiretap scenario in which eavesdroppers are assumed to have the capability of multiuser decoding and jointly wiretap the typical user [18]. Thus, most of the interference created by concurrent transmission of information signals can be completely resolved, and the rest of it can be incorporated into the constant noise. In other words, to an arbitrary eavesdropper, the non-ignorable interference is generated by AN.

When the typical user is connected with a MBS, the receive SINR at the most detrimental eavesdropper is given by

$$\mathrm{SINR}_M^{e^*} = \max_{e \in \Phi_E} \left\{ \frac{(1-\eta)P_1 h_{M,e} \beta \left| X_{M,e} \right|^{-\alpha_1}}{S\left(I_{M,e} + \delta^2\right)} \right\}, \tag{9}$$

where $h_{M,e} \sim \exp(1)$ and $\left| X_{M,e} \right|$ are the equivalent small-scale fading channel power gain and distance between the eavesdropper and its targeted MBS, respectively. The aggregate interference for a MBS eavesdropper can be written as

$$I_{M,e}=\sum_{l\in\Phi_1\setminus o_M}\frac{\eta P_1}{S}h_{e,l}\beta\left|X_{e,l}\right|^{-\alpha_1}, \tag{10}$$

where $h_{e,l}\sim\Gamma(S,1)$ and $\left|X_{e,l}\right|$ are the equivalent AN interfering channel power gain and distance between the eavesdropper and MBS l, respectively.

When the typical user is connected with a SBS in the k^{th} tier, the receive SINR at the most detrimental eavesdropper can be determined with

$$\mathrm{SINR}_k^{e^*}=\max_{e\in\Phi_E}\left\{\frac{P_k g_{k,e}\beta\left|X_{k,e}\right|^{-\alpha_k}}{I_{k,e}+\delta^2}\right\}, \tag{11}$$

where $g_{k,e}\sim\exp(1)$ and $\left|X_{k,e}\right|$ are the equivalent small-scale fading channel power gain and distance between the eavesdropper and its targeted SBS in the k^{th} tier, respectively. The aggregate interference for a SBS eavesdropper is given by

$$I_{k,e}=\sum_{l\in\Phi_1\setminus o_M}\frac{\eta P_1}{S}g_{e,l}\beta\left|X_{e,l}\right|^{-\alpha_1}, \tag{12}$$

where $g_{e,l}\sim\Gamma(S,1)$ and $\left|X_{e,l}\right|$ are the equivalent AN interfering channel power gain and distance between the eavesdropper and MBS l, respectively.

3. Secrecy Spectrum Efficiency and Secrecy Energy Efficiency

In this section, we investigate the network-wide spectrum efficiency and energy efficiency of the massive MIMO enabled HetNets based on the secrecy transmission capacity constraint, which is defined as the achievable rate of successful transmission of secret messages, i.e., achievable secrecy rate [25-26]. In an effort to assess the achievable secrecy rate, we first derive the achievable ergodic rate of the typical user and the most detrimental eavesdropper.

3.1 Achievable ergodic rate

Given that an accurate achievable ergodic rate of the typical macrocell user is difficult to obtain even for traditional HetNets, we first derive the lower bounds of achievable ergodic rate for the typical macrocell user in massive MIMO enabled HetNets.

Lemma 1. The lower bound on the achievable ergodic rate for a randomly selected macrocell user can be expressed as

$$R_M^L=\log_2\left(1+\frac{(1-\eta)P_1(N-S+1)\beta}{S\mu}\right), \tag{13}$$

where

$$\mu=\int_0^{\infty} x^{\alpha_1}\left(\mathrm{E}\{I_M\}+\delta^2\right) f_{|X_{M,o}|}(x)\mathrm{d}x \tag{14}$$

with

$$\mathrm{E}\{I_M\}=\frac{2\pi\lambda_1 P_1\beta}{\alpha_1-2}x^{2-\alpha_1}+\sum_{i=2}^{K}\frac{2\pi\lambda_i P_i\beta}{\alpha_i-2}\left(\frac{P_i B_i S x^{\alpha_1}}{(N-S+1)P_1}\right)^{\frac{2-\alpha_i}{\alpha_i}}, \tag{15}$$

$$f_{|X_{M,o}|}(x)=\frac{2\pi\lambda_1}{A_M}x\exp\left\{-\pi\lambda_1 x^2-\pi\sum_{i=2}^{K}\lambda_i\left(\frac{P_i B_i S x^{\alpha_1}}{(1-\eta)P_1(N-S+1)}\right)^{2/\alpha_i}\right\}, \tag{16}$$

and

$$A_M=2\pi\lambda_1\int_0^{\infty} r\exp\left\{-\pi\lambda_1 r^2-\pi\sum_{i=2}^{K}\lambda_i\left(\frac{P_i B_i S r^{\alpha_1}}{(1-\eta)P_1(N-S+1)}\right)^{2/\alpha_i}\right\}\mathrm{d}r\,. \tag{17}$$

Here, A_M is the probability that a typical user is associated with a MBS.

Proof. See Appendix A.

Lemma 2. When the typical user is connected with a MBS, the achievable ergodic rate for the most detrimental eavesdropper can be given by

$$R_M^{e^*}=\frac{1}{\ln 2}\int_0^{\infty}\frac{1-\mathrm{F}_{\mathrm{SINR}_M^{e^*}}(\gamma)}{1+\gamma}\mathrm{d}\gamma\,, \tag{18}$$

where

$$\mathrm{F}_{\mathrm{SINR}_M^{e^*}}(\gamma)=\exp\left(-2\pi\lambda_E\int_0^{\infty}L_{I_{M,e}}\exp\left(-\frac{\gamma S\delta^2 x^{\alpha_1}}{(1-\eta)P_1\beta}\right)x\mathrm{d}x\right) \tag{19}$$

with

$$L_{I_{M,e}}=\exp\left(-2\pi\lambda_1\sum_{n=1}^{S}\binom{S}{n}\frac{\left(\frac{\gamma\eta x^{\alpha_1}}{1-\eta}\right)^{\frac{2}{\alpha_1}}\Gamma\left(n-\frac{2}{\alpha_1}\right)\Gamma\left(-n+\frac{2}{\alpha_1}+S\right)}{\alpha_1\Gamma(S)}\right). \tag{20}$$

Proof. See Appendix B.

Lemma 3. For a randomly selected user associated with a SBS in the k^{th} tier, the achievable ergodic rate can be formulated as

$$R_k = \frac{1}{\ln 2}\int_0^{\infty} \frac{1-\mathrm{F}_{\mathrm{SINR}_k}(\gamma)}{1+\gamma}\mathrm{d}\gamma\,, \tag{21}$$

where

$$\mathrm{F}_{\mathrm{SINR}_k}(\gamma)=1-\int_0^{\infty} L_{I_k}\exp\left(-\frac{\gamma x^{\alpha_k}\delta^2}{P_k\beta}\right) f_{|X_{k,o}|}(x)\mathrm{d}x \tag{22}$$

with

$$\begin{aligned} L_{I_k} = \exp\Bigg\{ & -2\pi\lambda_1 \sum_{\nu=1}^{S}\binom{S}{\nu}\Bigg(\left(\frac{\eta P_1\gamma x^{\alpha_k}}{SP_k}\right)^{\frac{2}{\alpha_1}} \mathrm{B}_{\left(-\frac{\eta P_1\gamma x^{\alpha_k}}{SP_k}\left(D_M^k(x)\right)^{-\alpha_1}\right)}\left[\nu-\frac{2}{\alpha_1},1-S\right] \\ & +\left(\frac{(1-\eta)P_1\gamma x^{\alpha_k}}{SP_k}\right)^{\frac{2}{\alpha_1}} \mathrm{B}_{\left(\frac{(\eta-1)P_1\gamma x^{\alpha_k}}{SP_k}\left(D_M^k(x)\right)^{-\alpha_1}\right)}\left[\nu-\frac{2}{\alpha_1},1-S\right]\Bigg)(-1)^{\nu}\frac{1}{\alpha_1} \\ & -\sum_{i=2}^{K}\frac{2\pi\lambda_i P_i\gamma x^{\alpha_k}}{P_k(\alpha_i-2)}\left(D_i^k(x)\right)^{2-\alpha_i}\,{}_2F_1\left[\frac{\alpha_i-2}{\alpha_i},1;2-\frac{2}{\alpha_i};-\frac{\gamma x^{\alpha_k}P_i}{P_k\left(D_i^k(x)\right)^{\alpha_i}}\right]\Bigg\}, \end{aligned} \tag{23}$$

$$D_M^k(x)=\left(\frac{P_1(N-S+1)x^{\alpha_k}}{P_k B_k S}\right)^{\frac{1}{\alpha_1}}, \tag{24}$$

$$D_i^k(x)=\left(\frac{P_i B_i x^{\alpha_k}}{P_k B_k}\right)^{\frac{1}{\alpha_1}}, \tag{25}$$

$$f_{|X_{k,o}|}(x)=\frac{2\pi\lambda_k x}{A_k}\exp\left\{-\pi\lambda_1\left(\frac{(1-\eta)P_1(N-S+1)x^{\alpha_k}}{P_i B_i S}\right)^{\frac{2}{\alpha_1}}-\pi\sum_{i=2}^{K}\lambda_i\left(\frac{P_i B_i x^{\alpha_k}}{P_k B_k}\right)^{\frac{2}{\alpha_i}}\right\}, \tag{26}$$

and

$$A_k = 2\pi\lambda_k\int_0^{\infty} r\exp\left\{-\pi\lambda_1\left(\frac{(1-\eta)P_1(N-S+1)r^{\alpha_k}}{P_k B_k S}\right)^{\frac{2}{\alpha_1}}-\pi\sum_{i=2}^{K}\lambda_i\left(\frac{P_i B_i r^{\alpha_k}}{P_k B_k}\right)^{\frac{2}{\alpha_i}}\right\}\mathrm{d}r\,. \tag{27}$$

Proof. The proof of Lemma 3 follows similar lines of the proof in Lemma 1 and Lemma 2.

Lemma 4. When the typical user is connected with a SBS in the k^{th} tier, the achievable ergodic rate for the most detrimental eavesdropper can be expressed as

$$R_k^{e^*} = \frac{1}{\ln 2}\int_0^{\infty} \frac{1-\mathrm{F}_{\mathrm{SINR}_k^{e^*}}(\gamma)}{1+\gamma}\mathrm{d}\gamma\,, \tag{28}$$

where

$$\mathrm{F}_{\mathrm{SINR}_k^{e^*}}(\gamma) = \exp\left(-2\pi\lambda_E \int_0^{\infty} L_{I_{k,e}} \exp\left(-\frac{\gamma\delta^2 x^{\alpha_k}}{P_k\beta}\right) x\mathrm{d}x\right) \tag{29}$$

with

$$L_{I_{k,e}} = \exp\left(-2\pi\lambda_1 \sum_{n=1}^{S}\binom{S}{n}\left(\frac{\eta\gamma P_1}{SP_k}\right)^{\frac{2}{\alpha_1}} \frac{\Gamma\left(n-\frac{2}{\alpha_1}\right)\Gamma\left(-n+\frac{2}{\alpha_1}+S\right)}{\alpha_1\Gamma(S)x^{-2\alpha_k/\alpha_1}}\right). \tag{30}$$

Proof. Lemma 4 can be easily obtained following the approach in Lemma 2.

3.2 Secrecy spectrum efficiency

SSE, which is defined as the achievable secrecy rate over per unit of bandwidth, is proposed to measure the secrecy oriented spectrum efficiency performance in massive MIMO enabled HetNets. Based on the results derived in subsection 3.1, achievable secrecy rate is easy to be calculated and a tractable lower bound on SSE for massive MIMO enabled *K*-tier HetNets can be obtained.

Theorem 1. For the system model defined in Section 2, the lower bound on the SSE can be determined with

$$\mathrm{SSE}^L = A_M \times \mathrm{SSE}_M^L + \sum_{k=2}^{K} A_k \times \mathrm{SSE}_k\,, \tag{31}$$

where $\mathrm{SSE}_M^L = S \times R_{SM}^L$ and $R_{SM}^L = \left\{R_M^L - R_M^{e^*}\right\}^+$ denote the lower bound on the SSE and achievable ergodic secrecy rate for macrocells, respectively. As well as $\mathrm{SSE}_k = R_{Sk}$ and $R_{Sk} = \left\{R_k - R_k^{e^*}\right\}^+$ represent the SSE and achievable ergodic secrecy rate for the k^{th} tier small-cells, respectively.

Proof. The proof of Theorem 1 follows (13), (18), (21), and (28) as well as the law of total expectation.

3.3 Secrecy energy efficiency

SEE is used to evaluate the secrecy performance achieved with unit energy consumption. For sustainable operation of massive MIMO enabled HetNets, gaining theoretical understanding of SEE is as important as that of SSE. In this subsection, we present the lower bound of SEE, which is defined as the secrecy rate over the power ratio.

Theorem 2. The SEE for a massive MIMO enabled *K*-tier HetNet can be lower bounded as

$$\mathrm{SEE}^{L} = A_M \times \mathrm{SEE}_M^L + \sum_{k=2}^{K} A_k \times \mathrm{SEE}_k \,, \tag{32}$$

where $\mathrm{SEE}_M^L = S \times R_{SM}^L \big/ P_M^{\mathrm{total}}$ and $\mathrm{SSE}_k = R_{Sk} \big/ P_k^{\mathrm{total}}$ denote the SEE for macrocells (lower bound) and the k^{th} tier small-cells, respectively. The each channel total power consumptions for MBS and SBS in the k^{th} tier are given by $P_M^{\mathrm{total}} = P_1^0 + \frac{P_1}{\varepsilon_1} + \sum_{t=1}^{3}\left(S^{t\text{-}1}\left(\Delta_t + N\Lambda_t\right)\right)$ and $P_k^{\mathrm{total}} = P_k^0 + \frac{P_k}{\varepsilon_k}$, respectively. P_i^0 and ε_i represent the static hardware power consumption and the efficiency of the power amplifier for the i^{th} tier, respectively. The parameters Δ_t and Λ_t depends on the transceiver chains, precoding, coding and decoding, etc. [27-28].

Proof. The proof of Theorem 2 follows (13) and (19) in [7], as well as the similar lines of the proof in Theorem 1.

4. Numerical Results

In this section, the numerical results for the Monte Carlo simulations and the analyses are presented. The former verifies the analysis accuracy, and all the data listed in this section are averaged over 100,000 such simulations. The node locations are scattered with PPP, as described in Section 2. In this work, we consider a network with $K = 2$, $\alpha_1 = 3.5$, $\alpha_2 = 4$, $\lambda_1 = 10^{-3}$, $\lambda_2 = 2\lambda_1$, $P_1 = 40P_2$, $\delta^2 = 10^{-9}$, $\varepsilon_1 = \varepsilon_2 = 0.38$, $\Delta_1 = 4.8$, $\Delta_2 = 0$, $\Delta_3 = 2.08S \times 10^{-8}$, $\Lambda_1 = 1$, $\Lambda_2 = 9.5 \times 10^{-8}$, $\Lambda_3 = 6.25 \times 10^{-8}$, $P_1^0 = 4\mathrm{W}$, $P_2^0 = 13.6\mathrm{W}$, and $B_2 = 1 - \eta$ [27-28]. Other simulation parameters are presented in **Table 1**. For simplicity, lower bound and Monte Carlo are denoted by (L) and (MC) in legend, respectively.

In **Fig. 1-4**, we compare the SSE for massive MIMO enabled HetNets with AN power allocation ratio, MBS's transmit antenna number, number of users served by each MBS simultaneously, and eavesdropper density, respectively. A fact clearly shown from **Fig. 1-4** is that the SSE of MBS with massive MIMO is better than that of SBS in most instance. This is because the massive MIMO can serve more users in each resource block.

Fig. 1 shows that the SSE first improves then degrades with increasing η. With η at a value around 0.3, SEE reaches the peak. The reason is that: a) Increasing η increases the interference received by eavesdroppers, thus greatly degrades the receive SINR at the eavesdroppers in (9) and (11) as well as increases SSE when η is low. b) Increasing η also degrades the useful signal received by the MBS user, thus degrades the R_M^L in (13) and degrades the SSE_M^L when η is high. c) The SSE for SBS, denoted by SSE_2, does not substantially impact the SSE, since A_M is larger than A_k in this scenario. Moreover, SSE_2

improves with increasing η as the useful signal received by the SBS user would not be degraded by the η increasing.

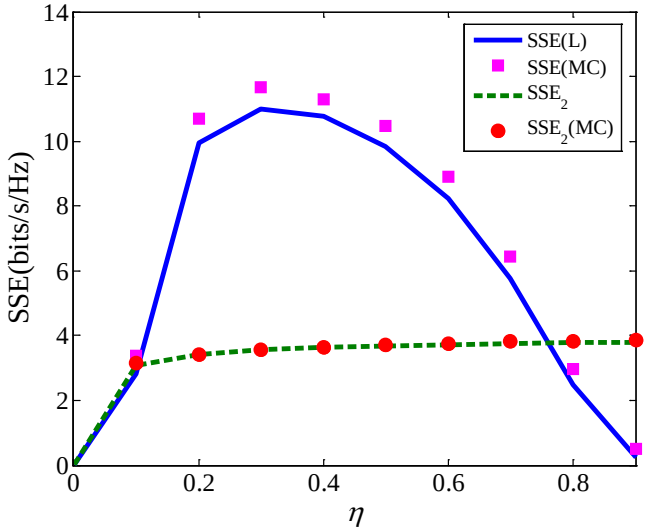

Fig. 1. SSE for different AN power allocation ratio

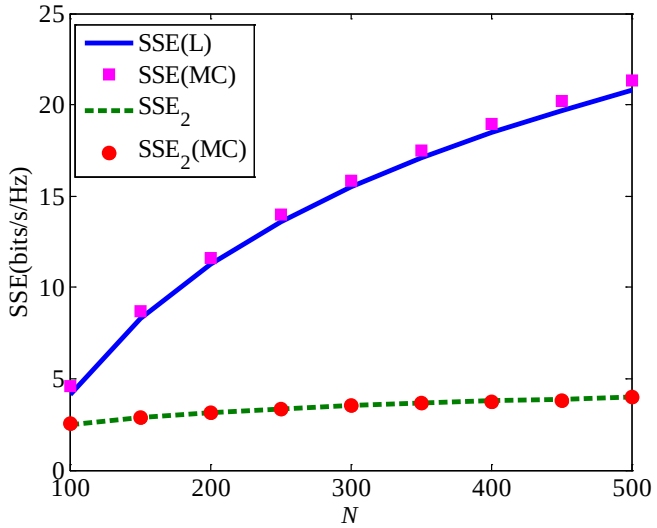

Fig. 2. SSE for different MBS's transmit antenna number

Table 1. Simulation parameters

Parameters	***N***	***S***	η	λ_E
Fig.1 & 5	150	10	various	$3\lambda_1$
Fig.2 & 6	various	10	0.3	$3\lambda_1$
Fig.3 & 7	200	various	0.3	$3\lambda_1$
Fig.4 & 8	200	10	0.3	various
Fig.9	various	various	various	$3\lambda_1$

For each curve in **Fig. 2**, it can be observed that both SSE and SSE_2 improves with increasing MBS's transmit antenna number. Of course, increasing N can significantly improve

radio spectral efficiency for MBS. It can also decreases the average distance between the SBS user and its serving BS by reducing the A_k in (27), thus increases both the R_{Sk} and SSE_2 in (31).

By presenting the SSE versus the number of users served by each MBS in **Fig. 3**, we found that the SSE does not grow monotonically with S and reaches the peak value with S at a value around 20. It's partly because the SSE_2 degrades with increasing S as shown in **Fig. 3**. For large S, the R_{SM}^L is more influential than S to $\mathrm{SSE}_M^L = S \times R_{SM}^L$ in (31) and the R_{SM}^L degrades with increasing S.

Fig. 4 plots the SSE versus the eavesdropper density. As eavesdropper density increases, the SSE accelerates to drop since both $R_M^{e^*}$ in (18) and $R_k^{e^*}$ in (28) increases.

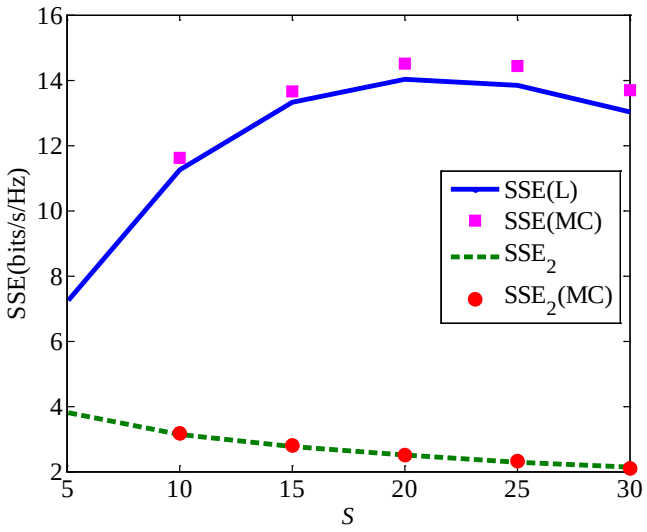

Fig. 3. SSE for different number of users served by each MBS simultaneously

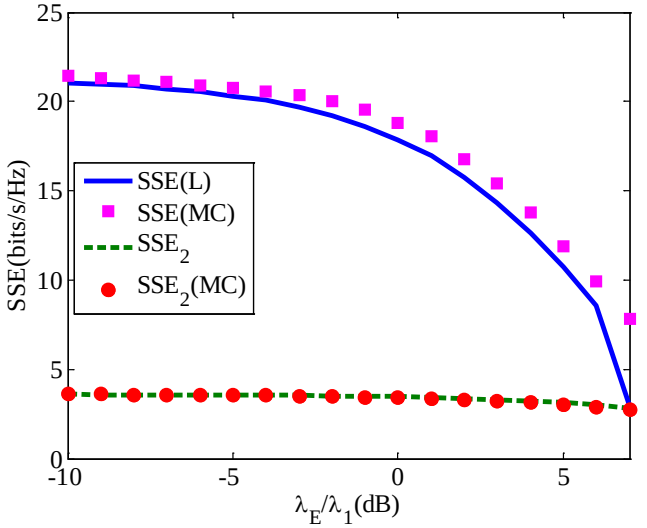

Fig. 4. SSE for different eavesdropper density

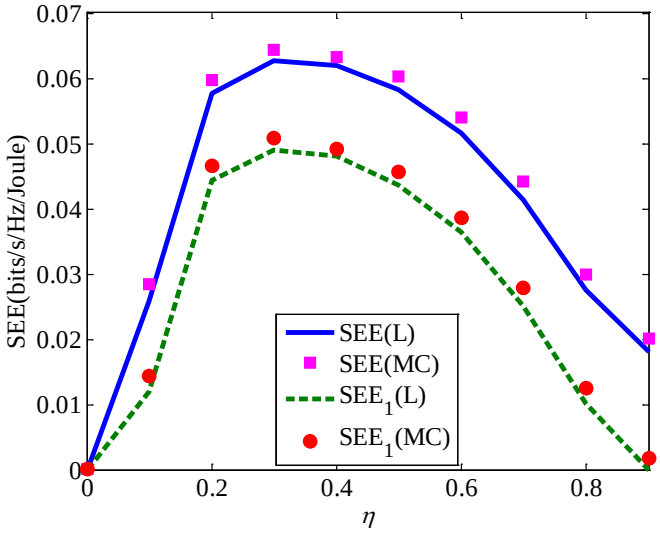

Fig. 5. SEE for different AN power allocation ratio

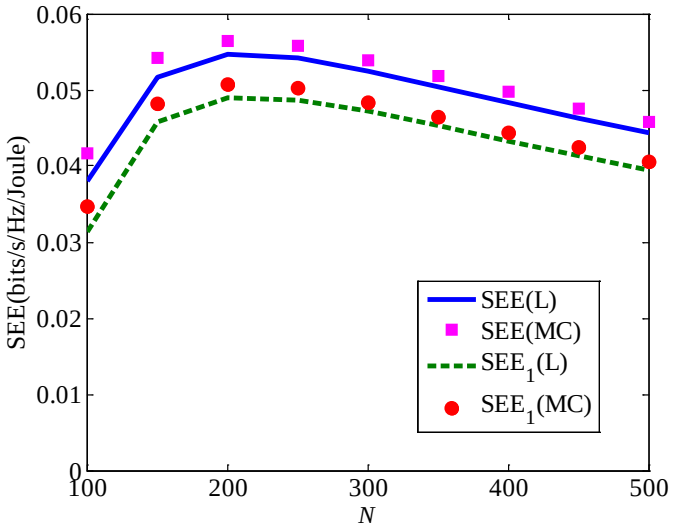

Fig. 6. SEE for different MBS's transmit antenna number

In **Fig. 5-8**, we compare the SEE for massive MIMO enabled HetNets with AN power allocation ratio, MBS's transmit antenna number, number of users served by each MBS simultaneously, and eavesdropper density, respectively. Most of the curves for SEE and the corresponding curves for SSE follow the same trend. Therefore, to avoid repetition, we only focus on the differences.

As shown in **Fig. 5-8**, the SEE for MBS, denoted by SEE_1, is lower than the SEE for the whole HetNet, which means the SEE of SBS is better than that of MBS. The reason is that the AN generated by MBS will deteriorate the $\mathrm{SINR}_k^{e^*}$ in (11) without any energy consumption on SBS.

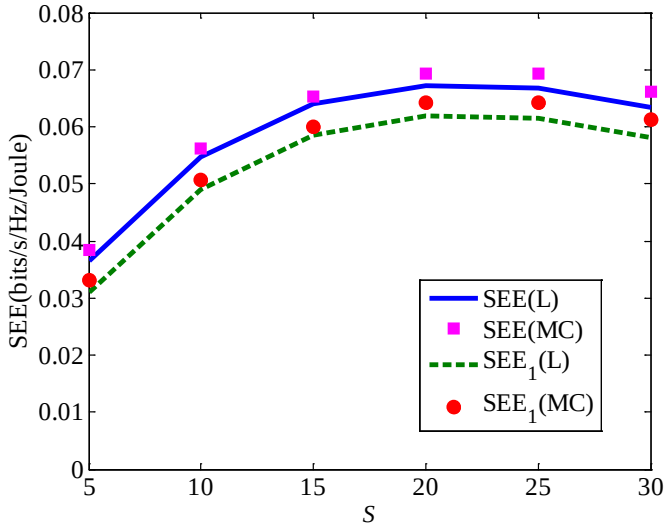

Fig. 7. SEE for different number of users served by each MBS simultaneously

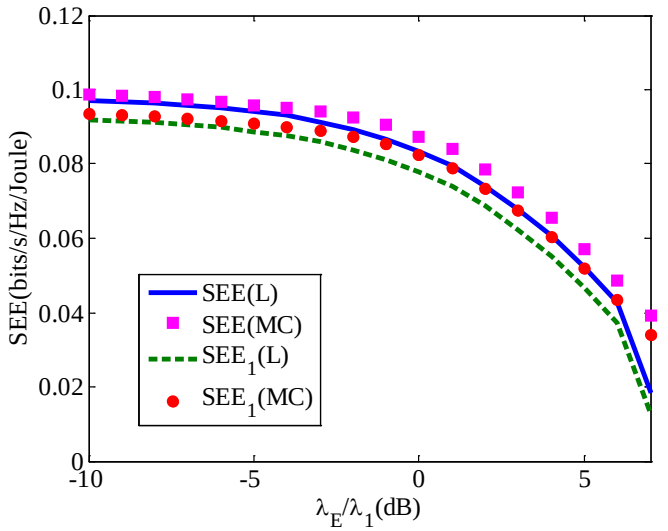

Fig. 8. SEE for different eavesdropper density

Different from SSE, as shown in **Fig. 6**, SEE does not grow monotonically with MBS's transmit antenna number and reaches the peak value at $N = 200$. Because increasing transmit antenna number not only improve the channel gain, but also increase the P_M^{total} in (32), which means higher energy consumption.

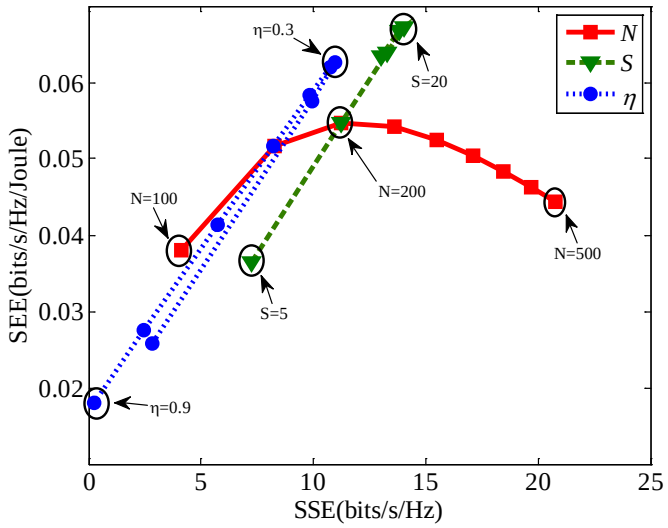

Fig. 9. SEE versus SSE for various values of different parameters

To balance the tradeoff between SSE and SEE, the AN power allocation ratio η, the number of users served by each MBS S, and the MBS's transmit antenna number N should be optimized. In order to illustrate the relation of SSE and SEE clearly, the SEE versus SSE for various values of different parameters are presented in **Fig. 9.** As can be observed from the curves in **Fig. 9**, SSE and SEE are aligned varying the value of η and S. The optimal value of η and S that maximize these two performance metrics (SSE and SEE) are 0.3 and 20, respectively. However, the optimal value of N that maximizes SSE is not the one that maximizes SEE. With N at a value around 200, the optimal SEE for the massive MIMO enabled HetNets is achieved. When N is more than 200, though further increase in MBS's transmit antenna number can still improve SSE, it will deteriorate SEE and greatly increase the cost and difficulty in antenna deployment. Therefore, the optimal value of N is 200 for the tradeoff between SSE and SEE. These optimal values can be used to guide the massive MIMO enabled HetNets design to meet the demand of security and resource-saving.

5. Conclusions

In this paper, we consider a K-tier massive MIMO enabled HetNet, where malicious users can cooperate to eavesdrop and the MBS adopting massive MIMO can generate AN to deteriorate the channels of eavesdroppers. Firstly, the achievable ergodic rate for MBS users, SBS users, and eavesdroppers are derived, respectively. Then, a fundamental analysis framework to evaluate the SSE and SEE performance in the networks described above is proposed based on stochastic geometry. Furthermore, the impacts of AN power allocation ratio, MBS's transmit antenna number, number of users served by each MBS, and eavesdropper density on SSE as well as SEE are examined. From the numerical results of our work, the optimal SSE-SEE tradeoff is achieved at $\eta = 0.3$, $S = 20$ and $N = 200$, which can be adopted for advancing the design of massive MIMO enabled HetNets.

For the future work, it is important to gain a deeper understanding into SSE-SEE tradeoff in coordinated multi-point (CoMP) HetNets. Additionally, it would be interesting to investigate the SSE and SEE with wireless backhaul or imperfect channel state information in HetNets.

Appendix

A. Proof of Lemma 1

Proof. Both $f_{|X_{M,o}|}(x)$ and A_M can be obtained following the approach in [29]. The achievable ergodic rate for a randomly selected macrocell user is denoted by R_M,

$$R_M = \mathrm{E}\left\{\log_2\left(1+\mathrm{SINR}_M\right)\right\} \geq \log_2\left(1+\frac{1}{\mathrm{E}\left\{\left(\mathrm{SINR}_M\right)^{-1}\right\}}\right) = R_M^L, \tag{A1}$$

and

$$\begin{aligned}\mathrm{E}\left\{\left(\mathrm{SINR}_M\right)^{-1}\right\} &= \mathrm{E}\left\{\frac{S\left(I_M+\delta^2\right)}{(1-\eta)P_1 h_{M,o}\beta\left|X_{M,o}\right|^{-\alpha_1}}\right\} \\ &\overset{(a)}{\approx} \frac{\mathrm{E}\left\{S\left(I_M+\delta^2\right)\left|X_{M,o}\right|^{\alpha_1}\right\}}{(1-\eta)P_1(N-S+1)\beta} \\ &= \frac{S\int_0^\infty\left(\mathrm{E}\left\{I_M\right\}+\delta^2\right)x^{\alpha_1} f_{|X_{M,o}|}(x)\mathrm{d}x}{(1-\eta)P_1(N-S+1)\beta}.\end{aligned} \tag{A2}$$

where step (a) follows from the law of large numbers and $\mathrm{E}\left\{I_M\right\} = \mathrm{E}\left\{I_{M,M}\right\} + \mathrm{E}\left\{I_{M,AN}\right\} + \mathrm{E}\left\{I_{M,S}\right\}$. $\mathrm{E}\left\{I_{M,M}\right\}$ can be evaluated as

$$\begin{aligned}\mathrm{E}\left\{I_{M,M}\right\} &= \mathrm{E}\left\{\sum_{l\in\Phi_1\setminus o_M}\frac{(1-\eta)P_1}{S}h_{M,l}\beta\left|X_{M,l}\right|^{-\alpha_1}\right\} \\ &\overset{(b)}{=} 2\pi\lambda_1\mathrm{E}\left\{h_{M,l}\right\}\int_x^\infty\frac{(1-\eta)P_1}{S}\beta y^{1-\alpha_1}\mathrm{d}y \\ &= 2\pi\lambda_1(1-\eta)P_1\beta\int_x^\infty y^{1-\alpha_1}\mathrm{d}y \\ &= \frac{2\pi\lambda_1(1-\eta)P_1\beta x^{2-\alpha_1}}{(\alpha_1-2)},\end{aligned} \tag{A3}$$

where step (b) follows from Campbell's theorem [30] and $\left|X_{M,l}\right|$ is rewritten by y for ease of exposition. Similarly, $\mathrm{E}\left\{I_{M,AN}\right\}$ can be obtained as

$$\begin{aligned}\mathrm{E}\left\{I_{M,AN}\right\} &= \mathrm{E}\left\{\sum_{l\in\Phi_1\setminus o_M}\frac{\eta P_1}{S}h_{AN,l}\beta\left|X_{M,l}\right|^{-\alpha_1}\right\}\\ &= 2\pi\lambda_1\mathrm{E}\left\{h_{AN,l}\right\}\int_x^{\infty}\frac{\eta P_1}{S}\beta y^{1-\alpha_1}\mathrm{d}y\\ &= \frac{2\pi\lambda_1\eta P_1\beta x^{2-\alpha_1}}{\left(\alpha_1-2\right)},\end{aligned} \tag{A4}$$

and $\mathrm{E}\left\{I_{M,S}\right\}$ can be derived as

$$\begin{aligned}\mathrm{E}\left\{I_{M,S}\right\} &= \mathrm{E}\left\{\sum_{i=2}^{K}\sum_{j\in\Phi_i}P_i h_{i,j}\beta\left|X_{i,j}\right|^{-\alpha_i}\right\}\\ &= \sum_{i=2}^{K}\mathrm{E}\left\{\sum_{j\in\Phi_i}P_i h_{i,j}\beta\left|X_{i,j}\right|^{-\alpha_i}\right\}\\ &= \sum_{i=2}^{K}2\pi\lambda_i\int_{D_i^M(x)}^{\infty}P_i\beta y^{1-\alpha_2}\mathrm{d}y\\ &= \sum_{i=2}^{K}\frac{2\pi\lambda_i P_i\beta\left(D_i^M\left(x\right)\right)^{2-\alpha_i}}{\alpha_i-2},\end{aligned} \tag{A5}$$

where $D_i^M\left(x\right)=\left(\frac{P_i B_i S x^{\alpha_1}}{\left(N-S+1\right)P_1}\right)^{\frac{1}{\alpha_i}}$ is the closest distance between the interfering BS in the i^{th} tier and the selected macrocell user.

Substituting (A2), (A3), (A4) and (A5) into (A1), we can arrive at the final result.

B. Proof of Lemma 2

Proof. When the typical user is connected with a MBS, the CDF of the receive SINR at the most malicious eavesdropper is derived as

$$R_M^{e^*}=\mathrm{E}\left\{\log_2\left(1+\mathrm{SINR}_M^{e^*}\right)\right\}=\frac{1}{\ln 2}\int_0^{\infty}\frac{1-\mathrm{F}_{\mathrm{SINR}_M^{e^*}}(\gamma)}{1+\gamma}\mathrm{d}\gamma, \tag{B1}$$

where

$$\begin{aligned}
\mathrm{F}_{\mathrm{SINR}_M^{e^*}}(\gamma) &= \mathrm{P}\left(\max_{e\in\Phi_E} \left\{ \frac{(1-\eta)P_1 h_{M,e}\beta \left| X_{M,e} \right|^{-\alpha_1}}{S\left(I_{M,e}+\delta^2\right)} \right\} \le \gamma \right) \\
&= \prod_{e\in\Phi_E} \mathrm{P}\left(h_{M,e} \le \frac{\gamma S\left(I_{M,e}+\delta^2\right)\left| X_{M,e} \right|^{\alpha_1}}{(1-\eta)P_1 h_{M,e}\beta} \right) \\
&= \mathrm{E}_{\left|X_{M,e}\right|}\left\{ \prod_{e\in\Phi_\mathrm{E}} \mathrm{P}\left(h_{M,e} \le \frac{\gamma S\left(I_{M,e}+\delta^2\right)x^{\alpha_1}}{(1-\eta)P_1 h_{M,e}\beta} \right) \right\} \\
&\overset{(c)}{=} \exp\left(-2\pi\lambda_E \int_0^\infty \mathrm{E}\left\{ \exp\left(-\frac{\gamma S\left(I_{M,e}+\delta^2\right)x^{\alpha_1}}{(1-\eta)P_1\beta} \right) \right\} x\mathrm{d}x \right).
\end{aligned} \tag{B2}$$

where step (c) follows from the probability generating functional (PGFL) of PPP [31], and

$$\mathrm{E}\left\{ \exp\left(-\frac{\gamma S\left(I_{M,e}+\delta^2\right)x^{\alpha_1}}{(1-\eta)P_1\beta} \right) \right\} = \mathrm{E}\left\{ \exp\left(-\frac{\gamma S I_{M,e}x^{\alpha_1}}{(1-\eta)P_1\beta} \right) \right\} \exp\left(-\frac{\gamma S\delta^2 x^{\alpha_1}}{(1-\eta)P_1\beta} \right). \tag{B3}$$

$\mathrm{E}\left\{ \exp\left(-\gamma S I_{M,e}x^{\alpha_1} / \left((1-\eta)P_1\beta\right) \right) \right\}$ can be obtained as

$$\begin{aligned}
\mathrm{E}\left\{ \exp\left(-\frac{\gamma S I_{M,e}x^{\alpha_1}}{(1-\eta)P_1\beta} \right) \right\} &= \mathrm{E}\left\{ \exp\left(-\frac{\gamma\eta x^{\alpha_1}}{1-\eta} \sum_{l\in\Phi_1\setminus o_M} h_{e,l}\left| X_{e,l} \right|^{-\alpha_1} \right) \right\} \\
&= \mathrm{E}_{y_e}\left\{ \prod_{l\in\Phi_1\setminus o_M} \mathrm{E}_{h_{e,l}}\left\{ \exp\left(-\frac{\gamma\eta x^{\alpha_1}}{1-\eta} h_{e,l} y_e^{-\alpha_1} \right) \right\} \right\} \\
&= \exp\left(-2\pi\lambda_1 \int_0^\infty \left(1 - \mathrm{E}_{h_{e,l}}\left\{ \exp\left(-\frac{\gamma\eta x^{\alpha_1}}{1-\eta} h_{e,l} y_e^{-\alpha_1} \right) \right\} \right) y_e \mathrm{d}y_e \right),
\end{aligned} \tag{B4}$$

where $\left|X_{e,l}\right|$ is rewritten by y_e for ease of notation, and $\mathrm{E}\left\{ \exp\left(-\gamma\eta x^{\alpha_1} h_{e,l} y_e^{-\alpha_1} / (1-\eta) \right) \right\}$ can be derived as

$$\begin{aligned}
\mathrm{E}_{h_{e,l}}\left\{ \exp\left(-\frac{\gamma\eta x^{\alpha_1}}{1-\eta} h_{e,l} y_e^{-\alpha_1} \right) \right\} &= \int_0^\infty \exp\left(-\frac{\gamma\eta x^{\alpha_1}}{1-\eta} h_{e,l} y_e^{-\alpha_1} \right) \frac{h_{e,l}^{S-1} e^{-h_{l,e}}}{(S-1)!} \mathrm{d}h_{l,e} \\
&= \left(1 + \frac{\gamma\eta x^{\alpha_1} y_e^{-\alpha_1}}{1-\eta} \right)^{-S}.
\end{aligned} \tag{B5}$$

Furthermore,

$$\begin{aligned}
&\int_0^{\infty}\left(1-\left(1+\frac{\gamma\eta x^{\alpha_1}y_e^{-\alpha_1}}{1-\eta}\right)^{-S}\right)y_e\mathrm{d}y_e\\
&=\int_0^{\infty}\sum_{n=1}^{S}\binom{S}{n}\left(\frac{\gamma\eta x^{\alpha_1}y_e^{-\alpha_1}}{1-\eta}\right)^{n}\left(1+\frac{\gamma\eta x^{\alpha_1}y_e^{-\alpha_1}}{1-\eta}\right)^{-S}y_e\mathrm{d}y_e\\
&=\frac{1}{\alpha_1}\int_0^{\infty}\sum_{n=1}^{S}\binom{S}{n}\left(\frac{\gamma\eta x^{\alpha_1}t}{1-\eta}\right)^{n}\left(1+\frac{\gamma\eta x^{\alpha_1}t}{1-\eta}\right)^{-S}t^{-(\alpha_1+2)/\alpha_1}\mathrm{d}t\\
&=\sum_{n=1}^{S}\binom{S}{n}\frac{\left(\frac{\gamma\eta x^{\alpha_1}}{1-\eta}\right)^{2/\alpha_1}\Gamma\left(n-\frac{2}{\alpha_1}\right)\Gamma\left(-n+\frac{2}{\alpha_1}+S\right)}{\alpha_1\Gamma(S)},
\end{aligned}\tag{B6}$$

where $t=y_e^{-\alpha_1}$.

With the above results, we can arrive at the final result.

References

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong and J. C. Zhang, "What will 5G be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065-1082, June, 2014. Article (CrossRef Link)

[2] H. S. Dhillon, R. K. Ganti, F. Baccelli and J. G. Andrews, "Coverage and ergodic rate in k-tier downlink heterogeneous cellular networks," in *Proc. of 49th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1627-1632, September 28-30, 2011. Article (CrossRef Link)

[3] X. Ge, R. Zi, H. Wang, J. Zhang and M. Jo, "Multi-user massive MIMO communication systems based on irregular antenna arrays," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5287-5301, August, 2016. Article (CrossRef Link)

[4] V. Jungnickel, K. Manolakis, W. Zirwas, B. Panzner, V. Braun, M. Lossow and et al., "The role of small cells, coordinated multipoint, and massive MIMO in 5G," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 44-51, May, 2014. Article (CrossRef Link)

[5] D. C. Araújo, T. Maksymyuk, A. L. Almeida, T. Maciel, J. C. Mota and M. Jo, "Massive MIMO: survey and future research topics," *IET Communications*, vol. 10, no. 15, pp. 1938-1946, October, 2016. Article (CrossRef Link)

[6] W. Liu, S. Jin, C. Wen and X. You, "A tractable approach to uplink spectral efficiency of two-tier massive MIMO cellular HetNets," *IEEE Communications Letters*, vol. 20, no. 2, pp. 348-351, February, 2016. Article (CrossRef Link)

[7] A. He, L. Wang, M. Elkashlan, Y. Chen and K. K. Wong, "Spectrum and energy efficiency in massive MIMO enabled HetNets: A stochastic geometry approach," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2294-2297, December, 2015. Article (CrossRef Link)

[8] A. Adhikary, H. S. Dhillon, and G. Caire, "Massive-MIMO meets HetNet: Interference coordination through spatial blanking," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1171-1186, June, 2015. Article (CrossRef Link)

[9] D. Liu, L. Wang, Y. Chen, T. Zhang, K. K. Chai and M. Elkashlan, "Distributed energy efficient fair user association in massive MIMO enabled HetNets," *IEEE Communications Letters*, vol. 19, no. 10, pp. 1770-1773, October, 2015. Article (CrossRef Link)

[10] Q. Ye, O. Y. Bursalioglu, H. C. Papadopoulos, C. Caramanis and J. G. Andrews, "User association and interference management in massive MIMO HetNets," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 2049-2065, May, 2016. Article (CrossRef Link)

[11] Y. Hao, Q. Ni, H. Li and S. Hou, "Energy and spectral efficiency tradeoff with user association and power coordination in massive MIMO enabled HetNets," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2091-2094, October, 2016. Article (CrossRef Link)
[12] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20-27, April, 2015. Article (CrossRef Link)
[13] H. Wang, T. Zhang and X. Xia, "Secure MISO wiretap channels with multi-antenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 94-106, January, 2015. Article (CrossRef Link)
[14] H. M. Wang, M. Luo, Q. Yin and X. G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2007-2020, December, 2013. Article (CrossRef Link)
[15] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735-2751, June, 2008. Article (CrossRef Link)
[16] T. Lv, H. Gao and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1154-1170, June, 2015. Article (CrossRef Link)
[17] H. Wu, X. Tao, N. Li and J. Xu, "Secrecy outage probability in Multi-RAT heterogeneous networks," *IEEE Communications Letters*, vol. 20, no. 1, pp. 53-56, January, 2016. Article (CrossRef Link)
[18] H. Wang, T. Zheng, J. Yuan, D. Towsley and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204-1219, March, 2016. Article (CrossRef Link)
[19] Y. Deng, L. Wang, K. K. Wong, A. Nallanathan, M. Elkashlan and S. Lambotharan, "Safeguarding massive MIMO aided HetNets using physical layer security," in *Proc. of Wireless Communications and Signal Processing (WCSP), 2015 IEEE*, pp. 1-5, 2015. Article (CrossRef Link)
[20] M. Xu, X. Tao, F. Yang, and H. Wu, "Enhancing secured coverage with COMP transmission in heterogeneous cellular networks," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2272-2275, November, 2016. Article (CrossRef Link)
[21] Z. Hasan, H. Boostanimehr and V. K. Bhargava, "Green cellular networks: a survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 524-540, November, 2011. Article (CrossRef Link)
[22] W. Yu, L. Musavian and Q. Ni, "Tradeoff analysis and joint optimization of link-layer energy efficiency and effective capacity toward green communications," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3339-3353, May, 2016. Article (CrossRef Link)
[23] Z. Song, Q. Ni, K. Navaie S. Hou, S. Wu, and Xin Sun, "On the spectral-energy efficiency and rate fairness tradeoff in relay-aided cooperative OFDMA systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6342-6355, September, 2016. Article (CrossRef Link)
[24] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th Edition, Elsevier, Burlington, 2007. Article (CrossRef Link)
[25] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, October, 1975. Article (CrossRef Link)
[26] P. C. Pinto, J. Barros and M. Z. Win, "Secure communication in stochastic wireless networks--Part I: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125-138, February, 2012. Article (CrossRef Link)
[27] E. Björnson, L. Sanguinetti, J. Hoydis and M. Debbah, "Designing multi-user MIMO for energy efficiency: When is massive MIMO the answer?," in *Proc. of Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, pp. 242-247, April 6-9, 2014. Article (CrossRef Link)

[28] G. Auer, V. Giannini, C. Desset, I. Godor, P. Skillermark, M. Olsson and et al., "How much energy is needed to run a wireless network?," *IEEE Wireless Communications*, vol. 18, no. 5, pp. 40-49, October, 2011. Article (CrossRef Link)
[29] H. Jo, Y. J. Sang, P. Xia and J. G. Andrews, "Heterogeneous cellular networks with flexible cell association: A comprehensive downlink SINR analysis," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3484-3495, October, 2012. Article (CrossRef Link)
[30] F. Baccelli, and B. Błlaszczyszyn, "Stochastic geometry and wireless networks: Volume I Theory," *Foundations and Trends in Networking*, vol. 3, no. 3-4, pp. 249-449, March, 2009. Article (CrossRef Link)
[31] S. N. Chiu, D. Stoyan, W. S. Kendall and J. Mecke, Stochastic Geometry and Its Applications, 3rd Edition, Wiley, New York, 2013. Article (CrossRef Link)

Zhihao Zhong is currently a M.S. candidate at National Digital Switching System Engineering & Technological Research Center, Henan, China. He received the B.E. degree in communication engineering from Nanjing University, Nanjing, China, in 2014. His major research interests include physical layer security, transmit and resource allocation in heterogeneous cellular networks.

Jianhua Peng received his M.S. degree in computer application in 1995. Now he is a professor and doctoral supervisor and also a deputy chief engineer in National Digital Switching System Engineering & Technological Research Center, Henan, China. His major research interests include network switching, wireless mobile communication.

Kaizhi Huang received her Ph.D. degree in communication and information system from Tsinghua University, Beijing, China. Now, she is a professor and supervisor of postgraduate student in National Digital Switching System Engineering & Technological Research Center, Henan, China. She is also serving as a leader of Wireless Mobile Communication Innovation Technology Team of Henan. Her major research interests include wireless mobile communication network and information secrecy.

Lu Xia received the B.E. degree in communication engineering from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2011, and M.S. degree in communication and information systems from National Digital Switching System Engineering & Technological Research Center, Henan, China, in 2014. He is working for National Digital Switching System Engineering & Technological Research Center from 2014 to now. His major research interests include wireless mobile communication and future network architecture.

Xiaohui Qi is currently a Ph.D. candidate at National Digital Switching System Engineering & Technological Research Center, Henan, China. Her major research interests include physical layer security, transmit and resource allocation in heterogeneous cellular networks.