Physical Layer Security in Random NOMA-Enabled Heterogeneous Networks

ELMIRA SHAHRAKI 1, MAHTAB MIRMOHSENI 2 (Senior Member, IEEE), AND HENGAMEH KESHAVARZI 1 (Senior Member, IEEE)

1Department of Electrical and Computer Engineering, University of Sistan and Baluchestan, Zahedan, Iran
2Institute for Communication Systems, Department of Electrical Engineering, University of Surrey, Guildford, U.K.

ABSTRACT The performance of physical layer secrecy approach in non-orthogonal multiple access (NOMA)-enabled heterogeneous networks (HetNets) is analyzed in this paper. A K-tier multi-cell HetNet is considered, comprising NOMA adopted in all tiers. The base stations, legitimate users (in a two-user NOMA setup), and passive eavesdroppers, all with single-antenna, are randomly distributed. Assuming independent Poisson point processes for node distribution, stochastic geometry approaches are exploited to characterize the ergodic secrecy rate. A lower bound on the ergodic secrecy rate along with closed-form expressions for the lower bound on the ergodic rates of the legitimate users in a special case are derived. Moreover, simpler expressions for the ergodic secrecy rate are obtained in the interference-limited regime with vanishing noise variance. The effect of multi-tier technology, NOMA, and physical layer secrecy are investigated using numerical results. The results reveal that applying HetNet to a secure multi-cell NOMA system improves the spectrum efficiency performance.

INDEX TERMS Ergodic secrecy rate, HetNets, NOMA, physical layer security, random networks.

I. INTRODUCTION

NOWADAYS, cellular systems focus on beyond 5G networks, where to meet high spectral efficiency, important new technologies such as heterogeneous networks (HetNets) and non-orthogonal multiple access (NOMA) are proposed [1], [2], [3]. HetNets are typically composed of macrocells with high transmission power and coverage. Macrocell, in turn, overlays smallcells such as picocells and femtocells which have low transmission power and coverage. Thus, network capacity is improved and the coverage is extended due to distance reduction between end users and access nodes. Channel reuse is also increased by deploying small base stations (BSs). Consequently, traffic can be offloaded to smallcells to target a higher spectral efficiency using HetNets [4], [5]. On the other hand, the basic idea of NOMA is to allocate the same time and frequency resources to different users, instead of using orthogonal spectrum. Therefore, significant improvements in spectral efficiency can be achieved by NOMA. Particularly, power-domain NOMA improves spectral efficiency by superposing multiple users in the power domain. This can be obtained by superposition coding (SC) at the transmitter and successive interference cancellation (SIC) at the receivers [6], [7].

Due to the broadcasting nature of transmission medium, security is an essential feature in wireless communication networks. The information theoretic methods to provide secrecy at the physical layer become popular in beyond 5G networks. Thanks to their easier key management and resistance against computationally powerful eavesdroppers [8], [9]. Physical layer security (PLS) methods exploit the physical characteristics of wireless channels including noise, fading, and interference [10], [11]. Given that NOMA, heterogeneous networks, and physical layer secrecy are promising technologies for beyond 5G networks, it is essential to investigate their interactions. In this paper, we study the performance of two beyond 5G key technologies, HetNet and NOMA, in the presence of PLS approaches.

The existing literature on secure NOMA system [12], [13], [14], [15], [16], [17], [18], [19], [20], secure HetNet [21], [22], [23], [24], [25], [26], and NOMA-based HetNet [27], [28], [29], [30] either optimize the system parameters for a single shot of a network or evaluate the performances of...
HetNet, NOMA, and PLS, separately, in random networks (i.e., a network with randomly located nodes). So far, there is no study on PLS in random NOMA-enabled HetNets, which is the main focus of this paper. In addition, a general study of evaluating the performance of the three enabling technologies, NOMA, HetNets, and PLS, is needed to investigate their interaction. Note that providing PLS in HetNets and multicell NOMA systems reduces spectrum efficiency. Hence, the motivation for studying NOMA-enabled HetNet under secrecy constraints is to measure this reduction. Another motivation to study a secure NOMA-enabled HetNet is to improve the ergodic secrecy rate by applying both NOMA and HetNet to the PLS technique. HetNets often experience a lot of interference from macrocells and smallcells, which is one of the main challenges in these networks. Additionally, the implementation of NOMA technology causes further interference. The PLS can exploit these interferences to its advantage. Therefore, it is important to analyze the effect of interference on the ergodic rate and ergodic leakage rate to enhance the secrecy performance. These interferences corrupt the eavesdropper’s signals in a friendly manner.

A. RELATED WORKS

PLS in NOMA-based systems was studied from various perspectives [12], [13], [14], [15], [16], [17], [18], [19], [20]. Optimization approaches were taken in [12] and [13]. The security in NOMA large scale networks was studied in [14] using stochastic geometry to calculate the secrecy outage probability, where the network consists of one BS, several legitimate users, and eavesdroppers in both single-antenna and multiple-antenna scenarios. This work does not consider the multi-cell and HetNet, and the ergodic secrecy rate is not derived. Secrecy outage probability and strictly positive secrecy rate were analyzed in [15], which investigate of a cooperative NOMA system with a single relay, one BS, and an eavesdropper. The PLS analysis in a two-way channel with a trusted multiple-antenna relay in the presence of eavesdroppers was studied in [16]. Artificial noise and full-duplex techniques were used at the relay to improve the secrecy performance. A closed-form expression for the ergodic secrecy rate was obtained in both single eavesdropper and multiple eavesdroppers cases. The secrecy outage analysis of an AN-aided scheme in a downlink large-scale NOMA network was studied in [17], with one BS, random users, and one passive eavesdropper. The secrecy performance of an AN-aided massive MIMO-NOMA network were analyzed in [18], which includes one multiple-antenna BS, multiple single-antenna users, and one passive single-antenna eavesdropper. The ergodic secrecy rate and its asymptotic value for a large number of transmit antennas and high transmit power at the base station were derived. In [19], the effective secrecy rate in the presence of an unknown internal and malicious external eavesdropper was studied, which focused on the downlink of a NOMA network with a single base station, multiple single-antenna NOMA users, and an eavesdropper. A downlink two-user NOMA system within a vehicle-to-vehicle communication framework, featuring a single source and an eavesdropper, was introduced in [20]. Secrecy outage probability and ergodic secrecy rate expressions were examined in two scenarios, considering the decoding capabilities of the eavesdropper. Thus, the ergodic secrecy rate analysis in the multi-cell NOMA systems has not been taken into account, which is addressed in this paper.

Exploiting PLS in HetNets for random networks was studied in [21], [22], [23], [24], [25], [26]. In [21], secrecy and connection probabilities along with sum secrecy rate were studied in a multi-tier heterogeneous cellular network. The position of BSs, legitimate users, and eavesdroppers are characterized by homogeneous Poisson point processes (HPPPs). Each BS employs the artificial noise transmission strategy and the user association policy is based on the truncated average received signal power. A dynamic coordinated multi-point transmission scheme is introduced in [22] for BS selection in heterogeneous cellular networks, where the received signal power for legitimate users are used in BS selection process. The secure coverage probability was calculated by considering co-channel interference and worst-case scenario for eavesdroppers. The area ergodic secrecy rate, the secrecy outage probability, and the energy efficiency in heterogeneous cloud radio access network (RAN) were studied in [23] considering soft fractional frequency reuse (S-FFR), where two-tier heterogeneous cloud RAN consists of massive MIMO macrocell BSs in the first tier and remote radio heads in the second tier. Locations of the macro BSs, the remote radio heads, and the passive eavesdroppers were modeled as HPPPs. In [24], artificial noise-aided PLS in multi-antenna smallcell networks was investigated. Closed-form expressions for the connection and the secrecy outage probabilities were obtained as well as a semi closed-form lower bound on the average secrecy rate. In [25], a user association based on the maximum secrecy capacity in two-tier heterogeneous cellular networks with in-band interference was studied. Keeping the user association scheme in mind, connection and secrecy probabilities and network secrecy throughput were analyzed. PLS was also studied for a heterogeneous spectrum-sharing cellular network in [26]. The network includes a macro BS and a small BS that send messages to legitimate macro and small users in the presence of an eavesdropper. Overall outage and intercept probabilities were obtained in closed-form and secrecy diversity analysis was performed to evaluate performance.

Without secrecy constraint, the outage probability and the ergodic rate of the HetNet-NOMA systems in random
networks were studied in [27], [28], [29], [30]. In [27], the coverage probability, the ergodic rate, and the energy efficiency in two-tier HetNets were analyzed. The first and the second tiers were equipped with massive MIMO and NOMA technologies, respectively. The coverage probability and achievable rate were analyzed in a downlink NOMA-based HetNet in [28]. For improvement of NOMA and SIC, a coordinated joint transmission NOMA method was introduced. Analysis of the coverage probability and the spectral efficiency in NOMA-based HetNets were studied in [29] regarding interference coordination. Two well-known methods, namely strict fractional frequency reuse and soft frequency reuse, were used to reduce inter-cell interference. The coverage probability and the achievable rate were characterized in [30] for a NOMA-based two-tier HetNet with non-uniform smallcell deployment.

Optimization approaches for secure NOMA-based HetNets were also studied in [31] and [32]. Cooperative jamming was utilized in a two-tier HetNet in [31]. The first tier and the second tier were equipped with massive MIMO and NOMA technologies, respectively. The proposed algorithms are presented to maximize the secrecy rate of target users subject to the QoS constraints of other users. In [32], a resource allocation algorithm (joint subcarrier and power allocation) was studied in a NOMA-based two-tier HetNet. The network consisted of one macro BS and multiple small BSs in both single-antenna and multiple-antennas modes.

It is worth noting that the aforementioned works do not investigate PLS in random NOMA-based HetNet. Table 1 provides the difference between the existing related works to clearly address our motivation. In contrary to [31] and [32], in this paper, we compute the ergodic secrecy rate of secure NOMA-based HetNet in random networks. Different from the conventional HetNets (without secrecy constraint and NOMA) [33], secure HetNet (without NOMA) [23], NOMA-enabled HetNet (without secrecy constraint) [27], we consider a secure K-tier multi-cell HetNet with NOMA enabled in all tiers in this treatise, which is more challenging.

### B. CONTRIBUTIONS AND ORGANIZATION

We consider a secure random NOMA-enabled HetNet (SNHet) in this work and our metric is the ergodic secrecy rate. This framework considers a K-tier multi-cell HetNet with NOMA enabled in all tiers, exploiting stochastic geometry approaches. The studied K-tier multi-cell HetNet consists of

---

2This paper considered a K-tier HetNets without secrecy constraint, where the NOMA technology is only adopted in the small cells.

3Optimization approaches for secure NOMA-based HetNets were studied in this paper.
single-antenna BSs in all tiers; the legitimate users employ a novel two-user NOMA approach, and the eavesdroppers passively intercept the secure messages. The legitimate users and eavesdroppers are equipped with a single-antenna. A novel two-user NOMA technique, distinct from existing works [27], is considered. The locations of BSs, legitimate users, and eavesdroppers are randomly distributed regarding HPPP. Our main contributions are as follows:

- We derive analytical expressions for the ergodic secrecy rate of the SN-Het. To this end, user association probability, probability density function (PDF) of users’ distances, SINR analysis considering NOMA transmission, and the characteristic function of interference are characterized. We face the challenges of the complexity of the obtained equations and then the ergodic secrecy rate equation through the calculations. The ergodic secrecy rate equations are triple integrals, while the integration interval is limited in one of the integrals. The challenges of analyzing SN-Het fall into the difficulty of deriving closed-form secrecy rate expressions. The challenges of analyzing SN-Het fall into the complexity of calculations and the difficulty of deriving closed-form secrecy rate expressions. The complexity of calculations in our work is comparable to the previous works, including the calculations of ergodic rates in HetNet [33] and NOMA-based HetNet [27], and the ergodic secrecy rate equation in the secure HetNet [23]. None of these calculations have been achieved in closed-form expressions. So, achieving a closed-form is more challenging due to its complexity. One of the challenging works is making the expressions computable. Thus, we propose the following approaches to resolve these challenges:

1) We simplified the obtained expressions to the maximum extent possible; then, we could numerically evaluate the derived ergodic secrecy rate. The simulation results confirm this numerical evaluation.

2) We derive lower bounds on the ergodic rates of the legitimate users using Jensen’s inequality to simplify the derived ergodic secrecy rate. As a result, simpler expressions are obtained in the form of a single integral. The lower bounds are reduced to closed-form in the special case of the same per-tier path loss exponents and no biasing.

3) Simpler expressions of the ergodic secrecy rate, in the form of a single integral, are derived for the special case of an interference-limited regime with the same path loss exponents and no biasing for all tiers.

- We derive the ergodic secrecy rate of multi-cell NOMA systems by assuming only one tier in the SN-Het ($K = 1$). To the best of our knowledge, the ergodic secrecy rate in multi-cell NOMA systems has not been investigated in the existing literature.

- We evaluate the performance of considered SN-Het by numerical and simulation results. To observe the impact of secrecy constraint as well as NOMA and HetNet technologies, the derived ergodic secrecy rate is compared with ergodic rates in HetNet [33] and HetNetNOMA [27], as well as the ergodic secrecy rate in the secure HetNet [23] and secure multi-cell NOMA. The results show that applying HetNet to a secure multi-cell NOMA system improves the spectrum efficiency while the secrecy constraint degrades the ergodic rate as expected. It is also inferred that increase in number of network tiers with a fixed density of BSs results in the ergodic secrecy rate improvement. On the other hand, in a two-tier network, the ergodic secrecy rate is improved by increasing the density of second tier BSs that results in proper interference for security.

The rest of the paper is organized as follows. In Section II, the secure random NOMA-enabled HetNets is described. In Section III, new analytical expressions for the ergodic secrecy rate of the secure NOMA-based HetNet are derived. Numerical results are presented in Section IV, which is followed by the conclusions in Section V.

II. PROBLEM DESCRIPTION

As shown in Fig. 1, a $K$-tier multi-cell HetNet with macrocells in the first tier and smallcells in remaining tiers is considered. Users are randomly distributed according to an HPPP $\Phi_u$ with intensity $\lambda_u$ and we exploit a two-user NOMA technique. A number of passive eavesdroppers are randomly distributed throughout the network to intercept the secrecy messages. The positions of eavesdroppers and BSs in the $j$-th tier are modeled according to HPPPs denoted as $\Phi_e$ and $\{\Phi_{bj}\}_{1,\ldots,K}$ with intensities $\lambda_e$ and $\lambda_j$, respectively. $\Phi_{ek}$

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{Illustration of the SN-Het system model.}
\end{figure}

For brevity, the interference of BSs in macrocells and the intersection of picocells and femtocells are not shown, though they are considered in the mathematical model.

The HPPP is a Poisson process with a constant Poisson parameter, which describes the average density of points in a given region of space.

We consider a two-user NOMA technique that is more practical and can improve spectral efficiency without much complexity [27].
is a set of eavesdroppers in the tier $k$. Users, eavesdroppers, and BSs are equipped with a single-antenna. It is assumed that the channel state information (CSI) of users at the BS is known. We considered the scenario involving a passive eavesdropper. However, at the BS, the instantaneous CSI of eavesdropper is unknown, while the eavesdropper is aware of individual CSI. Accordingly, the ergodic secrecy rate is calculated in this paper [34].

A. SIGNAL MODEL

Each BS communicates with a set of users in the presence of eavesdroppers. The set of all users at $q$-th BS in the $k$-th tier, $\mathcal{N}_{k,q}$, is defined as $\mathcal{N}_{k,q} = \{1, 2, \ldots, n_{k,q}\}$ where $n_{k,q}$ is a random variable. Without loss of generality, $\mathcal{N}_{k,q}$ divides $\mathcal{N}_{k,q}$ into $2^m$ subsets, to enable a two-user NOMA scheme with random pairing in each subset. We consider one of the subsets, including users $m$ and $n$. It is also assumed that user $m$ is farther from BS $k$ than user $n$. Employing NOMA scheme, BS $k$ transmits signal $\sqrt{a_{mk}} P_k s_{mk} + \sqrt{a_{nk}} P_k s_{nk}$, where $s_{mk}$ and $s_{nk}$ are the transmitted messages for user $m$ and user $n$, respectively. $P_k$ is the transmit power of BS $k$, $(a_{mk}, a_{nk})$ are the power allocation coefficients for users $m$ and $n$, while $a_{mk} \geq a_{nk}$ and $a_{mk} + a_{nk} = 1$. The received signals at user $m$ and user $n$ also the $e$-th eavesdropper are as [32, eq. (1)]:

$$y_{ik} = h_{ik} \sqrt{a_{mk}} P_k s_{mk} + \sqrt{a_{nk}} P_k s_{nk} + z_{ik} + \sum_{j=1}^{K} c_{i,j}(\{\mathcal{N}_{k,q}\}) h_{ij} \sqrt{a_{mj}} P_j s_{mj} + \sqrt{a_{nj}} P_j s_{nj}. \quad (1)$$

where $i \in \{m, n, e\}$; $h_{ik} = \sqrt{g_{ik}} d_{ik}^{-\alpha/2}$ is the channel coefficient between BS $k$ and the $i$-th user/eavesdropper in $\mathcal{N}_{k,q}/\Phi_{ek}$; $g_{ik} \sim \exp(1)$ denotes the small-scale fading transmission/eavesdropping channel power gain, $d_{ik}$ stands for the distance between $i$-th user/eavesdropper and BS $k$, and $\alpha$ is the path loss exponent of the $k$-th tier. Moreover, $h_{ij} = \sqrt{g_{ij}} d_{ij}^{-\alpha/2}$ is the channel coefficient between BS $j$ ($i$-th BS in tier $j$) and $i$-th user/eavesdropper in $\mathcal{N}_{k,q}/\Phi_{ek}$ where $g_{ij} \sim \exp(1)$ is the small-scale fading channel gain; $d_{ij}$ denotes the distance between $i$-th user/eavesdropper and BS $j$, $\Phi_{ek}$ stands for the complex additive white Gaussian noise (AWGN) with zero-mean and variance $\sigma^2$, $z_{ik} \sim CN(0, \sigma^2)$. Note that the amplitude $|h_i|$ follows the Rayleigh distribution [11] with scale parameter $\sqrt{d_i^{-\alpha/2}/2}$, denoted by $\mathcal{R}(\sqrt{d_i^{-\alpha/2}/2})$, while $h_i$ follows the circularly symmetric complex Gaussian (CSCG) distribution with mean zero and covariance $d_i^{-\alpha/2}$, denoted by $CN(0, d_i^{-\alpha/2})$.

B. USER ASSOCIATION STATISTICS AND DISTANCE DISTRIBUTION

The maximum biased average received power [12] of each tier is assumed for user association [33]. Keeping the $w$-th user, at tier $k$, as the associated user in mind, average biased received power is:

$$P_{w,k} = a_{wk} P_k B_k R_{wk} R_{wk}^{-\alpha_k}, \quad (2)$$

where $w \in \{m, n\}$, $B_k$ is a positive bias factor of tier $k$ (the bias factor of all BSs in tier $k$ is the same). $R_{wk}$ denotes the distance between a typical user and BS $k$. According to [33, Lemma 1], the probability of a typical user association with the secure NOMA-based HetNet BSs in tier $k$ is:

$$A_k = 2\pi/\lambda_k \int_0^{\infty} r \exp \left\{ -\pi \sum_{j=1}^{K} \lambda_j \left( \hat{P}_j \hat{B}_j \right)^2 q_{j/2} r^2 \right\} dr, \quad (3)$$

where $\hat{P}_j = \frac{P_j}{P_k}$, $\hat{B}_j = \frac{B_j}{B_k}$, and $\alpha_j = \frac{\alpha}{\alpha_k}$ are the ratios of the interfering $j$-th tier to the serving $k$-th tier. Regarding [33, Lemma 3], the PDF of distance $R_k = \arg \max_{k \in \{1, \ldots, K\}} \{P_{k} \}$ between a typical user and its serving BS in the $k$-th tier is as follows:

$$f_{R_k}(r) = \frac{2\pi/\lambda_k}{A_k} r \exp \left\{ -\pi \sum_{j=1}^{K} \lambda_j \left( \hat{P}_j \hat{B}_j \right)^2 q_{j/2} r^2 \right\} = \frac{2\pi/\lambda_k}{A_k} r \exp(\Delta(r)) \quad (4)$$

C. NOMA TRANSMISSION AND SINR ANALYSIS

Employing NOMA technique inspired from [27], the first user is assumed to associate with BS in the previous round of the user association and the second user is also connected to the same BS. In existing works on NOMA-HetNet systems, the distance between the first connected NOMA user and its associated BS was fixed [27]. On the contrary, we consider this distance as a random variable $R_a$. The distance between the second user and the connected BS is also a random

[10]If the CSI of the users is unknown at the BS, there is a high outage probability, bandwidth-consuming, and a reduction in spectrum efficiency.

[11]As part of our future work, we will take into account the alpha-mu fading distribution [35, 36].

[12]The user association process refers to a typical user connecting to BS in the $k$-th tier of HetNet. In this paper, the user association is based on the maximum biased-received-power (BRP), where a mobile user is associated with the strongest BS in terms of the long-term averaged BRP at the user.
variable $r_s$. The distances $r_s$ and $r_a$ follow the distribution $f_{r_{u}}(r)$ in (4) where $u \in \{a, s\}$. As shown in Fig. 2, two cases can be considered due to the uncertainty of whether the second user is farther or nearer. In Case I, user $m$ is the associated user and user $n$ is the second user which is nearer to BS$_{k,q}$ ($r_s \leq r_a$). In Case II, user $n$ is the associated user and user $m$ is the second user which is farther from BS$_{k,q}$ ($r_s > r_a$). Hence, user $m$ is always the far user and user $n$ is always the near user. The near user decodes messages of both $m$-th and $n$-th users and performs SIC, while the far user only decodes its own message. Thus, the following SINR is obtained for user $m$ by substituting $\{i \in m\}$ in (1):

$$\gamma_{m,m,q} = \frac{a_{mk,q}P_k g_{mk,q} d_{mk,q}^{-\alpha_k}}{a_{nk,q}P_k g_{nk,q} d_{nk,q}^{-\alpha_n} + I_{mk,q} + \sigma^2},$$

(5)

where $I_{mk,q} = \sum_{j=1}^{K} \sum_{i \in \Phi_0; \setminus [BS_q]} P_j g_{ij,l} d_{ij,l}^{\alpha_j}$ is the interference at user $m$ from the BSs in all macrocells and smallcells except its serving BS. Substituting $\{i \in n\}$ in (1), the SINR at the $n$-th user decoding the message of user $m$ is:

$$\gamma_{n,m,q} = \frac{a_{nk,q}P_k g_{nk,q} d_{nk,q}^{-\alpha_k}}{I_{nk,q} + \sigma^2},$$

(6)

where $I_{nk,q} = \sum_{j=1}^{K} \sum_{i \in \Phi_0; \setminus [BS_q]} P_j g_{ij,l} d_{ij,l}^{\alpha_j}$ is the interference at user $n$ from BSs in all macrocells and smallcells except its serving BS. The SINR at user $n$ for decoding its own message (after SIC) is calculated as follows by substituting $\{i \in n\}$ in (1),

$$\gamma_{n,n,q} = \frac{a_{nk,q}P_k g_{nk,q} d_{nk,q}^{-\alpha_k}}{I_{nk,q} + \sigma^2}.$$  

(7)

The SINR at users for Case I and Case II, respectively, can be obtained by substituting $\{d_{mk,q} = r_a, d_{nk,q} = r_s\}$ and $\{d_{mk,q} = r_s, d_{nk,q} = r_a\}$ in (5), (6), and (7).

We consider the non-colluding eavesdropping scenario, where the most malicious eavesdropper, i.e., the one with the largest SINR of the received signal, dominates the secrecy rate. The eavesdropper independently intercepts the information of legitimate users [37, Case I]. The received SINR at the most detrimental eavesdropper for detecting the message of the $w$-th user is obtained by substituting $\{i \in e\}$ in (1) as:

$$\gamma_{e_{max,k,q}} = \max_{e \in \Phi_0} \frac{a_{ek,q}P_k g_{ek,q} d_{ek,q}^{-\alpha_k}}{I_{ek,q} + \sigma^2},$$

(8)

where $I_{ek,q} = \sum_{j=1}^{K} \sum_{i \in \Phi_0; \setminus [BS_q]} P_j g_{ij,l} d_{ij,l}^{\alpha_j}$ is the interference at eavesdropper $e$ from BSs in all macrocells and smallcells except BS$_{k,q}$.

**D. INTERFERENCE CHARACTERISTIC FUNCTION**

The characteristic function of interference from the macro and small BSs at user $w$ is calculated using [27, Lemma 2] as:

$$L_{I_{w,k,q}}(s) = \mathbb{E}\left[e^{-s I_{w,k,q}} \right] = \exp\{\xi_1,w(s)\}$$

= \exp\left\{- \sum_{j=1}^{K} 2 \pi \lambda_j \frac{s P_j (y_j(r_w))^2}{\alpha_j - 2} \right\} \times 2 F_1 \left(1, 1 - \frac{2}{\alpha_j}; 2 - \frac{2}{\alpha_j}; - s P_j \frac{(y_j(r_w))^2}{\alpha_j} \right),$$

(9)

where $w \in \{m, n\}, u \in \{a, s\}$, and $2 F_1$ denotes the Gauss hypergeometric function [38]. The distance between user $w$ and the closest interferer in tier $j$ is $y_j(r_w) = \left(\frac{P_j B_j}{\gamma_j(r_w)^{1/\alpha_j}}\right)$. The characteristic function of interference at an eavesdropper is also obtained using [23, Th. 2] as:

$$L_{I_{w,k,q}}(s) = \mathbb{E}\left[e^{-s I_{w,k,q}} \right] = \exp\{\xi_1,w(s)\}$$

= \exp\left\{- \sum_{j=1}^{K} \pi \lambda_j \left(s \frac{P_j}{\alpha_j} \right)^2 \Gamma\left(1 + \frac{2}{\alpha_j}\right) \Gamma\left(1 - \frac{2}{\alpha_j}\right)\right\},$$

(10)

where $\Gamma$ stands for the Gamma function [38]. For the sake of simplicity, $L_{I_{w,k,q}}$ and $L_{I_{w,k,q}}$ are shown as $L_{I_w}$ and $L_{I_e}$, respectively, in subsequent descriptions.

**III. PERFORMANCE ANALYSIS**

In this section, performance of the considered SN-Het is analyzed in term of the ergodic secrecy rate. To this end, we first study each tier of the SN-Het. Initially, the ergodic rates of the legitimate users are derived in Lemma 1. The proof is in Appendix A.

**Lemma 1**: Based on the location of NOMA users, the ergodic rate is presented below.

1) Case I: The ergodic rates of the associated user (user $m$) and the second user (user $n$) in the $k$-th tier are derived as (11) and (12), respectively.

$$R_{m,k}^l = \frac{4 \pi^2 \lambda_k^2}{A_k^2 \ln 2} \int_0^\infty \int_0^{\frac{\pi}{\lambda_k} r_r a} r_r a \exp\left\{ - \frac{\pi^2 r_r a^2}{\alpha_k A_k} \right\} dt dr_a,$$

(11)

$$R_{n,k}^l = \frac{4 \pi^2 \lambda_k^2}{A_k^2 \ln 2} \int_0^\infty \int_0^{\frac{\pi}{\lambda_k} r_r a} r_r a \exp\left\{ - \frac{\pi^2 r_r a^2}{\alpha_k A_k} \right\} dt dr_a,$$

(12)

where $\bar{F}_{R_e}(s) = \int_s^\infty r \exp\{\Delta(r)\} dr$.

2) Case II: The ergodic rates of the associated user (user $m$) and the second user (user $m$) in the $k$-th tier are derived as (13) and (14), respectively.

$$R_{n,k}^l = \frac{4 \pi^2 \lambda_k^2}{A_k^2 \ln 2} \int_0^\infty \int_0^{\frac{\pi}{\lambda_k} r_r a} r_r a \exp\left\{ - \frac{\pi^2 r_r a^2}{\alpha_k A_k} \right\} dt dr_a,$$

(13)

$$R_{n,k}^l = \frac{4 \pi^2 \lambda_k^2}{A_k^2 \ln 2} \int_0^\infty \int_0^{\frac{\pi}{\lambda_k} r_r a} r_r a \exp\left\{ - \frac{\pi^2 r_r a^2}{\alpha_k A_k} \right\} dt dr_a.$$

(14)
where \( A \triangleq \frac{1}{a_{m, q} - \alpha m_q} \).

It should be noted that due to higher limit of the integral in (11) and (14), the integrand is easy to compute. Despite non-closed-form equations for ergodic rates of the legitimate users, they are efficiently computed numerically compared to Monte Carlo simulations which depend on repeated random sampling.

**Remark 1:** Considering the incremental behavior of distribution \( f_{\hat{R}}(\tilde{r}) \) with growth in density of BSs at the \( k \)-th tier (\( \lambda_k \)) in Lemma 1 and also increase in the exponential term and the characteristic function of interference with enhanced transmission power of BSs at the \( k \)-th tier (\( P_k \)), the ergodic rate of \( k \)-th tier is incremental.

To present simpler expressions, in the following lemma, lower bounds on the results of Lemma 1 are derived. The proof is in Appendix B.

**Lemma 2:** A lower bounds on the ergodic rates of the associated and the second users in the \( k \)-th tier for Case I and Case II are obtained at the bottom of this page for \( w \in \{ m, n \} \), we have \( E[R_{i,k}] = \sum_{j=1}^{K} \left( \frac{a_{m, q}}{\alpha m_q - \alpha} \right) \gamma_j(r_{i})^{2-m_q} \). Note that all logarithms are in base 2 in this paper.

The derived expressions in Lemma 2, relax the ergodic rates of the legitimate users in the \( k \)-th tier of Lemma 1 to a single integral form. Now, we define the following special case to derive the rate expressions in Lemma 2 in closed-form.

**Definition 1:** We define special case by considering three conditions: (1) the same path loss exponent for all tiers (\( \alpha_k = \alpha \)), (2) an unbiased association (\( \hat{B}_i = 1 \)), and (3) the interference-limited regime\(^{13} \) (\( \sigma^2 = 0 \)).

**Corollary 1:** Assuming the special case of conditions 1 and 2 of Definition 1, the lower bounds on the ergodic rates of the associated and the second users in the \( k \)-th tier for Case I and Case II are expressed in closed-form as:

\[
\tilde{R}_{m,k} = \log \left( 1 + \left( \frac{2a_{m, q}}{a_{m, q} - \alpha} \right) \left( 2 + \frac{7}{2(\alpha - 2)} \right) \right) - 1, \tag{19}
\]
\[
\tilde{R}_{n,k} = \log \left( 1 + \left( \frac{1}{a_{m, q} - \alpha} \right) \left( \frac{1}{\alpha - 2} + \frac{\tilde{A}}{2} \right) \right) - 1, \tag{20}
\]
\[
\tilde{R}_{II}_{m,k} = \log \left( 1 + \left( \frac{2a_{m, q}}{a_{m, q} - \alpha} \right) \left( 2 + \frac{7}{2(\alpha - 2)} \right) \right) - 1, \tag{21}
\]
\[
\tilde{R}_{II}_{n,k} = \log \left( 1 + \left( \frac{1}{a_{m, q} - \alpha} \right) \left( \frac{1}{\alpha - 2} + \frac{\tilde{A}}{2} \right) \right) - 1, \tag{22}
\]

where \( \tilde{A} \triangleq \frac{\sigma^2 (\alpha + 1)}{\alpha m_q P_k} \) and \( E \triangleq \sum_{j=1}^{K} \pi \lambda_j P_j^{\frac{1}{2}} \).

**Proof:** See Appendix C.

Next, the ergodic leakage rate of the most detrimental eavesdropper is provided in Lemma 3. The proof is in Appendix D.

**Lemma 3:** For \( w \in \{ m, n \} \), the ergodic leakage rate at the most detrimental eavesdropper for decoding the message of the\( w \)-th user in the \( k \)-th tier is expressed as [34, eq. (24)]:

\[
R_{e,k}^w = \frac{1}{\ln 2} \int_{0}^{\infty} \frac{1}{1 + \tilde{r}^2} \left( 1 - \exp \left\{ - \frac{\lambda_k}{\tilde{r}} \right\} \right) \exp \left\{ \frac{\sigma^2 \tilde{r}^2}{a_{m, q} P_k} \right\} \left[ \frac{1}{r} \right] dt. \tag{23}
\]

**Remark 2:** Eq. (23) confirms that higher density of eavesdroppers in the network leads to the ergodic leakage rate increase.

After studying each tier in the considered SN-Het system model, the ergodic secrecy rate\(^{14} \) of the SN-Het is calculated in Theorem 1 below.

**Theorem 1:** An ergodic secrecy rate of the SN-Het is calculated as follows:

\[
R_{sec} = \sum_{k=1}^{K} A_k \left( R_{sec,k}^{I} + R_{sec,k}^{II} \right), \tag{24}
\]

\[
R_{sec,k}^{I} = \left[ R_{n,k}^w - R_{e,k}^w \right] + \left[ R_{m,k}^n - R_{e,k}^m \right], \tag{25}
\]

\[
R_{sec,k}^{II} = \left[ R_{n,k}^w - R_{e,k}^w \right] + \left[ R_{m,k}^n - R_{e,k}^m \right], \tag{26}
\]

where \( [x]^+ = \max(x, 0) \). \( R_{sec,k}^{I} \) and \( R_{sec,k}^{II} \) represent the ergodic secrecy rates in the \( k \)-th tier for Case I and Case II, respectively. \( R_{n,k}^w - R_{e,k}^w \) and \( R_{m,k}^n - R_{e,k}^m \) denote the ergodic secrecy rates of the users \( n \) and \( m \) in the \( k \)-th tier for Case I, respectively (similarly for Case II). \( A_k \) is given in (3), \( R_{m,k}^n, R_{n,k}^{I}, R_{n,k}^{II}, R_{m,k}^{II}, R_{e,k}^{I}, \) and \( R_{e,k}^{II} \) are also derived in (11)-(14) and (23).

**Proof:** Based on [27, Proposition 1] at non-secure mode, the achievability of (24) could be shown by using wiretap coding for each of NOMA users. \( R_{sec,k}^{I} \) and \( R_{sec,k}^{II} \) are inferred from Lemma 1 and Lemma 3.

**Corollary 2:** A lower bound on the ergodic secrecy rate (\( R_{sec} \)) is obtained by substituting (15)-(18), as shown at the bottom of the previous page, (i.e., the lower bounds on ergodic rates of the legitimate users (\( R_{w,k} \))) into (24).

In the following corollary, we derive the ergodic secrecy rate of multi-cell NOMA systems, which has not been characterized in the existing literature to the best of our knowledge.

**Corollary 3:** An ergodic secrecy rate of multi-cell NOMA system is obtained by assuming one tier (\( K = 1 \)) in the SN-Het, \( R_{sec} = R_{sec,1}^{I} + R_{sec,1}^{II} \), which can be derived by substituting \( k = 1 \) in (11)-(14), (23), (25), and (26).

Now, the special case of interference-limited network is investigated by considering Definition 1. The interference-limited regime is of high importance in HetNets due to high BS density which results in domination of interference to

\(^{13}\) The interference-limited regime is a common assumption in stochastic geometry-based large-scale networks, where the noise can be neglected.

\(^{14}\) The ergodic rate defines the expectation of the achievable data rate that can be sent over the channel. The ergodic leakage rate measures the amount of information leaked to the eavesdroppers.
the noise power [33]. In the following corollary, the results of Lemma 1 and Lemma 3 are further simplified for this special case. The proof is in Appendix E.

**Corollary 4:** The ergodic rates of the associated and the second users in the $k$-th tier of Case I and Case II are presented below considering the special case of conditions 1, 2 and 3 of Definition 1:

$$R_{m,k}^I(\alpha, 1) = R_{m,k}^{II}(\alpha, 1) = \frac{1}{\ln 2} \int_0^{\frac{\alpha m_k}{a_{m_k,q}}} \frac{1}{2(1+t)(1+Z_m)^{\alpha}} dt,$$  \hspace{1cm} (27)

$$R_{n,k}^I(\alpha, 1) = R_{n,k}^{II}(\alpha, 1) = \frac{1}{\ln 2} \int_0^\infty \frac{1}{(1+t)(2+Z_m)} dt,$$  \hspace{1cm} (28)

where

$$Z_m \triangleq \frac{2tau}{(\alpha-2)} \times 2F_1\left(1, 1 - \frac{2}{\alpha}; 2 - \frac{2}{\alpha}; -tau \right),$$ \hspace{1cm} (29)

$$Z_n \triangleq \frac{2t}{a_{m_k,q}(\alpha-2)} \times 2F_1\left(1, 1 - \frac{2}{\alpha}; 2 - \frac{2}{\alpha}; -\frac{t}{a_{m_k,q}} \right).$$ \hspace{1cm} (30)

In addition, the ergodic leakage rate at the most detrimental eavesdropper for detecting the information of $w$-th user ($w \in \{m, n\}$) in the $k$-th tier is given by:

$$R_{w,k}^E(\alpha, 1) = \frac{1}{\ln 2} \int_0^\infty \frac{1}{1+t}\left(1 - \exp \left\{-Bt^{-\frac{3}{2}}\right\}\right) dt,$$ \hspace{1cm} (31)

where

$$B \triangleq \lambda_k a_{m_k,q} \sigma^2 \left(\sum_{j=1}^{K} \lambda_j \hat{P}_j \hat{\gamma} \left(1 + \frac{2}{\alpha}\right) \Gamma\left(1 - \frac{2}{\alpha}\right)\right)^{-1}.$$ \hspace{1cm} (32)

Considering the special cases of conditions 1, 2 and 3 of Definition 1, the ergodic secrecy rate of SN-Het is derived as

$$R_{m,k}^{sec} = \frac{1}{\ln 2} \times \int_0^{\frac{\alpha m_k}{a_{m_k,q}}} \frac{1}{2(1+t)(1+Z_m)^{\alpha}} dt,$$ \hspace{1cm} (27)

$$R_{n,k}^{sec} = \frac{1}{\ln 2} \times \int_0^\infty \frac{1}{(1+t)(2+Z_m)} dt.$$ \hspace{1cm} (28)

**Remark 3:** The provided ergodic rates of the legitimate users at (27) and (28) in the interference-limited regime neither depend on the number of tiers, nor on BS transmit power and BS density. The reason is that the effect of increasing BS density or BS transmit power on the desired power and BS density. The reason is that the effect of increasing BS density or BS transmit power on the desired power and BS density.

**IV. NUMERICAL RESULTS**

The derived analytical results ($R_{sec}$ in (24)) are numerically evaluated in this section. The Monte Carlo simulation results are also provided to verify the obtained analytical results. The general parameters used in the analytical derivations and simulations are summarized in Table 2, which are consistent with the papers [23], [27], [33]. The Monte Carlo simulation area is a circle with radius $10^4$ m.

Fig. 3 depicts behavior of the SN-Het ergodic secrecy rate versus $\lambda_e$ for different numbers of network tiers. $\lambda_e$ is drawn logarithmically due to its variable interval. The goal is to analyze the ergodic secrecy rate as number of tiers increase while a fixed density of BSs (i.e., $11\lambda_0$) is divided between tiers. As expected, the ergodic secrecy rate decreases as $\lambda_e$ increases, due to the increased leakage. Moreover, it is inferred that the ergodic rate improves as the number of tiers increases. It is worth noting that increase in the number of tiers reduces the inter-tier interference because of $P_1 > P_2 > P_3$ and $\alpha_2, \alpha_3 > \alpha_1$. Interestingly, adding one tier results in the increased secrecy rate.

The Monte Carlo simulations in this work are utilized to confirm the analytical results.

$$\hat{R}_{m,k}^{I} = \log\left(1 + \frac{2\alpha_m}{a_{m_k,q}} P_k \int_0^{\infty} \left\{E[I_{m_k,q}] + \sigma^2\right\} r_a^{\alpha_1}(1 - F_{R_m}(r_a)) f_{R_m}(r_a) dr_a\right)^{-1},$$ \hspace{1cm} (15)

$$\hat{R}_{n,k}^{I} = \log\left(1 + \frac{1}{a_{m_k,q}} P_k \int_0^{\infty} \left\{E[I_{m_k,q}] + \sigma^2\right\} r_a^{\alpha_1}(1 - F_{R_m}(r_a)) f_{R_m}(r_a) dr_a\right)^{-1},$$ \hspace{1cm} (16)

$$\hat{R}_{m,k}^{II} = \log\left(1 + \frac{1}{a_{m_k,q}} P_k \int_0^{\infty} \left\{E[I_{m_k,q}] + \sigma^2\right\} r_a^{\alpha_1} f_{R_m}(r_a) dr_a\right)^{-1},$$ \hspace{1cm} (17)

$$\hat{R}_{n,k}^{II} = \log\left(1 + \frac{2\alpha_m}{a_{m_k,q}} P_k \int_0^{\infty} \left\{E[I_{m_k,q}] + \sigma^2\right\} r_a^{\alpha_1} f_{R_m}(r_a) dr_a\right)^{-1}.$$ \hspace{1cm} (18)
tier is more beneficial for \( K = 1 \) to \( K = 2 \) compared with \( K = 2 \) to \( K = 3 \). In addition, another purpose in Fig. 3 is to allocate a fixed density of BSs (11\( \lambda_0 \)) between two tiers. It is observed that assigning more BSs to a tire with lower power and higher path loss (\( K = 2 \)) is more advantageous due to the reduction of interference. The analytical curves have a precise match to the results obtained with the Monte Carlo simulations.

In Fig. 4, behavior of the two-tier SN-Het ergodic secrecy rate is demonstrated versus \( \lambda_2 \) for both NOMA and OMA\(^{17} \) strategies. Unlike the previous analyses and existing results in [27], the first user distance (\( r_a \)) is not fixed here and the ergodic secrecy rate is calculated accordingly. The obtained lower bound on ergodic secrecy rate according to Corollary 2 is also plotted (denoted as lower bound). It is shown that NOMA significantly outperforms OMA. Furthermore, it is inferred that the ergodic secrecy rate improves as \( \lambda_2 \) increases. Not only the ergodic rate of the second tier is increased by increasing \( \lambda_2 \), but also the ergodic rate of the first tier increases, interestingly. This is due to the fact that increasing the second tier BSs results in more users with low SINR (i.e., at cell edge) at the first tier become associated with the second tier. In addition, increasing \( \lambda_2 \) results in more interference at the eavesdroppers and degrades the eavesdroppers’ channels. As it is inferred, the performance of NOMA is significantly better than OMA systems in networks with higher density of BSs which caused more interference. It is also observed that the obtained ergodic secrecy rates are reasonably close to the demonstrated lower bounds.

The ergodic secrecy rate versus \( B_2 \) is presented in Fig. 5 for all network tiers. As observed in [15], which is consistent with the prior existing works, the unbiased association\(^{18} \) always outperforms biasing from the study of rate at the overall network point of view. It is observed that increasing in \( B_2 \) causes the ergodic secrecy rate of the first tier to increase, while the ergodic secrecy rate decreases in the second tier. It is worth noting that more macro users with low SINR (i.e., at cell edge) are associated with the second tier as \( B_2 \) increases. This increased macro user association in the second tier degrades the ergodic secrecy rate of corresponding tier, but improves those of the first tier. However, reduction in the second tier ergodic secrecy rate is compensated by increase in \( \lambda_2 \). Thus, the biased association is an efficient method in load balancing between each tier of the HetNet. Furthermore, the probability of association to the second tier increases as \( B_2 \) increases, which causes a faster drop in the two-tier case compared to the second tier case.

Randomness to the first user distance is perceived in Fig. 6 as one of our contributions contrary to [27]. It is shown by dashed line that the ergodic secrecy rate is highly dependent on the value of \( r_d \) with fixed first user location (as in [27]). Hence, the ergodic secrecy rate over the locations of the first user is also depicted by solid line. Indeed, for a fixed \( r_d \), the obtained ergodic rate value cannot be considered a reliable system performance metric. Thus, by considering random \( r_d \), it becomes feasible to design a system that

\begin{table}[h]
\centering
\small
\caption{Network parameters.}
\begin{tabular}{|l|l|}
\hline
Parameter & Value \\
\hline
Number of iterations for simulations & \( 10^6 \) \\
\hline
AWGN power & \( \sigma^2 = -90 \text{ dBm} \) \\
\hline
BS transmit power & \( P_1 =40 \text{ dBm}, P_2 =30 \text{ dBm}, P_3 =20 \text{ dBm} \) \\
\hline
Path loss exponents & \( \alpha_1 =3.5, \alpha_2 = \alpha_3 =4 \) \\
\hline
NOMA power sharing coefficients\(^{16} \) & (0.6, 0.4) \\
\hline
Bias factor of the first tier & \( B_1 =1 \) \\
\hline
\end{tabular}
\end{table}
ergodic secrecy rate in [23] for secure HetNet is compared with HetNet without secrecy constraints, as follows. 1) The HetNet with secrecy constraint, 2) NOMA technique with secrecy constraint, and 3) the HetNet and NOMA-HetNet with secrecy constraints. Since the foundations of the studied model are secrecy, a lower bound on the ergodic secrecy rate is obtained. In [23], denoted as NOMA-HetNet with secrecy. In accordance to Fig. 7(a), the SN-Het has superiority over other methods due to enabled NOMA technique. 2) Secure multi-cell NOMA is prepared by eliminating HetNet from the SN-Het (K = 1) to study the effect of using multi-tiers with a fixed density of BSs in Fig. 7(b). It is observed that the ergodic secrecy rate in three-tier HetNet (K = 3) has a significant performance improvement compared to multi-cell NOMA (K = 1). This is consistent with the result of [40] which does not include NOMA and secrecy. 3) The ergodic rate of HetNets from [33] and the lower bound on the ergodic rate of NOMA-HetNet from [27] are provided in Fig. 7(c) to study the effect of secrecy constraints. Massive MIMO in the first tier of model in [27] is eliminated to be comparable with our model. Moreover, we consider our scheme without NOMA (denoted as HetNet with secrecy) and eliminating NOMA only at the first tier (as the network in [27], denoted as NOMA-HetNet with secrecy). In both with and without NOMA cases, secrecy constraint degrades the ergodic rates, especially at higher $\lambda_s$s. It is worth noting that NOMA-HetNet in $\lambda_s = 0$ is lower bound and lower than NOMA-HetNet with secrecy.

V. CONCLUSION

The physical layer security in a $K$-tier multi-cell HetNet with NOMA in all tiers is investigated. BSs, legitimate users, and eavesdroppers are randomly distributed in the considered system model. First, analytical expressions for the ergodic secrecy rate over all tiers of the network are derived. Next a lower bound on the ergodic secrecy rate is obtained. In addition, closed-form expressions for the lower bounds on the ergodic rates of legitimate users are provided in a special

$$\begin{align*}
\lambda &= 2, \\
\alpha &= 1, \\
K &= 3, \\
\beta &= 1.
\end{align*}$$

FIGURE 7. The effects of (a) NOMA technique ($K = 2, \lambda_1 = 10^{-3} = 1.2732 \times 10^{-3}, \lambda_2 = 10\lambda_1, B_2 = 1$), (b) multi-tier using HetNet ($r_s = 50, \lambda_s = 10^{-3} = 1.2732 \times 10^{-3}, \lambda_2 = 10\lambda_1, B_2 = 1$), and (c) secrecy constraints ($K = 2, r_s = 50, \lambda_1 = 10^{-3} = 1.2732 \times 10^{-3}, \lambda_2 = 10\lambda_1, B_2 = 1$).

FIGURE 6. The ergodic secrecy rate versus the first user distance ($K = 2, \lambda_1 = 10^{-3} = 1.2732 \times 10^{-3}, \lambda_2 = 10\lambda_1, \lambda_s = 10^3$).
The ergodic rate of NOMA users in the BSs, the users, and the eavesdroppers are all equipped with a density of BSs at the first tier is kept fix. However, the spectrum efficiency performance. It is also inferred that applying HetNet to a secure multi-cell NOMA system improves the spectrum efficiency performance. Moreover, the obtained results verify that increase in the number of network tiers with a fixed density of BSs improves the ergodic secrecy rate. The ergodic secrecy rate is also enhanced with increase in density of the second tier BSs in a two-tier network while density of BSs at the first tier is kept fix. However, the secrecy constraint degrades the ergodic rate as expected. An interesting future work is to consider the scenario where the BSs, the users, and the eavesdroppers are all equipped with multi-antennas.

**APPENDIX A**

**PROOF OF LEMMA 1**

The ergodic rate of NOMA users in the k-th tier is calculated as follows:

\[
R_{w,k} = \mathbb{E}_{(r_{a},r_{t})}E_{\gamma_{m,q}}[\Theta(\gamma_{m,q}(r_{t},r_{a}))]
\]

\[
= \int_{0}^{\infty} \int_{0}^{\infty} \mathbb{E}_{\gamma_{m,q}}[\Theta(\gamma_{m,q}(r_{t},r_{a}))] \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= \int_{0}^{\infty} \int_{0}^{r_{t}} \mathbb{E}_{\gamma_{m,q}}[\Theta(\gamma_{m,q}(r_{t},r_{a}))] \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
+ \int_{0}^{\infty} \int_{r_{a}}^{\infty} \mathbb{E}_{\gamma_{m,q}}[\Theta(\gamma_{m,q}(r_{t},r_{a}))] \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t} = \int_{r_{a}}^{\infty} \int_{0}^{r_{t}} \mathbb{E}_{\gamma_{m,q}}[\gamma_{m,q}^{\gamma_{m,q}}] \, [\Theta(\min(\gamma_{m,q}(r_{t},r_{a})), \gamma_{m,q}^{\gamma_{m,q}}(r_{t},r_{a}))) \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= \int_{0}^{\infty} \int_{0}^{r_{t}} \mathbb{E}_{\gamma_{m,q}}[\gamma_{m,q}^{\gamma_{m,q}}] \, [\Theta(\min(\gamma_{m,q}(r_{t},r_{a})), \gamma_{m,q}^{\gamma_{m,q}}(r_{t},r_{a}))) \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
+ \int_{0}^{\infty} \int_{r_{a}}^{\infty} \mathbb{E}_{\gamma_{m,q}}[\gamma_{m,q}^{\gamma_{m,q}}] \, [\Theta(\min(\gamma_{m,q}(r_{t},r_{a})), \gamma_{m,q}^{\gamma_{m,q}}(r_{t},r_{a}))) \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= R_{m,k} + R_{m,k} + R_{m,k}^{\gamma_{m,q}}.
\]

(A.1)

where \( \Theta(x) = \log(1+x) \) and (a) caused by random selection of second user from network and \( w \in \{m, n\} \).

Keeping (A.1) in mind, the ergodic rate of the associated user \( (m) \) in Case I is calculated as:

\[
R_{m,k}^{\gamma_{m,q}} = \int_{0}^{\infty} \int_{0}^{r_{a}} \mathbb{E}_{\gamma_{m,q}}[\gamma_{m,q}^{\gamma_{m,q}}] \, [\Theta(\min(\gamma_{m,q}(r_{t},r_{a})), \gamma_{m,q}^{\gamma_{m,q}}(r_{t},r_{a}))) \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= \int_{0}^{\infty} \int_{0}^{r_{a}} \mathbb{E}_{\gamma_{m,q}}[\gamma_{m,q}^{\gamma_{m,q}}] \, [\Theta(\min(\gamma_{m,q}(r_{t},r_{a})), \gamma_{m,q}^{\gamma_{m,q}}(r_{t},r_{a}))) \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= \int_{0}^{\infty} \int_{0}^{r_{a}} \left[ \frac{1}{2} \int_{0}^{\infty} \exp \left( - \gamma_{m,q}(r_{t},r_{a}) \right) \, dt \right] \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= \int_{0}^{\infty} \int_{0}^{\infty} \frac{1}{2} \int_{0}^{\infty} \exp \left( - \gamma_{m,q}(r_{t},r_{a}) \right) \, dt \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= \int_{0}^{\infty} \int_{0}^{\infty} \frac{1}{2} \int_{0}^{\infty} \exp \left( - \gamma_{m,q}(r_{t},r_{a}) \right) \, dt \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

\[
= \int_{0}^{\infty} \int_{0}^{\infty} \frac{1}{2} \int_{0}^{\infty} \exp \left( - \gamma_{m,q}(r_{t},r_{a}) \right) \, dt \times f_{R_{a},R_{t}}(r_{a},r_{t}) \, dr_{a} \, dr_{t}
\]

(A.5)

Then, based on defining \( \gamma_{n,q} \) for Case I by substituting \( \{d_{m,q} = r_{a}\} \) in (7), we have

\[
\text{Pr}\left( \gamma_{n,q}^{\gamma_{n,q}} > \gamma \right) = \exp \left\{ - \frac{\sigma^{2}}{\gamma_{n,q}} \right\}
\]

(A.6)
By substituting (A.6) into (A.5), we have
\[
R^l_{n,k} = \frac{1}{\ln 2} \int_0^\infty \int_0^\infty \int_0^\infty \frac{1}{1 + \tau} \exp \left\{ -\frac{\tau^2 r_{\gamma_k} a_k}{\ln 2 P_k^l} \right\} \times L_{k} \left[ \frac{r_{\gamma_k} a_k}{P_k^l} \right] \left[ f_{R_n}(r_k) f_{R_n}(r_k) \right] dr_n dr_n dx_n \\
= \frac{1}{\ln 2} \int_0^\infty \int_0^\infty \int_0^\infty \frac{1}{1 + \tau} \exp \left\{ -\frac{\tau^2 r_{\gamma_k} a_k}{\ln 2 P_k^l} \right\} \times L_{k} \left[ \frac{r_{\gamma_k} a_k}{P_k^l} \right] \left[ f_{R_n}(r_k) f_{R_n}(r_k) \right] dr_n dr_n dx_n \\
= \frac{1}{\ln 2} \int_0^\infty \int_0^\infty \int_0^\infty \int_0^\infty \frac{1}{1 + \tau} \exp \left\{ -\frac{\tau^2 r_{\gamma_k} a_k}{\ln 2 P_k^l} \right\} \times L_{k} \left[ \frac{r_{\gamma_k} a_k}{P_k^l} \right] \left[ f_{R_n}(r_k) f_{R_n}(r_k) \right] dr_n dr_n dx_n.
\] (A.7)
Thus, (12) is obtained. The proof of (13) and (14) is similar to (11) and (12), respectively. This completes the proof.

APPENDIX B

PROOF OF LEMMA 2

The ergodic rate of legitimate user in Case I or Case II is \( R_{w,k} = \mathbb{E} \left[ \log(1 + (\gamma_{w,k})^l) \right] \) with \( w \in \{ m,n \} \), which is expressed in (11)-(14). The Jensen’s inequality is utilized to derive a lower bound on the ergodic rate of the \( w \)-th user as below:
\[
R_{w,k} \geq \log \left( 1 + \frac{1}{\mathbb{E} \left[ \gamma_{w,k}^l \right]} \right). \tag{B.1}
\]
Thus, the right hand side of (B.1) is the lower bound on the ergodic rate of legitimate user in Case I or Case II (i.e., \( R_{w,k} \)), which is verified in this proof. Considering \( \gamma_{m,m_k}^q \) and \( \gamma_{n,m_k}^q \) for Case I obtained by substituting \( \{ d_{m_k}^q = r_a \} \) in (5) and \( \{ d_{n_k}^q = r_s \} \) in (6) as well as inequality \( \frac{w^q}{w^q} \leq \min(u,v) \) that results in \( u,v \geq 0 \) [41], the lower bound on the ergodic rate of the \( m \)-th user in Case I (\( R^l_{m,k} \)) is calculated at (B.2), as shown at the bottom of the page.

In (B.2), (a) results from \( \mathbb{E} \left[ \frac{1}{\gamma_{w,k}^l} \right] \geq \frac{1}{\mathbb{E} \gamma_{w,k}^l} \) due to the convexity of \( \frac{1}{\gamma_{w,k}^l} \) and considering \( g_{w,k}^l \sim \exp(1) \). Based on (5) and (6), \( \mathbb{E} \left[ I_{w,k}^l \right] \) can be calculated as:

\[
\mathbb{E} \left[ I_{w,k}^l \right] = \sum_{j=1}^K \sum_{i \in \Phi_j} \sum_{|S_{l,j}^k|} P_j g_{w,j}^l (1 - \gamma_{w,j}^l) \tag{B.3}
\]

Similarly, to calculate the lower bound on the ergodic rate of the \( n \)-th user in Case I (\( R^l_{n,k} \)), based on defining \( \gamma_{m,n_k}^q \) for Case I by substituting \( \{ d_{n_k}^q = r_s \} \) in (7), we have:
\[
\mathbb{E} \left[ I_{n,k}^l \right] = \frac{1}{\mathbb{E} \gamma_{n,k}^l} \left[ \left( \frac{I_{n,k}^l + \sigma^2}{{\gamma_{n,k}^l}} \right)^{\alpha_k} \right] = \sum_{j=1}^K \int_{\gamma_j(r_s)}^\infty \frac{2 \pi P_j \lambda_j}{a_j - 2} \left( \frac{a_j}{a_j - 2} \right) y_j(r_s)^{2-a_j} \tag{B.4}
\]

where (a) results from using Campbell’s theorem and \( g_{w,j}^l \sim \exp(1) \). Using \( \mathbb{E} \left[ I_{w,k}^l \right] \) in (B.3), (15) is obtained by substituting (B.2) into the right hand side of (B.1).

APPENDIX C

PROOF OF COROLLARY 1

Substituting \( \alpha_k = \alpha, k \in [1 : K] \) and \( B_1 = 1 \) in (15), the lower bound on the ergodic rate of the \( m \)-th user in Case I is:
\[
R^l_{m,k} = (1 + \frac{2a_{m,k}^q}{a_{m,k}^q P_k} + \frac{1}{a_{m,k}^q P_k}) \times \int_0^\infty \left[ \mathbb{E} \left[ I_{m,k}^l \right] + \sigma^2 \right] r^q a_k (1 - F_{R_n}(r_a)) f_{R_n}(r_a) dr_a \\
+ \frac{1}{a_{m,k}^q P_k} \left[ \mathbb{E} \left[ I_{m,k}^l \right] + \sigma^2 \right] r^q a_k f_{R_n}(r_a) dr_a \\ \tag{C.1}
\]

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
First, $\mathbb{E}[I_{w_k,q}]$ from (B.3) is rewritten as:
\[
\mathbb{E}[I_{w_k,q}] = \frac{2P_k}{\alpha - 2}E_r^2 r_s^{-\alpha},
\]
where (a) results from $y_j(r_s) = \hat{P}_j^{-1/\alpha} r_u$ and $E \triangleq \sum_{j=1}^K \pi \lambda_j \hat{P}_j^{2/\alpha}$.

Based on $\alpha_k = \alpha, k \in [1 : K]$ and $\hat{B}_j = 1, A_k$ in (3) is calculated as:
\[
A_k = 2\pi \lambda_k \int_0^\infty r \exp(-E_r^2) \, dr = \frac{\lambda_k}{\sum_{j=1}^K \lambda_j \hat{P}_j^{2/\alpha}}.
\]
Then, we have
\[
\frac{\lambda_k}{A_k} = \sum_{j=1}^K \lambda_j \hat{P}_j^{2/\alpha}.
\]

Considering $w = n$ in (C.2), $u = s$ in (4), and using (C.4), $C$ can be calculated as follows:
\[
C = \int_0^\infty 2E \left( \frac{2P_k}{\alpha - 2}E_r^2 r_s^{-\alpha} + \sigma^2 r_s^{-\alpha + 1} \right) \exp(-E_r^2) \, dr_s
\]
\[
= \int_0^\infty 4P_k E^2 \frac{\sigma^2}{\alpha - 2} r_s^{-2} \exp(-E_r^2) \, dr_s
\]
\[
+ \left( \frac{2P_k}{\alpha - 2} + \frac{\sigma^2}{2(2E)^2} \right) \frac{\alpha - 1}{\alpha - 2}.
\]

APPENDIX D

PROOF OF LEMMA 3

The ergodic leakage rate of the most detrimental eavesdropper for detecting information of the $w$-th user ($w \in \{m,n\}$) is written as:
\[
\mathbb{E}\left[ \log(1 + \gamma_{\text{max}_k}) \right] = \frac{1}{\ln 2} \int_0^\infty 1 - F_\gamma(t) \, dt.
\]

Based on (8), the CDF of $\gamma_{\text{max}_k}$ is calculated as:
\[
F_\gamma(t) = \Pr\left( \gamma_{\text{max}_k} < t \right)
\]
\[
= \Pr\left( \max_{c \in \Phi_c} \frac{a_{m_k} P_k \varepsilon_{c_m} d_{a_m}^2}{\lambda_{a_m} + \sigma^2} < t \right)
\]
\[
= \int_0^\infty \exp\left( - \lambda_c \int_0^\infty \Pr\left( \gamma_{r_s} > t \frac{\lambda_{a_m} + \sigma^2}{a_{m_k} P_k} r_s \right) \, dr_s \right)
\]
\[
= \int_0^\infty \exp\left( - 2\pi \lambda_c \int_0^\infty \exp\left( - t \frac{\lambda_{a_m} + \sigma^2}{a_{m_k} P_k} r_s \right) \, dr_s \right).
\]

where (a) and (b) are in accordance to use of the generating functional of the PPP $\Phi_c$ and the polar-coordinate system, respectively; $L_t$ is obtained by (10). Finally, (23) is obtained by substituting (D.2) into (D.1). This completes the proof.

APPENDIX E

PROOF OF COROLLARY 4

Substituting $\sigma^2 = 0, \alpha_k = \alpha, k \in [1 : K]$, and $\hat{B}_j = 1$ in (11), the ergodic rate of the associated user ($m$) in Case I is:
\[
R_{m,k}^l(\alpha, 1)
\]
\[
= \frac{1}{\ln 2} \int_0^\infty \frac{\lambda_{a_m}}{P_k} \frac{\tau_a}{(\lambda_{m_k} - \lambda_{a_m}) P_k} \frac{1}{1 + t L_{m_k} \left( \frac{\tau_a}{(\lambda_{m_k} - \lambda_{a_m}) P_k} \right)} \, dt d\tau_a d\tau \, d\tau
\]
where from (9) we obtain:
\[
L_{m_k} \left( \frac{\tau_a}{(\lambda_{m_k} - \lambda_{a_m}) P_k} \right) = \exp \left( - \sum_{j=1}^K \lambda_j \hat{P}_j^2 \right)
\]
\[
\hat{P}_j^2 = \frac{2tA}{\alpha - 2} \times \int \left( 1, 1 - \frac{2}{\alpha} \right) \hat{P}_j^2 Z_m
\]
where (a) and (b) follow from $A \triangleq \frac{1}{\alpha_{\text{avg},q} - \tau_{\text{avg},q}}$ and $Z_m \triangleq \frac{2a}{a^2 - 2} \times 2F_1(1, 1 - \frac{2}{a}; 2; 2 - \frac{2}{a}; -\tau A)$, respectively. Similarly, we use (9) to obtain:

$$L_{\text{h},(\alpha,1)} \left( \frac{tr_s^\alpha}{(a_{\text{avg},q} - \tau_{\text{avg},q}) P_k} \right) = \exp \left\{ -\sum_{j=1}^{K} \pi \lambda_j P_j^{\frac{2}{\alpha}} R_s \right\} \frac{Z_m}{1 + t} \times f_{R_s}(r_s) \, dt \, dr_s. \quad \text{(E.3)}$$

By substituting (E.2) and (E.3) into (E.1), $u = s$ in (4), and exploiting (C.4), (E.1) can be rewritten as:

$$R_{m,k}(\alpha, 1) = \frac{1}{\ln 2} \int_0^\infty \int_0^r \int_0^\infty \frac{K}{2\pi \lambda_j P_j^{\frac{2}{\alpha}}} \, r_s \exp \left\{ -\sum_{j=1}^{K} \pi \lambda_j P_j^{\frac{2}{\alpha}} R_s \right\} \frac{Z_m}{1 + t} \times f_{R_s}(r_s) \, dt \, dr_s. \quad \text{(E.4)}$$

The inner integral can be calculated as:

$$\int_0^{r_a} r_s G \, dr_s \equiv \int_0^{r_a} r_s \exp \left\{ -E(1 + Z_m) r_s^2 \right\} \exp \left\{ -E r_a^2 Z_m \right\} \, dr_s \exp \left\{ -E r_a^2 Z_m \right\} \frac{Z_m}{2E(1 + Z_m)} \left( 1 - \exp \left\{ -E(1 + Z_m) r_a^2 \right\} \right). \quad \text{(E.5)}$$

where (a) follows from $E \triangleq \sum_{j=1}^{K} \pi \lambda_j P_j^{\frac{2}{\alpha}}$ and $G$ is defined in (E.4). Thus, (E.1) can be rewritten by considering $u = a$ in (4) as follows:

$$R_{m,k}(\alpha, 1) = \frac{1}{\ln 2} \int_0^\infty \frac{1}{1 + t} \exp \left\{ -E r_a^2 Z_m \right\} \left( 1 - \exp \left\{ -E(1 + Z_m) r_a^2 \right\} \right) dt \, dr_a. \quad \text{(E.6)}$$

Finally, (27) is achieved after some simplifications and utilizing $\int_0^\infty r_a \exp \left\{ -E r_a^2 \right\} \, dr_a = \frac{1}{2E}$ based on [38, eq. (3.326.2)].

Similarly, the ergodic rate of the second user ($n$) in Case I is written by substituting $\sigma^2 = 0$, $\alpha_k = \alpha$, $k \in [1 : K]$, and $B_j = 1$ in (12) as:

$$R_{n,k}(\alpha, 1) = \frac{1}{\ln 2} \int_0^\infty \int_0^\infty \frac{1}{1 + t} \exp \left\{ -E r_a^2 Z_m \right\} \times \left( \exp \left\{ -E r_a^2 r_s^2 \right\} - \exp \left\{ -E r_a^2 (2 + Z_m) \right\} \right) dt \, dr_a. \quad \text{(E.7)}$$

By substituting $L_{\text{h},(\alpha,1)} \left( \frac{tr_s^\alpha}{a_{\text{avg},q} P_k} \right)$ from (9) into (E.7), $u = a$ in (4), and using (C.4), (E.7) can be rewritten as:

$$R_{n,k}(\alpha, 1) \equiv \frac{1}{\ln 2} \int_0^\infty \int_0^\infty \frac{K}{2\pi \lambda_j P_j^{\frac{2}{\alpha}}} \, r_s \exp \left\{ -\sum_{j=1}^{K} \pi \lambda_j P_j^{\frac{2}{\alpha}} r_s \right\} \frac{Z_m}{1 + t} \times f_{R_s}(r_s) \, dt \, dr_s, \quad \text{(E.8)}$$

where (a) follows from $Z_m \triangleq \frac{2a}{a^2 - 2} \times 2F_1(1, 1 - \frac{2}{a}; 2; 2 - \frac{2}{a}; -\frac{t}{a_{\text{avg},q}})$. The inner integral can be computed by considering $u = s$ in (4) as:

$$\int_0^\infty r_s H f_{R_s}(r_s) \, dr_s = \int_0^\infty r_s \exp \left\{ -E(2 + Z_m) r_s^2 \right\} \, dr_s = \frac{1}{2E(2 + Z_m)} \quad \text{(E.9)}$$

where $H$ is defined in (E.8). Finally, (28) is obtained based on [38, eq. (3.326.2)] after doing some simplifications.

The ergodic leakage rate in the most detrimental eavesdropper for detecting information of the $w$-th user ($w \in \{m, n\}$) is obtained as follows by substituting $\sigma^2 = 0$, $\alpha_k = \alpha$, $k \in [1 : K]$, and $B_j = 1$ in (23):

$$R_{w,k}(\alpha, 1) \equiv \frac{1}{\ln 2} \int_0^\infty \frac{1}{1 + t} \exp \left\{ -2\pi \lambda_e \int_0^\infty L_{\text{h},(\alpha,1)} \left( \frac{td_{w,k}^{\alpha}}{a_{\text{avg},q} P_k} \right) \, r \, dr \right\} \, dt. \quad \text{(E.10)}$$

Substituting $L_{\text{h},(\alpha,1)} \left( \frac{td_{w,k}^{\alpha}}{a_{\text{avg},q} P_k} \right)$ from (10) into (E.10) gives:

$$R_{w,k}^w(\alpha, 1) \equiv \frac{1}{\ln 2} \int_0^\infty \frac{1}{1 + t} \times \left( \exp \left\{ -2\pi \lambda_e \int_0^\infty \exp \left\{ -D_e r_s^2 \right\} \, dr \right\} \right), \quad \text{(E.11)}$$

where (a) results from defining $D_e \triangleq \sum_{j=1}^{K} \pi \lambda_j P_j^{\frac{2}{\alpha}}$ ($\frac{\pi \lambda_j P_j^{\frac{2}{\alpha}}}{(1 + \frac{2}{a}) \Gamma(1 + \frac{2}{a})} \Gamma(1 - \frac{2}{a})$). Using [38, eq. (3.326.2)], (31) is achieved after some simplifications. This completes the proof.

REFERENCES

[1] “5G white paper,” NGMN Alliance e.V., Düsseldorf, Germany, White Paper, vol. 1, 2015.

[2] A. Gupta and R. K. Jha, “A survey of 5G network: Architecture and emerging technologies,” IEEE Access, vol. 3, pp. 1206–1232, 2015.

[3] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” IEEE Commun. Surveys Tutts., vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[4] A. Damnjanovic et al., “A survey on 3GPP heterogeneous networks,” IEEE Wireless Commun., vol. 18, no. 3, pp. 10–21, Jun. 2011.

[5] S. Brueck, “Heterogeneous networks in LTE-advanced,” in Proc. 8th Int. Symp. Wireless Commun. Syst., 2011, pp. 171–175.

[6] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, “A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends,” IEEE J. Sel. Areas Commun., vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[7] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, “A survey of non-orthogonal multiple access for 5G,” IEEE Commun. Surveys Tutts., vol. 20, no. 3, pp. 2294–2323, 3rd Quart., 2018.

[8] 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.
[9] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, “A survey of physical layer security techniques for 5G wireless networks and challenges ahead,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, Apr. 2018.

[10] Y. Liu, H.-H. Chen, and L. Wang, “Physical layer security for next generation wireless networks: Theories, technologies, and challenges,” IEEE Commun. Surveys Tuts., vol. 19, no. 1, pp. 347–376, 1st Quart., 2016.

[11] T. Q. Duong, X. Zhou, and H. V. Poor, “Trusted Communications With Physical Layer Security for 5G and Beyond.” Stevenage, U. K.: Institt. Eng. Technol., Jan. 2017.

[12] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, “Secrecy sum rate maximization in non-orthogonal multiple access,” IEEE Commun. Lett., vol. 20, no. 5, pp. 930–933, May 2016.

[13] B. He, A. Liu, N. Yang, and V. K. Lau, “On the design of secure non-orthogonal multiple access systems,” IEEE J. Sel. Areas Commun., vol. 35, no. 10, pp. 2196–2206, Oct. 2017.

[14] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, “Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks,” IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[15] J. Chen, L. Yang, and M.-S. Alouini, “Physical layer security for cooperative NOMA systems,” IEEE Trans. Veh. Technol., vol. 67, no. 5, pp. 4645–4649, May 2018.

[16] B. Zheng et al., “Secure NOMA based two-way relay networks using artificial noise and full duplex,” IEEE J. Sel. Areas Commun., vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[17] C. Gong, X. Yue, Z. Zhang, X. Wang, and X. Dai, “Enhancing physical layer security with artificial noise in large-scale NOMA networks,” IEEE Trans. Veh. Technol., vol. 70, no. 3, pp. 2349–2361, Mar. 2021.

[18] M. Zeng, N.-P. Nguyen, O. A. Dobre, and H. V. Poor, “Securing downlink massive MIMO-NOMA networks with artificial noise,” IEEE J. Sel. Topics Signal Process., vol. 13, no. 3, pp. 685–699, Jun. 2019.

[19] W. Yu, A. Chorti, L. Musavian, H. V. Poor, and Q. Ni, “Effective secrecy rate for a downlink NOMA network,” IEEE Trans. Wireless Commun., vol. 18, no. 12, pp. 5673–5690, Dec. 2019.

[20] N. Jaiswal, A. Pandey, S. Yadav, and N. Purohit, “Physical layer security performance of NOMA-assisted vehicular communication systems over double-Rayleigh fading channels,” Phys. Commun., vol. 57, Apr. 2023, Art. no. 101968.

[21] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, “Physical layer security in heterogeneous cellular networks,” IEEE Trans. Commun., vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[22] M. Xu, X. Tao, F. Yang, and H. Wu, “Enhancing secured coverage with uplink NOMA transmission in heterogeneous cellular networks,” IEEE Commun. Lett., vol. 20, no. 11, pp. 2272–2275, Nov. 2016.

[23] L. Wang, K.-K. Wong, M. Elkashlan, A. Nallanathan, and S. Lambotharan, “Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference,” IEEE J. Sel. Topics Signal Process., vol. 10, no. 8, pp. 1375–1389, Dec. 2016.

[24] W. Wang, K. C. Teh, and K. H. Li, “Artificial noise aided physical layer security in multi-antenna small-cell networks,” IEEE Trans. Inf. Forensics Security, vol. 12, pp. 1470–1482, 2017.

[25] S. Wang, Y. Gao, C. Dong, N. Sha, and G. Zang, “Secure user association in two-tier heterogeneous cellular networks with in-band interference,” IEEE Access, vol. 6, pp. 38607–38615, 2018.

[26] Y. Zou, “Intelligent interference exploitation for heterogeneous cellular networks against eavesdropping,” IEEE J. Sel. Areas Commun., vol. 36, no. 7, pp. 1453–1464, Jul. 2018.

[27] Y. Liu, Z. Qin, M. Elkashlan, A. Nallanathan, and J. A. McCann, “Non-orthogonal multiple access in large-scale heterogeneous networks,” IEEE J. Sel. Areas Commun., vol. 35, no. 12, pp. 2667–2680, Dec. 2017.

[28] T. Han et al., “On downlink NOMA in heterogeneous networks with non-uniform small cell deployment,” IEEE Access, vol. 6, pp. 31099–31109, 2018.

[29] C.-H. Liu and D.-C. Liang, “Heterogeneous networks with power-domain NOMA: Coverage, throughput, and power allocation analysis,” IEEE Trans. Wireless Commun., vol. 17, no. 5, pp. 3524–3539, May 2018.

[30] C. Al-tay and M. Koza, “Stochastic geometry analysis of interference coordination in NOMA-based heterogeneous networks,” 2018, arXiv:1809.07410.