IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 27, 2017, accepted November 4, 2017, date of publication November 22, 2017,
date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2776119

Resource Allocation for Secure Communication in *K*-Tier Heterogeneous Cellular Networks: A Spatial-Temporal Perspective

BING WANG[1], KAIZHI HUANG[1], XIAOMING XU[1], LIANG JIN[1], ZHOU ZHONG[1], AND YI WANG[1,2]

[1]National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China
[2]School of Electronics and Communication Engineering, Zhengzhou University of Aeronautics, Zhengzhou 450046, China

Corresponding author: Xiaoming Xu (xiaomingxu.plaust@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61379006, in part by the National Natural Science Foundation of China under Grant 61401510, in part by the National Natural Science Foundation of China under Grant 1701538, and in part by the National Natural Science Foundation of China under Grant 61601514.

ABSTRACT Resource allocation in secure communication is of primary importance due to the fact that the next-generation wireless network (5G) aims to achieve high spectral efficiency and a high level of security. Different from previous studies, we study the resource allocation for secure transmission in *K*-tier dynamic heterogeneous cellular networks jointly considering the randomness of base stations (BSs) in spatial dimension and user equipment (UE) arrival and departure processes in temporal dimension. First, we develop a 3-D stochastic model by jointly taking into account the randomness of BSs in two spatial dimensions and UE arrival and departure processes in one temporal dimension. Second, we analyze the connection outage probability and secrecy outage probability of the typical UE. Their expressions admit quite simple closed-forms in some plausible special cases. Based on the outage analysis, the reliability and security performances of the network are evaluated, respectively. Third, we investigate the network-wide secrecy throughput in virtue of the outage analysis. Furthermore, we derive the optimal resource allocation factors of different tiers to maximize the secrecy throughput. Since the objective function of the maximization problem is not in closed form and non-convex, the concave upper and lower bounds are deduced and utilized, which leads to near-optimal solutions of the resource allocation factors of different tiers. It is demonstrated that apart from the spatial intensity and transmission power of each BS, UE arrival and departure processes are also key elements influencing the resource allocation factors of different tiers. Finally, numerical results show the usefulness and correctness of our theoretical conclusions.

INDEX TERMS Physical layer security, heterogeneous cellular networks, resource allocation, queueing theory, stochastic geometry.

I. INTRODUCTION

A. RELATED WORK AND MOTIVATION

Heterogeneous cellular networks (HCNs) can provide seamless wide-area coverage and high-capacity in hot-spot through reasonably deploying different types of base stations (BSs), e.g., pico and femto cell BSs, which is a key type of network deployment in the next generation cellular network (5G) [1], [2]. Nevertheless, due to the open nature of wireless channels, information security has always been an issue that we cannot avoid in 3G, 4G, and 5G networks [5]. Physical layer security (PLS) [8], [9] which exploits the fading characteristics of wireless channels to secure the wireless transmission, has drawn ever-increasing attention since Wyner's path breaking research [11]. Different from single-layer network, the unique network structure of heterogeneous cellular networks makes its security threats more serious (i) There are severe intra-tier and inter-tier interferences in HCNs due to the fact that BSs in different tiers may work on the same resource block (RB) [12]. (ii) BSs in different tiers have different abilities to ensure safety owing to different parameters of BSs in different tiers (spatial densities and transmission powers, etc.). Therefore, how to allocate the spectrum resource among different tiers to eliminate the interference and achieve the optimal network-wide secrecy is a meaningful problem.

With the wireless spectrum resources becoming increasingly scarce and expensive, resource allocation has become a hot topic for academia and industry [8], [16]–[20].

Shiqi *et al.* [18] investigated the joint optimization of power and subcarrier allocation to achieve the secure communications in HCNs. Considering that the illegal nodes may eavesdrop or jam the communication between the legitimate nodes, Sheikhzadeh *et al.* [19] designed a sub-carriers and transmit powers allocation strategy, such that the achievable secrecy rate is maximized. In order to maximize the secure capacity for both cellular users and D2D users, Zhang *et al.* [20] studied the secrecy-optimized resource allocation for the D2D communication underlaying HCNs. Further, taking account of the unplanned nature of the future wireless networks, Wang *et al.* [8] investigated the network-wide secrecy throughput under the connection and secrecy probability constraints using the stochastic geometry.

An important feature of resource allocation is that it is driven by traffic demand, which is ignored in the above studies accidently or not. A UE may arrive or departure the network at anytime and anywhere in the real environment [1], [21]–[25]. The traffic demand also changes with the UE arrival and departure processes. Thus, we must take the UE arrival and departure processes into consideration when we solve the problem of optimal resources allocation. Considering the randomness of UE in temporal dimension, Gharbieh *et al.* [23] developed a queueing model accounting for the traffic requirement per IoT device, and proposed three transmission schemes: baseline scheme, power-ramping scheme and back-off scheme. Taking the BS activity and temporal correlation of transmissions into consideration, Zhang *et al.* [24] studied the delay and reliability tradeoffs in HCNs. In order to maximize the downlink sum throughput, Bao and Liang [25] investigated the optimal radio resource allocation in the multiple tiers of HCNs. Unfortunately, the existing literature on HCNs which considering the UE arrival and departure processes has mainly focused on coverage probability and delay, little of them have involved security issues.

To the best of our knowledge, no prior work has investigated resource allocation for secure transmission jointly considering the randomness of BSs in spatial dimension and UE arrival and departure processes in temporal dimension. Therefore, considering the randomness in spatial and temporal dimensions, how to optimally allocate the expensive secure spectrum resource among different tiers to maximize the network-wide secrecy throughput remains an open problem.

B. OUR WORK AND CONTRIBUTIONS

In this paper, we investigate the resource allocation in K-tier HCNs by jointly taking into account the randomness of BSs in spatial dimension and UE arrival and departure processes in temporal dimension. We provide a comprehensive performance analysis using the queueing theory and stochastic geometry. The major contributions of this paper are summarized as follows:

1) In order to characterize the random spatial and temporal patterns of the K-tier dynamic HCNs, we first develop a three-dimensional stochastic model by jointly taking into account the randomness of BSs in two spatial dimensions and UE arrival and departure processes in one temporal dimension.

2) We analyze the connection outage probability (COP), secrecy outage probability (SOP) of the typical UE. Based on the outage probability results, reliability performance and security performance of the typical UE are evaluated, respectively. Furthermore, we investigate the network-wide secrecy throughput in virtue of the connection outage and secrecy outage analysis.

3) We answer the question, i.e., how to allocate the resource blocks among different tiers to achieve the network-wide secrecy throughput optimization. Due to the fact that the optimization problem is not in closed form and non-convex, we get the approximate solution by use of the upper and lower bounds of the objective function with gamma function.

According to the obtained results, we further provide some feasible predictions of network performance and guidance for future network designs. For example, a larger UE arrival rate benefits the security performance. Nevertheless, the network-wide secrecy throughput first increases and then remains unchanged with the increase of UE arrival rate.

The remainder of this paper is organized as follows. In Section II, we describe the system model and performance metrics. In Section III, we analyze the connection outage probability, secrecy outage probability, respectively. In Section IV, we investigate the network-wide secrecy throughput and derive the optimal resource allocation factors to maximize the network-wide secrecy throughput. In Section V, we show the numerical and simulation results. Section VI concludes the paper.

II. SYSTEM MODEL

A spatio-temporal stochastic model jointly considering the randomness of BSs in spatial dimension and UE arrival (departure) process in temporal dimension is established as Fig. 1.

A. SPATIAL DIMENSION AND PHYSICAL LAYER PARAMETERS

We consider downlink transmission in K-tier HCNs. BSs in different tiers have different parameters (spatial densities and transmission powers), while those in the same tier share the same parameters. The locations of kth tier ($k = 1, 2, \ldots, K$) BSs are modeled as a homogeneous Poisson point process (HPPP) ϕ_k with density λ_k in $\mathbb{R}^2$, $\phi_1, \phi_2, \ldots, \phi_K$ are assumed to be independent. The transmission power of BSs in tier k is P_k. There coexists UEs and eavesdroppers (EVEs), where UEs are legitimate nodes while EVEs attempt to intercept the secret information intended for UEs. The locations of EVEs follow another, independent, HPPP ϕ_E of density λ_E in $\mathbb{R}^2$. Each node in the HCNs has a single antenna. We focus on the interference-limited scenario and the effect of AWGN (Additive White Gaussian Noise) is not considered, signal-to-interference ratio (SIR) is used just like [26].

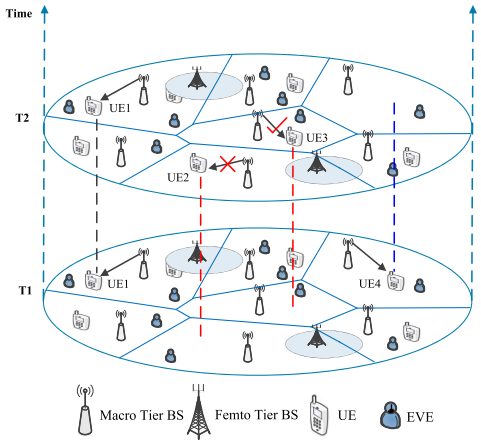


FIGURE 1. An example of spatio-temporal stochastic model in two-tier dynamic HCNs. For spatial dimension: A weighted Poisson-Voronoi tessellation is described based on the association policy. For temporal dimension: The new arrival UE may be rejected (UE2) or accepted by the networks (UE3). A UE may departure the system (UE4). A UE also may receive services all the time (UE1).

In addition, wireless channels are assumed to undergo flat Rayleigh fading together with large-scale path loss governed by the exponent α, and $\alpha > 2$.

The HCN is working on W orthogonal resource blocks (RBs). In order to eliminate the cross-tier interference, BSs in different tiers are operated on non-overlapping RBs [25], [27]. Without loss of generality, each UE requires a frequency bandwidth of 1 (i,e., unit frequency bandwidth). The network operator allocates $\mathrm{W}_k = \eta_k \mathrm{W}$ RBs to each tier-k BSs, where η_k is the resource allocation factor, and $\sum_{k=1}^{K} \eta_k = 1$. Let $\boldsymbol{\eta} = (\eta_1, \eta_1, \ldots, \eta_K)$. BSs in the same tier are working on the same RBs and will interfere at the co-tier UEs.

With the popularity of smart mobile devices, multimedia applications have proliferated in mobile networks. A defining characteristic of multimedia applications is inelasticity. Inelasticity means the required network throughput for a multimedia session is defined in discrete levels, and the minimum throughput must be satisfied, or the session is rejected [25], [28]. Considering that we assume each UE requires a unit frequency bandwidth in this paper, in other words, we can say that if the number of UEs is larger than RBs in the same BS, this UE will be rejected.

We assume open access, which means a UE is allowed to access any tier's BSs. Compared with closed-access, this access policy can provide best-case coverage. A typical UE is associated with the BS in tier k which can provide the highest average received signal power. In other words, a typical user associated with the kth BS when $P_k x_k^{-\alpha} > P_j x_j^{-\alpha}$ for all $j \in \{1, \ldots, K\}, j \neq k$. We assume that each BS has perfect CSI (Channel State Information) of the legitimate link while EVEs' CSI is unavailable at BSs [8], [9]. Considering the difficulties of codebook designing and any instantaneous CSI is not available for the BS, the codeword transmission rate R_t and confidential information rate R_m are assumed fixed over time [8]. Fixed-rate transmissions are often adopted in practice to reduce the complexity of systems, e.g., video streaming in multimedia applications.

B. TEMPORAL DIMENSION PARAMETERS

Taking the randomness of UE arrival and departure processes into consideration, queueing theory is used to analyze the number of UEs in each servicing BS just like [1], [23], [25], [28]. We assume the arrival process of UEs is modeled by an independent HPPP ϕ_u of density β_u in $\mathbb{R}^3$, which accounts for two spatial dimensions and one temporal dimension. Note that the spatial Poisson modeling of UEs is the same as conventional stochastic geometric studies in [4] and [6], and the Poisson arrival of UEs have been well supported in [17] and [20]. Further, the dynamics of the eavesdropper's behavior is not considered in this paper, since eavesdroppers are all passive.

Furthermore, since inelastic traffic is considered in this paper, there are several states of each UE. Firstly, the arriving UE may be rejected by the network. If the UE is rejected by the network, it leaves the networks immediately. Secondly, if it is accepted, it will stay in the network for a random duration time. We assume the duration time is exponentially distributed with mean $\frac{1}{v}$ minutes just like [25].

Jointly considering the above analysis of UE arrival and departure processes, we employ an $M/M/W_k/W_k$ discrete time Markov chain (DTMC) to track the time evolution of UEs with arrival rate β_u and departure rate v, where M represents the Poisson arrival (departure) process, W_k represents the number of RBs in tier k allocated from the network operator.

C. PERFORMANCE METRIC

1) CONNECTION OUTAGE PROBABILITY

The reliability performance of the network is illustrated by COP. COP is defined as the probability that the channel capacity from the BS to the intended UEs is below the transmission rate R_t, which quantifies the probability that the message cannot be decoded at the intended UEs without error. Define a threshold SIR value for connection outage of the typical UE as $\theta_{cop} = 2^{R_t} - 1$.

2) SECRECY OUTAGE PROBABILITY

The security performance of the network is illustrated by SOP. SOP is defined as the probability that the channel capacity from the transmitter to the eavesdropper is larger than the rate increment $R_t - R_m$, which quantifies the probability that the perfect secrecy of the information can not be guaranteed. Define a threshold SIR value for secrecy outage of the typical UE as $\theta_{sop} = 2^{(R_t - R_m)} - 1$, where R_m is the confidential information rate.

3) NETWORK-WIDE SECRECY THROUGHPUT

Network-wide secrecy throughput jointly measures the reliability and security performances of the network.

Similar with [8], [29], [30], network-wide secrecy throughput is defined as the product of BS density, the number of active RBs, the connection probability, the secrecy probability and the secrecy rate, which is given by

$$\begin{aligned}\psi &= \sum_{k=1}^{K} \lambda_k \psi_k \\ &= \sum_{k=1}^{K} \lambda_k \mathbb{E}\left(W_k\right)\left(1-P_{cop,k}\right)\left(1-P_{sop,k}\right) R_s, \end{aligned} \quad (1)$$

where ψ_k is the network-wide secrecy throughput of tier k, $\mathbb{E}\left(W_k\right)$ is the average number of active RBs of tier k, which will be given in the following part. $P_{cop,k}$ ($P_{sop,k}$) is the COP (SOP) that a UE connects with the BS in tier k.

III. PERFORMANCE ANALYSIS

In this section, considering the randomness of BSs in spatial dimension and UE arrival (departure) process in temporal dimension, we apply the stochastic geometry and queueing theory to analyze performances listed in section II-C.

A. COP ANALYSIS

Let ϕ_k' denote the point process corresponding to all tier k BSs other than the typical BS using the same RB. Based on the standard Palm theory, we find that ϕ_k' is a PPP with intensity $p_k\lambda_k$, where p_k is the probability that the same RB is actively in use at a non-typical tier k BS. Therefore, p_k is a key parameter influencing the density of interfering BSs. It should be noted that p_k is closely related to the arrival and departure processes of UEs in the network. Therefore, unlike most existing studies [5], [8], [9], [11], considering the UE arrival and departure processes, the realistic density of interfering BSs in tier k is $p_k\lambda_k$ instead of λ_k.

Considering an arbitrary typical link in the HCN, the SIR received by a typical UE from the correspond servicing BS in tier k is given by

$$\gamma_{u,k} = \frac{P_k g_{u,k} x^{-\alpha}}{\sum_{j\in\phi_k'} P_k h_{j,k} |Y_{j,k}|^{-\alpha}}, \quad (2)$$

where $g_{u,k}$ and $h_{j,i}$ are the Rayleigh fading channel gains from the servicing BS and interfering BS to the typical user, respectively. x and $|Y_{j,k}|$ are the distances from the servicing BS and interfering BS to the typical user, respectively.

Thus, the COP of the typical link from the BS in tier k is given by

$$\begin{aligned} P_{cop,k} &= \mathbb{P}\left(\gamma_{u,k} < \theta_{cop}\right) \\ &= 1 - \int_0^{\infty} \mathbb{P}\left(\gamma_{u,k}\left(x\right) > \theta_{cop}\right) f_{X_k(x)} dx, \end{aligned} \quad (3)$$

where $f_{X_k(x)}$ denotes the probability density function (PDF) of distance X_k between a typical user and its servicing BS.

Theorem 1: For an open access K-tier HCN, considering the UE arrival and departure processes, the COP of the typical link from the BS in tier k is

$$P_{cop,k} = 1 - \frac{1}{1+\mathcal{A}_k p_k \mathcal{Z}}, \quad (4)$$

where $\mathcal{Z} = \frac{2\theta_{cop}}{\alpha-2} {}_2F_1\left[1,\ 1-\frac{2}{\alpha};\ 2-\frac{2}{\alpha};\ -\theta_{cop}\right]$, $\mathcal{A}_k$ is the probability of a typical UE connecting the BS in tier k, and $\mathcal{A}_k = \lambda_k / \left(\sum_{j=1}^{K} \lambda_j \left(\frac{P_j}{P_k}\right)^{2/\alpha}\right)$. p_k denotes the probability that an RB is actively in use.

Proof: Please see Appendix A.

Corollary 1: If the path loss exponents $\alpha = 4$, the Gauss hypergeometric function ${}_2F_1$ in Theorem 1 collapses to a simple arctangent function denoted by arctan(). This provides a simple expression for the COP, which is given by

$$P_{cop,k} = 1 - \frac{1}{1+\mathcal{A}_k p_k \sqrt{\theta_{cop}} \arctan\left(\sqrt{\theta_{cop}}\right)}. \quad (5)$$

From (4), we know that p_k is a key factor influencing the COP of the typical UE, which is required to compute ψ. The core step to get p_k is calculating the proportion of total resource blocks being used by UEs in the network. Considering the UE arrival and departure processes, queueing theory is employed to get p_k.

Given the cell size of a tier k cell is $S_k = s$, the number of RBs allocated from the network operator in tier k is W_k. We first calculate the number of UE in a tier k cell s. An $M/M/W_k/W_k$ queueing model is given in section II-B. Using the queueing theory, the probability that there are n UEs in the cell s is

$$\mathbb{P}\left(M_k = n | S_k = s\right) = \frac{\left(\frac{\beta_u s}{\nu}\right)^n / n!}{\sum_{i=0}^{W_k} \left(\frac{\beta_u s}{\nu}\right)^i / i!}. \quad (6)$$

Next, we aim to get $p_k\left(s\right)$, which represents the probability that a RB in the tier k cell is actively in use.

$$p_k\left(s\right) = \sum_{n=0}^{W_k} \frac{n}{W_k} \frac{\left(\frac{\beta_u s}{\nu}\right)^n / n!}{\sum_{i=0}^{W_k} \left(\frac{\beta_u s}{\nu}\right)^i / i!} = \begin{cases} \frac{\beta_u s}{\nu W_k}, & \text{if } \frac{\beta_u s}{\nu W_k} < 1, \\ 1, & \text{if } \frac{\beta_u s}{\nu W_k} \geqslant 1. \end{cases} \quad (7)$$

From [31], the probability density function (PDF) of S_k is given as

$$f_{S_k}\left(s\right) = \frac{3.5^{3.5}}{\Gamma\left(3.5\right)} \frac{\lambda_k}{\mathcal{A}_k} \left(\frac{\lambda_k}{\mathcal{A}_k} s\right)^{2.5} \exp\left(-3.5 s \frac{\lambda_k}{\mathcal{A}_k}\right). \quad (8)$$

Mathematically, combing (7) and (8), p_k is given by

$$\begin{aligned} p_k &= \int_0^{\infty} p_k\left(s\right) f_{S_k}\left(s\right) ds \\ &= \frac{1}{\omega_k} - \frac{1}{\omega_k} \frac{3.5^{3.5}}{\Gamma\left(3.5\right)} \int_1^{\infty} \left(y-1\right) \omega_k^{4.5} y^{2.5} \exp\left(-3.5\omega_k y\right) dy, \end{aligned} \quad (9)$$

where $\omega_k = \frac{\lambda_k \nu W_k}{\mathcal{A}_k \beta_u}$. For presentation convenience, we define $f\left(\omega_k\right) = \frac{3.5^{3.5}}{\Gamma(3.5)} \int_1^{\infty} \left(y-1\right) \omega_k^{4.5} y^{2.5} e^{-3.5\omega_k y} dy$. Thus, p_k can be simply rewritten as $p_k = \frac{1}{\omega_k} - \frac{1}{\omega_k} f\left(\omega_k\right)$.

Remark 1: Different from the most existing works [8], [9], [11], [12], which imply that the COP is only related with spatial density and transmission power of each BS. We find that

P_{cop} is also an increasing function of UE arrival rate β_u when we consider the UE arrival and departure processes. This result makes sense when one realizes that as UE arrival rate β_u is increasing, there will be more UEs using the same RB, the interference will be more severe than before.

From (9), we can also get the average number of active RBs in tier k

$$\mathbb{E}(W_k) = p_k W_k = \frac{\mathcal{A}_k \beta_u}{\lambda_k v}(1 - f(\omega_k)). \tag{10}$$

Corollary 2: If $\alpha = 4$ and $\beta_u \to \infty$, which means each RBs of all BSs are occupied. From (7), we can get that $p_k = 1$. The COP in (4) is reduced to the case that the UE arrival and departure processes are not considered, which can be given as

$$P_{cop,k} = 1 - \frac{1}{1 + \mathcal{A}_k \sqrt{\theta_{cop}} \arctan\left(\sqrt{\theta_{cop}}\right)}. \tag{11}$$

B. SOP ANALYSIS

The instantaneous SIR received by an eavesdropper e from the BS in tier k is given by

$$\gamma_{E,k} = \frac{P_k g_{E,k} x^{-\alpha}}{\sum_{j \in \phi_k'} P_k h_{j,k} |Y_{j,k}|^{-\alpha}}, \tag{12}$$

where $g_{E,k}$ and $h_{j,i}$ are the Rayleigh fading channel gains from the BS in tier k and interfering BS to the eavesdropper, respectively. x and $|Y_{j,i}|$ are the distances from the BS in tie k and interfering BS to the eavesdropper, respectively.

Thus, the SOP of the typical link from the BS in tier k is expressed as

$$\begin{aligned} P_{sop,k} &= \mathbb{P}\left(\max_{e \in \phi_{E,k}} \gamma_{E,k} > \theta_{sop}\right) \\ &= 1 - \mathbb{P}\left(\max_{e \in \phi_{E,k}} \gamma_{E,k} < \theta_{sop}\right). \end{aligned} \tag{13}$$

Theorem 2: For an open access K-tier HCN, considering the UE arrival and departure processes, the SOP of the typical user is

$$P_{sop,k} = 1 - \exp\left(\frac{-\lambda_{E,k}}{c_0 \theta_{sop}^{\frac{2}{\alpha}} p_k \lambda_k}\right), \tag{14}$$

where $\lambda_{E,k}$ represents the density of eavesdroppers in tier k and $c_0 = \Gamma(1 + 2/\alpha)\Gamma(1 - 2/\alpha)$.

Proof: Please see Appendix B.

Remark 2: It is found that SOP is not only related with spatial density and transmission power of each BS, but also a decreasing function of UE arrival rate β_u. Therefore, bigger UE arrival rate benefits the security performance in HCNs.

From Remark 1 and Remark 2, it can be concluded that besides the spatial density and transmission power of each BS, UE arrival rate β_u also affects the tradeoff between reliability performance and security performance in K-tier HCNs.

IV. NETWORK-WIDE SECRECY THROUGHPUT MAXIMIZATION

Based on the COP and SOP analysis, we aim to answer the question, i.e., how to allocate the RB among different tiers to achieve the network-wide secrecy throughput optimization. Due to the optimization problem is not in closed form and non-convex, we get the approximate solution through taking the upper and lower bounds of the objective function with gamma function.

A. PROBLEM FORMULATION

Mathematically, combing (1), (4), (9) and (14), the network-wide secrecy throughput can be given as

$$\psi = \sum_{k=1}^{K} \lambda_k p_k W_k \frac{1}{1 + \mathcal{A}_k p_k \mathcal{Z}} \exp\left(\frac{-\lambda_{E,k}}{c_0 \theta_{sop}^{\frac{2}{\alpha}} p_k \lambda_k}\right) R_s. \tag{15}$$

Our goal is to maximize the network-wide secrecy throughput with respect to resource allocation factor $\boldsymbol{\eta}$. However, there are some constraints that need to be considered (i) Reliability and security constraints which are shown as (17). In order to achieve non-zero secrecy throughput, reliability and security requirement must be satisfied. (ii) Fairness constraints which are shown as (18). In order to avoid some tiers are allocated too many RBs than their average RBs demands while some other tiers allocated too few RBs to support their average RBs demands.

$$\mathbf{P1}: \max_{\boldsymbol{\eta}} \psi \tag{16}$$

$$s.t.\ P_{cop,k} \leqslant \delta_p,\ P_{sop,k} \leqslant \delta_s, \tag{17}$$

$$\sum_{k=1}^{K} \eta_k \leqslant 1,\ \frac{\mathcal{A}_k \beta_u}{\lambda_k v} \leqslant W_k,\ \forall k, \tag{18}$$

where δ_p and δ_s are the reliability and security requirement, respectively. $\frac{\mathcal{A}_k \beta_u}{\lambda_k v}$ is the average number of RB demands per tier-k cell, $\frac{\mathcal{A}_k \beta_u}{\lambda_k v}$ should be no greater than W_k. It should be noted that we only consider the scenario where $\sum_{k=1}^{K} \eta_k \leqslant 1$, i.e., the network has enough RBs to support its average RBs demands.

In Section III-A, we already have $\omega_k = \frac{\lambda_k v \eta_k W}{\mathcal{A}_k \beta_u}$, which means there is one-to-one mapping between $\boldsymbol{\eta}$ and $\boldsymbol{\omega} = (\omega_1, \omega_2, \ldots, \omega_K)$. Therefore, we instead investigate the optimization over $\boldsymbol{\omega}$ for analytical convenience. The constraints in (18) are also changed as (21). Accordingly, the optimization $\mathbf{P1}$ can be rewritten as

$$\mathbf{P2}: \max_{\boldsymbol{\omega}} \psi \tag{19}$$

$$s.t.\ P_{cop,k} \leqslant \delta_p,\ P_{sop,k} \leqslant \delta_s, \tag{20}$$

$$\sum_{k=1}^{K} \frac{\omega_k \mathcal{A}_k \beta_u}{\lambda_k v} \leqslant W,\ \omega_k \geqslant 1,\ \forall k. \tag{21}$$

From the above formulas, we find that the optimization problem $\mathbf{P2}$ is not in closed form due to $f(w_k)$, and non-convex which is mathematically intractable. Thus, we want to get the closed form of $f(\omega_k)$ through function scaling, further, we can get some valuable solutions of problem $\mathbf{P2}$.

B. BOUNDING THE OPTIMIZATION PROBLEM

From (9) and (15), we find that ψ is a decreasing function of $f(\omega)$. Thus, we can get the upper and lower bounds of ψ based on the lower and upper bounds of $f(\omega)$, respectively. Observing the expression of $f(\omega)$ in (9), we find that $f(\omega)$ and gamma function are very similar in the form. Therefore, we can remove the non-closed form expression in **P**2 by deriving the closed form lower and upper bounds of $f(\omega)$.

Define $g(y) = \begin{cases} 0 & \text{if } y \leqslant 1 \\ 1-1/y & \text{if } y > 1 \end{cases}$, and $\text{pdf}_Y(y)$ be the PDF of a gamma distributed random variable Y, $Y \sim \Gamma\left(4.5, \frac{1}{3.5w}\right)$. Thus, based on the definition of $f(w)$, we have

$$f(w) = \frac{3.5^{3.5}}{\Gamma(3.5)} \int_1^\infty (1-1/y)\omega^{4.5} y^{3.5} e^{-3.5\omega y} dy = \int_0^\infty g(y)\,\text{pdf}_Y(y)\,dy = \mathbb{E}(g(Y)). \quad (22)$$

In (22), we've established a link between $f(\omega)$ and $\Gamma\left(4.5, \frac{1}{3.5w}\right)$. Further, define $Y_{UB} \sim \Gamma\left(5, \frac{1}{3.5w}\right)$ and $Y_{LB} \sim \Gamma\left(4, \frac{1}{3.5w}\right)$. Based on the properties of gamma distribution, we have $\text{ccdf}_{Y_{UB}}(y) > \text{ccdf}_Y(y) > \text{ccdf}_{Y_{LB}}(y)$ on $[0, \infty)$, where $\text{ccdf}_{Y_{UB}}(y)$, $\text{ccdf}_Y(y)$ and $\text{ccdf}_{Y_{LB}}(y)$ are the complementary cumulative distribution of Y_{UB}, Y and Y_{LB} respectively. In order to utilize this property, we define another function $h(x) = \begin{cases} 0 & \text{if } x \leqslant 1 \\ 1-1/x^2 & \text{if x} > 1 \end{cases}$, thus, we have $g(y) = \int_0^y h(x)\,dx$. Further, we can show that

$$\mathbb{E}(g(Y)) = \int_0^\infty g(y)\text{pdf}_Y(y)\,dy = \int_0^\infty h(x)\text{ccdf}_Y(x)\,dx < \int_0^\infty h(x)\text{ccdf}_{Y_{UB}}(x)\,dx = \mathbb{E}(g(Y_{UB})), \quad (23)$$

where $\mathbb{E}(g(Y_{UB}))$ can be expressed in closed form as

$$\mathbb{E}(g(Y_{UB})) = \frac{3.5^5}{4!}\int_1^\infty (1-1/y)\omega^5 y^4 e^{-3.5\omega y} dy = \frac{3.5^5}{4!} e^{-3.5\omega}\left[\frac{\omega^3}{3.5^2} + \frac{6\omega^2}{3.5^3} + \frac{18\omega}{3.5^4} + \frac{24}{3.5^5}\right]. \quad (24)$$

Similarly, we can prove $\mathbb{E}(g(Y)) > \mathbb{E}(g(Y_{LB}))$, which is omitted here. $\mathbb{E}(g(Y_{LB}))$ is given by

$$\mathbb{E}(g(Y_{LB})) = \frac{3.5^4}{3!} e^{-3.5\omega}\left[\frac{\omega^2}{3.5^2} + \frac{4\omega}{3.5^3} + \frac{6}{3.5^4}\right]. \quad (25)$$

Finally, we have the lower and upper bounds of $f(w)$

$$f_{LB}(\omega) = \frac{3.5^4}{3!} e^{-3.5\omega}\left[\frac{\omega^2}{3.5^2} + \frac{4\omega}{3.5^3} + \frac{6}{3.5^4}\right]$$
$$f_{UB}(\omega) = \frac{3.5^5}{4!} e^{-3.5\omega}\left[\frac{\omega^3}{3.5^2} + \frac{6\omega^2}{3.5^3} + \frac{18\omega}{3.5^4} + \frac{24}{3.5^5}\right], \quad (26)$$

and we also have $f_{LB}(w) < f(w) < f_{UB}(w)$.

Since ψ is a decreasing function of $f(\omega)$, we can get the upper (ψ_{UB}) and lower bounds (ψ_{LB}) of ψ based on the lower and upper bounds of $f(\omega)$, respectively. Therefore, instead of solving problem **P**2, we transform the optimization problem **P**2 into two upper and lower bounds optimization problems **P**3 and **P**4, which is given as

$$\begin{aligned} \mathbf{P}3: &\max_{\boldsymbol{\omega}} \psi_{UB} \quad s.t.\ (20)\text{ and }(21) \\ \mathbf{P}4: &\max_{\boldsymbol{\omega}} \psi_{LB} \quad s.t.\ (20)\text{ and }(21) \end{aligned} \quad (27)$$

Then, we try to prove that there exits an unique $\boldsymbol{\omega}$ to achieve ψ_{UB} (ψ_{LB}) maximization. Combining f_{LB} in (26) and (15), we have

$$\psi_{k,LB} = \frac{Aw[1-f_{LB}(w)]}{B - Bf_{LB}(w) + w} \exp\left(\frac{-Cw}{1-f_{LB}(w)}\right), \quad (28)$$

where $A = \frac{\mathcal{A}_k \beta_u R_s}{v}$, $B = \mathcal{A}_k \mathcal{Z}$ and $C = \lambda_{E,k} / \left(c_0 \theta_{sop}^{\frac{2}{\alpha}} \lambda_k\right)$.

We first calculate the first-order derivative of $\psi_{k,LB}$ with respect to w, which is given as (29) at the bottom of next page. Define $q(w) = \frac{\partial \psi_{k,LB}}{\partial w}$. Since $f_{LB}(1) = 0.1623$, $\lim_{w\to\infty} f_{LB}(w) = 0$ and $f'_{LB}(w) < 0$, we find that $q(1) > 0$ and $\lim_{w\to\infty} q(w) < 0$. Further, by calculating the first-order derivative of $q(w)$, we numerically find that $\frac{\partial q(w)}{\partial (w)}$ is always negative when $w \in [1, \infty)$. Therefore, there exits an unique w to achieve ψ_{LB} maximization. The optimal w can be obtain by a bisection method that converges to a solution with a certain error tolerance ε_w with computation complexity $\mathcal{O}\left(\log_2 \frac{w_{\max}}{w}\right)$ [32], where $w_{\max}$ can be got from the constraint in (18). Similar property can be obtained on $\psi_{k,UB}$ in the same way, which is omitted here.

V. NUMERICAL RESULTS

In this section, we consider a 2-tier dynamic HCN with different parameters for each tier, which are listed in Table I. We first show the effects of the UE arrival rate β_u on the optimal network-wide secrecy throughput and the optimal resource allocation factors of tier 1 and tier 2, respectively. Then, we show how the spatial intensity and transmission power affect the optimal network-wide secrecy throughput and the optimal resource allocation factors. Finally, we present the impacts of the eavesdroppers intensity on the optimal network-wide secrecy throughput. The Monte Carlo area is a square of $[0, 1000]\,\text{m} \times [0, 1000]\,\text{m}$.

A. EFFECTS CAUSED BY UE ARRIVAL RATE ON THE OPTIMAL NETWORK-WIDE SECRECY THROUGHPUT AND OPTIMAL RESOURCE ALLOCATION FACTORS

UE arrival rate β_u is a key element in our dynamic HCNs, thus, we first illustrate the optimal network-wide secrecy throughput and optimal resource allocation factors under different β_u.

We depict the impacts of β_u on the optimal network-wide secrecy throughput in Fig. 2, in which λ_E is fixed at $\frac{1}{\pi 500^2}\text{nodes/m}^2$. As can be observed from the figure, there

TABLE 1. Simulation parameters.

Notation	Description	Simulation Value
P_k	Transmission power of the BS in tier k (W)	$P_1 = 2,\ P_2 = 20,$
λ_k	Density of the BS in the tier k (units/m^2)	$\lambda_1 = \frac{1}{\pi 500^2},\ \lambda_2 = \frac{5}{\pi 500^2}$
N	Number of Monte Carlo simulations	$N = 10^6$
W	The number of RBs	$W = 1000$
α	Path loss exponent	$\alpha = 4$
R_t	Codeword transmission rate	2bits/sec/Hz
R_m	Confidential information rate	1bits/sec/Hz
δ_p	COP constraint of HCNs	0.1
δ_s	SOP constraint of HCNs	0.1

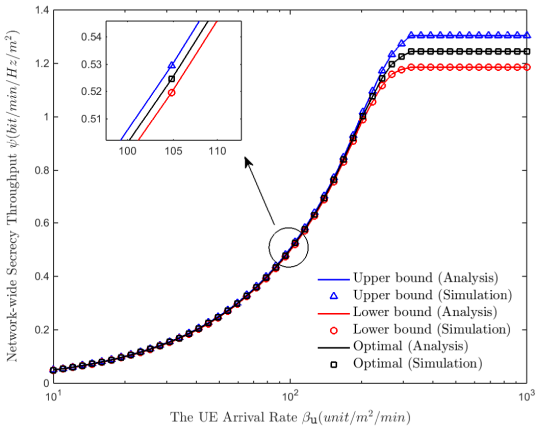


FIGURE 2. Optimal Network-wide secrecy throughput versus UE arrival rate β_u.

is nearly no gap between the analytical results and corresponding simulation results. We also find that the bounding approximations provide nearly optimal throughput for a wide range of UE arrival rate. This proves the accuracy of our analytical results. Furthermore, the optimal network-wide secrecy throughput first increases and then remains unchanged with the increase of UE arrival rate. This is because as the UE arrival rate increases, there will be more UE in the network. However, as the UE arrival rate increases further, the network cannot provide service to that part of UE, thus, the optimal network-wide secrecy throughput keeps unchanged.

The optimal resource allocation factors of tier 1 and tier 2 over different β_u is shown in Fig. 3, in which λ_E is fixed at $\frac{1}{\pi 500^2}$nodes/m^2. It is obvious that the optimal resource allocation factors first increase and then remains unchanged with the increase of UE arrival rate. Two reasons arise in

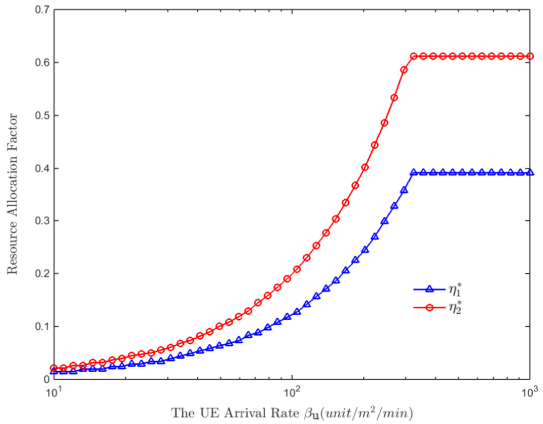


FIGURE 3. Optimal resource allocation factors versus UE arrival rate β_u.

this situation (i) When the user arrives at a relatively low rate, resource allocation factors are mainly influenced by the UE arrival rate. More UEs need more resource. (ii) When the UE arrives at a relatively high rate, resource allocation factors are mainly influenced by spatial intensity and transmission power of BSs in different tiers instead of UE arrival rate. From (i) and (ii), we can say that UE arrival rate is a key factor influencing the optimal resource allocation factors when the RB requirements of each UE are satisfied. When the network is overloaded, spatial intensity and transmission power of each BS are the main elements affecting resource allocation.

B. EFFECTS CAUSED BY THE INTENSITY OF BS IN TIER 2 ON THE OPTIMAL NETWORK-WIDE SECRECY THROUGHPUT AND OPTIMAL RESOURCE ALLOCATION FACTORS

We illustrate the impacts of BS intensity in tier 2 λ_2 on the optimal network-wide secrecy throughput in Fig. 4. As can be observed from the figure, the analytical results agree with simulation results. We also find that the bounding approximations provide nearly optimal throughput for a wide range of BS intensity in tier 2. This all proves the accuracy of our analytical results once again. Furthermore, the optimal network-wide secrecy throughput keeps increasing, but the increase rate slows down, with the increase of BS intensity in tier 2. This is because as the BS intensity of tier 2 increases, more UEs will connect the BS in tier 2, the network-wide secrecy throughput of tier 2 is increasing. However, the network-wide secrecy throughput of tier 1 decreases. All above two reasons lead to this situation.

$$\frac{\partial \psi_{k,LB}}{\partial w} = \frac{\left[A(1-f_{LB}(w))^2 - Awf'_{LB}(w)(1-f_{LB}(w)) + Aw\left[-(1-f_{LB}(w))\right]C + Cwf'_{LB}(w)\right]}{B+x-Bf_{LB}(w)} \exp\left(-\frac{Cw}{1-f_{LB}(w)}\right) - \frac{Aw(1-f_{LB}(w))^2\left(1-Bf'_{LB}(w)\right)}{(B+w-Bf_{LB}(w))^2}. \quad (29)$$

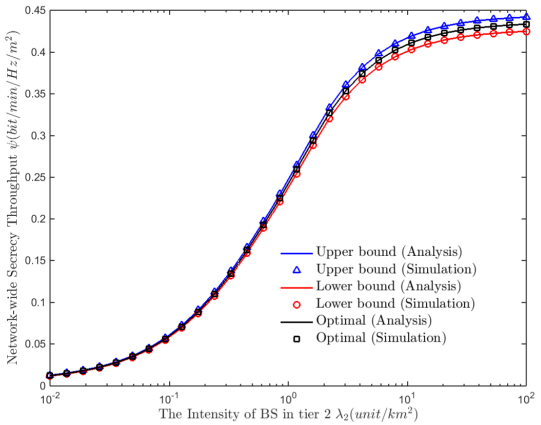


FIGURE 4. Optimal Network-wide secrecy throughput versus λ_2.

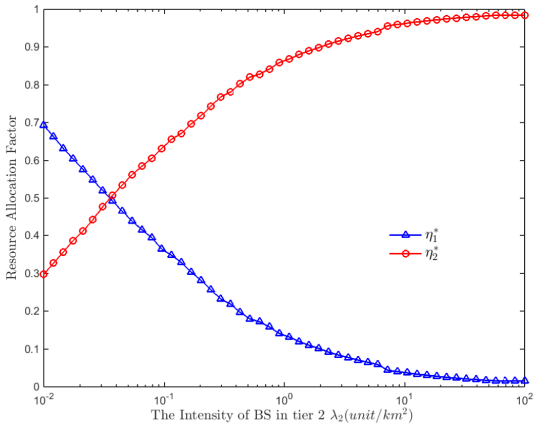


FIGURE 5. Optimal resource allocation factors versus λ_2.

The optimal resource allocation factors of tier 1 and tier 2 over different λ_2 is shown in Fig. 5. It is obvious that the optimal resource allocation factor of tier 2 increases with the increase of λ_2, while the optimal resource allocation factor of tier 1 decreases with the increase of λ_2. This is because with the increasing of λ_2, $\mathcal{A}_2$ is larger than before, which means the probability of a typical UE connecting the BS in tier 2 is increasing. Therefore, more resource should be allocated to tier 2.

C. EFFECTS CAUSED BY THE TRANSMISSION POWER OF BS IN TIER 2 ON THE OPTIMAL NETWORK-WIDE SECRECY THROUGHPUT AND OPTIMAL RESOURCE ALLOCATION FACTORS

We show the impacts of BS transmission power in tier 2 P_2 on the optimal network-wide secrecy throughput in Fig. 6. As can be observed from the figure, the optimal network-wide secrecy throughput first increases and then decreases with the increase of P_2. This is because as P_2 increases, more UEs will connect the BS in tier 2, the changes of

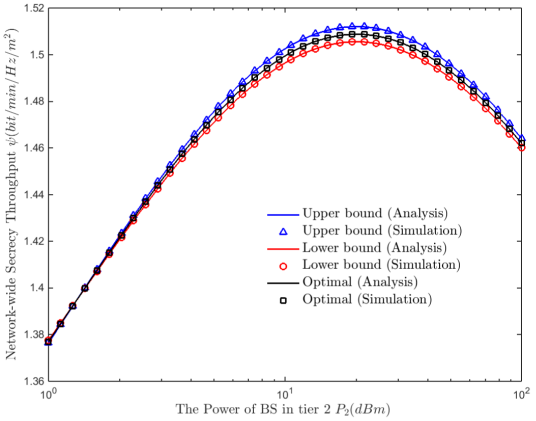


FIGURE 6. Optimal Network-wide secrecy throughput versus P_2.

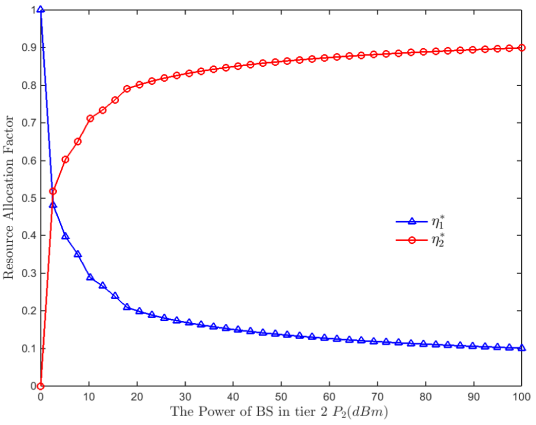


FIGURE 7. Optimal resource allocation factors versus P_2.

network-wide secrecy throughput in tier 2 dominate the overall security network-wide secrecy throughput. The reliability performance of tier 2 is increasing with the increase of P_2 while the security performance of tier 2 is decreasing with the increase of P_2. All above two reasons lead to this situation.

The optimal resource allocation factors of tier 1 and tier 2 over different P_2 are shown in Fig. 7. It is obvious that the optimal resource allocation factors of tier 2 increases with the increase of P_2, while the optimal resource allocation factors of tier 1 decreases with the increase of P_2. Since the reasons are similarly with Fig. 5, which is omitted here.

D. EFFECTS CAUSED BY THE INTENSITY OF EAVESDROPPERS ON THE OPTIMAL NETWORK-WIDE SECRECY THROUGHPUT

We illustrate the impacts of eavesdroppers intensity λ_E on the optimal network-wide secrecy throughput in Fig. 8. As can be observed from the figure, the optimal network-wide secrecy throughput decreases with the increase of λ_E, which is consistent with the actual situation. This is because as λ_E increases, the security performance decreases while the reliability performance keeps unchanged. Therefore, the overall performance decreases with the increase of λ_E.

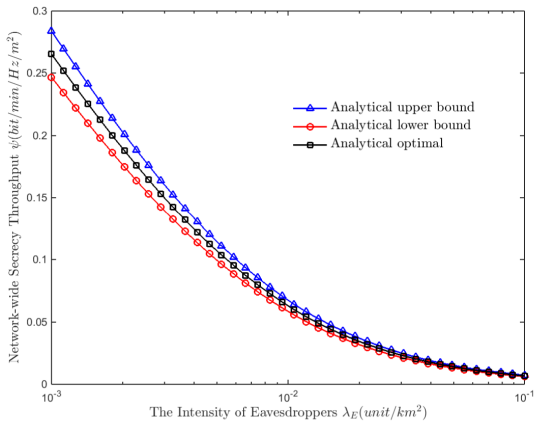


FIGURE 8. Optimal Network-wide secrecy throughput versus λ_E.

VI. CONCLUSION

In this paper, a novel secure-optimized resource allocation policy is proposed in K-tier random and dynamic HCNs, in which the randomness of base stations in spatial dimension and user equipment (UE) arrival and departure processes in temporal dimension are jointly considered. By exploiting queueing theory and stochastic geometry, the reliability performance and security performance are characterized by COP and SOP, respectively. Furthermore, the network-wide secrecy throughput is given based on the outage analysis. Finally, the optimal resource allocation factors of different tiers are derived by bounding the optimization problem. Different from previous works, our analysis highlighted apart from the spatial intensity and transmission power of each BS, UE arrival and departure processes are also key elements influencing the resource allocation factors of different tiers.

As the first step of studying resource allocation for secure communication in K-tier HCNs from a spatial-temporal perspective, this paper considered a fundamental scenario and thus has left several potential future work directions. For instance, the inelastic traffic is considered when we solve the problem of resource allocation for secure communication in HCNs. As such, one direction of future work is to conduct a thorough investigation on the secure resource allocation jointly considering the inelastic traffic and elastic traffic. Future research can also seek to more advanced system models, e.g., MIMO, general fading channels, and point processes that capture the characteristics of random networks with more accuracy. In addition, an extension from the scenario considered in this work to a more practical scenario in the real-word, where different users may occupy different units spectrum bandwidth, would be of practical interests.

APPENDIX A
PROOF OF THEOREM 1

We first calculate $\mathbb{P}\left(\gamma_{u,k}(x) > \theta_{cop}\right)$, rewritten $\gamma_{u,k}(x)$ as $\gamma_{u,k}(x) = \frac{g_{u,k}}{x^\alpha P_k^{-1} Q}$, where $Q = I_k$, and $I_k = P_k h_{j,k} |Y_{j,k}|^{-\alpha}$.

$$\begin{aligned}\mathbb{P}\left(\gamma_{u,k}(x) > \theta_{sus}\right) &= \mathbb{P}\left(g_{u,k} > x^\alpha P_k^{-1}\theta_{cop} Q\right)\\ &= \int_0^\infty \exp\left(-x^\alpha P_k^{-1}\theta_{cop} q\right) f_Q(q)\, dq\\ &= \mathcal{L}_{I_k}\left(x^\alpha P_k^{-1}\theta_{cop}\right), \end{aligned} \tag{30}$$

where

$$\begin{aligned}\mathcal{L}_{I_k}\left(x^\alpha P_k^{-1}\theta_{sus}\right) &\overset{a}{=} \exp\left(-2\pi p_k \lambda_k \int_d^\infty \frac{y}{1+\left(x^\alpha \theta_{cop}\right)^{-1} y^\alpha} dy\right)\\ &= \exp\left(-\pi p_k \lambda_k \theta_{cop}^{2/\alpha} x^2 \int_{\theta_{\theta_{cop}}^{2/\alpha}}^\infty \frac{1}{1+t^{\alpha/2}} dt\right), \end{aligned} \tag{31}$$

where a is supported by [33], $d = x$ represents the closest distance between the interfering BS and the typical UE.

Based on the [26, Lemma 3], we note that the PDF of distance X_k between a typical UE and its servicing BS is

$$f_{X_k(x)} = \frac{2\pi\lambda_k x}{\mathcal{A}_k} \exp\left(-\frac{\pi\lambda_k x^2}{\mathcal{A}_k}\right), \tag{32}$$

where $\mathcal{A}_k = \lambda_k / \left(\sum_{j=1}^K \lambda_j \left(\frac{P_j}{P_k}\right)^{2/\alpha}\right)$ is the probability that a typical user connects the BS in tier k, which can be got from [26, Lemma 1].

Mathematically, combing (30), (31) and (32), (3) can be further expressed as

$$\begin{aligned}P_{cop,k} &= 1 - \int_0^\infty \mathbb{P}\left(\gamma_{u,k}(x) > \theta_{cop}\right) f_{X_k(x)} dx\\ &= 1 - \int_0^\infty \mathcal{L}_{I_k}\left(x^\alpha P_k^{-1}\theta_{cop}\right) \frac{2\pi\lambda_k x}{\mathcal{A}_k} \exp\left(-\frac{\pi\lambda_k x^2}{\mathcal{A}_k}\right) dx\\ &= 1 - \frac{1}{1+\mathcal{A}_k p_k \mathcal{Z}}, \end{aligned} \tag{33}$$

where

$$\mathcal{Z} = \frac{2\theta_{cop}}{\alpha - 2} {}_2F_1\left[1, 1-\frac{2}{\alpha};\ 2-\frac{2}{\alpha};\ -\theta_{cop}\right] \tag{34}$$

and ${}_2F_1[\cdot]$ denotes the Gauss hypergeometric function.

APPENDIX B
PROOF OF THEOREM 2

The $P_{sop,k}$ in (13) can be further expressed as

$$P_{sop,k} = 1 - \mathbb{E}_{\phi_k}\mathbb{E}_{\phi_{E,k}}\left\{\prod_{e\in\phi_{E,k}} \mathbb{P}\left(\gamma_{E,k} < \theta_{sop} | \phi_{E,k}, \phi_k\right)\right\}, \tag{35}$$

where $\phi_{E,k}$ represents the location of eavesdroppers in tier k, and $\phi_E = \phi_{E,1} \cup \phi_{E,2} \cup \ldots \cup \phi_{E,K}$.

Using the generating function of the PPP ϕ_E in [35], (35) can be further expressed as

$$P_{sop,k} = 1 - \mathbb{E}_{\phi_k}\left\{-\lambda_{E,k} \int_{R^2} \mathbb{P}\left(\gamma_{E,k} > \theta_{sop} | \phi_k\right) de\right\}, \tag{36}$$

where $\lambda_{E,k}$ represents the density of eavesdroppers in tier k, and we have $\lambda_E = \sum_{k=1}^K \lambda_{E,k}$.

Applying the Jensen's inequality, an upper bound of $P_{sop,k}$ is given by

$$P_{sop,k} = 1 - \exp\left\{-\lambda_{E,k}\int_{R^2}\mathbb{P}\left(\gamma_{E,k} > \theta_{sop}|\phi_k\right)de\right\}. \quad (37)$$

We first calculate $\mathbb{P}\left(\gamma_{E,k} > \theta_{sop}|\phi_k\right)$,

$$\begin{aligned}\mathbb{P}\left(\gamma_{E,k} > \theta_{sop}|\phi_k\right) &= \mathbb{P}\left(\frac{P_k g_{E,k} x^{-\alpha}}{\sum_{j\in\phi_k'} P_k h_{j,k}|Y_{j,k}|^{-\alpha}} > \theta_{sop}|\phi_k\right)\\ &= \exp\left[-\pi c_0 \theta_{sop}^{\frac{2}{\alpha}} r_e^2 p_k \lambda_k\right], \end{aligned} \quad (38)$$

where r_e denotes the distance between the BS in tier k and eavesdropper e. Therefore, $P_{sop,k}$ can be further expressed as

$$P_{sop,k} = 1 - \exp\left[-2\pi\lambda_{E,k}\int_0^{\infty}\exp\left[-c_0\pi\theta_{sop}^{\frac{2}{\alpha}} p_k\lambda_k r_e^2\right] r_e dr_e\right]. \quad (39)$$

Then, by directly evaluating the integral in (39), an upper bound of $P_{sop,k}$ is obtained as

$$P_{sop,k} = 1 - \exp\left(\frac{-\lambda_{E,k}}{c_0\theta_{sop}^{\frac{2}{\alpha}} p_k\lambda_k}\right), \quad (40)$$

where $c_0 = \Gamma(1+2/\alpha)\Gamma(1-2/\alpha)$, $\Gamma(\cdot)$ denotes gamma function.

REFERENCES

[1] Y. Zhong, T. Q. S. Quek, and X. Ge, "Heterogeneous cellular networks with spatio-temporal traffic: Delay analysis and scheduling," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1373–1386, Jun. 2017.

[2] 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.

[3] D. Zhang, Y. Liu, Z. Ding, Z. Zhou, A. Nallanathan, and T. Sato, "Performance analysis of non-regenerative massive-MIMO-NOMA relay systems for 5G," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4777–4790, Nov. 2017.

[4] V. W. S. Wong, R. Schober, D. Wing, K. Ng, and L.-C. Wang, Eds., *Key Technologies for 5G Wireless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[5] H. Wang and T. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer, 2016.

[6] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

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

[8] 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.

[9] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706–2722, Oct. 2016.

[10] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.

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

[12] L. Li, A. P. Petropulu, Z. Chen, and J. Fang, "Improving wireless physical layer security via exploiting co-channel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1433–1448, Dec. 2016.

[13] Y. Zou. (2017). "Intelligent interference exploitation for heterogeneous cellular networks against eavesdropping." [Online]. Available: https://arxiv.org/abs/1710.10587

[14] D. Zhang, Z. Zhou, S. Mumtaz, J. Rodriguez, and T. Sato, "One integrated energy efficiency proposal for 5G IoT communications," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1346–1354, Dec. 2016.

[15] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[16] Y. Wang, C. Li, Y. Huang, D. Wang, T. Ban, and L. Yang, "Energy-efficient optimization for downlink massive MIMO FDD systems with transmit-side channel correlation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7228–7243, Sep. 2016.

[17] Q. Song, X. Wang, T. Qiu, and Z. Ning, "An interference coordination-based distributed resource allocation scheme in heterogeneous cellular networks," *IEEE Access*, vol. 5, pp. 2152–2162, Mar. 2017.

[18] G. Shiqi, X. Chengwen, F. Zesong, and K. Jingming, "Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper," *China Commun.*, vol. 13, no. 3, pp. 82–95, Mar. 2016.

[19] S. Sheikhzadeh, M. R. Javan, and N. Mokari, "Radio resource allocation for physical-layer security in OFDMA based HetNets with unknown mode of adversary," in *Proc. IWICT*, Tehran, Iran, May 2017, pp. 1–6.

[20] K. Zhang, M. Peng, P. Zhang, and X. Li, "Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1822–1834, Feb. 2017.

[21] B. Blaszczyszyn, M. Jovanovic, and M. K. Karray, "Quality of real-time streaming in wireless cellular networks—Stochastic modeling and analysis," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3124–3136, Jun. 2014.

[22] V. Joseph, S. Borst, and M. I. Reiman, "Optimal rate allocation for adaptive wireless video streaming in networks with user dynamics," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 406–414.

[23] M. Gharbieh, H. ElSawy, A. Bader, and M.-S. Alouini, "Spatiotemporal stochastic modeling of iot enabled cellular networks: Scalability and stability analysis," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3585–3600, Aug. 2017.

[24] G. Zhang, T. Q. S. Quek, A. Huang, and H. Shan, "Delay and reliability tradeoffs in heterogeneous cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1101–1113, Feb. 2016.

[25] W. Bao and B. Liang, "Radio resource allocation in heterogeneous wireless networks: A spatial-temporal perspective," in *Proc. IEEE INFOCOM*, Apr./May 2015, pp. 334–342.

[26] R. W. Heath, Jr., M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using poisson point processes," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 4114–4126, Aug. 2013.

[27] W. C. Cheung, T. Q. S. Quek, and M. Kountouris, "Throughput optimization, spectrum allocation, and access control in two-tier femtocell networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 561–574, Apr. 2012.

[28] W. Bao and B. Liang, "Insensitivity of user distribution in multicell networks under general mobility and session patterns," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6244–6254, Dec. 2013.

[29] Y. Cai, X. Xu, and W. Yang, "Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise," *IET Commun.*, vol. 10, no. 15, pp. 1904–1913, Aug. 2016.

[30] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

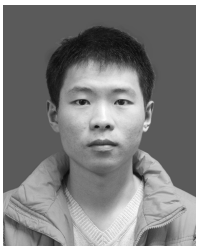
[31] S. Singh, H. S. Dhillon, and J. G. Andrews, "Offloading in heterogeneous networks: Modeling, analysis, and design insights," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2484–2497, May 2013.

[32] G. R. Wood, "The bisection method in higher dimensions," *Math. Program.*, vol. 55, nos. 1–3, pp. 319–337, Jan. 1992.

[33] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.

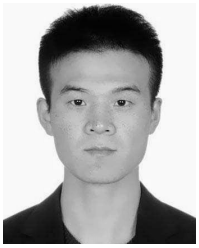
[34] H.-S. Jo, Y. J. Sang, P. Xia, and J. G. Andrews, "Heterogeneous cellular networks with flexible cell association: A comprehensive downlink SINR analysis," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3484–3495, Oct. 2012.

[35] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.



BING WANG received the B.E. degree in communication engineering from the Wuhan University of Technology, Wuhan, China, in 2015. He is currently pursuing the B.S. degree with the National Digital Switching System Engineering and Technological Research Center, Zhengzhou. His research interests include wireless communication, physical layer security, and stochastic geometry.

KAIZHI HUANG received the Ph.D. degree in communication and information system from Tsinghua University, Beijing, China. She is currently a Professor and a Doctoral Supervisor of the National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China. Her research interests include wireless mobile communication network and physical-layer security.



XIAOMING XU received the Ph.D. degree in communications and information system from the PLA University of Science and Technology, Nanjing, China, in 2017. His research interests include the stochastic geometry, cooperative communications, and physical-layer security of wireless communications.

LIANG JIN received the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China, in 1999. He is currently a Professor with the China National Digital Switching System Engineering and Technological Research Center. His research interests include ultra wideband wireless communication and smart antenna.

ZHOU ZHONG has been a Faculty Member of the China National Digital Switching System Engineering and Technological Research Center. His research interests include physical-layer security.

YI WANG received the B.S. degree from PLA Information Engineering University, Zhengzhou, China, in 2006, and the M.S. and Ph.D. degrees from the School of Information Science and Engineering, Southeast University, China, in 2009 and 2016, respectively. Since 2016, he has been with the School of Electronics and Communication Engineering, Zhengzhou University of Aeronautics, China. His current research interests include signal processing, energy-efficient communication, relay-aided system, and massive MIMO. He received the Best Paper Awards of IEEE WCSP in 2015.