Secrecy Spectrum and Energy Efficiency Analysis in Massive MIMO-Enabled Multi-Tier Hybrid HetNets

Anum Umer, Syed Ali Hassan, *Senior Member, IEEE*, Haris Pervaiz, *Member, IEEE*, Leila Musavian, Qiang Ni, *Senior Member, IEEE*, and Muhammad Ali Imran, *Senior Member, IEEE*

***Abstract*—Massive multiple antenna systems in conjunction with millimeter (mmWave) communication have gained tremendous attention in the recent years owing to their high speed data delivery. However, security in these networks has been overlooked; thereby necessitating a comprehensive study. This paper analyzes the physical layer security performance of the downlink of a massive multiple-input multiple-output (MIMO)-based hybrid heterogeneous network (HetNet) where both mmWave and sub-6 GHz small cells coexist. Specifically, a tractable approach using stochastic geometry is proposed to analyze the secrecy outage probability, secrecy energy efficiency (SEE) and secrecy spectrum efficiency (SSE) of the hybrid HetNets. Our study further characterizes the impact of large antenna arrays, directional beamforming gains, transmit power, and cell density on the above mentioned secrecy performance measures. The results show that at low transmit power operation, the secrecy performance enhances for higher small cell density. It has also been observed that the higher directivity gains at mmWave cells lead to a drop in secrecy performance of the network; thus a tradeoff exists between better coverage or secrecy.**

***Index Terms*—Heterogeneous networks, millimeter wave, sub-6 GHz bands, massive MIMO, stochastic geometry, secrecy outage, secrecy energy efficiency, secrecy spectrum efficiency.**

I. Introduction

OWING to the widespread usage of intelligent devices and exponential growth in wireless data traffic, the conventional sub-6 GHz communication ways are almost saturated and are incapable of meeting the increase in traffic demands. New access technologies under the umbrella of fifth generation (5G) communications are gearing up in both academia as well as industry. The key enablers for 5G networks at the physical layer include heterogeneous cellular networks (HetNets) with massive multiple-input multiple-output (MIMO) technology and millimeter wave (mmWave) communication at 10 to 300 GHz radio frequency bands with bandwidths as high as 2 GHz [2]–[4]. The HetNets create a layer of overlay deployment of small cells of low-powered base stations (BS), variable communication ranges, and operating frequencies on the existing sub-6 GHz macro cells thus providing enhanced coverage and throughput to the end users by bringing network closer to them [5].

Massive MIMO technologies produce highly directional beam gains and enhanced radio spectral efficiency in HetNets by deploying large-scale antenna arrays at the transmitting nodes. On the other hand, mmWave communication, takes place at a smaller wavelength than the conventional microwave networks, provides higher spectral efficiency while being sensitive to blockages and certain materials such as concrete cause severe propagation losses and thereby higher path loss which limits the coverage size of mmWave cells. Because of the mmWave small wavelength, a large number of antennas can be deployed in a small area. Using these directional antenna arrays, beamforming can be implemented at mmWave BSs to compensate for path loss since measurements show significant differences in line-of-sight (LoS) and non-line-of-sight (NLoS) path loss properties [4], [6]. Beamforming gains also tend to overcome the additional noise power and out-of-cell interference in mmWave communication [7].

While talking about 5G communications, the main focus is on maximizing the coverage probability and achievable rate at the end user. However, the idea of end user's information integrity and secrecy is equally important and it presents the gap in recent studies, which is investigated in this study. Physical layer security (PLS) can be a less complex solution for the protection of confidential information in complex wireless networks [8]. Particularly, PLS in massive MIMO-enabled hybrid HetNets with mmWave small cells is important since the aforementioned networks present the most common deployment scenario for the future 5G communication networks. This paper analyses the PLS in massive MIMO-enabled hybrid HetNets by digging into unique advantageous properties of massive MIMO and mmWave channel.

A. Related Works and Motivation

Major research developments have been made recently in the area of PLS for wireless networks where the secrecy

Manuscript received November 24, 2018; revised May 6, 2019 and October 1, 2019; accepted November 11, 2019. Date of publication November 27, 2019; date of current version March 18, 2020. This work was supported by the DARE Project through EPSRCs Global Challenges Research Fund Allocation under Grant EP/P028764/1 and European Union Horizon 2020, and in part by the RISE 2018 Scheme (H2020-MSCA-RISE-2018) through the Marie Skłodowska-Curie grant under Agreement 823903 (RECENT). The associate editor coordinating the review of this article and approving it for publication was M. Ismail. *(Corresponding author: Syed Ali Hassan.)*

A. Umer and S. A. Hassan are with the School of Electrical Engineering and Computer Science, National University of Sciences and Technology, Islamabad 46000, Pakistan (e-mail: aumer.msee15seecs@seecs.edu.pk; ali.hassan@seecs.edu.pk).

H. Pervaiz and Q. Ni are with the School of Computing and Communications, Lancaster University, Lancaster LA1 4YW, U.K. (e-mail: h.b.pervaiz@lancaster.ac.uk; q.ni@lancaster.ac.uk).

L. Musavian is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, U.K. (e-mail: leila.musavian@essex.ac.uk).

M. A. Imran is with the School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K. (e-mail: muhammad.imran@glasgow.ac.uk).

Digital Object Identifier 10.1109/TGCN.2019.2956433

outage probability and secrecy rate are the important tools of investigation. The effects of fading on secrecy outage probability, which is the probability that the confidentiality of information sent to legitimate receiver has been compromised, is studied in [9], [10]. Techniques such as cooperative jamming, Wyner codes, beamforming, and artificial noise can improve the secrecy by degrading eavesdropper's channel as investigated in [8], [12]. Spectrum allocation and transmit beamforming are designed for a two-tier HetNet to improve secrecy rate in [13]. The stochastic modeling of secrecy outage probability and network throughput of a HetNet is studied in [14]. An access threshold-based secrecy mobile association policy for a K-tier HetNet is proposed in [15]. The authors in [16] studied secure transmission based on coordinated multipoint scheme in HetNets. The secrecy rate and energy efficiency in massive MIMO-based heterogeneous centralized radio access network (C-RAN) is analyzed in [17] where it is shown that the centralized and distributed large-scale antenna systems collectively contribute to improved secrecy. Authors investigate the artificial noise aided physical layer security in massive MIMO multiple access channels where legitimate users and eavesdoppers have large antenna arrays and derive use insights [40].

All of the aforementioned literature focuses on PLS analysis of HetNets based on conventional sub-6 GHz low frequency tiers. Since the propagation properties of mmWave communication are different from sub-6 GHz channels, traditional studies and results in PLS do not necessarily apply to mmWave communication systems. For instance, secrecy behavior of a point-to-point mmWave link is studied in [18], which shows that mmWave has an enhanced secrecy in contrast to sub-6 GHz conventional systems. The large available bandwidth at mmWave frequencies and large-scale antenna arrays providing high directivity gain can pave the way for high speed secure links achievable [18]. In [19], the authors have investigated the impact of blockages on the secrecy rate in a network with both mmWave and sub-6 GHz BSs in the presence of eavesdroppers. Secrecy outage probability for mmWave network is analyzed when the users and eavesdropping nodes are single antenna omnidirectional transceivers in [20]. In [21], mmWave secrecy beamforming schemes are proposed to maximize the secrecy sum rate in two-way amplify-and-forward MIMO relaying networks. Physical layer security in large-scale mmWave ad hoc networks is analyzed in [22] where it is assumed that the eavesdroppers are randomly located and can intercept the confidential information if they reside in a single beam. We would like to highlight that the aforementioned work in the recent literature solely focuses on the secrecy outage analysis of mmWave cellular networks only or mmWave overlaid sub-6 GHz networks. According to the best of our knowledge, there is no analytical work in the literature which investigates the secrecy spectrum efficiency (SSE) and secrecy energy efficiency (SEE) for massive MIMO-enabled hybrid HetNets incorporating both sub-6 GHz and mmWave small cells in the presence of eavesdroppers.

B. Approach and Contributions

This paper studies the PLS in proposed three tier hybrid HetNet with massive MIMO in macro tier and sub-6 GHz and mmWave frequency small cells. We propose a tractable approach for SSE and SEE analysis that accounts for the key features of massive MIMO technology, mmWave channel, number of transmitting antennas, beamforming gains and node densities. The main contributions and insights are listed as follows.

- We model the proposed downlink of a three tier hybrid HetNet with massive MIMO-enabled macro tier incorporating sub-6 GHz and mmWave frequency small cells with the aid of stochastic geometry, which characterizes the random spatial distributions of transmitting BSs, legitimate users and eavesdroppers. The secrecy outage probability for each of three tiers is derived to quantify the effects of important system parameters. Our results show that at high antenna gains, secrecy outage of the network increases and a tradeoff exists between enhanced coverage or secrecy performance. With increased number of antennas at massive MIMO-enabled Macro BSs (MBSs), secrecy performance of the network decreases.
- We develop an analytical tractable framework for the evaluation of average achievable ergodic rate for each of three tiers and eavesdroppers to determine average achievable secrecy rate of the network. Based on average achievable secrecy rate, the secrecy oriented spectrum and energy efficiency performance of the massive MIMO-enabled three tier hybrid HetNet is derived. Our results demonstrate that increasing the number of antennas at MBSs results in a drop in SSE and SEE of the network. By increasing the transmit power of small cell BSs, SSE and SEE of the network improve.

II. System Model

In this work, we consider the time-division duplex (TDD)-based downlink transmission scheme in a hybrid HetNet where spatially distributed access points (or BSs) transmit the information to the legitimate users in the presence of multiple malicious eavesdroppers. The macro cells operating at sub-6 GHz constitute tier 1, whereas small cells operating at sub-6 GHz and small cells operating at mmWave band constitute tier 2 and 3, respectively. It is assumed that the location of BSs follow a two dimensional homogeneous Poisson point process (HPPP) with intensity Φ_k and density λ_k where $k \in \{1, 2, 3\}$. Similarly, the location of legitimate users and eavesdroppers are modeled as HPPP with intensity Φ_u and its density λ_u and Φ_e with density λ_e, respectively. It is assumed that the MBSs are provided with multiple antennas forming an array while the small cell BSs, legitimate users and eavesdroppers are equipped with a single omni-directional antenna. Massive MIMO is adopted at the macro cells such that each MBS has N antennas that can communicate simultaneously with U users ($N \gg U \geq 1$) with equal power distribution among all users [23].

In this work, we assume perfect synchronization and downlink channel state information (CSI) is known at the MBS and focus on zero-forcing precoding. Because in the practical TDD massive MIMO systems, the downlink CSI can be obtained through channel reciprocity based on uplink training. The main focus of this work is to carry out the detailed performance analysis of massive MIMO-enabled three-tier hybrid heterogeneous networks for the perfectly estimated CSI case. The imperfect CSI or outdated CSI can adversely affect the system performance [24]–[25] and its impact on the performance analysis is not main scope of this work. It is assumed that each MBS uses linear zero forcing beamforming (ZFBF) to transmit *U* data streams with equal power assignment [26]. In the k^{th} tier, each BS has the total transmit power P_k and path loss exponent α_k. In accordance with Slivnyak's Theorem, the analysis of the network is performed for a typical user located at the origin and an open access scheme is assumed where the user can connect to any tier BS based on the maximum average received power.

A. Received Signal Power Model

1) mmWave Network: In mmWave networks, since mmWave signals are transmitted with narrow beamwidths, therefore, the effects of multipath fading is not that severe as the delay spread of the channel is small. It is also clearly outlined in [2, 5] that the small-scale fading can be ignored in the analysis carried out for the mmWave network. For an analytical tractability, in this work the Nakagami fading model is considered. Using the Nakagami fading model, the envelope of the fading has the probability density function (PDF) given as

$$|h| \sim f_{|h|}\big(y, N_q\big) \triangleq \frac{N_q^{N_q} y^{N_q-1} \exp\{-N_q y\}}{\Gamma\big(N_q\big)}, \ \forall y > 0, \quad (1)$$

where N_q is the Nakagami fading parameter wherein $q \in \{L_m, N_m\}$ and $\Gamma(N_q)$ is the gamma function. Here L_m and N_m represent the LoS and NLoS propagation environments, respectively, and the Nakagami parameter is characterized for each environment differently. In the assumed system model, the small scale fading between the mmWave small cell BS and the typical user is considered to be independent Nakagami fading with Nakagami fading parameter N_{L_m} and N_{N_m} for LoS and NLoS links, respectively. Both N_{L_m} and N_{N_m} are considered as positive integers for the ease of tractability.

We perform our analysis on a typical outdoor user where a typical user at the origin *O* is LoS to the mmWave small cell at *A* if and only if there is no blockage intersecting the link *OA*. By employing independent thinning theorem, Φ_3 is divided into $\Phi_3^{L_m}$ and $\Phi_3^{N_m} = \Phi_3/\Phi_3^{L_m}$ using LoS probability function, $p(x)$, as independent PPPs of LoS and NLoS mmWave small cells, respectively [27]. Thus, $\Phi_3^{L_m}$ and $\Phi_3^{N_m}$ have the densities $p(x)\lambda_3$ and $(1-p(x))\lambda_3$, respectively. The LoS probability function, $p(x)$, is a measure of probability that a link of length x is LoS while NLoS probability of a link is $1-p(x)$. The LoS probability function $p(x)$ can be obtained by field measurements or from stochastic blockage models. Using stochastic blockage models, $p(x)$ is defined as, $p(t) = e^{-\beta x}$ where β is the dependent on statistics of blockages and x is the link distance between the serving BS and the typical user.

The mmWave tier BSs use directional beamforming for data transmission for compensating the notable path loss at mmWave frequencies. The antenna pattern is approximated using a sectored model, where the array gains are assumed to be constant for all angles in the main lobe and another constant in the side lobe. Beam direction is assumed to be independent and uniformly distributed between (0, 2π]. Hence, the effective antenna gain distribution, $G_{T,R}$, at a typical receiver, *r*, for an interferer, *t*, is given as,

$$G_{T,R} = \begin{cases} M_r M_t & \text{with prob. } \dfrac{\theta_r \theta_t}{4\pi^2} \\ M_r m_t & \text{with prob. } \dfrac{\theta_r(2\pi-\theta_t)}{4\pi^2} \\ m_r M_t & \text{with prob. } \dfrac{(2\pi-\theta_r)\theta_t}{4\pi^2} \\ m_r m_t & \text{with prob. } \dfrac{(2\pi-\theta_r)(2\pi-\theta_t)}{4\pi^2}, \end{cases} \quad (2)$$

where M_j is the main lobe gain with beamwidth θ_j, m_j donates the side lobe gain and θ_j is the half power beamwidth (or 3-dB beamwidth where $j \in \{t, r\}$). We assume that the typical transmitting BS, *t*, and receiver, *r*, are perfectly aligned thus maximum directivity gain $M_r M_t$ can be achieved. Likewise, the antenna gain seen at the eavesdropper $e \in \{EV_1, EV_2, \ldots, EV_E\}$[1] from serving BS, *t*, is defined as

$$G_{T,e} = \begin{cases} M_e M_t & \text{withprob. } \dfrac{\theta_e \theta_t}{4\pi^2} \\ M_e m_t & \text{withprob. } \dfrac{\theta_e(2\pi-\theta_t)}{4\pi^2} \\ m_e M_t & \text{withprob. } \dfrac{(2\pi-\theta_e)\theta_t}{4\pi^2} \\ m_e m_t & \text{withprob. } \dfrac{(2\pi-\theta_e)(2\pi-\theta_t)}{4\pi^2}, \end{cases} \quad (3)$$

where M_e, m_e and θ_e are the main lobe gain, half power beamwidth and the side lobe gain at the eavesdropper *e*, respectively.

2) Sub-6 GHz Network: The channel modeling in the sub-6 GHz network can be formulated in a similar manner to that of the mmWave network with the exception that the antennas in sub-6 GHz BSs are omni-directional with the transmission power of P_i with the path loss exponent $\alpha_i, \forall i \in \{1, 2\}$. We assume that the Macro BS operating at sub-6 GHz are equipped with *N* antennas whereas Small cell BS operating at sub-6 GHz are equipped with a single antenna, i.e., $N = 1$. It is important to highlight that for the sub-6 GHz network, *h* is assumed to be independent and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and unit variance, which is the same as assuming the fading to be Nakagami with $N_q = 1$. An i.i.d Rayleigh fading channel is considered for the massive MIMO enabled macrocell BS and small cell BS operating at sub-6 GHz band with the typical user. It is worthwhile to mention that for single input single output (SISO) transmission (for the case of sub-6 GHz small cells tier or tier 2), there is no precoding and

[1] *E* is the total number of eavesdroppers.

the channel gain for the both interfering and direct link follow $\exp(1)$ distribution which is same as $\Gamma(1,1)$ distribution. If the desired link is established between the transmitter and receiver, $G_{T,R} = G_u G_k$ where G_u is user's gain and $G_{(.)}$ denotes the main lobe gain for $k \in \{1,2\}$. It is also important to highlight that the effective antenna gain $G_{T,R}$ for the sub-6 GHz links are not affected by the half-power beamwidth and the side lobe gain. As the legitimate users (or eavesdroppers) are equipped with a single omni-directional antenna so the effective antenna gain G_u (or G_e) is equal to 1, $G_{T,R} = G_k$.

B. Downlink User Association

In this work, it is assumed that the legitimate user connects to the BS that provides maximum average received power [28]. Thus, the typical user located at the origin will connect to tier j only if

$$\begin{aligned} j &= \arg \max_{k \in \{1,2,3\}} C_k P_k G_{T,R} x^{-\alpha_k} \\ &= \arg \max_{k \in \{1,2,3\}} \overline{P_k} G_{T,R} x^{-\alpha_k}, \end{aligned}$$

where the normalized transmission power of the k^{th} tier is given by $\overline{P_k} = C_k \times P_k = \dfrac{P_k}{(\frac{4\pi}{\lambda_c})^2}$. λ_c is the carrier wavelength corresponding to the carrier frequency f_c, C_k is the frequency dependent path loss at a reference distance of 1 m given by $(\frac{\lambda_c}{4\pi})^2$ and the path loss between typical user and serving BS for the separating distance x is given by $x^{-\alpha_k}$.

The average received power for a user establishing connection with the MBS, M (from Φ_1 or tier 1) denoted by P_1^{avg} can be expressed as,

$$P_1^{\text{avg}} = G_M \frac{\overline{P_1}}{U} x^{-\alpha_1}, \tag{4}$$

where G_M is the antenna array gain expressed as ($N-U+1$) for ZFBF transmission [26]. Using the orthogonality property of ZFBF, each user is provided with the same number of spatial degrees of freedom given by ($N-U+1$). The average received power for a user establishing connection with small cell BS can be expressed as,

$$P_l^{\text{avg}} = \overline{P_l} G_l x^{-\alpha_l}, \quad \text{where} \quad l \in \{2,3\}, \tag{5}$$

where G_l can be defined as follow:

$$G_l = \begin{cases} 1, & \text{sub} - 6 \text{ GHz small cell}, \\ G_{T,R}, & \text{defined in (2), mmWave small cell}. \end{cases}$$

C. Signal-to-Interference Plus Noise Ratio (SINR) Model

In this subsection, we analyze SINR of the considered three tier HetNet. It is observed that the secrecy performance improves manyfolds when the eavesdropper channel is distorted because of interference. It is important to highlight that the eavesdroppers are the users who are acting malicious. It is also important to note that the sub-6 GHz users operate at lower frequency with higher wavelength which makes it infeasible to equip the users (eavesdropper or legitimate users) with more than one antenna. For a fair comparison, it is assumed that all the users are equipped with a single antenna. In this work, we have also assumed that the eavesdropper acts on its own which means they do not cooperate with each other, i.e., the SINR for the eavesdropper is coming from the most malicious user. This assumption also validates that each eavesdropper has only one antenna.

The received SINR between a typical receiver and any eavesdropper[2] establishing a connection with the serving MBS, where $M \in \hat{\Phi}_1$ can be expressed as

$$\text{SINR}_M^o = \frac{\frac{\overline{P_1}}{U} \left|\mathbf{h}_{o,M} \boldsymbol{\omega}_o\right|^2 G_M x^{-\alpha_1}}{\sigma^2 + \sum_{v \in \overline{\Phi_1}} \frac{\overline{P_1}}{U} \left|\mathbf{h}_{v,M} \boldsymbol{\omega}_v\right|^2 G_v x_v^{-\alpha_1} + I_S}, \tag{6}$$

$$\text{SINR}_M^{e^*} = \frac{\frac{\overline{P_1}}{U} \left|\mathbf{h}_{e,M} \boldsymbol{\omega}_e\right|^2 G_e x_e^{-\alpha_1}}{\sigma^2 + \sum_{v \in \overline{\Phi_1}} \frac{\overline{P_1}}{U} \left|\mathbf{h}_{v,M} \boldsymbol{\omega}_v\right|^2 G_v x_{v,e}^{-\alpha_1} + I_S}, \tag{7}$$

where $\mathbf{h}_{o,v} = [h_{o,v}^1, \ldots, h_{o,v}^N] \in \mathcal{C}^{1 \times N}$ is the downlink channel between the v^{th} sub-6 GHz MBS to the typical user with the subscript o. Each entry in $\mathbf{h}_{o,v}$ is independently identically distributed (iid) complex Gaussian random variable with zero mean and unit variance. The separate encoding scheme is considered at each MBS, v^{th} MBS sends an information symbol via a linear ZFBF vector $\boldsymbol{\omega}_v = [\omega_v^1, \ldots, \omega_v^N]$ with unit norm, i.e., $||\omega_v|| = 1, v \in \overline{\Phi}_1$, where $\overline{\Phi}_1$ is the set of interfering BSs, i.e., interference from all other macrocell BSs excluding the serving macrocell BS such that $\hat{\Phi}_1 \cup \overline{\Phi}_1 = \Phi_1$ and $N << \infty$ is the number of antennas at v^{th} MBS. I_S is the inter cell interference from the small cell operating in sub-6 GHz band given by $\sum_{s \in \Phi_2} \overline{P_2} |h_s|^2 x_s^{-\alpha_2}$. h_s, $h_{v,M}$, $h_{o,M}$ are the small scale fading gains at the typical user from the interfering channel such that $h_s \sim \exp(1)$, from the interfering MBS such that $h_{v,M} \sim \Gamma(U,1)$ and from serving MBS for U users such that $h_{o,M} \sim \Gamma(N-U+1,1)$ [26]. Here, the fading gain at eavesdropper at the separation distance x_e from the serving BS is denoted by $h_{e,M} \sim \exp(1)$. Similarly, x_s and x_v are the distances measured from the typical user to small cell BS $s \in \Phi_2$ and from the typical user to MBS $v \in \overline{\Phi}_1$, and σ^2 is the thermal noise.

The received SINR between a typical user and any eavesdropper at separation distance x_e establishing connection with the small cell BS operating at sub-6 GHz band, where $S \in \Phi_2$ can be defined as

$$\text{SINR}_S^o = \frac{\overline{P_2} |h_{o,S}|^2 x^{-\alpha_2}}{\sigma^2 + \sum_{s \in \overline{\Phi}_2} \overline{P_2} |h_{s,S}|^2 x_s^{-\alpha_2} + I_{\overline{\text{M}}}}, \tag{8}$$

$$\text{SINR}_S^{e^*} = \frac{\overline{P_2} |h_{e,S}|^2 x_e^{-\alpha_2}}{\sigma^2 + \sum_{s \in \overline{\Phi}_2} \overline{P_2} |h_{s,S}|^2 x_{s,e}^{-\alpha_2} + I_{\overline{\text{M}}}}, \tag{9}$$

[2]There is a possibility that all or several eavesdroppers can cooperate with each other by combining their observations forwarded to the central entity to decode the message of the legitimate user. This cooperation among the eavesdroppers can result in a group of cooperating eavesdroppers, i.e., $|U_e|$ resulting in a powerful user with an access to U_e antennas whose aggregate received power is the summation of the received power on all the antennas leading to the maximum secrecy outage. This cooperating mechanism is mentioned here for the sake of completeness, but it is not the main focus of this work. It is also assumed that the eavesdropping channels and legitimate user channels are independent of each other, thus the eavesdropper with the highest received SINR is the most malicious one and it dominates the secrecy rate. Therefore, the SINRs discussed in this subsection are for the most malicious eavesdropper, i.e., $\text{SINR}_i^{e^*} = \max_{e \in \Phi_e} \{\text{SINR}_i^e\}$ where $i \in \{M, S, m\}$.

where $I_{\overline{\mathrm{M}}}$ is the intercell interference from macro cells given by $\sum_{v\in\Phi_1}\frac{\overline{P_1}}{U}|h_v|^2 x_v^{-\alpha_1}$. Here, $h_{s,S}$, $h_{o,S}$, $h_{e,S}$ and h_v are the small scale fading gain from the interfering channel such that $h_{s,S}\sim\exp(1)$, $h_{o,S}\sim\exp(1)$, $h_{e,S}\sim\exp(1)$ and $h_v\sim\Gamma(U,1)$. Here, x_s and x_v are the distance measured of the typical user from small cell BS s and MBS v, respectively.

The received SINR between the typical user and any eavesdropper establishing connection with mmWave small cell denoted by $b_{o,m}$ can be expressed as

$$\mathrm{SINR}_m^o=\frac{\overline{P_3}M_rM_t|h_{o,m}|^2x^{-\alpha_3^{(q)}}}{\sigma^2+\overline{P_3}\sum_{q\in\{L_m,N_m\}}\sum_{l\in\overline{\Phi}_3^q}G_l|h_{l,m}|^2x_l^{-\alpha_3^{(q)}}},\tag{10}$$

$$\mathrm{SINR}_m^{e^*}=\frac{\overline{P_3}G_e|h_{e,m}|^2x_e^{-\alpha_3^{(q)}}}{\sigma^2+\overline{P_3}\sum_{q\in\{L_m,N_m\}}\sum_{l\in\overline{\Phi}_3^q}G_l|h_{l,m}|^2x_{l,e}^{-\alpha_3^{(q)}}},\tag{11}$$

where $h_{o,m}$ and $h_{e,m}$ are small scale fading gain, G_l and G_e are the directivity gains of interfering BSs, given by (2) and (3) and $q\in\{L_m,N_m\}$ identifies the interfering link as either LoS (L) or NLoS (N), respectively.

D. Power Consumption Model

The total power consumption at MBS in each channel is given by

$$P_1^{total}=\rho_1+\frac{P_1}{\epsilon_1}+\sum_{t=1}^{3}(U)^t(\Delta_t+N\Lambda_t),\tag{12}$$

where ρ_1 is load independent circuit power or static hardware power consumption of MBS, ϵ_1 is power amplifier efficiency, parameters Δ_t and Λ_t depend on transceiver chains, coding, decoding and precoding [29].

The total power consumption in small cells of tier 2 and tier 3 is given by

$$P_l^{total}=\rho_l+\frac{P_l}{\epsilon_l}\quad\text{for}\quad l\in\{2,3\},\tag{13}$$

where ρ_l is load independent circuit power of SBS, $l\in\{2,3\}$ and ϵ_l is power amplifier efficiency of the small cell BS of the l-th tier.

E. Secure Transmission Characterization

In this proposed network scenario, it is assumed that all tier links are eavesdropped. We consider the case of passive eavesdropping where eavesdroppers do not perform any active attacks to deteriorate downlink transmission information. To protect the confidential information from intrusion, a secrecy coding scheme called Wyner code is adopted at each link such that each BS encodes its data using Wyner coding scheme before transmission [30]. Based on this scheme, two kinds of code rates need to be specified before data transmission at the transmitter, i.e., the rate of the transmitted confidential message signal R_m, and rate of transmitted code words R_c where the cost of maintaining the confidential message secrecy is R_c-R_m [30]. We assume that rates R_c and R_m remain fixed during information transmission [31], [32]. Depending on the choice of R_m and R_c at the BS, the secrecy outage events may occur and due to quasi-static channel it is not possible to ensure perfect secrecy.

In order to prevent the secrecy outage event, the wiretapping capacity of the channel between the serving BS and eavesdropper R_e should be less than the rate R_c-R_m, meaning that the received SINR at any eavesdropper is above a certain threshold. In this trend, the secrecy outage probability is defined as $P_{so}^k(\gamma_e)=\Pr(\mathrm{SINR}_k^e>\gamma_e)$. SSE is the measure of the average secrecy rate per unit bandwidth and it is used to define the spectrum efficiency in terms of secrecy measure in a 3-tier massive MIMO enabled hybrid HetNet. SEE is defined as the secrecy performance of a 3-tier massive MIMO enabled hybrid HetNet achieved with unit energy consumption.

III. Secrecy Performance Evaluation

The secrecy transmission capacity constraint is defined as the average achievable rate of successful transmission of confidential information [30], [33]. In the proposed 3-tier massive MIMO-enabled hybrid HetNet, the average achievable secrecy rate for each tier k is defined as

$$R_{Sk}=[R_k-R_k^e]^+\quad\text{for}\quad k\in\{1,2,3\},\tag{14}$$

where $R_k=\mathbb{E}[\log_2(1+\mathrm{SINR}_k^u)]$ is the average achievable ergodic rate of the channel between the serving base station of tier k and the typical receiver node, $R_k^e=\mathbb{E}[\log_2(1+\mathrm{SINR}_k^{e^*})]$ is the average achievable ergodic rate of the channel between the serving base station and most malicious eavesdropper and $[y]^+=\max\{0,y\}$.

Since the eavesdropper nodes are non-colluding, i.e., they intercept the confidential information message passively without actively intruding the transmission, the CSI of eavesdropper node is unknown at the serving BS. Thus the ergodic transmission rate of the serving BS is only dependent on the CSI of the link between itself and legitimate intended receiver. In this work, we considered the case of most malicious eavesdropper, hence, the average achievable ergodic rate in a random wiretap channel cannot exceed R_k^e.

A. Achievable Ergodic Rate

Using the mathematical notations defined in (14), we first derive the achievable ergodic rate at the intended legitimate user as follows.

Lemma 1: When the legitimate typical user is associated with MBS, the exact achievable average ergodic rate between the serving BS and the most malicious eavesdropper is given by [39, Th. 3] [38]

$$\begin{aligned}R_1^e&=Pr(R_1^e>\gamma_e)\\&=Pr[\log_2(1+SINR_M^e)>\gamma_e],\\R_1^e&=Pr(SINR_M^e>2^{\gamma_e}-1),\\R_1^e&=\frac{1}{\ln(2)}\int_0^\infty Pr(SINR_M^e>e^{\gamma_e}-1),\\R_1^e&=\frac{1}{\ln(2)}\int_0^\infty\frac{P_C^1(\gamma_e)}{1+\gamma_e}d\gamma_e,\end{aligned}$$

$$R_1^e = \frac{1}{\ln 2}\int_0^\infty \frac{1-P_{so}^1(\gamma_e)}{1+\gamma_e}d\gamma_e, \tag{15}$$

where $P_{so}^1(\gamma_e)$ is CDF of $\mathrm{SINR}_M^{e^*}$ given as,

$$P_{so}^1(\gamma_e) = 1-\exp\Bigg(-2\pi\lambda_e\sum_{i=1}^{N}\binom{N}{i}(-1)^{i+1} \times\int_0^\infty r_e\exp\Big[-\frac{i\gamma_e r_e^{\alpha_1}\sigma^2}{\hat{P}_1}-\zeta_1^1-\zeta_2^1\Big]dr_e\Bigg), \tag{16}$$

where $\hat{P}_1=\frac{\overline{P_1}}{U}$, ζ_1^1 and ζ_2^1 are given as,

$$\zeta_1^1 = 2\pi\lambda_1\sum_{c=1}^{U}\binom{U}{c}\int_{r_e}^\infty \frac{\left(u\hat{P}_1 r^{-\alpha_1}\right)^c}{\left(1+u\hat{P}_1 r^{-\alpha_1}\right)^U}rdr$$

and

$$\zeta_2^1 = 2\pi\lambda_2\int_{\left(\frac{\overline{P_2}}{(N-U+1)\hat{P}_1}\right)^{\frac{1}{\alpha_2}} r_e^{\frac{\alpha_1}{\alpha_2}}}^\infty \left(\frac{u\overline{P_2}r^{-\alpha_2}}{1+u\overline{P_2}r^{-\alpha_2}}\right)rdr,$$

where $u=(\frac{i\gamma_e r_e^{\alpha_1}}{\hat{P}_1})$.

Proof: A detailed proof is provided in Appendix B. ■

Lemma 2: The achievable ergodic rate at the intended legitimate user associated with MBS is given by

$$R_1 = \frac{1}{\ln 2}\int_0^\infty \frac{P_C^1(\gamma)}{1+\gamma}d\gamma, \tag{17}$$

where $P_C^1(\gamma)=\int_0^\infty P_C^1(\gamma,x)f_{X_1}(x)dx$ is the complementary cumulative distribution function (CCDF) of SINR_M^u. Here, $f_{X_1}(x)$ is the probability density function (PDF) of the distance between the serving MBS and typical user and $P_C^1(\gamma,x)$ is the conditional coverage probability for given distance x between the typical user and serving MBS.

Proof: A detailed proof is provided in Appendix C. ■

By substituting (15) and (17) in (14), we can finally calculate the average achievable secrecy rate for sub-6 GHz macro tier.

Lemma 3: The achievable ergodic rate at the intended legitimate user establishing connection with sub-6 GHz small cell BS can be expressed as

$$R_2 = \frac{1}{\ln 2}\int_0^\infty \frac{P_C^2(\gamma)}{1+\gamma}d\gamma, \tag{18}$$

where $P_C^2(\gamma)=\int_0^\infty P_C^2(\gamma,x)f_{X_2}(x)dx$ is the CCDF of SINR_S^u. Here, $f_{X_2}(x)$ is the PDF of the distance between the serving sub-6 GHz small cell BS and typical user and $P_C^2(\gamma,x)$ is the conditional coverage probability of the typical user. The PDF of distance, $f_{X_2}(x)$, is given as,

$$f_{X_2}(x) = \frac{2\pi\lambda_2}{A_2}x\exp\Bigg(-\pi\lambda_2 x^2-2\pi\lambda_3 D(x) -\pi\lambda_1\left(\frac{\overline{P_1}(N-U+1)x^{\alpha_2}}{\overline{P_2}U}\right)^{2/\alpha_1}\Bigg), \tag{19}$$

where A_2 is the association probability that a user is connected to sub-6 GHz small cell BS given by

$$A_2 = 2\pi\lambda_2\int_0^\infty x\exp\Bigg(-\pi\lambda_2 x^2-2\pi\lambda_3 D(x) -\pi\lambda_1\left(\frac{\overline{P_1}(N-U+1)x^{\alpha_2}}{\overline{P_2}U}\right)^{2/\alpha_1}\Bigg)dx, \tag{20}$$

where $D(x)$ is given by (A.4), $\delta_N(x)=(\frac{\overline{P_3}G}{\overline{P_2}})^{\frac{1}{\alpha_L}}x^{\frac{\alpha_2}{\alpha_L}}$ and $\delta_L(x)=(\frac{P_3G}{P_2})^{\frac{1}{\alpha_N}}x^{\frac{\alpha_2}{\alpha_N}}$.

Conditional coverage probability, $P_C^2(\gamma,x)$, is defined as,

$$P_C^2(\gamma,x) = \exp\Bigg(-\frac{\gamma\sigma^2x^{\alpha_2}}{\overline{P_2}}-2\pi\lambda_1\sum_{z=1}^{U}\binom{U}{z} \times\left(\frac{\overline{P_1}\gamma x^{\alpha_2}}{U\overline{P_2}}\right)^z\times\frac{\left(-\frac{\gamma x^{\alpha_2}\overline{P_1}}{U\overline{P_2}}\right)^{-z+\frac{2}{\alpha_1}}}{\alpha_1} \times B_{\left(\frac{\overline{P_1}\gamma x^{\alpha_2}}{U\overline{P_2}}(H(x))^{-1}\right)}\left[z-\frac{2}{\alpha_1},1-U\right] -2\pi\lambda_2\gamma x^{\alpha_2}\frac{x^{2-\alpha_2}}{\alpha_2-2}\times_2 F_1 \times\left[\frac{\alpha_2-2}{\alpha_2},1;2-\frac{2}{\alpha_2};-\gamma\right]\Bigg), \tag{21}$$

where $H(x)=(\frac{(N-U+1)}{U\overline{P_2}}\overline{P_1}x^{\alpha_2})$.

Proof: The proof follows on the similar lines from Lemma 1. However, for better understanding, readers can follow the proof from Appendix C. ■

Lemma 4: When the legitimate typical user establishes connection with sub-6 GHz small cell, the exact achievable average ergodic rate between the serving BS and the most malicious eavesdropper is given by

$$R_2^e = \frac{1}{\ln 2}\int_0^\infty \frac{1-P_{so}^2(\gamma_e)}{1+\gamma_e}d\gamma_e, \tag{22}$$

where $P_{so}^2(\gamma_e)$ is the CDF of $\mathrm{SINR}_S^{e^*}$ given as,

$$P_{so}^2(\gamma_e) = 1-\exp\Bigg(-2\pi\lambda_e\int_0^\infty r_e\exp\Big[-\frac{\gamma_e r_e^{\alpha_2}\sigma^2}{\overline{P_2}}-\zeta_1^2-\zeta_2^2\Big]dr_e\Bigg), \tag{23}$$

where

$$\zeta_1^2 = 2\pi\lambda_1\sum_{\mu=1}^{U}\binom{U}{\mu} \times\int_{\left(\frac{N-U+1}{\overline{P_2}}\hat{P}_1\right)^{\frac{1}{\alpha_1}} r_e^{\frac{\alpha_2}{\alpha_1}}}^\infty \frac{\left(u\hat{P}_1 r^{-\alpha_1}\right)^\mu}{\left(1+u\hat{P}_1 r^{-\alpha_1}\right)^U}rdr,$$

$$\zeta_2^2 = 2\pi\lambda_2 \int_{r_e}^{\infty} \left(\frac{u\overline{P_2} r^{-\alpha_2}}{1 + u\overline{P_2} r^{-\alpha_2}} \right) r dr,$$

where $u = (\frac{\gamma_e r_e^{\alpha_2}}{\overline{P_2}})$.

Proof: It can be proved by following the approach used in Lemma 2. ∎

By substituting (18) and (22) in (14), we can thus calculate the average achievable secrecy rate for sub-6 GHz small cell tier.

Lemma 5: The achievable ergodic rate at the intended legitimate user associated with mmWave small cell BS is given by

$$R_3 = \frac{1}{\ln 2} \int_0^{\infty} \frac{P_C^3(\gamma)}{1+\gamma} d\gamma, \tag{24}$$

where $P_C^3(\gamma) = \sum_{q \in \{L,N\}} A_{3,q} P_C^{3,q}(\gamma)$, is the CCDF of SINR_m^u, $P_C^{3,L_m}(\gamma)$ and $P_C^{3,N_m}(\gamma)$ are the conditional coverage probabilities when the typical user, associated with mmWave small cell tier, forms a link with the BS in $\Phi_3^{L_m}$ and $\Phi_3^{N_m}$, $A_{3,q}$ are the probabilities of typical user connecting with LoS or NLoS link, respectively.

The conditional coverage probabilities, $P_C^{3,q}(\gamma, x)$ can be evaluated by

$$P_C^{3,q}(\gamma) = \sum_{j=1}^{N_q} (-1)^{j+1} \binom{N_q}{j} \times \int_0^{\infty} \exp\left(\frac{-j\eta_q x^{\alpha_q} \gamma \sigma^2}{M_r M_t} - C_{q,j}(\gamma, x) \right) f_q(x) dx, \tag{25}$$

where $C_{q,j}(\gamma, x)$ is shown in (26) and (27), at the bottom of the page, where $\overline{\delta_{L_m}}(x) = x^{\frac{\alpha_{L_m}}{\alpha_{N_m}}}$, $\overline{\delta_{N_m}}(x) = x^{\frac{\alpha_{N_m}}{\alpha_{L_m}}}$, $F(N_q, x) = 1 - 1/(1+x)^{N_q}$ and $\eta_q = N_q (N_q!)^{-\frac{1}{N_q}}$, $q \in \{L_m, N_m\}$. Parameters $\hat{a}_i = a_i / M_r M_t$, a_i and p_i are defined in Section II-A.

Proof: A detailed proof is provided in Appendix D. ∎

Remark 1: For the special case of Rayleigh small scale fading, the conditional coverage probability, $P_C^{3,q}(\gamma)$ can be approximated by setting $N_{L_m} = N_{N_m} = 1$ and $\eta_{L_m} = \eta_{N_m} = 1$ as follow:

$$P_C^{3,q}(\gamma) = \int_0^{\infty} \exp\left(\frac{-j\eta_q x^{\alpha_q} \gamma \sigma^2}{M_r M_t} - C_{q,j}(\gamma, x) \right) f_q(x) dx,$$

where $C_{q,j}, q \in \{L_m, N_m\}$ can be approximated from (26) and (27) by replacing $N_{L_m} = N_{N_m} = 1$, $\eta_{L_m} = \eta_{N_m} = 1$ and $F(N_q, x) = 1 - \frac{1}{1+x}$.

Lemma 6: When the legitimate typical user is associated with mmWave small cell, the exact achievable average ergodic rate between the serving BS and the most malicious eavesdropper is given by

$$R_3^e = \frac{1}{\ln 2} \int_0^{\infty} \frac{1 - P_{so}^3(\gamma_e)}{1+\gamma_e} d\gamma_e, \tag{28}$$

where $P_{so}^2(\gamma_e)$ is the CDF of $\mathrm{SINR}_m^{e^*}$ given as,

$$P_{so}^3(\gamma_e) = 1 - \exp\left(-2\pi\lambda_e \sum_{j \in \{L_m, N_m\}} \sum_{i=1}^{N_j} \binom{N_j}{i} (-1)^{i+1} \times \int_0^{\infty} r_e \exp\left[-\frac{i\gamma_e r_e^{\alpha_j} \sigma^2}{\overline{P_3} G_e} - \zeta_{3,j} \right] p_j(r_e) dr_e \right), \tag{29}$$

where $p_L(r_e) = e^{(-\beta r_e)}$ is the LoS probability function and $p_N(r_e) = 1 - e^{(-\beta r_e)}$ is the NLoS probability function for the eavesdropper wiretapping the transmission from serving mmWave BS to the intended receiver node. Here, $\zeta_{3,L_m} = C_{L,j}(\gamma_e, r_e)$ and $\zeta_{3,N_m} = C_{N,j}(\gamma_e, r_e)$ where $C_{L_m,j}(\gamma_e, r_e)$ and $C_{N_m,j}(\gamma_e, r_e)$ can be computed by setting $\gamma = \gamma_e$ and $r = r_e$ in (26) and (27), respectively.

Proof: It can be proved by following the approach used in Lemma 2, separately, for LoS and NLoS link. By substituting (24) and (28) in (14), we can thus calculate the average achievable secrecy rate for mmWave tier. ∎

B. Special Cases

Example 1: By setting $N = U = 1$, the association probability of MBS, sub-6 GHz small cells and mmWave small cells can be given, respectively, by:

$$A_1 = 2\pi\lambda_1 \int_0^{\infty} x \exp\left(-\pi\lambda_2 \left(\frac{\overline{P_2} x^{\alpha_1}}{\overline{P_1}} \right)^{2/\alpha_2} - \pi\lambda_1 x^2 - 2\pi\lambda_3 \left(\frac{\overline{P_3}}{\overline{P_1}} \right)^{2/\alpha_3} D(x) \right) dx, \tag{30}$$

$$A_2 = 2\pi\lambda_2 \int_0^{\infty} x \exp\left(-\pi\lambda_2 x^2 - 2\pi\lambda_3 D(x) - \pi\lambda_1 \left(\frac{\overline{P_1} x^{\alpha_2}}{\overline{P_2}} \right)^{2/\alpha_1} \right) dx, \tag{31}$$

$$C_{L_m,j}(\gamma, x) = 2\pi\lambda_3 \sum_{i=1}^{4} p_i \left[\int_x^{\infty} F\left(N_{L_m}, \frac{j\eta_{L_m} \hat{a}_i \gamma x^{\alpha_{L_m}}}{N_{L_m} t^{\alpha_{L_m}}} \right) p(t) t dt + \int_{\overline{\delta_L}(x)}^{\infty} F\left(N_{N_m}, \frac{j\eta_{L_m} \hat{a}_i \gamma x^{\alpha_{L_m}}}{N_{N_m} t^{\alpha_{N_m}}} \right) (1 - p(t)) t dt \right] \tag{26}$$

$$C_{N_m,j}(\gamma, x) = 2\pi\lambda_3 \sum_{i=1}^{4} p_i \left[\int_{\overline{\delta_N}(x)}^{\infty} F\left(N_{L_m}, \frac{j\eta_{N_m} \hat{a}_i \gamma x^{\alpha_{N_m}}}{N_{L_m} t^{\alpha_{L_m}}} \right) p(t) t dt + \int_x^{\infty} F\left(N_{N_m}, \frac{j\eta_{N_m} \hat{a}_i \gamma x^{\alpha_{N_m}}}{N_{N_m} t^{\alpha_{N_m}}} \right) (1 - p(t)) t dt \right] \tag{27}$$

$$A_{3,L_m} = 2\pi\lambda_3 \int_0^\infty xp(x)\exp\{(-2\pi\lambda_3 M(x) - Z(x) - Y(x))\}, \quad (32)$$

$$A_{3,N_m} = 1 - A_1 - A_2 - A_{3,L_m}, \quad (33)$$

where $D(x)$ is given by (18), $Z(x) = \pi\lambda_1(\frac{\overline{P_1}x^{\alpha_{L_m}}}{\overline{P_3}})^{2/\alpha_1}$ and $Y(x) = \pi\lambda_2(\frac{\overline{P_2}x^{\alpha_1}}{\overline{P_1}})^{2/\alpha_2}$. This change in setting is equal to the previous result corresponding to the cellular network in [19].

Case 1: Similarly, for the case of same path-loss exponents for all k tiers, i.e., $\alpha_1 = \alpha_2 = \alpha_{3,L_m} = \alpha_{3,N_m} = \alpha$, the association probabilities and $D(x)$ in (18) can be further simplified as below:

$$A_1 = 2\pi\lambda_1 \int_0^\infty x\exp\left(-\pi\lambda_2\left(\frac{\overline{P_2}}{\overline{P_1}}\right)^{2/\alpha}x^2 - \pi\lambda_1 x^2 - 2\pi\lambda_3\left(\frac{\overline{P_3}}{\overline{P_1}}\right)^{2/\alpha}D(x)\right)dx, \quad (34)$$

$$A_2 = 2\pi\lambda_2 \int_0^\infty x\exp\left(-\pi\lambda_2 x^2 - 2\pi\lambda_3 D(x) - \pi\lambda_1\left(\frac{\overline{P_1}}{\overline{P_2}}\right)^{2/\alpha}x^2\right)dx, \quad (35)$$

$$A_{3,L_m} = 2\pi\lambda_3 \int_0^\infty xp(x)\exp\{(-2\pi\lambda_3 M(x) - Z(x) - Y(x))\}, \quad (36)$$

where $Z(x) = \pi\lambda_1(\frac{\overline{P_1}}{\overline{P_3}})^{2/\alpha}x^2$ and $Y(x) = \pi\lambda_2(\frac{\overline{P_2}}{\overline{P_1}})^{2/\alpha}x^2$.

$$A_{3,N_m} = 1 - A_1 - A_2 - A_{3,L_m}, \quad (37)$$

and,

$$D(x) = \int_0^{\delta_{N_m}(x)} tp(t)dt + \int_0^{\delta_{L_m}(x)} t(1-p(t))dt, \quad (38)$$

where $\delta_{N_m}(x) = (\frac{\overline{P_3}G}{\overline{P_1}})^{\frac{1}{\alpha}}x$, $\delta_{L_m}(x) = (\frac{\overline{P_3}G}{\overline{P_1}})^{\frac{1}{\alpha}}x$.

Example 2: For the special case, when both MBS and sub-6 GHz small cells operate at different frequency bands, hence there is no cross-tier interference, i.e., only co-tier interference from same tier BSs and all tiers have same path-loss exponent α, the coverage probability of tier k can be simplified as follow:

$$P_C^1(\gamma, x) = \sum_{l=0}^{\eta_1} \frac{(x^\alpha)^l}{(l!)(-1)^l} \sum \frac{l!}{\prod_{j=1}^l n_j!(j!)^{n_j}} \times \exp\left(-\frac{\gamma\sigma^2 Ux^\alpha}{\overline{P_1}} - \overline{\Xi}\left(\frac{\gamma U x^\alpha}{\overline{P_1}}\right)\right) \times \prod_{j=1}^{l}\left(\overline{\Psi}^{(j)}((x^\alpha))\right)^{n_j}, \quad (39)$$

where $\eta_1 = N - U$. In (39), $\overline{\Xi}(e), \overline{\Psi}^{(1)}(i)$ and $\overline{\Psi}^{(j)}(i)$ are given by (40)–(42), shown at the bottom of this page.

Case 2: Similarly, $P_C^2(\gamma, x)$ can also be found by using $N = 1$ and $U = 1$ in (27). Similarly, $P_{so}^1(\gamma_e)$ and $P_{so}^2(\gamma_e)$ can also be obtained accordingly.

Example 3: For the mmWave tier operating in noise limited regime, $\sigma^2 >> (I_L + I_N)$, the coverage probability from Lemma 5 can be expressed as follow:

$$P_C^3(\gamma) = \sum_{q\in\{L_m,N_m\}}\sum_{j=1}^{N_q}(-1)^{j+1}\binom{N_q}{j} \times \int_0^\infty \exp\left(\frac{-j\eta_q x^{\alpha_q}\gamma\sigma^2}{M_r M_t}\right)\hat{f}_q(x)dx, \quad (43)$$

by equating $C_{q,j}(\gamma, x), q \in \{L_m, N_m\}$ to zero and $\hat{f}_q(x) = A_{3,q} \times f_q(x)$.

Case 3.1: Similarly, for the case in mmWave tier when the LoS interference is far more dominant than the NLoS interference, i.e., $I_{L_m} >> I_{N_m}$, the coverage probability from Lemma 5 can be expressed as follow:

$$P_C^3(\gamma) = \sum_{q\in\{L_m,N_m\}}\sum_{j=1}^{N_q}(-1)^{j+1}\binom{N_q}{j} \times \int_0^\infty \exp\left(\frac{-j\eta_q x^{\alpha_q}\gamma\sigma^2}{M_r M_t} - C_{q,j}(\gamma, x)\right)\hat{f}_q(x)dx, \quad (44)$$

where

$$C_{L_m,j}(\gamma, x) = 2\pi\lambda_3\sum_{i=1}^{4}p_i \times \int_x^\infty F\left(N_{L_m}, \frac{j\eta_{L_m}\hat{a}_i\gamma x^{\alpha_{L_m}}}{N_{L_m}t^{\alpha_{L_m}}}\right)tp(t)dt, \quad (45)$$

$$C_{N_m,j}(\gamma, x) = 2\pi\lambda_3\sum_{i=1}^{4}p_i \times \int_{x^{\frac{\alpha_{N_m}}{\alpha_{L_m}}}}^\infty F\left(N_{L_m}, \frac{j\eta_{N_m}\hat{a}_i\gamma x^{\alpha_{N_m}}}{N_{L_m}t^{\alpha_{L_m}}}\right)tp(t)dt, \quad (46)$$

$$\overline{\Xi}(e) = 2\pi\lambda_1\sum_{z=1}^{U}\binom{U}{z}\left(\frac{\overline{P}_1}{U}\right)^z e^z\left(\left(-e\frac{\overline{P}_1}{U}\right)^{-z+\frac{2}{\alpha}}\right)B_{\left(-e\frac{\overline{P}_1}{U}x^{-\alpha}\right)}\left[z-\frac{2}{\alpha}, 1-U\right] \quad (40)$$

$$\overline{\Psi}^{(1)}(i) = -\frac{\gamma\sigma^2 U}{\overline{P_1}} - 2\pi\lambda_1 U\gamma\frac{x^{2-\alpha}}{\alpha-2}\ {}_2F_1\left[\frac{\alpha-2}{\alpha}, U+1; 2-\frac{2}{\alpha}; -i\gamma x^{-\alpha}\right] \quad (41)$$

$$\overline{\Psi}^{(j)}(i) = 2\pi\lambda_1(-\gamma)^{\frac{2}{\alpha}}\frac{(U+j-1)!}{(U-1)!}\frac{(i)^{-j+\frac{2}{\alpha}}}{\alpha}B_{(-\gamma i x^{-\alpha})}\left[j-\frac{2}{\alpha}, 1-U-j\right] \quad (42)$$

Case 3.2: Similarly, for the case of dense mmWave network corresponding to the interference limited regime, i.e., $(I_{L_m} + I_{N_m}) >> \sigma^2$, where all the users would end up having LoS connections with their mmWave small cell, i.e., $I_{N_m} \approx 0$. For the dense deployment of mmWave small cells, the coverage probability from Lemma 5 can be expressed as follow:

$$P_C^3(\gamma) = \sum_{j=1}^{N_{Lm}} (-1)^{j+1} \binom{N_{L_m}}{j} \times \int_0^\infty \exp\left(\frac{-j\eta_{L_m} x^{\alpha_{L_m}} \gamma \sigma^2}{M_r M_t} - C_{L_m,j}(\gamma, x) \right) \hat{f}_q(x)\, dx, \quad (47)$$

where

$$C_{L_m,j}(\gamma, x) = 2\pi\lambda_3 \sum_{i=1}^{4} p_i \times \int_x^\infty F\left(N_{L_m}, \frac{j\eta_{L_m} \hat{a}_i \gamma x^{\alpha_{L_m}}}{N_{L_m} t^{\alpha_{L_m}}} \right) tp(t)\, dt. \quad (48)$$

C. Secrecy Outage Probability

The total secrecy outage probability, P_{so}, for the proposed three tier network with massive MIMO enabled MBS and mmWave small cells, is defined as

$$P_{so} = \sum_{k=1}^{3} P_{so}^k A_k, \quad (49)$$

where A_k is the association probability of tier k.

D. Secrecy Spectrum Efficiency

For the proposed 3-tier hybrid HetNet with massive MIMO in macro tier and mmWave small cells, using the law of total expectation and from [11], [15], the tractable lower bound on the SSE is given by

$$\text{SSE}^L = \sum_{k=1}^{3} A_k \times \text{SSE}_k, \quad (50)$$

where $\text{SSE}_1 = U \times R_{S1}$ is SSE for massive MIMO enabled macro tier and $\text{SSE}_k = R_{Sk}$ for $k \in \{2, 3\}$ is SSE for small cell tiers, respectively. Average achievable secrecy rate R_{Sk} for each tier k is defined in (14).

E. Secrecy Energy Efficiency

For the sustainable and optimal operation of the proposed 3-tier hybrid HetNet with massive MIMO in macro tier and mmWave small cells, theoretical understanding of SEE and SSE is equally important. Thus, the SEE for the proposed network is lower bounded as [23], [36]

$$\text{SEE}^L = \sum_{k=1}^{3} A_k \times \text{SEE}_k, \quad (51)$$

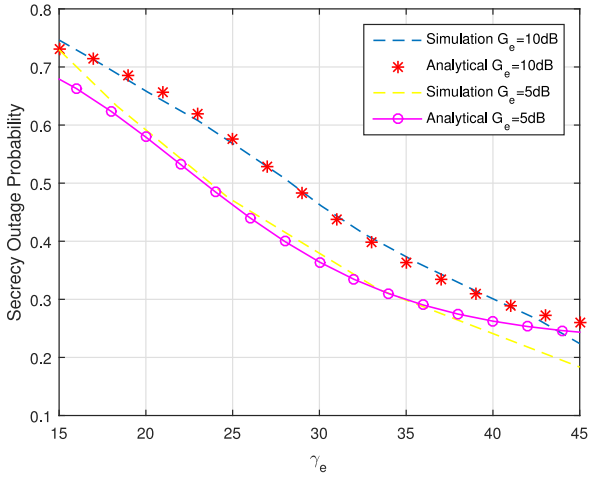

Fig. 1. Secrecy outage probability of the 3-tier network versus γ_e (dB) for $\lambda_2 = \lambda_3 = 30\lambda_1$, $N = 5$.

where $\text{SEE}_1 = \frac{U \times R_{S1}}{P_1^{total}}$ is SEE for massive MIMO enabled macro tier and $\text{SEE}_k = \frac{R_{Sk}}{P_k^{total}}$ for $k \in \{2, 3\}$ is SEE for small cell tiers, respectively. Average achievable secrecy rate R_{Sk} for each tier k is defined in (14).

IV. Simulation and Numerical Results

In the considered simulation setup, a 3-tier HetNet is assumed with MBS density $\lambda_1 = \frac{1}{(500^2 \times \pi)}$, whereas λ_2 and λ_3 are considered to be multiples of MBS density. The sub-6 GHz tiers are assumed to be operating at a carrier frequency of 1 GHz, 10 MHz bandwidth, path loss exponents $\alpha_1 = 3.5$, $\alpha_2 = 4$ and transmit power $P_1 = 46$ dBm and $P_2 = 30$ dBm, respectively. The density of eavesdropper is taken as $\lambda_e = 1 \times 10^{-6}$, unless stated otherwise. For mmWave tier, the operating frequency is 28 GHz, 100 MHz bandwidth, path loss exponent for LoS, $\alpha_L = 2$ and for NLoS, $\alpha_N = 4$ and transmit power $P_3 = 30$ dBm. Nakagami fading parameters for mmWave tier, N_N and N_L, are taken as 2 and 3, respectively. Array gains for all angles in main lobe are taken as $M_r = 10$ dB and $M_t = 10$ dB and for the side lobes $m_r = -10$ dB and $m_t = 0$ dB. The main lobe beamwidth is taken to be $\theta_r = 90^\circ$ and $\theta_t = 30^\circ$. A noise power $\sigma^2 = -90$ dBm is taken with a noise figure of 10 dB. The blockage parameter, β, is $1/\beta = 141.4$ meters [35]. We assume coefficients of energy efficiency of power amplifier as $\epsilon_1 = \epsilon_2 = \epsilon_3 = 0.38$ [23], load independent circuit power as $\rho_1 = 4$ W, $\Delta_1 = 4.8, \Delta_2 = 0, \Delta_3 = 2.08 \times 10^{-8}$, $\Lambda_1 = 1$, $\Lambda_2 = 9.5 \times 10^{-8}$ and $\Lambda_3 = 6.25 \times 10^{-8}$ [29]. Load independent circuit power for small cell tiers is taken as $\rho_2 = 13.6$ W and $\rho_3 = 13.6$ W, respectively [37]. Monte Carlo simulations are used to validate the analytical results.

Fig. 1 shows the plot for secrecy outage probability, obtained from (49), versus the SINR threshold at the eavesdropper for varying eavesdropper antenna gains for the mmWave tier. We observe that the secrecy outage probability decreases with γ_e whereas the higher directivity gains

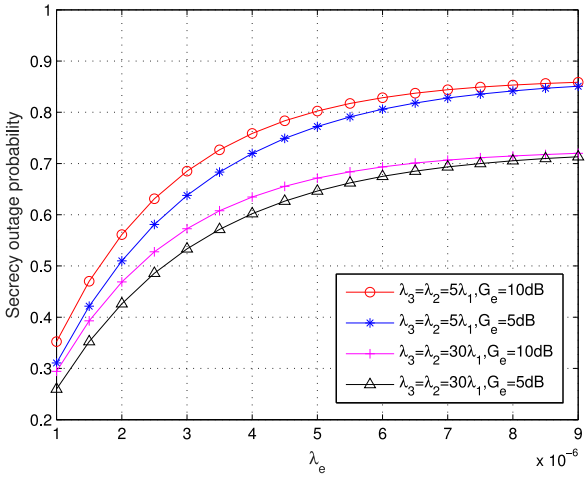

Fig. 2. Secrecy outage probability of the 3-tier network as the function of λ_e for $\gamma_e = 40$ dB, $N = 5$.

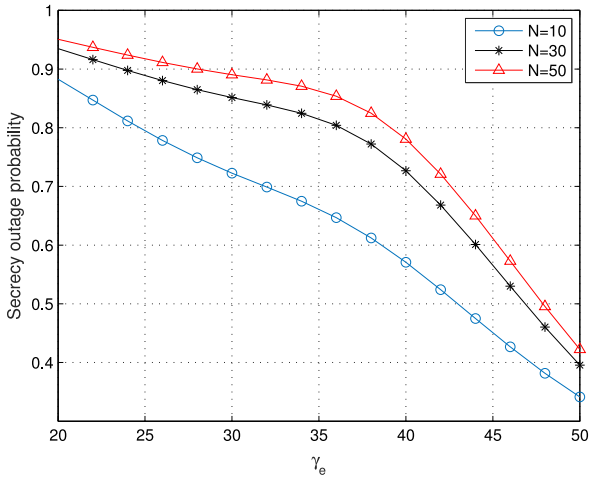

Fig. 3. Secrecy outage probability versus γ_e (dB) for $G_e = 15$ dB, $\lambda_2 = \lambda_3 = 30\lambda_1$.

causes an increase in the secrecy outage. An interesting observation is that with highly directional beamforming antennas, the secrecy outage increases. This happens because, although highly directional beamforming at mmWave tier prompts enhanced coverage probability at the legitimate users, but the eavesdroppers nodes will also benefit with having higher gains. Henceforth, there is a more possibility that their SINR goes above the predefined threshold limit. Thus, the confidential information secrecy may be compromised. The result demonstrates the existence of a tradeoff pinpointing that it is unrealistic to use high directional beams at mmWave BSs to improve connection outage while overlooking its effect on secrecy outage. Moreover, analytical results have been shown to be in close agreement with the theoretical results.

Fig. 2 shows the effects of the density of eavesdropper nodes on the behavior of secrecy outage probability, obtained using (49), for different small cell BS densities and directional antenna gains at the eavesdroppers. We see that by increasing the eavesdroppers density, the secrecy outage probability increases implying that a large number of eavesdroppers harm the network secrecy. However, the secrecy of the network increases with an increase in the small cell BS density. This is due to the fact that higher small cell density results in higher overall network interference prompting uncertainty at any eavesdropper and its SINR falls below the threshold, i.e., secrecy outage probability improves. Moreover, by keeping the small cell density fixed, lower directional antenna gains at the eavesdropper improves the secrecy capacity of the network transmissions. To summarize, the lower directional gain and increased cell density collectively negates the possibility of eavesdroppers' SINR being above the threshold.

Fig. 3 illustrates the secrecy outage probability, obtained using (49), versus the threshold for varying number of antennas at the MBSs. We see that the secrecy outage probability increases with the number of antennas at MBS. This is due to the fact that MBSs have higher transmission power in contrast to the small cell BSs resulting in better transmission at legitimate as well as eavesdropper nodes, therefore, eavesdroppers are more likely to have SINR well above threshold. Moreover,

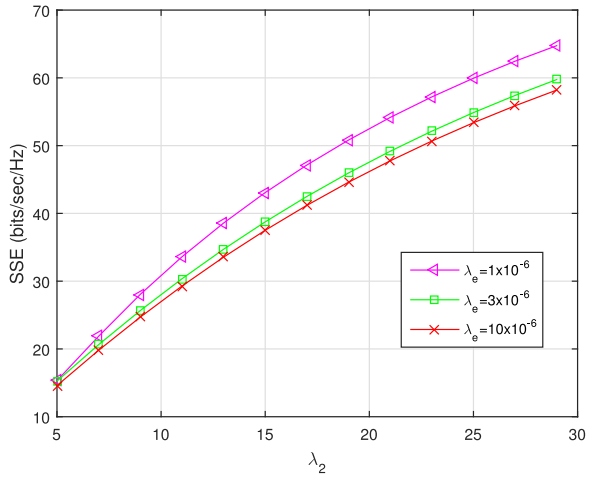

Fig. 4. SSE versus varying small cells BS density as multiple of MBS density for $\lambda_3 = \lambda_2$, $G_e = 15$ dB, $N = 40$, $U = 5$.

MBSs give higher array gains at higher antenna density and the users are more averse to be offloaded to small cells. Hence the interference of the network drops that prompts less uncertainty at the eavesdroppers. Further, the figure shows that there is no huge increment in secrecy outage probability after the number of antennas is increased past a certain limit due to the fact that the user association with tiers does not have any significant variation.

Fig. 4 shows the effects of varying small cells BS density of tier 2 and tier 3 on SSE. We observe that the SSE of the network increases with the density of small cells and it decreases slightly when the density of eavesdropper nodes increases. The SSE of the network elevates because with increased small cell density, the average cell radius decreases and more users are offloaded to small cells leading to better transmission to the intended legitimate user. With a decrease in the cell sizes, the distance between the intended user and the transmitting nodes decreases prompting stronger links between them and hence achieving higher secrecy rate. As for the mmWave cells, the LoS probability function $p(R)$, is a function

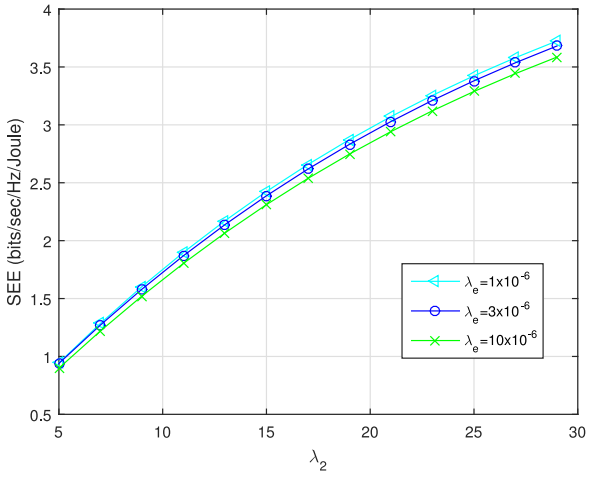

Fig. 5. SEE versus varying small cells BS density as multiple of MBS density for $\lambda_3 = \lambda_2$, $G_e =$ 15 dB, $N = 30$, $U = 5$.

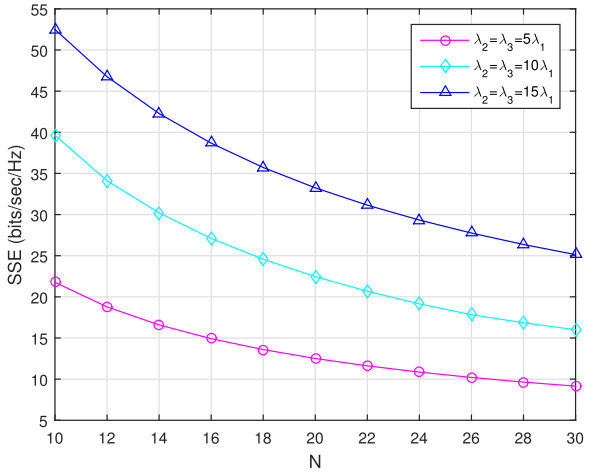

Fig. 6. SSE versus different number of antennas at macro BS for $G_e = 15$ dB, $U = 5$.

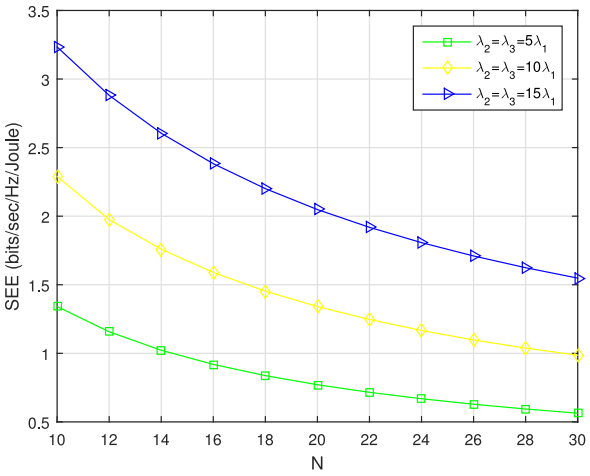

Fig. 7. SEE versus different number of antennas at macro BS for $G_e = 15$ dB, $U = 5$.

of distance, therefore, when distance decreases, LoS association probability increases such that the users are now more likely to form low path loss LoS links with mmWave BSs than NLoS links. The association of users with MBSs declines though they are high power entities but have low BS density than the small cells. Moreover, interference in the network increases because of super dense transmitting nodes which is why the increase in eavesdroppers density has insignificant impact on SSE.

Fig. 5 includes the plots for SEE, given by (51), versus the small cells density. We observe that with increasing λ_2 and λ_3, the SEE also increases. This can be attributed to the increasing SSE, shown in Fig. 4, over the identical power consumption. With increasing λ_2 and λ_3, more users are offloaded to small cell BSs that are low power nodes compared to macro cells BSs. This may lead to a power efficient network but it comes at small cell BSs deployment cost. Thus, the elevation of average achievable secrecy rate leads to improvement of SEE. As the interference in the network increases because of super dense transmitting nodes, therefore, an increase in eavesdroppers density has no prominent effect on SEE.

Fig. 6 shows the effects of number of transmitting antennas at the MBS on the SSE of the proposed three tier network over different small cell densities. We see that the network SSE drops with increasing number of transmitters at MBSs and it improves significantly with increased small cell density. This occurs because with increased *N*, radio spectral efficiency of MBSs increases but since MBSs have higher transmission power in contrast to small cell BSs therefore transmission to eavesdropper nodes in the network improves significantly that elevates R^e. Moreover, with increase in number of antennas at MBSs, cell association gets biased towards them because of their high array gains, and few users connect with BSs of sub-6 GHz and mmWave small cells. In this way the overall interference in the network drops leading to better reception at eavesdropper nodes.

In Fig. 7, we see the variation in SEE of the network given by (51) with increasing number of antennas at MBSs and we observe that with increasing *N*, SEE declines. This is due to the fact that SSE decreases over the identical power consumption, as shown in Fig. 6. With increase in transmitting nodes at MBSs, less users are offloaded to small cells. Since MBSs have higher transmission power as compared to the small cell BSs leading to a power inefficient network. Thus SEE drops with the elevation of average achievable rate at eavesdropper nodes. Interference in the network increases with small cell density that leads to drop in R^e thus SEE improves with it.

Fig. 8 shows the effects of transmitting power of small cell BSs on the SSE of the assumed three tier network over different small cell densities. It is observed that the SSE of the network improves with the small cells BSs transmit power and improvement becomes more significant as the small cell BSs density is increased. The reason is that since small cells have smaller coverage area, associated users are located at distance closer to BSs, therefore when BSs transmit power is increased, they get to deliver stronger signal strength with low path loss to the associated users that enhances the average achievable rate of the legitimate users. This results in significant enhancement of secrecy rate of the entire network. Average distance between transmitting and receiver nodes decreases when small

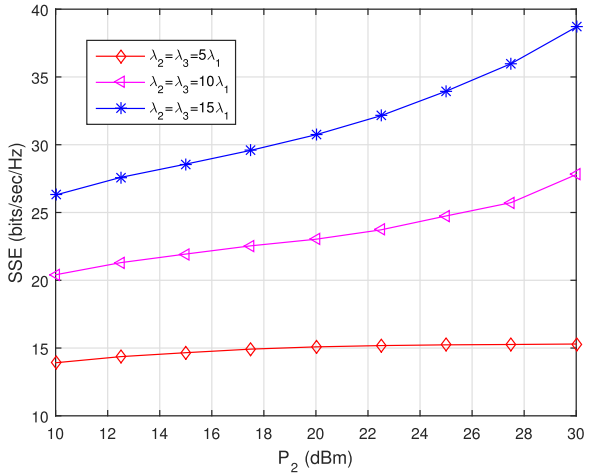

Fig. 8. SSE versus transmit power of small cells BSs for $P_3 = P_2$, $G_e = 15$ dB, $U = 5$, $N = 30$.

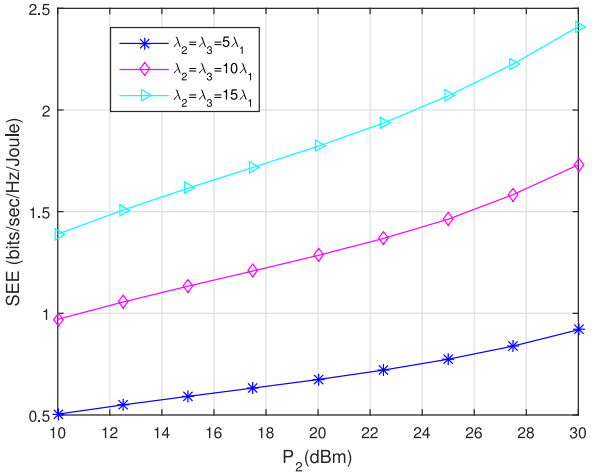

Fig. 9. SEE versus transmit power of small cells BSs for $P_3 = P_2$, $G_e = 15$ dB, $U = 5$, $N = 30$.

cells become more dense that enhances the transmission rate between them. This justifies the increase in SSE with increase in small cell density.

In Fig. 9, we see the variation in SEE of the network given by (51) with increasing transmit power of small cell BSs and we observe that with increasing P_2 and P_3, SEE inclines. This can be attributed to the increase in SSE over the identical power consumption, as shown in Fig. 8. Since small cells BSs are lower power nodes compared to MBSs therefore, this prompts a power efficient network.

V. Conclusion

In this paper, considering the unique features of massive MIMO and mmWave communication, we concentrated on characterizing the secure communication in massive MIMO-enabled three tier hybrid HetNet by using PLS. We derived the secrecy outage probability and achievable ergodic rate at each network tier and eavesdropper. A tractable approach was developed to evaluate network-wide SSE and SEE. Simulation results highlight the impact of number of antennas at MBS, transmit power, node density, antenna gains and eavesdroppers density on secrecy performance. Study has revealed that at low transmit power operation, secrecy performance enhances at higher small cell density. We have found that when node density is high, network-wide interference elevates that dominates the secrecy performance. Moreover, higher gains at mmWave cells lead to a drop in secrecy performance thus a tradeoff exists between better coverage and secrecy. Number of antennas at MBS cannot be increased beyond limit as it may lead to deterioration of secrecy performance of the overall network. Therefore, the number of antennas at the massive MIMO macro cells and directivity gains at mmWave cells need to be carefully analyzed and chosen for secrecy performance enhancement of the entire network.

Appendix A
Detailed Derivation of Association Probability and PDF of Distance

Proof of Association Probability: Using [38, Lemma 3], we donate k as the tier index with which legitimate user connects. When $P_{r,l} > P_{r,n}$ for $n \in \{1,2,3\}$ and $n \neq l$ a typical user associates with l^{th} tier, i.e., $k = l$. Therefore,

$$\begin{aligned} A_l &= \mathbb{P}[k=l] = \mathbb{E}_{R_l}\left[\mathbb{P}[P_{r,l} > \max_{n,n\neq l} P_{r,n}]\right] \\ &= \mathbb{E}_{R_l}\left[\prod_{n=1,n\neq l}^{3} \mathbb{P}[P_{r,l} > P_{r,n}]\right] \\ &\overset{(a)}{=} \mathbb{E}_{R_l}\left[\prod_{n=1,n\neq l}^{3} \mathbb{P}\left[R_n > \left(\frac{\overline{P_n} G_n R_l^{\alpha_l}}{\overline{P_l} G_l}\right)^{\frac{1}{\alpha_n}}\right]\right] \\ &= \int_0^\infty \underbrace{\left[\prod_{n=1,n\neq l}^{3} \mathbb{P}\left[R_n > \left(\frac{\overline{P_n} G_n R_l^{\alpha_l}}{\overline{P_l} G_l}\right)^{\frac{1}{\alpha_n}}\right]\right]}_{\Omega} f_{R_l}(x)\,dx, \end{aligned} \tag{A.1}$$

where (a) is based on Section II-B. The probability $\mathbb{P}[R_n > (\frac{\overline{P_n} G_n R_l^{\alpha_l}}{\overline{P_l} G_l})^{\frac{1}{\alpha_n}}]$ is evaluated using the null probability for a 2-D PPP given by, $\exp\{-\lambda A\}$, where λ donates density of PPP in area A.

$$\begin{aligned} \Omega &= \prod_{n=1,n\neq l}^{3} \mathbb{P}\left[\text{BS no nearer than}\left(\frac{\overline{P_n} G_n x^{\alpha_l}}{\overline{P_l} G_l}\right)^{\frac{1}{\alpha_n}} \text{in } n^{th}\text{tier}\right] \\ &= \left(\prod_{n=1,n\neq l}^{2} \exp\left\{-\lambda_n \pi \left(\frac{P_n x^{\alpha_l}}{P_l}\right)^{\frac{2}{\alpha_n}}\right\}\right) \\ &\quad + \exp\{-2\pi\lambda_3 D(x)\}, \end{aligned} \tag{A.2}$$

$$f_{R_l}(x) = 2\lambda_l \pi x \exp\left\{-\lambda_l \pi x^2\right\}. \tag{A.3}$$

For the mmWave tier case, let us assume $q \in \{L, N\}$, $R_{3,q}$ be the distance of typical user to the closest BS in $\Phi_{3,q}$. Since, transmission power is same for all links of tier 3 therefore association of typical user to $\Phi_{3,q}$ is based on link length.

Since mmWave BSs are assumed as independent tiers of LoS and NLoS BSs therefore,

$$\begin{aligned} &W(x)\\ &= \mathbb{P}[P_{r,l} > P_{r,3}]\\ &= \mathbb{P}[P_{r,l} > \overline{P_3} G x^{-\alpha_L}]\mathbb{P}[P_{r,l} > \overline{P_3} G x^{-\alpha_N}]\\ &= \mathbb{P}\left[x > \left(\frac{\overline{P_3}G}{\overline{P_l}}\right)^{\frac{1}{\alpha_L}} x^{\frac{\alpha_l}{\alpha_L}}\right]\mathbb{P}\left[x > \left(\frac{\overline{P_3}G}{\overline{P_l}}\right)^{\frac{1}{\alpha_N}} x^{\frac{\alpha_l}{\alpha_N}}\right]\\ &\overset{(a)}{=} \exp\left\{-2\lambda_3\pi\left(\underbrace{\int_0^{\delta_N(x)} tp(t)dt + \int_0^{\delta_L(x)} t(1-p(t))dt}_{D(x)}\right)\right\}, \end{aligned} \tag{A.4}$$

where $\delta_N(x) = (\frac{\overline{P_3}G}{\overline{P_l}})^{\frac{1}{\alpha_L}} x^{\frac{\alpha_l}{\alpha_L}}$, $\delta_L(x) = (\frac{\overline{P_3}G}{\overline{P_l}})^{\frac{1}{\alpha_N}} x^{\frac{\alpha_l}{\alpha_N}}$ and (a) follows from null probability with ball centered at origin having radius $\delta_N(x)$ and $\delta_L(x)$ respectively, and $p(t)$ is the LoS probability function. Similarly, by substitution of $D(x)$ from (A.4) and $f_{R_l}(x)$ from (A.3) into (A.2), A_1, A_2 and A_3 can be computed.

Proof of PDF of distance: For any tier k for $k \in \{1, 2, 3\}$

$$\begin{aligned} &\mathbb{P}[X_k > x]\\ &= \frac{\mathbb{P}[R_k > x, \text{userassociatedwithtier}k]}{\mathbb{P}[\text{userassociatedwithtier}k]}.\\ &\mathbb{P}[X_k > x]\\ &= \frac{2\pi\lambda_k \int_x^\infty \left(x\exp\left\{-\pi \sum_{j=1}^{2} \lambda_j \left(\frac{\overline{P_j} x^{\alpha_k}}{\overline{P_k}}\right)^{\frac{1}{\alpha_j}}\right\} + D(x)\right) dx}{A_k} \end{aligned}$$

Hence, the conditional PDF of distance to serving BS, given that the user is connected with k^{th} tier, $f_{X_k}(x)$ can be evaluated as

$$f_{X_k}(x) = \frac{d}{dx}(1 - \mathbb{P}[X_k > x]),$$

with it, PDF of distance for each tier are evaluated. Association probability per tier is strongly affected by the transmit power of BSs of each tier, number of antennas at MBS and small cells BS density.

Appendix B
Derivation of Lemma 1

The average rate, R_1^e, is calculated as,

$$R_1^e = \frac{1}{\ln 2} \int_0^\infty \frac{1 - P_{so}^1(\gamma_e)}{1 + \gamma_e} d\gamma_e, \tag{B.1}$$

where

$$\begin{aligned} P_{so}^1(\gamma_e) &= \Pr(\text{SINR}_M^e < \gamma_e) = 1 - \Pr(\text{SINR}_1^e > \gamma_e)\\ &\overset{(a)}{=} 1 - \mathbb{E}_{\Phi_1}\left[\mathbb{E}_{\Phi_e}\left[\prod_{e\in\Phi_e} (1 - \Pr(\text{SINR}_M^e > \gamma_e))\right]\right]\\ &\overset{(b)}{=} 1 - \mathbb{E}_{\Phi_1}\left[\exp\left[-\lambda_e \int_{\mathbb{R}^2} \Pr(\text{SINR}_M^e > \gamma_e) de\right]\right], \end{aligned} \tag{B.2}$$

where (b) gives the upper bound on (a) by using independence of fading at each eavesdropper and generating functional of PPP. Taking the integral expression from (B.2),

$$\begin{aligned} &= \int_0^\infty \Pr\left(\frac{\hat{P}_1 h_{e,M} r_e^{-\alpha_1}}{\sigma^2 + \underbrace{\sum_{j\in\overline{\Phi}_1} \frac{\overline{P_1}}{U} h_{j,M} L_{j,M}(x_j)}_{I_M} + I_S} > \gamma_e\right)\\ &= \int_0^\infty \Pr\left(h_{e,M} > \frac{\gamma_e r_e^{\alpha_1}(\sigma^2 + I_M + I_S)}{\hat{P}_1}\right)\\ &\overset{(a)}{=} \sum_{i=1}^{N} \binom{N}{i} (-1)^{i+1} \int_0^\infty r_e \left(\exp\left\{-\frac{i\gamma_e r_e^{\alpha_1}\sigma^2}{\hat{P}_1}\right\}\right)\\ &\quad \times \mathcal{L}\left(\exp\left\{-\frac{\gamma_e r_e^{\alpha_1} I_M}{\hat{P}_1}\right\}\right)\mathcal{L}\left(\exp\left\{-\frac{\gamma_e r_e^{\alpha_1} I_S}{\hat{P}_1}\right\}\right) dr_e, \end{aligned} \tag{B.3}$$

where (a) follows from exponential distribution of $h_{e,M}$, binomial expansion and independence of I_M and I_S.

The average achievable ergodic rate at the eavesdropper is strongly affected by MBS transmit power and its distance from MBS. For the macro tier,

$$\begin{aligned} &\mathcal{L}_{I_M}(e)\\ &= \mathbb{E}\left[\exp\left(-e \sum_{j\in\overline{\Phi}_1} \frac{\overline{P_1}}{U} h_{j,M} L_{j,M}(x_j)\right)\right]\\ &\overset{(a)}{=} \exp\left(-\int_x^\infty \left(1 - \mathbb{E}_{h_{j,M}}\left[\mathrm{e}^{-e\frac{\overline{P_1}}{U} h_{j,M} t^{-\alpha_1}}\right]\right)\lambda_1 2\pi t dt\right)\\ &\overset{(b)}{=} \exp\left(-\lambda_1 2\pi \sum_{c=1}^{U} \binom{U}{c} \int_x^\infty \frac{\left(\frac{\overline{P_1}}{U} e t^{-\alpha_1}\right)^c}{\left(1 + \frac{\overline{P_1}}{U} e t^{-\alpha_1}\right)^U} t dt\right), \end{aligned} \tag{B.4}$$

where the generating functional of PPP is used to get (a) and binomial expansion to arrive at (b) and $e = \exp\{-\frac{\gamma_e r_e^{\alpha_1} I_M}{\hat{P}_1}\}$.

Similarly, $\mathcal{L}_{I_S}(e)$ is the Laplace transform of the PDF of interference from the sub-6 GHz small cell tier is evaluated as follows

$$\begin{aligned} &\mathcal{L}_{I_S}(e)\\ &= \mathbb{E}\left[\exp\left(-e \sum_{q\in\overline{\Phi}_2} \overline{P_q} h_q L_q(x_q)\right)\right]\\ &= \exp\left(-2\pi\lambda_2 \int_{\left(\frac{\overline{P_2}U}{(N-U+1)\hat{P}_1}\right)^{\frac{1}{\alpha_2}}}^\infty x^{\frac{\alpha_1}{\alpha_2}} \left(\frac{e\overline{P_2} t^{-\alpha_2}}{1 + e\overline{P_2} t^{-\alpha_2}}\right) t dt\right), \end{aligned} \tag{B.5}$$

where lower limit of integral is the distance between the typical user and the nearest BS of sub-6 GHz small cell tier.

By substituting (B.4) and (B.5) into (B.3), the R.H.S of (B.3) can be rewritten as

$$\begin{aligned}&\int_{\mathbb{R}^2}\Pr(\mathrm{SINR}_M^e>\gamma_e)\\&=\sum_{i=1}^{N}\binom{N}{i}(-1)^{i+1}\int_0^{\infty}r_e\exp\Bigg(-\frac{i\gamma_e r_e^{\alpha_1}\sigma^2}{\hat{P}_1}\\&\quad\overbrace{-2\pi\lambda_1\sum_{c=1}^{U}\binom{U}{c}\int_x^{\infty}\frac{\left(\frac{\overline{P_1}}{U}et^{-\alpha_1}\right)^c}{\left(1+\frac{\overline{P_1}}{U}et^{-\alpha_1}\right)^U}tdt}^{\zeta_1^1}\\&\quad\underbrace{-2\pi\lambda_2\int_{\left(\frac{\overline{P_2}U}{(N-U+1)\overline{P_1}}\right)^{\frac{1}{\alpha_2}}x^{\frac{\alpha_1}{\alpha_2}}}^{\infty}\left(\frac{e\overline{P_2}t^{-\alpha_2}}{1+e\overline{P_2}t^{-\alpha_2}}\right)tdt\,dr_e}_{\zeta_2^1},\end{aligned}\tag{B.6}$$

(B.2) can be rewritten as follow:

$$\begin{aligned}P_{so}^1(\gamma_e)&=1-\mathbb{E}_{\Phi_1}\left[\exp\left[-\lambda_e\int_{\mathbb{R}^2}\Pr(\mathrm{SINR}_M^e>\gamma_e)de\right]\right]\\P_{so}^1(\gamma_e)&=1-\exp\left(-2\pi\lambda_e\int_{\mathbb{R}^2}\Pr(\mathrm{SINR}_M^e>\gamma_e)de\right),\end{aligned}\tag{B.7}$$

The final expression of (16) is obtained by substituting the closed form expression of integral from (B.6) in (B.7) and changing the variables $e=u$.

Appendix C
Derivation of Lemma 2

The average achievable ergodic rate at the typical user associated with MBS can be defined as

$$\begin{aligned}R_1=\mathbb{E}[\log_2(1+\mathrm{SINR}_M^u)]&=\frac{1}{\ln 2}\int_0^{\infty}\frac{P_C^1(\gamma)}{1+\gamma}d\gamma\\&=\frac{1}{\ln 2}\int_0^{\infty}\frac{\int_0^{\infty}P_C^1(\gamma,x)f_{X_1}(x)dx}{1+\gamma}d\gamma\end{aligned}\tag{C.1}$$

Conditional coverage probability $P_C^1(\gamma,x)$ can be computed as,

$$\begin{aligned}&P_C^1(\gamma,x)\\&=\Pr\left(\frac{\frac{\overline{P_1}}{U}h_{o,M}L_{o,M}(x)}{\sigma^2+\underbrace{\underbrace{\sum_{j\in\overline{\Phi_1}}\frac{\overline{P_1}}{U}h_{j,M}L_{j,M}(x_j)}_{I_1}+I_S}_{I}}>\gamma\right)\\&=\int_0^{\infty}\Pr\left(h_{o,M}>\frac{x^{\alpha_1}U\gamma(\sigma^2+T)}{\overline{P_1}}\right)d\Pr(I_1\le T)\\&=\int_0^{\infty}e^{-\frac{x^{\alpha_1}U\gamma\left(\sigma^2+T\right)}{\overline{P_1}}}\sum_{j=0}^{N-U}\frac{\left(\frac{x^{\alpha_1}U\gamma\left(\sigma^2+T\right)}{\overline{P_1}}\right)^j}{j!}d\Pr(I_1\le T).\end{aligned}\tag{C.2}$$

By using change of variables $y=x^{\alpha_1}$, expanding the derivative in (C.2) it can be rewritten as

$$P_C^1(\gamma,x)=\sum_{j=0}^{N-U}\frac{(x^{\alpha_1})^j}{j!(-1)^j}\frac{d^j}{dy^j}\left[e^{-\frac{yU\gamma\sigma^2}{\overline{P_1}}}\mathcal{L}_I\left(\frac{yU\gamma}{\overline{P_1}}\right)\right],\tag{C.3}$$

where $\mathcal{L}_I(e)$ is product of Laplace transform of the PDF of interference from macro tier and sub-6 GHz small cell tier. On combining (B.4) and (B.5), we get $\mathcal{L}_{I(e)}=\exp(\Xi(e))$ given by (15) [24] and on substituting it in (C.3), using Faa di Bruno's formula, we get (14) [24] giving $P_C^1(\gamma,x)$. By substituting (C.3) into (C.1), we can calculate the average achievable ergodic rate at the typical user associated with MBS which completes the proof.

Appendix D
Derivation of Lemma 5

The average rate, R_3, is calculated as

$$R_3=\mathbb{E}[\log_2(1+\mathrm{SINR}_m^u)]=\frac{1}{\ln 2}\int_0^{\infty}\frac{P_C^3(\gamma)}{1+\gamma}d\gamma,\tag{D.1}$$

and based on thinning theorem, we evaluate the coverage probability separately for LoS and NLoS PPPs. Given that user is connected with BS in $\hat{\Phi}_3^q$ where $q\in\{L,N\}$, the conditional coverage probability is computed as

$$P_C^{3,q}(\gamma)=A_{3,q}\int_0^{\infty}\mathbb{P}\left[\frac{\overline{P_3}M_rM_th_{o,m}x^{-\alpha_q}}{\sigma^2+I_L+I_N}>\gamma\right]f_q(x)dx,\tag{D.2}$$

where

$$\begin{aligned}A_{3,L}=2\pi\lambda_3\int_0^{\infty}&xp(x)\exp\{(-2\pi\lambda_3M(x)\\&-Z(x)-Y(x))\}\end{aligned}$$

$M(x)=(\int_0^x tp(t)dt+\int_0^{x^{\frac{\alpha_L}{\alpha_N}}}(1-p(t))tdt)$, $Z(x)=\pi\lambda_1(\frac{\overline{P_1}(N-U+1)x^{\alpha_L}}{\overline{P_3}U})^{2/\alpha_1}$ and $Y(x)=\pi\lambda_2(\frac{\overline{P_2}Ux^{\alpha_1}}{\overline{P_1}(N-U+1)})^{2/\alpha_2}$

$$A_{3,N}=1-A_1-A_2-A_{3,L}$$

are the probabilities of typical user connecting with LoS or NLoS link.

Here, $f_N(x)=\frac{2\pi\lambda_3x(1-p(x))}{A_{3,L}}\exp\{-2\pi\lambda_3\int_0^x t(1-p(t))dt+\int_0^{\delta_N(x)}tp(t)dt\}$ is the conditioned PDF of the distance between the typical user to the NLoS mmWave BS and $f_L(x)=\frac{2\pi\lambda_3xp(x)}{A_{3,N}}\exp\{-2\pi\lambda_3\int_0^x tp(t)dt+\int_0^{\delta_L(x)}t(1-p(t))dt\}$ is the conditioned PDF of the distance between the typical user to the LoS mmWave BS [35].

Where $I_L=\overline{P_3}\sum_{i\in\hat{\Phi}_3^L,m}G_lh_{i,m}R_i^{-\alpha_L}$ and $I_N=\overline{P_3}\sum_{i\in\hat{\Phi}_3^N,m}G_lh_{i,m}R_i^{-\alpha_N}$ are the interference strengths from

LoS and NLoS BSs, respectively. Since we assumed the Nakagami fading therefore, $h_{o,m}$ is a normalized gamma random variable with parameter N_q, we obtain the approximation

$$
\begin{aligned}
&= \mathbb{P}\Big[\overline{P_3} M_r M_t h_{o,m} x^{-\alpha_q} > \gamma\Big(\sigma^2 + I_L + I_N\Big)\Big] \\
&= \mathbb{P}\left[h_{o,m} > \frac{x^{\alpha_q}\gamma\big(\sigma^2 + I_L + I_N\big)}{\overline{P_3} M_r M_t}\right] \\
&\overset{(a)}{=} 1 - \mathbb{E}\left[\left(1 - \exp\left(-\frac{\eta_q x^{\alpha_q}\gamma\big(\sigma^2 + I_L + I_N\big)}{\overline{P_3} M_r M_t}\right)\right)^{N_q}\right] \\
&\overset{(b)}{=} \sum_{j=1}^{N_q} (-1)^{j+1} \binom{N_q}{j} \\
&\mathbb{E}\left[\exp\left(-\frac{j\eta_q x^{\alpha_q}\gamma\big(\sigma^2 + I_L + I_N\big)}{\overline{P_3} M_r M_t}\right)\right] \\
&\overset{(c)}{=} \sum_{j=1}^{N_q} (-1)^{j+1} \binom{N_q}{j} \mathrm{e}^{-\frac{j\eta_q x^{\alpha_q}\gamma\sigma^2}{\overline{P_3} M_r M_t}} \\
&\mathbb{E}_{I_L}\left[\mathrm{e}^{-\frac{j\eta_q x^{\alpha_q}\gamma I_L}{\overline{P_3} M_r M_t}}\right] \mathbb{E}_{I_N}\left[\mathrm{e}^{-\frac{j\eta_q x^{\alpha_q}\gamma I_N}{\overline{P_3} M_r M_t}}\right],
\end{aligned}
\tag{D.3}
$$

where (a) follows from [35, Lemma 6] and $\eta_q = N_q(N_q!)^{-\frac{1}{N_q}}, q \in \{L, N\}$, (b) from binomial expansion and (c) from the independence of Φ_3^L and Φ_3^N PPPs. Now calculating $\mathbb{E}_{I_L}$ for $q = L$ we have

$$
\begin{aligned}
&= \mathbb{E}_{I_L}\left[\mathrm{e}^{-\frac{j\eta_L x^{\alpha_L}\gamma\sum_{i\in\overline{\Phi}_3^L} G_l h_{i,m} R_i^{-\alpha_L}}{M_r M_t}}\right] \\
&\overset{(d)}{=} \mathrm{e}^{-2\pi\lambda_3 \sum_{i=1}^{4} p_i \int_x^\infty \left(1 - \mathbb{E}_g\left[\mathrm{e}^{-j\eta_L x^{\alpha_L}\gamma g \hat{a}_i t^{-\alpha_L}}\right]\right) p(t) t dt} \\
&\overset{(e)}{=} \prod_{i=1}^{4} \mathrm{e}^{-2\pi\lambda_3 p_i \int_x^\infty \left(1 - 1/\left(j\eta_L \hat{a}_i \gamma (x/t)^{\alpha_L} N_L^{-1}\right)^{N_L}\right) p(t) t dt},
\end{aligned}
\tag{D.4}
$$

where (d) is obtained by Laplace transform of $\overline{\Phi}_3^L$ [35], g in (d) is a normalized Gamma random variable with parameter N_L, $\hat{a}_i$ is the gain a_i normalized by $M_r M_t$ where a_i and p_i are given by (2) and (e) is the outcome of computing moment generating functional of g, respectively.

Likewise, calculation of $\mathbb{E}_{I_N}$ is similar where channel gain is the normalized Gamma random variable with parameter N_N. Final expression is given as

$$
= \prod_{i=1}^{4} \mathrm{e}^{-2\pi\lambda_3 p_i \int_{\delta_L(x)}^\infty \left(1 - 1/\left(j\eta_L \hat{a}_i \gamma (x)^{\alpha_L} N_N^{-1} t^{-\alpha_N}\right)^{N_N}\right)(1 - p(t)) t dt}.
\tag{D.5}
$$

Thus we obtain (26) from (D.4) and (D.5) by combining them using linearity of integrals where $\overline{\delta}_L(x) = x^{\frac{\alpha_L}{\alpha_N}}$. For $q = N$, exactly similar steps are followed to obtain (27) which are not outlined here due to the space limitations.

REFERENCES

[1] A. Umer, S. A. Hassan, H. Pervaiz, Q. Ni, L. Musavian, and S. H. Ahmed, " Secrecy outage analysis for massive MIMO-enabled multi-tier 5G hybrid HetNets," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Kansas City, MO, USA, 2018, pp. 1–6.

[2] A. Umer, "Stochastic modeling and performance analysis of multi-tier HetNets," M.S. thesis, School Elect. Eng. Comput. Sci., Nat. Univ. Sci. Technol., Islamabad, Pakistan, 2017.

[3] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[4] J. Zhang, X. Ge, Q. Li, M. Guizani, and Y. Zhang, "5G millimeter-wave antenna array: Design and challenges," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 106–112, Apr. 2017.

[5] J. Ye, X. Ge, G. Mao, and Y. Zhong, "5G ultradense networks with nonuniform distributed users," *IEEE Trans. Veh. Tech.*, vol. 67, no. 3, pp. 2660–2670, Mar. 2018.

[6] E. Turgut and M. C. Gursoy, "Energy efficiency in relay-assisted mmWave cellular networks," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Montreal, QC, Canada, Sep. 2016, pp. 1–5.

[7] M. Ding, P. Wang, D. López-Pérez, G. Mao, and Z. Lin, "Performance impact of LoS and NLoS transmissions in dense cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2365–2380, Mar. 2016.

[8] H.-M. Wang, T. Zhang, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[9] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[10] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[11] X. Ge, B. Du, Q. Li, and D. S. Michalopoulos, "Energy efficiency of multiuser multiantenna random cellular networks with minimum distance constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1696–1708, Feb. 2017.

[12] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[13] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[14] H. Wu, X. Tao, N. Li, and J. Xu, "Secrecy outage probability in multi-RAT heterogeneous networks," *IEEE Commun. Lett.*, vol. 20, no. 1, pp. 53–56, Jan. 2016.

[15] 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.

[16] 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.

[17] 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.

[18] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, Jr., "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *Proc. IEEE 15th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Toronto, ON, Canada, 2014, pp. 115–119.

[19] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3507–3519, Aug. 2016.

[20] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

[21] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2059–2071, Mar. 2017.

[22] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[23] Y. Hao, Q. Ni, H. Li, and S. Hou, "On the energy and spectral efficiency tradeoff in massive MIMO-enabled HetNets with capacity-constrained backhaul links," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4720–4733, Nov. 2017, doi: 10.1109/TCOMM.2017.2730867.
[24] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6437–6449, Dec. 2018.
[25] S. Kusaladharma, W.-P. Zhu, and W. Ajib, "Stochastic geometry-based modeling and analysis of massive MIMO-enabled millimeter wave cellular networks," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 288–301, Jan. 2019.
[26] K. Hosseini, W. Yu, and R. S. Adve, "Large-scale MIMO versus network MIMO for multicell interference mitigation," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 930–941, Oct. 2014.
[27] M. S. Omar, M. A. Anjum, S. A. Hassan, H. Pervaiz, and Q. Niv, "Performance analysis of hybrid 5G cellular networks exploiting mmWave capabilities in suburban areas," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, 2016, pp. 1–6.
[28] A. Umer, S. A. Hassan, H. Pervaiz, Q. Ni, and L. Musavian, "Coverage and rate analysis for massive MIMO-enabled heterogeneous networks with millimeter wave small cells," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, 2017, pp. 1–5.
[29] C. Yang, J. Li, Q. Ni, A. Anpalagan, and M. Guizani, "Interference-aware energy efficiency maximization in 5G ultra-dense networks," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 728–739, Feb. 2017.
[30] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[31] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.
[32] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.
[33] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.
[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
[35] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.
[36] A. He, L. Wang, M. Elkashlan, Y. Chen, and K.-K. Wong, "Spectrum and energy efficiency in massive MIMO enabled HetNets: A stochastic geometry approach," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2294–2297, Dec. 2015.
[37] G. Auer *et al.*, "How much energy is needed to run a wireless network?" *IEEE Wireless Commun.*, vol. 18, no. 5, pp. 40–49, Oct. 2011.
[38] 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.
[39] 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.
[40] Y.-Y. Zhang, J.-K. Zhang, and H.-Y. Yu, "Physically securing energy-based massive MIMO MAC via joint alignment of multi-user constellations and artificial noise," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 829–844, Apr. 2018.
[41] H. Q. Ngo, L.-N. Tran, T. Q. Duong, M. Matthaiou, and E. G. Larsson, "On the total energy efficiency of cell-free massive MIMO," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 25–39, Mar. 2018.

Anum Umer received the B.E. degree in electrical (telecommunication) engineering and the M.S. degree in electrical engineering from the National University of Science and Technology (NUST), Pakistan, in 2015 and 2017, respectively, where she was a Research Associate with the System Analysis and Verification Lab, School of Electrical Engineering and Computer Science in 2018. She is currently a Research Engineer with the Research and Development Wing, Military College of Signals, NUST. Her broader area of research includes wireless communication.

Syed Ali Hassan (S'09–M'12–SM'17) received the B.E. degree (Hons.) in electrical engineering from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2004, the M.S. degree in electrical engineering from the University of Stuttgart, Stuttgart, Germany, in 2007, and the M.S. degree in mathematics and the Ph.D. degree in electrical engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2011. He was a Visiting Professor with Georgia Tech in 2017. He is currently an Associate Professor with the School of Electrical Engineering and Computer Science, NUST, where he is also the Director of the Information Processing and Transmission Research Group, which focuses on various aspects of theoretical communications. His research interest includes signal processing for communications.

Haris Pervaiz (S'09–M'09) received the M.Sc. degree in information security from the Royal Holloway University of London, Egham, U.K., in 2005, and the Ph.D. degree from the School of Computing and Communication, Lancaster University, Lancaster, U.K., in 2016, where he is currently working as a Lecturer with InfoLab21. He was a Research Fellow with the 5G Innovation Centre, University of Surrey, Guildford, U.K., from 2017 to 2018 and an EPSRC Doctoral Prize Fellow with the School of Computing and Communication, Lancaster University from 2016 to 2017. His current research interests include green heterogeneous wireless communications and networking, 5G and beyond, millimeter wave communication, and energy and spectral efficiency. He has been actively involved in projects, such as CROWN, CogGREEN, TWEETHER, and Energy proportional EnodeB for LTE-Advanced and Beyond and the DARE project, and an ESPRC funded project. He is an Associate Editor of IEEE ACCESS, an editorial board member of *Emerging Telecommunications Technologies* (Wiley), and an Associate Editor of *Internet Technology Letters* (Wiley).

Leila Musavian received the Ph.D. degree in telecommunications from Kings College London, U.K. She was a Lecturer with InfoLab21, Lancaster University from 2012 to 2016. She is currently working as a Deputy Pro-Vice-Chancellor for Research with the University of Essex and as a Reader of telecommunications with the School of Computer Science and Electronic Engineering, University of Essex. She was a Research Associate with McGill University from 2011 to 2012, a Research Associate with Loughborough University, U.K., from 2009 to 2010, and a Post-Doctoral Fellow with INRS-EMT, Canada, from 2006 to 2008. Her research interests lie in radio resource management for low latency communications, B5G/5G, mmWave communications, massive MIMO, and energy harvesting communications. She is an Editor of the IEEE TRANSACTIONS OF WIRELESS COMMUNICATIONS. She has been an Executive Editor of the *Transactions on Emerging Telecommunications Technologies* from 2016 to 2019. She was an Associate Editor of *Internet Technology Letters* (Wiley). She has been the Lead Chair UHS5G WP in IEEE Globecom in 2018, UHSLLS WP in IEEE WCNC 2019, and the URLLC Special Session in IEEE PIMRC 2018, the TPC Co-Chair of CorNer 2016 (in conjunction with ISWCS 2016), the mmWave 5G (STEMCOM 2016), and the TPC member of several conferences, including IEEE ICC, IEEE GLOBECOM, IEEE WCNC, IEEE ICCCN, IEEE PIMRC, and ChinaCom. She is currently the Workshop Co-Chair of VTC-Spring-2020 and the Wireless Communications Symposium Co-Chair for IEEE ICC 2021.

Qiang Ni (M'04–SM'08) received the B.Sc., M.Sc., and Ph.D. degrees in engineering from the Huazhong University of Science and Technology, China. He is currently a Professor and the Head of the Communication Systems Group, School of Computing and Communications, Lancaster University, Lancaster, U.K. His research interests include the area of future generation communications and networking, including green communications and networking, millimeter-wave wireless communications, cognitive radio network systems, nonorthogonal multiple access, heterogeneous networks, 5G and 6G, SDN, cloud networks, energy harvesting, wireless information and power transfer, IoT, cyber physical systems, AI and machine learning, big data analytics, and vehicular networks. He has authored or coauthored over 200 papers in the above areas. He was an IEEE 802.11 Wireless Standard Working Group Voting Member and a Contributor to the IEEE Wireless Standards.

Muhammad Ali Imran (M'03–SM'12) heads the Communications, Sensing and Imaging CSI Research Group, University of Glasgow. He is the Dean of the University of Glasgow, UESTC. He is an Affiliate Professor with the University of Oklahoma, USA, and a Visiting Professor with the 5G Innovation Centre, University of Surrey, U.K. He has over 20 years of combined academic and industry experience with several leading roles in multi-million pounds funded projects. He is a Professor of wireless communication systems with research interests in self organized networks, wireless networked control systems, and the wireless sensor systems. He has filed 15 patents; has authored/coauthored over 400 journal and conference publications; was an Editor of five books and author of more than 20 book chapters; and has successfully supervised over 40 postgraduate students at doctoral level. He has been a consultant to international projects and local companies in the area of self-organized networks. He has been interviewed by BBC, Scottish TV, and many radio channels on the topic of 5G technology. He is a fellow of IET and a Senior Fellow of HEA.