Physical Layer Security in 5G Hybrid Heterogeneous Networks

Anum Umer and Syed Ali Hassan

1 Introduction

The paradigm of communication is shifting toward fifth-generation (5G) technology as the increased traffic demands cannot be met with existing conventional sub-6 GHz communication. This is because today's era is saturated with widespread usage of smart devices and ever-increasing wireless data traffic. The 5G communication encompasses certain key enabler technologies at the physical layer that makes 5G networks plausible. This includes the massive multiple-input multiple-output (MIMO) technology and millimeter wave (mmW) communication, at 10 to 300 GHz radio frequency bands with bandwidth above 2 GHz, which are envisioned in conjunction with heterogeneous cellular networks (HetNets) [1, 2]. The HetNets provide enhanced coverage and throughput to the end users by operating in such a fashion that they create a layer of overlay deployment of small cells over the existing sub-6 GHz macro cells, thus, bringing network close to the user. Small cells consist of low-powered base stations (BS) with variable operating frequencies and communication ranges [3].

In HetNets, massive MIMO technology works by deploying a range of large-scale antenna arrays at the transmitting nodes to produce highly directional beam gains and optimal radio spectral efficiency [4]. Whereas mmW communication cells have limited coverage because of operation at smaller wavelength and higher path loss [5] due to sensitivity to blockages and severe propagation losses, however, the small wavelength of mmW communication allows placement of large array of antennas in small area; therefore, beamforming can be implemented to compensate

A. Umer · S. A. Hassan (✉)
School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan
e-mail: ali.hassan@seecs.edu.pk

D. N. K. Jayakody et al. (eds.), *5G Enabled Secure Wireless Networks*,
https://doi.org/10.1007/978-3-030-03508-2_4

for path losses, additional noise power, and out-of-cell interference [7]. It has been proved through measurements that there are significant differences in path loss of line-of-sight (LoS) and non-line-of-sight (NLoS) mmW propagation paths [2, 6].

Shifting the focus from coverage probability and achievable rate at the end user, in 5G communication, investigation of its secrecy and information integrity aspects has recently become an important discussion in both academia and industry. The subsequent discussion will aim to analyze the aspects of physical layer security (PLS) in massive MIMO-enabled hybrid HetNet with mmW small cells, since the physical layer security (PLS) presents an important, low complexity solution for protection of confidential information in complex networks and the aforementioned network presents a common deployment scenario for future 5G communication networks.

In this chapter, we study the PLS in three-tier hybrid HetNets with massive MIMO in macro tier and mmW frequency and sub-6 GHz small cells. Specifically, we analyze the performance of the proposed network, through analytical modeling and simulation, in terms of secrecy outage probability, secrecy spectral efficiency (SSE), and secrecy energy efficiency (SEE). The developed tractable approach of analysis of the network accounts for key features of mmW communication, massive MIMO technology, beamforming gains, number of transmitting antennas at BSs, and node densities. Secrecy outage probability modeling for each tier of the network is performed to quantify the effects of various system parameters on secrecy outage. Following it, tractable model is developed for achievable ergodic rate at the legitimate users and eavesdropper to model average achievable secrecy rate of the network. The SSE and SEE of massive MIMO-enabled three-tier hybrid HetNet are modeled and studied based on the aforementioned average achievable secrecy rate. Finally, with the help of numerical simulations, analytical models are verified, and relation between secrecy outage probability (SOP), SEE, SSE, key features of mmW communication, massive MIMO technology, beamforming gains, number of transmitting antennas at BSs, and node densities is studied.

2 Background

PLS in 5G communication networks is an emerging field of study in wireless technologies. In this respect, major research studies have been done in recent years. Liang et al. [9] and Wang et al. [10] have shown in their work the effects of fading on secrecy outage probability of the network. Wang et al. [8] and Wang et al. [11] investigated that the secrecy performance can be improved by degrading the eavesdropper channel with the help of techniques such as jamming, artificial noise, beam forming, and Wyner codes. Lv et al. [12] designed the techniques for spectrum allocation and transmit beamforming that can improve secrecy rate in two-tier HetNet. Wu et al. [13] stochastically modeled secrecy outage probability and throughout of a HetNet and studied the model for different system parameters. Wang et al. [14] proposed a mobile association policy, based on access threshold, for K-tier HetNet, and Deng

et al. [15] worked on secrecy rate in massive MIMO-enabled HetNets. Wang et al. [16] investigated jamming aspects of secrecy in a network where multiple antenna-aided transmitter transmits to a single-antenna user. Xu et al. [17] studied secrecy in HetNets based on coordinated multipoint scheme, and Wang et al. [18] derived and analyzed energy efficiency and secrecy rate in massive MIMO-based heterogeneous centralized radio access network (C-RAN) and showed that secrecy improves with both centralized and distributed large-scale antenna systems in such networks. All the aforementioned works are focused on PLS in conventional sub-6 GHz networks. Sharma et al. [19] present the novel methodology for secure exchange of 3D way points between unmanned aerial vehicles (UAVs), and Sharma et al. [20] discuss a DMM scheme for secure and energy-efficient handover between the mobile nodes in 5G communication empowered fog networks. Jameel et al. [21] studied the secrecy rate outage probability at the legitimate transmitter and receiver in the presence of eavesdroppers capable of energy harvesting and information decoding.

mmW communication has different propagation properties from sub-6 GHz communication, and investigation of its PLS properties is an emerging study. For instance, Wang et al. [22] studied the secrecy properties of point-to-point mmW link and showed that mmW systems have better secrecy as compared to the conventional systems. Vuppala et al. [23] derived the effects of blockages on secrecy rate of a networks with both sub-6 GHz and mmW frequency cells. Wang et al. [24] analyzed the secrecy outage probability in a mmW communication network with omnidirectional single-antenna-assisted users and eavesdroppers. Gong et al. [25] proposed a beamforming scheme for mmW communication networks to maximize their secrecy rate. This approach has been specifically developed for two-way amplify-and-forward MIMO relaying mmW networks. Umer et al. [26] studied the coverage and rate trends of a network with mmW base stations installed in combination with massive MIMO-enabled hybrid HetNets. Umer et al. [27] used stochastic geometry to model and discuss the secrecy outage probability aspects of aforementioned network model.

The rest of the chapter is organized as follows. We first develop the system model and channel model before proceeding to derive the analytical model for the secrecy outage probability, SEE, and SSE of the network. Subsequently, the numerical results for secrecy outage probability and other parameters are discussed. Finally we draw conclusion at the end of the chapter.

3 The System Layout

Consider a time-division duplex-based downlink transmission scenario of three-tier hybrid HetNet consisting of macro cells operating at sub-6 GHz at tier 1 and small cells operating at sub-6 GHz and mmW band at tier 2 and tier 3, respectively, as shown in Fig. 1. The BSs of each tier, legitimate users and eavesdroppers, are spatially distributed, following a two-dimensional homogeneous Poisson point process (HPPP) with intensity Φ_k and density λ_k where $k \in \{1, 2, 3\}$, Φ_u, and its

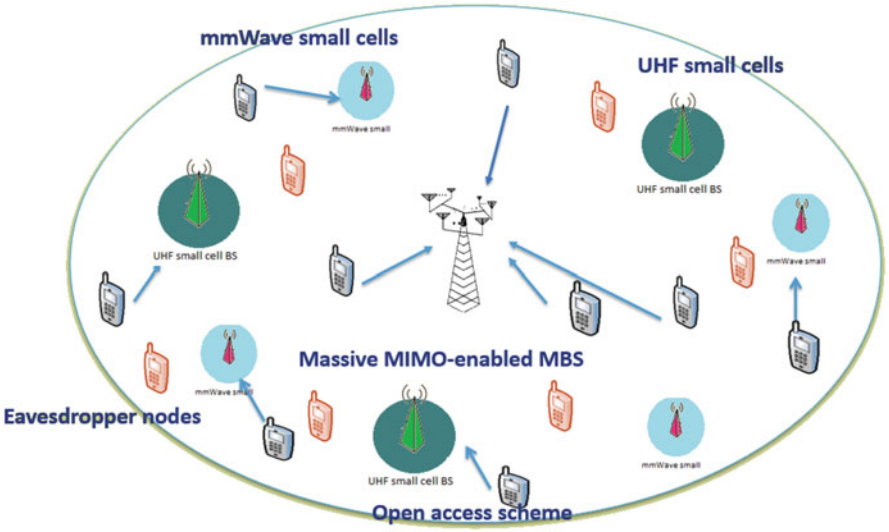

Fig. 1 Proposed three-tier massive MIMO-enabled hybrid HetNet with mmW small cells

density λ_u and Φ_e with density λ_e, respectively. Each BS of kth tier has transmit power P_k and path loss exponent α_k. Thus, the transmission from BS to the legitimate user takes place in the presence of spatially distributed eavesdroppers. The users and eavesdroppers are equipped with single omnidirectional antenna, and massive MIMO is implemented at macro cells where each macro base station (MBS) is equipped with multiple antennas forming an array, i.e., each MBS has N antennas that simultaneously transmit to U users ($N \gg U \geq 1$) with equal power distribution among all users [28]. Assume that channel state information (CSI) is known at the MBS that uses zero-forcing beamforming (ZFBF) to transmit U data streams [29]. Following Slivnyak's theorem, we perform the analysis of the network for a typical user located at the origin. A set of parameters used in this paper are outlined in Table 1.

Since mmW frequencies suffer significant path loss, therefore, directional beamforming is implemented at the mmW small cells BSs. We employ a sectored model to define the antenna pattern at the BSs of mmW tier such that constant array gains are assumed for the main lobes as well as the side lobes. Beam direction is uniformly distributed between $(0, 2\pi]$. The effective antenna gain, G_l, at a typical receiver, r, for an interferer, t, for possible directions $l = \{1, 2, 3, 4\}$ is given as

$$G_l = \begin{cases} a_l = M_r M_t & \text{with} \quad \text{prob.} \quad p_l = (\frac{\theta_r}{2\pi}\frac{\theta_t}{2\pi}) \\ a_l = M_r m_t & \text{with} \quad \text{prob.} \quad p_l = (\frac{\theta_r}{2\pi}(1 - \frac{\theta_t}{2\pi})) \\ a_l = m_r M_t & \text{with} \quad \text{prob.} \quad p_l = ((1 - \frac{\theta_r}{2\pi})\frac{\theta_t}{2\pi}) \\ a_l = m_r m_t & \text{with} \quad \text{prob.} \quad p_l = ((1 - \frac{\theta_r}{2\pi})(1 - \frac{\theta_t}{2\pi})), \end{cases} \tag{1}$$

Table 1 Table of nomenclature

Parameter	Description	Parameter	Description
λ_k	Tier k BS density	f_k	Operating frequency of kth tier
B_k	Bandwidth of kth tier	α_k	Path loss exponent of kth tier
λ_u	User density	P_k	kth tier BS transmission power
λ_e	Eavesdropper density	N	Number of antennas at MBS
U	Users served by a MBS	α_L	Patloss exponent of LoS mmW BS
α_N	Patloss exponent of NLoS mmW BS	N_N	Nakagami parameter at NLoS mmW BS
N_L	Nakagami parameter at LoS mmW BS	M_r	Main lobe gain at receiver
M_t	Main lobe gain at transmitter/ interferer	m_r	Side lobe gain at receiver
m_t	Side lobe gain at transmitter/ interferer	θ_r	Beamwidth at receiver
θ_t	Beamwidth at transmitter/ interferer	σ^2	Noise power
R_{Sk}	Average achievable secrecy rate at kth tier	β	Blockage density [30]
R_k	Achievable ergodic rate at user associated with kth tier	$SINR_k^u$	SINR at user associated with kth tier
$SINR_k^{e^*}$	SINR at most malicious eavesdropper associated with kth tier	P_k^{total}	Power consumption in kth tier

where M_j, θ_j, m_j, and p_l donate the main lobe gain, beamwidth, side lobe gain, and the probability of occurrence of certain gain G_l, where $j = \{t, r\}$. It is assumed that the typical transmitting BS, t, and receiver, r, are perfectly aligned; hence maximum directivity gain $M_r M_t$ can be achieved.

Following the legitimate typical user, antenna gain seen at the eavesdropper $e \in \Phi_e$ from serving BS, t, is defined as

$$G_e = \begin{cases} M_e M_t & \text{with} \quad \text{prob.} \quad \left(\frac{\theta_e}{2\pi}\frac{\theta_t}{2\pi}\right) \\ M_e m_t & \text{with} \quad \text{prob.} \quad \left(\frac{\theta_e}{2\pi}\left(1-\frac{\theta_t}{2\pi}\right)\right) \\ m_e M_t & \text{with} \quad \text{prob.} \quad \left(\left(1-\frac{\theta_e}{2\pi}\right)\frac{\theta_t}{2\pi}\right) \\ m_e m_t & \text{with} \quad \text{prob.} \quad \left(\left(1-\frac{\theta_e}{2\pi}\right)\left(1-\frac{\theta_t}{2\pi}\right)\right), \end{cases} \tag{2}$$

where M_e is the main lobe gain, m_e is the back lobe gain, and θ_e is the main lobe beamwidth at the eavesdropper e, respectively.

Analysis is performed for the typical user to whom mmW BS can form line-of-sight (LoS) or non-line-of-sight (NLoS) link. Moreover, we infer that the typical user at the origin will only form the LoS link to the mmW small cell BS when there is no blockage in path of their link. Thus, to define blockage model for mmW communication in this network, in accordance with independent thinning theorem,

we divide Φ_3 to Φ_3^L and $\Phi_3^N = \Phi_3/\Phi_3^L$, with densities $p(x)\lambda_3$ and $(1 - p(x))\lambda_3$, using LoS probability function $p(x)$, as independent PPPs of LoS and NLoS mmW small cells, respectively [30]. We define $p(x)$ as a probability measure that a link of length x is LoS, i.e., $1 - p(x)$ is NLoS probability of a link. Based on stochastic blockage models, $p(x)$ is given as $p(x) = e^{-\beta x}$ where β is dependent on statistics of blockages at a certain cell location and x is the measure of link distance from the serving BS to the typical user [31].

It is assumed that the small-scale fading in sub-6 GHz links is independent and identically distributed (i.i.d) and follows a Rayleigh distribution, whereas for mmW links, it is assume to be independent Nakagami fading with Nakagami fading parameter N_L and N_N for LoS and NLoS links, respectively. Nakagami fading parameters are considered as positive integers for ease of tractability [37].

An open access scheme for users' connectivity to BSs is assumed where user connects with any tier BS based on the maximum average received power. Thus, the typical user will connect to tier j if

$$j = \arg \max_{k \in \{1,2,3\}} \overline{P_k} L_k(x), \tag{3}$$

where $\overline{P_k} = \dfrac{P_k}{(\frac{4\pi}{\lambda_c})^2}$ and $L_k(x) = x_k^{-\alpha_k}$ are the normalized transmission power of the kth tier and path loss function. λ_c is the carrier wavelength and x is the link distance from typical user to serving BS.

We define the average received power at a typical user connected with the MBS tier as

$$P_{r,1} = G_M \frac{\overline{P_1}}{U} L_{j,M}(x), \tag{4}$$

where $G_M = (N - U + 1)$ is the array gain for ZFBF transmission and $L_{j,M}(x) = x_3^{-\alpha_3}$ is the path loss function [29]. Likewise, we define average received power at the typical user associated with small cell tier BS as

$$P_{r,i} = \overline{P_i} G_i L_i(x), \quad \text{where} \quad i \in \{2, 3\}, \tag{5}$$

where G_i is given as

$$G_i = \begin{cases} 1, \text{ sub} - 6\,\text{GHz small cell}, \\ G_l, \text{ defined in (1), mmW small cell}, \end{cases}$$

For the channel modeling of considered three-tier HetNet, we model the signal-to-interference-plus-noise ratio (SINR) for the entire network. It is assumed that the transmission channels of eavesdroppers and legitimate user are independent of each other, and distortion of eavesdropper channel with interference leads to enhanced

secrecy performance of overall network. We define most malicious eavesdropper for any transmission link as one with the highest received SINR; thus it dominates the secrecy rate. The SINRs discussed below are for the most malicious eavesdropper, i.e., $\text{SINR}_i^{e^*} = \max_{e \in \Phi_e} \{\text{SINR}_i^e\}$ where $i \in \{M, S, m\}$.

We define received SINR for a typical receiver and any eavesdropper connected with the MBS $b_{o,M}$ as

$$\text{SINR}_M^u = \frac{\frac{\overline{P_1}}{U} h_{o,M} L_{o,M}(x)}{\sigma^2 + \sum_{v \in \Phi_1 \setminus b_{o,M}} \frac{\overline{P_1}}{U} h_{v,M} L_{v,M}(x_v) + I_S}, \tag{6}$$

$$\text{SINR}_M^{e^*} = \frac{\frac{\overline{P_1}}{U} h_{e,M} r_e^{-\alpha_1}}{\sigma^2 + \sum_{v \in \Phi_1} \frac{\overline{P_1}}{U} h_{v,M} L_{v,M}(x_v) + I_S}, \tag{7}$$

where $L_s(x_s) = x_s^{-\alpha_2}$, $L_{o,M}(x) = x^{-\alpha_1}$, and $I_S = \sum_{s \in \Phi_2} \overline{P_2} h_s L_s(x_s)$ are the intercell interferences from sub-6 GHz small cells and $h_s \sim \exp(1)$, $h_{v,M} \sim \Gamma(U, 1)$, and $h_{o,M} \sim \Gamma(N - U + 1, 1)$ are the small-scale fading gains at the typical user from the interfering channel, interfering MBS, and from serving MBS for U users [29]. Here, $h_{e,M} \sim \exp(1)$ is fading gain at eavesdropper at the distance r_e from the serving BS, x_s and x_v are the distances between the receiver and small cell BS and receiver and MBS v, and σ^2 is the noise power.

We define the SINR of a typical receiver with link distance x and an eavesdropper with link distance r_e connected with the sub-6 GHz band small cell BS $b_{o,S}$ as

$$\text{SINR}_S^u = \frac{\overline{P_2} h_{o,S} L_{o,S}(x)}{\sigma^2 + \sum_{s \in \Phi_2 \setminus b_{o,S}} \overline{P_2} h_{s,S} L_{s,S}(x_s) + I_{\overline{\text{M}}}}, \tag{8}$$

$$\text{SINR}_S^{e^*} = \frac{\overline{P_2} h_{e,S} r_e^{-\alpha_2}}{\sigma^2 + \sum_{s \in \Phi_2} \overline{P_2} h_{s,S} L_{s,S}(x_s) + I_{\overline{\text{M}}}}, \tag{9}$$

where $L_{s,S}(x_s) = x_s^{-\alpha_2}$, $L_{o,S}(x) = x^{-\alpha_2}$, and $I_{\overline{\text{M}}} = \sum_{v \in \Phi_1} \frac{\overline{P_1}}{U} h_v L_v(x_v)$ are the intercell interferences from macro cells and $h_{s,S} \sim \exp(1)$, $h_{o,S} \sim \exp(1)$, $h_{e,S} \sim \exp(1)$, and $h_j \sim \Gamma(U, 1)$ are the small-scale fading gains from the interfering channel. Here, x_s and x_v are the link distance between typical user and small cell BS s and MBS v, respectively.

The SINR for the typical receiver and an eavesdropper connected with mmW small cell $b_{o,m}$ is defined as

$$\text{SINR}_m^u = \frac{\overline{P_3} M_r M_t h_{o,m} L_{o,m}(x)}{\sigma^2 + \overline{P_3} \sum_{q \in \{L,N\}} \sum_{l \in \Phi_3^q \setminus b_{o,m}} G_l h_{l,m} L_{l,m}(x_l)}, \tag{10}$$

$$\text{SINR}_m^{e^*} = \frac{\overline{P_3} G_e h_{e,m} r_e^{-\alpha_3^{(q)}}}{\sigma^2 + \overline{P_3} \sum_{q \in \{L,N\}} \sum_{l \in \Phi_3^q} G_l h_{l,m} L_{l,m}(x_l)}, \tag{11}$$

where $L_{o,m}(x) = x^{-\alpha_3^{(q)}}$ is path loss, $h_{o,m}$ and $h_{e,m}$ are small-scale fading gains, and G_l and G_e are the directivity gains of interfering BSs, given by (1) and (2). Here, $q \in \{L, N\}$ identifies the interfering link as either LoS (L) or NLoS (N), respectively.

The power consumption model for the assumed three-tier hybrid HetNet needs to be quantified for the evaluation of SSE and SEE, respectively. We define total power consumption at MBS as

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

where ρ_1 and ϵ_1 are load-independent circuit power of BD and efficiency of power amplifier, respectively. Parameters Δ_t and Λ_t are dependent on the length of transceiver chains and coding, decoding, and precoding involved in the transmission [32].

The power consumption in sub-6 GHz and mmW small cells is defined as

$$P_i^{\text{total}} = \rho_i + \frac{P_i}{\epsilon_i} \quad \text{for} \quad i \in \{2, 3\}, \tag{13}$$

where $i \in \{2, 3\}$, ρ_i is load-independent circuit power, and ϵ_i is the efficiency of power amplifier of the BS of the i-th tier.

To characterize the secure transmission scenario for the proposed network, we first assume that all tier links are eavesdropped such that eavesdroppers do not attempt attacks to change information transmitted from BS to legitimate receiver, i.e., passive non-colluding eavesdropping. A secrecy coding scheme, Wyner code, is adopted at each transmission link for the protection of confidential messages from intrusion from eavesdroppers. Under the Wyner coding scheme, each BS encodes data using this scheme before transmitting it to the legitimate user [33]. Thus, the rate of the transmitted confidential message signal R_m and rate of transmitted code words R_c are defined at the BS before data transmission commences. The cost of maintaining the confidential message secrecy from eavesdroppers is $R_c - R_m$ [33]. It is assumed that the aforementioned rates remain fixed during transmission [34, 35]. During transmission from BS to the legitimate user, whenever the wiretapping capacity of the link from the serving BS to the eavesdropper R_e is higher than the rate $R_c - R_m$, secrecy outage event occurs. Thus, the secrecy outage probability is defined as $P_{so}^k(\gamma_e) = \Pr(\text{SINR}_k^e > \gamma_e)$, i.e., the SINR at any eavesdropper node is higher than threshold. We quantify SSE and SEE based on secrecy outage probability where SSE is the average secrecy rate per unit bandwidth and SEE is the secrecy performance of a three-tier hybrid HetNet based on unit energy consumption.

4 System Performance Evaluation

We specify the average achievable rate associated with successful transmission of confidential information from BS to the legitimate user in proposed hybrid HetNet as secrecy transmission capacity constraint [33, 36]. Thus, the average achievable secrecy rate for the network tiers is represented as

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

where $[y]^+ = \max\{0, y\}$, $R_k = \mathbb{E}[\log_2(1+\text{SINR}_k^u)]$, and $R_k^e = \mathbb{E}[\log_2(1+\text{SINR}_k^{e^*})]$ are the average achievable ergodic rates of the channel between the serving kth tier BS and the typical receiver and most malicious eavesdropper . As we are performing the analysis for the most malicious eavesdropper, therefore, the average achievable ergodic rate cannot exceed R_k^e. The ergodic transmission rate of the serving BS is dependent on the CSI of the link between itself and legitimate user only as CSI of eavesdroppers is unknown at the BS because of their non-colluding nature.

4.1 Achievable Rates

Following up from (14), we derive the achievable ergodic rate at the legitimate user connected with MBS as

$$R_1 = \frac{1}{\ln 2} \int_0^\infty \frac{P_C^1(\gamma)}{1+\gamma} d\gamma, \tag{15}$$

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, $f_{X_1}(x)$ is the probability density function (PDF) of the distance between the MBS and typical receiver, and $P_C^1(\gamma, x)$ is the conditional coverage probability for the given distance x between the typical user and serving MBS [27]. In this scenario when the legitimate receiver is connected with MBS, the average ergodic rate on the link between serving BS and the most malicious eavesdropper is given by

$$R_1^e = \frac{1}{\ln 2} \int_0^\infty \frac{1 - P_{so}^1(\gamma_e)}{1+\gamma_e} d\gamma_e, \tag{16}$$

where $P_{so}^1(\gamma_e)$ is CDF of $\text{SINR}_M^{e^*}$. Following up from (14), we derive the achievable ergodic rate at the legitimate user connected with sub-6 GHz small cell as

$$R_2 = \frac{1}{\ln 2} \int_0^\infty \frac{P_C^2(\gamma)}{1+\gamma} d\gamma, \tag{17}$$

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, $f_{X_2}(x)$ 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.

In a scenario when the legitimate receiver is connected with sub-6 GHz small cell BS, the average ergodic rate on the link between serving BS and the most malicious eavesdropper is given by

$$R_2^e = \frac{1}{\ln 2} \int_0^\infty \frac{1 - P_{so}^2(\gamma_e)}{1 + \gamma_e} d\gamma_e, \tag{18}$$

where $P_{so}^2(\gamma_e)$ is the CDF of $\text{SINR}_S^{e^*}$.

Following up from (14), we derive the achievable ergodic rate at the legitimate user connected with mmW small cell as

$$R_3 = \frac{1}{\ln 2} \int_0^\infty \frac{P_C^3(\gamma)}{1 + \gamma} d\gamma, \tag{19}$$

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 and $P_C^{3,L}(\gamma)$ and $P_C^{3,N}(\gamma)$ are defined as the conditional coverage probability when the typical receiver, connected with mmW small cell, connects with the BS in Φ_3^L and Φ_3^N, respectively. $A_{3,q}$ are the probabilities of typical receiver associating with LoS or NLoS link.

In a scenario when the legitimate receiver is connected with mmW small cell BS, the average ergodic rate on the link between serving BS and the most malicious eavesdropper is given by

$$R_3^e = \frac{1}{\ln 2} \int_0^\infty \frac{1 - P_{so}^3(\gamma_e)}{1 + \gamma_e} d\gamma_e, \tag{20}$$

where $P_{so}^2(\gamma_e)$ is the CDF of $\text{SINR}_m^{e^*}$. By substituting (19) and (20) in (14), we obtain the average achievable secrecy rate for mmW tier.

4.2 Physical Layer Security Parameters

The secrecy outage probability, P_{so}, for the entire network is defined as

$$P_{so} = \sum_{k=1}^{3} P_{so}^k A_k, \tag{21}$$

where A_k is the association probability of tier k. Similarly, a lower bound on the SSE, using the law of total expectation, is given by

$$\mathrm{SSE}^L = \sum_{k=1}^{3} A_k \times \mathrm{SSE}_k, \tag{22}$$

where $\mathrm{SSE}_1 = U \times R_{S1}$ is the value of SSE for massive MIMO-enabled sub-6 GHz macro tier and $\mathrm{SSE}_k = R_{Sk}$ for $k \in \{2, 3\}$ is the value of SSE for sub-6 GHz and mmW small cell tiers, respectively. Average achievable secrecy rate R_{Sk} for each tier k of the network is given by (14).

The lower bound on SEE for the proposed network is defined as [28, 38]:

$$\mathrm{SEE}^L = \sum_{k=1}^{3} A_k \times \mathrm{SEE}_k, \tag{23}$$

where $\mathrm{SEE}_1 = \frac{U \times R_{S1}}{P_1^{\mathrm{total}}}$ is the value of SEE for massive MIMO sub-6 GHz enabled macro tier and $\mathrm{SEE}_k = \frac{R_{Sk}}{P_k^{\mathrm{total}}}$ for $k \in \{2, 3\}$ is SEE for sub-6 GHz and mmW small cell tiers, respectively. Average achievable secrecy rate R_{Sk} for each tier k of the network is given by (14).

5 Simulation Results and Performance Analysis

In this section, numerical results are shown to study and understand the impact of massive MIMO large antenna arrays and mmW channel characteristics on the secrecy outage probability, SSE, and SEE of the network. The simulation parameters are outlined in Table 2. Monte Carlo simulations are used to study the system performance.

We begin by studying the performance of the proposed network's secrecy outage probability in terms of density of eavesdropper nodes, as shown in Fig. 2. This plot has been obtained using (21) while taking varying small cell BS densities and directional antenna gains at the eavesdroppers nodes of the network. The secrecy outage probability of the network increases with increasing eavesdropper's density, thereby notifying that a large number of eavesdropping nodes in the network harm the network secrecy. However, there is another important observation to be noted that higher small cell BS density optimizes the secrecy of the network even though the eavesdropper's density might be high. These results allude to the fact that higher small cell density results in the increase in interference in the network. Thus, the uncertainty at eavesdropper nodes elevates leading to their SINR falling below the threshold. This results in improvement in secrecy outage probability of the network. The reader may notice that when the small cell density in the network is kept fixed,

Table 2 Simulation parameters

Parameter	Value	Parameter	Value
λ_1	$(500^2 \times \lambda)^{-1}$	$f_1 = f_2$	1 GHz
$B_1 = B_2$	10 MHz	α_1	3.5
α_2	4	P_1	46 dBm
P_2	30 dBm	λ_e	1×10^{-6}
f_3	28 GHz	B_3	100 MHz
P_3	30 dBm	α_L	2
α_N	4	N_N	2
N_L	3	M_r	10 dB
M_t	10 dB	m_r	−10 dB
m_t	0 dB	θ_r	90°
θ_t	30°	σ^2	−90 dBm
Noise figure	10 dB	$1/\beta$	141.4 m [30]
$\epsilon_1 = \epsilon_2 = \epsilon_3$	0.38 [28]	ρ_1	4 W
Δ_1	4.8	Δ_2	0
Δ_3	2.08×10^{-8}	Λ_1	1
Λ_2	9.5×10^{-8}	Λ_3	6.25×10^{-8}
ρ_2	13.6 W [39]	ρ_3	13.6 W [39]

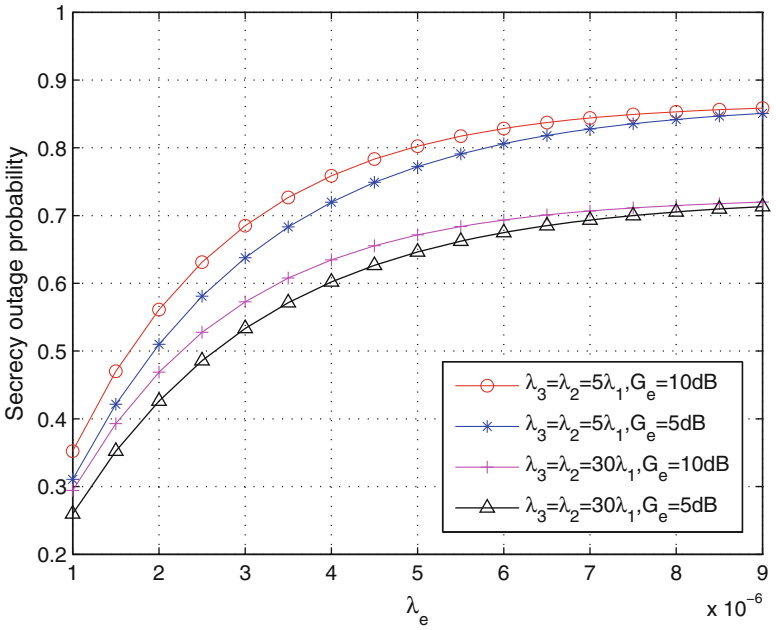

Fig. 2 Secrecy outage probability of the three-tier network as the function of λ_e for $\gamma_e = 40$ dB, $N = 5$

the secrecy rate of the transmissions in the network improves with small directional antenna gains at the eavesdroppers. We conclude that lower directional gains at the eavesdroppers and higher cell density in the network are the two major settings

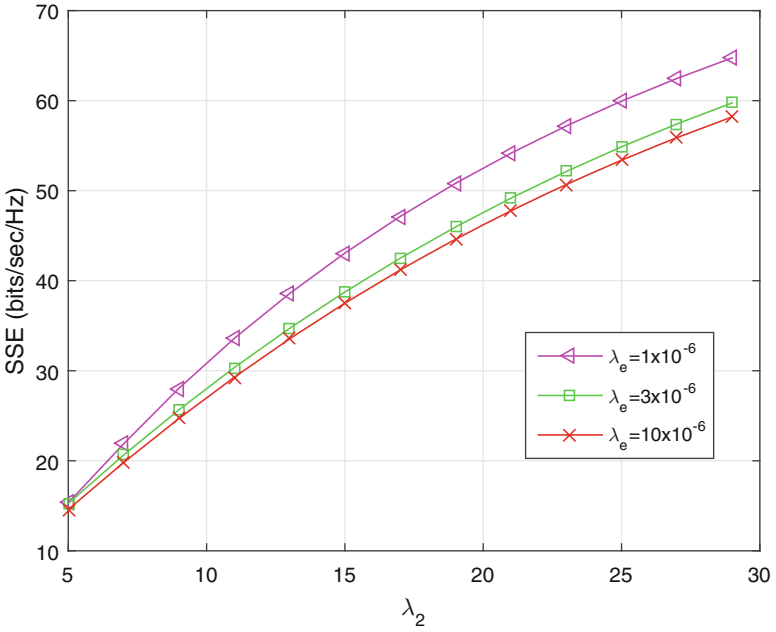

Fig. 3 SSE versus varying small cells BS density as multiple of MBS density for $\lambda_3 = \lambda_2$, $G_e = 15$ dB, $N = 40$, $U = 5$

that reduce the probability of eavesdroppers having SINR above the predefined threshold.

Now, we study the SSE behavior based on varying small cell BS density of tier 2 and tier 3 for various eavesdropper's densities. Figure 3 plots the SSE of the network versus varying small cell densities. It can be seen that the SSE increases with the increase in small cell density and falls when the eavesdropper node's density increases. This is because, the average cell radius decreases when small cell density is increased. Therefore, more users are offloaded to small cells so the transmission from the BS to the intended legitimate user becomes better. When the cell sizes decrease, the distance from the intended receiver to the transmitting nodes decreases that causes stronger links and enhanced secrecy rate between them. If we consider the case of mmW small cells, the LoS probability function $p(R)$ is directly related to distance; thus, the LoS association probability increases with decrease in distance. In such scenario, low path loss LoS links between mmW BSs and legitimate users are more likely to be formed than NLoS links. Another interesting observation is that user's association with MBSs declines in the presented scenario though they are high-power nodes but have low BS density compared to the small cells. Interference in the network increases as transmitting node density is notably high; therefore, an increase in eavesdropper's density has little impact on SSE of the network.

Figure 4 illustrates the relationship between the SEE and the small cell density. This plot has been obtained using (23). As a preliminary observation, it may be

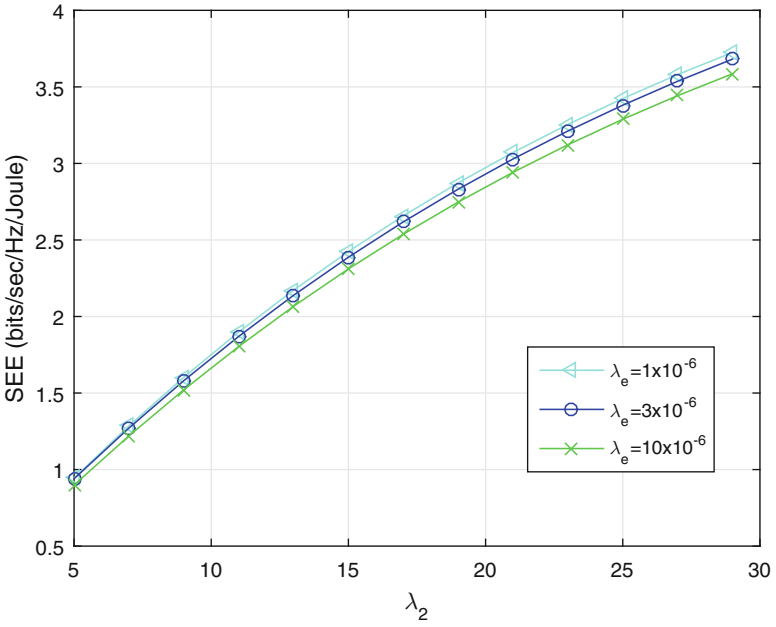

Fig. 4 SEE versus varying small cells BS density as multiple of MBS density for $\lambda_3 = \lambda_2$, $G_e = 15$ dB, $N = 30$, $U = 5$

stated that the SEE is higher for greater values of λ_2 and λ_3, respectively . This is because of the increase in SSE over the identical power consumption, shown in Fig. 3. Moreover, on increasing small cell densities, λ_2 and λ_3, more users associate with low-power small cell BSs compared to high-power macro cell BSs. This shift in association leads to a power-efficient network; however, it comes at the cost of small cell BS deployment. Here again it may be noted that the interference in the three-tier network is higher with dense transmitting BS nodes; therefore, an increase in eavesdropper's density has little impact on SEE of the network.

Extending the previous discussion, we now vary the number of transmitting antennas on the massive MIMO-enabled MBS of the network and then observe the effects on SSE of the three-tier hybrid HetNet over different small cell densities. The results are shown in Fig. 5. It can be seen that the SSE of the network falls with the increasing number of antennas at the MBSs and shows significant increase with higher small cell density. This is because, when N increases, spectral efficiency of MBSs increases. As the MBSs are high power nodes, transmission to eavesdroppers in the network improves significantly that results in increases secrecy rate, R^e. Legitimate user to BS association gets biased toward MBSs because of their high array gains at increased number of antennas. Thus, fewer portion of users connect with small cells BSs. Hence, interference in the network reduces leading to better reception at eavesdroppers.

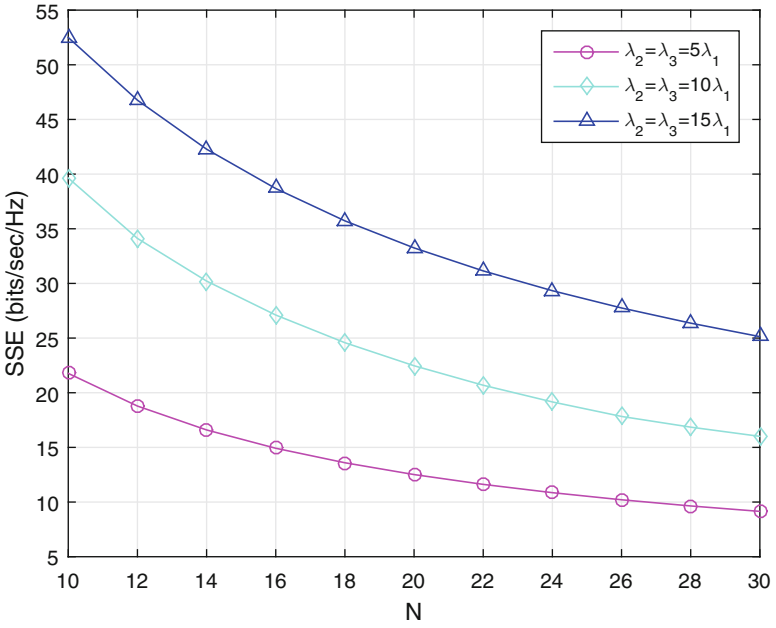

Fig. 5 SSE versus different number of antennas at macro BS for $G_e = 15$ dB, $U = 5$

Figure 6 illustrates the variation in SEE with increasing number of antennas at massive MIMO-enabled MBSs. Plot is based on (23). It can be seen that SEE of the network drops with increasing N. It follows from the previous result that SSE drops over the identical power consumption. In addition, users are more likely to connect to macro cell BSs with increase in transmitting nodes at their BSs, and since macro cells are higher-power-consuming entities compared to small cells, therefore, overall network setting shifts to a power-inefficient network. As a result, SEE of the network decreases with the increase in average achievable rate at eavesdroppers. The reader may notice that the interference in the network elevates with small cell density; therefore, SEE improves with drop in eavesdroppers' secrecy rate R^e.

Early on, we mentioned that mmW and massive MIMO technologies are the candidates for being the enabling technologies for 5G networks due to their higher gains and superior bandwidth as for mmW technology. We conclude the Results section by highlighting these very important points that we cannot increase the directional beamforming gains at mmW nodes neither can we increase the number of antennas at massive MIMO-enabled nodes limitlessly to have optimum coverage in the proposed network, without entertaining drop in the overall secrecy performance of the network.

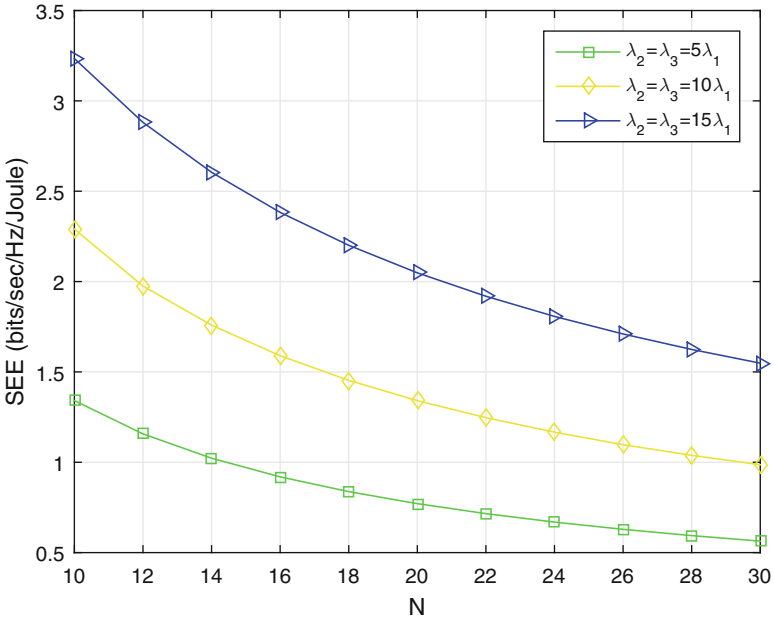

Fig. 6 SEE versus different number of antennas at macro BS for $G_e = 15\,\text{dB}$, $U = 5$

6 Conclusion

In this chapter, we characterized the secure communication in massive MIMO-enabled three-tier hybrid HetNet based on the unique features of massive MIMO and mmW communication by using PLS. Particularly, we evaluated the secrecy outage probability and achievable ergodic rate at each of the three network tiers and most malicious eavesdropper node. The expressions were then used to develop a tractable approach to determine network-wide SSE and SEE. It was observed that network-wide interference elevates on high BS density that in turn dominates the secrecy performance of the network. Moreover, the secrecy performance of the networks drops at higher beamforming gains at mmW cells; therefore, a tradeoff exists between optimal coverage and secrecy in the network. The relationship between the secrecy outage probability, SSE, and SEE of the network and number of antennas at MBS, BS density, antenna gains, and eavesdropper's density has also been studied through simulation results. Through these results, we conclude that the number of antennas at the massive MIMO-enabled macro cell BSs and beamforming directivity gains at mmW cells shall be carefully chosen for optimal secrecy performance of the network.

References

1. J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, A.C. Soong, J.C. Zhang, What will 5G be? IEEE J. Sel. Areas Commun. **32**(6), 1065–1082 (2014)
2. J. Zhang, X. Ge, Q. Li, M. Guizani, Y. Zhang, 5G millimeter-wave antenna array: design and challenges. IEEE Wirel. Commun. **24**(2), 106–112 (2017)
3. J. Ye, X. Ge, G. Mao, Y. Zhong, 5G ultra-dense networks with non-uniform distributed users. IEEE Trans. Veh. Technol. **67**(3), 2660–2670 (2018)
4. X. Ge, R. Zi, H. Wang, J. Zhang, M. Jo, Multi-user massive MIMO communication systems based on irregular antenna arrays. IEEE Trans. Wirel. Commun. **15**(8), 5287–5301 (2016)
5. R.W. Heath, T. Bai, R. Vaze, Analysis of blockage effects on urban cellular networks. IEEE Trans. Wirel. Commun. **13**(9), 5070–5083 (2014)
6. E. Turgut, M.C. Gursoy, Energy efficiency in relay-assisted mmW cellular networks, in *IEEE 84th Vehicular Technology Conference (VTC-Fall)*, Sept 2016, pp. 1–5
7. M. Ding, P. Wang, D. Lopez-Perez, G. Mao, Z. Lin, Performance impact of LoS and NLoS transmissions in dense cellular networks. IEEE Trans. Wirel. Commun. **15**(3), 2365–2380 (2016)
8. H. Wang, T. Zhang, X. Xia, Secure MISO wiretap channels with multi-antenna passive eavesdropper: artificial noise vs. artificial fast fading. IEEE Trans. Wirel. Commun. **14**(1), 94–106 (2015)
9. Y. Liang, H.V. Poor, S. Shamai, Secure communication over fading channels. IEEE Trans. Inf. Theory **54**(6), 2470–2492 (2008)
10. L. Wang, N. Yang, M. Elkashlan, P.L. Yeoh, J. Yuan, Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels. IEEE Trans. Inf. Forensics Secur. **9**(2), 247–258 (2014)
11. H.M. Wang, M. Luo, Q. Yin, X.G. Xia, Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. IEEE Trans. Inf. Forensics Secur. **8**(12), 2007–2020 (2013)
12. T. Lv, H. Gao, S. Yang, Secrecy transmit beamforming for heterogeneous networks. IEEE J. Sel. Areas Commun. **33**(6), 1154–1170 (2015)
13. H. Wu, X. Tao, N. Li, J. Xu, Secrecy outage probability in multi-RAT heterogeneous networks. IEEE Commun. Lett. **20**(1), 53–56 (2016)
14. H. Wang, T. Zheng, J. Yuan, D. Towsley, M.H. Lee, Physical layer security in heterogeneous cellular networks. IEEE Trans. Commun. **64**(3), 1204–1219 (2016)
15. Y. Deng, L. Wang, K.K. Wong, A. Nallanathan, M. Elkashlan, S. Lambotharan, Safeguarding massive MIMO aided hetnets using physical layer security, in *Proceedings of Wireless Communications and Signal Processing*, 2015, pp. 1–5
16. J. Wang, J. Lee, F. Wang, T.Q.S. Quek, Jamming-aided secure communication in massive MIMO rician channels. IEEE Trans. Wirel. Commun. **14**(12), 6854–6868 (2015)
17. M. Xu, X. Tao, F. Yang, H. Wu, Enhancing secured coverage with COMP transmission in heterogeneous cellular networks. IEEE Commun. Lett. **20**(11), 2272–2275 (2016)
18. L. Wang, K.K. Wong, M. Elkashlan, A. Nallanathan, S. Lambotharan, Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: a new look at interference. IEEE J. Sel. Top. Sign. Proces. **10**(8), 1375–1389 (2016)
19. V. Sharma, D. N. K. Jayakody, I. You, R. Kumar, J. Li, Secure and efficient context-aware localization of drones in urban scenarios. IEEE Commun. Mag. **56**(4), 120–128 (2018)
20. V. Sharma et al., Secure and energy efficient handover in fog networks using blockchain-based DMM. IEEE Commun. Mag. **56**, 22–31 (2018)
21. F. Jameel et al., Secure communication for separated and integrated receiver architectures in SWIPT. IEEE Wirel. Commun. Netw. Conf. **2018**, 1–6 (2018)
22. L. Wang, M. Elkashlan, T.Q. Duong, R.W. Heath Jr., Secure communication in cellular networks: the benefits of millimeter wave mobile broadband, in *IEEE 15th International Workshop on Signal Processing and Advances in Wireless Communication (SPAWC)*, 2014, pp. 115–119

23. S. Vuppala, S. Biswas, T. Ratnarajah, An analysis on secure communication in millimeter/micro-wave hybrid networks. IEEE Trans. Commun. **64**(8), 3507–3519 (2016)
24. C. Wang, H.M. Wang, Physical layer security in millimeter wave cellular networks. IEEE Trans. Wirel. Commun. **15**(8), 5569–5585 (2016)
25. S. Gong, C. Xing, Z. Fei, S. Ma, Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks. IEEE Trans. Veh. Technol. Early Access Articles, **66**, 1–12 (2016)
26. A. Umer, S.A. Hassan, H. Pervaiz, Q. Ni, L. Musavian, Coverage and rate analysis for massive MIMO-enabled heterogeneous networks with millimeter wave small cells, in *IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, Sydney, pp. 1–5
27. A. Umer, S.A. Hassan, H. Pervaiz, Q. Ni, L. Musavian, S.H. Ahmed, Secrecy outage analysis for massive MIMO-enabled multi-tier 5G hybrid hetnets, in *2018 IEEE International Conference on Communications Workshops*, 2018, Kansas City, pp. 1–6
28. Y. Hao, Q. Ni, H. Li, S. Hou, On the energy and spectral efficiency tradeoff in massive MIMO enabled hetnets with capacity-constrained Backhaul links. IEEE Trans. Commun. (2017, in press). https://doi.org/10.1109/TCOMM.2017.2730867
29. K. Hosseini, W. Yu, R.S. Adve, Large-scale mimo versus network mimo for multicell interference mitigation. IEEE J. Sel. Top. Sign. Proces. **8**(5), 930–941 (2014)
30. M. Omar, M. Anjum, S.A. Hassan, H. Pervaiz, Q. Ni, Performance analysis of hybrid 5G cellular networks exploiting mmW capabilities in suburban areas, in *IEEE Internation Conference on Communications*, Kuala Lumpur, 2016
31. E. Turgut, M.C. Gursoy, Coverage in heterogeneous downlink millimeter wave cellular networks. IEEE Trans. Commun. **65**, 4463–4477 (2017)
32. C. Yang, J. Li, Q. Ni, A. Anpalagan, M. Guizani, Interference-aware energy efficiency maximization in 5G ultra-dense networks. IEEE Trans. Commun. **65**(2), 728–739 (2017)
33. A.D. Wyner, The wire-tap channel. Bell Labs Tech. J. **54**(8), 1355–1387 (1975)
34. X. Zhang, X. Zhou, M.R. McKay, Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks. IEEE Trans. Inf. Forensics Secur. **8**(11), 1802–1814 (2013)
35. C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, X. Wang, Interference exploitation in D2D-enabled cellular networks: a secrecy perspective. IEEE Trans. Commun. **63**(1), 229–242 (2015)
36. P.C. Pinto, J. Barros, M.Z. Win, Secure communication in stochastic wireless networks–part I: connectivity. IEEE Trans. Inf. Forensics Secur. **7**(1), 125–138 (2012)
37. T. Bai, R.W. Heath, Coverage and rate analysis for millimeter-wave cellular networks. IEEE Trans. Wirel. Commun. **14**(2), 1100–1114 (2015)
38. H. Pervaiz, L. Musavian, Q. Ni, Z. Ding, Energy and spectrum efficient transmission techniques under QoS constraints toward green heterogeneous networks. IEEE Access **3**, 1655–1671 (2015)
39. G. Auer, V. Giannini, C. Desset, I. Godor, P. Skillermark, M. Olsson et al., How much energy is needed to run a wireless network? IEEE Wirel. Commun. **18**(5), 40–49 (2011)

Anum Umer received the B.E. degree in Electrical(Telecommunication) Engineering from the National University of Science and Technology (NUST), Pakistan in 2015 and the M.S. degree in Electrical Engineering from NUST, Pakistan in 2017. Her broader area of research includes wireless communication, massive MIMO and millimeter wave communication. She is currently a Researcher with the System Analysis and Verification Lab, School of Electrical Engineering and Computer Science, NUST.

Syed Ali Hassan received the B.E. degree (Hons.) in electrical engineering from the National University of Sciences and Technology (NUST), Pakistan, in 2004, the M.S. degree in elec- trical engineering from the University of Stuttgart, Germany, in 2007, and the M.S. degree in mathe- matics and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2011. His broader area of research is signal processing for communications. He is currently an Assistant Professor with the NUST School of Electrical Engineering and Computer Science, where he is also the Director of Information Processing and Transmission Research Group, which focuses on various aspects of theoretical communications. He was a visiting professor at Georgia Tech in Fall 2017 and also held industry position at Cisco Systems Inc, CA, USA.