Secrecy Outage Analysis for Massive MIMO-enabled Multi-Tier 5G Hybrid HetNets

Anum Umer*, Syed Ali Hassan*, Haris Pervaiz†, Qiang Ni‡, Leila Musavian§ and Syed Hassan Ahmed¶

*School of Electrical Engineering & Computer Science (SEECS), NUST, Pakistan.
†Home of 5GIC, University of Surrey, UK.
‡School of Computing & Communications, Lancaster University, UK.
§ School of Computer Science & Electronics Engineering, University of Essex, UK.
¶ University of Central Florida, Orlando, FL, USA.
Emails:{aumer.msee15seecs, ali.hassan}@seecs.edu.pk, h.pervaiz@surrey.ac.uk, q.ni@lancaster.ac.uk, leila.musavian@essex.ac.uk and sh.ahmed@ieee.org

***Abstract*—The existing cellular systems operating in ultra high frequency bands suffer from severe bandwidth congestion and therefore the paradigm of cellular spectrum is shifting towards millimeter wave (mmWave) bands under the umbrella of fifth generation (5G) networks to provide higher capacity. On the other hand, providing secure and reliable transmission of data to the desired users is gaining more importance in recent years. This paper analyzes the impact of co-existence of mmWave small cells and massive multiple-input multiple-output (MIMO) on connection outage and secrecy outage of the network. Specifically, we consider a three-tier network consisting of small cells operating at both the sub-6 GHz and mmWave frequency bands overlaid with massive MIMO-enabled macro base stations where eavesdroppers under variable eavesdroppers density and antenna gains are present. The user location of both the desired entities and eavesdroppers are modeled by independent Poisson point processes. Based on this stochastic model, we investigate the downlink secrecy outage probability and connection outage probability of the entire network. Numerical results show that massive MIMO-enabled hybrid heterogeneous networks (HetNet) alongside mmWave small cells significantly reduces both the connection outage and secrecy outage probability of the network for higher small cells base station density.**

I. Introduction

Over the years, the explosive growth in the mobile data traffic calls for shifting the paradigm of cellular spectrum to higher frequency bands. Since the existing wireless spectrum is almost saturated, the key enablers for 5G technology are millimeter wave (mmWave) base stations (BSs) operating at 10 to 300 GHz radio frequency bands with bandwidths as high as 2 GHz and large-scale antenna arrays at sub-6 GHz band. Thus, the 5G technology can be visualized as a combination of a mixed heterogeneous network (HetNet) composed of multiple network tiers of variable sizes, transmit powers, range and operating frequencies.

The amalgamation of HetNets, massive multiple-input multiple-output (MIMO) and mmWave small cells has gathered considerable attention recently. For instance, a stochastic geometry-based model for standalone mmWave network is investigated in [1] for the analysis of coverage and rate trends. The user association per tier and coverage probability for K-tier HetNets with massive MIMO in the macro tier is stochastically modeled in [2]. Whereas much emphasis is laid on connection and rate performance of these networks, a considerable work has been done on physical layer security implementation in wireless networks. For instance, the secrecy capacity of unicast links in the presence of eavesdroppers where transmission to the desired node is based on distance is studied in [3]. Similarly, secrecy outage probability for wireless fading channel was investigated in [4]. The authors in [5] have studied the secrecy and outage capacity under the effect of blockages for mmWave overlaid microwave network in the presence of eavesdroppers.

While the aforementioned literature explains the efficiency of mmWave overlaid microwave networks in terms of their connection and secrecy outage behavior, an analytical approach to investigate the impact of co-existence of massive MIMO and mmWave cells on connection outage and secrecy outage in a HetNet in the presence of eavesdroppers has not been explored yet. In this paper, we use stochastic geometry for the downlink transmission analysis of a 3-tier network composed of mmWave and sub 6-GHz small cells overlaid massive MIMO-enabled sub 6-GHz macro cells. To the best of our knowledge, no prior work has analyzed secrecy and connection outage of mmWave small cells coexisting with traditional HetNets with massive MIMO enabled macro BSs (MBSs) in the presence of eavesdropper. The mmWave and sub-6 GHz small cells BSs are deployed at higher density than MBSs and user association, connection outage and secrecy outage trends are discussed.

II. System Model

We consider the time-division duplex (TDD) downlink transmission scenario of a three-tier HetNet comprising of sub-6 GHz macro cells overlaid with small cells operating at sub-6 GHz and mmWave frequency band [6]. It is assumed that sub-6 GHz macro cell base stations (MBSs) are provided with large antenna arrays. The sub-6 GHz small cells constitute tier 2 while tier 3 constitutes small cells operating at mmWave frequency band. The BSs of each k^{th} tier are uniformly located following a two dimensional homogeneous

Poisson point process (HPPP) Φ_k with density λ_k where $k \in \{1,2,3\}$. The user equipment and eavesdroppers are also uniformly distributed as HPPP Φ_u and Φ_e with density λ_u and λ_e, respectively. It is assumed that each macro cells has N antennas which is transmitting consecutively to S users such that $N \gg S \geq 1$ [7]. Each MBS utilises Zero forcing beamforming (ZFBF) to transmit S data streams with equal power assignment. It is considered that the small cell BSs and users are omni-directional, i.e., $N = 1$. It is also assumed that the downlink channel state information is perfectly estimated at the MBS [2]. According to Slivnyak's Theorem, a typical user is assumed to be located at the origin to analyse the network performance. The typical user can establish either line-of-sight (LoS) or non-line-of-sight (NLoS) connection with mmWave small cells. Thus, we divide , By the aid of independent thinning theorem, the intensity of mmWave tier Φ_3 can be divided into two independent PPPs of LoS and NLoS mmWave small cells such as Φ_3^L and Φ_3^N, with respective intensities of $p(x)\lambda_3$ and $(1-p(x))\lambda_3$, using LoS probability function $p(x)$. The $p(x)$ is used to determine if a link of length x is LoS or NLoS [1]. The LoS probability function $p(x)$ is discussed further in this section. More details can also be found in [8].

In this work, an open access scheme is considered such that each user has the flexibility to connect to any tier BS based on the maximum average received power, i.e., a user will connect to tier j only if

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

where P_k is the transmission power of the k^{th} tier, $L_k(x) = x_k^{-\alpha_k}$ is the path loss function where x is distance between typical user and serving BS and α_k is the path loss exponent.

It is assumed that the tier 1 and 2 follow independent and identically distributed (i.i.d) Rayleigh fading and independent Nakagami fading is assumed for tier 3. 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 $i \in \{M, S, m\}$. The received signal-to-interference-plus-noise ratio (SINR) for a typical user and any eavesdropper associated with the MBS $b_{o,M}$ is represented as

$$\text{SINR}_M^u = \frac{\frac{P_1}{S} h_{o,M} L_{o,M}(x)}{\sigma^2 + \sum_{j \in \Phi_1 \backslash b_{o,M}} \frac{P_1}{S} h_{j,M} L_{j,M}(x_j) + I_S}, \tag{2}$$

$$\text{SINR}_M^e = \frac{\frac{P_1}{S} h_{e,M} r_e^{-\alpha_1}}{\sigma^2 + \sum_{j \in \Phi_1} \frac{P_1}{S} h_{j,M} L_{j,M}(x_j) + \sum_{q \in \Phi_2} P_q h_q L_q(x_q)}, \tag{3}$$

where h_q is the small scale fading gain from the interfering channel such that $h_q \sim \exp(1)$, x_q is the distance between the typical user and small cell BS q, $h_{o,M}$ and $h_{e,M}$ are the small scale fading gains of the typical user at the distance x and eavesdropper at the distance r_e from the serving BS such that $h_{o,M} \sim \Gamma(N-S+1, 1)$ [9]. $h_{j,M}$ is small scale fading power gain such that $h_{j,M} \sim \Gamma(S, 1)$, x_j is distance between typical user and MBS j and $L_q(x_q) = x_q^{-\alpha_2}$ and σ^2 is the noise power.

The SINR of a typical user with link distance x and any eavesdropper at distance r_e associated with the small cell BS $b_{o,S}$ operating at sub-6 GHz band is represented as

$$\text{SINR}_S^u = \frac{P_2 h_{o,S} L_{o,S}(x)}{\sigma^2 + \sum_{q \in \Phi_2 \backslash b_{o,S}} P_2 h_{q,S} L_{q,S}(x_q) + I_{\overline{\text{M}}}}, \tag{4}$$

$$\text{SINR}_S^e = \frac{P_2 h_{e,S} r_e^{-\alpha_2}}{\sigma^2 + \sum_{q \in \Phi_2} P_2 h_{q,S} L_{q,S}(x_q) + I_{\overline{\text{M}}}}, \tag{5}$$

where $I_{\overline{\text{M}}} = \sum_{j \in \Phi_1} \frac{P_j}{S} h_j L_j(x_j)$ is the intercell interference from macro cells, $L_{q,S}(x_q) = x_q^{-\alpha_2}$ and $L_{o,S}(x) = x^{-\alpha_2}$. Here, $h_{q,S}$ is the small scale fading gain from the interfering channel such that $h_{q,S} \sim \exp(1)$. Similarly, $h_{o,S}$ and $h_{e,S}$ are the small scale fading gain of the typical user such that $h_{o,S} \sim \exp(1)$ while h_j is small scale fading power gain such that $h_j \sim \Gamma(S, 1)$. Here, $L_{q,S}(x_q) = x_q^{-\alpha_2}$ and $L_{o,S}(x) = x^{-\alpha_2}$.

The SINR for the typical user and any eavesdropper associated with mmWave small cell $b_{o,m}$ is represented as

$$\text{SINR}_m^u = \frac{P_3 M_r M_t h_{o,m} L_{o,m}(x)}{\sigma^2 + P_3 \sum_{j \in \{L,N\}} \sum_{i \in \Phi_3^j \backslash b_{o,m}} G_l h_{i,m} L_{i,m}(x_i)}, \tag{6}$$

$$\text{SINR}_m^e = \frac{P_3 G_e h_{e,m} r_e^{-\alpha_3^{(j)}}}{\sigma^2 + P_3 \sum_{j \in \{L,N\}} \sum_{i \in \Phi_3^j} G_l h_{i,m} L_{i,m}(x_i)}, \tag{7}$$

where $L_{o,m}(x) = x^{-\alpha_3^{(j)}}$, $h_{o,m}$ and $h_{e,m}$ are small scale fading gain where Nakagami fading parameter are unique positive integers N_j for $j \in \{L, N\}$, M_a are the main lobe gains for $a \in \{transmitter, receiver\}$, G_l and G_e are the directivity gains of interfering BSs and eavesdropper. We assume that both the BSs and the users have their main lobe aligned in the direction of dominant propagation path so the directivity gain of the desired link signal is $M_r M_t$. It is assumed that the beam direction is independently and uniformly distributed between $(0, 2\pi]$. Hence G_l for $l = \{1,2,3,4\}$ is given as,

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

A blockage model based on stochastic geometry approach is assumed for mmWave small cells [10]. Hence the LoS probability function $p(x)$ is given as, $p(x) = e^{-\beta x}$ where β is the dependent on statistics of blockages and x is the BS to typical user link distance.

III. Performance Analysis

In the proposed network scenario, it is assumed that all tier links are eavesdropped and for enhanced secrecy, a secrecy coding scheme called Wyner code is adopted at each link [11]. Based on this scheme, we need to specify two kind of rates at the transmitter, i.e., rate of the transmitted message signal R_m, and rate of transmitted code words R_c. In the considered network scenario, when a BS of any tier intends to make a reliable and secure transmission, depending of the choice of R_m and R_c at the BS, the following outage events are bound to occur.

a) Connection outage occurs when the capacity of the link between typical user and its associated BS falls below the transmitted message rate R_m, i.e., SINR of the received signal is below a certain threshold. Hence, we define connection outage probability as $C_{co}^k(\Gamma) = \Pr(\text{SINR}_k^u < \Gamma)$.

b) Secrecy outage occurs when the capacity of the channel between the serving BS and any eavesdropper is above the rate R_e and message security is breached, i.e., received SINR at any eavesdropper is above a certain threshold. Hence, we define secrecy outage probability as $C_{so}^k(\Gamma_e) = \Pr(\text{SINR}_k^e > \Gamma_e)$.

A. Association Probability

The association probability that a typical user is connected to the MBS is given by,

$$A_1 = 2\pi\lambda_1 \int_0^\infty x\exp\Bigg(-\pi\lambda_2\left(\frac{P_2 S x^{\alpha_1}}{P_1(N-S+1)}\right)^{2/\alpha_2} -\pi\lambda_1 x^2 - 2\pi\lambda_3\left(\frac{P_3 S}{P_1(N-S+1)}\right)^{2/\alpha_3} Y(x)\Bigg)dx, \quad (8)$$

where $Y(x)$ is given by,

$$Y(x) = \int_0^{\delta_N(x)} tp(t)dt + \int_0^{\delta_L(x)} t(1-p(t))dt, \quad (9)$$

where $\delta_N(x) = \left(\frac{P_3 G}{P_1}\right)^{\frac{1}{\alpha_L}} x^{\frac{\alpha_1}{\alpha_L}}$, $\delta_L(x) = \left(\frac{P_3 G}{P_1}\right)^{\frac{1}{\alpha_N}} x^{\frac{\alpha_1}{\alpha_N}}$. The probability density function (PDF) of users distance to serving MBS, $f_{X_1}(r)$, is given as [6],

$$f_{X_1}(r) = \frac{2\pi\lambda_1}{A_1} x\exp\Bigg(-\pi\lambda_2\left(\frac{P_2 S r^{\alpha_1}}{P_1(N-S+1)}\right)^{2/\alpha_2} -\pi\lambda_1 r^2 - 2\pi\lambda_3\left(\frac{P_3 S}{P_1(N-S+1)}\right)^{2/\alpha_3} Y(r)\Bigg). \quad (10)$$

The association probability that a typical user is connected to sub-6 GHz small cell BS is given by,

$$A_2 = 2\pi\lambda_2 \int_0^\infty x\exp\Bigg(-\pi\lambda_2 x^2 - 2\pi\lambda_3 Y(x) - \pi\lambda_1\left(\frac{P_1(N-S+1)x^{\alpha_2}}{P_2 S}\right)^{2/\alpha_1}\Bigg)dx. \quad (11)$$

The PDF of the distance of the typical user to serving sub-6 GHz small cell BS, $f_{X_2}(r)$, is given as [6],

$$f_{X_2}(r) = \frac{2\pi\lambda_2}{A_2} r\exp\Bigg(-\pi\lambda_2 r^2 - 2\pi\lambda_3 Y(r) - \pi\lambda_1\left(\frac{P_1(N-S+1)r^{\alpha_2}}{P_2 S}\right)^{2/\alpha_1}\Bigg). \quad (12)$$

The association probability that a user is associated to a mmWave small cell BS is given as

$$A_3 = 1 - \sum_{k\in\{1,2\}} A_k. \quad (13)$$

For mmWave links, the probability of connecting with NLoS link is given by, $A_N = \eta_N \int_0^\infty \exp\left\{-2\pi\lambda_3 \int_0^{\delta_N(x)} tp(t)dt\right\} f_N(x)dx$ [1]. Hence, the probability of connecting with LoS link is $A_L = 1 - A_N$. Here, $f_N(x) = 2\pi\lambda_3 x(1-p(x))\exp(-2\pi\lambda_3\int_0^x t(1-p(t))dt)/\eta_N$ is the PDF of the distance of the typical user to the NLoS BS and for LoS link, $f_L(x) = 2\pi\lambda_3 x p(x)\exp(-2\pi\lambda_3\int_0^x tp(t)dt)/\eta_L$ [Eq. 4 of [1], [10], Theorem 8] where $\eta_N = 1 - \exp\left\{-2\pi\lambda_3\int_0^\infty t(1-p(t))dt\right\}$ is probability that the user has at least one NLoS link, likewise, $\eta_L = 1 - \exp\left\{-2\pi\lambda_3\int_0^\infty tp(t)dt\right\}$ for LoS link. The PDF of the distance of the typical user to serving BS given that it is connected with LoS link is $\hat{f}_L(x) = \frac{\eta_L f_L(x)}{A_L}\exp\left\{-2\pi\lambda_3\int_0^{\delta_L(x)} t(1-p(t))dt\right\}$ and for NLoS link $\hat{f}_N(x) = \frac{\eta_N f_N(x)}{A_N}\exp\left\{-2\pi\lambda_3\int_0^{\delta_N(x)} tp(t)dt\right\}$.

B. Connection Outage Probability

Connection outage probability of a typical user associated with sub-6 GHz macro or small cell BS is given as

$$\begin{aligned} C_{co}^k(\Gamma) &= \Pr(\text{SINR}_k^u < \Gamma) = 1 - \Pr(\text{SINR}_k^u > \Gamma) \\ &= 1 - \int_0^\infty \Pr(\text{SINR}_k^u > \Gamma | X_k = x) f_{X_k}(x)dx \\ &= 1 - \int_0^\infty C^k(\Gamma, x) f_{X_k}(x)dx \quad where \quad k\in\{1,2\}. \end{aligned}$$

Here $C^1(\Gamma, x)$ for a typical user associated with MBS at the distance x is given by

$$C^1(\Gamma, x) = \sum_{w=0}^{N-S} \frac{(x^{\alpha_1})^w}{(w!)(-1)^w} \sum \frac{w!}{\prod_{j=1}^{w} n_j!(j!)^{n_j}} \times\exp\left(-\frac{\Gamma\sigma^2 S x^{\alpha_1}}{P_1} - F\left(\frac{\Gamma S x^{\alpha_1}}{P_1}\right)\right)\prod_{j=1}^{w}(D^{(j)}(x^{\alpha_1}))^{n_j}, \quad (14)$$

where $F(.)$ and $D^{(j)}(.)$ are given as,

$$F(q) = 2\pi\lambda_1 \sum_{z=1}^{S}\binom{S}{z}\left(\frac{P_1}{S}\right)^z q^z \left(\frac{(-q\frac{P_1}{S})^{-z+\frac{2}{\alpha_1}}}{\alpha_1}\right) B_{(-q\frac{P_1}{S}x^{-\alpha_1})}\left[z - \frac{2}{\alpha_1}, 1-S\right] + 2\pi\lambda_2 q P_2 \frac{(O(x))^{\frac{2-\alpha_2}{\alpha_2}}}{\alpha_2 - 2} {}_2F_1\left[\frac{\alpha_2-2}{\alpha_2}, 1; 2-\frac{2}{\alpha_2}; -qP_2(O(x))^{-1}\right], \quad (15)$$

$$D^{(1)}(i) = -\frac{\Gamma\sigma^2 S x^{\alpha_1}}{P_1} - 2\pi\lambda_1 S\Gamma\frac{x^{2-\alpha_1}}{\alpha_1 - 2} {}_2F_1\left[\frac{\alpha_1-2}{\alpha_1}, S+1; 2-\frac{2}{\alpha_1}; -i\Gamma x^{-\alpha_1}\right] - 2\pi\lambda_2\frac{\Gamma S}{P_1} \frac{(O(x))^{\frac{2-\alpha_2}{\alpha_2}}}{\alpha_2 - 2} {}_2F_1\left[\frac{\alpha_2-2}{\alpha_2}, 2; 2-\frac{2}{\alpha_2}; -\frac{i\Gamma S}{P_1}P_2(O(x))^{-1}\right], \quad (16)$$

$$D^{(j)}(i) = 2\pi\lambda_1(-\Gamma)^{\frac{2}{\alpha_1}}\frac{(S+j-1)!}{(S-1)!}\frac{(i)^{-j+\frac{2}{\alpha_1}}}{\alpha_1} B_{(-\Gamma i x^{-\alpha_1})}\left[j - \frac{2}{\alpha_1}, 1-S-j\right] + 2\pi\lambda_2(j!)\frac{(i)^{-j+\frac{2}{\alpha_1}}}{\alpha_1} \left(-\frac{\Gamma S P_2}{P_1}\right)^{\frac{2}{\alpha_1}} B_{(-P_2\frac{\Gamma S i}{P_1}(O(x))^{\frac{-\alpha_1}{\alpha_2}})}\left[j - \frac{2}{\alpha_1}, -j\right], \quad (17)$$

where $O(x) = \left(\frac{P_2 S x^{\alpha_1}}{(N-S+1)P_1}\right)$.

Similarly, $C^2(\Gamma, x)$ for a typical user associated with sub-6 GHz small cell BS at distance x is given as,

$$C^2(\Gamma, x) = \exp\Bigg(-\frac{\Gamma\sigma^2 x^{\alpha_2}}{P_2} - 2\pi\lambda_1 \sum_{z=1}^{S} \binom{S}{z} \left(\frac{P_1 \Gamma x^{\alpha_2}}{SP_2}\right)^z \times \frac{\left(-\frac{\Gamma x^{\alpha_2} P_1}{SP_2}\right)^{-z+\frac{2}{\alpha_1}}}{\alpha_1} B_{\left(\frac{P_1\Gamma x^{\alpha_2}}{SP_2}(M(x))^{-1}\right)}\left[z - \frac{2}{\alpha_1}, 1-S\right] - 2\pi\lambda_2 \Gamma x^{\alpha_2} \frac{x^{2-\alpha_2}}{\alpha_2 - 2} \times {}_2F_1\left[\frac{\alpha_2 - 2}{\alpha_2}, 1; 2 - \frac{2}{\alpha_2}; -\Gamma\right]\Bigg), \tag{18}$$

where $M(x) = \left(\frac{N-S+1}{SP_2} P_1 x^{\alpha_2}\right)$. It can be found following the same steps as outlined in [2].

The connection outage probability for a user associated with mmWave small cell is given by,

$$C^3_{co}(\Gamma) = 1 - \Bigg[A_L C_{3,L}(\Gamma) + A_N C_{3,N}(\Gamma)\Bigg], \tag{19}$$

where $C_{3,L}$ and $C_{3,N}$ are given as,

$$C_{3,L} \approx \sum_{j=1}^{N_L} (-1)^{j+1} \binom{N_L}{j} \times \int_0^\infty \exp\bigg(\frac{-j\epsilon_L x^{\alpha_L}\Gamma\sigma^2}{M_r M_t} - \gamma_j(\Gamma, x) - \theta_j(\Gamma, x)\bigg)\hat{f}_L(x)dx,$$

and

$$C_{3,N} \approx \sum_{j=1}^{N_N} (-1)^{j+1} \binom{N_N}{j} \times \int_0^\infty \exp\bigg(\frac{-j\epsilon_N x^{\alpha_N}\Gamma\sigma^2}{M_r M_t} - \overline{\gamma}_j(\Gamma, x) - \overline{\theta}_j(\Gamma, x)\bigg)\hat{f}_N(x)dx.$$

where

$$\gamma_j(\Gamma, x) = 2\pi\lambda_3 \sum_{i=1}^{4} p_i \int_x^\infty W\bigg(N_L, \frac{j\epsilon_L \hat{a}_i \Gamma x^{\alpha_L}}{N_L t^{\alpha_L}}\bigg)p(t)tdt,$$

$$\theta_j(\Gamma, x) = 2\pi\lambda_3 \sum_{i=1}^{4} p_i \int_{\delta_L(x)}^\infty W\bigg(N_N, \frac{j\epsilon_L \hat{a}_i \Gamma x^{\alpha_L}}{N_N t^{\alpha_N}}\bigg)(1-p(t))tdt,$$

$$\overline{\gamma}_j(\Gamma, x) = 2\pi\lambda_3 \sum_{i=1}^{4} p_i \int_{\delta_N(x)}^\infty W\bigg(N_L, \frac{j\epsilon_N \hat{a}_i \Gamma x^{\alpha_N}}{N_L t^{\alpha_L}}\bigg)p(t)tdt,$$

$$\overline{\theta}_j(\Gamma, x) = 2\pi\lambda_3 \sum_{i=1}^{4} p_i \int_x^\infty W\bigg(N_N, \frac{j\epsilon_N \hat{a}_i \Gamma x^{\alpha_N}}{N_N t^{\alpha_N}}\bigg)(1-p(t))tdt,$$

and $W(N, x) = 1 - 1/(1+x)^N$. Here $\epsilon_L = N_L(N_L!)^{-\frac{1}{N_L}}$ and $\epsilon_N = N_N(N_N!)^{-\frac{1}{N_N}}$. Parameter $\hat{a}_i = a_i/M_r M_t$, a_i and p_i are defined in Section II. The proof is omitted here due to the space limitation and can be found in [1].

The total connection outage probability, C_{co}, is calculated using law of total probability as

$$C_{co} = \sum_{k=1}^{3} C^k_{co} A_k. \tag{20}$$

C. Secrecy Outage Probability

The secrecy outage probability is the measure that at least one of the eavesdroppers is causing the secrecy breach. It is defined for a typical link of k^{th} tier as

$$C^k_{so}(\Gamma_e) = \text{Pr}(\text{SINR}^e_k < \Gamma_e) = 1 - \text{Pr}(\text{SINR}^e_k > \Gamma_e)$$
$$\overset{(a)}{=} 1 - \mathbb{E}_{\phi_k}\Bigg[\mathbb{E}_{\phi_e}\Bigg[\prod_{e\in\phi_e}\bigg(1 - \text{Pr}(\text{SINR}^e_k > \Gamma_e)\bigg)\Bigg]\Bigg]$$
$$\overset{(b)}{=} 1 - \mathbb{E}_{\phi_k}\Bigg[\exp\Bigg[-\lambda_e \int_{\mathbb{R}^2} \text{Pr}(\text{SINR}^e_k > \Gamma_e)de\Bigg]\Bigg],$$

where (b) gives the upper bound on (a) by using independence of fading at each eavesdropper and generating functional of PPP.

The total secrecy outage probability, P_{so}, for the three tier network is defined as

$$C_{so} = \sum_{k=1}^{3} C^k_{so} A_k. \tag{21}$$

The conditional secrecy outage probability for a typical user associated with sub-6 GHz MBS is given as,

$$C^1_{so}(\Gamma_e) = 1 - \exp\Bigg(-2\pi\lambda_e \sum_{i=1}^{N} \binom{N}{i} (-1)^{i+1} \times \int_0^\infty r_e \exp\Bigg[-\frac{i\Gamma_e r_e^{\alpha_1}\sigma^2}{\hat{P}_1} - \zeta^1_1 - \zeta^1_2\Bigg]dr_e\Bigg), \tag{22}$$

where $\hat{P}_1 = \frac{P_1}{S}$ and ζ^1_1 and ζ^1_2 is the characterization of interference from sub-6 GHz MBSs and small cell BSs given as,

$$\zeta^1_1 = 2\pi\lambda_1 \sum_{\mu=1}^{S} \binom{S}{\mu} \int_{r_e}^\infty \frac{(u\hat{P}_1 r^{-\alpha_1})^\mu}{(1 + u\hat{P}_1 r^{-\alpha_1})^S} rdr,$$

$$\zeta^1_2 = 2\pi\lambda_2 \int_{\left(\frac{P_2}{(N-S+1)\hat{P}_1}\right)^{\frac{1}{\alpha_2}} r_e^{\frac{\alpha_1}{\alpha_2}}}^\infty \bigg(\frac{uP_2 r^{-\alpha_2}}{1 + uP_2 r^{-\alpha_2}}\bigg)rdr,$$

respectively, where $u = (\frac{i\Gamma_e r_e{}^{\alpha_1}}{\hat{P}_1})$. Similarly, the conditional secrecy outage probability for a typical user associated with sub-6 GHz small cell BS is given as

$$C^2_{so}(\Gamma_e) = 1 - \exp\Bigg(-2\pi\lambda_e \int_0^\infty r_e \exp\Bigg[-\frac{\Gamma_e r_e^{\alpha_2}\sigma^2}{P_2} - \zeta^2_1 - \zeta^2_2\Bigg]dr_e\Bigg), \tag{23}$$

where

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

$$\zeta^2_2 = 2\pi\lambda_2 \int_{r_e}^\infty \bigg(\frac{uP_2 r^{-\alpha_2}}{1 + uP_2 r^{-\alpha_2}}\bigg)rdr,$$

TABLE I
SIMULATION PARAMETERS

Parameter	Value	Parameter	Value
λ_1	$(500^2 \times \pi)^{-1}$	$f_1 = f_2$	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 [1]

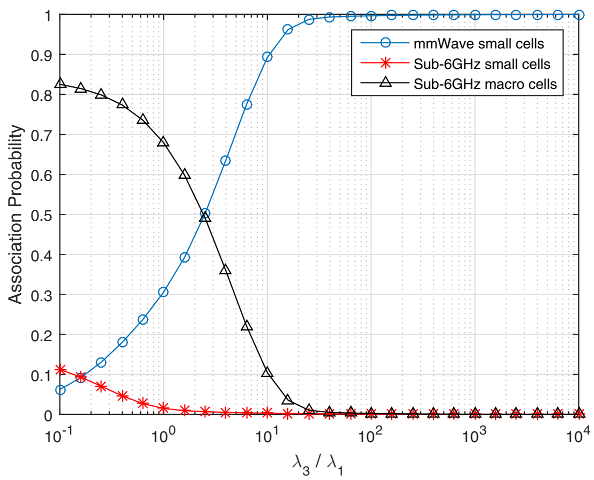

Fig. 1. Connection probability versus λ_3/λ_1 with $\lambda_2 = 30\lambda_1$, $N = 100$ and $S = 5$

where $u = (\frac{\Gamma_e r_e{}^{\alpha_2}}{P_2})$. The conditional secrecy outage probability for a typical user associated with mmWave small cell BS is given as,

$$C_{so}^3(\Gamma_e) = 1 - \exp\Bigg(-2\pi\lambda_e \sum_{j\in\{L,N\}} \sum_{i=1}^{N_j} \binom{N_j}{i} (-1)^{i+1} \times \int_0^\infty r_e \exp\Bigg[-\frac{i\Gamma_e r_e^{\alpha_j}\sigma^2}{P_3 G_e} - \zeta_{3,j}\Bigg] p_j(r_e) dr_e\Bigg), \tag{24}$$

where $p_L(r_e) = e^{(-\beta r_e)}$, $p_N(r_e) = 1 - e^{(-\beta r_e)}$, $\zeta_{3,L} = \gamma_i(\Gamma_e, r_e) + \theta_i(\Gamma_e, r_e)$ and $\zeta_{3,N} = \overline{\gamma}_i(\Gamma_e, r_e) + \overline{\theta}_i(\Gamma_e, r_e)$ respectively.

IV. SIMULATION AND NUMERICAL RESULTS

In this section, we validate the system model by taking a 3-tier HetNet, wherein the first tier (or MBS) and the second tier (or SBS) are assumed to be operating at sub-6GHz band whereas the third tier (or SBS) is operating at the mmWave band. The simulation parameters are outlined in Table I.

We observe the relationship between the association probability and varying mmWave small BS density λ_3 as depicted in Fig. 1. It can be observed that the connection probability with mmWave tier increases with an increase in λ_3. This is due to the fact that with increasing density, the average cell radius of the mmWave small cells decreases bringing the users closer to the mmWave BSs. As mentioned earlier, the LoS probability $p(R)$ is a function of the link distance so bringing the users closer increases the LoS association probability resulting in lesser penetration losses. Although macro BSs have higher transmit power and large array gains, association with macro BSs decreases due to their lower BS density.

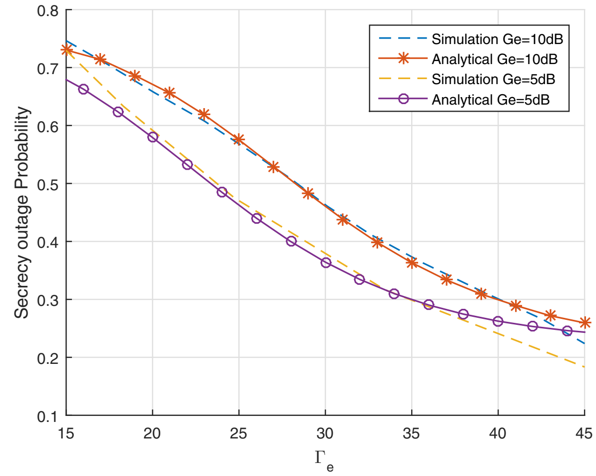

Fig. 2. Secrecy outage probability versus Γ_e(dB) for $\lambda_2 = \lambda_3 = 30\lambda_1$, $N = 5$

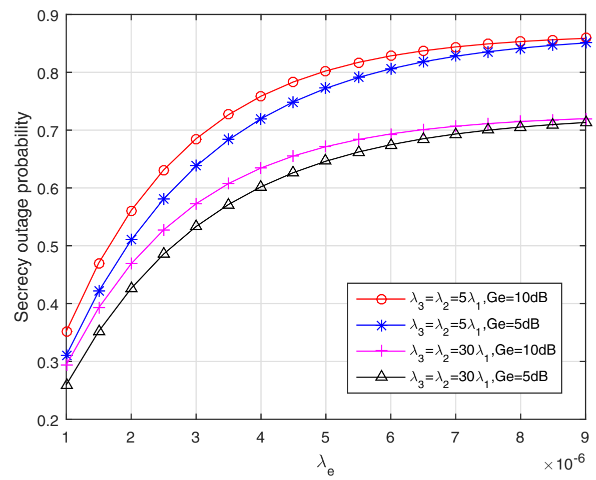

Fig. 3. Secrecy outage probability as the function of λ_e for $\Gamma_e = 40$ dB, $N = 5$

In Fig. 2 we can see the variation in secrecy outage probability versus SINR threshold at the eavesdropper for different eavesdropper antenna gains for mmWave tier and it is observed that secrecy outage probability falls with increase in Γ_e and higher directivity gains lead to increased secrecy outage. Highly directional beamforming at mmWave tier leads to lower connection outage probability but since eavesdroppers too will have higher gains, there is a greater probability of them having SINR greater than threshold and thus transmission secrecy is compromised. Thus, there exists a tradeoff and it is not possible to set highly directional beams at mmWave BSs to improve connection outage while ignoring secrecy outage.

Fig. 3 shows the behavior of secrecy outage probability as the density of eavesdropper is varied for different small cell BS

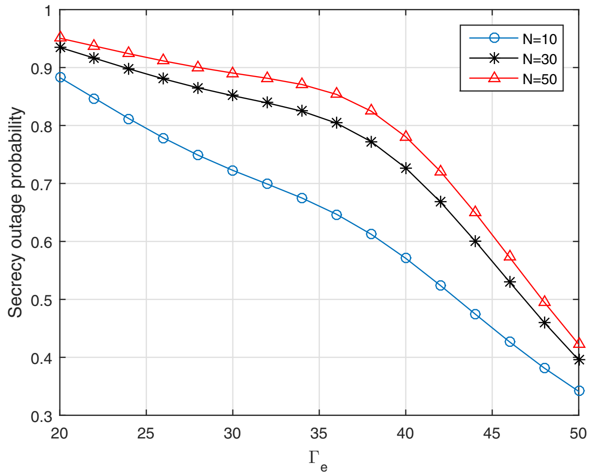

Fig. 4. Secrecy outage probability versus Γ_e(dB) for $G_e = 15$ dB, $\lambda_2 = \lambda_3 = 30\lambda_1$

densities and directional antenna gains at the eavesdroppers. It is observed that higher small cell BS density improves the secrecy of the network as higher density yields greater overall network interference that leads to uncertainty at the eavesdropper and its SINR falls below the threshold. Moreover it is observed that keeping small cell density fixed, lower directional antenna gains at the eavesdroppers improves the secrecy capacity of the network transmissions. Thus lower directional gain and increased interference collectively decrease the chance of eavesdroppers SINR being above threshold.

Fig. 4 shows the secrecy outage probability variation with Γ_e for different number of antennas at macro BSs and it is observed that as the number of antennas at MBSs increases, the secrecy outage probability also increases. This is due to the fact that MBSs are higher power nodes as compared to small cell BSs that leads to better transmission at legitimate as well as eavesdroppers nodes thus eavesdroppers are more likely to have SINR well above threshold. Moreover, when MBSs have higher antenna density, they provide higher array gains and users are less likely to be offloaded to small cells, therefore, overall interference of the network drops, leading to less uncertainty at the eavesdroppers. It can be observed from the figure that there is no substantial increase in secrecy outage after the number of antennas is increased beyond certain limit because after that user association with tiers does not have significant variation.

Fig. 5 shows the connection outage probability for various small cell BS densities and we observe that an increase in small cell BS density results in more users being offloaded to the small cells and it significantly decreases the connection outage probability of the network. As the transmission power of small cell BSs are lower leading to power-efficient network wherein high powered macro BS have lower traffic and density but at the expense of high density of small cell BSs. Moreover, analytical model is validated by simulations.

V. Conclusion

In this paper, we have investigated the impact of massive MIMO and mmWave small cells on the connection and secrecy outage probability of a 3-tier heterogeneous network. User association with BS is based on maximum average received power. Association probability for fixed number of antennas at the MBSs is biased towards mmWave small cells. It has been observed that higher density of sub-6 GHz and mmWave small cells leads to considerable decrease in connection outage and secrecy outage probability. Moreover, it is critical to mention that directivity gains for mmWave BSs and number of antennas at MBSs cannot be increased limitlessly to offload traffic to small cells and decrease network outage capacity since that elevates the secrecy outage capacity, i.e., there exist a tradeoff between secrecy outage and connection outage probability.

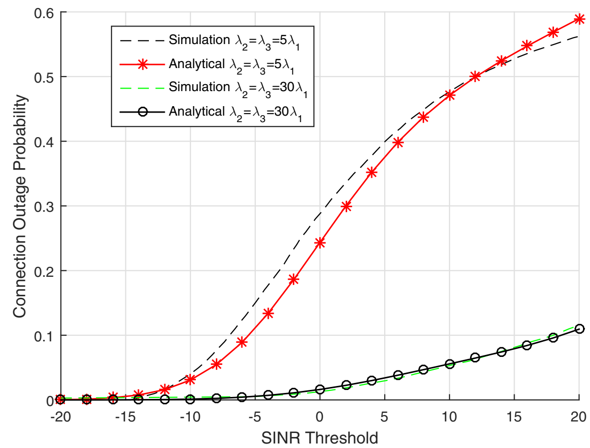

Fig. 5. Connection outage probability versus SINR threshold Γ(dB) with $N = 4$ and $S = 2$

References

[1] 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, 2015.

[2] A.He, L.Wang, Y. Chen, M. Elkashlan and K.K.Wong, "Massive mimo in k-tier heterogeneous cellular networks: Coverage and rate," *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, pp. 1-6, 2015.

[3] S. Vuppala and G. T. F. de Abreu, "Unicasting on the secrecy graph,"*IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1469-1481, 2013.

[4] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, 2008.

[5] 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, 2016.

[6] 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," *85th IEEE Vehicular Technology Conference (VTC Spring), 2017*, pp. 1-5, June 2017.

[7] V. Jungnickel *et al.*,"The role of small cells, coordinated multipoint, and massive MIMO in 5G,"*IEEE Commun. Mag.*, vol. 52, no. 5, pp. 44-51, 2014.

[8] A. Umer, "Stochastic Modeling and Performance Analysis of Multi-tier HetNets," *M.S. Thesis*, School of Electrical Engineering and Computer Science, NUST, Pakistan, 2017.

[9] K. Hosseini , W. Yu and R. S. Adve, "Large-scale mimo versus network mimo for multicell interference mitigation," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 930-941, 2014.

[10] R. W. Heath T. Bai, R. Vaze, "Analysis of blockage effects on urban cellular networks,"*IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 5070-5083, 2014.

[11] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.