An Analysis on Secure Communication in Millimeter/Micro-Wave Hybrid Networks

An Analysis on Secure Communication in Millimeter/Micro-Wave Hybrid Networks

Satyanarayana Vuppala, *Member, IEEE*, Sudip Biswas, *Student Member, IEEE*
and Tharmalingam Ratnarajah, *Senior Member, IEEE*

***Abstract*—The secrecy outage of millimeter wave (mmWave) overlaid micro wave (μWave) networks under the impact of blockages is analyzed, and closed form as well as integral expressions are provided. Specifically, using a network model that accounts for uncertainties both in node locations and blockages, we characterize the conditional connection outage probability and the secrecy outage probability of hybrid networks with multiple eavesdroppers under basic factors such as density of eavesdropping nodes, antenna gain and blockage density. Upper and lower bounds of the conditional secrecy outage probability for both line-of-sight and non line-of-sight links are derived. As a desirable side effect, certain factors such as blockages and reduced antenna gain can decrease the secrecy outage probability in mmWave networks. This can be considered as a tradeoff between outage capacity and secrecy outage capacity with respect to blockages. Hence, blockages which have been proved to be detrimental for achieving higher data rates in mmWave systems, can be helpful for systems with secrecy constraints. Finally, we have shown the co-existence of mmWave and μWave networks from a secrecy perspective.**

***Index Terms*—Secrecy outage, random networks, blockages, millimeter wave**

I. Introduction

In recent years, the explosive growth of mobile data traffic has led to an ever-growing demand for much higher capacity and lower latency in wireless networks. It has culminated in the development of the fifth generation (5G) wireless communication systems, expected to be deployed by the year 2020, with key goals of data rates in the range of Gbps, billions of connected devices, lower latency, improved coverage and reliability, and low-cost, energy efficient and environment-friendly operation. To meet the ever-increasing demands, and keeping in mind that the current wireless spectrum is almost saturated, it is imperative to shift the paradigm of cellular spectrum to a new range of frequencies. In this regard, millimeter wave (mmWave) bands with significant amounts of unused or lightly used bandwidths appear to be a viable way to move forward. With bands of 20-100 GHz available for communication, mmWave can be the cornerstone in the design of 5G networks.

MmWave bands are weak and cannot penetrate through obstacles like buildings, concrete walls, vehicles, trees etc. Due to these limitations, such bands were not considered suitable for cellular transmission for a long time. However, recent studies and measurements [1], [2] have revealed that the significant increase in omnidirectional path loss can be compensated by the proportional increase in overall antenna gain with appropriate beamforming. It was stated in [3] that blockages cause substantial differences in the LOS and NLOS path loss characteristics. Hence, it is important to appropriately model the LOS and NLOS links in mmWave networks. The measurements for path loss were carried out for 73 GHz frequency in [4] and [5] where the first omnidirectional large-scale path loss model was created for backhaul and mobile access in New York City (Urban Environment).

The performance of mmWave cellular systems was analyzed in [6] using real time propagation channel measurements. In [7] a blockage model for mmWave was used to analyze the rate and coverage area of such systems, a distance dependent path loss model along with antenna gain parameters were considered in [8] to characterize the propagation environment in mmWave systems. While, recent literature [2], [6]–[8] focuses on the coverage probability and transmission capacity, physical layer security in mmWave communication has not yet been properly explored.

The implementation of physical layer security in mmWave communication systems is a very promising domain. Some factors have been listed in [9] to leverage mmWave characteristics for exploiting the physical layer security. On one hand, the favorable factors of mmWave systems such as larger bandwidth, directionality, large antenna arrays and short range transmissions can be exploited to provide stronger physical layer security while on the other hand, the propagation characteristics at mmWave frequencies needs to be modeled precisely.

For example, the malicious user can implant highly directional antennas to intercept the communication. Also, larger antenna arrays at the malicious user will give him higher degrees of freedom to decode the message. Furthermore, the addition of blockages may add uncertainty to the performance of legitimate communication. This uncertainty may be beneficial or a hindrance to the legitimate node, which we will explore in a later section of the paper. It is of paramount importance to characterize the achievable secrecy in mmWave networks along with current micro wave (μWave) cellular systems.

A great effort has been made to develop information-theoretic security [10]–[12], which indicates the possibility of securing communication links without cryptography and in the presence of transparent eavesdroppers. The theoretical foundations of information-theoretic security were led by

This work is supported by the Seventh Framework Programme for Research of the European Commission under grant number ADEL-619647. T. Ratnarajah is supported by the U.K. Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/L025299/1.

S. Vuppala, S. Biswas, and T. Ratnarajah are with the Institute for Digital Communications, the University of Edinburgh, King's Building, Edinburgh, UK, EH9 3JL.

Wyner, who introduced the concept of wire-tap channel and analyzed the existence of a reliable transmission condition to achieve perfect secrecy in discrete memoryless channels [10]. Since then, the concept of information-theoretic security, i.e. physical layer security, has been extended to specific channels, such as, additive white Gaussian noise (AWGN) channels by Cheong and Hellman [11], and broadcast wireless channel by Csiszár and Körner [12]. In this direction, channel propagation effect has been taken into consideration. For instance, the secrecy capacity of wireless fading channels was investigated in [13] based on the channel state information (CSI). Expressions for the outage probability and average secrecy capacity of quasi-static fading channels were derived in [14] by studying both the perfect and imperfect CSI scenarios.

Noticeably, previous works in the area such as those aforementioned are marked by significant abstraction from practical applicability, with various factors of relevance ignored for the sake of simplicity, to include: 1) the fact that wireless channels are often *subjected to fading* and 2) the fact that communicating devices often compose *networks* of *unknown topology* (randomly distributed nodes).

A few decades later, the increasing prospect of putting information theoretical secrecy concepts to actual use has motivated the community to deepen its understanding of the inherent secrecy capabilities of wireless systems by taking into account more realistic conditions of the wireless medium. Addressing point 1, for instance, the secrecy capacity of wireless fading channels was investigated in [13], [15] with expressions for the outage probability and average secrecy capacity of quasi-static fading channels also derived expressions in [14]. Considering point 2, and specifically when studying wireless secrecy in random networks using stochastic-geometric tools [16], the notion of *secrecy graphs* has emerged [17].

Following this trend, secrecy capacity scaling laws were studied in [18] and recently a new perspective on the role of node spatial distribution with wireless propagation mediums and aggregate network interference on network secrecy has been given in [19]. The secrecy capacity of unicast links in the presence of eavesdroppers was investigated in [20], where the transmission to the k-th legitimate node was based on the order of the distance between the source and the destination. Although there is an increasing tendency of research on intrinsic secrecy in random wireless networks, most current works focus on μWave systems which do not take into consideration the effect of blockages. Hence, it is imperative to devise a more general model which can take into account blockage effects and various wireless propagation mediums.

To the best of the authors' knowledge, characterization of secrecy outage considering blockages at the legitimate user or eavesdropper has not yet been evaluated in mmWave random networks. In this article, we consider a mmWave overlaid μWave network in the presence of eavesdroppers. We model the received signal-to-interference-noise ratio (SINR) distributions at the user and eavesdroppers and consequently the expressions for the connection outage probability and secrecy outage probability of random mmWave networks in the presence of eavesdroppers are derived. At this point we would like to state that this model is applicable only to an outdoor typical user. We consider a stochastic geometry approach to characterize the spatially distributed μWave, mmWave base stations (BSs) and the eavesdroppers. It is assumed that the BSs and the eavesdroppers in the mmWave overlaid network follow PPPs but are independent of each other.

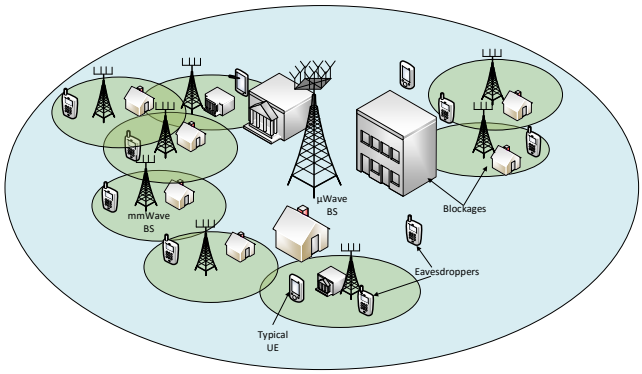


Fig. 1: An illustration of a mmWave overlaid μWave network model.

The remainder of the paper is organized as follows. The system model is described in Section II, where the formulations of the blockage model and the received SINR's are briefly revised and preliminaries about perfect transmission and association probabilities are discussed in Section III. In Section IV, we characterize the connection and secrecy outage probabilities for μWave links, while Section V models the outage probabilities for mmWave links. Based on those derived expressions, numerical results are drawn and briefly discussed in Section VI. Finally, concluding remarks are offered in section VII.

II. System Model

We consider the secure downlink transmission in a hybrid cellular network comprising of both mmWave and μWave networks as shown in Fig. 1. The mmWave BSs are modeled as a two dimensional homogeneous poisson point process (HPPP) Φ_m with density λ_m, while the μWave BSs follow another homogeneous PPP Φ_μ with density λ_μ. The eavesdroppers also follow a PPP Φ_e with density λ_e. All the processes are independent of each other. A typical user equipment (UE) is assumed to be located at origin. A simple offloading technique is adopted wherein the typical UE is offloaded to the μWave network if the capacity achieved on the mmWave network drops below a certain threshold. Similar offloading strategies were analyzed in [8] and stated to be reasonable for mmWave based networks.

Directional beamforming modeling: Due to the small wavelength of mmWaves, directional beamforming can be exploited for compensating the path loss and additional noise. Accordingly, antenna arrays are deployed at the transmitter and receiver pairs. In our model, we assume all the transmit and receiver pairs to be equipped with directional antennas with sectorized gain pattern. In particular, we assume that both the transmit and receiver pairs implement beamforming and main

lobe is aligned in the direction of dominant propagation path while side lobe directs energy in all other directions. Let θ be the beamwidth of the main lobe. Then the antenna gain pattern of node about some angle ϕ is given as [21]

$$G_q(\theta) = \left\{ \begin{array}{ll} G_q^{\max} & \text{if} |\phi| \leq \theta \\ G_q^{\min} & \text{if} |\phi| \geq \theta \end{array} \right\}, \quad (1)$$

where $q \in \text{UE}, \text{BS}$, $\phi \in [0, 2\pi)$ is the angle of boresight direction, $G_q^{(max)}$ and $G_q^{(min)}$ are the array gains of main and side lobes, respectively. Similarly, the user gain pattern can also be modeled. However, following the approach as used in [8], we consider omnidirectional antennas at the UE. The beams of all non-intended links are assumed to be randomly oriented with respect to each other and hence the effective antenna gains on the interfering links are random. For simplicity, we assume that the link between the BS and the UEs is aligned and henceforth, we consider the gain to be G.

Blockage modeling: We consider the blockages to be stationary blocks which are invariant with respect to directions. Leveraging the modeling of blockage in [22], we consider a two state statistical model for each and every link. The link can be either LOS or NLOS. LOS link occurs when there is a direct propagation path between the BS and the UE while NLOS occurs when the link is blocked and the UE receives the signal through reflection from a blockage. Let the LOS link be of length r, then the probabilities of occurrence $p_{\text{L}}(.)$ and $p_{\text{N}}(.)$ of LOS and NLOS states respectively can be given as a function of r as

$$p_{\text{L}}(r) = e^{-\beta r}, \quad p_{\text{N}}(r) = 1 - e^{-\beta r}, \quad (2)$$

where β is the blockage density.

Another model that has been considered in literature is a fixed LOS probability model, as was depicted in [8]. Let the LOS area within a circular ball of radius r_D be centered around the reference point. Then, if the LOS link is of length r, the probability of the connection link to be LOS is given by p_{L} if $r < r_D$ and 0 otherwise. The parameters r and r_D are dependent on the geographical and deployment scenario of the network. Our results are based on the data from [8].

SINR modeling: By a slight abuse of notation, we consider Φ_m to be the set of interfering locations. The received SINR for the typical UE can now be defined as

$$\zeta_{m_l} \triangleq \frac{P_m G_l |h_{m_l}|^2 {r_l}^{-\alpha_m}}{\sigma_m^2 + \sum\limits_{i \in \Phi_m} P_m G_i |h_{m_i}|^2 r_i^{-\alpha_m}}, \quad (3)$$

where G_l is the antenna array gain function, h_{m_l} is the fading gain at the UE of interest, r_l is the link length, σ_m^2 is the noise power. h_{m_i} denotes each interference fading gain and r_i is the distance from the interferer i to the typical UE.

Similarly, SINR at any eavesdropper can be given as

$$\zeta_{m_{\text{e}}} \triangleq \frac{P_m G_{\text{e}} |h_{m_{\text{e}}}|^2 {r_{\text{e}}}^{-\alpha_m}}{\sigma_m^2 + \sum\limits_{i \in \Phi_m} P_m G_i |h_{m_i}|^2 r_i^{-\alpha_m}}. \quad (4)$$

In mmWave networks, small scale fading does not have as much of an impact on transmitted signals as compared to lower frequency systems. It is mentioned in literature [1], [2] that in mmWave analysis, small scale fading can be ignored. However, to capture generalized propagation environment and for analytical tractability, we consider Nakagami fading model[1].

TABLE I: Notations

Notation	Description
Φ_μ	Poisson Point Process (PPP) of μWave BS
λ_μ	Density of μWave BS
Φ_m	PPP of mmWave BS
λ_m	Density of mmWave BS
Φ_{e}	Poisson Point Process (PPP) of eavesdropper
λ_{e}	Density of eavesdropper
ζ_{μ_l}	The received SINR from μWave BS
ζ_{m_l}	The received SINR from mmWave BS
m	Nakagami-m Figure
P_μ	Transmit power at μWave BS
P_m	Transmit power at mmWave BS
α_μ	Path loss exponent for μWave systems
α_m	Path loss exponent for mmWave systems
G_{e}	Antenna gain at eavesdropper

Under Nakagami-m channel model [16], the channel power is distributed according to

$$H_m \sim f_{H_m}(x; m) \triangleq \frac{m^m x^{m-1} e^{-mx}}{\Gamma(m)}, \quad (5)$$

where m is the Nakagami fading parameter and $\Gamma(m)$ is the gamma function.

μWave modeling: The μWave channels are modeled similarly to its mmWave counterparts with the only exception that the antennas[2] are now omni-directional with transmitted signal power P_μ at μWave BSs and path loss exponent α_μ. It is to be noted that blockage effects are neglected for μWave systems due to very low penetration loss of μWave signals.

Under the consideration of separate encoding scheme at each BS, ith BS sends an information symbol s_i through a linear beamforming vector $\mathbf{v}_i = [\nu_i^1, \cdots, \nu_i^{N_t}]^T$ with unit norm, i.e., $||\mathbf{v}_i||_2 = 1, i \in \Phi_\mu$. Here, N_t is the number of antennas at the ith μWave BS. Therefore, the received signal at the typical UE can be given as

$$y = \sqrt{P_\mu} \mathbf{h}_{1,l} \mathbf{v}_l {r_l}^{-\alpha_\mu/2} s_l + \sum_{i \in \Phi_\mu} \mathbf{h}_{1,i} \mathbf{v}_i {r_i}^{-\alpha_\mu/2} s_i + \omega_1, \quad (6)$$

where $\mathbf{h}_{1,i} = [h_{1,i}^1, \cdots, h_{1,i}^{N_t}] \in \mathbb{C}^{1 \times N_t}$ is the downlink channel between ith μWave BS to the typical UE[3] and each entry is independently identically distributed (IID) complex gaussian random variable with zero mean and unit variance. ω denotes the additive Gaussian noise.

Without loss of generality, we consider a μWave UE located at the origin. For notational simplicity, we remove the subscript 1 from the channel vector. Accordingly, the received SINR

[1]The choice of Nakagami-m fading to simulate the small scale fading is commonly used in literature [1], [21], [22].

[2]We assume that the μWave BSs are equipped with N_t antennas and UEs are equipped with single antenna.

[3]The subscript 1 in $\mathbf{h}_{1,l}$ corresponds to the typical UE.

for the typical UE and any eavesdropper can now be given respectively as

$$\zeta_{\mu_l} \triangleq \frac{P_\mu |\mathbf{h}_{\mu_l}\mathbf{v}_l|^2 r_l{}^{-\alpha_\mu}}{\sigma_\mu^2 + \sum\limits_{i\in\Phi_\mu} P_\mu |\mathbf{h}_{\mu_i}\mathbf{v}_i|^2 r_i^{-\alpha_\mu}}, \tag{7}$$

$$\zeta_{\mu_e} \triangleq \frac{P_\mu |\mathbf{h}_{\mu_e}\mathbf{v}_l|^2 r_e{}^{-\alpha_\mu}}{\sigma_\mu^2 + \sum\limits_{i\in\Phi_\mu} P_\mu |\mathbf{h}_{\mu_i}\mathbf{v}_i|^2 r_i^{-\alpha_\mu}}. \tag{8}$$

III. Definitions and Preliminaries

A. Perfect transmission characterization

In our system model, the communication links in both the microwave and mmWave are assumed to be eavesdropped. To combat this and enhance security, each link adopts a secrecy coding scheme called Wyner code [10]. Hence, two kinds of rates, namely the rate of transmitted confidential code words R_s and the rate of the transmitted messages R_l, need to be characterized at the transmitter. Depending on the choices of R_l and R_s in the Wyner encoding scheme, the following outage schemes are bound to happen.

Consider a scenario where a BS wishes to reliably and securely transmit the confidential messages to its intended user in the presence of eavesdroppers. In such a scenario, the following definitions in [23] are worth mentioning here:

Non-zero capacity event: This occurs if the rate of transmitted message R_ℓ is below the capacity of the link and the received message is decoded with an arbitrarily small error.

Non-zero secrecy capacity event: This happens if the rate $R_s - R_\ell$ is above the rate of the most detrimental eavesdropping link and the received message at the user provides no information about the transmitter.

Remark 1: For given SINR thresholds T_l and T_e, any transmission is said to be perfect if $\zeta_{m_l/\mu_l} > T_l$ and $\zeta_\mathrm{e} < T_\mathrm{e}$[4].

However, due to the wireless medium of communication, it is appropriate to characterize their corresponding non-outage probabilities with the perfect transmission scheme.

Remark 2: Therefore, the transmission is said to be (θ,ϵ)-perfect transmission if $\Pr\{\zeta_{m_l/\mu_l} > T_l\} \geq \theta$ and $\Pr\{\zeta_\mathrm{e} < T_\mathrm{e}\} \geq \epsilon$ where θ and ϵ denote the minimum non-outage constraints at the user and the most detrimental eavesdropper respectively.

Consequently, any transmission is said to be secure if and only if (1,1)-perfect transmission is achieved. Additionally, for (θ,ϵ)-perfect transmission, $1-\theta$ and $1-\epsilon$ represent the maximum connection outage probability and maximum secrecy outage probability respectively. Accordingly, we define two important metrics of interest as given below.

Connection outage probability: We assume that the typical UE associates itself with its strongest BS node. Thus, the connection outage probability can occur when the UE is connected to the strongest BS and if the received SINR falls below T_l. It can be mathematically represented as

$$\mathcal{P}_\mathrm{co}(T_l) = \Pr\left[\max_{x\in\Phi_{m_l/\mu_l}} \zeta(x) < T_l\right]. \tag{9}$$

Since the mmWave and μWave networks follow two independent PPPs, it is possible to perform the analysis on both the processes independently with an association probability. Let p_{mm} be the probability that the typical UE is offloaded to the mmWave network, then $p_\mu = 1 - p_{mm}$ is the probability that the typical UE is offloaded to the μWave network. Accordingly, the total connection outage probability can be given as

$$\mathcal{P}_\mathrm{co}(T_l) = \mathcal{P}_\mathrm{co}^\mathrm{mm}(T_l)p_{mm} + \mathcal{P}_\mathrm{co}^\mu(T_l)p_\mu \tag{10}$$

where $\mathcal{P}_\mathrm{co}^\mathrm{mm}(T_l)$ and $\mathcal{P}_\mathrm{co}^\mu(T_l)$ denotes the conditional connection outage probabilities of mmWave and μWave networks, respectively.

Secrecy outage probability: If the capacity of the channel from the BS to any eavesdroppers is above the rate R_e, *i.e.*, $\log_2(1+\zeta_\mathrm{e}) > R_\mathrm{e}$, the security of the message is compromised. In other words, the confidential message may not be perfectly secure against the eavesdropper in $\mathbb{R}^2$. The probability of this event is known as secrecy outage probability [23], which is denoted by $\mathcal{P}_s$.

Assume a set of eavesdroppers that can cause secrecy outage as $B_e = \{i \in \Phi_e : \zeta_i > T_\mathrm{e}\}$. Hence, we can define the indicator function, $\mathbf{1}_A(e)$, which equals to 1 when the eavesdropper e is in the set B_e. The secrecy outage probability can thus be described as the probability that at least one of the eavesdroppers in set B_e causes a secrecy outage, which can be written as [23],

$$\mathcal{P}_s(T_\mathrm{e}) = 1 - \mathbb{E}_{\Phi_{m_l/\mu_l}}\left[\mathbb{E}_{\Phi_\mathrm{e}}\left[\mathbb{E}_X\Big[\prod_{\mathrm{e}\in B_\mathrm{e}}\big(1-1_A(\mathrm{e})\big)\Big]\right]\right], \tag{11}$$

$$= 1 - \mathbb{E}_{\Phi_{m_l/\mu_l}}\left[\mathbb{E}_{\Phi_\mathrm{e}}\Big[\prod_{\mathrm{e}\in\Phi_\mathrm{e}}\big(1-\Pr(\zeta_\mathrm{e} > T_\mathrm{e})\big|_{\Phi_{m_l/\mu_l},\Phi_\mathrm{e}}\Big]\right].$$

This follows from the independence of fading at each eavesdropper so that the expectation on $X = (h_{m_\mathrm{e}}/h_{\mu_\mathrm{e}}, h_{m_i}/h_{\mu_i})$ can be moved inside the product of Φ_e. Since it is difficult to express $\mathcal{P}_s(T_\mathrm{e})$, we consider the upper bound of equation (11) which can be obtained by using the generating functional of a PPP [23], [24] as[5]

$$\mathcal{P}_s(T_\mathrm{e}) = 1 - \mathbb{E}_{\Phi_{m_l/\mu_l}}\left[\exp\Big[-\lambda_\mathrm{e}\int_{\mathbb{R}^2}\Pr\big(\zeta_\mathrm{e} > T_\mathrm{e}\big|_{\Phi_{m_l/\mu_l}}\big)de\Big]\right]. \tag{12}$$

Similar to connection outage probability characterization, the total secrecy outage probability can be given as

$$\mathcal{P}_s(T_\mathrm{e}) = \mathcal{P}_s^{mm}(T_\mathrm{e})p_{mm} + \mathcal{P}_s^\mu(T_\mathrm{e})p_\mu \tag{13}$$

where $\mathcal{P}_s^{mm}(T_\mathrm{e})$ and $\mathcal{P}_s^\mu(T_\mathrm{e})$ denotes the conditional secrecy outage probabilities of mmWave and μWave networks, respectively.

[4]The subscripts μ_e and m_e are replaced with e hereinafter as the eavesdropper can operate in both mmWave or μWave frequencies. $T_l \triangleq 2^{R_l} - 1$ and $T_\mathrm{e} \triangleq 2^{R_e} - 1$ are the threshold SINR of any legitimate and eavesdropper nodes, respectively.

[5]Unless explicitly mentioned in the equations, we perform the analyses using the secrecy outage expression for upper bound as given in (12).

In addition, the lower bound of the secrecy outage probability can be obtained by considering only the nearest eavesdropper as

$$\mathcal{P}_s^{\mathrm{LB}}(T_{\mathrm{e}}) = \int_0^{\infty} \Pr\{\zeta_{\mathrm{e}}(r) > T_{\mathrm{e}}\} f_{r_e}(r_{\mathrm{e}}) \mathrm{d}r_{\mathrm{e}}, \tag{14}$$

where $f_{r_e}(r)$ represents the probability distribution function (PDF) of the distance between the nearest eavesdropper to the associated BS. As the eavesdroppers are distributed according to a homogeneous PPP distribution with density λ_{e}, the distribution of the nearest neighbor is shown in [24] as

$$f_{r_{\mathrm{e}}}(r_{\mathrm{e}}) = 2\pi\lambda_{\mathrm{e}} r_{\mathrm{e}} \exp(-\lambda\pi r_{\mathrm{e}}^2). \tag{15}$$

B. Association probability

In this subsection, we give some qualitative comments on μWave and mmWave tiers' association probabilities. It is assumed that the typical UE is associated with the best BS, which provides the UE with the strongest signal. We consider an identical bias factor B_μ or B_{mm} [25], [26], which is always positive. When $B = 1$, no biasing is considered and the association goes back to a traditional cell association based on maximum received power or nearest node. We consider that the UE is offloaded to either μWave or mmWave network depending on the maximum received signal from BSs. Leveraging the analysis from [25], we consider that the UE is connected to the best BS in terms of long term averaged biased received power. In such cases, the UE association is generally conditioned on the least path loss distribution. So, it is important to characterize such distributions in mmWave networks under the effect of blockages. As mentioned earlier in section II, any link *i.e* the distance between the UE and BS in a mmWave network depends on the exponential blockage probability model. Therefore, the least pathloss distribution in a mmWave network is not the same as for the case of a μWave network, as given in (15).

Lemma 1. *The least path loss distribution in a mmWave network can be given as*

$$\begin{aligned} F_{\xi_l}^{\mathrm{mm}}(r) = 1 - \exp\Bigg(& -\pi\lambda_m (rP_m G_l B_m)^{\frac{1}{\alpha_N}} \\ & - \tfrac{2\pi\lambda_m}{\beta^2}\left(1 - e^{-\beta(rP_m G_l B_m)^{\frac{1}{\alpha_L}}}\left(1 + \beta(rP_m G_l B_m)^{\frac{1}{\alpha_L}}\right)\right) \\ & + \tfrac{2\pi\lambda_m}{\beta^2}\left(1 - e^{-\beta(rP_m G_l B_m)^{\frac{1}{\alpha_N}}}\left(1 + \beta(rP_m G_l B_m)^{\frac{1}{\alpha_N}}\right)\right)\Bigg). \end{aligned} \tag{16}$$

Proof. The proof of this lemma can be obtained from the proof of Theorem 1 of [27]. However, we present a sketch of the proof here, since we repeatedly use the following approach in later sections of the paper. Consider a point process, where the points represent the path loss between the UE and randomly placed BSs in a mmWave network. Let $\phi_{\mathrm{mm}} = \left\{\xi_l \triangleq \frac{x_l^{\alpha_m}}{P_m G_l B_m}\right\}$ be a homogeneous PPP of intensity λ_m. Here, the distance is a random variable, and its LOS state occurs with the probability of $e^{-\beta x}$. By using Mapping theorem [28, Theorem 2.34], the density function of this one dimensional PPP under the effect of blockages can be given as

$$\begin{aligned} \Lambda([0,r]) = & \int_0^{(rP_m G_l B_m)^{\frac{1}{\alpha_L}}} 2\pi\lambda_m x e^{-\beta x} \mathrm{d}x \\ & + \int_0^{(rP_m G_l B_m)^{\frac{1}{\alpha_N}}} 2\pi\lambda_m x (1 - e^{-\beta x}) \mathrm{d}x. \end{aligned} \tag{17}$$

Using the void probability of a PPP and with the help of (17), the least path loss distribution in a mmWave network can be given as (16). □

Proposition 1. *The association probability that a typical UE is connected to the μWave network is given by*

$$p_\mu = 2\pi\lambda_\mu \int_0^{\infty} r \exp\left(-\Lambda_m\left(\left(\tfrac{\bar{P}_{\mathrm{mm}}}{\bar{P}_\mu}\right)^{\frac{1}{\alpha_m}} r^{\frac{\alpha_\mu}{\alpha_m}}\right)\right) e^{-\pi\lambda_\mu r^2} \mathrm{d}r, \tag{18}$$

where $\bar{P}_{\mathrm{mm}} = P_m G_l B_m; \bar{P}_\mu = P_\mu B_\mu$ and

$$\begin{aligned} \Lambda_m\left(\tfrac{\bar{P}_{\mathrm{mm}}}{\bar{P}_\mu}^{\frac{1}{\alpha_m}} r^{\frac{\alpha_\mu}{\alpha_m}}\right) = & \pi\lambda_m \left(\tfrac{\bar{P}_{\mathrm{mm}}}{\bar{P}_\mu}\right)^{\frac{1}{\alpha_N}} r^{\frac{\alpha_\mu}{\alpha_N}} \\ & - \tfrac{2\pi\lambda_m}{\beta^2}\left(1 - e^{-\beta\left(\frac{\bar{P}_{\mathrm{mm}}}{\bar{P}_\mu}\right)^{\frac{1}{\alpha_N}} r^{\frac{\alpha_\mu}{\alpha_N}}}\left(1 + \beta\left(\tfrac{\bar{P}_{\mathrm{mm}}}{\bar{P}_\mu}\right)^{\frac{1}{\alpha_N}} r^{\frac{\alpha_\mu}{\alpha_N}}\right)\right) \\ & + \tfrac{2\pi\lambda_m}{\beta^2}\left(1 - e^{-\beta\left(\frac{\bar{P}_{\mathrm{mm}}}{\bar{P}_\mu}\right)^{\frac{1}{\alpha_L}} r^{\frac{\alpha_\mu}{\alpha_L}}}\left(1 + \beta\left(\tfrac{\bar{P}_{\mathrm{mm}}}{\bar{P}_\mu}\right)^{\frac{1}{\alpha_L}} r^{\frac{\alpha_\mu}{\alpha_L}}\right)\right). \end{aligned} \tag{19}$$

Proof. This proof can be obtained by leveraging results of Lemma 1 and [25, Lemma 1]. A sketch of the proof is given in Appendix A for the sake of completeness. □

Similarly, one can obtain the association probability p_{mm} using the above analysis.

IV. Secrecy Outage Probability: μWave Link

In this section, we derive the conditional connection outage probability and the conditional secrecy outage probability of μWave links. Before proceeding further, we would like to state that we will start this section with the noise limited scenario. This is just to keep the analysis tractable with respect to mmWave systems, where it has been explicitly mentioned in [2], [6], [8] that these networks in urban settings tend to be noise limited rather than interference limited. However, it is different for μWave systems where interference dominates the noise. Accordingly, we will also consider the case where both noise and interference play equivalent roles in determining the SINR. Let us first consider the noise limited case where noise power dominates the interference power. Using (9), the connection outage probability of any microwave link by neglecting interference is given in Proposition 1.

Proposition 2. *The conditional connection outage probability of a typical μWave link in mmWave overlaid cellular networks is given as*

$$\mathcal{P}_{\rm co}^{\mu}(T_l) = \exp\left(-\pi\lambda_{\mu} P_{\mu}^{\frac{2}{\alpha}} T_{\ell}^{\frac{-2}{\alpha}} \mathbb{E}_{H_{\mu}}\left(h_{\mu_l}^{\frac{2}{\alpha}}\right)\right). \tag{20}$$

Proof. The proof is given in Appendix B. □

Similarly, the conditional secrecy outage probability is given in Proposition 2.

Proposition 3. *The conditional secrecy outage probability of a typical μWave link in mmWave overlaid cellular networks is given as*

$$\mathcal{P}_{s}^{\mu}(T_{\rm e}) = 1 - \times \exp\left(-\frac{2\pi\lambda_{\rm e}\Gamma(\frac{2}{\alpha_{\mu}})}{\alpha_{\mu}}\left(\frac{AT_{\rm e}\sigma_{\mu}^2}{P_{\mu}}\right)^{\frac{-2}{\alpha_{\mu}}}\sum_{i=1}^{N_t}\binom{N_t}{i}(-1)^{i+1} i^{\frac{-2}{\alpha_{\mu}}}\right). \tag{21}$$

Proof. Denoting the integral expression in (12) as $\mathcal{M}$, we have

$$\begin{aligned}
\mathcal{M} &= \int_0^{\infty} \Pr\left(\frac{P_{\mu}|\mathbf{h}_{\mu_{\rm e}}\mathbf{v}_{\rm e}|^2 {r_{\rm e}}^{-\alpha_{\mu}}}{\sigma_{\mu}^2} > T_{\rm e}\right), \qquad (22)\\
&= \int_0^{\infty} \Pr\left(|\mathbf{h}_{\mu_{\rm e}}\mathbf{v}_{\rm e}|^2 > \frac{T_{\rm e}{r_{\rm e}}^{\alpha_{\mu}}\sigma_{\mu}^2}{P_{\mu}}\right),\\
&\overset{(a)}{=} \int_0^{\infty} r_{\rm e}\left(1 - \left(1 - e^{-\frac{AT_{\rm e}{r_{\rm e}}^{\alpha_{\mu}}}{P_{\mu}}}\right)^{N_t}\right){\rm d}r_{\rm e},\\
&\overset{(b)}{=} \sum_{i=1}^{N_t}\binom{N_t}{i}(-1)^{i+1}\int_0^{\infty} r_{\rm e} e^{-\frac{iAT_{\rm e}{r_{\rm e}}^{\alpha_{\mu}}}{P_{\mu}}}{\rm d}r_{\rm e},\\
&= \frac{\Gamma(\frac{2}{\alpha_{\mu}})}{\alpha_{\mu}}\left(\frac{AT_{\rm e}\sigma_{\mu}^2}{P_{\mu}}\right)^{\frac{-2}{\alpha_{\mu}}}\sum_{i=1}^{N_t}\binom{N_t}{i}(-1)^{i+1} i^{\frac{-2}{\alpha_{\mu}}},
\end{aligned}$$

where (a) is the result of $H_{\mu} = |\mathbf{h}_{\mu_{\rm e}}\mathbf{v}_{\rm e}|^2$, which follows a chi-square distribution [29] with $2N_t$ degrees of freedom and uses the tight upper bound of gamma random variable of parameter ξ as

$$\Pr\{H_{\mu} < \gamma\} < (1 - e^{-A\gamma})^{\xi}, \tag{23}$$

with $A = \frac{\xi}{(\xi!)^{-1/\xi}}$ and (b) is the result of binomial expansion. This proof concludes by substituting the closed form expression of $\mathcal{M}$ in (12). □

Now taking interference into account, the conditional secrecy outage probability can be derived similarly as

$$\mathcal{P}_{s}^{\mu}(T_{\rm e}) = 1 - \exp\left(-2\pi\lambda_{\rm e}\sum_{i=1}^{N_t}\binom{N_t}{i}(-1)^{i+1} \times \int_0^{\infty} r_{\rm e} e^{-\frac{iAT_{\rm e}\sigma_{\mu}^2{r_{\rm e}}^{\alpha_{\mu}}}{P_{\mu}}}\mathbb{E}_{I_{\mu}}\left[e^{-\frac{iAT_{\rm e}{r_{\rm e}}^{\alpha_{\mu}}}{P_{\mu}}I_{\mu}}\right]{\rm d}r_{\rm e}\right), \tag{24}$$

where $\mathbb{E}_{I_{\mu}}[.]$ is the Laplace characterization of interference from all other μWave BSs.

V. Secrecy Outage Probability: mmWave Link

In this section[6], we derive the conditional connection outage probability and the conditional secrecy outage probability of mmWave cellular links. As discussed before, such networks in urban settings tend to be noise limited rather than interference limited, which is due to the fact that in the presence of blockages, the signals received from unintentional sources are close to negligible. In such densely blocked scenarios (typical for urban settings), SNR provides a good enough approximation to SINR for directional mmWave networks. As mentioned before, in the following analysis we consider two blockage models:

A. Random blockage model

Here, we leverage the modeling of blockage from [22] where blockages are modeled randomly with LOS probability of $e^{-\beta r}$. In conjunction to the previous section, we characterize the conditional secrecy outage probability without considering interference in first part, and interference in the second.

Proposition 4. *The conditional connection outage probability of a typical mmWave link for random blockage model is given as*

$$\mathcal{P}_{\rm co}^{\rm mm}(T_l) = \exp\left(-\sum_{j\in{\rm L,N}}\frac{2\pi\lambda_m}{\alpha_j}\left(\frac{P_m G_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}} \times \int_{T_l}^{\infty} y^{\frac{-2}{\alpha_j}-1}\int_0^{\infty} p_j(\tfrac{y}{z}) z^{\frac{2}{\alpha_j}} f_{H_m}(z)\,{\rm d}z{\rm d}y\right). \tag{25}$$

Proof. The proof is given in Appendix C. □

***Corollary* 1.** *The conditional connection outage probability of the typical mmWave link for the case of Additive white Gaussian noise (AWGN) is given as*

$$\mathcal{P}_{\rm co}^{\rm mm}(T_l) = \exp\left(\pi\lambda\left(\frac{T_l\sigma_m^2}{P_m G_l}\right)^{-\frac{1}{\alpha_{\rm N}}} - \frac{2\pi\lambda}{\beta^2}\sum_{j\in{\rm L,N}}\left(\frac{P_m G_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}} \left(e^{-\beta\left(\frac{T_l\sigma_m^2}{P_m G_l}\right)^{-\frac{1}{\alpha_j}}}\left(-1 - \beta\left(\frac{T_l\sigma_m^2}{P_m G_l}\right)^{-\frac{1}{\alpha_j}}\right)\right)\right). \tag{26}$$

Proof. A detailed proof is given in Appendix D. □

Proposition 5. *The conditional secrecy outage probability of a typical mmWave for random blockage model link can be given as*

$$\mathcal{P}_{s}^{\rm mm}(T_{\rm e}) = 1 - \exp\left(-2\pi\lambda_{\rm e}\sum_{j\in{\rm L,N}}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1} \times \int_0^{\infty} r_{\rm e} e^{-\frac{iAT_{\rm e}\sigma_m^2{r_{\rm e}}^{\alpha_j}}{P_m G_{\rm e}}} p_j(r_{\rm e}){\rm d}r_{\rm e}\right). \tag{27}$$

[6]For tractable analysis, we take the interference into account only for the case secrecy outage probability.

Proof. The proof follows from the Proposition 2. However, for better understanding, readers can follow the proof from Appendix E. □

LOS analysis: In mmWave systems, the performance gap between LOS and NLOS regimes is quite large. Therefore, it is of paramount importance to characterize the LOS regime.

***Corollary* 2.** *The conditional secrecy outage probability in LOS regime is given as*

$$\mathcal{P}_s^{\mathrm{mm}}(T_\mathrm{e}) = 1-\exp\left(-2\pi\lambda_\mathrm{e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\left[\frac{P_m G_\mathrm{e}}{iAT_\mathrm{e}\sigma_m^2}\right.\right. \quad (28)$$
$$\left.\left. -\frac{\sqrt{\pi}P_m^{3/2}e^{\frac{\beta^2 P_m G_\mathrm{e}}{4iAT_\mathrm{e}\sigma_m^2}}}{4(iAT_\mathrm{e}\sigma_m^2)^{3/2}}\mathrm{erfc}\left(\frac{\beta\sqrt{P_m G_\mathrm{e}}}{2\sqrt{iAT_\mathrm{e}\sigma_m^2}}\right)\right]\right).$$

Proof. Considering $\alpha = 2$, the integral expression $\mathcal{M}$ in (12) under LOS scenario follows from proposition 4 as

$$\mathcal{M} = 2\pi\lambda_\mathrm{e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\int_0^\infty r_\mathrm{e}e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^2}{P_m G_\mathrm{e}}}e^{-\beta r_\mathrm{e}}\mathrm{d}r_\mathrm{e}. \quad (29)$$

Now, substituting the closed form expression of (29) in (12), the desired proof is obtained. □

***Corollary* 3.** *The lower bound of conditional secrecy outage probability in LOS regime is given in* (30) *on top of the following page.*

Proof. Considering $\alpha = 2$, the conditional secrecy outage probability (14) under LOS scenario can be given as

$$\mathcal{P}_s^{mm_{\mathrm{LB}}}(T_\mathrm{e}) = \int_0^\infty \Pr\{\zeta_\mathrm{e}(r) > T_\mathrm{e}\} f_{r_e}(r_\mathrm{e})e^{-\beta r_\mathrm{e}}\mathrm{d}r_\mathrm{e}, \quad (31)$$
$$= \int_0^\infty \Pr\left\{\frac{P_m G_\mathrm{e} h_{m_\mathrm{e}} r_\mathrm{e}^{-\alpha}}{\sigma_m^2} > T_\mathrm{e}\right\} f_{r_e}(r_\mathrm{e})e^{-\beta r_\mathrm{e}}\mathrm{d}r_\mathrm{e},$$
$$\overset{(a)}{=} \sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\int_0^\infty e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^2}{P_m G_\mathrm{e}}} f_{r_e}(r_\mathrm{e})e^{-\beta r_\mathrm{e}}\mathrm{d}r_\mathrm{e},$$
$$\overset{(b)}{=} 2\pi\lambda_\mathrm{e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\int_0^\infty r_\mathrm{e}e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^2}{P_m G_\mathrm{e}}}e^{-\pi r_\mathrm{e}^2}e^{-\beta r_\mathrm{e}}\mathrm{d}r_\mathrm{e},$$

where (a) and (b) follow the same analyses as in proposition 2. Now, substituting the closed form expression of (31) in (12), we obtain the desired proof. □

At this point, it is worthwhile to mention some insights on interference modeling in mmWave networks. As mentioned earlier in beginning of this section, it is widely accepted that interference may not play a significant role in urban mmWave systems. However, Ad-hoc networks and indoor mmWave systems may still be susceptible to some amount of interference as depicted in [21]. In order to not to deviate from the analysis, we now characterize conditional secrecy outage probability by taking interference into account.

Thus, the conditional secrecy outage probability of a typical mmWave link can be given as

$$\mathcal{P}_s^{\mathrm{mm}}(T_\mathrm{e}) = 1-\exp\left(-2\pi\lambda_\mathrm{e}\sum_{j\in L,N}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\right. \quad (32)$$
$$\left.\times\int_0^\infty r_\mathrm{e}e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^{\alpha_j}}{P_m G_\mathrm{e}}}\mathbb{E}_{I_m}\left[e^{-\frac{iAT_\mathrm{e}r_\mathrm{e}^{\alpha_j}}{P_m G_i}I_m}\right]p_j(r_\mathrm{e})\mathrm{d}r_\mathrm{e}\right),$$

where $\mathbb{E}_{I_m}[.]$ is the Laplace representation of interference from all other mmWave BSs. The detailed characterization of the above integral is given in Appendix D.

Since we model the links between the BSs and the typical UE as LOS and NLOS which are independent of each other, we leverage the notion of mark from stochastic geometry to further split the Poisson point processes into two independent LOS and NLOS sub processes. Therefore, the interference I_m can be expressed as

$$I_m = I_m^{\Phi_\mathrm{L}} + I_m^{\Phi_\mathrm{N}}. \quad (33)$$

Hence, the conditional secrecy outage probability of a typical mmWave link can now be given as

$$\mathcal{P}_s^{\mathrm{mm}}(T_\mathrm{e}) = 1-\exp\left(-2\pi\lambda_\mathrm{e}\sum_{j\in L,N}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\right. \quad (34)$$
$$\left.\times\int_0^\infty r_\mathrm{e}e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^{\alpha_j}}{P_m G_\mathrm{e}}}\prod_j\mathbb{E}_{I_m}\left[e^{-\frac{iAT_\mathrm{e}r_\mathrm{e}^{\alpha_j}}{P_m G_i}I_m^j}\right]p_j(r_\mathrm{e})\mathrm{d}r_\mathrm{e}\right).$$

B. Fixed LOS model

Leveraging the modeling of blockage in [8], we consider a simple LOS model for each and every link[7]. At this point, we would like to note that the adoption offixed LOS probability model in our analysis enables faster calculations of the connection and secrecy outage probability, as it simplifies expressions for the evaluation of the numerical integrals. It has been shown via simulations in [22], [30] that the error due to such an approximation (LOS step model) is generally small in dense mmWave networks, which also motivates the use of this first-order approximation of the LOS probability function. This significantly simplifies the dense network analysis. As shown in [22], the step function approximation generally provides a lower bound of the actual SINR distribution, and errors due to the approximation become smaller when the base station density increases.

Proposition 6. *The conditional connection outage probability of a typical mmWave link for random blockage model is given as*

$$\mathcal{P}_{\mathrm{co}}^{\mathrm{mm}}(T_l) = \exp\left(-\sum_{j\in\mathrm{L,N}}\frac{2\pi\lambda_m}{\alpha_j}\left(\frac{P_m G_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}}(AT_l)^{\frac{-2}{\alpha_j}}\right. \quad (35)$$
$$\left.\times\sum_{i=0}^{m}\binom{m}{i}(-1)^{i+1}i^{\frac{-2}{\alpha_j}}\Gamma\left(\tfrac{2}{\alpha_j},\tfrac{iAt}{r_d}\right)\right).$$

[7]Here, we elucidate the conditional secrecy outage probability only. The conditional connection outage probability follows easily from the previous subsection with fixed p_L.

$$\mathcal{P}_s^{\mathrm{mm}}(T_\mathrm{e}) = 2^{-1}\left(\frac{iAT_\mathrm{e}\sigma_m^2}{P_m G_\mathrm{e}}+\pi\right)^{-1/2} - \beta\, e^{\frac{\beta^2}{4\left(\frac{iAT_\mathrm{e}\sigma_m^2}{P_m G_\mathrm{e}}+\pi\right)}}\sqrt{\pi}\mathrm{erfc}\left(\beta 2^{-1}\left(\frac{iAT_\mathrm{e}\sigma_m^2}{P_m G_\mathrm{e}}+\pi\right)^{-1/2}\right) 4\left(\frac{iAT_\mathrm{e}\sigma_m^2}{P_m G_\mathrm{e}}+\pi\right)^{-3/2}. \quad (30)$$

Proof. The proof follows from Proposition 3. □

Proposition 7. *The conditional secrecy outage probability of a typical mmWave link for fixed LOS Model is given as*

$$\mathcal{P}_s^{\mathrm{mm}}(T_\mathrm{e}) = 1 - \exp\left(-\sum_{j\in \mathrm{L,N}} p_j \frac{2\pi\lambda_\mathrm{e} r_d^2}{\alpha_j}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1} \times \mathrm{E}_{\frac{\alpha-2}{\alpha}}\left(\frac{\mathrm{iAT_e}\sigma_\mathrm{m}^2 \mathrm{r_d^{\alpha_j}}}{\mathrm{P_m G_e}}\right)\right), \quad (36)$$

where $\mathrm{E_a(b)}$ *denotes the exponential integral.*

Proof. The proof follows from Proposition 4. □

LOS analysis: Similar to the previous analysis on LOS using the random blockage model, here we characterize the conditional secrecy outage probability for fixed blockage model.

***Corollary* 4.** *The conditional secrecy outage probability using the fixed blockage model can be given as*

$$\mathcal{P}_s^{\mathrm{mm}}(T_\mathrm{e}) = 1 - \exp\left(-p_\mathrm{L}\pi\lambda_\mathrm{e}\frac{P_m G_\mathrm{e}}{T_\mathrm{e}\sigma_m^2}\sum_{i=1}^{m}\binom{m}{i}\frac{(-1)^{i+1}}{i} \times\left(1-\exp\left(-\frac{i.AT_\mathrm{e}\sigma_m^2 r_d^2}{P_m G_\mathrm{e}}\right)\right)\right). \quad (37)$$

Proof. Consider $\alpha = 2$, then the integral expression $\mathcal{M}$ in (12) under LOS scenario is given as

$$\mathcal{M} = 2\pi\lambda_\mathrm{e}\sum_{i=1}^{m} p_\mathrm{L}\binom{m}{i}(-1)^{i+1}\int_0^\infty r_\mathrm{e} e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^2}{P_m G_\mathrm{e}}}\mathrm{d}r_\mathrm{e}. \quad (38)$$

Therefore, by substituting the closed form expression of (38) in (12), this proof concludes. □

***Corollary* 5.** *The lower bound of conditional secrecy outage probability in LOS regime is given as*

$$\mathcal{P}_s^{\mathrm{mm_{LB}}}(T_\mathrm{e}) = \frac{P_m G_\mathrm{e}}{2\left(iAT_\mathrm{e}\sigma_m^2 + \pi P_m G_\mathrm{e}\right)}. \quad (39)$$

Proof. Considering $\alpha = 2$, the conditional secrecy outage probability equation (14) under LOS scenario can be written as

$$\mathcal{P}_s^{\mathrm{mm_{LB}}}(T_\mathrm{e}) = \int_0^\infty \Pr\{\zeta_\mathrm{e}(r) > T_\mathrm{e}\} f_{r_e}(r_\mathrm{e}) dr_\mathrm{e}, \quad (40)$$
$$\overset{(b)}{=} 2\pi\lambda_\mathrm{e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\int_0^\infty r_\mathrm{e} e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^2}{P_m G_\mathrm{e}}} e^{-\pi r_\mathrm{e}^2}\mathrm{d}r_\mathrm{e}.$$

Similar to the previous proofs, this proof concludes by substituting the closed form expression of (40) in (14). □

Now, by taking interference into account, the conditional secrecy outage probability of a typical mmWave link can now be given as

$$\mathcal{P}_s^{\mathrm{mm}}(T_\mathrm{e}) = 1 - \exp\left(-2\pi\lambda_\mathrm{e}\sum_{j\in L,N} p_j \sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1} \times\int_0^\infty r_\mathrm{e} e^{-\frac{iAT_\mathrm{e}\sigma_m^2 r_\mathrm{e}^{\alpha_j}}{P_m G_\mathrm{e}}}\mathbb{E}_{I_m}\left[e^{-\frac{iAT_\mathrm{e} r_\mathrm{e}^{\alpha_j}}{P_m G_i} I}\right]\mathrm{d}r_\mathrm{e}\right), \quad (41)$$

where $\mathbb{E}_{I_m}[.]$ is the interference from all other mmWave BSs. The characterization of $\mathbb{E}_{I_m}[.]$ follows from the previous subsection.

VI. Numerical Results

In this section, we validate the system model and also verify the results derived in the propositions. In general, the computations are done through Monte Carlo simulations which are then used to validate the analytical expressions. Unless stated otherwise, most of the values of the parameters used are inspired from literature mentioned in the references. For the system guidelines, we mention these parameters and their corresponding values in Table II.

With the expressions already derived, we can now study the availability of secrecy in random mmWave overlaid μWave networks in the presence of randomly distributed eavesdroppers. In particular, we analyze the effect of change of parameters such as G_e, α, λ_e and T_e on conditional secrecy outage probability in Figures 3, 4, 5 and 6. The latter part of numerical section and figures are devoted to explaining the importance of blockage modeling from secrecy perspective.

A network of cell radius of 200m is considered. The transmit power is set at 30dBm for mmWave and 43dBm for μWave BS with thermal noise density of -174dBm/Hz. We begin by plotting the association probability, p_μ of μWave network with respect to mmWave network in Fig. 2. It can be seen from the figure that the association probability of μWave network increases with the density of μ BSs, which is quite obvious. It can also be seen that increasing the path loss exponent reduces p_μ. However, one interesting observation from the figure is that, the blockage parameter, β has a significant impact on the association probability when the μWave network experiences higher path loss. Accordingly, the typical UE associates itself to the mmWave network when it experiences more path loss in the μWave network. This result confirms that, the typical UE is always associated with the best BS (either mmWave or μWave), providing the strongest signal.

TABLE II: Simulation Parameters

Notation	Parameter	Values
m	Nakagami-m figure	10
λ_{e}	Density	0.00001
R_s	Target rate	0.1
α	Path loss exponent	2, 3.5, 4
G_{e}	Antenna gain	2, 3, 5, 10dB
N_t	Antenna number at μWave BSs	10

Since, now we have established the association probabilities of the typical UE for the mmWave and μWave networks, hereinafter, we analyze the conditional secrecy and connection outage probability in the following figures. Fig. 3 shows the conditional secrecy outage probability as a function of λ_{e} for both the μWave and mmWave link which follows from (24) and (41). It is evident from Fig. 3a that interference is beneficial for secrecy capacity in μWave systems from the perspective of increasing uncertainty at the eavesdropper. This is due to the fact that as the density of BS λ_μ increases, the conditional secrecy outage probability decreases. However, in mmWave systems, due to the blockages, interference doesn't play major role, which is clearly evident from Fig. 3b. It can also be seen that the increase in directional antenna gain at the eavesdropper increases the secrecy outage probability.

In Fig. 4, we plot the conditional secrecy outage probability as a function of T_{e} considering the random blockage model for different values of eavesdroppers antenna gains and path loss exponents. Fig. 4a shows that the conditional secrecy outage probability decreases with the increase in T_{e}. It is evident from this figure that highly directional beamforming may not always be useful from a secrecy perspective as the eavesdroppers too will have high gains and can force the communication into secrecy outage. Therefore, there is a trade-off between the achievable outage capacity and secrecy outage capacity.

Similar to Fig. 4a, Fig. 4b is plotted as a function of T_{e} for different values of α_{N}. From this figure, it can be seen that conditional secrecy outage probability decreases with the increase in α. It is more likely to have higher path loss exponent in mmWave systems than μWave systems. Hence, it is intuitively acceptable that higher values of path loss exponents degrade the communication more. Consequently, the eavesdropper receives less information from the BS.

As mentioned earlier, any perfect transmission takes place if and only if the transmitted messages satisfy both the minimum connection outage and secrecy outage constraints. Fig. 5 shows the connection outage probability as a function of mmWave BS density. The connection outage probability decreases as the mmWave BS density increases. From this figure, It is worthwhile to mention that the increase in p_{L} provides better communication from the BS to the typical UE. Henceforth, to characterize any perfect transmission scheme, we opt for a higher LOS probability and a decent mmWave BS density.

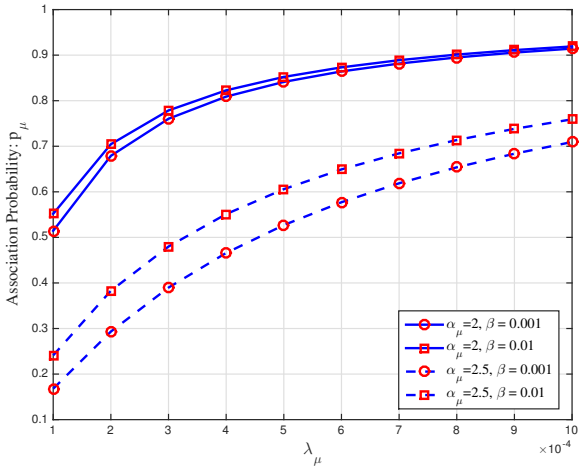
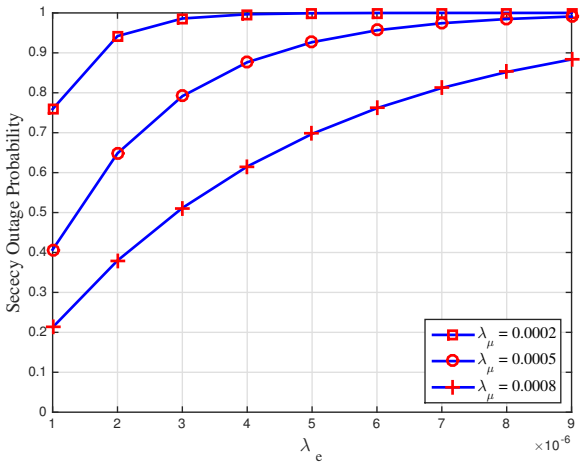
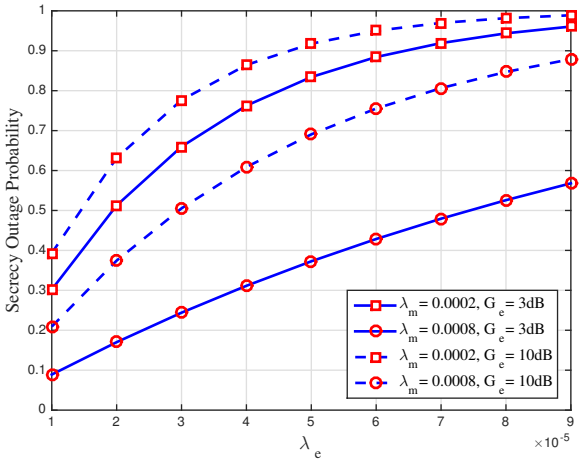


Fig. 2: Association probability of μWave network with respect to mmWave network. Here, $P_m = 30$dBm, $P_\mu = 43$dBm, $\lambda_m = 0.0001$, $\alpha_L = 2$, $\alpha_N = 4$.

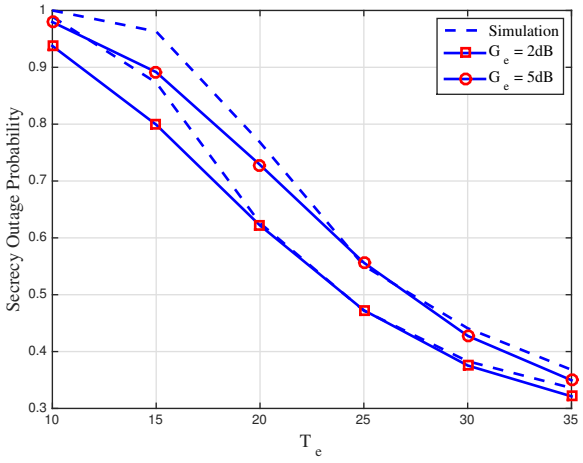


(a) As a function of λ_{e} for different λ_l under μWave link.

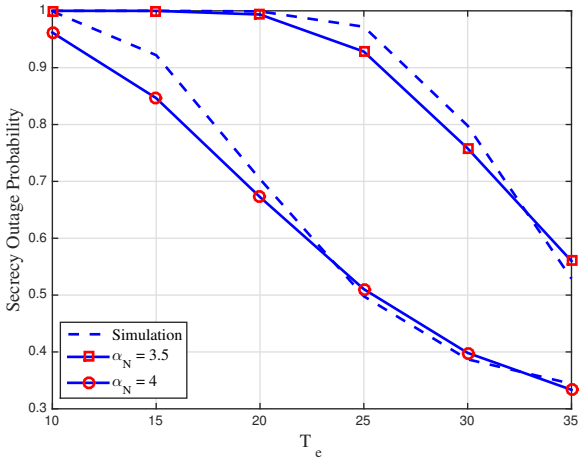


(b) As a function of λ_{e} for different λ_l under mmWave link.

Fig. 3: conditional secrecy outage probability as a function of λ_{e}. Parameters - mmWave: m=10, T_{e}=15dB, μWave: m=10, T_{e}=1dB.



(a) As a function of T_{e} for different G_{e}.



(b) As a function of T_{e} for different α_{N}.

Fig. 4: Conditional secrecy outage probability as a function of T_{e} considering generalized blockage model.

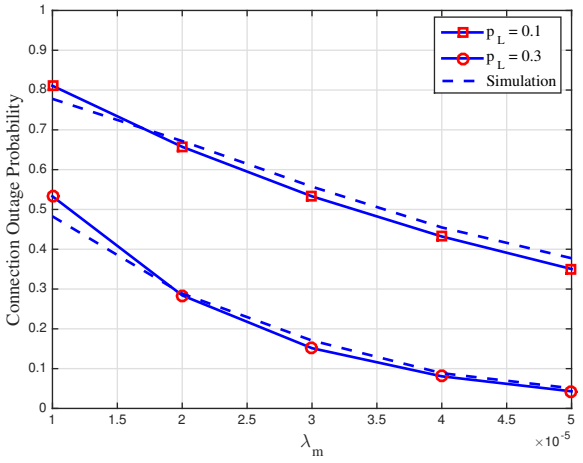


Fig. 5: Connection outage probability as a function of λ_m.

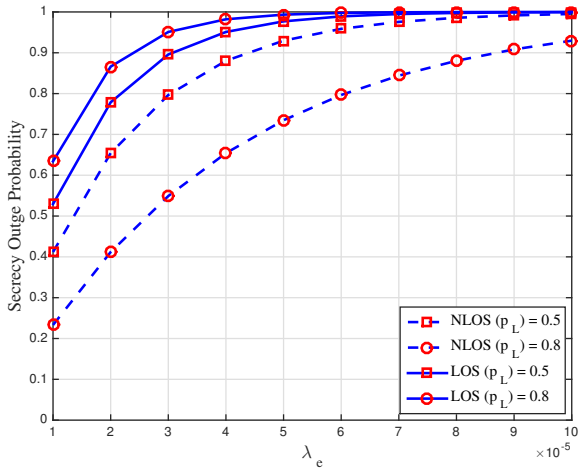


Fig. 6: Comparison of conditional secrecy outage probability for LOS and NLOS scenarios.

Fig. 6 shows the comparison between LOS and NLOS scenarios under the fixed blockage model. It can be observed from the figure that the conditional secrecy outage probability decreases as we move from LOS scenario to NLOS scenario. Hence, it is evident that the NLOS scenario helps the communication to transmit the message securely. This is due to the fact that the blockage density is higher in NLOS scenario, which provides higher signal loss at the eavesdropper.

Fig. 7 shows the conditional secrecy outage probability as a function of λ_{e} for mmWave link considering the two blockage models described under various blockage probabilities. This analysis follows from (28) and (37). It is clearly evident from the figure that the outage probability decreases with the increase in blockage density. It can also be seen from the figure that the performance gap between the two models used is minimal. While from a practical standpoint, the random blockage model may intuitively sound more functional, the fixed LOS model can be categorically stated to be more useful in obtaining analytical closed form expressions.

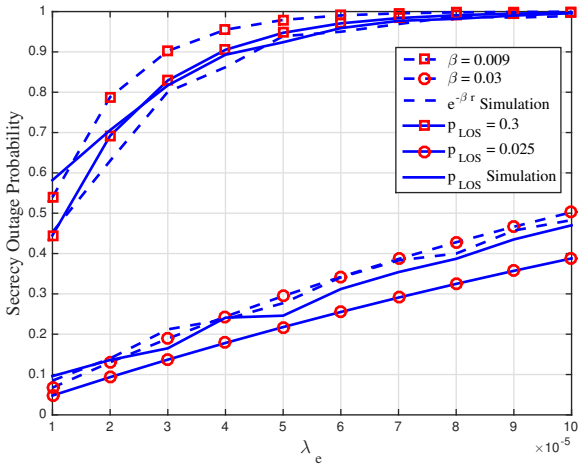


Fig. 7: Conditional secrecy outage probability as a function of λ_{e} under mmWave link with m=10, G_{e}=10dB, T_{e}=10dB, r_d=200m.

At this point, it is worthwhile to mention the fact that higher path loss exponents, NLOS scenarios and dense blockage environments can aid secrecy capacity in mmWave overlaid μWave networks. In order to design a secure system in a hybrid network, one should calculate the total secrecy outage probability from (13) with respect to association and conditional secrecy outage probabilities of mmWave and μWave networks.

VII. Conclusion

The secrecy outage of mmWave overlaid μWave networks under the impact of blockages was analyzed. A tradeoff between outage capacity and secrecy outage capacity with respect to blockages was seen. This can be expertly exploited by network engineers to maintain a balance between higher data rates and security. Furthermore, in mmWave systems high antenna gains are usually preferred. However, this may not always be useful from a secrecy perspective as the eavesdroppers too will have high gains and can force the communication into secrecy outage. Moreover, higher path loss exponents, NLOS scenarios and dense blockage environments were found to aid secrecy capacity in such network models.

Our results are useful in quantifying the performance of blockages on the conditional secrecy outage probability of mmWave networks. Specifically, we would like to state that the work presented in this paper gives the required initial analyses, while reiterating some very important results, that can be considered as a cornerstone for future works in enhancing hybrid network security. We have also shown that co-existence of mmWave and μWave networks from a secrecy perspective is possible when the total secrecy outage probability with respect to association and conditional secrecy outage probabilities of mmWave and μWave networks is available.

Appendix A
Proof of Proposition 1

Let p_μ be the association probability of a typical user connected to a μWave network, *i.e.*, the probability that all mmWave BSs have maximum path loss when the user is connected to the nearest μWave BS. If r_μ is the nearest μWave BS node, then p_μ can be represented as

$$\begin{aligned} p_\mu &= \mathbb{E}_{r_\mu}\left[\Pr\left[P_\mu B_\mu r_\mu^{-\alpha_\mu} > P_m G_l B_m r_m^{-\alpha_m}\right]\right], \\ &= \int_0^\infty \Pr\left(\tfrac{r_m^{\alpha_m}}{P_m G_l B_m} > \tfrac{r_\mu^{\alpha_\mu}}{P_\mu B_\mu}\right) f_{r_\mu}(r)\mathrm{d}r, \end{aligned} \tag{42}$$

where $\Pr\left(\frac{r_m^{\alpha_m}}{P_m G_l B_m} > \frac{r_\mu^{\alpha_\mu}}{P_\mu B_\mu}\right)$ can be obtained by taking complementary cumulative distribution function of equation (16) in Lemma 1 and $f_{r_\mu}(r)$ is obtained similar to equation (15).

Appendix B
Proof of Proposition 2

Let $\phi_\mu = \left\{x_l \triangleq \frac{P_\mu}{\sigma_\mu^2} r_l^{-\alpha_\mu}\right\}$ be a path gain process. By using Mapping theorem [28, Theorem 2.34], the density function of this point process can be given as

$$\lambda(x) = \frac{2\pi\lambda_\mu}{\alpha}\left(\tfrac{P_\mu}{\sigma_\mu^2}\right)^{\frac{2}{\alpha}} x^{\frac{-2}{\alpha}-1}. \tag{43}$$

Since our propagation process ϕ_μ is also affected by fading H_μ, *i.e* $\phi_\mu = \{y_i \triangleq h_i x_i\}$, the density of this marked point process using the displacement theorem [28] can be given as

$$\hat{\lambda}(y) = \int_0^\infty \lambda(x)\rho(x,y)\,\mathrm{d}x, \tag{44}$$

where

$$\rho(x,y) = \frac{\mathrm{d}}{\mathrm{dy}}(1 - F_{H_\mu}(y/x)) = -\tfrac{y}{x^2} f_{H_\mu}(y/x). \tag{45}$$

where $H_\mu = |\mathbf{h}_{1,i}\mathbf{v}_1|^2$ is chi-squared with $2N_t$ degrees of freedom. For more insights on this fading distribution, interested readers can refer to [29, Lemma 2].

Therefore (44) can now be given as

$$\begin{aligned} \hat{\lambda}(y) &= \frac{1}{\alpha}\int_0^\infty 2\pi\lambda_\mu\left(\tfrac{P_\mu}{\sigma_\mu^2}\right)^{\frac{2}{\alpha}} x^{\frac{-2}{\alpha}-1}\rho(x,y)\,\mathrm{d}x \\ &= \frac{1}{\alpha}\int_0^\infty 2\pi\lambda_\mu\left(\tfrac{P_\mu}{\sigma_\mu^2}\right)^{\frac{2}{\alpha}} x^{\frac{-2}{\alpha}-1} f_{H_\mu}(y/x)\tfrac{1}{x}\,\mathrm{d}x \\ &\overset{(z=\frac{y}{x})}{=} \frac{1}{\alpha}2\pi\lambda_\mu\left(\tfrac{P_\mu}{\sigma_\mu^2}\right)^{\frac{2}{\alpha}} y^{\frac{-2}{\alpha}-1}\int_0^\infty z^{\frac{2}{\alpha}} f_{H_\mu}(z)\,\mathrm{d}z \\ &= \frac{1}{\alpha}2\pi\lambda_\mu\left(\tfrac{P_\mu}{\sigma_\mu^2}\right)^{\frac{2}{\alpha}} y^{\frac{-2}{\alpha}-1}\mathbb{E}_{H_\mu}\left(h_{\mu_l}^{\frac{2}{\alpha}}\right). \end{aligned} \tag{46}$$

Using the void probability of a PPP and from the definition of connection outage probability according to (9), the connection outage probability in (T_l, ∞) can thus be given as

$$\begin{aligned} \mathcal{P}_{\mathrm{co}}(T_l) &= \exp\left(-\int_{T_l}^\infty \hat{\lambda}(y)\mathrm{dy}\right) \\ &= \exp\left(-\frac{2\pi\lambda_\mu}{\alpha}\left(\tfrac{P_\mu}{\sigma_\mu^2}\right)^{\frac{2}{\alpha}}\mathbb{E}_{H_\mu}\left(h_{\mu_l}^{\frac{2}{\alpha}}\right)\int_{T_l}^\infty y^{\frac{-2}{\alpha}-1}\mathrm{dy}\right). \end{aligned} \tag{47}$$

The proof concludes by evaluating the above integral in equation (47).

Appendix C
Proof of Proposition 4

Let $\phi_m = \left\{x_l = \frac{P_m G_l}{\sigma_m^2} r_l^{-\alpha_j}\right\}$ be a path gain process, where $j \in \{\mathrm{L},\ \mathrm{N}\}$. Similar to the proof of Proposition 1, by using Mapping theorem [28], the density function under the effect of blockages can be given as

$$\lambda(x) = \sum_{j\in\mathrm{L,N}} \frac{2\pi\lambda_m}{\alpha_j}\left(\tfrac{P_m G_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}} p_j(x) x^{\frac{-2}{\alpha_j}-1}. \tag{48}$$

We can obtain the density of marked point process as below. Now (48) becomes

$$\hat{\lambda}(y) = \sum_{j\in\mathrm{L,N}} \frac{2\pi\lambda_m}{\alpha_j}\int_0^\infty \left(\tfrac{P_m G_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}} p_j(x) x^{\frac{-2}{\alpha_j}-1}\rho(x,y)\,\mathrm{d}x, \tag{49}$$

$$\overset{(z=\frac{y}{x})}{=} \sum_{j\in\mathrm{L,N}} \frac{2\pi\lambda_m}{\alpha_j}\left(\tfrac{P_m G_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}} y^{\frac{-2}{\alpha_j}-1}\int_0^\infty p_j(\tfrac{y}{z}) z^{\frac{2}{\alpha_j}} f_{H_m}(z)\,\mathrm{d}z.$$

Using the void probability of a PPP, the path gain distribution for best relay in interval of (T_l, ∞) can thus be given as

$$\begin{aligned}\mathcal{P}_{\rm co}(T_l) &= \exp\left(-\int_{T_l}^{\infty}\hat{\lambda}(y)\mathrm{d}y\right),\\ &= \exp\left(-\sum_{j\in\mathrm{L,N}}\frac{2\pi\lambda_m}{\alpha}\left(\frac{P_mG_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}}\right.\\ &\qquad\left.\times\int_{T_l}^{\infty}y^{\frac{-2}{\alpha_j}-1}\int_0^{\infty}p_i(\tfrac{y}{z})z^{\frac{2}{\alpha_j}}f_{H_m}(z)\,\mathrm{d}z\mathrm{d}y\right).\end{aligned}\tag{50}$$

APPENDIX D
PROOF OF COROLLARY 1

Similar to the proofs of previous Propositions 2 and 4, the density function of a marked point process in AWGN case can be given as

$$\begin{aligned}\lambda(x) &= \sum_{i\in\mathrm{L,N}}\frac{2\pi\lambda_m}{\alpha}\left(\frac{P_mG_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}}p_i(x)x^{\frac{-2}{\alpha}-1},\\ &= \frac{2\pi\lambda_m}{\alpha_{\rm L}}\left(\frac{P_mG_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_L}}e^{-\beta P^{\frac{1}{\alpha_{\rm L}}}x^{-\frac{1}{\alpha_{\rm L}}}}x^{\frac{-2}{\alpha_{\rm L}}-1}\\ &\quad+\frac{2\pi\lambda_m}{\alpha_{\rm N}}\left(\frac{P_mG_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_{\rm N}}}\left(1-e^{-\beta P^{\frac{1}{\alpha_{\rm N}}}x^{-\frac{1}{\alpha_{\rm N}}}}\right)x^{\frac{-2}{\alpha_{\rm N}}-1}.\end{aligned}\tag{51}$$

Therefore, the connection outage probability can be simplified as

$$\begin{aligned}\mathcal{P}_{\rm co}(T_l) &= \exp\left(-\int_{T_l}^{\infty}\lambda(x)\mathrm{d}x\right)\\ &= \exp\left(\pi\lambda_m\left(\frac{T_l\sigma_m^2}{P_mG_l}\right)^{-\frac{1}{\alpha_{\rm N}}}-\frac{2\pi\lambda_m}{\beta^2}\sum_{j\in\mathrm{L,N}}\left(\frac{P_mG_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}}\right.\\ &\qquad\left.\left(e^{-\beta\left(\frac{T_l\sigma_m^2}{P_mG_l}\right)^{-\frac{1}{\alpha_j}}}\left(-1-\beta\left(\frac{T_l\sigma_m^2}{P_mG_l}\right)^{-\frac{1}{\alpha_j}}\right)\right)\right).\end{aligned}\tag{52}$$

APPENDIX E
CHARACTERIZATION OF SECRECY OUTAGE PROBABILITY

Let us denote the integrand in the (12) as $\mathcal{M}$.

Therefore,

$$\mathcal{M} = 2\pi\lambda_{\rm e}\sum_{j\in L,N}\int_{\mathbb{R}^2}\Pr\left\{\frac{P_mG_{\rm e}h_{m_{\rm e}}r_{\rm e}^{-\alpha}}{\sigma_m^2}>T_{\rm e}|j\right\}\mathrm{d}r,\tag{53}$$

$$\begin{aligned}&\overset{(a)}{=} 2\pi\lambda_{\rm e}\sum_{j\in L,N}\int_{\mathbb{R}^2}\left(1-\Pr\left\{h_{m_{\rm e}}<\frac{T_{\rm e}r_{\rm e}^{\alpha}\sigma_m^2}{P_mG_{\rm e}}|j\right\}\right)\mathrm{d}r,\\ &= 2\pi\lambda_{\rm e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\\ &\times\left(\int_0^{\infty}r_{\rm e}e^{-\frac{iA\sigma_m^2T_{\rm e}r_{\rm e}^{\alpha_L}}{P_mG_{\rm e}}}\mathbb{E}_{I_m}\left[e^{-\frac{iAT_{\rm e}r_{\rm e}^{\alpha_L}}{P_mG_{\rm e}}I_m}\right]e^{-\beta r_{\rm e}}\mathrm{d}r_{\rm e}\right.\\ &\left.+\int_0^{\infty}r_{\rm e}e^{-\frac{iAT_{\rm e}r_{\rm e}^{\alpha_N}}{P_mG_{\rm e}}}\mathbb{E}_{I_m}\left[e^{-\frac{iAT_{\rm e}\sigma_m^2r_{\rm e}^{\alpha_N}}{P_mG_{\rm e}}I_m}\right](1-e^{-\beta r_{\rm e}})\mathrm{d}r_{\rm e}\right),\end{aligned}$$

where (a) follows the same analyses as in Proposition 2.

REFERENCES

[1] M. R. Akdeniz, Y. Liu, M. K. Samimi, S. Shun, S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave channel modeling and cellular capacity evaluation," *IEEE J. Select. Areas Commun.*, vol. 32, no. 6, pp. 1164–1179, June 2014.

[2] A. Ghosh, T. N. Thomas, M. C. Cudak, R. Ratasuk, P. Moorut, F. W. Vook, T. S. Rappaport, G. R. MacCartney, S. Shun, and S. Nie, "Millimeter-wave enhanced local area systems: A high data-rate approach for future wireless networks," *IEEE J. Select. Areas Commun.*, vol. 32, no. 6, pp. 1153–1163, June 2014.

[3] S. Rajagopal, S. Abu-Surra, and M. Malmirchegini, "Channel feasibility for outdoor non-line-of-sight mmWave mobile communication," in *Proc. IEEE* 57th *Vehicular Technology Conference (VTC'12 Fall)*, 2012, pp. 1–6.

[4] G. R. MacCartney and T. S. Rappaport, "73GHz millimeter wave propagation measurements for outdoor urban mobile and backhaul communications in New York city," in *Proc. IEEE International Conference on Communications*, Sydney, Austrlia, June 2014, pp. 2429–2433.

[5] S. Nie, G. R. MacCartney, S. Shun, and T. S. Rappaport, "72 GHz millimeter wave indoor measurements for wireless and backhaul communications," in *Proc. IEEE* 24^{th} *International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'13)*, Sept. 2013, pp. 2429–2433.

[6] M. Akdeniz, Y. Liu, S. Rangan, and E. Erkip, "Millimeter wave picocellular system evaluation for urban deployments," in *Proc. IEEE Global Telecommunications Conference (Globecom'13)*, Dec. 2013, pp. 105–110.

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

[8] S. Singh, M. N. Kulkarni, A. Ghosh, and J. G. Andrews, "Tractable model for rate in self-backhauled millimeter wave cellular networks," *IEEE J. Select. Areas Commun.*, vol. 33, no. 10, pp. 2196 – 2211, Oct. 2015.

[9] N. Yang, L. Wang, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, pp. 20–27, Apr. 2015.

[10] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 –1367, Oct. 1975.

[11] L. Y. Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451 – 456, Jul. 1978.

[12] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339 – 348, May 1978.

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

[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515 – 2534, Jun. 2008.

[15] Y. Liang, V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470 – 2492, Jun. 2008.
[16] M. Haenggi, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5500 – 5510, Dec. 2008.
[17] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—part i: Connectivity," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 125 – 138, Feb. 2012.
[18] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Information Theory.*, vol. 58, no. 5, pp. 3000 – 3015, May. 2012.
[19] A. Rabbachin, A. Conti, and M. Z. Win, "Wireless network intrinsic secrecy," *IEEE/ACM Transactions on Networking*, vol. 23, no. 1, pp. 56–69, Feb. 2015.
[20] S. Vuppala and G. Abreu, "Unicasting on the secrecy graph," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 9, pp. 1469 – 1481, Sep. 2013.
[21] A. Thornburg, T. Bai, and R. W. Heath, "Performance analysis of mmWave ad hoc networks," *IEEE Trans. Signal Process.*, vol. xx, no. xx, Apr. 2016.
[22] 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.
[23] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
[24] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic geometry and its applications*, ser. Wiley series in probability and mathematical statistics: Applied probability and statistics. Wiley, 1987.
[25] 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.
[26] S. Singh, H.-S. Dhillon, and J. G. Andrews, "Offloading in heterogeneous networks: Modeling, analysis, and design insights," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2484–2497, May 2013.
[27] D. Maamari, N. Devroye, and D. Tuninetti, "Coverage in mmwave cellular networks with base station co-operation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2981–2994, Apr. 2016.
[28] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge University Press, 2012.
[29] N. Lee, D. Morales-Jimenez, A. Lozano, and R. W. Heath, "Spectral efficiency of dynamic coordinated beamforming: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 230–241, Jan. 2015.
[30] S. Biswas, S. Vuppala, J. Xue, and T. Ratnarajah, "On the performance of relay aided millimeter wave networks," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 576–588, 2015.

Satyanarayana Vuppala (S'12-M'16) received the B.Tech. degree with distinction in Computer Science and Engineering from JNTU Kakinada, India, in 2009, and the M.Tech. degree in Information Technology from the National Institute of Technology, Durgapur, India, in 2011. He received the Ph.D. degree in Electrical Engineering from Jacobs University Bremen in 2014. He is currently a post-doctoral researcher at IDCOM in University of Edinburgh. His main research interests are physical, access, and network layer aspects of wireless security. He also works on performance evaluation of mmWave systems. He is a recipient of MHRD, India scholarship during the period of 2009-2011.

Sudip Biswas (S'15) received the B.Tech. degree in electronics and communication engineering from the Sikkim Manipal Institute of Technology, Sikkim, India, in 2010, and the M.Sc. degree in signal processing and communications from the University of Edinburgh, Edinburgh, U.K., in 2013. He is currently pursuing the Ph.D. degree in digital communications at the University of Edinburgh's Institute for Digital Communications. His research interests include various topics in wireless communications and network information theory with particular focus on stochastic geometry and possible 5G technologies such as massive MIMO, mmWave, and full-duplex.

Tharmalingam Ratnarajah (A'96-M'05-SM'05) is currently with the Institute for Digital Communications, University of Edinburgh, Edinburgh, UK, as a Professor in Digital Communications and Signal Processing. His research interests include signal processing and information theoretic aspects of 5G wireless networks, full-duplex radio, mmWave communications, random matrices theory, interference alignment, statistical and array signal processing and quantum information theory. He has published over 300 publications in these areas and holds four U.S. patents. He is currently the coordinator of the FP7 projects ADEL (3.7M€) in the area of licensed shared access for 5G wireless networks. Previously, he was the coordinator of the FP7 project HARP (3.2M€) in the area of highly distributed MIMO and FP7 Future and Emerging Technologies projects HIATUS (2.7M€) in the area of interference alignment and CROWN (2.3M€) in the area of cognitive radio networks. Dr Ratnarajah is a Fellow of Higher Education Academy (FHEA), U.K., and an associate editor of the IEEE Transactions on Signal Processing.