ANALYSIS OF SECURE COMMUNICATION IN MILLIMETER WAVE NETWORKS: ARE BLOCKAGES BENEFICIAL?

S. Vuppala, S. Biswas, T. Ratnarajah

School of Engineering
The University of Edinburgh
Edinburgh, UK

M.Sellathurai

School of Eng. and Physical Sciences
Herriot Watt University
Edinburgh, UK

ABSTRACT

The secrecy outage of millimeter wave (mmWave) networks under the impact of blockages is derived. Specifically, using a network model that accounts for uncertainties both in node locations and blockages, we characterize the connection outage probability and the secrecy outage probability of mmWave networks with multiple eavesdroppers under basic factors such as density of eavesdropping nodes, antenna gain and blockage density. As a desirable side effect, certain factors such as blockages and reduced antenna gain can decrease the secrecy outage probability. This however is in contrast to general mmWave systems where it has been shown that reduced blockages and high antenna gains provide higher capacities.

Index Terms— Blockages, mmWave, secrecy, stochastic geometry.

1. INTRODUCTION

In future fifth generation (5G) wireless communication systems, millimeter wave (mmWave) bands with significant amounts of unused or lightly used bandwidths (20-100 GHz) appear to be a viable way to move forward to meet the ever increasing demands of enhanced data rates and increasing energy efficiency. However, mmWave bands are weak and cannot penetrate through obstacles like buildings, concrete walls, vehicles, trees, etc., which are also termed as blockages. 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 omni-directional path loss can be compensated by the proportional increase in overall antenna gain with appropriate beamforming. While recent literature [2–5] on mmWave focuses on the coverage probability and transmission capacity, physical layer security in mmWave communication has not yet been properly explored.

Physical layer security for mmWave networks: The implementation of physical layer security in any wireless communication system is a very promising domain and mmWave is no exception to that. Some factors have been listed in [6] to leverage mmWave characteristics for exploiting the physical layer security. While 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, the malicious user can use larger antenna arrays too and attain higher degrees of freedom, thus decoding 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 the subsequent sections of the paper.

Physical layer security for microwave networks: Great efforts have already been made to develop information-theoretic security in microwave (μWave) systems [7], which indicate the possibility of securing communication links without cryptography in the presence of transparent eavesdroppers. The increasing prospect of putting information theoretical secrecy concepts to actual use has motivated researchers to deepen their understanding of the inherent secrecy capabilities of wireless systems by taking into account more realistic conditions of the wireless medium. For example, the secrecy capacity of wireless fading channels was investigated in [8, 9] with expressions for the outage probability and average secrecy capacity of quasi-static fading channels derived in [10].

Stochastic geometry approaches have recently gained significant attention to develop tractable models to analyze the performance of wireless networks [11, 12]. Inspired by this approach to analyze the performance of conventional cellular systems, we design a framework for the evaluation of secrecy performance in mmWave networks from the perspective of physical layer security. 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.

2. SYSTEM MODEL

We consider the secure downlink transmission in a hybrid cellular network comprising of both mmWave and μWave networks. The mmWave base stations (BSs) are modeled as a two dimensional homogeneous point process (PPP) Φ_m with density λ_m, while the μWave BSs follows 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 receiver is assumed to be located

This work was supported by the UK EPSRC under grant number EP/L025299/1. The work of M. Sellathurai was supported by the EPSRC under grant EP/M014126/1.

at origin. A simple offloading technique is adopted wherein the typical user 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 [4] and stated to be reasonable for mmWave based networks. Furthermore, due to the small wavelengths of mmWaves, directional beamforming can be exploited for compensating the path loss and additional noise. Accordingly, directional antennas are deployed at the communication nodes such that, $G_m^{(max)}$ and $G_m^{(min)}$ are the array gains of main and side lobes respectively. For simplicity, we assume that the link between the BS and the receiver 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 [5], 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 source and the destination while NLOS occurs when the link is blocked and the destination receives the signal through reflection from a blockage. Let the LOS link be of length r, then the probabilities of occurrence $p_{\mathrm{L}}(.)$ and $p_{\mathrm{N}}(.)$ of LOS and NLOS states respectively can be given as a function of r as,

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

where β is the blockage density.

Another model that has been considered in literature is a fixed LOS probability model, as was depicted in [4]. 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 [4].

SINR modeling: By a slight abuse of notation, we consider Φ_m to be the set of interfering locations. The received signal to noise plus inteference ratio (SINR) for the typical receiver can now be defined as

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

where G_l is the antenna array gain function, h_{m_l} is the fading gain at the receiver 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 receiver.

Similarly, SINR at any eavesdropper can be given as

$$\zeta_{m_{\mathrm{e}}} \triangleq \frac{P_m G_{\mathrm{e}} |h_{m_{\mathrm{e}}}|^2 {r_{\mathrm{e}}}^{-\alpha_m}}{\sigma_m^2 + \sum\limits_{i \in \Phi_m} P_m G_i |h_{m_i}|^2 r_i^{-\alpha_i}}. \tag{3}$$

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, we consider Nakagami-m fading model.

The μWave channels are modeled similarly to its mmWave counterparts with the only exception that the antennas are now omni-directional with transmitted signal power P_μ and path loss exponent α_μ. It is to be noted that the blockage effects are neglected for μWave systems. Accordingly, the received SINR for the typical receiver and any eavesdropper can now be given respectively as

$$\zeta_{\mu_l} \triangleq \frac{P_\mu |h_{\mu_l}|^2 {r_l}^{-\alpha_\mu}}{\sigma_\mu^2 + \sum\limits_{i \in \Phi_\mu} P_\mu |h_{\mu_i}|^2 r_i^{-\alpha_i}}, \tag{4}$$

$$\zeta_{\mu_{\mathrm{e}}} \triangleq \frac{P_\mu |h_{\mu_{\mathrm{e}}}|^2 {r_{\mathrm{e}}}^{-\alpha_\mu}}{\sigma_\mu^2 + \sum\limits_{i \in \Phi_\mu} P_\mu |h_{\mu_i}|^2 r_i^{-\alpha_i}}. \tag{5}$$

In our system model, the communication links in both the μwave and mmWave are assumed to be eavesdropped. 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 $\zeta_{\mathrm{e}} < T_{\mathrm{e}}$[1]. However, due to the wireless medium of communication, its appropriate to characterize their corresponding non-outage probabilities with the perfect transmission scheme. 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 receiver 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 receiver associates itself with its strongest BS node. Thus, the connection outage probability can occur when the user is connected to the strongest BS and if the received SINR falls below T_ℓ. It can be mathematically represented as

$$\mathcal{P}_{\mathrm{co}}(T_\ell) = \Pr\left[\max_{x \in \Phi_{m_l/\mu_l}} \zeta(x) < T_\ell\right]. \tag{6}$$

Secrecy outage probability: If the capacity of the channel from the BS to any eavesdroppers is above the rate τ_e, *i.e.*, $\log_2(1+\zeta_{\mathrm{e}}) > \tau_e$, the security of the message is compromised. In other words, the confidential message may not be perfectly secure against the eavesdropper in $\mathbb{R}^d$. The probability of this event is known as secrecy outage probability [13], which is denoted by $\mathcal{P}_s$.

Assume a set of eavesdroppers that can cause secrecy outage as $R_e = \{i \in \Phi_e : \zeta_i > T_{\mathrm{e}}\}$, where $T_{\mathrm{e}} \triangleq 2^{\tau_e} - 1$ is the threshold SINR. Hence, we can define the indicator function, $\mathbf{1}_A(e)$, which equals to 1 when the eavesdropper e is in the set R_e. The secrecy outage probability can thus be described as the probability that at least one of the eavesdroppers in R_e causes a secrecy outage, which can be written as [13],

$$\mathcal{P}_s(T_{\mathrm{e}}) = 1 - \mathbb{E}_{\Phi_{m_l/\mu_l}}\left[\mathbb{E}_{\Phi_{\mathrm{e}}}\left[\mathbb{E}_X\Big[\prod_{\mathrm{e} \in R_{\mathrm{e}}} \big(1 - 1_A(\mathrm{e})\big)\Big]\right]\right], \tag{7}$$

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

[1]The subscripts μ_e and m_e are replaced with e hereinafter as the eavesdropper can operate in both mmWave or μWave frequencies.

This follows from the independence of fading at each eavesdropper so that the expectation on X 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 (8) which can be obtained by using the generating functional of a PPP [13, 14] as

$$\mathcal{P}_s(T_\mathrm{e}) = 1\text{–}\mathbb{E}_{\Phi_{m_l/\mu_l}}\left[\exp\left[-\lambda_\mathrm{e}\int_{\mathbb{R}^d}\Pr\big(\zeta_\mathrm{e} > T_\mathrm{e}\big|_{\Phi_{m_l/\mu_l}}\big)de\right]\right]. \tag{8}$$

3. PERFECT TRANSMISSION ANALYSIS

In this section, we derive the connection outage probability and the secrecy outage probability of μWave and mmWave cellular links. Furthermore, it has been mentioned in [2–4] that mmWave networks in urban settings tend to be noise limited. This 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. In our analysis we consider both the noise limited and interference case into account so that it is comparable to recent mmWave literature.

3.1. μWave link

Let us consider the noise limited case where noise power dominates the interference power. Using (6), the connection outage probability of any microwave link by neglecting interference is given in Proposition 1.

Proposition 1. *The connection outage probability of a typical μWave link in mmWave overlaid cellular networks is given as*

$$\mathcal{P}_\mathrm{co}(T_\ell) = \exp\left(-\pi\lambda_\mu P_\mu^{\frac{2}{\alpha}} T_\ell^{\frac{-2}{\alpha}}\,\mathbb{E}_H\left(h_{\mu_l}^{\frac{2}{\alpha}}\right)\right). \tag{9}$$

Proof. Due to space limitations, the proof is omitted here. □

Similarly, the secrecy outage probability is given in Proposition 2 according to (8). It is to be noted that this result is vital for the corresponding analyses in the paper and hence we give the detailed proof for this proposition.

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

$$\mathcal{P}_s(T_\mathrm{e}) = 1-\exp\left(-\frac{2\pi\lambda_\mathrm{e}\Gamma(\frac{2}{\alpha_\mu})}{\alpha}\left(\frac{AT_\mathrm{e}\sigma_\mu^2}{P_\mu}\right)^{\frac{-2}{\alpha_\mu}}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}i^{\frac{-2}{\alpha_\mu}}\right). \tag{10}$$

Proof. Denoting the integral expression in (8) as $\mathcal{M}$, we have

$$\mathcal{M} \overset{(a)}{=} \sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\int_0^\infty r_\mathrm{e} e^{-\frac{iAT_\mathrm{e}r_\mathrm{e}^{\alpha_\mu}}{P_\mu}}\,\mathrm{d}r_\mathrm{e}, \tag{11}$$

$$= \frac{\Gamma(\frac{2}{\alpha_\mu})}{\alpha_\mu}\left(\frac{AT_\mathrm{e}\sigma_\mu^2}{P_\mu}\right)^{\frac{-2}{\alpha_\mu}}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}i^{\frac{-2}{\alpha_\mu}},$$

where we use the tight upper bound of gamma random variable of parameter m as

$$\Pr\{h<\gamma\} < (1-e^{-A\gamma})^m, \tag{12}$$

with $A = \frac{m}{(m!)^{-1/m}}$. This proof concludes by substituting the closed form expression of $\mathcal{M}$ in (8). □

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

$$\mathcal{P}_s(T_\mathrm{e}) = 1-\exp\left(-2\pi\lambda_\mathrm{e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\times\int_0^\infty r_\mathrm{e}e^{-\frac{iAT_\mathrm{e}r_\mathrm{e}^{\alpha_\mu}}{P_\mu}}\mathbb{E}_{I_\mu}\left[e^{-\frac{iAT_\mathrm{e}r_\mathrm{e}^{\alpha_\mu}}{P_\mu}I}\right]\mathrm{d}r_\mathrm{e}\right), \tag{13}$$

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

3.2. mmWave link - Random blockage model

Here, we leverage the modeling of blockage from [5] where blockages are modeled randomly with LOS probability of $e^{-\beta r}$. In conjunction to the previous sub-section, we characterize the secrecy outage probability without considering interference in first part, and interference in the second.

Proposition 3. *The connection outage probability of a typical mmWave link for random blockage model is given as*

$$\mathcal{P}_\mathrm{co}(T_\ell) = \exp\left(-\sum_{j\in\mathrm{L,N}}\frac{2\pi\lambda_m}{\alpha_j}\left(\frac{P_mG_l}{\sigma_m^2}\right)^{\frac{2}{\alpha_j}}\times\int_{T_\ell}^\infty y^{\frac{-2}{\alpha_j}-1}\int_0^\infty p_j(\tfrac{y}{z})z^{\frac{2}{\alpha_j}}f_{h_{m_\mathrm{e}}}(z)\,\mathrm{d}z\mathrm{d}y\right). \tag{14}$$

Proof. The proof follows from Proposition 1. □

Proposition 4. *The secrecy outage probability of a typical mmWave for random blockage model link can be given as*

$$\mathcal{P}_s(T_\mathrm{e}) = 1-\exp\left(-2\pi\lambda_\mathrm{e}\sum_{j\in\mathrm{L,N}}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\times\int_0^\infty r_\mathrm{e}e^{-\frac{iAT_\mathrm{e}\sigma_m^2r_\mathrm{e}^{\alpha_j}}{P_mG_\mathrm{e}}}p_j(r_\mathrm{e})\mathrm{d}r_\mathrm{e}\right). \tag{15}$$

Proof. The proof follows from the Proposition 2. □

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.

Consider $\alpha = 2$, then the integral expression $\mathcal{M}$ in (8) under LOS scenario is given as

$$\mathcal{M} = 2\pi\lambda_\mathrm{e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\int_0^\infty r_\mathrm{e}e^{-\frac{iAT_\mathrm{e}\sigma_m^2r_\mathrm{e}^2}{P_mG_\mathrm{e}}}e^{-\beta r_\mathrm{e}}\mathrm{d}r_\mathrm{e}. \tag{16}$$

Therefore, by substituting the closed form expression of (16) in (8), the secrecy outage probability in LOS regime without considering interference is given as

$$\mathcal{P}_s(T_\mathrm{e}) = 1-\exp\left(-2\pi\lambda_\mathrm{e}\sum_{i=1}^{m}\binom{m}{i}(-1)^{i+1}\left[\frac{P_mG_\mathrm{e}}{iAT_\mathrm{e}\sigma_m^2}-\frac{\sqrt{\pi}P_m^{3/2}e^{\frac{\beta^2P_mG_\mathrm{e}}{4iAT_\mathrm{e}\sigma_m^2}}}{4(iAT_\mathrm{e}\sigma_m^2)^{3/2}}\mathrm{erfc}\left(\frac{\beta\sqrt{P_mG_\mathrm{e}}}{2\sqrt{iAT_\mathrm{e}\sigma_m^2}}\right)\right]\right). \tag{17}$$

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

$$\mathcal{P}_s(T_{\rm e}) = 1 - \exp\left(-2\pi\lambda_{\rm e} \sum_{j\in L,N} \sum_{i=1}^{m} \binom{m}{i} (-1)^{i+1} \right. \quad (18)$$
$$\left. \times \int_0^{\infty} r_{\rm e} e^{-\frac{iAT_{\rm e}\sigma_m^2 r_{\rm e}^{\alpha_j}}{P_m G_{\rm e}}} \mathbb{E}_{I_m}\left[e^{-\frac{iAT_{\rm e} r_{\rm e}^{\alpha_j}}{P_m G_i} I} \right] p_j(r_{\rm e}) {\rm d}r_{\rm e} \right).$$

where $\mathbb{E}_{I_m}[.]$ is the inteference from all other mmWave BSs.

3.3. mmWave link - Fixed LOS model

Leveraging the modeling of blockage in [4], we consider a simple LOS model for each and every link[2].

Proposition 5. *The secrecy outage probability of a typical mmWave link for fixed LOS Model is given as*

$$\mathcal{P}_s(T_{\rm e}) = 1 - \exp\left(-\sum_{j\in {\rm L,N}} p_j \frac{2\pi\lambda_{\rm e} r_d^2}{\alpha_j} \sum_{i=1}^{m} \binom{m}{i} (-1)^{i+1} \right. \quad (19)$$
$$\left. \times {\rm E}_{\frac{\alpha-2}{\alpha}}\left(\frac{{\rm iAT_e}\sigma_{\rm m}^2 {\rm r_d}^{\alpha_{\rm j}}}{{\rm P_m G_e}} \right) \right).$$

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

Proof. The proof follows from Proposition 4. □

LOS analysis: Consider $\alpha = 2$, the secrecy outage probability can then be given as

$$\mathcal{P}_s(T_{\rm e}) = 1 - \exp\left(-p_{\rm L}\pi\lambda_{\rm e} \frac{P_m G_{\rm e}}{T_{\rm e}\sigma_m^2} \sum_{i=1}^{m} \binom{m}{i} \frac{(-1)^{i+1}}{i} \right. \quad (20)$$
$$\left. \times \left(1 - \exp\left(-\frac{i.AT_{\rm e}\sigma_m^2 r_d^2}{P_m G_{\rm e}} \right) \right) \right).$$

4. SIMULATION RESULTS

With the expressions already derived, we now analyze the availability of secrecy in mmWave overlaid μWave networks in the presence of randomly distributed eavesdroppers. Due to limitations in space, we do not give the numerical analysis for the connection outage probability. Hereinafter, we perform the analyses under the assumption that the system is above a certain threshold T_l. A network of cell radius of 200m under α-LOS = 2 and α-NLOS = 4 is considered. The transmit power is set at 30dBm for mmWave and 43dBm for μWave BS with thermal noise density of -174dBm/Hz. Fig. 1 shows the secrecy outage probability as a function of $\lambda_{\rm e}$ for both the μWave and mmWave link which follows from (13) and (18). It is evident from Fig. 1a that interference is beneficial for secrecy capacity in μWave systems. This is due to the fact that as the density of BS λ_μ increases, the secrecy outage probability decreases. However, in mmWave systems interference doesn't play a major role which is evident from Fig. 1b. It can also be seen that the increase in directional antenna gain at the eavesdropper increases the secrecy outage probability.

[2]Here, we elucidate the secrecy outage probability only due to constraints in space. The connection outage probability follows easily from the previous subsection with fixed $p_{\rm L}$.

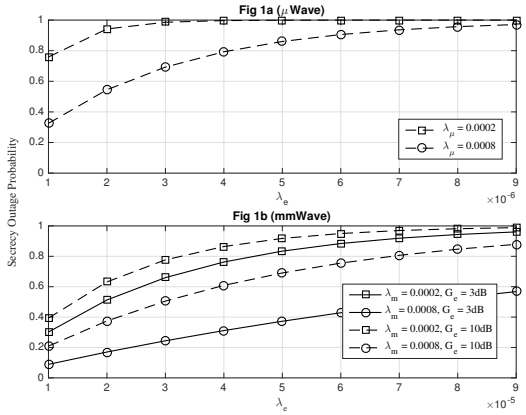

Fig. 1: Secrecy outage probability as a function of $\lambda_{\rm e}$. Parameters - mmWave: m=10, $T_{\rm e}$=15dB, μWave: m=10, $T_{\rm e}$=1dB.

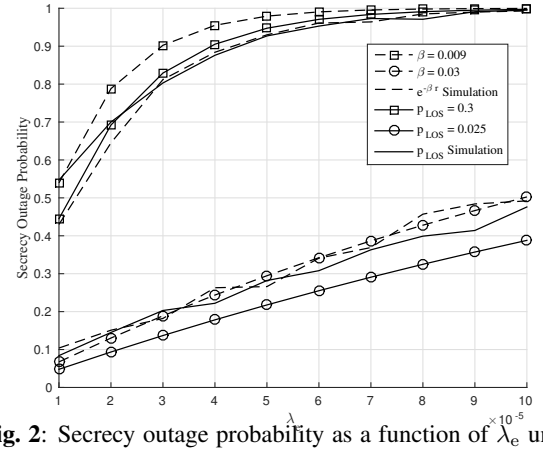

Fig. 2: Secrecy outage probability as a function of $\lambda_{\rm e}$ under mmWave link with m=10, $G_{\rm e}$=10dB, $T_{\rm e}$=10dB, r_d=200m.

Fig. 2 shows the secrecy outage probability as a function of $\lambda_{\rm e}$ for mmWave link considering the two blockage models described under various blockage probabilities. This analysis follows from (17) and (20). 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.

5. CONCLUSION

While blockages have been proved to be detrimental for achieving higher data rates in mmWave systems, they can be helpful for systems with secrecy constraints. Hence, there is a trade off between outage capacity and secrecy outage capacity with respect to blockages which 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.

6. 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] 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.

[4] S. Singh, M. N. Kulkarni, A. Ghosh, and J. G. Andrews, "Tractable model for rate in self-backhauled millimeter wave cellular networks," can be found at http://arxiv.org/pdf/1407.5537v2.pdf, 2015.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

[11] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and congnitive cellular wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 996 – 1019, July 2013.

[12] R. W. Heath, M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using Poisson point processes," *IEEE Transactions on Signal Processing*, vol. 61, no. 16, pp. 4114 – 4126, Aug. 2013.

[13] 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 Comm.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[14] 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.