Physical Layer Security in Large-Scale Millimeter Wave Ad Hoc Networks

Yongxu Zhu*, Lifeng Wang*, Kai-Kit Wong*, and Robert W. Heath, Jr.†
*Department of Electronic and Electrical Engineering, University College London, London, UK
† Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, Texas, USA

***Abstract*—Wireless networks with directional antennas, like millimeter wave networks, have enhanced security. For a large-scale mmWave ad hoc network in which eavesdroppers are randomly located, however, eavesdroppers can still intercept the confidential messages, since they may reside in the signal beam. This paper explores the potential of physical layer security in the mmWave ad hoc networks. Specifically, we characterize the impact of mmWave channel characteristics and large antenna arrays on the secrecy performance. We also characterize the impact of artificial noise in this networks. Our results reveal that in the low transmit power regime, the use of low mmWave frequency achieves better secrecy performance, when increasing transmit power, a transition from low mmWave frequency to high mmWave frequency is demanded for obtaining more secrecy rate. Eavesdroppers can intercept more information by using wide beam pattern. Furthermore, the use of artificial noise may be unable to enhance the secrecy rate for the case of low node density.**

I. Introduction

Millimeter wave (mmWave) ad hoc networks enable higher rate coverage with the assistance of directional transmissions and large bandwidths [1]. They have application in several areas including tactical networks [2], device-to-device, and personal area networking. Since the open nature of wireless medium makes the wireless transmission vulnerable to eavesdropping, security is also an important requirement for mmWave ad hoc networks. Physical layer security provides an alternative for safeguarding wireless transmission [3], by exploiting randomness in the wireless channel.

Physical layer security in mmWave systems has attracted recent interest [4–7], due to the peculiar mmWave channel characteristics. In [4], mmWave antenna subset modulation was designed to secure point-to-point communication by introducing randomness in the received constellation, which confounds the eavesdropper. In [5], the mmWave multiple-input, single-output, multiple-eavesdroppers channel was considered in a single cell, and it was indicated that high-speed secure link at the mmWave frequencies could be reached. The work of [6] illustrated the impacts of key factors such as large bandwidth and directionality on the physical layer security in mmWave networks, and provided more opportunities and challenges in this field. In [7], it was shown that even only one eavesdropper may be able to successfully intercept highly directional mmWave transmission. In the work of [7], although the eavesdropper was located outside the signal beam, reflections could be exploited by the eavesdropper that used small-scale reflectors within the beam, which has little blockage effect on the legitimate receiver's performance. While the prior works are mainly focused on eavesdroppers with fixed locations (See [4–7]), secrecy in large scale mmWave networks with randomly located eavesdroppers has not been conducted yet.

In this paper, we analyze physical layer security in large scale mmWave ad hoc networks using stochastic geometry. Our analysis accounts for the key features of mmWave channel and the impacts of antenna array gain. We also examine the case of using artificial noise for potential secrecy enhancement. The results provide insight into the interplay between transmit power and mmWave frequency. Compared to eavesdropping, the performance is dominated by the surrounding interference in the high node density case. Moreover, artificial noise may not be beneficial to enhance secrecy rate in this networks.

II. System Description

Consider a mmWave ad hoc network, where a group of transmitting nodes are randomly distributed following a homogeneous Poisson point process (PPP) Φ with density λ. The dipole model is adopted [8], where the distance for a typical transmitting node-receiver is fixed at r, and the typical receiver is assumed to be located at the origin. Both the transmitting node and its corresponding receiver use directional beamforming for data transmission, which is intercepted by multiple eavesdroppers. We consider the passive eavesdropping without any active attacks to deteriorate the information transmission. The locations of eavesdroppers are modeled following an independent homogeneous PPP Φ_e with density λ_e. Following [9], we use a sectored model to analyze the beam pattern, i.e., the effective antenna gain for an interferer i seen by the typical receiver is expressed as

$$G_i = \begin{cases} G_{\mathrm{M}}^2, & \Pr_{\mathrm{MM}}=\left(\frac{\theta}{2\pi}\right)^2 \\ G_{\mathrm{M}}G_{\mathrm{m}}, & \Pr_{\mathrm{Mm}}=\frac{\theta(2\pi-\theta)}{(2\pi)^2} \\ G_{\mathrm{m}}G_{\mathrm{M}}, & \Pr_{\mathrm{Mm}}=\frac{\theta(2\pi-\theta)}{(2\pi)^2} \\ G_{\mathrm{m}}^2, & \Pr_{\mathrm{mm}}=\left(\frac{2\pi-\theta}{2\pi}\right)^2 \end{cases}, \tag{1}$$

where G_{M} denotes the main-lobe gain with the beamwidth θ, G_{m} denotes the back-lobe gain, and $\Pr_{\ell k}$ $(\ell, k \in \{\mathrm{M}, \mathrm{m}\})$ denotes the probability that the antenna gain $G_\ell G_k$ occurs. We assume that the maximum array gain $G_{\mathrm{M}}G_{\mathrm{M}}$ is obtained for the typical transmitting node-receiver.

In light of the blockage effects in the outdoor scenario, the signal path can be line-of-sight (LoS) mmWave BS or

non-line-of-sight (NLoS) [10]. We denote $f_{\rm Pr}(R)$ as the probability that a link at a distance R is LoS, while the NLoS probability of a link is $1-f_{\rm Pr}(R)$. The LoS probability function $f_{\rm Pr}(R)$ can be obtained from field measurements or stochastic blockage models [9].

We employ a short-range propagation model in which given a distance $|X_i|$, the path loss function is denoted as $L(|X|) = \beta(\max(d,|X|))^{-\alpha}$ with a reference distance d [11], here, β is the frequency independent constant parameter of the path loss, and α is the path loss exponent depending on the LoS or NLoS link, namely $\alpha=\alpha_{\rm LoS}$ for LoS link and $\alpha=\alpha_{\rm NLoS}$ for NLoS link. Note that the sparse scattering mmWave environment makes many traditional fading distributions invalid for the modeling of the mmWave channel [12], for tractability, we neglect small scale fading as [13] argues that fading is not significant in LOS links with significant beamforming. Hence the signal-to-interference-plus-noise ratio (SINR) at the typical receiver is written as

$$\gamma_o = \frac{P_t G_{\rm M}^2 L(r)}{\sum_{i\in\Phi/o} P_t G_i L(|X_i|)+\sigma_o^2}, \tag{2}$$

where P_t denotes the transmit power, $|X_i|$ is the distance between the typical receiver and the interferer $i\in\Phi/o$ (except the typical transmitting node), and σ_o^2 is the noise power.

When the eavesdropping channel is degraded under the effect of interference, secrecy indeed becomes better. In this paper, we focus on the worst-case eavesdropping scenario, where all the eavesdroppers can mitigate the interference. In fact, eavesdroppers are usually assumed to have strong ability, and they may cooperate with each other to cancel the interference, as seen in [14]. In such a scenario, the most malicious eavesdropper that has the largest SINR of the received signal dominates the secrecy rate [15]. Thus, the SINR at the most malicious eavesdropper is written as

$$\gamma_{e^*} = \max_{e\in\Phi_e}\left\{\frac{P_t G_e L(|X_e|)}{\sigma_e^2}\right\}, \tag{3}$$

where $|X_e|$ is the distance between the typical transmitting node and the eavesdropper $e\in\Phi_e$, σ_e^2 is the power of noise and weak interference, and G_e is the antenna gain seen from the eavesdropper $e\in\Phi_e$ described by

$$G_e = \begin{cases} G_{\rm M}G_{\rm M}^e, & {\rm Pr}_{\rm MM}=\frac{\theta\phi}{(2\pi)^2} \\ G_{\rm M}G_{\rm m}^e, & {\rm Pr}_{\rm Mm}=\frac{\theta(2\pi-\phi)}{(2\pi)^2} \\ G_{\rm m}G_{\rm M}^e, & {\rm Pr}_{\rm Mm}=\frac{2\pi-\theta\phi}{(2\pi)^2} \\ G_{\rm m}G_{\rm m}^e, & {\rm Pr}_{\rm mm}=\frac{(2\pi-\theta)(2\pi-\phi)}{(2\pi)^2} \end{cases}, \tag{4}$$

in which ϕ, $G_{\rm M}^e$ and $G_{\rm m}^e$ are the beamwidth of the main-lobe, main-lobe gain and back-lobe gain of the beam pattern used by the eavesdropper $e\in\Phi_e$, respectively.

III. Secrecy Evaluation

In this section, we analyze the average secrecy rate in mmWave ad hoc networks. As shown in [3], physical layer security is commonly characterized by the secrecy rate $R_{\rm s}$, which is defined as

$$R_{\rm s} = [\log_2(1+\gamma_o) - \log_2(1+\gamma_{e^*})]^+. \tag{5}$$

Using Jensen's inequality, the average secrecy rate is lower bounded as

$$\overline{R}_{\rm s}^{\rm L} = \left[\overline{R}-\overline{R}_{e^*}\right]^+, \tag{6}$$

where $[x]^+=\max\{x,0\}$, $\overline{R}=\mathbb{E}[\log_2(1+\gamma_o)]$ is the average rate of the channel between the typical transmitting node and its receiver, and $\overline{R}_{e^*}=\mathbb{E}[\log_2(1+\gamma_{e^*})]$ is the average rate of the channel between the typical transmitting node and the most malicious eavesdropper.

To evaluate the average secrecy rate, we first derive the average rate $\overline{R}$, which is given by the following theorem.

***Theorem** 1:* The exact average rate between the typical transmitting node and its intended receiver is given by

$$\overline{R} = \frac{1}{\ln 2}\int_0^\infty \frac{1}{z}(1-\Xi_1(z))\Xi_2(z)e^{-z\sigma_o^2}dz, \tag{7}$$

where $\Xi_1(z)$ and $\Xi_2(z)$ are respectively given by (8) and (9) at the top of next page.

***Proof** 1:* Using [16, Lemma 1], the average rate $\overline{R}$ is calculated as

$$\begin{aligned}\overline{R} =& \mathbb{E}[\log_2(1+\gamma_0)] = \frac{1}{\ln 2}\int_0^\infty \frac{1}{z}(1-e^{-z\gamma_o})e^{-z}dz \\ =& \frac{1}{\ln 2}\mathbb{E}\left[\int_0^\infty \frac{1}{z}(1-e^{-zY})e^{-z(\mathcal{I}+\sigma_0^2)}dz\right] \\ =& \frac{1}{\ln 2}\int_0^\infty \frac{1}{z}(1-\underbrace{\mathbb{E}\left[e^{-zY}\right]}_{\Xi_1(z)})\underbrace{\mathbb{E}\left[e^{-z\mathcal{I}}\right]}_{\Xi_2(z)}e^{-z\sigma_0^2}dz, \end{aligned} \tag{10}$$

where $Y = P_t G_{\rm M}^2 L(r)$ is dependent on the LoS or NLoS condition given a distance r, and the interference $\mathcal{I}$ is

$$\mathcal{I} = \sum_{i\in\Phi/o} P_t G_i L(|X_i|). \tag{11}$$

Based on the law of total expectation, we can directly obtain $\Xi_1(z)$ as (8). Then, we see that $\Xi_2(z)$ is the Laplace transform of $\mathcal{I}$. To solve it, using the thinning theorem [17], the mmWave transmitting nodes are divided into two independent PPPs, namely LoS point process $\Phi_{\rm LoS}$ with density function $\lambda f_{\rm Pr}(R)$, and NLoS point process $\Phi_{\rm NLoS}$ with density function $\lambda(1-f_{\rm Pr}(R))$. Accordingly, by using the Slivnyak's theorem [17], $\Xi_2(z)$ is given by

$$\begin{aligned}\Xi_2(z) &= \mathbb{E}\left[e^{-z\mathcal{I}}\right] = \mathbb{E}\left[e^{-z(\mathcal{I}_{\rm LoS}+\mathcal{I}_{\rm NLoS})}\right] \\ &= \mathbb{E}\left[e^{-z\mathcal{I}_{\rm LoS}}\right]\mathbb{E}\left[e^{-z\mathcal{I}_{\rm NLoS}}\right] \end{aligned} \tag{12}$$

with

$$\begin{cases} \mathcal{I}_{\rm LoS} = \sum_{i\in\Phi_{\rm LoS}} P_t G_i L(|X_i|), \\ \mathcal{I}_{\rm NLoS} = \sum_{i\in\Phi_{\rm NLoS}} P_t G_i L(|X_i|). \end{cases} \tag{13}$$

$$\Xi_1(z) = f_{\rm Pr}\left(r\right) e^{-zP_t G_{\rm M}^2 \beta (\max\{r,d\})^{-\alpha_{\rm LoS}}} + (1 - f_{\rm Pr}\left(r\right)) e^{-zP_t G_{\rm M}^2 \beta (\max\{r,d\})^{-\alpha_{\rm NLoS}}} \tag{8}$$

$$\Xi_2(z) = \exp\Big(-2\pi\lambda \int_0^\infty f_{\rm Pr}\left(u\right)\left(1 - \Omega_1(z,u)\right) u du - 2\pi\lambda \int_0^\infty (1 - f_{\rm Pr}\left(u\right))\left(1 - \Omega_2(z,u)\right) u du \Big) \tag{9}$$

with

$$\begin{cases} \Omega_1(z,u) = \sum\limits_{\ell,k\in\{\rm M,m\}} {\rm Pr}_{\ell k} \times e^{-zP_t G_\ell G_k \beta (\max\{u,d\})^{-\alpha_{\rm LoS}}} \\ \Omega_2(z,u) = \sum\limits_{\ell,k\in\{\rm M,m\}} {\rm Pr}_{\ell k} \times e^{-zP_t G_\ell G_k \beta (\max\{u,d\})^{-\alpha_{\rm NLoS}}} \end{cases}$$

By applying the Laplace functional of the PPP [17],

$$\mathbb{E}\left[e^{-z\mathcal{I}_{\rm LoS}}\right] = \exp\Big(-2\pi\lambda \times \int_0^\infty f_{\rm Pr}\left(u\right)\Big(1 - \underbrace{\mathbb{E}\left[e^{-zP_t G_i \beta (\max\{u,d\})^{-\alpha_{\rm LoS}}}\right]}_{\Omega_1}\Big) u du\Big). \tag{14}$$

Based on the array gain distribution in (1) and the law of total expectation, Ω_1 is obtained as

$$\Omega_1(z,u) = \sum_{\ell,k\in\{\rm M,m\}} {\rm Pr}_{\ell k} \times e^{-zP_t G_\ell G_k \beta (\max\{u,d\})^{-\alpha_{\rm LoS}}}. \tag{15}$$

Likewise, we can derive $\mathbb{E}\left[e^{-z\mathcal{I}_{\rm NLoS}}\right]$. Then, we get $\Xi_2(z)$ in (9). Based on (10) and (9), we attain the desired result in (7).

We next derive the average rate between the typical transmitting node and the most malicious eavesdropper, which is given by the following theorem.

***Theorem** 2:* The exact average rate between the typical transmitting node and the most malicious eavesdropper is given by

$$\overline{R}_{e^*} = \frac{1}{\ln 2} \int_0^\infty \frac{\left(1 - \mathcal{P}_1\left(x\right)\mathcal{P}_2\left(x\right)\right)}{1+x} dx, \tag{16}$$

where $\mathcal{P}_1\left(x\right)$ and $\mathcal{P}_2\left(x\right)$ are given in (17) and (18) with $\mathbf{1}\left(A\right)$ representing the indicator function that returns one if the condition A is satisfied.

***Proof** 2:* The average rate $\overline{R}_{e^*}$ is calculated as

$$\begin{aligned} \overline{R}_{e^*} &= \mathbb{E}\left[\log_2\left(1 + \gamma_{e^*}\right)\right] \\ &= \frac{1}{\ln 2} \int_0^\infty \frac{\left(1 - F_{\gamma_{e^*}}\left(x\right)\right)}{1+x} dx, \end{aligned} \tag{19}$$

where $F_{\gamma_{e^*}}\left(\cdot\right)$ is the cumulative distribution function (CDF) of γ_{e^*}. By using the thinning theorem [8], the eavesdroppers are divided into the LoS point process $\Phi_e^{\rm LoS}$ with density function $\lambda_e f_{\rm Pr}(R)$, and NLoS point process $\Phi_e^{\rm NLoS}$ with density function $\lambda_e(1 - f_{\rm Pr}(R))$. Then, $F_{\gamma_{e^*}}\left(\cdot\right)$ is given by

$$\begin{aligned} F_{\gamma_{e^*}}\left(x\right) &= \Pr\left(\gamma_{e^*} < x\right) = \Pr\left(\max\left\{\gamma_{e^*}^{\rm LoS}, \gamma_{e^*}^{\rm NLoS}\right\} < x\right) \\ &= \underbrace{\Pr\left(\gamma_{e^*}^{\rm LoS} < x\right)}_{\mathcal{P}_1(x)} \underbrace{\Pr\left(\gamma_{e^*}^{\rm NLoS} < x\right)}_{\mathcal{P}_2(x)}, \end{aligned} \tag{20}$$

where

$$\begin{cases} \gamma_{e^*}^{\rm LoS} = \max\limits_{e\in\Phi_e^{\rm LoS}} \left\{ \dfrac{P_t G_e L\left(|X_e|\right)}{\sigma_e^2} \right\}, \\ \gamma_{e^*}^{\rm NLoS} = \max\limits_{e\in\Phi_e^{\rm NLoS}} \left\{ \dfrac{P_t G_e L\left(|X_e|\right)}{\sigma_e^2} \right\}. \end{cases} \tag{21}$$

We first derive $\mathcal{P}_1\left(x\right)$ as

$$\begin{aligned} \mathcal{P}_1\left(x\right) &= \Pr\left(\gamma_{e^*}^{\rm LoS} < x\right) \\ &= \mathbb{E}\left[\prod_{e\in\Phi_e^{\rm LoS}} \Pr\left(\frac{P_t G_e \beta \left(\max\left\{r_e, d\right\}\right)^{-\alpha_{\rm LoS}}}{\sigma_e^2} < x\right)\right]. \end{aligned} \tag{22}$$

Using the Laplace functional [17], after some manipulations, we get $\mathcal{P}_1\left(x\right)$ in (17). Then, $\mathcal{P}_2\left(x\right)$ is similarly derived as (18).

Substituting (7) and (16) into (5), we obtain the average secrecy rate in this network.

IV. Artificial Noise Aided Transmission

In this section, we evaluate the secrecy performance for the artificial noise aided transmission [6]. For this case, the total power per transmission is $P_t = P_S + P_A$, where the power allocated to the information signal is $P_S = \mu P_t$, and the power allocated to the artificial noise is $P_A = (1-\mu)P_t$. Here, μ is the fraction of power assigned to the information signal. The effective antenna gain G_i^S for the information signal of an interfering i seen by the typical receiver is expressed as

$$G_i^S = \begin{cases} G_{\rm M}^S G_{\rm M}, & {\rm Pr}_{\rm MM}^S = \frac{\vartheta\theta}{(2\pi)^2} \\ G_{\rm M}^S G_{\rm m}, & {\rm Pr}_{\rm Mm}^S = \frac{\vartheta(2\pi-\theta)}{(2\pi)^2} \\ G_{\rm m}^S G_{\rm M}, & {\rm Pr}_{\rm mM}^S = \frac{(2\pi-\vartheta)\theta}{(2\pi)^2} \\ G_{\rm m}^S G_{\rm m}, & {\rm Pr}_{\rm mm}^S = \frac{(2\pi-\vartheta)(2\pi-\theta)}{(2\pi)^2} \end{cases}, \tag{23}$$

where ϑ, $G_{\rm M}^S$ and $G_{\rm m}^S$ are the beamwidth of the main-lobe, main-lobe gain and back-lobe gain for the information signal of an interfering i, respectively. Likewise, the effective antenna

$$\mathcal{P}_1(x) = \exp\left\{-2\pi\lambda_e \sum_{\ell,n\in\{\mathrm{M},\mathrm{m}\}} \mathrm{Pr}_{\ell n} \int_0^\infty \mathbf{1}\left(\max\{r_e,d\} < \left(\frac{P_t G_\ell G_n^e \beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{LoS}}}}\right) f_{\mathrm{Pr}}(r_e) r_e dr_e\right\} \tag{17}$$

$$\mathcal{P}_2(x) = \exp\left\{-2\pi\lambda_e \sum_{\ell,n\in\{\mathrm{M},\mathrm{m}\}} \mathrm{Pr}_{\ell n} \int_0^\infty \mathbf{1}\left(\max\{r_e,d\} < \left(\frac{P_t G_\ell G_n^e \beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{NLoS}}}}\right) (1 - f_{\mathrm{Pr}}(r_e)) r_e dr_e\right\} \tag{18}$$

gain for the artificial noise of an interfering i seen by the typical receiver is expressed as

$$G_i^A = \begin{cases} G_{\mathrm{M}}^A G_{\mathrm{M}}, & \mathrm{Pr}_{\mathrm{MM}}^A = \frac{\varsigma\theta}{(2\pi)^2} \\ G_{\mathrm{M}}^A G_{\mathrm{m}}, & \mathrm{Pr}_{\mathrm{Mm}}^A = \frac{\varsigma(2\pi-\theta)}{(2\pi)^2} \\ G_{\mathrm{m}}^A G_{\mathrm{M}}, & \mathrm{Pr}_{\mathrm{mM}}^A = \frac{(2\pi-\varsigma)\theta}{(2\pi)^2} \\ G_{\mathrm{m}}^A G_{\mathrm{m}}, & \mathrm{Pr}_{\mathrm{mm}}^A = \frac{(2\pi-\varsigma)(2\pi-\theta)}{(2\pi)^2} \end{cases}, \tag{24}$$

where ς, G_{M}^A and G_{m}^A are the beamwidth of the main-lobe, main-lobe gain and back-lobe gain for the artificial noise of an interfering i, respectively. The effective antenna gain G_e^S and G_e^A for the information signal and artificial noise of the typical transmitting node seen by the eavesdropper $e \in \Phi_e$ can be respectively given from (23) and (24) by interchanging the parameters $G_{\mathrm{M}} \to G_{\mathrm{M}}^e$, $G_{\mathrm{m}} \to G_{\mathrm{m}}^e$ and $\theta \to \phi$.

Considering that the artificial noise sent by the typical transmitting node has negligible effect on the typical receiver [6], the SINR at the typical receiver is given by

$$\widetilde{\gamma}_o = \frac{P_S G_{\mathrm{M}}^S G_{\mathrm{M}} L(r)}{\sum_{i\in\Phi/o} \left(P_S G_i^S + P_A G_i^A\right) L(|X_i|) + \sigma_o^2}. \tag{25}$$

The SINR at the most malicious eavesdropper is given by

$$\widetilde{\gamma}_{e^*} = \max_{e\in\Phi_e} \left\{ \frac{P_S G_e^S L(|X_e|)}{P_A G_e^A L(|X_e|) + \sigma_e^2} \right\}. \tag{26}$$

Following (6), the average secrecy rate for the artificial noise aided transmission is lower bounded as

$$\widetilde{R}_S^{\mathrm{L}} = \left[\widetilde{R} - \widetilde{R}_e^*\right]^+, \tag{27}$$

where $\widetilde{R} = \mathbb{E}\left[\log_2(1+\widetilde{\gamma}_o)\right]$ and $\widetilde{R}_e^* = \mathbb{E}\left[\log_2(1+\widetilde{\gamma}_{e^*})\right]$, $\widetilde{R}$ and $\widetilde{R}_e^*$ are given by the following theorems.

***Theorem** 3:* The exact average rate for the artificial noise aided transmission between the typical transmitting node and its intended receiver is given by

$$\widetilde{R} = \frac{1}{\ln 2} \int_0^\infty \frac{1}{z} (1 - \widetilde{\Xi}_1(z)) \widetilde{\Xi}_2(z) e^{-z\sigma_0^2} dz, \tag{28}$$

where $\widetilde{\Xi}_1(z)$ and $\widetilde{\Xi}_2(z)$ are respectively given by (29) and (30) at the top of next page. In (30), $\mathrm{Pr}_{\mathrm{M}} = \frac{\theta}{2\pi}$ and $\mathrm{Pr}_{\mathrm{m}} = 1 - \mathrm{Pr}_{\mathrm{M}}$.

***Proof** 3:* It can be proved by following a similar approach shown in the **Theorem** 1 .

We next present the average rate between the typical transmitting node and the most malicious eavesdropper as follows.

TABLE I
PATH LOSS EXPONENT FOR MM-WAVE OUTDOOR CHANNELS [18].

Path loss exponent	38 GHz	60 GHz
LOS	2	2.25
Strongest NLOS	3.71	3.76

TABLE II
ANTENNA PATTERN [19].

Number of antenna elements	N
Beamwidth θ	$\frac{2\pi}{\sqrt{N}}$
Main-lobe gain	N
Side-lobe gain	$\frac{1}{\sin^2(3\pi/2\sqrt{N})}$

***Theorem** 4:* The exact average rate for the artificial noise aided transmission between the typical transmitting node and the most malicious eavesdropper is given by

$$\widetilde{R}_e^* = \frac{1}{\ln 2} \int_0^\infty \frac{\left(1 - \widetilde{\mathcal{P}}_1(x)\,\widetilde{\mathcal{P}}_2(x)\right)}{1+x} dx, \tag{31}$$

where $\widetilde{\mathcal{P}}_1(x)$ and $\widetilde{\mathcal{P}}_2(x)$ are respectively given by (32) and (33) at the top of next page. In (32) and (33), $\mathrm{Pr}_{\mathrm{M}}^e = \frac{\phi}{2\pi}$ and $\mathrm{Pr}_{\mathrm{m}}^e = 1 - \mathrm{Pr}_{\mathrm{M}}^e$.

***Proof** 4:* It can be proved by following a similar approach shown in the **Theorem** 2.

Substituting (28) and (16) into (27), we obtain the average secrecy rate for the artificial noise aided transmission.

V. NUMERICAL RESULTS

Numerical results are presented to understand the impact of mmWave channel characteristics and large antenna array on the secrecy rate. We assume that the LoS probability function is $f_{\mathrm{Pr}}(R) = e^{-\varrho R}$ with $\varrho = 141.4$ m [9]. The mmWave bandwidth is BW = 2 GHz, the noise figure is Nf = 10 dB, the noise power is $\sigma_o^2 = \sigma_e^2 = -174 + 10\log 10(\mathrm{BW}) + \mathrm{Nf}$ dBm, and the reference distance is $d = 1$.

We focus on the carrier frequency at 38 GHz and 60 GHz, in which their LoS and NLoS path loss exponents are shown in Table I based on the practical channel measurements [18].

A. Average Secrecy Rate without artificial noise

We consider the uniform planar array (UPA) with the antenna pattern shown in Table II. The transmitting nodes and

$$\widetilde{\Xi}_1(z) = f_{\Pr}(r)\, e^{-zP_S G_{\mathrm{M}}^S G_{\mathrm{M}} \beta (\max\{r,d\})^{-\alpha_{\mathrm{LoS}}}} + (1 - f_{\Pr}(r)) e^{-zP_S G_{\mathrm{M}}^S G_{\mathrm{M}} \beta (\max\{r,d\})^{-\alpha_{\mathrm{NLoS}}}} \tag{29}$$

$$\widetilde{\Xi}_2(z) = \exp\Big(-2\pi\lambda \int_0^\infty f_{\Pr}(u)\,(1 - \widetilde{\Omega}_1(z,u)) u du - 2\pi\lambda \int_0^\infty (1 - f_{\Pr}(u))(1 - \widetilde{\Omega}_2(z,u)) u du \Big) \tag{30}$$

with

$$\begin{cases} \widetilde{\Omega}_1(z,u) = \sum_{\ell,\nu,k \in \{\mathrm{M,m}\}} \dfrac{\Pr_{\ell k}^S \Pr_{\nu k}^A}{\Pr_k} \times e^{-z(P_S G_\ell^S G_k + P_A G_\nu^A G_k)\beta (\max\{u,d\})^{-\alpha_{\mathrm{LoS}}}} \\ \widetilde{\Omega}_2(z,u) = \sum_{\ell,\nu,k \in \{\mathrm{M,m}\}} \dfrac{\Pr_{\ell k}^S \Pr_{\nu k}^A}{\Pr_k} \times e^{-z(P_S G_\ell^S G_k + P_A G_\nu^A G_k)\beta (\max\{u,d\})^{-\alpha_{\mathrm{NLoS}}}} \end{cases}$$

$$\widetilde{\mathcal{P}}_1(x) = \exp\Big\{ -2\pi\lambda_e \sum_{\ell,\nu,n \in \{\mathrm{M,m}\}} \frac{\Pr_{\ell n}^S \Pr_{\nu n}^A}{\Pr_n^e} \int_0^\infty \mathbf{1}\left(\max\{r_e, d\} < \Big(\frac{P_S G_\ell^S G_n^e \beta - P_A G_\nu^A G_n^e \beta x}{x\sigma_e^2} \Big)^{\frac{1}{\alpha_{\mathrm{LoS}}}} \right) f_{\Pr}(r_e) r_e dr_e \Big\} \tag{32}$$

$$\widetilde{\mathcal{P}}_2(x) = \exp\Big\{ -2\pi\lambda_e \sum_{\ell,\nu,n \in \{\mathrm{M,m}\}} \frac{\Pr_{\ell n}^S \Pr_{\nu n}^A}{\Pr_n^e} \int_0^\infty \mathbf{1}\left(\max\{r_e, d\} < \Big(\frac{P_S G_\ell^S G_n^e \beta - P_A G_\nu^A G_n^e \beta x}{x\sigma_e^2} \Big)^{\frac{1}{\alpha_{\mathrm{NLoS}}}} \right) (1 - f_{\Pr}(r_e)) r_e dr_e \Big\} \tag{33}$$

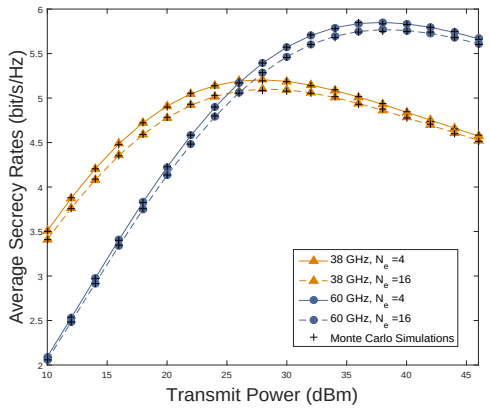

Fig. 1. Effects of transmit power on the average secrecy rate at 38 GHz and 60 GHz: $\lambda = 50/\mathrm{km}^2$, $\lambda_e = 100/\mathrm{km}^2$, $N = 16$, and $r = 15$ m.

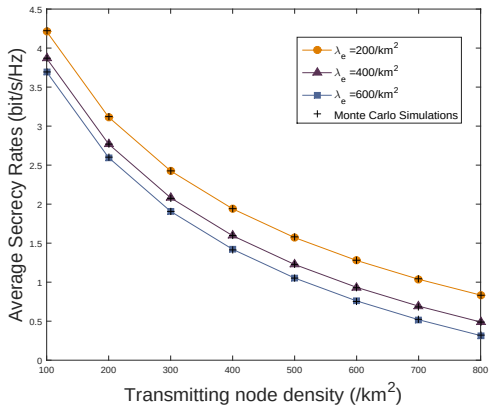

Fig. 2. Effects of transmitting node density on the average secrecy rate at 60 GHz: $N = 16$, $N_e = 16$, $r = 15$ m, and $P_t = 30$ dBm.

their receivers are equipped with N antennas each, and each eavesdropper is equipped with N_e antennas.

Fig. 1 shows the effects of transmit power on the average secrecy rate. The analytical curves are obtained from (6), which are validated by the Monte Carlo simulations marked by '+'. We observe that there exist optimal transmit power values for maximizing average secrecy rate at both 38 GHz and 60 GHz. In the low transmit power regime, better secrecy performance is achieved at 38 GHz, and higher average secrecy rate can be obtained in the higher mmWave frequency band (60 GHz) as the transmit power becomes large, which indicates the interplay between the transmit power and mmWave frequency. Additionally, using the antenna pattern in Table II, average secrecy rate is a bit lower at $N_e = 16$ than that at $N_e = 4$, due to fact that more effective antenna gain obtained by eavesdroppers using UPA with $N_e = 16$, which deteriorates the secrecy performance.

Fig. 2 shows the effects of transmitting node density on the average secrecy rate at 60 GHz. We see that when increasing the transmitting node density, the average secrecy rate declines. The reason is that when the transmitting nodes are dense, mmWave ad hoc networks becomes interference-limited, and the interference caused by other transmitting nodes dominate the performance. It is confirmed that in the large-scale mmWave ad hoc networks, more eavesdroppers have a detrimental effect on the secrecy.

Fig. 3 shows the effects of transmit power with different typical distances on the average rate at 60 GHz. The blue curve obtained from (7) represents the average rate between the typical transmitting node and its intended receiver, and the red curve obtained from (16) represents the average rate in the most malicious eavesdropping channel. We observe that

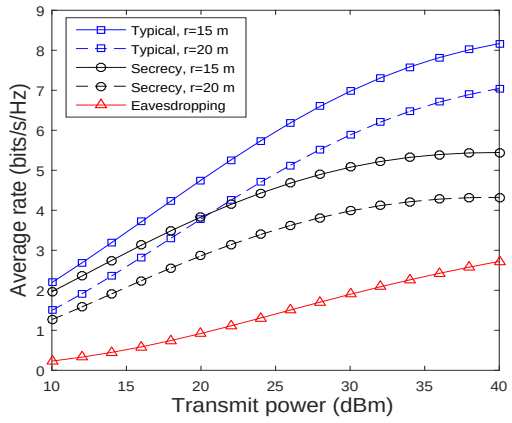

Fig. 3. Effects of transmit power with different typical distances on the average rate at 60 GHz: $\lambda = 50/\text{km}^2$, $\lambda_e = 100/\text{km}^2$, $N = 16$, and $N_e = 16$.

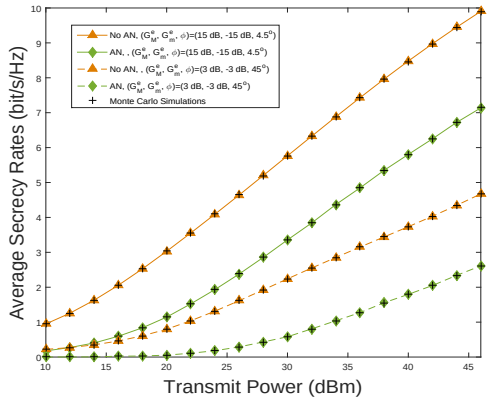

Fig. 4. Effects of transmit power with/without AN on the average secrecy rate at 60 GHz: $\lambda = 20/\text{km}^2$, $\lambda_e = 300/\text{km}^2$, $r = 50$ m, and $\mu = 0.85$.

when the transmit power is large (> 30 dB in this figure), the average secrecy rate slightly increases due to a big increase in the average rate of the most eavesdropping channel. In addition, shorter distances between the typical transmitting node and its desired receiver brings an improvement in the secrecy performance.

B. Average Secrecy Rate with Artificial Noise

In this subsection, we consider that the antenna beam patterns of sending information signal and artificial noise (AN) at the transmitting node are $(G_{\text{M}}^S, G_{\text{m}}^S, \vartheta) = (3\text{ dB}, -3\text{ dB}, 45^o)$ and $(G_{\text{M}}^A, G_{\text{m}}^A, \varsigma) = (3\text{ dB}, -3\text{ dB}, 45^o)$, respectively, and the antenna beam pattern of only sending information signal without AN at the transmitting node is $(G_{\text{M}}, G_{\text{m}}, \theta) = (10\text{ dB}, -10\text{ dB}, 15^o)$, as seen in [1].

Fig. 4 shows the effects of transmit power with/without AN at 60 GHz. The analytical curves without/with AN are obtained from (6) and (27), respectively. We see that when the transmitting nodes are not dense ($\lambda = 20/\text{km}^2$ in this figure), the average secrecy rate increases with the transmit power. In this case, the use of AN is unable to improve secrecy, and more power should be allocated to the information signal. Moreover, it is indicated that eavesdroppers using wide beam pattern can intercept more information.

VI. Conclusion

We analyzed physical layer security in the large-scale mmWave ad hoc networks. We derived the average secrecy rate without/with artificial noise. The results provided important insights for understanding physical layer security in such networks.

References

[1] A. Thornburg, T. Bai, and R. W. Heath Jr., "Performance analysis of mmWave ad hoc networks," *arXiv preprint arXiv: 1412.0765v2*, 2016.

[2] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

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

[4] N. Valliappan, A. Lozano, and R. W. Heath Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, Aug. 2013.

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

[6] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, 2015.

[7] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *IEEE Conf. on Commun. and Netw. Security (CNS)*, 2015, pp. 335–343.

[8] F. Baccelli and B. Błaszczyszyn, *Stochastic Geometry and Wireless Networks, Volume II: Applications*. Now Publishers Inc. Hanover, MA, USA, 2009.

[9] T. Bai and R. W. Heath Jr., "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1100–1114, Feb. 2015.

[10] T. Bai, A. Alkhateeb, and R. W. Heath Jr., "Coverage and capacity of millimeter-wave cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 9, pp. 70–77, Sep. 2014.

[11] F. Baccelli, B. Błaszczyszyn, and P. Muhlethaler, "An Aloha protocol for multihop mobile wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.

[12] O. El Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath Jr., "Spatially sparse precoding in millimeter wave MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1499–1513, Mar. 2014.

[13] T. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[14] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, June 2014.

[15] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[16] K. A. Hamdi, "Capacity of MRC on correlated rician fading channels," *IEEE Trans. Commun.*, vol. 56, no. 5, pp. 708–711, May 2008.

[17] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, 2009.

[18] T. S. Rappaport, E. Ben-Dor, J. N. Murdock, and Y. Qiao, "38 GHz and 60 GHz angle-dependent propagation for cellular & peer-to-peer wireless communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2012, pp. 4568–4573.

[19] K. Venugopal, M. C. Valenti, and R. W. Heath Jr., "Interference in finite-sized highly dense millimeter wave networks," in *Information Theory and Applications Workshop (ITA), 2015*, 2015, pp. 175–180.