Secure Communications in Millimeter Wave Ad Hoc Networks

Yongxu Zhu, Lifeng Wang, *Member, IEEE*, Kai-Kit Wong, *Fellow, IEEE*, and Robert W. Heath, Jr., *Fellow, IEEE*

***Abstract*— Wireless networks with directional antennas, like millimeter wave (mmWave) 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 mmWave ad hoc networks. Specifically, we characterize the impact of mmWave channel characteristics, random blockages, and antenna gains on the secrecy performance. For the special case of uniform linear array (ULA), a tractable approach is proposed to evaluate the average achievable secrecy rate. We also characterize the impact of artificial noise in such networks. Our results reveal that in the low transmit power regime, the use of low mmWave frequency achieves better secrecy performance, and when increasing transmit power, a transition from low mmWave frequency to high mmWave frequency is demanded for obtaining a higher secrecy rate. More antennas at the transmitting nodes are needed to decrease the antenna gain obtained by the eavesdroppers when using ULA. Eavesdroppers can intercept more information by using a wide beam pattern. Furthermore, the use of artificial noise may be ineffective for enhancing the secrecy rate.**

***Index Terms*— Ad hoc, millimeter wave, beamforming, uniform linear array, average achievable secrecy rate.**

I. Introduction

WIRELESS ad hoc networks have been widely applied in several areas including tactical networks, device-to-device, and personal area networking. Unfortunately, interference from nearby transmitters severely deteriorate the throughput of ad hoc networks either through reducing the link quality, or reducing the number of links that can operate simultaneously. Due to the lack of central coordination, beamforming or directional antennas are one approach for suppressing interference [2]. Recently, millimeter wave (mmWave) has been viewed as a promising technology for supporting high-speed data rate in the mobile cellular systems [3]. MmWave with directional transmissions and large bandwidths provides rich opportunities for ad hoc networks. Compared to the lower frequency counterpart, mmWave ad hoc networks experience less interference and achieve greater rate coverage [4].

Security in ad hoc networks is important [5]. The traditional higher-layer key distribution and management may increase the burden of transmitting confidential messages in such decentralized networks. Recent developments have shown that by leveraging the randomness inherent in wireless channels, physical layer security can be a low-complexity alternative for safeguarding complex wireless networks [6]. By taking advantage of unique mmWave channel features, this paper establishes the potential of physical layer security in mmWave ad hoc networks.

A. Related Works and Motivation

Early work has studied the effects of channel fading on physical layer security, see, e.g., [7], [8] and the references therein. The implementation of cooperative jamming and artificial noise can degrade the eavesdropper's channel and further improve secrecy [6], [9]. Recently, new network architectures and emerging transmission technologies such as heterogeneous networks (HetNets) and massive multiple-input multiple-output (MIMO) have promoted more research on physical layer security. In HetNets, dense small cells are deployed, which results in ubiquitous inter-tier and intra-tier interference. For secrecy communications at the physical layer, such interference can be utilized for confounding the eavesdroppers. In [10], spectrum allocation and transmit beamforming were designed for maximizing the secrecy rate in a two-tier HetNet. In [11], an access threshold-based secrecy mobile association policy was proposed in a K-tier HetNet. Massive MIMO uses large number of antennas to provide high array gains for legitimate receivers. The work of [12] studied the case of jamming when the transmitter equipped with large number of antennas served one single-antenna receiver. It was shown in [13] that the application of random artificial noise in massive MIMO cellular networks can achieve a better performance/complexity tradeoff compared to the conventional null space based artificial noise. In [14], secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN was studied, which showed that the centralized and distributed large-scale antenna systems can coexist to enhance the

Manuscript received August 2, 2016; revised November 18, 2016 and February 4, 2017; accepted February 13, 2017. Date of publication March 17, 2017; date of current version May 8, 2017. This work was supported by the U.K. Engineering and Physical Sciences Research Council under Grant EP/N007840/1 and Grant EP/M016005/1. This paper was presented at IEEE Global Telecommunications Conference, Washington, D.C., USA, 2016 [1]. The associate editor coordinating the review of this paper and approving it for publication was J. Lee. *(Corresponding author: Lifeng Wang.)*

Y. Zhu, L. Wang, and K.-K. Wong are with the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, U.K. (e-mail: yongxu.zhu.13@ucl.ac.uk; lifeng.wang@ucl.ac.uk; kai-kit.wong@ucl.ac.uk).

R. W. Heath is with the Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78712 USA (e-mail: rheath@ece:utexas.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2017.2676087

secrecy and cut power consumption. While the aforementioned literature has provided a solid understanding of physical layer security in the wireless systems with lower-frequency bands (sub-6 GHz), the research on mmWave secrecy communication is in its infancy.

Physical layer security in decentralized wireless networks such as sensor and ad hoc type of networks has been investigated in [15]–[18]. In [15], secrecy transmission capacity under connection outage and secrecy outage concerns was examined in an ad hoc network, in which both legitimate nodes and eavesdroppers are randomly distributed. In [16], the average achievable secrecy rate was examined in a three-tier sensor networks consisting of sensors, access points and sinks, and it was shown that there exists optimal number of access points for maximizing the average achievable secrecy rate. Secrecy enhancement in ad hoc networks was studied in [17], where two schemes for the generation of artificial noise were compared. In [18], relay transmission in ad hoc networks was evaluated from the perspective of security connectivity. Again, these works solely focus on the lower-frequency secrecy communications in decentralized wireless networks.

Due to the peculiar mmWave channel characteristics, physical layer security in mmWave systems has recently attracted much interest [19]–[22]. In [19], mmWave antenna subset modulation was designed to secure point-to-point communication by introducing randomness in the received constellation, which confounds the eavesdropper. In [20], 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 with the assistance of large antenna arrays and large mmWave bandwidths. The work of [21] 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 [22], it was shown that even only one eavesdropper may be able to successfully intercept highly directional mmWave transmission. In the work of [22], 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. Secrecy outage of an mmWave cellular network was analyzed in [23], where authorized users and eavesdroppers were assumed to be single-omnidirectional-antenna nodes. In [24], secrecy outage of a mmWave overlaid microwave network was derived by considering a specific blockage model and assuming that mmWave channel undergoes Nakagami-m fading for tractability. In two-way amplify-and-forward MIMO relaying networks, [25] proposed mmWave secrecy beamforming schemes to maximize the secrecy sum rate.

Prior work only pays attention to the physical layer security in lower-frequency ad hoc networks. In mmWave ad hoc networks, the directional communication with narrow beam is more robust against eavesdropping. The mmWave link is sensitive to the blockage and experiences higher propagation loss, and mmWave channel undergoes rapid fluctuation and has much lower coherence time than the today's networks because of much larger Doppler spread [26]. Hence mmWave link is more random and hard to be intercepted by malicious eavesdroppers compared to the low-frequency counterpart.

B. Approach and Contributions

This paper studies physical layer security in mmWave ad hoc networks. Our analysis accounts for the key features of mmWave channel and the effects of different antenna array gains and node densities. The detailed contributions and insights are summarized as follows.

- We model the mmWave ad hoc networks with the help of stochastic geometry, to characterize the random spatial locations of transmitting nodes and eavesdroppers. The effect of blockage is also incorporated such that links are either line-of-sight (LoS) or non-line-of-sight (NLoS). The average achievable secrecy rate is derived to quantify the impacts of key system parameters such as antenna gain, transmitting node and eavesdropper densities on the secrecy performance. Our results show that with increasing transmit power, a transition from low mmWave frequency to high mmWave frequency is needed for achieving better secrecy performance. Compared to eavesdropping, the performance is dominated by the surrounding interference in the high node density case. The use of different mmWave frequencies has a big impact on the secrecy performance, which needs to be carefully selected in practice.
- We develop an approach to evaluate the average achievable secrecy rate when utilizing uniform linear array (ULA). Our results show that adding more antennas at the transmitting node decreases antenna gains obtained by eavesdroppers.
- We examine the impact of artificial noise on the secrecy rate. Our results show that in mmWave ad hoc networks, the use of artificial noise can still enhance the secrecy when power allocation between the information signal and artificial noise is properly set. Moreover, the use of artificial noise may have an adverse effect on the secrecy rate in the low node density scenarios, where more transmit power should be allocated to improve the transmission rate between the transmitting node and its intended receiver.

The remainder of this paper is organized as follows. Section II presents the network and the mmWave channel model. Section III evaluates the average achievable secrecy rate of this network and also discusses the implementation of uniform linear array. Section IV analyzes the use of artificial noise on the secrecy performance. Numerical results are provided in Section V and conclusion is drawn in Section VI.

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 λ. The dipole model is adopted [27], 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 case of 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 λ_e. We consider the directional beamforming and use a sectored model to analyze the beam pattern [4], [28]–[30] (See Fig. 1 in [4]), i.e., the effective antenna gain for an interferer i seen by the typical receiver is expressed as

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

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 LoS or NLoS. We denote $f_{\Pr}(R)$ as the probability that a link at a distance R is LoS, while the NLoS probability of a link is $1 - f_{\Pr}(R)$. The LoS probability function $f_{\Pr}(R)$ can be obtained from field measurements or stochastic blockage models [29].

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 [31], where α is the path loss exponent depending on the LoS or NLoS link, namely $\alpha = \alpha_{\mathrm{LoS}}$ for LoS link and $\alpha = \alpha_{\mathrm{NLoS}}$ for NLoS link, and β is the frequency independent constant parameter of the path loss, which is commonly set as $(\frac{c}{4\pi f_c})^2$ with $c = 3 \times 10^8 \mathrm{m/s}$ and the carrier frequency f_c. Hence there are different β values for different mmWave frequencies, which allows us to examine the effects of using different mmWave frequencies. Note that the sparse scattering mmWave environment makes many traditional fading distributions invalid for the modeling of the mmWave channel [32]. For tractability, we neglect small scale fading as [33] argues that fading is not significant in LOS links with significant beamforming. Hence the signal-to-interference-plus-noise ratio (SINR) at a typical receiver is written as

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

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 [34]. We assume that the eavesdropping channels are independent of the legitimate channel.[1] In such a scenario, the most malicious eavesdropper that has the largest SINR of the received signal dominates the secrecy rate [36]. 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

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

in which ϕ, G_{M}^e and G_{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 achievable secrecy rate in mmWave ad hoc networks. As shown in [37], physical layer security is commonly characterized by the secrecy rate R_{s}, which is defined as

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

Based on (5), we have the following proposition.

Proposition 1: In mmWave ad hoc networks, the average achievable secrecy rate is given by

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

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

Proof: We first show that the average rate $\overline{R}$ is achievable by considering the fact that mmWave channel experiences rapid fluctuation, and the coherence time in mmWave frequencies is around an order of magnitude lower than that at sub-6 GHz as the Doppler shift linearly scales with frequency [26], [38]. Moreover, mmWave links undergo more dramatic swings between LoS and NLoS due to the high level of shadowing [26]. Therefore, coding over many coherence intervals is possible, and thus the average rate $\overline{R}$ can be achieved.

[1] We highlight that the secrecy in the mmWave correlated wiretap channel is a novel and important research area, and the existing contributions at lower frequencies can be seen in [35].

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

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

with

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

Since the malicious eavesdroppers only intercept the secrecy massages passively without any transmissions, the channel state information (CSI) of the eavesdropping channels cannot be obtained by the transmitting node, and the transmission rate of a typical transmitting node is only dependent on the CSI of the channel between itself and the typical receiver. In addition, the maximum average rate in an arbitrary wiretap channel cannot exceed $\overline{R}_{e^*}$. As such, we obtain the average achievable secrecy rate in mmWave ad hoc networks as (6). ■

To evaluate the average achievable 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), shown at the top of this page.[2]

Proof: See Appendix A. ■

The exact average rate given in (7) can be lower bounded as a simple expression, which is as follows.

Theorem 2: The lower bound of the average rate $\overline{R}$ is given by

$$\overline{R}_1^{\rm L} = \log_2\left(1 + \frac{G_{\rm M}^2\beta r^{-\overline{\alpha}}}{\lambda\bar{G}\Lambda + \frac{N_o}{P_t}}\right), \tag{10}$$

where $\overline{\alpha} = (\alpha_{\rm LoS} - \alpha_{\rm NLoS})\, f_{\rm Pr}(r) + \alpha_{\rm NLoS}$, the average antenna gain $\bar{G} = \sum_{\ell,k\in\{\rm M,m\}} G_\ell G_k {\rm Pr}_{\ell k}$, and Λ is

$$\Lambda = \beta 2\pi \Big(\int_0^d \big((d^{-\alpha_{\rm LoS}} - d^{-\alpha_{\rm NLoS}}) r\, f_{\rm Pr}(r) + d^{-\alpha_{\rm NLoS}} r \big) dr + \int_d^{\infty} \big((r^{1-\alpha_{\rm LoS}} - r^{1-\alpha_{\rm NLoS}}) f_{\rm Pr}(r) + r^{1-\alpha_{\rm NLoS}} \big) dr \Big). \tag{11}$$

[2]We consider that the typical legitimate channel and the interfering channels are independent, due to the fact that the coherence time of mmWave channel is around an order of hundreds of microseconds and much shorter than today's cellular systems, and mmWave links experience more dramatic swings in path loss [26].

When the LoS probability is $f_{\rm Pr}(R) = e^{-\varrho R}$ [29], (10) reduces to a closed-form expression with

$$\Lambda = \beta 2\pi \times \Big[\frac{1 - e^{-d\varrho}(1 + d\varrho)}{\varrho^2} \Big(\frac{1}{d^{\alpha_{\rm LoS}}} - \frac{1}{d^{\alpha_{\rm NLoS}}} \Big) + \frac{\Gamma(2 - \alpha_{\rm LoS}, d\varrho)}{\varrho^{2-\alpha_{\rm LoS}}} + \frac{\alpha_{\rm NLoS} \cdot d^{2-\alpha_{\rm NLoS}}}{2(\alpha_{\rm NLoS} - 2)} - \frac{\Gamma(2 - \alpha_{\rm NLoS}, d\varrho)}{\varrho^{2-\alpha_{\rm NLoS}}} \Big]. \tag{12}$$

Proof: See Appendix B. ■

From **Theorem 2**, we find that as the transmit power grows large, the average rate is asymptotically lower bounded as $\overline{R}_1^{\rm L} \to \log_2\left(1 + \frac{G_{\rm M}^2\beta r^{-\overline{\alpha}}}{\lambda\bar{G}\Lambda}\right)$. It is explicitly shown from (10) that the average rate between the typical transmitting node and its receiver is a decreasing function of transmitting node density, and increases with narrower beam due to the lower average interfering antenna gain. In addition, we have the following important corollary.

Corollary 1: Given a required average rate $\overline{R}_{\rm th}$ between the typical transmitting node and its receiver, it is achievable when the transmitting node density in the mmWave ad hoc network satisfies

$$\lambda \le \left(\frac{G_{\rm M}^2\beta r^{-\overline{\alpha}}}{2^{\overline{R}_{\rm th}} - 1} - \frac{N_o}{P_t} \right) \bar{G}^{-1}\Lambda^{-1}. \tag{13}$$

From (13), we see that narrower beams allow mmWave ad hoc networks to accommodate more transmitting nodes.

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

Theorem 3: The exact average rate between the typical transmitting node and the most malicious eavesdropper is given by

$$\overline{R}_{e^*} = \frac{1}{\ln 2} \int_0^{\infty} \frac{(1 - \mathcal{P}_1(x)\, \mathcal{P}_2(x))}{1 + x} dx, \tag{14}$$

where $\mathcal{P}_1(x)$ and $\mathcal{P}_2(x)$ are given in (15) and (16), as shown at the top of next page, with $\mathbf{1}(A)$ representing the indicator function that returns one if the condition A is satisfied.

Proof: See Appendix C. ■

Substituting (7) and (14) into (5), we can thus evaluate the average achievable secrecy rate in this network.

$$\mathcal{P}_1(x) = \exp\left\{-2\pi\lambda_e \int_0^\infty f_{\mathrm{Pr}}(r_e) r_e \sum_{\ell,n\in\{\mathrm{M,m}\}} \mathbf{1}\left(\max\{r_e, d\} < \left(\frac{P_t G_\ell G_n^e \beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{LoS}}}}\right) \mathrm{Pr}_{\ell n} dr_e\right\} \tag{15}$$

$$\mathcal{P}_2(x) = \exp\left\{-2\pi\lambda_e \int_0^\infty (1 - f_{\mathrm{Pr}}(r_e)) r_e \sum_{\ell,n\in\{\mathrm{M,m}\}} \mathbf{1}\left(\max\{r_e, d\} < \left(\frac{P_t G_\ell G_n^e \beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{NLoS}}}}\right) \mathrm{Pr}_{\ell n} dr_e\right\} \tag{16}$$

A. Simplified LoS MmWave Model

The aforementioned analysis is derived by considering an arbitrary LoS probability, which is general. In this subsection, we employ a simplified LoS mmWave model, as mentioned in [29], [39]. In this model, the mmWave link is LoS if the distance for a typical transmitting node-receiver is not larger than the maximum LoS distance $\mathrm{D_{LoS}}$, and otherwise it is outage. When an LoS link between a typical transmitting node and its receiver is established (i.e., $r < \mathrm{D_{LoS}}$), the exact average rate between the typical transmitting node and its intended receiver given in **Theorem 1** can be simplified as

$$\hat{R} = \frac{1}{\ln 2}\int_0^\infty \frac{1}{z}(1 - e^{-z P_t G_{\mathrm{M}}^2 L(r)})\hat{\Xi}_2(z) e^{-z\sigma_o^2} dz, \tag{17}$$

where $\hat{\Xi}_2(z)$ is calculated as

$$\begin{aligned}\hat{\Xi}_2(z) = \exp\Bigg\{ &- 2\pi\lambda\Bigg[\frac{\mathrm{D_{LoS}^2}}{2} - \sum_{\ell,k\in\{\mathrm{M,m}\}} \mathrm{Pr}_{\ell k} \\ &\times\Big(\frac{d^2}{2} e^{-z P_t G_{\mathrm{M}}^2 \beta d^{-\alpha_{\mathrm{LoS}}}} + \alpha_{\mathrm{LoS}}^{-1} (z P_t G_\ell G_k \beta)^{2/\alpha_{\mathrm{LoS}}} \\ &\times\Big(\Gamma\Big(-\frac{2}{\alpha_{\mathrm{LoS}}}, z P_t G_\ell G_k \beta \mathrm{D_{LoS}}^{-\alpha_{\mathrm{LoS}}}\Big) \\ &-\Gamma\Big(-\frac{2}{\alpha_{\mathrm{LoS}}}, z P_t G_\ell G_k \beta d^{-\alpha_{\mathrm{LoS}}}\Big)\Big)\Big)\Bigg]\Bigg\}. \end{aligned} \tag{18}$$

Here, $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function [40, (8.350)].

It is explicitly shown from (17) that $\hat{R}$ is a decreasing function of λ, since adding more transmitting nodes results in larger interference.

Likewise, the exact average rate between the typical transmitting node and the most malicious eavesdropper given in **Theorem 3** can be simplified as

$$\overline{R}_{e^*} = \frac{1}{\ln 2}\int_0^\infty \frac{1 - \exp\left(-2\pi\lambda_e \hat{F}_e(x)\right)}{1+x} dx, \tag{19}$$

where the cumulative distribution function is given by

$$\hat{F}_e(x) = \sum_{\ell,n\in\{\mathrm{M,m}\}} \left(\mathbf{1}\left(d < \eta\left(G_\ell, G_n^e, x\right)\right)\frac{d^2}{2} + \frac{\varrho^2 - d^2}{2}\right)\mathrm{Pr}_{\ell n} \tag{20}$$

with $\eta\left(G_\ell, G_n^e, x\right) = \left(\frac{P_t G_\ell G_n^e \beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{LoS}}}}$ and $\varrho = \min\left(\mathrm{D_{LoS}}, \eta\left(G_\ell, G_n^e, x\right)\right)$.

It is explicitly shown from (19) that $\overline{R}_{e^*}$ is an increasing function of λ_e, which means that the exact average rate between the typical transmitting node and the most malicious eavesdropper increases with the number of eavesdroppers.

Substituting (17) and (19) into (6), we can obtain the average achievable secrecy rate.

B. Uniform Linear Array

We proceed to evaluate the secrecy performance when all the nodes in this networks are equipped with ULA. Assume that the number of antennas possessed by each eavesdropper and the transmitting node are denoted by N_e and N, respectively, and each receiver has the same number of antennas as its transmitting node.

For ULA configuration with q antennas, the elements are placed along the y-axis of the propagation plane with $\Delta\tau$ spacing. Hence, the array steering and response vectors for the transmitting node and its receiver are written as [41]

$$\mathbf{a}_t(\varphi, q) = \left[1,\ e^{-j\frac{2\pi}{\omega}\Delta\tau\sin(\varphi)},\ldots,\ e^{-j\frac{2\pi}{\omega}(q-1)\Delta\tau\sin(\varphi)}\right]^T \tag{21}$$

and

$$\mathbf{a}_r(\xi, q) = \left[1,\ e^{-j\frac{2\pi}{\omega}\Delta\tau\sin(\xi)},\ldots,\ e^{-j\frac{2\pi}{\omega}(q-1)\Delta\tau\sin(\xi)}\right]^T, \tag{22}$$

respectively, where ω is the wavelength, $\varphi \sim U(0, 2\pi)$ and $\xi \sim U(0, 2\pi)$ are the azimuth angle of departure (AoD) and angle of arrival (AoA), respectively, and $(\cdot)^T$ denotes transpose. The channel model is established as $\mathbf{H} = \sqrt{L(R)}\mathbf{A}(\xi_r, \varphi_t)$ with the ULA steering matrix $\mathbf{A}(\xi_r, \varphi_t) = \mathbf{a}_r(\xi_r, q)\mathbf{a}_t^H(\varphi_t, q)$, where $(\cdot)^H$ is the conjugate transpose.

We consider that matched filter (MF) beamforming is adopted at all the nodes including eavesdroppers, the transmitting nodes and their receivers for maximizing the received signal power. Note that MF is the optimal beamforming for eavesdroppers, since interference is negligible at the eavesdroppers. Hence, the antenna gain for a typical transmitting node seen by its receiver is

$$G_o = \left|\frac{\mathbf{a}_r^H(\xi_{r_o}, N)}{\sqrt{N}}\mathbf{A}\left(\xi_{r_o}, \varphi_{t_o}\right)\frac{\mathbf{a}_t(\varphi_{t_o}, N)}{\sqrt{N}}\right|^2 = N^2, \tag{23}$$

and the antenna gain for an interferer i seen by the typical receiver is

$$G_i = \left|\frac{\mathbf{a}_r^H(\xi_{r_o}, N)}{\sqrt{N}}\mathbf{A}\left(\xi_{r_{i,o}}, \varphi_{t_{i,o}}\right)\frac{\mathbf{a}_t(\varphi_{t_i}, N)}{\sqrt{N}}\right|^2. \tag{24}$$

Based on (21) and (22), after some manipulations, we have

$$G_i = \frac{1}{N^2}\frac{\left[1 - \cos(N\mathcal{K}_1(\xi_{r_{i,o}}))\right]\left[1 - \cos(N\mathcal{K}_2(\varphi_{t_{i,o}}, \varphi_{t_i}))\right]}{\left[1 - \cos(\mathcal{K}_1(\xi_{r_{i,o}}))\right]\left[1 - \cos(\mathcal{K}_2(\varphi_{t_{i,o}}, \varphi_{t_i}))\right]}, \tag{25}$$

$$\mathcal{P}_1^{\mathrm{ULA}}(x) = \exp\left\{-2\pi\lambda_e \int_0^{\infty}\int_0^{2\pi} \mathbf{1}\left(\max\{r_e, d\} < \left(\frac{P_t G_e(\varphi_{t_{e,o}})\beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{LoS}}}}\right) \frac{f_{\mathrm{Pr}}(r_e)}{2\pi} r_e d\varphi_{t_{e,o}} dr_e\right\} \tag{30}$$

$$\mathcal{P}_2^{\mathrm{ULA}}(x) = \exp\left\{-2\pi\lambda_e \int_0^{\infty}\int_0^{2\pi} \mathbf{1}\left(\max\{r_e, d\} < \left(\frac{P_t G_e(\varphi_{t_{e,o}})\beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{NLoS}}}}\right) \frac{1 - f_{\mathrm{Pr}}(r_e)}{2\pi} r_e d\varphi_{t_{e,o}} dr_e\right\} \tag{31}$$

where $\mathcal{K}_1\left(\xi_{r_{i,o}}\right) = 2\pi\frac{\Delta\tau}{\omega}(\sin(\xi_{r_o}) - \sin(\xi_{r_{i,o}}))$, $\mathcal{K}_2\left(\varphi_{t_{i,o}}, \varphi_{t_i}\right) = 2\pi\frac{\Delta\tau}{\omega}(\sin(\varphi_{t_{i,o}}) - \sin(\varphi_{t_i}))$.

Based on **Theorem 2**, the average rate between the typical transmitting node and its intended receiver is lower bounded as

$$\overline{R}_{\mathrm{ULA}}^{\mathrm{L}} = \log_2\left(1 + \frac{N^2\beta r^{-\overline{\alpha}}}{\lambda\bar{G}\Lambda_{\mathrm{ULA}} + \frac{N_o}{P_t}}\right), \tag{26}$$

where Λ_{ULA} is given from (11) with the average antenna gain

$$\bar{G} = \mathbb{E}[G_i] = \frac{1}{N^2}\mathbb{E}\left[\frac{1 - \cos(N\mathcal{K}_1(\xi_{r_{i,o}}))}{1 - \cos(\mathcal{K}_1(\xi_{r_{i,o}}))}\right] \times \mathbb{E}\left[\frac{1 - \cos(N\mathcal{K}_2(\varphi_{t_{i,o}}, \varphi_{t_i}))}{1 - \cos(\mathcal{K}_2(\varphi_{t_{i,o}}, \varphi_{t_i}))}\right]. \tag{27}$$

Since the beam-direction of the typical node and each interferer is a uniform random variable on $[0, 2\pi]$, we can further obtain

$$\bar{G} = \frac{1}{N^2}\int_0^{2\pi} \frac{1 - \cos(N\mathcal{K}_1(\xi_{r_{i,o}}))}{1 - \cos(\mathcal{K}_1(\xi_{r_{i,o}}))}\frac{1}{2\pi} d\xi_{r_{i,o}} \times \int_0^{2\pi}\int_0^{2\pi} \frac{1 - \cos(N\mathcal{K}_2(\varphi_{t_{i,o}}, \varphi_{t_i}))}{1 - \cos(\mathcal{K}_2(\varphi_{t_{i,o}}, \varphi_{t_i}))}\frac{1}{4\pi^2} d\varphi_{t_{i,o}} d\varphi_{t_i}. \tag{28}$$

Likewise, the antenna gain G_e seen from the eavesdropper $e \in \Phi_e$ is

$$G_e\left(\varphi_{t_{e,o}}\right) = \left|\frac{\mathbf{a}_r^H(\xi_{r_{e,o}}, N_e)}{\sqrt{N}}\mathbf{A}\left(\xi_{r_{e,o}}, \varphi_{t_{e,o}}\right)\frac{\mathbf{a}_t(\varphi_{t_o}, N)}{\sqrt{N}}\right|^2 = \left(\frac{N_e}{N}\right)^2 \frac{1 - \cos(N\mathcal{K}_3(\varphi_{t_{e,o}}))}{1 - \cos(\mathcal{K}_3(\varphi_{t_{e,o}}))}, \tag{29}$$

where $\mathcal{K}_3\left(\varphi_{t_{e,o}}\right) = 2\pi\frac{\Delta\tau}{\omega}(\sin(\varphi_{t_{e,o}}) - \sin(\varphi_{t_o}))$. From (29), we find that increasing the number of antennas at the transmitting node decreases the antenna gain obtained by the eavesdroppers, which is helpful for degrading the signal strength at the eavesdroppers. Based on **Theorem 3**, the exact average rate $\overline{R}_{e^*}^{\mathrm{ULA}}$ between the typical transmitting node and the most malicious eavesdropper is given from (14) by interchanging $\mathcal{P}_1(x) \to \mathcal{P}_1^{\mathrm{ULA}}(x)$ and $\mathcal{P}_2(x) \to \mathcal{P}_2^{\mathrm{ULA}}(x)$, where $\mathcal{P}_1^{\mathrm{ULA}}(x)$ and $\mathcal{P}_2^{\mathrm{ULA}}(x)$ are given by (30) and (31), as shown at the top of this page, respectively. Thus, by using ULA, the average achievable secrecy rate can at least reach

$$\overline{R}_{s,\mathrm{ULA}}^{L} = \left[\overline{R}_{\mathrm{ULA}}^{\mathrm{L}} - \overline{R}_{e^*}^{\mathrm{ULA}}\right]^+. \tag{32}$$

IV. Artificial Noise Aided Transmission

In this section, we evaluate the secrecy performance for the artificial noise aided transmission [21]. 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

$$G_i^S = \begin{cases} G_{\mathrm{M}}^S G_{\mathrm{M}}, & \mathrm{Pr}_{\mathrm{MM}}^S = \dfrac{\vartheta\theta}{(2\pi)^2}, \\ G_{\mathrm{M}}^S G_{\mathrm{m}}, & \mathrm{Pr}_{\mathrm{Mm}}^S = \dfrac{\vartheta(2\pi - \theta)}{(2\pi)^2}, \\ G_{\mathrm{m}}^S G_{\mathrm{M}}, & \mathrm{Pr}_{\mathrm{mM}}^S = \dfrac{(2\pi - \vartheta)\theta}{(2\pi)^2}, \\ G_{\mathrm{m}}^S G_{\mathrm{m}}, & \mathrm{Pr}_{\mathrm{mm}}^S = \dfrac{(2\pi - \vartheta)(2\pi - \theta)}{(2\pi)^2}, \end{cases} \tag{33}$$

where ϑ, G_{M}^S and G_{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 gain for the artificial noise of an interfering i seen by the typical receiver is expressed as

$$G_i^A = \begin{cases} G_{\mathrm{M}}^A G_{\mathrm{M}}, & \mathrm{Pr}_{\mathrm{MM}}^A = \dfrac{\varsigma\theta}{(2\pi)^2}, \\ G_{\mathrm{M}}^A G_{\mathrm{m}}, & \mathrm{Pr}_{\mathrm{Mm}}^A = \dfrac{\varsigma(2\pi - \theta)}{(2\pi)^2}, \\ G_{\mathrm{m}}^A G_{\mathrm{M}}, & \mathrm{Pr}_{\mathrm{mM}}^A = \dfrac{(2\pi - \varsigma)\theta}{(2\pi)^2}, \\ G_{\mathrm{m}}^A G_{\mathrm{m}}, & \mathrm{Pr}_{\mathrm{mm}}^A = \dfrac{(2\pi - \varsigma)(2\pi - \theta)}{(2\pi)^2}, \end{cases} \tag{34}$$

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 (33) and (34) by interchanging the parameters $G_{\mathrm{M}} \to G_{\mathrm{M}}^e$, $G_{\mathrm{m}} \to G_{\mathrm{m}}^e$ and $\theta \to \phi$.

Since the beam of the artificial noise at the typical transmitting node will not be directed to the typical receiver, the artificial noise sent by the typical transmitting node has negligible effect on the typical receiver [21], the SINR at the typical receiver is given by

$$\widetilde{\gamma}_o = \frac{P_S G_{\mathrm{M}}^S G_{\mathrm{M}} L(r)}{\sum_{i\in\Phi/o}\left(P_S G_i^S + P_A G_i^A\right) L(|X_i|) + \sigma_o^2}. \tag{35}$$

The SINR at the most malicious eavesdropper is given by

$$\widetilde{\gamma}_{e^*} = \max_{e\in\Phi_e}\left\{\frac{P_S G_e^S L(|X_e|)}{P_A G_e^A L(|X_e|) + \sigma_e^2}\right\}. \tag{36}$$

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

$$\widetilde{R}_S = \left[\widetilde{R} - \widetilde{R}_e^*\right]^+, \tag{37}$$

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

Theorem 4: The exact average rate for the artificial noise aided transmission between the typical transmitting node and its intended receiver is given by

$$\widetilde{R} = \frac{1}{\ln 2}\int_0^\infty \frac{1}{z}(1-\widetilde{\Xi}_1(z))\widetilde{\Xi}_2(z)e^{-z\sigma_0^2}dz, \tag{38}$$

where $\widetilde{\Xi}_1(z)$ and $\widetilde{\Xi}_2(z)$ are respectively given by (39) and (40), shown at the bottom of this page. In (40), $\mathrm{Pr_M} = \frac{\theta}{2\pi}$ and $\mathrm{Pr_m} = 1 - \mathrm{Pr_M}$.

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

Using the similar approach shown in the Appendix B, the exact average rate given in (38) can be lower bounded as a simple expression, which is given by the following theorem.

Theorem 5: The lower bound of the average rate $\widetilde{R}$ is

$$\widetilde{R}_1^{\mathrm{L}} = \log_2\left(1 + \frac{G_{\mathrm{M}}^S G_{\mathrm{M}}\beta r^{-\overline{\alpha}}}{\lambda\widetilde{\Lambda} + \frac{N_o}{\mu P_t}}\right), \tag{41}$$

where $\widetilde{\Lambda}$ is

$$\begin{aligned}\widetilde{\Lambda} = &\left(\bar{G}_S + \frac{1-\mu}{\mu}\bar{G}_A\right)\beta 2\pi \\ &\times\Big(\int_0^d (d^{-\alpha_{\mathrm{LoS}}} - d^{-\alpha_{\mathrm{NLoS}}}) r\, f_{\mathrm{Pr}}(r) + d^{-\alpha_{\mathrm{NLoS}}} r dr \\ &+ \int_d^\infty (r^{1-\alpha_{\mathrm{LoS}}} - r^{1-\alpha_{\mathrm{NLoS}}}) f_{\mathrm{Pr}}(r) + r^{1-\alpha_{\mathrm{NLoS}}} dr\Big).\end{aligned} \tag{42}$$

with

$\bar{G}_S = \sum_{\ell,k\in\{\mathrm{M,m}\}} G_\ell^S G_k \mathrm{Pr}_{\ell k}^S$, $\bar{G}_A = \sum_{\nu,k\in\{\mathrm{M,m}\}} G_\nu^A G_k \mathrm{Pr}_{\nu k}^A$.

Based on **Theorem** 5, we have the following important corollary.

Corollary 2: The required average rate $\widetilde{R}_{\mathrm{th}}$ between the typical transmitting node and its receiver can be achieved when the transmitting node density satisfies

$$\lambda \le \left(\frac{G_{\mathrm{M}}^S G_{\mathrm{M}}\beta r^{-\overline{\alpha}}}{2^{\widetilde{R}_{\mathrm{th}}} - 1} - \frac{N_o}{\mu P_t}\right)\widetilde{\Lambda}^{-1}. \tag{43}$$

TABLE I

PATH LOSS EXPONENT FOR mm-WAVE OUTDOOR CHANNELS [42], [43]

Path loss exponent	28GHz	38 GHz	60 GHz	73 GHz
LOS	2	2	2.25	2
Strongest NLOS	3	3.71	3.76	3.4

TABLE II

ANTENNA PATTERN [44]

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

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

Theorem 6: The exact average rate for the artificial noise aided transmission between the typical transmitting node and the most malicious eavesdropper is given by

$$\widetilde{R}_e^* = \frac{1}{\ln 2}\int_0^\infty \frac{\left(1-\widetilde{\mathcal{P}}_1(x)\,\widetilde{\mathcal{P}}_2(x)\right)}{1+x}dx, \tag{44}$$

where $\widetilde{\mathcal{P}}_1(x)$ and $\widetilde{\mathcal{P}}_2(x)$ are respectively given by (45) and (46), as shown at the bottom of the next page. In (45) and (46), $\mathrm{Pr}_{\mathrm{M}}^e = \frac{\phi}{2\pi}$ and $\mathrm{Pr}_{\mathrm{m}}^e = 1 - \mathrm{Pr}_{\mathrm{M}}^e$.

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

Substituting (38) and (44) into (37), we obtain the average achievable 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 achievable secrecy rate. We assume that the LoS probability function is $f_{\mathrm{Pr}}(R) = e^{-\varrho R}$ with $1/\varrho = 141.4$ m [29]. 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 28 GHz, 38 GHz, 60 GHz, and 73GHz, in which their LoS and NLoS path loss exponents are shown in Table I based on the practical channel measurements [42], [43].

$$\widetilde{\Xi}_1(z) = f_{\mathrm{Pr}}(r)\, e^{-zP_S G_{\mathrm{M}}^S G_{\mathrm{M}}\beta(\max\{r,d\})^{-\alpha_{\mathrm{LoS}}}} + (1 - f_{\mathrm{Pr}}(r)) e^{-zP_S G_{\mathrm{M}}^S G_{\mathrm{M}}\beta(\max\{r,d\})^{-\alpha_{\mathrm{NLoS}}}} \tag{39}$$

$$\widetilde{\Xi}_2(z) = \exp\Big(-2\pi\lambda\int_0^\infty f_{\mathrm{Pr}}(u)\,(1-\widetilde{\Omega}_1(z,u))u du - 2\pi\lambda\int_0^\infty (1-f_{\mathrm{Pr}}(u))(1-\widetilde{\Omega}_2(z,u))u du\Big) \tag{40}$$

with

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

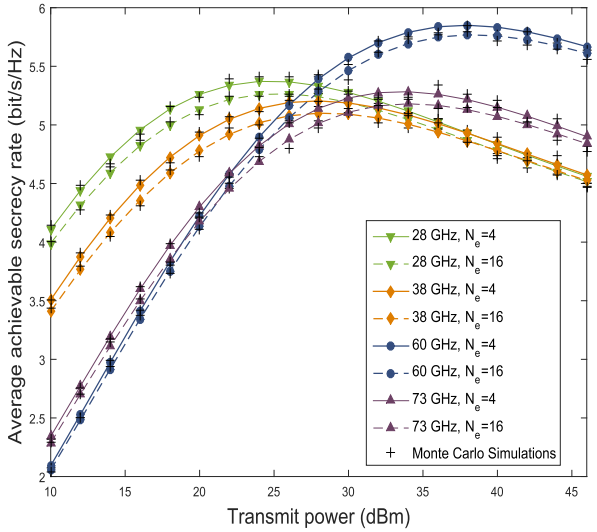


Fig. 1. Effects of transmit power on the average achievable secrecy rate at 28 GHz, 38 GHz, 60 GHz and 73 GHz: $\lambda = 50/\text{km}^2$, $\lambda_e = 100/\text{km}^2$, $N = 16$, and $r = 15$ m.

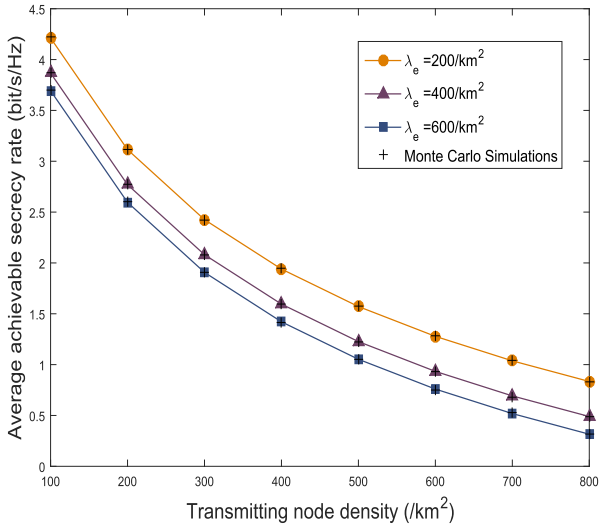


Fig. 2. Effects of transmitting node density on the average achievable secrecy rate at 60 GHz: $N = 16$, $N_e = 16$, $r = 15$ m, and $P_t = 30$ dBm.

A. Average Achievable Secrecy Rate

In this subsection, we consider the uniform planar array (UPA) with the antenna pattern shown in Table II. The transmitting nodes and 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 achievable secrecy rate. We utilize four commonly-considered mmWave carrier frequencies, namely 28 GHz, 38 GHz, 60 GHz and 73 GHz, which have different β values given by $\beta = (\frac{c}{4\pi f_c})^2$ in Section II and path loss exponents in Table I. 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 achievable secrecy rate at all the commonly-considered mmWave frequencies. In the low transmit power regime, better secrecy performance is achieved at 28 GHz, and higher average achievable secrecy rate can be obtained in the higher mmWave frequency band (60 GHz and 73 GHz) as the transmit power becomes large. The reason is that in the low transmit power regime, mmWave ad hoc network tends to be noise-limited, and mmWave link at lower mmWave frequencies experiences lower path loss and has stronger signal strength, which results in better performance. However, in the high transmit power regime, mmWave ad hoc network becomes interference-limited. In this case, the interference received by a legitimate node becomes lower and the signal strength of the eavesdropper is also reduced at higher mmWave frequencies, due to the higher path loss at higher mmWave frequencies. In addition, it is shown that the secrecy performance at 60 GHz is better than that at 73 GHz when the transmit power is large enough, due to the fact that mmWave link at 60 GHz has higher LoS path loss exponent than that at 73 GHz [42], [43] (2.25 at 60 GHz and 2 at 73 GHz in this figure based on the practical channel measurements in [42], [43]), which leads to less interference received by a legitimate node and lower signal strength of the eavesdropper at 60 GHz. Additionally, using the antenna pattern in Table II, average achievable 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 achievable secrecy rate at 60 GHz. We see that when increasing the transmitting node density, the average achievable 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 different typical distances on the average rate at 60 GHz. The green solid and dashed curves with triangles obtained from (7) and (10) represent the exact and lower-bound average rate between the typical transmitting node and its intended receiver, respectively, and the orange solid curve with circles obtained from (14) represents the

$$\widetilde{\mathcal{P}}_1(x) = \exp\Big\{-2\pi\lambda_e \int_0^\infty f_{\text{Pr}}(r_e) r_e \sum\nolimits_{\ell,\nu,n\in\{\text{M,m}\}} \frac{\text{Pr}_{\ell n}^S \text{Pr}_{\nu n}^A}{\text{Pr}_n^e} \mathbf{1}\Big(\max\{r_e, d\} < \big(\frac{P_S G_\ell^S G_n^e \beta - P_A G_\nu^A G_n^e \beta x}{x\sigma_e^2}\big)^{\frac{1}{\alpha_{\text{LoS}}}}\Big) dr_e\Big\} \quad (45)$$

$$\widetilde{\mathcal{P}}_2(x) = \exp\Big\{-2\pi\lambda_e \int_0^\infty (1 - f_{\text{Pr}}(r_e)) r_e \sum\nolimits_{\ell,\nu,n\in\{\text{M,m}\}} \frac{\text{Pr}_{\ell n}^S \text{Pr}_{\nu n}^A}{\text{Pr}_n^e} \mathbf{1}\Big(\max\{r_e, d\} < \big(\frac{P_S G_\ell^S G_n^e \beta - P_A G_\nu^A G_n^e \beta x}{x\sigma_e^2}\big)^{\frac{1}{\alpha_{\text{NLoS}}}}\Big) dr_e\Big\} \quad (46)$$

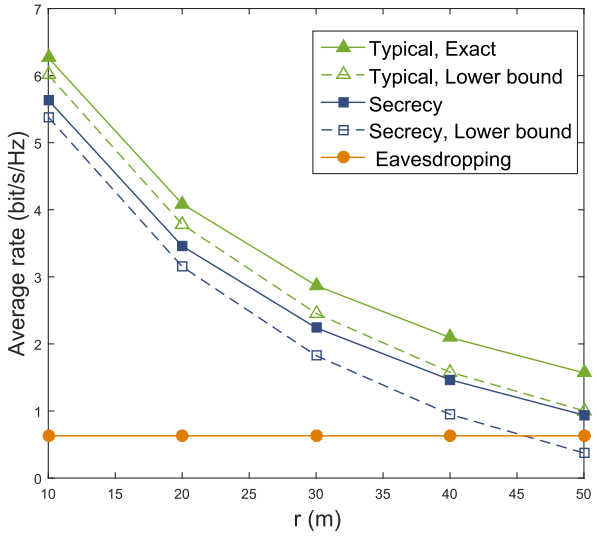


Fig. 3. Effects of transmit power with different typical distances on the average rate at 28 GHz: $P_t = 10$ dBm, $\lambda = 10/\text{km}^2$, $\lambda_e = 100/\text{km}^2$, $N = 16$, and $N_e = 16$.

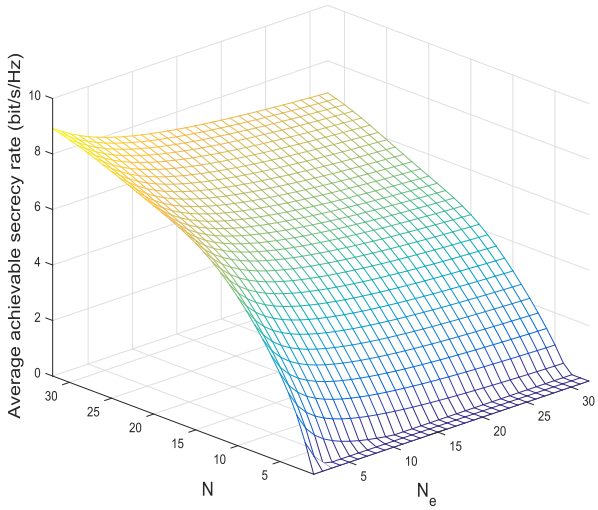


Fig. 4. Effects of different antenna numbers on the average achievable secrecy rate at 38 GHz: $\lambda = 50/\text{km}^2$, $\lambda_e = 100/\text{km}^2$, $r = 20$ m, $P_t = 10$ dBm, $\xi_{r_o} = \pi/3$, $\varphi_{t_o} = \pi/3$.

average rate in the most malicious eavesdropping channel. We observe that the lower bound curves can efficiently predict the performance behavior. It is shown that when the communication distance grows large, there is a significant decrease in the average achievable secrecy rate, due to the fact that the average rate between the typical transmitting node and its receiver decreases while the average rate in the most malicious eavesdropper's channel is unaltered. This illustrates that the secrecy rate in mmWave ad hoc networks is highly dependent on the communication distance between the transmitting node and its receiver.

B. Average Achievable Secrecy Rate With ULA

In this subsection, we consider the ULA configuration, and choose the antenna spacing as $\triangle\tau = \frac{1}{2}\omega$. The results in Figs. 4 and 5 are obtained from (32).

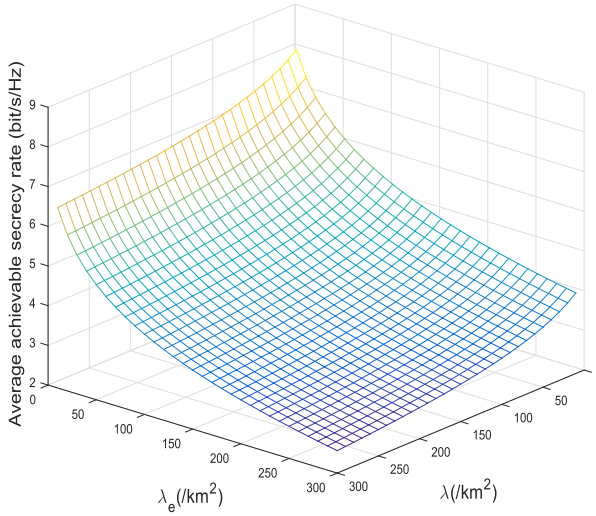


Fig. 5. Effects of different node densities on the average achievable secrecy rate at 38 GHz: $N = 16$, $N_e = 4$, $r = 20$ m, $P_t = 10$ dBm, $\xi_{r_o} = \pi/3$, $\varphi_{t_o} = \pi/3$.

Fig. 4 shows the average achievable secrecy rate with different number of antennas at the transmitting nodes and eavesdroppers. It is observed that the average achievable secrecy rate increases with the number of antennas at the transmitting nodes, and decreases when eavesdroppers are equipped with more antennas. Moreover, the average achievable secrecy rate becomes very small when the transmitting node only has a couple of antennas. The reason is that the information signal beam is not narrow and more eavesdroppers can receive strong signals when they have more receive antennas.

Fig. 5 shows the achievable average achievable secrecy rate for different node densities. We see that more eavesdroppers located in the networks are indeed harmful for secrecy. However, when the density of transmitting nodes increases, the secrecy performance also degrades, which indicates that interference can still be a concern for super dense transmitting nodes without highly directional antennas.

C. Average Achievable Secrecy Rate With Artificial Noise

In this subsection, we examine the effects of artificial noise (AN) on the secrecy performance.

Fig. 6 shows the effects of transmit power with/without AN at 60 GHz. We consider that the antenna beam patterns of sending information signal and AN at the transmitting node are $(G_{\text{M}}^S, G_{\text{m}}^S, \vartheta) = (3\text{ dB}, -3\text{ dB}, 45°)$ and $(G_{\text{M}}^A, G_{\text{m}}^A, \varsigma) = (3\text{ dB}, -3\text{ dB}, 45°)$, respectively, and the antenna beam pattern of only sending information signal without AN at the transmitting node is $(G_{\text{M}}, G_{\text{m}}, \theta) = (10\text{ dB}, -10\text{ dB}, 15°)$, as seen in [4]. The analytical curves without/with AN are obtained from (6) and (37), respectively. We see that when the transmitting nodes are not dense ($\lambda = 20/\text{km}^2$ in this figure), the average achievable secrecy rate increases with the transmit power. In this case, the use of AN with power allocation factor $\mu = 0.85$ may not be able to improve secrecy,[3]

[3]Note that the optimal power allocation for AN aided transmission is infeasible in the passive eavesdropping scenario, where the CSI of the eavesdropping channels cannot be obtained by the transmitting node or legitimate receiver.

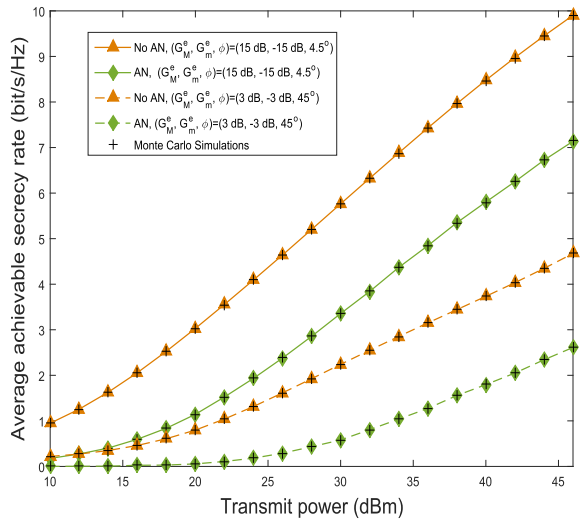


Fig. 6. Effects of transmit power with/without AN on the average achievable secrecy rate at 60 GHz: $\lambda = 20/\text{km}^2$, $\lambda_e = 300/\text{km}^2$, $r = 50$ m, and $\mu = 0.85$.

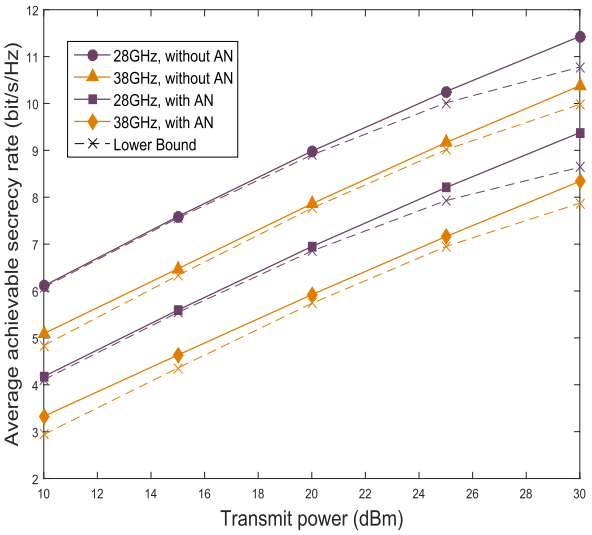


Fig. 7. Effects of transmit power with AN on the average achievable secrecy rate at 28 and 38 GHz: $\lambda = 30/\text{km}^2$, $\lambda_e = 500/\text{km}^2$, $r = 20$ m, $\mu = 0.85$, $(G_\text{M}, G_\text{m}, \theta) = (15\text{ dB}, -15\text{ dB}, 4.5°)$, $(G^S_\text{M}, G^S_\text{m}, \theta) = (10\text{ dB}, -10\text{ dB}, 15°)$, $(G^A_\text{M}, G^A_\text{m}, \theta) = (3\text{ dB}, -3\text{ dB}, 45°)$, $(G^e_\text{M}, G^e_\text{m}, \phi) = (3\text{ dB}, -3\text{ dB}, 45°)$.

and more power should be allocated to the information signal, to combat the severe interference and mmWave pathloss. Such phenomenon has also been mentioned in the prior work [45] with lower frequencies (See Fig. 7 in [45]), which is different from the results in the non large-scale physical layer security model. Moreover, it is indicated that eavesdroppers using wide beam pattern can intercept more information.

Fig. 7 shows the effects of transmit power with/without AN in different frequency bands, i.e., 28 GHz and 38 GHz. The lower-bound results with/without AN are obtained by using (41) and (10) to calculate the average rate between the transmitting node and its receiver, respectively. We see that the lower bound results can well approximate the exact ones when the transmit power is not large (< 30 dBm in this figure). The average achievable secrecy rate at 28 GHz is larger than that

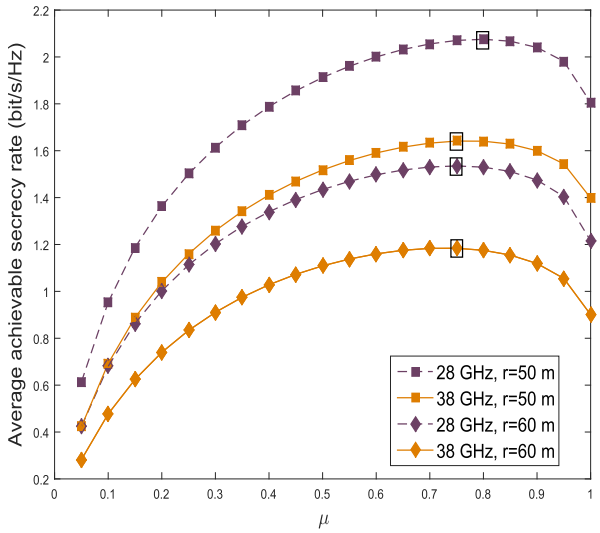


Fig. 8. Effects of transmit power allocation factor on the average achievable secrecy rate at 28 and 38 GHz: $\lambda = 50/\text{km}^2$, $\lambda_e = 500/\text{km}^2$, $P_t = 30$ dBm, $(G_\text{M}, G_\text{m}, \theta) = (10\text{ dB}, -10\text{ dB}, 15°)$, $(G^S_\text{M}, G^S_\text{m}, \vartheta) = (3\text{ dB}, -3\text{ dB}, 45°)$, $(G^A_\text{M}, G^A_\text{m}, \varsigma) = (3\text{ dB}, -3\text{ dB}, 45°)$.

at 38 GHz, which indicates that the use of lower frequency bands could achieve better secrecy performance. The average achievable secrecy rate increases with transmit power, and the use of AN cannot improve the secrecy. The reason is that in this circumstance, more power should be used to enhance the transmission rate between the transmitting node and its receiver.

Fig. 8 shows the effects of transmit power allocation factor on the average achievable secrecy rate. We see that there exists an optimal μ to maximize the average achievable secrecy rate, which reveals that AN can help enhance secrecy when the power allocation between the information signal and AN is properly set. Again, we see that larger communication distance r deteriorates the secrecy performance. In addition, for a given r, secrecy transmission at 28 GHz is better than that at 38 GHz.

VI. Conclusion

We concentrated on the secure communication in mmWave ad hoc networks by using physical layer security. We derived the average achievable secrecy rate without/with artificial noise. A tractable approach was developed to evaluate the average achievable secrecy rate when nodes are equipped with ULA. The results have highlighted the impacts of different mmWave frequencies, transmit power, node density and antenna gains on the secrecy performance. Important insights have been provided into the interplay between transmit power and mmWave frequency. When the node density is dense, the interference from nearby nodes dominates the secrecy performance. It is shown that power allocation between the information signal and AN needs to be carefully determined for secrecy performance enhancement.

In this paper, we assume that the distance r between the typical transmitting node and its receiver is constant. In the future work, we highlight that it is important to study the case of the dynamic r following a certain distribution to model the

specified scenarios. In addition, new antenna pattern models are needed to well characterize the effective antenna gain for a random interferer seen by the typical receiver when the number of mmWave antennas grows large.

APPENDIX A
A DETAILED DERIVATION OF THEOREM 1

Using [46, Lemma 1], the average rate $\overline{R}$ is calculated as

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

where step (a) is obtained based on the fact that Y and I are independent in the ad hoc networks, $Y = P_t G_{\mathrm{M}}^2 L(r)$ is dependent on the LoS or NLoS condition given a distance r, and the interference I is

$$I = \sum\nolimits_{i\in\Phi/o} P_t G_i L(|X_i|). \tag{A.2}$$

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 I. To solve it, using the thinning theorem [47], the mmWave transmitting nodes are divided into two independent PPPs, namely LoS point process Φ_{LoS} with density function $\lambda f_{\mathrm{Pr}}(R)$, and NLoS point process Φ_{NLoS} with density function $\lambda(1 - f_{\mathrm{Pr}}(R))$. Accordingly, by using the Slivnyak's theorem [47], $\Xi_2(z)$ is given by

$$\begin{aligned}\Xi_2(z) &= \mathbb{E}\left[e^{-zI}\right] = \mathbb{E}\left[e^{-z(I_{\mathrm{LoS}}+I_{\mathrm{NLoS}})}\right] \\ &= \mathbb{E}\left[e^{-zI_{\mathrm{LoS}}}\right]\mathbb{E}\left[e^{-zI_{\mathrm{NLoS}}}\right] \end{aligned} \tag{A.3}$$

with

$$\begin{cases} I_{\mathrm{LoS}} = \sum_{i\in\Phi_{\mathrm{LoS}}} P_t G_i L(|X_i|), \\ I_{\mathrm{NLoS}} = \sum_{i\in\Phi_{\mathrm{NLoS}}} P_t G_i L(|X_i|). \end{cases} \tag{A.4}$$

By applying the Laplace functional of the PPP [47],

$$\begin{aligned}\mathbb{E}\left[e^{-zI_{\mathrm{LoS}}}\right] = \exp\Big(&-2\pi\lambda\times\int_0^\infty f_{\mathrm{Pr}}(u) \\ &\times\Big(1-\underbrace{\mathbb{E}\left[e^{-zP_tG_i\beta(\max\{u,d\})^{-\alpha_{\mathrm{LoS}}}}\right]}_{\Omega_1}\Big)udu\Big). \end{aligned} \tag{A.5}$$

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

$$\Omega_1(z,u) = \sum_{\ell,k\in\{\mathrm{M,m}\}} \mathrm{Pr}_{\ell k}\times e^{-zP_tG_\ell G_k\beta(\max\{u,d\})^{-\alpha_{\mathrm{LoS}}}}. \tag{A.6}$$

Likewise, we can derive $\mathbb{E}\left[e^{-zI_{\mathrm{NLoS}}}\right]$. Then, we get $\Xi_2(z)$ in (9). Based on (A.1) and (9), we attain the desired result in (7) and complete the proof.

APPENDIX B
A DETAILED DERIVATION OF EQ. (10)

The average rate between the typical transmitting node and its intended receiver can be tightly lower bounded as [48]

$$\bar{R}_1^{\mathrm{L}} = \log_2\left(1+e^{\mathbb{E}[\ln\gamma_o]}\right), \tag{B.1}$$

where $\mathbb{E}\left[\ln\gamma_o\right]$ is calculated as

$$\begin{aligned}\mathbb{E}\left[\ln\gamma_o\right] = &\underbrace{\mathbb{E}\left[\ln\left(P_tG_{\mathrm{M}}^2\beta r^{-\alpha_o}\right)\right]}_{Z_1} \\ &+\underbrace{\mathbb{E}\left[\ln\left(\frac{1}{\sum_{i\in\Phi/o}P_tG_i\beta\left|X_{i,o}\right|^{-\alpha_i}+N_o}\right)\right]}_{Z_2}. \end{aligned} \tag{B.2}$$

Since the typical link can be either LoS or NLoS, using the law of total probability, Z_1 is calculated as

$$\begin{aligned}Z_1 = &\ln\left(P_tG_{\mathrm{M}}^2\beta\right) \\ &-\left(f_{\mathrm{Pr}}(r)\,\alpha_{\mathrm{LoS}}+(1-f_{\mathrm{Pr}}(r))\,\alpha_{\mathrm{NLoS}}\right)\ln r, \end{aligned} \tag{B.3}$$

where α_{LoS} and α_{NLoS} are the path loss exponents of the LoS and the NLoS, respectively.

Considering the convexity of $\ln\left(\frac{1}{1+x}\right)$ and using Jensen's inequality, we derive the lower bound on the Z_2 as

$$Z_2^{\mathrm{L}} = \ln\left(\frac{1}{\underbrace{\mathbb{E}\Big[\sum_{i\in\Phi/o}P_tG_i\beta\left|X_{i,o}\right|^{-\alpha_i}\Big]}_{\Lambda}+N_o}\right). \tag{B.4}$$

Using a similar approach in (A.3), Λ is derived as

$$\begin{aligned}\overline{\Lambda} = &\mathbb{E}\Big[\sum\nolimits_{i\in\Phi_{\mathrm{LoS}}}P_tG_i\beta\left(\max\{|X_{i,o}|,d\}^{-\alpha_{\mathrm{LoS}}}\right)\Big] \\ &+\mathbb{E}\Big[\sum\nolimits_{i\in\Phi_{\mathrm{NLoS}}}P_tG_i\beta\left(\max\{|X_{i,o}|,d\}^{-\alpha_{\mathrm{NLoS}}}\right)\Big] \\ \overset{(b)}{=} &P_t\bar{G}\beta 2\pi\lambda\times\Big(\int_0^d\big((d^{-\alpha_{\mathrm{LoS}}}-d^{-\alpha_{\mathrm{NLoS}}})r\,f_{\mathrm{Pr}}(r) \\ &\qquad+d^{-\alpha_{\mathrm{NLoS}}}r\big)dr \\ &+\int_d^\infty\big((r^{1-\alpha_{\mathrm{LoS}}}-r^{1-\alpha_{\mathrm{NLoS}}})f_{\mathrm{Pr}}(r)+r^{1-\alpha_{\mathrm{NLoS}}}\big)dr\Big), \end{aligned} \tag{B.5}$$

where $\bar{G}$ is the average array gain. Here, step (b) results from using Campbell's theorem [27]. Based on (1) and using the law of total expectation, $\bar{G}$ is calculated as

$$\bar{G} = \mathbb{E}\{G_i\} = \sum\nolimits_{\ell,k\in\{\mathrm{M,m}\}} G_{\ell k}\mathrm{Pr}_{\ell k}. \tag{B.6}$$

Substituting (B.3), (B.4) and (B.5) into (B.2), we obtain $\mathbb{E}\{\ln\gamma_o\}$ in (B.1), and the desired result (10).

APPENDIX C
A DETAILED DERIVATION OF THEOREM 2

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

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

where $F_{\gamma_{e^*}}(\cdot)$ is the cumulative distribution function (CDF) of γ_{e^*}. By using the thinning theorem [27], the eavesdroppers are divided into the LoS point process Φ_e^{LoS} with density function $\lambda_e f_{\mathrm{Pr}}(R)$, and NLoS point process Φ_e^{NLoS} with density function $\lambda_e(1-f_{\mathrm{Pr}}(R))$. Then, $F_{\gamma_{e^*}}(\cdot)$ is given by

$$\begin{aligned}F_{\gamma_{e^*}}(x) &= \Pr\left(\gamma_{e^*}<x\right) \\ &= \Pr\left(\max\left\{\gamma_{e^*}^{\mathrm{LoS}},\gamma_{e^*}^{\mathrm{NLoS}}\right\}<x\right) \\ &= \underbrace{\Pr\left(\gamma_{e^*}^{\mathrm{LoS}}<x\right)}_{\mathcal{P}_1(x)}\underbrace{\Pr\left(\gamma_{e^*}^{\mathrm{NLoS}}<x\right)}_{\mathcal{P}_2(x)}, \end{aligned} \tag{C.2}$$

where

$$\begin{cases}\gamma_{e^*}^{\mathrm{LoS}} = \max\limits_{e\in\Phi_e^{\mathrm{LoS}}}\left\{\dfrac{P_t G_e L\left(|X_e|\right)}{\sigma_e^2}\right\}, \\ \gamma_{e^*}^{\mathrm{NLoS}} = \max\limits_{e\in\Phi_e^{\mathrm{NLoS}}}\left\{\dfrac{P_t G_e L\left(|X_e|\right)}{\sigma_e^2}\right\}. \end{cases} \tag{C.3}$$

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

$$\begin{aligned}&\mathcal{P}_1(x) \\ &= \Pr\left(\gamma_{e^*}^{\mathrm{LoS}}<x\right) \\ &= \mathbb{E}\left[\prod_{e\in\Phi_e^{\mathrm{LoS}}}\Pr\left(\frac{P_t G_e\beta\left(\max\{r_e,d\}\right)^{-\alpha_{\mathrm{LoS}}}}{\sigma_e^2}<x\right)\right] \\ &\overset{(c)}{=} \exp\Bigg\{-2\pi\lambda_e\times\int_0^{\infty}\underbrace{\Pr\left(\frac{P_t G_e\beta\left(\max\{r_e,d\}\right)^{-\alpha_{\mathrm{LoS}}}}{\sigma_e^2}>x\right)}_{\Theta} \\ &\qquad\times f_{\mathrm{Pr}}(r_e)r_e dr_e\Bigg\}, \end{aligned} \tag{C.4}$$

where step (c) is obtained by using the Laplace functional. Based on the law of total probability, Θ is calculated as

$$\Theta = \sum_{\ell,n\in\{\mathrm{M},\mathrm{m}\}}\mathbf{1}\left(\max\{r_e,d\}<\left(\frac{P_t G_\ell G_n^e\beta}{x\sigma_e^2}\right)^{\frac{1}{\alpha_{\mathrm{LoS}}}}\right)\mathrm{Pr}_{\ell n}, \tag{C.5}$$

Substituting (C.5) into (C.4), we get $\mathcal{P}_1(x)$ in (15). Then, $\mathcal{P}_2(x)$ is similarly derived as (16).

REFERENCES

[1] Y. Zhu, L. Wang, K. K. Wong, and, R. W. Heath, Jr., "Physical layer security in large-scale millimeter wave ad hoc networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[2] K. Huang, J. G. Andrews, D. Guo, R. W. Heath, Jr., and R. A. Berry, "Spatial interference cancellation for multiantenna mobile ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1660–1676, Mar. 2012.

[3] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101–107, Jun. 2011.

[4] A. Thornburg, T. Bai, and R. W. Heath, Jr., "Performance analysis of outdoor mmWave ad hoc networks," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4065–4079, Aug. 2016.

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

[6] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[8] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[9] X. Zhou and M. R. Mckay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[10] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[11] H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[12] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[13] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[14] L. Wang, K. K. Wong, M. Elkashlan, A. Nallanathan, and S. Lambotharan, "Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1375–1389, Dec. 2016.

[15] 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.

[16] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.

[17] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[18] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 624–632, Apr. 2014.

[19] 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, pp. 3231–3245, Aug. 2013.

[20] 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 *Proc. IEEE 15th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2014, pp. 115–119.

[21] 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, Apr. 2015.

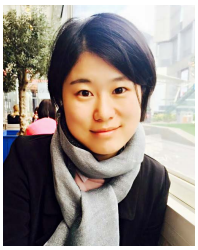
[22] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Sep. 2015, pp. 335–343.

[23] C. Wang and H. M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug. 2016.

[24] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3507–3519, Aug. 2016.

[25] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2059–2071, Mar. 2017.

[26] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.
[27] F. Baccelli and B. Błaszczyszyn, *Stochastic Geometry and Wireless Networks, Volume II-Applications*. Hanover, MA, USA: Now Publishers, 2009.
[28] A. M. Hunter, J. G. Andrews, and S. Weber, "Transmission capacity of ad hoc networks with spatial diversity," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5058–5071, Dec. 2008.
[29] 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.
[30] S. Singh, M. N. Kulkarni, A. Ghosh, and J. G. Andrews, "Tractable model for rate in self-backhauled millimeter wave cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2196–2211, Oct. 2015.
[31] B. F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "An Aloha protocol for multihop mobile wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.
[32] 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.
[33] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.
[34] 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, Jun. 2014.
[35] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated Ergodic fading channels at high MRC," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.
[36] 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.
[37] 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, Jun. 2008.
[38] H. Shokri-Ghadikolaei, C. Fischione, G. Fodor, P. Popovski, and M. Zorzi, "Millimeter wave cellular networks: A MAC layer perspective," *IEEE Trans. Commun.*, vol. 63, no. 10, pp. 3437–3458, Oct. 2015.
[39] J. Park, S. L. Kim, and J. Zander, "Tractable resource management with uplink decoupled millimeter-wave overlay in ultra-dense cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4362–4379, Jun. 2016.
[40] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
[41] N. Moraitis and P. Constantinou, "Indoor channel capacity evaluation utilizing ULA and URA antennas in the millimeter wave band," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2007, pp. 1–5.
[42] S. Deng, M. K. Samimi, and T. S. Rappaport, "28 GHz and 73 GHz millimeter-wave indoor propagation measurements and path loss models," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 1244–1250.
[43] 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)*, Jun. 2012, pp. 4568–4573.
[44] K. Venugopal, M. C. Valenti, and R. W. Heath, Jr., "Interference in finite-sized highly dense millimeter wave networks," in *Proc. Inf. Theory Appl. Workshop (ITA)*, 2015, pp. 175–180.
[45] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May 2016.
[46] K. A. Hamdi, "Capacity of MRC on correlated Rician fading channels," *IEEE Trans. Commun.*, vol. 56, no. 5, pp. 708–711, May 2008.
[47] 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, Sep. 2012.
[48] L. Wang, H. Q. Ngo, M. Elkashlan, Q. Trung Duong, and K. K. Wong, "Massive MIMO in spectrum sharing networks: Achievable rate and power efficiency," *IEEE Syst. J.*, vol. 11, no. 1, pp. 20–31, Mar. 2017.



Yongxu Zhu received the M.S. degree from the Beijing University of Posts and Telecommunications in 2012, the M.S. degree from Dublin City University in 2013, and the Ph.D. degree in wireless communications from the Department of Electronic and Electrical Engineering, University College London, U.K. She is currently a Research Associate with Loughborough University, Loughborough, U.K. Her research interests are in the areas of energy harvesting wireless communications, power control, millimeter-wave communications, heterogeneous cellular networks, massive MIMO, and physical-layer security.

Lifeng Wang (M'16) received the Ph.D. degree in electronic engineering from the Queen Mary University of London in 2015. He is currently a Post-Doctoral Research Fellow with the Department of Electronic and Electrical Engineering, University College London. His research interests include millimeter-wave communications, massive MIMO, cloud-RAN, dense HetNets, ad hoc and sensor networks, caching and IoT enabled networks, cognitive radio, physical layer security, and wireless energy harvesting. He received the Exemplary Editor Certificate and the Exemplary Reviewer Certificate of the IEEE COMMUNICATIONS LETTERS in 2013 and 2016, respectively.

Kai-Kit Wong (M'01–SM'08–F'16) received the B.Eng., M.Phil., and the Ph.D. degrees in electrical and electronic engineering from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. He is currently a Professor of wireless communications with the Department of Electronic and Electrical Engineering, University College London, U.K. He is a fellow of IET. He is a Senior Editor of the IEEE COMMUNICATIONS LETTERS and the IEEE WIRELESS COMMUNICATIONS LETTERS.

Robert W. Heath, Jr. (S'96–M'01–SM'06–F'11) received the B.S. and M.S. degrees from the University of Virginia, Charlottesville, VA, USA, in 1996 and 1997, respectively, and the Ph.D. degree from Stanford University, Stanford, CA, USA, in 2002, all in electrical engineering. From 1998 to 2001, he was a Senior Member of the Technical Staff and then a Senior Consultant with Iospan Wireless Inc., San Jose, CA, USA, where he was involved in the design and implementation of the physical and link layers of the first commercial MIMO-OFDM communication system. Since 2002, he has been with the Department of Electrical and Computer Engineering, The University of Texas at Austin, where he is currently a Cullen Trust for Higher Education Endowed Professor, and a member of the Wireless Networking and Communications Group. He is also the President and CEO of MIMOWireless Inc. He has authored *Introduction to Wireless Digital Communication* (Prentice Hall, 2017), co-authored *Millimeter Wave Wireless Communications* (Prentice Hall, 2014), and authored *Digital Wireless Communication: Physical Layer Exploration Lab Using the NI USRP* (National Technology and Science Press, 2012). He has been a co-author of 15 award winning conference and journal papers, including recently the 2010 and 2013 *EURASIP Journal on Wireless Communications and Networking* Best Paper Awards, the 2012 *Signal Processing Magazine* Best Paper Award, the 2013 Signal Processing Society Best Paper Award, the 2014 *EURASIP Journal on Advances in Signal Processing* Best Paper Award, the 2014 *Journal of Communications and Networks* Best Paper Award, the 2016 IEEE Communications Society Fred W. Ellersick Prize, and the 2016 IEEE Communications and Information Theory Societies Joint Paper Award. He was a Distinguished Lecturer of the IEEE Signal Processing Society. He is an ISI Highly Cited Researcher. He is also an elected member of the Board of Governors for the IEEE Signal Processing Society and a licensed amateur radio operator.