IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 17, NO. 4, APRIL 2018

Safeguarding Millimeter Wave Communications Against Randomly Located Eavesdroppers

Ying Ju*, Hui-Ming Wang*, Senior Member, IEEE, Tong-Xing Zheng†, Member, IEEE,
Qinye Yin, and Moon Ho Lee, Life Senior Member, IEEE

Abstract—Mm-wave offers a sensible solution to the capacity crunch faced by 5G wireless communications. This paper comprehensively studies physical layer security in a multi-input single-output mm-wave system, where multiple single-antenna eavesdroppers are randomly located. Concerning the specific propagation characteristics of mm-wave, we investigate two secure transmission schemes, namely maximum ratio transmitting beamforming and artificial noise (AN) beamforming. Specifically, we first derive closed-form expressions of the connection probability for both schemes. We then analyze the secrecy outage probability in both non-colluding eavesdroppers and colluding eavesdroppers scenarios. Also, we maximize the secrecy throughput under a secrecy outage probability constraint, and obtain optimal transmission parameters, especially the power allocation between AN and the information signal for AN beamforming. Numerical results are provided to verify our theoretical analysis. We observe that the density of eavesdroppers, the spatially resolvable paths of the destination and eavesdroppers all contribute to the secrecy performance and the parameter design of mm-wave systems.

Index Terms—Physical layer security, mm-wave, multipath, stochastic geometry, artificial noise, secrecy outage, secrecy throughput.

I. INTRODUCTION

DRIVEN by an increasing number of smart devices and wireless data applications, an explosive growth of demand for spectrum in wireless communications appears during the past years. Exploiting mm-wave becomes a promising approach for providing plentiful spectrum resources to improve the system capacity [1], [2]. Following this trend, the study on mm-wave communications has attracted great research affords. Mm-wave channel modeling [3], [4], beamforming schemes [5]–[9] and network performance [10], [11] have been investigated intensively in the past few years. It becomes a promising candidate for the 5G cellular system.

Given the open feature of the wireless channels, security is a significant concern when designing wireless transmission schemes. Physical layer security has become a popular way to improve the secrecy performance of wireless communication systems by utilizing wireless channel characteristics [12]–[14]. Thanks to the application of multi-antenna techniques, physical layer security is greatly enhanced in [15], [16]. With multiple antennas, the transmitter can use transmit beamforming either to enhance the legitimate user's channel, i.e., maximum ratio transmitting (MRT) beamforming [17], or to deteriorate eavesdroppers' channels by emitting artificial noise (AN), i.e., AN beamforming [18], [19]. Also, transmit antenna selection technique can be exploited as an effective approach to improve the quality of the legitimate user's channel [20]. When designing secure transmission schemes, reducing secrecy outage probability (SOP) [17], [20] and increasing secrecy throughput [19] are two significant goals.

In wiretap scenarios, eavesdroppers are always passive and their locations are hard to acquire in practice. To model the unknown locations of potential eavesdroppers, stochastic geometry theory has provided a powerful tool recently, with which eavesdroppers’ positions can be represented by a spatial distribution such as a Poisson point process (PPP) [21], [22]. This makes the secure transmission scheme design and secrecy performance evaluation possible in the wireless systems with potentially unknown eavesdroppers.

We should point out that, the wireless channel significantly influences the design and analysis of physical layer security, and the mm-wave channel is truly different from the traditional microwave channel which has rich scattering [23]. Based on the measurements conducted in New York City, the ray cluster channel model, constituted by several clusters of propagation paths, is built for mm-wave systems [4]. This model is further adopted in [5]–[8] to design and analyze mm-wave beamforming schemes. Therefore, the major concern for the implementation of physical layer security in mm-wave communication systems is the specific propagation characteristics.
of mm-wave, which can be described as follows. Firstly, due to the sparse multipaths and scattering of the mm-wave propagation environment, traditional statistically independent fading distributions are no longer suitable to model the mm-wave channel. Channels in the mm-wave band are correlated fading rather than independent and identically distributed (i.i.d.) Rayleigh. Secondly, the small carrier wavelength of mm-wave enables the realization of large antenna arrays, which can produce extremely high beamforming gain and directionality [24]. This helps to improve the secrecy performance of mm-wave transmission [25].

Driven by the new propagation features, studies on secure transmissions in mm-wave systems spring up, both in point-to-point transmissions [26]–[32] and networks [33]–[35]. Specifically, for the point-to-point mm-wave systems, switched array techniques are utilized in [26], [27], where a subset of transmit antennas is randomly selected to emit signals with every symbol period. This results in a clear constellation in the legitimate user’s direction and a high symbol error rate in undesired directions. This method that needs only a single RF chain is easy to implement in mm-wave systems. However, the switching speed to be matched at per-symbol rate leads to a huge system overhead, and the antenna sparsity caused by switching makes the secure transmission vulnerable to attacking [36]. Hybrid beamforming design for mm-wave systems to resist eavesdropping is studied in [28], [29]. Furthermore, in our previous work [30]–[32], we design beamforming schemes and analyze secrecy performance for the mm-wave system which contains only one eavesdropper. For the scope of mm-wave networks, the authors in [33]–[35] analyze the secrecy performance of cellular or Ad hoc networks under the stochastic geometry framework. Both the noise-limited and AN-assisted cellular networks are considered in [33]. The tradeoff between the connection outage probability and secrecy outage probability is investigated for a microwave and mm-wave hybrid cellular network in [34]. The impact of random blockages and antenna gain on the secrecy performance of Ad hoc networks is analyzed in [35]. These three works focus on the network-wide performance analysis, and the beam pattern is approximated by a sectored antenna model for mathematical tractability.

In all the aforementioned studies, they either do not consider multipath transmission, or do not investigate the effect of multiple randomly distributed eavesdroppers. To the best of our knowledge, no previous work has provided secure transmission schemes and comprehensive secrecy performance analysis under a more practical ray cluster channel model that characterizes multipath propagation for a mm-wave system with the stochastic geometry framework. So far, how to safeguard the point-to-point mm-wave system against randomly located eavesdroppers under a more practical mm-wave channel model is still unknown, which motivates our work.

A. Our Work and Contributions

In this paper, we study physical layer security in a multi-input single-output (MISO) mm-wave system considering multipath propagation under a stochastic geometry framework, where the locations of multiple single-antenna eavesdroppers are modeled as a homogeneous PPP. Connection probability, SOP and secrecy throughput are studied to evaluate the secrecy performance of the transmission schemes. Our contributions are summarized as follows:

1) In the presence of multiple randomly located eavesdroppers, we investigate two transmission schemes, namely MRT beamforming and AN beamforming, under the discrete angular domain channel model which characterized by multiple spatially resolvable paths. We obtain the probability distribution function (PDF) for the number of overlapped common channel paths between the destination and an arbitrary eavesdropper to facilitate the secrecy performance analysis.

2) We derive the closed-form connection probability for both transmission schemes and evaluate the impact of the number of destination’s resolvable paths on the connection. Then we obtain the closed-form expressions of SOP for the non-colluding eavesdroppers scenario and the accurate approximation of SOP for the colluding eavesdroppers scenario. In addition, we maximize the secrecy throughput for both schemes, and derive the optimal power allocation between AN and the information signal for the AN scheme. We observe that more power should be allocated to AN in the dense eavesdroppers scenario or in the situation where the number of the destination’s resolvable paths or that of the eavesdropper’s resolvable paths is large.

3) We reveal that AN beamforming has a better secrecy performance than MRT beamforming when the number of the eavesdropper’s resolvable paths is large, the density of eavesdroppers is large or the transmit power is high. Otherwise, MRT beamforming as a simple method shows its superiority. Furthermore, we find that the decrease of the number of the destination’s resolvable paths is beneficial for improving the secrecy performance in both beamforming schemes, while the impact of the number of the eavesdropper’s resolvable paths on the secrecy throughput are different between two schemes.

B. Organization and Notations

This paper is organized as follows. In Section II, we build the channel model, analyze spatially resolvable paths, and describe performance metrics. In Section III, we propose two secure transmission schemes against randomly located eavesdroppers. In Sections IV and V, we analyze the connection probability, the SOP and the secrecy throughput for both schemes. In Section VI, we provide numerical results to verify our theoretical analysis. In Section VII, we conclude our paper.

We use the following notations in this paper: bold uppercase (lowercase) letters denote matrices (vectors). \((\cdot)^*\), \((\cdot)^T\), \((\cdot)^H\), \(|\cdot|\), \(|\cdot|\), \(|\cdot|\), \(\mathbb{P}\{\cdot\}\) and \(\mathbb{E}_A\{\cdot\}\) denote conjugate, transpose, conjugate transpose, absolute value, Euclidean norm, probability, and mathematical expectation with respect to \(A\), respectively. \(CN(\mu, \sigma^2)\), \(\mbox{Exp}(\lambda)\) and \(\Gamma(N, \lambda)\) denote circularly symmetric complex Gaussian distribution with mean \(\mu\) and variance \(\sigma^2\), exponential distribution with parameter \(\lambda\), and gamma distribution with parameters \(N\) and \(\lambda\), respectively. \(\mathbb{C}^{M \times N}\) denotes the space of all \(M \times N\) matrices with complex-valued elements. \(\mathbb{Z}^+\) denotes positive integer domain. log\((\cdot)\),
lg(\cdot) and ln(\cdot) denote base-2, base-10 and natural logarithms, respectively. F_u(\cdot) and F_u^{-1}(\cdot) denote the PDF, cumulative distribution function (CDF) of \( u \) and inverse function of \( F_u(\cdot) \), respectively. The intersection, union and difference between two sets \( \Omega_1 \) and \( \Omega_2 \) are denoted by \( \Omega_1 \cap \Omega_2, \Omega_1 \cup \Omega_2 \) and \( \Omega_1 \setminus \Omega_2 \), respectively. \( E_i(\cdot) = \int_{-\infty}^{\infty} e^{-i} dt \) with \( x > 0 \).

II. System Model

We consider a mm-wave system where a transmitter communicates with a destination while randomly located eavesdroppers attempt to intercept the information. The transmitter is equipped with \( N_t \) antennas, the destination and eavesdroppers are all equipped with single antenna. Without loss of generality, we assume the transmitter is located at the origin and the destination is located at coordinate \((r_d, 0)\). As shown in Fig. 1(a), eavesdroppers are located according to a homogeneous PPP \( \Phi_e \) of density \( \lambda \) on the 2-D plane with the \( k^{th} \) eavesdropper having a distance \( r_k \) from the transmitter.

A. Discrete Angular Domain Channel Model

Due to the sparse characteristics of the mm-wave propagation environment, mm-wave channels can be described by a ray cluster based spatial channel model [4]– [8]. The channel is assumed to be a sum of the contributions of \( N_c \) clusters with \( N_t \) paths in each cluster and can be formulated as \( h = \sqrt{\frac{1}{N_c N_t}} \sum_{l=1}^{N_c} \sum_{l=1}^{N_t} g_{c,l} a(\theta_{c,l}, l)^H \), where \( \beta \) is the average path loss between the transmitter and the receiver, \( g_{c,l} \) is the complex gain of the \( l^{th} \) path in the \( k^{th} \) cluster, \( a(\theta_{c,l}) \) is the normalized array response at the azimuth angle of departure (AOD) of \( \theta_{c,l} \), and \( \Theta_{l, d} = \sin(\theta_{c,l}) \). When a uniform linear array (ULA) is adopted, the normalized array response can be described as \( a(\Theta) = \frac{1}{\sqrt{N_t}} \lbrack e^{-j \frac{2 \pi}{\lambda} d \sin(\Theta)}, e^{-j \frac{2 \pi}{\lambda} 2d \sin(\Theta)}, \ldots, e^{-j \frac{2 \pi}{\lambda} (N_t-1)d \sin(\Theta)} \rbrack^T \), where \( d \) is the antenna spacing, \( \lambda \) is the wavelength, and generally \( d = \frac{\lambda}{2} \).

Based on the ray cluster model, in order to conduct the theoretical analysis of the transmission schemes, the mm-wave channel is modeled as a discrete angular domain channel model in existing literature [3], [37], [38] and our previous work [30], which can be described as

\[
h = \sqrt{\frac{1}{N_c N_t}} \sum_{l=1}^{N_c} \sum_{l=1}^{N_t} g_{c,l} a(\Theta_{l,d}, l)^H, \tag{1}
\]

where \( g = [g_1, g_2, \ldots, g_{N_t}] \) is the complex gain vector, \( r = \frac{\sqrt{d}}{\lambda} \) is the average path loss, \( r \) is the distance between the transmitter and the receiver, \( U \triangleq [a(\Psi_1), a(\Psi_2), \ldots, a(\Psi_{N_t})] \) is the spatially orthogonal basis with \( \Psi_i \triangleq \frac{1}{\sqrt{N_t}} (i-1 - \frac{N_t-1}{2}) \) and \( M = N_t \frac{\lambda}{2} \). This model is based on the principle that every aperture-limited system has a finite angular resolution [37]. Since paths with \( \Theta \) differing by less than \( \frac{\lambda}{4} \) are not resolvable by the array, the angular domain can be sampled at a fixed spacing \( \frac{\lambda}{4} \) and represented by the spatially orthogonal basis

![Fig. 1. Mm-wave system model with stochastic geometry framework.](image)

U. Experimental results in [4] and [39] show that the mm-wave channel most likely contains only one cluster where the overwhelming proportion of transmit power is concentrated on. Therefore, we assume that signals are transmitted through one cluster and all the AODs of paths are distributed within the angular range \([\theta_{min}, \theta_{max}]\). If \( \Psi_i \in [\sin(\theta_{min}), \sin(\theta_{max})] \), the \( i^{th} \) column of \( U \) (the \( i^{th} \) orthogonal basis vector) represents a spatially resolvable path and we assume that the \( i^{th} \) complex gain \( g_i \) is a complex Gaussian coefficient with \( g_i \sim CN(0, 1) \); otherwise, \( g_i = 0 \) [4], [24], [30]. \( L \) is defined as the number of spatially resolvable paths with \( L < N_t \). Then the channels of the destination and the \( k^{th} \) eavesdropper can be described as \( h_d = \sqrt{\frac{1}{L_d}} g_d U^H \) and \( h_k = \sqrt{\frac{1}{L_k}} g_k U^H \), where \( L_d \) and \( L_e \) are the numbers of the destination’s and each eavesdropper’s resolvable paths, respectively.

We assume the AODs of all the destination’s paths and those of the \( k^{th} \) eavesdropper’s paths are distributed within the angular range \([\theta_{d,min}, \theta_{d,max}]\) and \([\theta_{k,min}, \theta_{k,max}]\) respectively. As shown in Fig. 1(b), we define the set \( \Omega_d \triangleq [I_{d,1}, I_{d,2}, \ldots, I_{d,L_d}] \in \mathbb{Z}^+, \Psi_{d,i} \in [\sin(\theta_{d,min}), \sin(\theta_{d,max})], I_{d,i} < I_{d,i+1} < \ldots < I_{d,L_d} \), where \( I_{d,i} \) is an index of the orthogonal basis vector which represents a destination’s spatially resolvable path. Define the set \( \Omega_k \triangleq [I_{k,1}, I_{k,2}, \ldots, I_{k,L_k}] \in \mathbb{Z}^+, \Psi_{k,i} \in [\sin(\theta_{k,min}), \sin(\theta_{k,max})], I_{k,i} < I_{k,i+1} < \ldots < I_{k,L_k} \),
where $I_{k,i}$ is an index of the orthogonal basis vector which represents a resolvable path of the $k^{th}$ eavesdropper. Define $\Omega = \{1, 2, \ldots, N_t\}$, $\Omega_d = \Omega \setminus \Omega_{d_i}$, $\Omega_{c,k} = L_c \cap \Omega_k$ and $\Omega_{p,k} = \Omega_{d} \setminus \Omega_{c,k}$, $\Omega_{n,k} = \Omega_{b} \setminus \Omega_{c,k}$. Also, we denote $L_{c,k}$ as the number of the overlapped common paths between the destination and the $k^{th}$ eavesdropper. For notational brevity, we omit $k$ from $L_{c,k}$, $\Omega_{c,k}$, $\Omega_{p,k}$ and $\Omega_{n,k}$, and treat $L_c$, $\Omega_c$, $\Omega_p$ and $\Omega_n$ as functions of $k$ by default. We define the function $S(B, \Omega_k)$ to generate a matrix whose columns are selected from $B$, and $\Omega_k$ contains all the selected columns’ indexes. Define $g_{\Omega_k} \triangleq S(g_{\Omega_k}, \Omega_k) \in \mathbb{C}^{L \times Ln}$, where $\varrho \in \{d, k\}$, $v \in \{c, p, n, a\}$, and $L_v$ is the cardinality of $\Omega_v$.

We assume that the instantaneous channel state information (CSI) of the destination is perfectly known at the transmitter [18], [19]. Since eavesdroppers passively receive signals, their instantaneous CSIs are unknown, whereas the distribution of $g_k$ is available.

**B. Spatially Resolvable Paths**

Unlike the traditional wireless channels with rich scattering, the mm-wave channel involves a limited angular coverage which is represented by the directions of propagation paths. As we have demonstrated in [30], the secrecy performance of the mm-wave system is dramatically influenced by $L_c$, which is the number of the overlapped common paths between the eavesdropper’s and the destination’s spatially resolvable paths. When $L_c$ becomes larger, the correlation between the channel of the destination and that of the eavesdropper is larger. More confidential information is leaked to the eavesdropper so that the secrecy performance will be poorer. However, under the stochastic geometry framework, it is hard to get the exact value of $L_c$ due to the randomness of eavesdroppers’ locations and the lack of eavesdroppers’ CSIs. Fortunately, we derive the PDF of $L_c$ in the following lemma, which will be extensively used in subsequent sections.

**Lemma 1:** The PDF of $L_c$ can be given by

$$p(L_c) = \begin{cases} \frac{\pi}{2 \omega_i}, & L_c = L_i, \\ \frac{\pi}{2}, & L_c = 1, 2, \ldots, L_i - 1, \\ 1 - \frac{\pi}{2}, & L_c = 0, \end{cases}$$

where $\omega_i = \arcsin\left(\frac{\pi}{N_t - L_{d,i} + 1}\right) - \arcsin\left(\frac{\pi}{N_t - L_{d,i}}\right)$, $L_i = \min(L_d, L_c)$ and $L_u = \max(L_d, L_c)$.

**Proof:** Eavesdroppers are located according to a homogeneous PPP so that the angles of eavesdroppers’ locations are uniformly distributed within the range $[-\frac{\pi}{2}, \frac{\pi}{2}]$. In order to get the probability of $L_c = m$, $m \in \{0, 1, \ldots, \min(L_d, L_c)\}$, we need to know the angular range $\gamma_m$ which satisfies that, the destination and the $k^{th}$ eavesdropper will have $m$ overlapped common resolvable paths when the $k^{th}$ eavesdropper is located in $\gamma_m$. In other words, $[\theta_{k,\min}, \theta_{k,\max}]$ should cover $m$ destination’s spatially resolvable paths, where $[\theta_{k,\min}, \theta_{k,\max}]$ is the angular range where AODs of the $k^{th}$ eavesdropper’ paths are distributed in as discussed in the last subsection. Then we can obtain the probability $p(m) = \frac{\psi(m)}{2\pi}$, where $\psi(.)$ denotes the width of an angular range. With this idea in mind, we move the $k^{th}$ eavesdropper to find out the angular range $\gamma_m$ as shown in Fig. 2.

Since the destination is located at $(r_d, 0)$ and with $L_d$ resolvable paths, we have $\Omega_d = (\frac{\pi}{N_t - L_d + 1}, \frac{\pi}{N_t - L_d + 2}, \ldots, \frac{\pi}{N_t - L_d})$ where $\Omega_{d,i} = \left(\frac{\pi}{N_t - L_d + i} + \arcsin\left(\frac{\pi}{N_t - L_{d,i} + 1}\right)\right)$.

![Fig. 2. Distribution for the number of the overlapped common paths between the destination and the $k^{th}$ eavesdropper.](Image)

The pink area shows the overlapping common paths of the destination and the $k^{th}$ eavesdropper. The green area shows the angular range $\left[\theta_{k,\min}, \theta_{k,\max}\right]$ where AODs of the $k^{th}$ eavesdropper’s paths are distributed in. Red solid lines are the spatially resolvable paths of the destination. Each red dashed line represents an angle in $\Delta_i$ but not the spatially resolvable path of the destination. (a) describes the situation that $L_c = 1$, which is similar to all the situations when $L_c < L_d$; (b) describe the situation that $L_c = L_d$ with $L_d > L_c$ and and $L_d < L_c$ respectively.

![Fig. 2. Distribution for the number of the overlapped common paths between the destination and the $k^{th}$ eavesdropper.](Image)
and the width $o_i \triangleq \mathcal{W}(\Delta_i) = \arcsin \left( \frac{\Psi_{N_i-L_d-\mu}}{\pi} \right) - \arcsin \left( \frac{\Psi_{N_i-L_d+i}}{\pi} \right)$. We find that $\Delta_i$ describes the angular range between the $i^{th}$ and the $(i+1)^{th}$ spatially resolvable paths of the destination when $1 \leq i \leq L_d - 1$. Due to the symmetry of the sine function and the definition of $\Psi_i$, we have $o_i \equiv o_{i+1}$.

As shown in Fig. 2(a), if $\theta_{k,\text{max}}$ is located within $\Delta_1$ or $\theta_{k,\text{min}}$ is located within $\Delta_{L_d-1}$, we have $L_c = 1$. Thus we derive the PDF of $L_c = 1$, which is $p(1) = \frac{2\pi}{\omega + \omega(L_d-1)}$. Then we analyze two different cases $L_d \geq L_c$ and $L_d < L_c$.

1) $L_d \geq L_c$

In this case, $0 \leq L_c \leq L_d$. From the analysis of $L_c = 1$ given above, we derive the PDFs $p(L_c) = \frac{2\pi}{\omega L_c}$, $L_c = 1, 2, \cdots, L_d - 1$ by analogy. The situation when $L_c = L_d$ is special. As shown in Fig. 2(b), when $\theta_{k,\text{max}} \in \Delta_{L_d} \cup \Delta_{L_d+1} \cup \cdots \cup \Delta_{L_d}$, $L_c = L_d$, hence we have $p(L_c) = \frac{2\pi}{\omega L_c \omega}$. Combining the above two cases completes the proof.

C. Wiretap Encoding Scheme and Performance Metrics

We consider both non-colluding eavesdroppers and colluding eavesdroppers scenarios. In non-colluding eavesdroppers scenario, each eavesdropper individually decodes confidential messages and the equivalent signal-to-interference-plus-noise ratio (SINR) of the wiretap channel can be expressed as $\xi_k = \frac{\sum_{i \in \Omega_k} \xi_i}{\sum_{i \in \Omega_k} \xi_i}$, where $\xi_k$ is the received SINR of the $k^{th}$ eavesdropper. In colluding eavesdropper scenario, eavesdroppers jointly decode confidential messages with maximum ratio combining reception and $\xi_k = \frac{\sum_{i \in \Omega_k} \xi_i}{\sum_{i \in \Omega_k} \xi_i}$. Then the capacities of the destination’s channel and the wiretap channel are $C_d = \log(1 + \gamma_d)$ and $C_e = \log(1 + \gamma_e)$. Adopting the well-known Wyner’s wiretap encoding scheme, we denote the codeword rate and secrecy rate as $R_t$ and $R_s$. In addition, we define $R_e \triangleq R_t - R_s$ as the rate redundancy to resist the interception. We analyze the following metrics to evaluate the secrecy performance of transmission schemes.

1) Connection Probability: Only if $C_d > R_t$, the destination is able to decode the confidential message correctly. This corresponds to a reliable connection event. We define connection probability as

$$P_c = P[C_d > R_t].$$

2) Secrecy Outage Probability: If $C_e > R_{e}$, perfect secrecy is broken and a secrecy outage occurs. We adopt an on-off transmission scheme proposed in [19], where the transmitter decides whether to transmit or not based on the instantaneous CSI of the destination. Throughout the paper, for notational brevity, we define $\mu \equiv |\mathbf{g}_d|^2$ as the overall channel gain of the destination and $\delta$ as the transmission threshold. Since the channel gain $\mu$ varies from time to time, the transmitter emits signals only when $\mu > \delta$; otherwise, the transmission suspends. The SOP is defined as

$$P_{so} = P[C_e > R_t, R_s|\mu], \quad \forall \mu > \delta.$$  

3) Secrecy Throughput: Secrecy throughput is defined as the effective average transmission rate of the confidential message, which is formulated as

$$\tau = E_{\mu}[R_s(\mu)],$$

where $R_s(\mu) = 0$ for $\mu \leq \delta$.

III. Transmission Schemes

In this section, we propose two transmission schemes, namely MRT beamforming and AN beamforming, to resist overhearing of multiple randomly located eavesdroppers.

A. MRT Beamforming

By exploiting MRT beamforming, the signals received at the destination and the $k^{th}$ eavesdropper are $y_d^{MRT} = \sqrt{\eta} \mathbf{h}_d \mathbf{w}_1 s + n_d$ and $y_k^{MRT} = \sqrt{\eta} \mathbf{h}_k \mathbf{w}_1 s + n_k$, where $\mathbf{w}_1 = \mathbf{g}_d^H/||\mathbf{g}_d||$ is the beamforming vector, $P$ is the total transmit power, $s$ is the information bearing signal with $\mathbb{E}[|s|^2] = 1$, $n_d$ and $n_k$ are i.i.d. additive white Gaussian noise with $n_d \sim \mathcal{CN}(0, \sigma_n^2)$ and $n_k \sim \mathcal{CN}(0, \sigma_k^2)$. We define $\mu_{c,k} \triangleq ||\mathbf{g}_d||^2$ and $\mu_{p,k} \triangleq ||\mathbf{g}_k||^2$ as the destination’s channel gain of the common paths and the non-common paths with the $k^{th}$ eavesdropper. For notational brevity, we omit $k$ from $\mu_{c,k}$ and $\mu_{p,k}$, and treat them as functions of $k$ by default. We easily find that $\mu = \mu_{c} + \mu_{p}$. Then the SNRs of the destination and the $k^{th}$ eavesdropper can be respectively described as

$$\xi_{d}^{MRT} = \frac{P_{r_{d}}}{\sigma_n^2} ||\mathbf{g}_d||^2 = c \mu r_{d}^{-\alpha},$$

$$\xi_{k}^{MRT} = \frac{P_{r_{k}}}{\sigma_n^2} ||\mathbf{g}_k||^2 = \frac{c \mu_{c,k}^{-\alpha} ||\mathbf{g}_d||^2}{||\mathbf{g}_k||^2}.$$  

where $\alpha \triangleq \frac{P}{\sigma_n^2}$ and $c \triangleq \frac{L_{e}}{r_{d}}$. We find that $g_{k,i}g_{d,i}^{H} \neq 0$ only if $i \in \Omega_d \cap \Omega_k$, i.e., $i \in \Omega_c$. Thus we have $g_k^H = g_k^H g_{d,c}^H$.

B. AN Beamforming

Based on the CSI of the destination, we design the AN beamforming matrix as $\mathbf{W}_2 = \mathcal{S}(\mathbf{U}, \Omega_d)$ to transmit AN to the null space of the destination’s channel. Since $\Omega_d = \Omega_d \setminus \Omega_d$, we have $\mathbf{h}_d \mathbf{W}_2 = 0$, hence the destination is not influenced by AN. We observe that by leveraging the specific propagation characteristics of mm-wave, we form the null space only through selecting some columns from $\mathbf{U}$, which is really simple to operate. Then signals received by the destination and the $k^{th}$ eavesdropper can be described as $y_d^{AN} = \sqrt{\eta} \mathbf{h}_d \mathbf{w}_1 s + \sqrt{\frac{(1-\eta)}{N_{i} - L_d}} \mathbf{h}_d \mathbf{w}_2 z + n_d$ and $y_k^{AN} = \sqrt{\eta} \mathbf{h}_k \mathbf{w}_1 s + \sqrt{\frac{(1-\eta)}{N_{i} - L_d}} \mathbf{h}_k \mathbf{w}_2 z + n_k$, where $z \in \mathbb{C}^{(N_{i} - L_d) \times 1}$ is the AN bearing signal with $\mathbb{E}[zz^H] = \mathbf{I}_{N_{i} - L_d}$, $\eta$ is the power allocation ratio of the information signal power to the total transmit power with $0 \leq \eta \leq 1$. When $\eta = 1$, AN beamforming is equivalent to MRT beamforming where
information signal is transmitted with full power. The SINRs of the destination and the \( k^{th} \) eavesdropper can be respectively formulated as

\[
\begin{align*}
\mathcal{z}_d & = \frac{\eta P_{t,x}^a}{\sigma_n^2} \|g_d U^H\|^2 = \eta \mu r_{d}^{-a}, \\
\mathcal{z}_k & = \frac{\eta P_{t,x}^a}{\sigma_n^2 \|g_k U^H U g_k^H\|^2} \sum_{n=1}^{N_l} \left( \frac{1-\eta P_{t,x}^a}{(N_l-\eta P_{t,x}^a)} \|g_k U^H w_2\|^2 + \sigma_n^2 \right) = \frac{\eta \mu r_{k}^{-a}}{\|g_k \|^2}, \\end{align*}
\]

By denoting \( g_k U^H w_2 = [\zeta_1, \zeta_2, \cdots, \zeta_{(N_l-L_d)}] \), we have \( \zeta_j = \sum_{l=1}^{N_l} g_{k,l} a(\Psi_l) H w_{2,l} \). Since \( W_2 = S(U, \Omega_k) \) and \( U \) is a unitary matrix, we get \( g_k U^H w_2 = g_{k,a} \). Since \( \Omega_k = \Omega_k \backslash \Omega_c \), by getting rid of those zero elements in \( g_{k,a} \), we have \( \|g_{k,a}\| = \|g_k\| \).

IV. SECRECY PERFORMANCE OF MRT BEAMFORMING

In this section, we analyze the secrecy performance in terms of the connection probability, the SOP and the secrecy throughput for MRT beamforming.

A. Connection Probability

Since \( \mu \sim \text{Gamma}(L_d, 1) \), connection probability of MRT beamforming defined in (3) can be described as

\[
\mathcal{P}_c = \mathbb{P}\{C_d > R_t\} = \mathbb{P}\{z_{d}^{\text{MRT}} > 2R_t - 1\} = \frac{1}{\Gamma(L_d)} \left( \frac{L_d}{(2R_t - 1) \mu} \right)^{L_d - 1} e^{-\frac{L_d}{\mu}}.
\]

(10)

where \( \Gamma(\cdot) \) is the gamma function, and \( \Gamma(\cdot, \cdot) \) denotes the upper incomplete gamma function with \( \Gamma(n, x) = (n - 1)! e^{-x} \sum_{m=0}^{n-1} \frac{x^m}{m!} \).

B. Secrecy Outage Performance

1) Non-Colluding Eavesdroppers: We first derive the CDF of \( \zeta_{d}^{\text{MRT}} \) in (7). Define \( u = \|g_k \|^2 \), since each element of \( g_k \) follows a Gaussian distribution with zero mean and unit variance, which is independent of the unit-norm vector \( g_k \), we have \( u \sim \text{Exp}(1) \). The CDF of \( \zeta_{d}^{\text{MRT}} \) is given by

\[
F_{\zeta_{d}}(x) = \mathbb{P}\{ u < x \} = 1 - e^{-\frac{\mu x}{\mu x}}.
\]

(11)

From the definition of \( \mu_c \), we find that \( \mu_c \sim \text{Gamma}(L_c, 1) \). Then the CDF of \( \zeta_e \) can be calculated as

\[
F_{\zeta_{e}}(x) = \mathbb{P}\{ \zeta_{e} < x \} = \mathbb{E}_{\Phi_{e}(\mu_c)} \left[ \prod_{\zeta_{e} \in \Phi_{e}} \mathbb{P}\{ \zeta_{e} < x \} \right] \]

\[
= \exp \left\{ -\lambda \int_{0}^{\infty} \int_{0}^{2\pi} \mathbb{E}_{\mu_c} \left[ e^{-\frac{\mu x}{\mu x}} \right] r_\theta d\theta dr_k \right\} \]

\[
= \exp \left\{ -\pi \lambda \Gamma \left( \frac{2}{\alpha} + 1 \right) \left( \frac{\mu x}{\alpha} \right)^{-2/\alpha} \sum_{L_c=1}^{L_t} p(L_c) \right\}
\]

(12)

where (a) holds for the probability generating functional lemma (PGFL) over PPP. We need to mention that when \( L_c = 0 \), \( g_k \), and \( g_{k}^H \) in (7) both equal to 0, hence we have \( \zeta_{e} = 0 \) and \( \mathbb{P}\{ \zeta_{e} < x \} = 1 \). Since the formula \( \mathbb{E}_{\mu_c} \) is a multiplication operation, the case \( L_c = 0 \) does not contribute to \( F_{\zeta_{e}}(x) \). Therefore, we only consider \( L_c \) from 1 to \( L_t \).

With the CDF of \( \zeta_{e} \), we obtain the SOP defined in (4) as

\[
\mathcal{P}_{so}(\mu) = \mathbb{P}\{C_e > C_d - R_t | \mu\} = \mathbb{P}\{\zeta_{e}^{\text{MRT}} > \frac{z_{d}^{\text{MRT}} - (T - 1)}{T}\}
\]

\[
= 1 - \exp \left\{ -\pi \lambda \Gamma \left( \frac{2}{\alpha} + 1 \right) \left( \frac{\mu_c r_{d}^{-a} - (T-1)}{aT} \right)^{-2/\alpha} \right\}
\]

\[
\times \sum_{L_c=1}^{L_t} p(L_c) \frac{\Gamma(L_c + \frac{2}{\alpha})}{\Gamma(L_c)}
\]

(13)

where \( T = 2R_t \).

2) Colluding Eavesdroppers: In this scenario, secrecy outage probability can be written by

\[
\mathcal{P}_{so}(\mu) = \mathbb{P}\left\{ \frac{a}{\mu} \sum_{\zeta_{e} \in \Phi_{e}} \mu_c r_{k}^{-a} > c r_{d}^{-a} - (T - 1) \right\} = \mathbb{P}\{I_e > \frac{a[\mu_c r_{k}^{-a} - (T - 1)]}{r_{d}^{-a}} \}, \quad \text{where} \quad I_e = \sum_{\zeta_{e} \in \Phi_{e}} \mu_c r_{k}^{-a}.
\]

We first calculate the Laplace transform of \( I_e \) by

\[
L_{I_e}(s) = \mathbb{E}_{\Phi_{e}, \mu_c} \left[ e^{-s \sum_{\zeta_{e} \in \Phi_{e}} \mu_c r_{k}^{-a}} \right]
\]

\[
= \mathbb{E}_{\Phi_{e}} \left[ \prod_{\zeta_{e} \in \Phi_{e}} \mathbb{E}_{\mu_c} \left[ \exp \left\{ -s \mu_c r_{k}^{-a} \right\} \right] \right] \]

\[
= \exp \left\{ -\lambda \sum_{L_c=1}^{L_t} 2\pi p(L_c) \right\}
\]

\[
= \exp \left\{ -\pi \lambda \sum_{L_c=1}^{L_t} p(L_c) \frac{2}{\alpha} \frac{\Gamma(1 + \frac{2}{\alpha})}{\Gamma(L_c)} \right\}
\]

\[
= \exp \left\{ -\pi \lambda \Gamma \left( \frac{2}{\alpha} + 1 \right) \left( \frac{\mu c}{\alpha} \right)^{-2/\alpha} \sum_{L_c=1}^{L_t} p(L_c) \frac{\Gamma(L_c + \frac{2}{\alpha})}{\Gamma(L_c)} \right\}
\]

(14)

where (b) holds for PGFL over PPP.
Fig. 3. SOP versus $R_s$ for different $N$’s, with $N_t=100$, $P=0$dBm, $r_d=50m$, $L_d=20$, $L_e=20$, $a=4$ and $\lambda=10^{-5}$.

After deriving $L_{L_e}(s)$, we can obtain the CDF of $I_e$ through inverse Laplace transform, and then get the SOP. However, inverse Laplace transform causes considerable calculation complexity and induces analysis intractable. Therefore, we provide an approximation of $P_{so}$ in the following theorem.

Theorem 1: The SOP in the scenario of colluding eavesdroppers for MRT beamforming can be approximated as

$$P_{so} \geq \sum_{n=0}^{N} \frac{(-1)^n L_{L_e}}{(\mu c \gamma_d^{-\alpha} - (T - 1))}, \quad (15)$$

where $L_{L_e}(s)$ is given by (14), $q \triangleq \frac{N(N+1)^{-1}}{N}$ and $N$ is defined as the number of terms used in approximation.

Proof: Defining $i$ as a normalized gamma random variable with the shape parameter $N$, we have

$$P_{so}(\mu) = \sum_{i=0}^{L_d} \frac{aT_i}{\mu c \gamma_d^{-\alpha} - (T - 1)} > 1$$

$$\geq \sum_{i=0}^{L_d} \frac{aT_i}{\mu c \gamma_d^{-\alpha} - (T - 1)} \geq \left[ 1 - \exp \left( -\frac{qaT_i}{\mu c \gamma_d^{-\alpha} - (T - 1)} \right) \right]^{N}, \quad (16)$$

where (c) holds for the fact that a normalized gamma random variable converges to identity when its shape parameter goes to infinity, and (d) follows the CDF bound of a normalized gamma random variable [10], [33]. By using binomial expansion, we obtain the tight lower bound of $P_{so}$ given in (15).

As shown in Fig. 3, $P_{so}$ given in Theorem 1 is more similar to the simulation results when $N$ becomes larger, and we get a good approximation when $N$ increases to 5. Thus we use $N = 5$ in the following numerical analysis. In addition, we find that $P_{so}$ increases when $R_s$ increases. The underlying reason is that when we set a higher $R_s$, the rate redundancy $R_e = R_t - R_s$ which is utilized to against the eavesdropping becomes lower and the secrecy outage requirement $C_e > R_e$ is easier to meet.

C. Secrecy Throughput Maximization

In this subsection, we maximize the secrecy throughput subject to a tolerable SOP constraint in the non-colluding eavesdroppers scenario. We first maximize $R_s(\mu)$ and formulate the optimization problem as

$$\max_{R_s(\mu)} \quad r_s(\mu),$$

$$\text{s.t.} \quad 0 < R_s(\mu) < R_t \leq C_d, \quad (17a)$$

$$P_{so}(\mu) \leq \epsilon, \quad (17b)$$

where $\epsilon \in [0, 1]$ is the SOP threshold. Following the definition formula of the SOP in (4), the SOP constraint can be rewritten as $P_{so}(\mu) = 1 - F_{\psi e}(2R_t/R_s - 1) \leq \epsilon$. Since $F_{\psi e}(x)$ is a monotonically increasing function, we obtain $R_s \leq R_t - \log(1 + F_{\psi e}^{-1}(1-\epsilon))$, where $F_{\psi e}^{-1}(\cdot)$ denotes the inverse function of $F_{\psi e}(\cdot)$. As $R_s$ should not exceed $C_d$, we set $R_t$ equal to $C_d$ to achieve a maximum $R_s$, which is

$$R_s^*(\mu) = (C_d - \log(1 + F_{\psi e}^{-1}(1-\epsilon)))^+.$$

From (12), by denoting $\rho \triangleq F_{\psi e}^{-1}(1-\epsilon)$, we have $\rho = \frac{a\mu}{\rho}$ with $\sigma\triangleq \left[ -\frac{\pi \Gamma(\frac{3}{2})}{\ln(1-\rho)} \sum_{L_i=1}^{L_\iota} p(L_i) \Gamma(L_i+\frac{3}{2}) \right]^{\frac{1}{2}}$. In addition, in order to obtain a positive $R_s^*$, $C_d > \log(1+\rho)$ should be satisfied. Since $C_d = \log(1+c\mu\gamma_d^{-\alpha})$, the maximum $R_s(\mu)$ of MRT beamforming can be given by

$$R_s^*(\mu) = \log \left( 1 + c \mu \gamma_d^{-\alpha} \right), \quad (19)$$

with the transmission constraint $\mu > \delta = \sqrt{\frac{\lambda_1}{\lambda_2}}$, where $\lambda_1 \triangleq \sigma \alpha = \rho \mu$, and $\delta$ is the transmission threshold. According to the on-off transmission scheme, the transmitter radiates signals with $R_s(\mu)$ only when $\mu > \delta$; otherwise, the transmitter keeps silence and we set $R_s(\mu) = 0$. After obtaining $R_s^*(\mu)$, we calculate the maximum secrecy throughput according to (5).

Theorem 2: The maximum secrecy throughput of MRT beamforming can be given by

$$\tau^* = \sum_{m=0}^{L_d-1} e^{-\frac{\delta L_d - 1 - m}{\Gamma(L_d - m)}} \left[ V \left( \frac{1}{\delta} \right) + V \left( \frac{c \mu \gamma_d^{-\alpha}}{1 + c \mu \gamma_d^{-\alpha}} \right) \right] - V \left( \frac{1}{\delta + \lambda_1} \right) + \log \left( \frac{\delta(1 + c \mu \gamma_d^{-\alpha})}{\delta + \lambda_1} \right), \quad (20)$$

where $V(x) = \frac{1}{\ln 2} \sum_{m=1}^{n} \frac{(-1)^{m-1}}{(m - 1)! \gamma_n} \left( 1 + \frac{1}{x} \right)^{m-1} Ei \left( -\frac{1}{x} \right) + \sum_{k=1}^{n} (k - 1)! (\frac{1}{x})^{n-k}$. Proof: Please see Appendix A.

Corollary 1: $\tau^*$ monotonically decreases with $r_d$ and $\lambda$, while monotonically increases with $\epsilon$.

Proof: From $\tau^* = \int_{\delta}^{\infty} R_s^*(x) f_\mu(x) dx = \int_{\delta}^{\infty} \log \left( 1 + c \mu \gamma_d^{-\alpha} \right) f_\mu(x) dx$, we have $\frac{\partial \tau^*}{\partial \epsilon} < 0$, $\frac{\partial \tau^*}{\partial c \mu} < 0$, and $\frac{\partial \tau^*}{\partial \gamma_d} < 0$, hence we derive $\frac{\partial \tau^*}{\partial \gamma_d} = \frac{\partial \tau^*}{\partial \delta} \frac{\partial \delta}{\partial \gamma_d} + \frac{\partial \tau^*}{\partial \epsilon} \frac{\partial \epsilon}{\partial \gamma_d} < 0$. Therefore, we obtain $\frac{d \tau^*}{d \gamma_d} = \frac{d \tau^*}{d \delta} \frac{d \delta}{d \gamma_d} + \frac{d \tau^*}{d \epsilon} \frac{d \epsilon}{d \gamma_d} > 0$ and $\frac{d \tau^*}{d r_d} = \frac{d \tau^*}{d \delta} \frac{d \delta}{d r_d} + \frac{d \tau^*}{d \epsilon} \frac{d \epsilon}{d r_d} < 0$.

Corollary 1 implies that MRT beamforming achieves higher secrecy throughput in a sparser eavesdroppers scenario, under
a more moderate SOP constraint, or when the distance between the destination and the transmitter is smaller.

Corollary 2: At the high transmit power regime, i.e., $P \to \infty$, the maximum secrecy throughput of MRT beamforming is given in (21), and is independent of $P$.

$$\tau^* = \frac{L_d - 1}{\Gamma(L_d - m)} V \left( \frac{1}{\delta} \right). \quad (21)$$

Proof: When $P \to \infty$, we have $a \to \infty$ and $c \to \infty$. Following (19), $\lim_{P \to \infty} R^s_\mu(\mu) = \log \frac{c^2 \left( \frac{r_\mu a^2}{\eta} \right)}{\omega_{av}} = \log \frac{\mu^2}{\Gamma_d \omega_{av}}$. By exploiting the same integration method as Theorem 2, we derive the result given in (21). Since $\delta = \sqrt{\frac{\sigma_0 \Delta_{av}}{\lambda_{av}}}$ is independent of $P$, we have that $\tau^*$ is independent of $P$ when $P \to \infty$.

V. SECRECY PERFORMANCE OF AN BEAMFORMING

In this section, we first investigate the connection and secrecy outage performance of AN beamforming. Then we maximize the secrecy throughput under a given SOP constraint and derive the optimal power allocation ratio $\eta^*$.

A. Connection Probability

Given $\xi_{AN} = \eta_c \mu^2 r_d^2$, from (10), the connection probability of AN beamforming can be given by

$$P_c = \frac{1}{\Gamma(L_d)} \left( L_d, \frac{2L_t - 1}{\eta c} \right). \quad (22)$$

B. Secrecy Outage Performance

1) Non-Colluding Eavesdroppers: Define $\nu \triangleq \|\mathbf{g}_{se}\|^2$, we have $\nu \sim \text{Gamma}(L_c - L_e, 1)$. Since $\Omega_c \cap \Omega_m = \emptyset$, $u$ and $v$ are independent to each other. The CDF of $\xi_{AN}$ can be given by

$$F_{\xi_e}(x) = 1 - \mathbb{E}_u \left[ e^{-\frac{(1-\eta)\mu x}{\eta \mu_c(N_t - L_d)}} \right] - (L_e - L_c), \quad (25)$$

where $e$ holds for the integration formula [40, 326.2]. The CDF of $\xi_{AN}$ can be calculated as

$$F_{\xi_e}(x) = \mathbb{E}_{\Phi_c, (\mu_c)} \left[ \prod_{\xi \in \Phi_c} P[\xi < x] \right]$$

$$= \exp \left\{ -\lambda \int_0^\infty \int_0^{2\pi} \mathbb{E}_{\mu_c} \left[ \left( 1 + \frac{(1-\eta)\mu x}{\eta \mu_c(N_t - L_d)} \right)^{-L_e - L_c} \right] \right\}$$

$$\times \int \left( \frac{\mu x}{\eta \mu_c(N_t - L_d)} \right)^{-\frac{\alpha}{\alpha} - 1} \text{d}x \text{d}\theta \text{d}r_k$$

$$= \exp \left\{ -\lambda \int_0^\infty \int_0^{2\pi} \mathbb{E}_{\mu_c} \left[ \left( 1 + \frac{(1-\eta)\mu x}{\eta \mu_c(N_t - L_d)} \right)^{-L_e - L_c} \right] \right\}$$

$$\times \int \left( \frac{\mu x}{\eta \mu_c(N_t - L_d)} \right)^{-\frac{\alpha}{\alpha} - 1} \text{d}x \text{d}\theta \text{d}r_k$$

$$\times \mathbb{E}_{\mu_c} \left[ \left( 1 + \frac{(1-\eta)\mu x}{\eta \mu_c(N_t - L_d)} \right)^{-L_e - L_c} \left( \frac{1}{\mu_c} \right)^{-\frac{\alpha}{\alpha}} \right], \quad (24)$$

Denoting $b \triangleq \frac{(1-\eta)\mu x}{\eta(N_t - L_d)}$, yields

$$F_{\xi_e}(x) = \exp \left\{ -\lambda \Gamma \left( 2 - 1 + \frac{\mu x}{\eta \mu_c(N_t - L_d)} \right)^{-\frac{\alpha}{\alpha} - 1} \sum_{L_e = 1}^{L_t} p(L_e) \right\}$$

$$\times \int_0^{\infty} \left( \mu \mu_c + b \right)^{-L_e - L_c} \mu_c \frac{L_e - L_c + \alpha}{L_c} \left( \frac{1}{\mu_c} \right)^{-\frac{\alpha}{\alpha}} \text{d}t_c$$

$$\times \int_0^{\infty} y^{-L_e - L_c} (y - b)^{\frac{\alpha}{\alpha} + 1} e^{-y} \text{d}y,$$
expression for droppers, the SOP of AN beamforming can be approximated through the non-colluding eavesdroppers scenario. Power Allocation

\[ F_{\text{AN}}^{(\eta)}(\eta) = \frac{P}{\eta c_\mu r_d^{-\alpha}} \approx \frac{P}{\eta c_\mu r_d^{-\alpha}} \]

rewriting the definition formula of \( \eta \) versus \( \pi / \Gamma(\eta) \)
\[ \eta = 0.3, 0.5, 0.7 \]

Lemma 2: The Laplace transform of \( I_e \) can be given by
\[ L_e(s) = \exp \left[ -\frac{\pi \lambda \Gamma(1+2\alpha)}{\Gamma(1-2\alpha) \Gamma(\leq 2-\alpha)} z_3^{2-\alpha-1} \right] \]
\[ \times \sum_{L_e=1}^{L_l} p(L_e) L_e F \left( L_e+1, 2\alpha+1; L_e+\frac{3}{2}; -\frac{s z_2}{z_3} \right) \]

Proof: Please see Appendix B.

Following Theorem 1, in the scenario of colluding eavesdroppers, the SOP of AN beamforming can be approximated as
\[ \mathcal{P}_{\text{so}} \approx \sum_{n=0}^{N} \left( \frac{N-n}{n} \right) (-1)^n L_e \left( \frac{q T_n}{\eta c_\mu r_d^{-\alpha}} \right) \]

C. Secrecy Throughput Maximization and Optimal Power Allocation

In this subsection, we optimize \( \eta \) to get a maximum secrecy throughput under the SOP constraint for the AN scheme in the non-colluding eavesdroppers scenario.

According to (18) and by denoting \( \rho(\eta) = \frac{F_{\text{so}}^{-1}(1-\epsilon)}{\eta} \) for the AN scheme, the optimization problem can be formulated as
\[ \max_{\eta} \mathcal{R}_0(\mu) = \log \frac{1 + \eta c_\mu r_d^{-\alpha}}{1 + \eta p(\eta)} , \]
\[ s.t. 0 \leq \eta \leq 1, \ \rho(\eta) < c_\mu r_d^{-\alpha} \]

Lemma 3: \( \rho(\eta) \) is a monotonically increasing and convex function of \( \eta \) in the range \( \eta \in [0, 1] \).

Proof: Please see Appendix C.

From the definition of \( \rho \), we easily obtain that \( \rho \geq 0 \). Due to Lemma 3, the maximum \( \rho \) is achieved at \( \eta = 1 \). Then we can obtain \( \rho_{\text{max}} = (\sum_{l=1}^{L} I_{l} z_4^{-\alpha}) \]
from \( J(\rho) - Q = 0 \). We define \( \Xi(\rho) = J(\rho)^{-1} - Q^{-1} \). Evidently, for an given \( \Xi(\rho) \), \( \rho(\eta) \) is a monotonically increasing function of \( \rho \). Since \( \Xi(0) = -Q^{-1} < 0 \) and \( \rho(\text{max}) = (\sum_{l=1}^{L} I_{l} z_4^{-\alpha}) \]
\( \Xi(\rho) \) has the unique zero-crossing point. Therefore, we can obtain the unique root \( \rho \) of \( \Xi(\rho) = 0 \) by utilizing the bisection method within the range \( [0, \rho_{\text{max}}] \).

Theorem 3: Given \( \rho < c_\mu r_d^{-\alpha} \), \( R_s \) is a concave function of \( \eta \). The optimal \( \eta^* \) that maximizes \( R_s \) is given by
\[ \eta^* = \begin{cases} 1, & \frac{\rho}{c_\mu r_d^{-\alpha}} + \rho_{\text{max}} + \frac{\alpha \mu}{1 + \rho_{\text{max}}} \rho_{\text{max}}^2 > 0, \\ \eta^*, & \text{otherwise,} \end{cases} \]

where \( \eta^* \) is the unique root of the following equation
\[ \frac{d R_s}{d \eta} = \frac{1}{\ln 2} \left( \frac{c_\mu r_d^{-\alpha}}{1 + \eta c_\mu r_d^{-\alpha}} - \frac{\rho + \eta \eta d}{\eta_{d}} \right) = 0, \]

with \( \eta_{d} \) defined in (36).

Proof: Please see Appendix D.

The above theorem provides the solution of the optimization problem (30), and supplies an efficient approach, i.e., the bisection method, that can be used to search the optimal \( \eta^* \), due to the concavity of \( R_s \) on \( \eta \). Then we investigate how the optimal power allocation ratio \( \eta^* \) varies in different scenarios in the following corollary.

Corollary 3: The optimal \( \eta^* \) monotonically decreases with \( \lambda \) and \( r_d \), and monotonically increases with \( \epsilon \).

Proof: Please see Appendix E.

Corollary 3 indicates that when the transmission is more vulnerable to eavesdropping, i.e., with a poorer quality of the destination’s channel, in a denser eavesdroppers scenario or under a more rigorous SOP constraint, we should allocate more power to AN.

Next, we calculate the transmission threshold \( \delta \). We have already derived the transmission constraint \( \rho(\eta) < c_\mu r_d^{-\alpha} \) to guarantee a positive \( R_s \). Since \( \rho(\eta) \) monotonically increases with \( \eta \), if \( \rho(0) \), the minimum \( \rho(\eta) \), is not below \( c_\mu r_d^{-\alpha} \), i.e., \( \rho(0) \geq c_\mu r_d^{-\alpha} \Rightarrow \mu < \frac{c_\mu r_d^{-\alpha}}{\rho(0)} \), the transmission constraint \( \rho(\eta) < c_\mu r_d^{-\alpha} \) cannot be satisfied. Hence we can not find a feasible \( \eta \) to maintain the positivity of \( R_s \). Therefore,
As shown in the figure, \( \mu > \rho_0 \) must be guaranteed, and as a consequence we set \( \delta = \frac{\rho_0}{\epsilon} \), which corresponds to an on-off transmission, i.e., when \( \mu > \delta \), the transmitter radiates signals with \( R_x^*(\mu) \); otherwise, the transmission suspends and we set \( R_x^*(\mu) = 0 \).

From (5), the maximum secrecy throughput of AN beamforming can be given by

\[
\tau^* = \int_{\rho_0}^{\infty} R_x^*(\mu) f_\mu(x)dx,
\]

where \( f_\mu(x) = \frac{(\rho_0 - 1)}{\Gamma(L_d)} e^{-x} \).

VI. NUMERICAL RESULTS

In this section, numerical results are presented to verify our theoretical analysis. The transmitter is equipped with a ULA containing 100 antennas. We set the pass loss exponent \( \alpha = 4 \) and the noise power \( \sigma_n^2 = -60 \text{dBm} \) [30], [33], [35].

A. Connection and Secrecy Outage Performance

Fig. 5 describes connection probability versus \( L_d \) for different values of \( r_d \). We find that when \( r_d \) is small, connection probability increases as the number of resolvable paths \( L_d \) increases. The trend is opposite when \( r_d \) is large. The underlying reason is that when the number of paths becomes larger, the influence of paths with either very high or very low gain becomes weaker, i.e., the received power is closer to its mean and the randomness is smaller. When \( r_d \) is small, the mean of SNR is high. Therefore, with the increase of \( L_d \), SNR is closer to its higher mean and the connection probability will increase. Otherwise, when \( r_d \) is large, SNR approaches to its lower mean and the connection probability will decrease. We also observe that connection probability of AN beamforming is lower than that of MRT beamforming due to the fact that partial transmit power is allocated to the AN transmission.

Fig. 6 presents \( P_\text{sop} \) versus \( L_d \) for different values of \( \lambda \). As shown in the figure, \( P_\text{sop} \) is higher in colluding eavesdroppers scenario than that in non-colluding eavesdroppers scenario. The differences are more obvious when eavesdroppers are denser. For both AN beamforming and MRT beamforming, \( P_\text{sop} \) decreases when \( L_d \) reduces. The underlying reason is that when \( L_d \) becomes larger, more paths are resolvable and \( \lambda \) increases, the transmit beam of the information signal covers more spatially resolvable directions, so that eavesdroppers’ resolvable paths are more likely to fall into that beam, which means that eavesdroppers will receive more information signals. Thus we should give a larger fraction of transmit power to AN transmission in order to interfere with eavesdroppers.

B. Optimal Power Allocation of AN Beamforming

Fig. 7 investigates the optimal power allocation ratio \( \eta^* \) versus \( L_d \) for different values of \( r_d \). We find that \( \eta^* \) increases with the decrease of \( r_d \). The figure also shows that for a given \( L_d = 20 \), when \( L_d \) varies from 10 to 30, \( \eta^* \) is getting smaller. It is because that when \( L_d \) becomes larger, the transmit beam of the information signals covers more spatially resolvable directions, so that eavesdroppers’ resolvable paths are more likely to fall into that beam, which means that eavesdroppers will receive more information signals. Thus we should give a larger fraction of transmit power to AN transmission in order to interfere with eavesdroppers.

Fig. 8 plots the optimal power allocation ratio \( \eta^* \) that maximizes the secrecy throughput versus \( L_d \) for different values of \( L_e \). As shown in the figure, \( \eta^* \) decreases as \( L_e \) increases, which implies that we should increase AN power when secure transmissions become more vulnerable to intercepting. In addition, the value of \( \eta^* \) falls down with an increase in \( L_e \). The underlying reason is that when \( L_e \) becomes larger, more resolvable
paths of eavesdroppers and those of the destination are more likely to overlap, and then eavesdroppers are able to wiretap more confidential messages. Therefore, more power is ought to be allocated to AN transmission in order to deteriorate eavesdroppers’ channels.

Fig. 9 illustrates the optimal power allocation ratio $\eta^*$ that maximizes the secrecy throughput versus $P$ for different values of $\epsilon$. $\eta^*$ keeps 1 at the low transmit power region and then drops as $P$ increases, which implies that we should transmit information signals with full power to achieve a higher message rate at the low power regime and give a larger fraction of power to AN transmission when the transmit power becomes higher. We also find that for a given transmit power $P$, as $\epsilon$ decreases, $\eta^*$ decreases.

C. Secrecy Throughput Performance

Fig. 10 describes the secrecy throughput versus $L_d$ for different values of $r_d$. Secrecy throughput becomes higher with the decrease of $r_d$, which confirms the fact that a better destination’s channel contributes to a promotion of secrecy throughput. We also find that the secrecy throughput increases as $L_d$ decreases. The underlying reason is that confidential signals are radiated through all the directions of the destination’s resolvable paths. In the small $L_d$ scenario, the transmit beam which contains secrecy messages is narrow. It is hard for eavesdroppers to intercept. Therefore, smaller $L_d$ is beneficial for enhancing the secrecy throughput.

Fig. 11 presents the secrecy throughput versus $L_e$ for different values of $\lambda$. We observe that the secrecy throughput increases with a smaller $\lambda$ for both transmission schemes, which indicates that secrecy performance improves in a sparse eavesdropper scenario. As the number of the eavesdropper’s resolvable paths $L_e$ changes, the variation tendencies of MRT beamforming and AN beamforming are different. For MRT beamforming, the secrecy throughput turns to be lower as $L_e$ increases. It is because that in the large $L_e$ situation, eavesdroppers’ resolvable paths are more likely to cover the destination’s resolvable paths in which directions the information signals emit. Thus eavesdroppers overhear more secrecy messages and the secrecy performance will be poorer. Although a heavier leakage to eavesdroppers also happens in the AN beamforming case when $L_e$ grows, the transmitter gives more power to AN transmission as shown in Fig. 8, so that the interference received by eavesdroppers increases too. With the transmission of AN, the SINR of eavesdroppers may drop. Therefore, the results in the figure show that the secrecy throughput increases when $L_e$ increases for the AN scheme. In addition, we observe that the gap between the secrecy throughput of AN beamforming and that of MRT beamforming is more evident in the denser eavesdropper scenario.
Fig. 12. Secrecy throughput versus $P$ for different $\epsilon$’s, with $N_t = 100$, $P = 10\text{dBm}$, $L_d = 20$, $L_e = 20$, $r_d = 50\text{m}$ and $\lambda = 5 \times 10^{-6}$.

Fig. 12 describes the secrecy throughput versus $P$ for different values of $\epsilon$. Obviously, by increasing transmit power $P$, the secrecy throughput increases. We also see that MRT beamforming presents a comparable performance to AN beamforming in the low transmit power scenario. As revealed in Corollary 2, the secrecy throughput of MRT beamforming at the high transmit power regime converges to a constant which is irrespective to $P$. However, since more power is allocated to the AN transmission to confuse eavesdroppers as shown in Fig. 9, the secrecy throughput of AN beamforming keeps increasing, and the superiority of AN beamforming becomes more obvious. Meanwhile, as the increase of the SOP constraint threshold $\epsilon$, the secrecy throughput becomes higher.

VII. CONCLUSION

This paper has comprehensively studied secure transmissions in mm-wave systems where the locations of eavesdroppers are modeled as an independent homogeneous PPP. We have established a discrete angular domain channel model which characterized by spatially resolvable paths to facilitate the theoretical design and analysis of secure transmission schemes. Then we have evaluated the performance of MRT beamforming and AN beamforming by obtaining the connection probability, the SOP and the secrecy throughput. Particularly, we have derived the optimal power allocation between AN and the information signal that maximizes the secrecy throughput for AN beamforming. Through our analysis, we have revealed that the superiority of AN beamforming over MRT beamforming is highly significant in dense eavesdroppers scenario, at the high transmit power regime or in the situation that the number of the eavesdropper’s spatially resolvable paths is large.

APPENDIX A

PROOF OF THEOREM 2

Since $\mu \sim \text{Gamma}(L_d, 1)$, the PDF of $\mu$ can be given by $f_\mu(x) = \frac{\mu x^{L_d-1}}{\Gamma(L_d)} e^{-x}$. By substituting (19), we derive the maximum secrecy throughput of MRT beamforming as

\[
\tau^* = \int_0^\infty R^*_s(x) f_\mu(x) dx
\]

where (h) holds for the transformation $y = x - \delta$. According to [40, 4.337.5], the final result shown in (20) is obtained.

APPENDIX B

PROOF OF LEMMA 2

\[
\mathcal{L}_I(s) = \mathbb{E}_{\Phi_c, \mu, v, \mu_c} \left[ e^{-s \sum_{k \in \Phi_c} z_2 \mu_c} \right]
\]

\[
= \exp \left\{ -2\pi \lambda \sum_{L_e=1}^{L_i} p(L_c) \times \mathbb{E}_{\mu, v, \mu_c} \left[ \int_0^\infty \left[ 1 - \exp \left( -s \frac{z_2 \mu_c}{z_3} v + r_k^c \right) \right] r_k dr_k \right] \right\}
\]

\[
= \exp \left\{ -2\pi \lambda \sum_{L_e=1}^{L_i} p(L_c) \int_0^\infty \int_0^\infty \int_0^\infty s z_2 \mu_c \times (r_k^c + s z_2 \mu_c + z_3 v)^{-1} r_k dr_k f(v) f(\mu_c) d\mu_c \right\}
\]

where $f(u) = e^{-u}$, $f(v) = \frac{1}{(\lambda(L_e+1))} e^{-\alpha}$ and $f(\mu_c) = \frac{1}{\Gamma(L_d)} e^{-\mu_c}$ are PDFs of $u$, $v$ and $\mu_c$ respectively, (i) holds for the transformation $x = r^c_k$ and the integration formula [40, 3.194], (j) holds for the transformation $y = z_3 v + s z_2 \mu_c$ and the integration formula [40, 3.383.4]. By utilizing the integration formula [40, 7.621.3], we obtain the result in (28).
APPENDIX C

PROOF OF LEMMA 3

The first-order and second-order derivatives of $\rho(\eta)$ can be given by

$$\frac{d\rho}{d\eta} = \frac{\partial J / \partial \eta}{\partial J / \partial \rho} = \frac{\rho^2}{\rho(1-\eta) + \frac{\sigma}{\alpha}}$$

(36)

$$\frac{d^2\rho}{d\eta^2} = \frac{2}{\rho} \left( \frac{d\rho}{d\eta} \right)^2 + \frac{\rho^2 [\zeta - \frac{2d_0}{d\eta}] + \rho [\rho(1-\eta) + \frac{\sigma}{\alpha}]^2}{[\rho(1-\eta) + \frac{\sigma}{\alpha}]^3},$$

(37)

where $\sigma \equiv \frac{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - \sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}$, and $\zeta \equiv \rho - (1-\eta) \frac{d_0}{d\eta}$. Since $\sigma > 0$, obviously $\frac{d\rho}{d\eta} > 0$. By substituting (36), we have $\zeta = \frac{2d_0}{d\eta} > 0$. Denoting $C_1 \equiv \frac{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}$ and $C_2 \equiv \frac{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}$, we have

$$\frac{d\sigma}{d\eta} = \frac{dC_2}{d\eta} = \frac{dC_1}{d\eta}$$

where $C_1 \equiv \frac{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}$ and $C_2 \equiv \frac{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}{\sum_{\ell=1}^{L_1} z_4 [1+z_5(1-\eta)\rho]^{-(L_e-L_c)} - 1}$.

APPENDIX D

PROOF OF THEOREM 3

The second-order derivative of $R_\alpha$ can be described as

$$\frac{d^2 R_\alpha}{d\eta^2} = -\frac{1}{\ln 2} \left\{ \left( \frac{c_\mu \rho^{\alpha-2}}{1+c_\mu \rho^{\alpha-2}} \right)^2 + \frac{1}{(1+\eta \rho)^2} \times \left[ (1+\eta \rho) \left( \frac{d\rho}{d\eta} + \eta \frac{d^2\rho}{d\eta^2} \right) - \rho + \eta \frac{d\rho}{d\eta} \right] ^2 \right\}$$

(39)

with $\frac{d\rho}{d\eta}$ and $\frac{d^2\rho}{d\eta^2}$ given by (36) and (37). Substituting $\frac{d^2\rho}{d\eta^2} < \frac{2}{\rho} \left( \frac{d\rho}{d\eta} \right)^2 > 0$ (see Appendix C) into the above equation yields

$$\frac{d^2 R_\alpha}{d\eta^2} < -\frac{1}{\ln 2} \left[ \left( \frac{c_\mu \rho^{\alpha-2}}{1+c_\mu \rho^{\alpha-2}} \right)^2 - \frac{\rho^2}{1+\eta \rho} \right].$$

Since $c_\mu \rho^{\alpha-2} > \rho$, we have $d^2 R_\alpha < 0$, i.e., $R_\alpha$ is a concave function of $\eta$.

For the concavity of $R_\alpha$, the maximum value of $R_\alpha$ is achieved either at the boundaries or at the zero-crossing point of $\frac{dR_\alpha}{d\eta}$. From the first-order derivative formula of $R_\alpha$ in (32), we obtain $\frac{dR_\alpha}{d\eta} |_{\eta=0} = \frac{1}{\ln 2} \left( c_\mu \rho^{\alpha-2} - \rho \right) > 0$, and $\frac{dR_\alpha}{d\eta} |_{\eta=1} = \frac{1}{\ln 2} \left[ \frac{c_\mu \rho^{\alpha-2} - \rho \max}{1+c_\mu \rho^{\alpha-2} - \rho \max} \right] > 0$. If $\frac{dR_\alpha}{d\eta} |_{\eta=1} > 0$, $R_\alpha$ monotonically increases with $\eta$, and the optimal value of $\eta$ is 1 with the condition directly obtained from $\frac{dR_\alpha}{d\eta} |_{\eta=1} > 0$. If $\frac{dR_\alpha}{d\eta} |_{\eta=1} \leq 0$, $R_\alpha$ first increases and then decreases, and the optimal value of $\eta$ is the unique root of $\frac{dR_\alpha}{d\eta}$.

REFERENCES

[1] 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.

[2] 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.

[3] J. Brady, N. Behzad, and A. M. Sayeed, “Beamspace MIMO for millimeter-wave communications: System architecture, modeling, analysis, and measurements,” IEEE Trans. Antennas Propag., vol. 61, no. 7, pp. 3814–3827, Jul. 2013.

[4] M. R. Akdeniz et al., “Millimeter wave channel modeling and cellular capacity evaluation,” IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1164–1179, Jun. 2014.

[5] A. Adhikary et al., “Joint spatial division and multiplexing for mm-Wave channels,” IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1239–1255, Jun. 2014.

[6] 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.

[7] Y.-Y. Lee, C.-H. Wang, and Y.-H. Huang, “A hybrid RF/baseband precoding processor based on parallel-index-selection matrix-inversion-bypass simultaneous orthogonal matching pursuit for millimeter wave MIMO systems,” IEEE Trans. Signal Process., vol. 63, no. 2, pp. 305–317, Jan. 2015.
[8] A. Alkhateeb, O. El Ayach, G. Leus, and R. W. Heath, Jr., “Channel estimation and hybrid precoding for millimeter wave cellular systems,” *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 831–846, Oct. 2014.

[9] S. Hur, T. Kim, D. J. Love, J. V. Krogmeier, T. A. Thomas, and A. Ghosh, “Millimeter wave beamforming for wireless backhaul and access in small cell networks,” *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4391–4403, Oct. 2013.

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

[11] 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.

[12] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1375, 1975.

[13] 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.

[14] H.-M. Wang and X.-G. Xia, “Enhancing wireless secrecy via cooperation: Signal design and optimization,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 57–63, Dec. 2015.

[15] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The MISOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[16] H.-M. Wang, T. Zheng, and X.-G. Xia, “Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[17] S. Bashar, Z. Ding, and G. Y. Li, “On secrecy of codebook-based transmission beamforming under receiver limited feedback,” *IEEE Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[18] H.-M. Wang, C. Wang, D. W. K. Ng, M. H. Lee, and J. Xiao, “Artificial noise assisted secure transmission for distributed antenna systems,” *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.

[19] Y. Zhu, L. Wang, K. P. Wong, and R. W. Heath, Jr., “Secure communications in millimeter wave ad hoc networks,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[20] C. Rusu, N. González-Prelcic, and R. W. Heath, Jr., “An attack on antenna subset modulation for millimeter wave communication,” in *Proc. IEEE ICASSP*, Brisbane, QLD, Australia, Apr. 2015, pp. 2914–2918.

[21] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[22] A. M. Sayeed, “Deconstructing multiantenna fading channels,” *IEEE Trans. Signal Process.*, vol. 50, no. 10, pp. 2563–2579, Oct. 2002.

[23] A. Ghosh et al., “Millimeter-wave enhanced local area systems: A high-data-rate approach for future wireless networks,” *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1152–1163, Jun. 2014.

[24] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, D. Zwillinger, and S. Technica, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[25] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

**Ying Ju** received the B.S. and M.S. degrees from the School of Electronic Information Engineering, Tianjin University, Tianjin, China, in 2008 and 2010, respectively. She is currently pursuing the Ph.D. degree with the School of Electronic Information Engineering, Xi’an Jiaotong University, Xi’an, China. She is also an Engineer with the State Radio Monitoring Center, Department of Shaanxi Monitoring Station, Xi’an, China. From 2016 to 2017, she was a Visiting Scholar with the Department of Computer Science, University of California, Santa Barbara, CA, USA. Her research interests include physical layer security of wireless communications, millimeter wave communication systems, and stochastic geometry.

**Hui-Ming Wang** (S’07–M’10–SM’16) received the B.S. and Ph.D. degrees (Hons.) in electrical engineering from Xi’an Jiaotong University, Xi’an, China, in 2004 and 2010, respectively. From 2007 to 2010, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Delaware, DE, USA. He is currently a Full Professor with the Department of Information and Communications Engineering, Xi’an Jiaotong University, and also with the Ministry of Education Key Laboratory for Intelligent Networks and Network Security, China. His research interests include cooperative communication systems, physical-layer security of wireless communications, MIMO, and space–time coding. He has co-authored the book *Physical Layer Security in Random Cellular Networks* (Springer, 2016), and has authored or co-authored over 100 IEEE journal and conference papers. Ten of his papers are ESI Highly Cited Papers. He received the National Excellent Doctoral Dissertation Award in China in 2012, the Best Paper Award from the International Conference on Wireless Communications and Signal Processing in 2011, and the Best Paper Award from the IEEE/CIC International Conference on Communications in China in 2014. He has served as a TPC member of the various IEEE sponsored conferences, including the IEEE GLOBECOM, ICC, WCNC, VTC, and PIMRC. He also served as the Symposium Chair of the Wireless Communications and Networking in CHINACOM 2015 and a Technical Program Committee Member for the Workshop on Physical Layer Security in the IEEE GLOBECOM 2016. He is currently an Associate Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE ACCESS.
Tong-Xing Zheng (S’14–M’16) received the B.S. and Ph.D. degrees from the School of Electronic and Information Engineering, Xi’an Jiaotong University, Xi’an, China, in 2010 and 2016, respectively. He is currently a Lecturer with the Department of Information and Communications Engineering, Xi’an Jiaotong University, and also with the Ministry of Education Key Laboratory for Intelligent Networks and Network Security, China. He is also a Visiting Scholar at the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia.

He has co-authored the book *Physical Layer Security in Random Cellular Networks* (Springer, 2016). His current research interests include physical-layer security of wireless communications, wireless caching, heterogeneous cellular networks, full-duplex communications, and stochastic geometry theory and its applications.

Qinye Yin received the B.S., M.S., and Ph.D. degrees in communication and electronic systems from Xi’an Jiaotong University, Xi’an, China, in 1982, 1985, and 1989, respectively. He is currently a Professor with the Information Engineering Institute, Xi’an Jiaotong University. His research interests focus on the joint time-frequency analysis and synthesis, the theory and applications of wireless sensor networks, multiple antenna MIMO broadband communication systems (including smart antenna systems), parameter estimation, and array signal processing.

Moon Ho Lee (S’81–M’85–SM’86–LSM’15) received the Ph.D. degree in electrical engineering from Chonnam National University, South Korea, in 1984, and The University of Tokyo, Japan, in 1990. He held a post-doctoral position with the University of Minnesota, MN, USA, from 1985 to 1986. He was a Chief Engineer with Namyang MBC Broadcasting from 1970 to 1980. He joined Chonbuk National University, South Korea, as a Professor. He is currently a Professor with and the former Chair of the Department of Electronics Engineering, Chonbuk National University. He has made significant original contributions in the areas of mobile communication code design, channel coding, and multi-dimensional source and channel coding. He holds 116 Patents. He is also a member of the National Academy of Engineering, South Korea, and a Foreign Fellow of the Bulgaria Academy of Sciences. He was the inventor of Jacket Matrix and was cited over 95,559 times, in 2014, in Wikipedia.