



Article

Secure Transmission in mmWave Wiretap Channels: On Sector Guard Zone and Blockages

Yi Song ^{1,2} , Weiwei Yang ^{1,*}, Zhongwu Xiang ¹ , Yiliang Liu ³ and Yueming Cai ¹

¹ College of Communications Engineering, Army Engineering University of PLA, No. 88 Houbiaoying, Qinhuai District, Nanjing 210007, China; sy@hytc.edu.cn (Y.S.); xzwnoon@live.com (Z.X.); caiym@vip.sina.com (Y.C.)

² School of Physics and Electronic Electrical Engineering, Huaiyin Normal University, Huai'an 223300, China

³ Communications Research Center, Harbin Institute of Technology, Harbin 150001, China; alanliuyiliang@gmail.com

* Correspondence: wwyang1981@163.com; Tel.: +86-025-8082-9409

Received: 2 January 2019; Accepted: 17 April 2019; Published: 22 April 2019



Abstract: Millimeter-wave (mmWave) communication is one of the key enabling technologies for fifth generation (5G) mobile networks. In this paper, we study the problem of secure communication in a mmWave wiretap network, where directional beamforming and link blockages are taken into account. For the secure transmission in the presence of spatially random eavesdroppers, an adaptive transmission scheme is adopted, for which sector secrecy guard zone and artificial noise (AN) are employed to enhance secrecy performance. When there exists no eavesdroppers within the sector secrecy guard zone, the transmitter only transmits information-bearing signal, and, conversely, AN along with information-bearing signal are transmitted. The closed-form expressions for secrecy outage probability (SOP), connection outage probability (COP) and secrecy throughput are derived under stochastic geometry. Then, we evaluate the effect of the sector secrecy guard zone and AN on the secrecy performance. Our results reveal that the application of the sector secrecy guard zone and AN can significantly improve the security of the system, and blockages also can be utilized to improve secrecy performance. An easy choice of transmit power and power allocation factor is provided for achieving higher secrecy throughput. Furthermore, increasing the density of eavesdroppers not always deteriorates the secrecy performance due to the use of the sector secrecy guard zone and AN.

Keywords: physical layer security; millimeter wave; sector secrecy guard zone; artificial noise

1. Introduction

In recent years, data traffic increases significantly with the rapid popularization of various mobile intelligent devices and the growth of wireless data, and millimeter wave (mmWave) communication is an especially promising approach to meet the data traffic demand in the 5G and beyond wireless communication system because of the abundant available bandwidth of mmWave frequency [1,2]. There have been plenty of works presented in terms of achievable rate and coverage for mmWave communication system [3–5]. However, due to the wireless characteristic of electromagnetic wave and the openness of wireless channel, security remains a challenge to the design of mmWave systems. In this vein, there has been a heightened interest for safeguarding complex wireless networks by physical layer security (PLS).

The main idea of PLS is to make use of the normal randomness of wireless communication channel to guarantee that the confidential information is transferred to the legitimate receiver and that the confidential information will not be decoded by illegal users [6–10]. Reference [11] provided a detailed, transparent and accurate information on the latest developments in the use of collaborative techniques

to improve PLS. In addition, different cooperation technologies were classified, and their merits and demerits were discussed. It showed that the design of PLS schemes was still an important research field in 5G networks security. Recently, various technologies, like multiple-antenna, wiretap coding and signal processing technologies [12–14], especially guard zone and artificial noise (AN) [15,16], have become effective methods to enhance PLS. Using AN to enhance the reliability of legitimate links and interfere with eavesdropping links, so as to enlarge the gap between legitimate links and eavesdropping links to improve security. For different network applications, References [17,18] proposed the secrecy enhancement by using secrecy protected zone and AN, and discussed the relationship among protected zone, the transmission power and AN. In [19], the secrecy guard zone protocol was studied for achieving the secure transmission in an underlay cognitive radio network. However, all the aforementioned works on secrecy guard zone are only considered in the conventional microwave networks; they can not be directly applied and need to be re-evaluated in an mmWave system because of the unique characteristics of the mmWave communication system.

PLS in mmWave systems has attracted interest with enthusiasm [20–23]. The characteristics of mmWave communication system, such as larger bandwidth, large antenna arrays, directionality and short range transmission, could provide stronger PLS for mmWave system. Using analog beamforming in the mmWave base station, the secrecy throughput was analyzed from the perspectives of delay-tolerant and delay-limited transmissions in [24]. Considering the characteristics of mmWave cellular networks, Referecne [25] studied the secrecy performance of the noise-limited and the AN-assisted mmWave networks under the stochastic geometry framework. Referecne [26] examined the impact of AN on the secrecy rate; it was shown that power allocation between the information signal and AN need to be carefully determined for secrecy performance enhancement. A discrete angular domain channel model considering spatial discernibility path was proposed in [27], and three secure transmission schemes were investigated by depending on whether there was a common path between the destination and the eavesdropper. Although many insightful conclusions have been drawn in [25,27,28], the effects of blockages and the information leakage problem of the side lobe are not considered, but they are assumed to be ignored. In fact, blockages have different effects on communications in different environments, and side lobe may also lead to information leakage. On the other hand, directional beamforming is an important technique for mmWave systems because it provides array gains which overcome the huge path loss and acquire adequate link margins [4]. For mathematical tractability [29], when the simple maximum signal-to-noise ratio (SNR) beam steering is assumed, it is meaningful to approximate the actual array pattern with the sector pattern, where the directional gains of the main lobe and the side lobe are constant. The approximation of the sector mode makes it possible to describe the complex beamforming mode. Nevertheless, the locations of eavesdroppers in mmwave wiretap channels are randomly distributed, thus they may be located in signal beams and then could intercept confidential information. However, for a mmWave wiretap network, comprehensive secrecy performance analysis has not been provided under a sector secrecy guard zone, which motivates our work.

In this paper, we investigated secrecy performance under the Nakagami fading channel in a mmWave wiretap network. In order to improve the secrecy performance of mmWave wiretap network, a secrecy guard zone is introduced around the transmitter, in which eavesdroppers are not allowed to roam. It is assumed that the eavesdroppers can be detected, provided that they enter secrecy guard zone. Considering a more practical mmWave communication scenario, the effects of blockage are taken into account such that links are either line-of-sight (LOS) or non-line-of-sight (NLOS). In our prior conference paper [30], we discussed how to use sector guard zone in mmWave networks. Based on our previous work, assuming the transmitter is capable of detecting the existence of eavesdroppers in the finite guard zone, an adaptive transmission scheme is adopted for secrecy transmission. Our diversified contributions and insights are listed as follows:

- According to the characteristics of mmWave beam pattern, both the main lobe and side lobe are taken into consideration. Specifically, a sector secrecy guard zone model is considered

to achieve theoretical design and analysis. Depending on the locations of eavesdroppers detected by a transmitter, an adaptive transmission scheme is proposed which chooses two types of transmission strategies adaptively. The first-type is direct transmission when there exists no eavesdroppers in the sector secrecy guard zone and the second-type is the AN assisted transmission when one or more eavesdroppers in the sector secrecy guard zone.

- Stochastic geometry is adopted in proposed mmWave wiretap network to characterize the random spatial locations of eavesdroppers. The closed-form expressions of secrecy outage probability (SOP), connection outage probability (COP) and secrecy throughput are derived in the proposed scheme. In addition, we provide a further insight of the system parameters, i.e., transmit power, power allocation factor, secrecy guard zone radius and central angle, blockage density, antenna gain, and the intensity of the eavesdroppers into secrecy performance.
- The results show that enlarging the radius of sector secrecy guard zone improves secrecy performance. In addition, recruiting AN also enhances secrecy performance especially when the density of eavesdroppers is dense. In addition, blockage plays an important role in the transmission of mmWave, which can be utilized to improve secrecy performance. Furthermore, in our adaptive transmission scheme, increasing the density of eavesdroppers not always deteriorates the secrecy performance. Ultimately, simulations provide an easy choice of transmit power and power allocation factor for achieving higher secrecy throughput.

The remainder of this paper is organized as follows. Section 2 presents the system model and the performance metric. Section 3 introduces the secure transmission strategies. Section 4 derives the expressions of secrecy performance for adaptive transmission scheme. Numerical and simulation results verified our theoretical analysis are presented in Section 5. Finally, we conclude this paper in Section 6.

2. System Description and Performance Metrics

2.1. System Description

Let's consider a mmWave wiretap network, which consists of a transmitter, a legitimate receiver and multiple random distributed eavesdroppers, as shown in Figure 1. The transmitter equipped with M multiple antennas uses directional beamforming for transmitting the confidential information. Both the legitimate receiver and the eavesdroppers equip a single antenna [31]. Furthermore, the locations of eavesdroppers, denoted by Φ_E , are modeled as an independent homogeneous Poisson point process (HPPP) with density λ_E . Without loss of generality, similar to [32], a sector model is used to analyze the beam pattern in this paper, particularly

$$G_S(\theta) = \begin{cases} M_S, & \text{if } |\theta| \leq \theta_S, \\ m_S, & \text{otherwise,} \end{cases} \quad (1)$$

where M_S represents the main lobe gain with the beam width θ_S , and m_S represents the array gain of side lobe. We assume that the transmitter can get the perfect channel state information (CSI) of the legitimate receiver; then, they can trim their antenna steering orientation array to their legitimate receiver and maximize the directivity gains. In practical terms, estimating the CSI may be a nontrivial task, so our work actually provides an upper bound on achievable secrecy performance. In this model, the eavesdroppers have been in the attempt to intercept the confidential information of the system, the CSIs of eavesdroppers are assumed to be unknown at the transmitter. The nearest eavesdropper is not necessarily the most detrimental one, but the one possessing the best channel to the transmitter. In addition, we consider non-colluding eavesdroppers in this work.

The secrecy performance of the system is further improved by using the sector secrecy guard zone and AN. It is assumed that the eavesdroppers can be detected by scanning nearby eavesdropping devices before transmission [17,18], provided that they are close enough to the transmitter. Therefore,

a sector secrecy guard zone having a radius of r is introduced, and the eavesdroppers may be in or out of the sector secrecy guard zone. Therefore, a sector secrecy guard zone having a radius of r is introduced, and the eavesdroppers may be in or out of the sector secrecy guard zone. Similar to the secrecy guard zone mechanism in Referecne [17], considering the characteristics of mmWave beam pattern, we model the finite range around the transmitter as a sector secrecy guard zone with radius r and central angle θ_s . Considering the generalized fading environment, mmWave communication channel is modeled as a Nakagami fading model. It is different from [33], which studied the secrecy performance of random multiple-input multiple- output (MIMO) wireless networks based on homogeneous Poisson point process (HPPP) over the α - μ fading channel. It is worth pointing out that the estimation of mmWave channel is more consistent with the actual communication system, but it is beyond the scope of this paper.

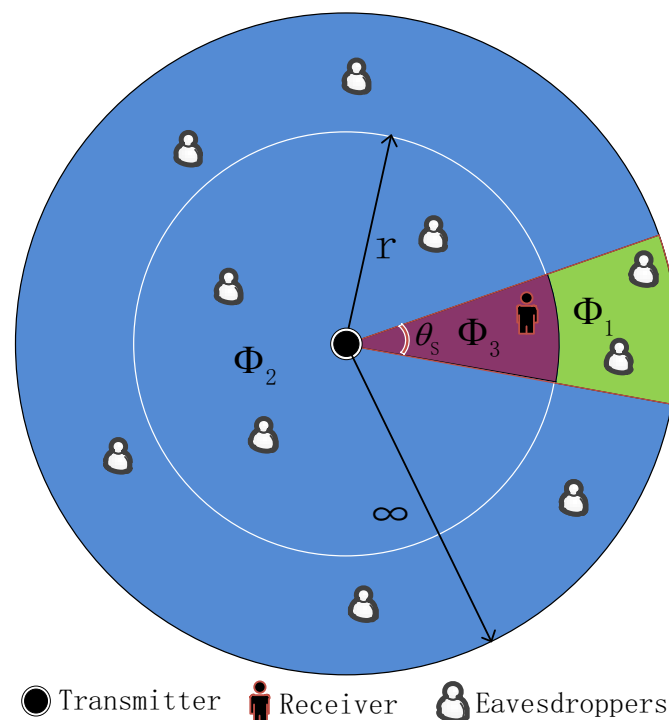


Figure 1. Network topology for the considered mmWave wiretap network. A sector secrecy guard zone is employed to approximate the beamforming pattern. Φ_1 , Φ_2 , Φ_3 indicate the different areas where the eavesdroppers are located.

According to the characteristics of mmWave in an outdoor scenario, the confidential information reaches to the legitimate receiver may be via LOS or NLOS [26]. According to 3GPP standards and the blockage model with random shape theory [34], the probability of a LOS with distance r_d is represented by $P_L(r_d)$, while the NLOS probability is $P_N(r_d)$. The probability $P_L(r_d)$ and $P_N(r_d)$ are given as $P_L(r_d) = e^{-\beta r_d}$ or $P_N(r_d) = 1 - e^{-\beta r_d}$, which can be acquired from stochastic blockage models or field measurements, where β is the blockage density.

In light of the pass-loss model and small-scale fading presented in [35], the channel gain received by the legitimate receiver can be expressed as $M_S|h_D|^2L(r_D)$ and the eavesdroppers can be expressed as $M_S|h_E|^2L(r_E)$ or $m_S|h_E|^2L(r_E)$, where both $|h_D|^2$ and $|h_E|^2$ are normalized Gamma random variable with following $\Gamma(N_L, 1/N_L)$ or $\Gamma(N_N, 1/N_N)$, r_D and r_E denote the distance from the transmitter to the legitimate receiver and the distance from the transmitter to the eavesdropper, N_L, N_N are the Nakagami fading parameter of LOS and NLOS, respectively. $L(r_D)$ and $L(r_E)$ denote the path loss function which are modeled as $L(r_j) = C_L r_j^{-\alpha_L}$ or $C_N r_j^{-\alpha_N}$, $j \in \{D, E\}$, r_j is the distance in meters, C_L and α_L are the constant and path loss exponent depending on the LOS, C_N and α_N depend on the NLOS.

Based on the aforementioned adaptive transmission scheme, there are serious security threats when there exist one or more eavesdroppers in the sector secrecy guard zone. In order to enhance the secure transmission performance, using the superposition coding [18], the transmitter transmits information-bearing signals and sends AN, namely AN assisted transmission. If there exists no eavesdroppers in the sector secrecy guard zone, the transmitter still transmits useful information signals, namely direct transmission. As previously assumed, the locations of eavesdroppers are randomly distributed, the probability of no eavesdropper existed within the sector secrecy guard zone is given by $p_{e1} = \exp(-\theta_S \lambda_E r^2 / 2)$, and the probability of eavesdropper existed within the sector secrecy guard zone is given by $p_{e2} = 1 - \exp(-\theta_S \lambda_E r^2 / 2)$ [36].

2.2. Performance Metrics

In the following, we use the SOP, the COP and the secrecy throughput to measure secrecy performance [37].

2.2.1. Secrecy Outage Probability and Connection Outage Probability

If the perfect security of confidential information can not be guaranteed, that is, a portion of the confidential information sent from the transmitter is decoded by at least one eavesdropper, the secrecy outage event takes place, the SOP is written as

$$p_{so} = \Pr(\gamma_E > 2^{R_B - R_S} - 1), \quad (2)$$

where γ_E denotes signal-to-interference-plus-noise received by the eavesdropper. Adopting Wyner code, R_S and R_B are the confidential information rate and codeword transmission rate, respectively, where $R_B \geq R_S$ [15,38].

If the confidential information cannot be decoded without error at the legitimate receiver, the connection outage event occurs, then the COP can be expressed as

$$p_{co} = \Pr(\gamma_D < 2^{R_B} - 1), \quad (3)$$

where γ_D denotes signal-to-interference-plus-noise received by the legitimate receiver.

2.2.2. Secrecy Throughput

The secrecy throughput represents the average secrecy rate when information is both secure and reliably transmitted. When p_{co} and p_{so} are independent of each other, the secrecy throughput is given by [19]

$$\eta = (1 - p_{co})(1 - p_{so}) R_S. \quad (4)$$

3. Secure Transmission Strategies

In this section, we focus on the SNR received by the receiver and eavesdroppers in the mmWave wiretap network. We assume that the transmitter is able to detect the existence of eavesdroppers within the sector secrecy guard zone. We first analyze that the eavesdroppers are not in the sector secrecy guard zone, and then consider the eavesdroppers in the sector secrecy guard zone. It is worth mentioning that whether there are eavesdroppers in the sector secrecy guard zone or not, the transmitter transmits useful information signals. When the eavesdroppers are in the sector secrecy guard zone, we further exploit AN and produce positive effects through power adjustment control.

3.1. Eavesdroppers Are Detected Beyond the Sector Secrecy Guard Zone

If there do not exist eavesdroppers within the sector secrecy guard zone, the transmitter keeps sending the confidential information to the legitimate receiver. In this case, eavesdroppers distribute

beyond the sector secrecy guard zone to intercept confidential information. Therefore, the SNR at the receiver is defined as

$$\gamma_{D_A} = \frac{PM_S|h_D|^2L(r_D)}{\sigma_D^2}, \quad (5)$$

and the instantaneous SNR of detecting the information of the legitimate receiver at the most detrimental eavesdropper is given by

$$\gamma_{E_A} = \frac{\max_{E \in \Phi_1} (PM_S|h_E|^2L(r_{E_A}))}{\sigma_E^2}, \quad (6)$$

or

$$\gamma_{E_{A1}} = \frac{\max_{E \in \Phi_2} (Pm_S|h_E|^2L(r_{E_{A1}}))}{\sigma_E^2}. \quad (7)$$

where $E \in \Phi_1$ denotes that eavesdroppers reside in the signal beam out of the sector secrecy guard zone, and then the SNR at the eavesdropper is γ_{E_A} . $E \in \Phi_2$ denotes that eavesdroppers may reside anywhere except in the signal beam where the sector secrecy guard zone is located, and then the SNR at the eavesdropper is $\gamma_{E_{A1}}$. The distance r_{E_A} from the eavesdropper to the transmitter is larger than the radius r of the sector secrecy guard zone. $r_{E_{A1}}$ is the distance from the eavesdropper to the transmitter in the side lobes, and $\sigma_v^2, v \in \{D, E\}$ denotes the additive white Gaussian power.

3.2. Eavesdropper Is Detected in the Sector Secrecy Guard Zone

If there exist eavesdroppers within the sector secrecy guard zone, the transmitter emits AN with power P_A while transmitting the signal with power P_S . The total transmit power is denoted as P , $P_S = \mu P, P_A = (1 - \mu) P$, where μ is the power allocation factor of the confidential information power to the total transmit power P with $0 \leq \mu \leq 1$ [36]. Then, the SNR at the receiver is given by

$$\gamma_{D_B} = \frac{P_S M_S |h_D|^2 L(r_D)}{\sigma_D^2}, \quad (8)$$

and the instantaneous SNR at the most detrimental eavesdropper is written as

$$\gamma_{E_B} = \max_{E \in \Phi_3} \left\{ \frac{(P_S M_S |h_E|^2 L(r_{E_B}))}{P_A M_S |h_E|^2 L(r_{E_B}) + \sigma_E^2} \right\}, \quad (9)$$

or

$$\gamma_{E_{B1}} = \frac{\max_{E \in \Phi_2} (Pm_S|h_E|^2L(r_{E_{B1}}))}{\sigma_E^2}, \quad (10)$$

where $E \in \Phi_3$ denotes that eavesdroppers may reside in the sector secrecy guard zone, and then the SNR at the eavesdropper is γ_{E_B} . $\gamma_{E_{B1}}$ is the SNR of the eavesdropper at $E \in \Phi_2$. The distance r_{E_B} from the eavesdropper to the transmitter is smaller than the radius r of the sector secrecy guard zone. $r_{E_{B1}}$ is the distance from the eavesdropper to the transmitter in the side lobes. Note that, in our paper, to prevent eavesdroppers from eavesdropping, the transmitter adds AN to the transmit signals. AN is generated so as to be canceled out at the legitimate receiver; thus, only eavesdroppers are affected by AN. Similar methods are presented in [39–41]. However, it is beyond the scope of our paper and could be our future research.

4. Performance Analysis

Hereinafter, we first analyze secrecy performance of the direct transmission in term of the COP, the SOP and the secrecy throughput. Then, according to the same performance metrics, AN assisted transmission is investigated. Actually, direct transmission and AN assisted transmission are two special cases of adaptive transmission. Finally, considering the probabilities aforementioned that eavesdroppers may be beyond the sector secrecy guard zone and within the sector secrecy guard zone, we study the secrecy performance of the adaptive transmission scheme.

4.1. Direct Transmission

For the direct transmission, there does not exist an eavesdropper within the sector secrecy guard zone, the transmitter keeps sending the confidential information to the legitimate receiver.

Substituting Equation (5) into Equation (3), the COP is derived as

$$\begin{aligned}
 p_{coa} &= \Pr(\gamma_{D_A} < 2^{R_B} - 1) = \Pr\left(\frac{PM_S|h_D|^2 L(r_D)}{\sigma_D^2} < 2^{R_B} - 1\right) = \Pr\left(|h_D|^2 < \frac{(2^{R_B} - 1)\sigma_D^2}{PM_S L(r_D)}\right) \\
 &= \sum_{i \in \{L, N\}} \left(\frac{Y\left(N_i, \frac{(2^{R_B} - 1)\sigma_D^2}{PM_S L(r_D)} N_i\right)}{\Gamma(N_i)} \right) P_i(r_D), \tag{11}
 \end{aligned}$$

where $Y(\cdot, \cdot)$ is the lower incomplete gamma function [42] (Equation (8.350)).

In the case of $E \in \Phi_1$, substituting Equation (6) into Equation (2), the SOP is calculated as follows:

$$p_{soa} = \Pr(\gamma_{E_A} > 2^{R_B - R_S} - 1) = \int_{2^{R_B - R_S} - 1}^{\infty} f_{\gamma_{E_A}}(x) dx, \tag{12}$$

where $f_{\gamma_{E_A}}(\cdot)$ stands for the probability density function of γ_{E_A} . By using the thinning theorem [26,43,44], the eavesdroppers are divided into two independent PPPs, namely LOS point process Φ_1^{LOS} with density function $\lambda_E P_L(r_d)$, and NLOS point process Φ_1^{NOS} with density function $\lambda_E (1 - P_L(r_d))$. Then, the cumulative distribution function of γ_{E_A} is derived as

$$\begin{aligned}
 F_{\gamma_{E_A}}(x) &= \Pr(\gamma_{E_A} < x) = \Pr\left\{ \frac{\max_{E \in \Phi_1} (PM_S|h_E|^2 L(r_{E_A}))}{\sigma_E^2} < x \right\} \\
 &= \underbrace{\Pr\left\{ \frac{\max_{E \in \Phi_1^L} (PM_S|h_E|^2 L(r_{E_A}))}{\sigma_E^2} < x \right\}}_{Z_1} \times \underbrace{\Pr\left\{ \frac{\max_{E \in \Phi_1^N} (PM_S|h_E|^2 L(r_{E_A}))}{\sigma_E^2} < x \right\}}_{Z_2}, \tag{13}
 \end{aligned}$$

where Φ_1^L and Φ_1^N are the set of LOS and NLOS eavesdroppers, respectively. Z_1 and Z_2 are calculated by Equations (14) and (15). In Z_1 , step (a) follows the probability generating functional of the PPP, and step (b) is based on [42] (Equation (8.354.1)). In Z_2 , step (c) follows the probability generating functional of the PPP, step (d) is based on [42] (Equation (3.381.9)):

$$\begin{aligned}
 Z_1 &= \Pr\left\{ \frac{\max_{E \in \Phi_1^L} (PM_S|h_E|^2 L(r_E))}{\sigma_E^2} < x \right\} \stackrel{a}{=} \exp\left(-\theta_S \lambda_E \int_r^\infty \Pr\left(|h_E|^2 > \frac{x \sigma_E^2 r^{\alpha_L}}{PM_S C_L}\right) e^{-\beta r} r_E dr\right) \\
 &\stackrel{b}{=} \exp\left(-\theta_S \lambda_E \left(\frac{\Gamma(2, \beta r)}{\beta^2} - \frac{\left(\frac{N_L x \sigma_E^2}{PM_S C_L}\right)^{N_L}}{\Gamma(N_L)} \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{N_L x \sigma_E^2}{PM_S C_L}\right)^n}{n!(N_L+n)} \frac{\Gamma(\alpha_L(N_L+n)+2, \beta r)}{\beta^{\alpha_L(N_L+n)+2}} \right)\right), \tag{14}
 \end{aligned}$$

$$\begin{aligned}
 Z_2 &= \Pr \left\{ \frac{\max_{E \in \Phi_1^N} (PM_S |h_E|^2 L(r_{E_A}))}{\sigma_E^2} < x \right\} = E \left\{ \prod_{E \in \Phi_1^N} \Pr \left(|h_E|^2 < \frac{x \sigma_E^2}{PM_S L(r_{E_A})} \right) \mid \Phi_1^N \right\} \\
 &\stackrel{c}{=} \exp \left(-\theta_S \lambda_E \int_r^\infty \Pr \left(|h_E|^2 > \frac{x \sigma_E^2 r_{E_A}^{N_N}}{PM_S C_N} \right) (1 - e^{-\beta r_{E_A}}) r_{E_A} dr_{E_A} \right) \\
 &\stackrel{d}{=} \exp \left(-\theta_S \lambda_E \left(\left(\frac{(N_N - 1)!}{\Gamma(N_N)} \right) \sum_{m=0}^{N_N - 1} \frac{\left(\frac{x \sigma_E^2 N_N}{PM_S C_N} \right)^m}{m!} \times \frac{\Gamma \left(\frac{m \alpha_N + 2}{\alpha_N}, \frac{x \sigma_E^2 N_N}{PM_S C_N} r^{\alpha_N} \right)}{\alpha_N \left(\frac{x \sigma_E^2 N_N}{PM_S C_N} \right)^{\frac{m \alpha_N + 2}{\alpha_N}}} \right. \right. \\
 &\quad \left. \left. - \left(\frac{\Gamma(2, \beta r)}{\beta^2} - \frac{\left(\frac{N_N x \sigma_E^2}{PM_S C_N} \right)^{N_N}}{\Gamma(N_N)} \sum_{n=0}^\infty \frac{(-1)^n \left(\frac{N_N x \sigma_E^2}{PM_S C_N} \right)^n}{n! (N_N + n)} \frac{\Gamma(\alpha_N (N_N + n) + 2, \beta r)}{\beta^{\alpha_N (N_N + n) + 2}} \right) \right) \right). \tag{15}
 \end{aligned}$$

For the sake of simplicity, $F_{\gamma_{E_A}}(x)$ can be simplified as

$$F_{\gamma_{E_A}}(x) = \exp(-\theta_S \lambda_E (B + A_N - A_L)), \tag{16}$$

where $B = \left(\frac{(N_N - 1)!}{\Gamma(N_N)} \right) \sum_{m=0}^{N_N - 1} \frac{q^m}{m!} \times \frac{\Gamma \left(\frac{m \alpha_N + 2}{\alpha_N}, q r^{\alpha_N} \right)}{\alpha_N q^{\frac{m \alpha_N + 2}{\alpha_N}}}$; here, $\Gamma(\cdot, \cdot)$ is the upper incomplete gamma function [42] (Equation (8.350)), $A_N = \frac{q^{N_N}}{\Gamma(N_N)} \sum_{n=0}^\infty \frac{(-1)^n q^n}{n! (N_N + n)} \frac{\Gamma(\alpha_N (N_N + n) + 2, \beta r)}{\beta^{\alpha_N (N_N + n) + 2}}$, $A_L = \frac{p^{N_L}}{\Gamma(N_L)} \sum_{n=0}^\infty \frac{(-1)^n p^n}{n! (N_L + n)} \frac{\Gamma(\alpha_L (N_L + n) + 2, \beta r)}{\beta^{\alpha_L (N_L + n) + 2}}$, $q = \frac{x \sigma_E^2 N_N}{PM_S C_N}$, $p = \frac{N_L x \sigma_E^2}{PM_S C_L}$.

Based on Equations (12) and (16), the SOP is derived as

$$\begin{aligned}
 p_{soa} &= \Pr \left(\gamma_{E_A} > 2^{R_B - R_S} - 1 \right) = \int_{2^{R_B - R_S} - 1}^\infty f_{\gamma_{E_A}}(x) dx \\
 &= 1 - \exp(-\theta_S \lambda_E (B + A_N - A_L)). \tag{17}
 \end{aligned}$$

Substituting Equations (11) and (17) into Equation (4), the secrecy throughput η_a is derived as

$$\begin{aligned}
 \eta_a &= (1 - p_{coa}) (1 - p_{soa}) R_S \\
 &= \left(1 - \sum_{i \in \{L, N\}} \left(\frac{Y \left(N_i, \frac{(2^{R_B} - 1) \sigma_D^2}{PM_S L(r_D)} N_i \right)}{\Gamma(N_i)} \right) P_i(r_D) \right) \\
 &\quad \times \exp(-\theta_S \lambda_E (B + A_N - A_L)) R_S. \tag{18}
 \end{aligned}$$

Remark 1. It can be deduced from Equation (11) that the COP is a decreasing function of P , this implies that the reliability performance of system is strengthened as P increases. For the case of $E \in \Phi_1$, Equation (17) shows that the SOP increases with P when the sector secrecy guard zone is invariant. Correspondingly, when P is fixed, the secrecy performance becomes better with the increase of the sector secrecy guard zone. It means that, in this case, increasing power makes it possible to leak confidential information to eavesdroppers, and, at the same time, using the sector guard zone to keep eavesdroppers away from legitimate user. In addition, from Equation (18), it can be deduced that, in addition to P and λ_E , the secrecy throughput has a close relationship with radius r and central angle θ_S of the secrecy guard zone.

In the case of $E \in \Phi_2$, i.e., eavesdroppers may reside anywhere except in the signal beam where the sector secrecy guard zone is located. Substituting Equation (7) into Equation (2), the SOP is derived as

$$p_{soa1} = \Pr \left(\gamma_{E_{A1}} > 2^{R_B - R_S} - 1 \right) = \int_{2^{R_B - R_S} - 1}^\infty f_{\gamma_{E_{A1}}}(x) dx. \tag{19}$$

The cumulative distribution function of $\gamma_{E_{A1}}$ is derived as

$$\begin{aligned}
 F_{\gamma_{E_{A1}}}(x) &= \Pr(\gamma_{E_{A1}} < x) = \Pr\left\{ \frac{\max_{E \in \Phi_2} (Pm_S |h_E|^2 L(r_{E_{A1}}))}{\sigma_E^2} < x \right\} \\
 &= \underbrace{\Pr\left\{ \frac{\max_{E \in \Phi_2^L} (Pm_S |h_E|^2 L(r_{E_{A1}}))}{\sigma_E^2} < x \right\}}_{Z_3} \times \underbrace{\Pr\left\{ \frac{\max_{E \in \Phi_2^N} (Pm_S |h_E|^2 L(r_{E_{A1}}))}{\sigma_E^2} < x \right\}}_{Z_4}, \tag{20}
 \end{aligned}$$

where Φ_2^L and Φ_2^N are the set of LOS and NLOS eaversdroppers, respectively. Z_3 and Z_4 are calculated by (14) and (15). In Z_3 , step (e) is based on [42] (Equation (3.351.2)). In Z_4 , step (f) is based on [42] (Equation (3.381.9)):

$$\begin{aligned}
 Z_3 &= \Pr\left\{ \frac{\max_{E \in \Phi_2^L} (Pm_S |h_E|^2 L(r_{E_{A1}}))}{\sigma_E^2} < x \right\} = E \left\{ \prod_{E \in \Phi_2^L} \Pr\left(|h_E|^2 < \frac{x\sigma_E^2}{Pm_S L(r_{E_{A1}})} \right) \mid \Phi_2^L \right\} \\
 &\stackrel{e}{=} \exp\left(- (2\pi - \theta_S) \lambda_E \left(\frac{\Gamma(2)}{\beta^2} - \frac{\left(\frac{N_L x \sigma_E^2}{Pm_S C_L}\right)^{N_L}}{\Gamma(N_L)} \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{N_L x \sigma_E^2}{Pm_S C_L}\right)^n}{n!(N_L+n)} \frac{\Gamma(\alpha_L(N_L+n)+2)}{\beta^{\alpha_L(N_L+n)+2}} \right) \right), \tag{21}
 \end{aligned}$$

$$\begin{aligned}
 Z_4 &= \Pr\left\{ \frac{\max_{E \in \Phi_2^N} (Pm_S |h_E|^2 L(r_{E_{A1}}))}{\sigma_E^2} < x \right\} = E \left\{ \prod_{E \in \Phi_2^N} \Pr\left(|h_E|^2 < \frac{x\sigma_E^2}{Pm_S L(r_{E_{A1}})} \right) \mid \Phi_2^N \right\} \\
 &\stackrel{f}{=} \exp\left(- (2\pi - \theta_S) \lambda_E \left(\left(\frac{(N_N-1)!}{\Gamma(N_N)} \sum_{m=0}^{N_N-1} \frac{\left(\frac{x\sigma_E^2 N_N}{Pm_S C_N}\right)^m}{m!} \times \frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N}\right)}{\alpha_N \left(\frac{x\sigma_E^2 N_N}{Pm_S C_N}\right)^{\frac{m\alpha_N+2}{\alpha_N}}} \right. \right. \\
 &\quad \left. \left. - \left(\frac{\Gamma(2)}{\beta^2} - \frac{\left(\frac{N_N x \sigma_E^2}{Pm_S C_N}\right)^{N_N}}{\Gamma(N_N)} \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{N_N x \sigma_E^2}{Pm_S C_N}\right)^n}{n!(N_N+n)} \frac{\Gamma(\alpha_N(N_N+n)+2)}{\beta^{\alpha_N(N_N+n)+2}} \right) \right) \right). \tag{22}
 \end{aligned}$$

Upon further simplification, $F_{\gamma_{E_{A1}}}(x)$ can be simplified as

$$F_{\gamma_{E_{A1}}}(x) = \exp\left(- (2\pi - \theta_S) \lambda_E (D + C_N - C_L) \right), \tag{23}$$

where $D = \left(\frac{(N_N-1)!}{\Gamma(N_N)} \sum_{m=0}^{N_N-1} \frac{u^m}{m!} \times \frac{\Gamma\left(\frac{m\alpha_N+2}{\alpha_N}\right)}{\alpha_N u \frac{m\alpha_N+2}{\alpha_N}} \right)$, $u = \frac{x\sigma_E^2 N_N}{Pm_S C_N}$, $C_N = \frac{u^{N_N}}{\Gamma(N_N)} \sum_{n=0}^{\infty} \frac{(-1)^n u^n}{n!(N_N+n)} \frac{\Gamma(\alpha_N(N_N+n)+2)}{\beta^{\alpha_N(N_N+n)+2}}$, $C_L = \frac{k^{N_L}}{\Gamma(N_L)} \sum_{n=0}^{\infty} \frac{(-1)^n k^n}{n!(N_L+n)} \frac{\Gamma(\alpha_L(N_L+n)+2)}{\beta^{\alpha_L(N_L+n)+2}}$, $k = \frac{N_L x \sigma_E^2}{Pm_S C_L}$.

Based on Equations (19) and (23), the SOP is derived as

$$\begin{aligned}
 p_{soa1} &= \Pr\left(\gamma_{E_{A1}} > 2^{R_B - R_S} - 1 \right) = \int_{2^{R_B - R_S} - 1}^{\infty} f_{\gamma_{E_{A1}}}(x) dx \\
 &= 1 - \exp\left(- (2\pi - \theta_S) \lambda_E (D + C_N - C_L) \right). \tag{24}
 \end{aligned}$$

Substituting Equations (11) and (24) into Equation (4), the secrecy throughput is derived as

$$\begin{aligned} \eta_{soa1} &= (1 - p_{coa}) (1 - p_{soa1}) R_S \\ &= \left(1 - \sum_{i \in \{L, N\}} \left(\frac{Y \left(N_i, \frac{(2^{R_B} - 1) \sigma_D^2}{P M_S L(r_D)} N_i \right)}{\Gamma(N_i)} \right) P_i(r_D) \right) \\ &\quad \times \exp(- (2\pi - \theta_S) \lambda_E (D + C_N - C_L)) R_S. \end{aligned} \tag{25}$$

Remark 2. In the case of $E \in \Phi_2$, the eavesdroppers are not in the beam where the sector secrecy guard zone is located; security threats come mainly from sidelobe. Referecne Equation (24) shows that the SOP is an increasing function of P and m_S , which indicates that the secrecy performance becomes better as P and m_S decreases. It means that, when the eavesdroppers are in the sidelobe, increasing power P and m_S may lead to a leakage of confidential information. At the same time, increasing the central angle θ_S of the sector guard zone can reduce the risk of eavesdropping. In addition, from Equation (25), it can be deduced that, in addition to P and eavesdropper density λ_E , the secrecy throughput has a close relationship with radius r and central angle θ_S of the secrecy guard zone as well.

On the basis of the locations for the eavesdroppers, both $E \in \Phi_1$ and $E \in \Phi_2$ are considered together, i.e., eavesdroppers may reside anywhere except the sector secrecy guard zone. The SOP is derived as

$$\begin{aligned} p_{sot} &= \Pr \left(\max(\gamma_{E_A}, \gamma_{E_{A1}}) > 2^{R_B - R_S} - 1 \right) \\ &= 1 - \Pr(\gamma_{E_A} < 2^{R_B - R_S} - 1) \times \Pr(\gamma_{E_{A1}} < 2^{R_B - R_S} - 1) \\ &= 1 - \exp(-\theta_S \lambda_E (B + A_N - A_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L)). \end{aligned} \tag{26}$$

The total secrecy throughput of eavesdroppers in $E \in \Phi_1$ and $E \in \Phi_2$ is derived as

$$\begin{aligned} \eta_t &= (1 - p_{coa}) (1 - p_{sot}) R_S \\ &= \left(1 - \sum_{i \in \{L, N\}} \left(\frac{Y \left(N_i, \frac{(2^{R_B} - 1) \sigma_D^2}{P M_S L(r_D)} N_i \right)}{\Gamma(N_i)} \right) P_i(r_D) \right) \\ &\quad \times \exp(-\theta_S \lambda_E (B + A_N - A_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L)) R_S. \end{aligned} \tag{27}$$

4.2. AN Assisted Transmission

For AN assisted transmission, once the eavesdroppers locate in the sector secrecy guard zone, the transmitter emits information-bearing signal along with AN.

Thus, substituting Equation (8) into Equation (3), the COP is derived as

$$\begin{aligned} p_{cob} &= P(\gamma_{D_B} < 2^{R_B} - 1) = \Pr \left(\frac{P_S M_S |h_D|^2 L(r_D)}{\sigma_D^2} < 2^{R_B} - 1 \right) \\ &= \sum_{i \in \{L, N\}} \Pr \left(|h_D|^2 < \frac{(2^{R_B} - 1) \sigma_D^2}{P_S M_S L(r_D)} \middle| i \right) P_i(r_D) \\ &= \sum_{i \in \{L, N\}} \left(\frac{Y \left(N_i, \frac{(2^{R_B} - 1) \sigma_D^2}{P_S M_S L(r_D)} N_i \right)}{\Gamma(N_i)} \right) P_i(r_D). \end{aligned} \tag{28}$$

In the case of $E \in \Phi_3$, i.e., eavesdroppers reside in the sector secrecy guard zone. Substituting Equation (9) into Equation (2), the SOP is derived as

$$p_{sob} = \Pr(\gamma_{E_B} > 2^{R_B - R_S} - 1) = \int_{2^{R_B - R_S} - 1}^{\infty} f_{\gamma_{E_B}}(x) dx, \tag{29}$$

where $f_{\gamma_{E_B}}(\cdot)$ stands for the probability density function of γ_{E_B} ; then, the cumulative distribution function of γ_{E_B} is derived as

$$\begin{aligned} F_{\gamma_{E_B}}(x) &= \Pr(\gamma_{E_B} < x) \\ &= \Pr\left\{ \max_{E \in \Phi_3} \left\{ \frac{(P_S M_S |h_E|^2 L(r_{E_B}))}{P_A M_S |h_E|^2 L(r_E) + \sigma_E^2} \right\} < x \right\} \\ &= \Pr\left\{ \underbrace{\max_{E \in \Phi_3^L} \left\{ \frac{(P_S M_S |h_E|^2 L(r_{E_B}))}{P_A M_S |h_E|^2 L(r_{E_B}) + \sigma_E^2} \right\}}_{Z_5} < x \right\} \times \Pr\left\{ \underbrace{\max_{E \in \Phi_3^N} \left\{ \frac{(P_S M_S |h_E|^2 L(r_{E_B}))}{P_A M_S |h_E|^2 L(r_{E_B}) + \sigma_E^2} \right\}}_{Z_6} < x \right\}, \end{aligned} \tag{30}$$

where Φ_3^L and Φ_3^N are the set of LOS and NLOS eavesdroppers, respectively. Z_5 and Z_6 are calculated by Equations (31) and (32). In Z_5 , step (g) follows the probability generating functional of the PPP, step (h) is based on [42] (Equation(3.351.2)). In Z_6 , step (p) follows the probability generating functional of the PPP, step (q) is based on [42] (Equation (3.381.9)):

$$\begin{aligned} Z_5 &= \Pr\left\{ \max_{E \in \Phi_3^L} \left\{ \frac{(P_S M_S |h_E|^2 L(r_{E_B}))}{P_A M_S |h_E|^2 L(r_{E_B}) + \sigma_E^2} \right\} < x \right\} \\ &\stackrel{g}{=} U\left(x - \frac{P_S}{P_A}\right) + U\left(\frac{P_S}{P_A} - x\right) \exp\left(-\theta_S \lambda_E \int_0^r \Pr\left(|h_E|^2 > \frac{x \sigma_E^2}{L(r_{E_B})(P_S M_S - P_A M_S x)}\right) e^{-\beta r_{E_B}} r_{E_B} dr_{E_B}\right) \\ &\stackrel{h}{=} U\left(x - \frac{P_S}{P_A}\right) + U\left(\frac{P_S}{P_A} - x\right) \exp\left(-\theta_S \lambda_E \left(\frac{Y(2, \beta r)}{\beta^2} - \frac{v^{N_L}}{\Gamma(N_L)} \sum_{n=0}^{\infty} \frac{(-1)^n v^n}{n!(N_L+n)} \frac{Y(\alpha_L(N_L+n)+2, \beta r)}{\beta^{\alpha_L(N_L+n)+2}}\right)\right), \end{aligned} \tag{31}$$

$$\begin{aligned} Z_6 &= \Pr\left\{ \max_{E \in \Phi_3^N} \left\{ \frac{(P_S M_S |h_E|^2 L(r_{E_B}))}{P_A M_S |h_E|^2 L(r_{E_B}) + \sigma_E^2} \right\} < x \right\} \\ &\stackrel{p}{=} U\left(x - \frac{P_S}{P_A}\right) + U\left(\frac{P_S}{P_A} - x\right) \exp\left(-\theta_S \lambda_E \int_0^r \Pr\left(|h_E|^2 > \frac{x \sigma_E^2}{L(r_{E_B})(P_S M_S - P_A M_S x)}\right) (1 - e^{-\beta r_{E_B}}) r_{E_B} dr_{E_B}\right) \\ &\stackrel{q}{=} U\left(x - \frac{P_S}{P_A}\right) + U\left(\frac{P_S}{P_A} - x\right) \exp\left(-\theta_S \lambda_E \left(\left(\frac{(N_N-1)!}{\Gamma(N_N)}\right) \sum_{m=0}^{N_N-1} \frac{w^m}{m!} \times \frac{Y\left(\frac{m \alpha_N + 2}{\alpha_N}, w r^{\alpha_N}\right)}{\alpha_N w^{\frac{m \alpha_N + 2}{\alpha_N}}}\right.\right. \\ &\quad \left.\left. - \left(\frac{Y(2, \beta r)}{\beta^2} - \frac{w^{N_N}}{\Gamma(N_N)} \sum_{n=0}^{\infty} w \frac{Y(\alpha_N(N_N+n)+2, \beta r)}{\beta^{\alpha_N(N_N+n)+2}}\right)\right)\right). \end{aligned} \tag{32}$$

Upon further simplification, $F_{\gamma_{E_B}}(x)$ can be simplified as

$$F_{\gamma_{E_B}}(x) = \exp(-\theta_S \lambda_E (F + E_N - E_L)), \tag{33}$$

where $F = \left(\frac{(N_N-1)!}{\Gamma(N_N)}\right) \sum_{m=0}^{N_N-1} \frac{w^m}{m!} \times \frac{Y\left(\frac{m \alpha_N + 2}{\alpha_N}, w r^{\alpha_N}\right)}{\alpha_N w^{\frac{m \alpha_N + 2}{\alpha_N}}}$, $E_N = \frac{w^{N_N}}{\Gamma(N_N)} \sum_{n=0}^{\infty} \frac{(-1)^n w^n}{n!(N_N+n)} \times \frac{Y(\alpha_N(N_N+n)+2, \beta r)}{\beta^{\alpha_N(N_N+n)+2}}$,

and $w = \frac{x \sigma_E^2 N_N}{(P_S M_S - P_A M_S x) C_N}$, $v = \frac{N_L x \sigma_E^2}{(P_S M_S - P_A M_S x) C_L}$, and $E_L = \frac{v^{N_L}}{\Gamma(N_L)} \sum_{n=0}^{\infty} \frac{(-1)^n v^n}{n!(N_L+n)} \frac{Y(\alpha_L(N_L+n)+2, \beta r)}{\beta^{\alpha_L(N_L+n)+2}}$.

Based on Equations (29) and (33), the SOP is derived as

$$\begin{aligned} p_{sob} &= \Pr(\gamma_{E_B} > 2^{R_B - R_S} - 1) = \int_{2^{R_B - R_S} - 1}^{\infty} f_{\gamma_{E_B}}(x) dx \\ &= 1 - \exp(-\theta_S \lambda_E (F + E_N - E_L)). \end{aligned} \tag{34}$$

Substituting Equations (28) and (34) into Equation (4), the secrecy throughput is derived as

$$\begin{aligned} \eta_b &= (1 - p_{cob}) (1 - p_{sob}) R_S \\ &= \left(1 - \sum_{i \in \{L, N\}} \left(\frac{Y \left(N_i, \frac{(2^{R_B} - 1) \sigma_D^2}{P_S M_S L(r_D)} N_i \right)}{\Gamma(N_i)} \right) P_i(r_D) \right) \\ &\quad \times \exp(-\theta_S \lambda_E (F + E_N - E_L)) R_S. \end{aligned} \tag{35}$$

Remark 3. From Equation (28), it is explicitly shown that the COP is a decreasing function about transmitting power. Adding more transmitting power could help the improvement of reliability performance. In the case of $E \in \Phi_3$, the eavesdroppers are located in the sector secrecy guard zone, and the transmitter allocates a portion of the power to transmit the AN to confuse the eavesdroppers. From Equation (34), we see that the SOP has a close relationship with central angle θ_S , eavesdropper density λ_E and AN power. Additionally, Equation (35) shows that, in addition to central angle θ_S and eavesdropper density λ_E , the transmit power allocation factor μ is of vital importance.

In addition, the eavesdroppers may be in the case of $E \in \Phi_1$ and $E \in \Phi_2$, the derivation process and results are similar to those in Section 4.1.

4.3. Adaptive Transmission

In order to adapt to the actual scenario, both $E \in \Phi_1$, $E \in \Phi_2$ and $E \in \Phi_3$ are considered together, and the adaptive transmission scheme is adopted. That is, when the eavesdroppers are beyond the sector secrecy guard zone, the system adopts direct transmission, and when the eavesdroppers are in the sector secrecy guard zone, AN assisted transmission is used. Considering the probabilities aforementioned that eavesdroppers may be beyond the sector secrecy guard zone and within the sector secrecy guard zone, we study the secrecy performance of an adaptive transmission scheme.

Combined with the probability p_{e1} that the eavesdroppers may not be in sector secrecy guard zone, we deduce the SOP, which is derived as

$$\begin{aligned} p_{soc1} &= p_{e1} \times \Pr(\max(\gamma_{E_{A1}}, \gamma_{E_{A1'}}) > 2^{R_B - R_S} - 1) \\ &= p_{e1} \times (1 - \exp(-\theta_S \lambda_E (B + A_N - A_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L))). \end{aligned} \tag{36}$$

Correspondingly, considering the probability p_{e2} of eavesdroppers in sector secrecy guard zone, we deduce SOP, which is expressed as

$$\begin{aligned} p_{soc2} &= p_{e2} \times \Pr(\max(\gamma_{E_{A1'}}, \gamma_{E_B}) > 2^{R_B - R_S} - 1) \\ &= p_{e2} \times (1 - \exp(-\theta_S \lambda_E (F + E_N - E_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L))). \end{aligned} \tag{37}$$

Finally, we derive the SOP of the whole system under the random distribution of eavesdroppers, which is written as

$$\begin{aligned} p_{soc} &= p_{soc1} + p_{soc2} \\ &= p_{e1} \times (1 - \exp(-\theta_S \lambda_E (B + A_N - A_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L))) \\ &\quad + p_{e2} \times (1 - \exp(-\theta_S \lambda_E (F + E_N - E_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L))). \end{aligned} \tag{38}$$

As a result, the total secrecy throughput of the whole system is derived as

$$\begin{aligned} \eta &= (1 - p_{cob}) (1 - p_{soc}) R_S \\ &= \left(1 - \sum_{i \in \{L, N\}} \left(\frac{Y \left(N_i, \frac{(2^{R_B} - 1) \sigma_D^2}{P M_S L(r_D)} N_i \right)}{\Gamma(N_i)} \right) P_i(r_D) \right) \\ &\quad \times (1 - p_{e1} \times (1 - \exp(-\theta_S \lambda_E (B + A_N - A_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L))) \\ &\quad - p_{e2} \times (1 - \exp(-\theta_S \lambda_E (F + E_N - E_L) - (2\pi - \theta_S) \lambda_E (D + C_N - C_L)))) R_S. \end{aligned} \tag{39}$$

5. Numerical Results

In this section, some representative simulation results are presented to verify our theoretical analysis, and characterize the secrecy performance of the mmWave wiretap network. A set of closed-form expressions are derived in an adaptive transmission scheme to analyze the effects for different system parameters. We assume that the noise power is $\sigma_D^2 = \sigma_E^2 = -70$ dBm, and the LOS probability function is $P_L(r) = e^{-\beta r}$ with $\frac{1}{\beta} = 141.4$. According to [45], we focus on the carrier frequency of 28 GHz and 73 GHz. The Nakagami fading parameters of the LOS (NLOS) link are $N_L = 3$ ($N_N = 2$), the parameters of path-loss model are $\beta_L = 61.4$ dB, $\alpha_L = 2$, $\beta_N = 72$ dB, $\alpha_N = 2.92$ and $\beta_L = 69.8$ dB, $\alpha_L = 2$, $\beta_N = 82.7$ dB, $\alpha_N = 2.69$, $C_L = 10^{-\frac{\beta_L}{10}}$ and $C_N = 10^{-\frac{\beta_N}{10}}$ can be regarded as path-loss intercepts on the reference distance of LOS and NLOS links.

Figure 2 presents the effects of the p_{co} and p_{so} versus the transmit power in different frequency bands, namely 28 GHz and 73 GHz. Obviously, with the increasing of P , the reliability performance of the legitimate receiver increases due to the decrease of the COP for a given power allocation factor, while the secrecy performance would decline. When the power increases to a certain value, the SNR received by the eavesdropper is close to a fixed value from Equation (6), the SOP remains unchanged and the COP of the legitimate receiver is close to zero. This can be explained as follows: on the one hand, although the eavesdropper is in the sector guard zone, the system can still guarantee a secure link to a legitimate receiver by transmitting AN to confuse the eavesdropper. On the other hand, it is because P has different effects on the COP and SOP in the case of LOS and NLOS. In addition, when P is large, the difference of SNR between legitimate link and eavesdropping link tends to be constant. It means that the reliability of the system can be improved effectively by increasing the power of the system. Again, we obtain an important observation that secrecy transmission at 28 GHz is better than that at 73 GHz in a low transmit power region.

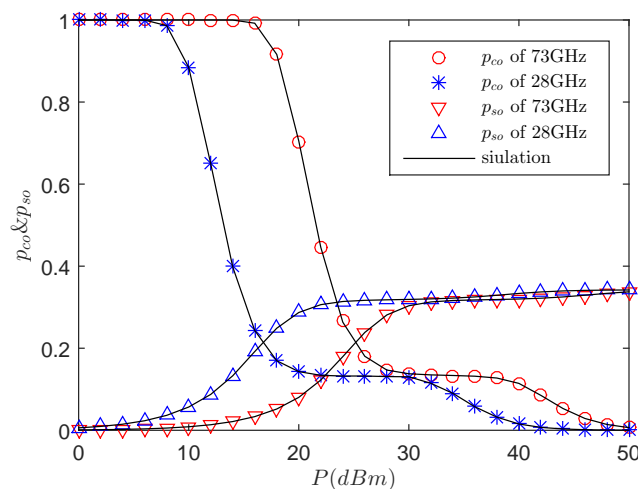


Figure 2. The p_{co} and p_{so} versus P with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $\lambda_E = 0.0002$ nodes/m², $r = 20$ m, $\theta_S = \frac{\pi}{3}$, $\mu = 0.6$, $m_S = 0.1$ and $M_S = 200$.

Figure 3 presents the effects of the SOP, p_{so} , and the COP, p_{co} , versus the eavesdropper density λ_E with the different frequency. As λ_E increases, we see that the p_{so} keeps increasing and the p_{co} remains constant for given a power P . In particular, compared with the 73 GHz band, the 28 GHz band reduces the p_{co} and improves the reliability of the system, but at the same time increases the p_{so} and reduces the secrecy performance of the system. These observations can help the system designer to select different frequency bands according to the actual performance requirements. For example, when the actual system requires high reliability, it is suitable to select the 28 GHz band.

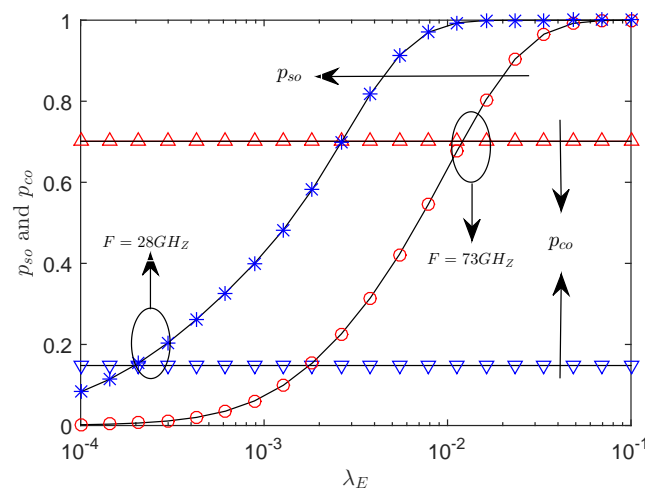


Figure 3. The p_{co} and p_{so} versus λ with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $P = 30$ dBm, $r = 50$ m, $\theta_S = \frac{\pi}{3}$, $\mu = 0.6$, $m_S = 0.1$ and $M_S = 200$.

Figure 4 presents the effects of the η versus the transmit power with the different sector secrecy guard zone radius r and frequency. We see that there exists an optimal P for maximizing the secrecy throughput at the considered mmWave frequencies. At a low transmission power region, the secrecy throughput of 28 GHz is better, and the same result can be achieved at 73 GHz when the transmission power becomes sufficiently large. The reason is that, in the case of low transmission power regime, mmWave link at lower mmWave frequencies experiences lower path loss and has stronger signal strength, thus achieving better performance. However, in the high transmission power regime, due to the high path loss at higher mmWave frequencies, the interference received by the legitimate user becomes lower, and the signal strength of the eavesdropper is also reduced at higher mmWave frequencies. In addition, we observe that the secrecy throughput of $r = 50$ m is always superior to that of $r = 20$ m. The reason is that there does not exist an eavesdropper within the sector secrecy guard zone when transmitting, and the secrecy performance becomes better with r increasing. Again, for achieving the same secrecy throughput, the transmit power required at 28 GHz is lower than 73 GHz.

Figure 5 presents the central angle θ_S of sector secrecy guard zone on the secrecy throughput. It is obvious that the secrecy throughput of the system decreases with the central angle θ_S of the sector secrecy guard zone when the transmit power and the power allocation factor are sufficiently large. Specifically, under the same conditions, the performance of 73 GHz is superior to that of 28 GHz, which is mainly due to the difference path loss [45]. In addition, in the larger central angle region, the smaller radius is better than the larger radius due to fact that the larger sector secrecy guard zone may contain more eavesdroppers, which is detrimental to the secrecy performance.

Figure 6 presents the effects of transmit power allocation factor on the secrecy throughput with the different frequency. We note that there exists an optimal transmit power allocation factor μ to maximize the secrecy throughput. When the μ is very small, it means that almost all power is allocated to AN, and the secrecy throughput is very small. With the increase of the power allocated to the information signal, that is, the increase of the power allocation factor, the secrecy throughput increases gradually.

However, when the power allocation factor increases to a certain value, the secrecy throughput starts to accelerate drop, the reason is that when the power allocation factor is increased to a certain value, the power used to AN decreases, which increases the possibility that an eavesdropper can intercept information, and the security cannot be guaranteed. Therefore, more power should be allocated to the AN to interfere with the eavesdropper, which demonstrates that it is very important to set the power allocation of the AN and the information signal properly. In addition, when the power allocated to AN is reduced to a certain value, the attenuation of η in the wider main lobe is faster, which is because more eavesdroppers may be located in the wider sector secrecy guard zone. Again, for the same circumstance, when the power allocation factor is increased to a certain value, the secrecy throughput reaches the maximum value, and the performance of 73 GHz is better than that of 28 GHz with the further increase of power allocation factor for a given r .

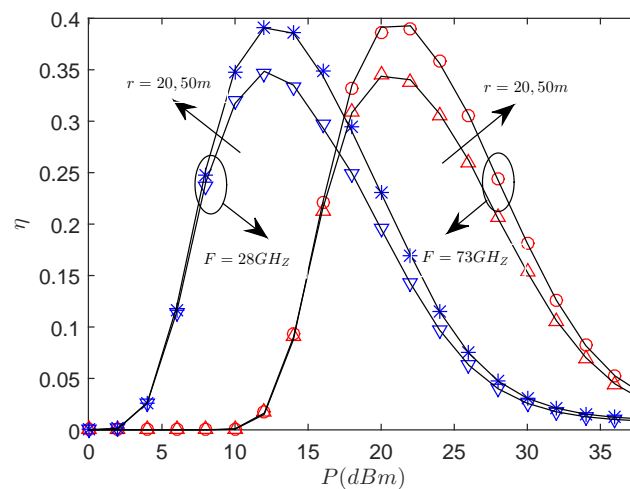


Figure 4. The η versus P with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $\theta_S = \frac{\pi}{3}$, $\lambda_E = 0.0002$ nodes/m², $m_S = 0.1$ and $M_S = 200$.

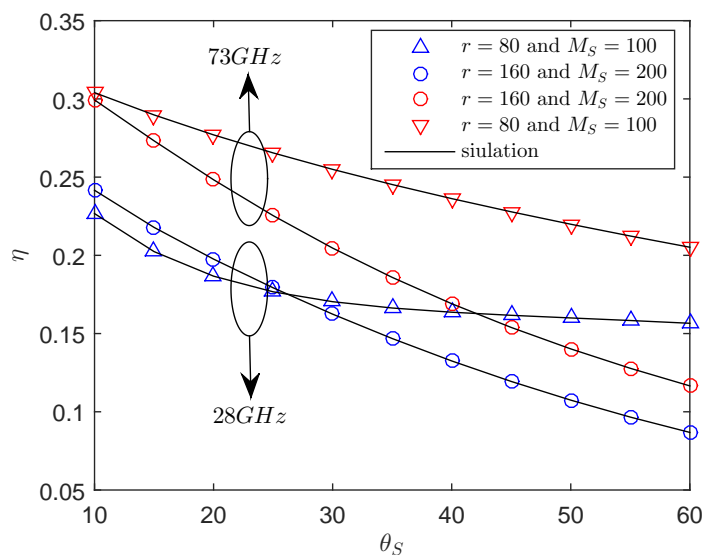


Figure 5. The η versus θ_S with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $P = 30$ dBm, $\mu = 0.6$, $\lambda_E = 0.0002$ nodes/m², $m_S = 0.1$.

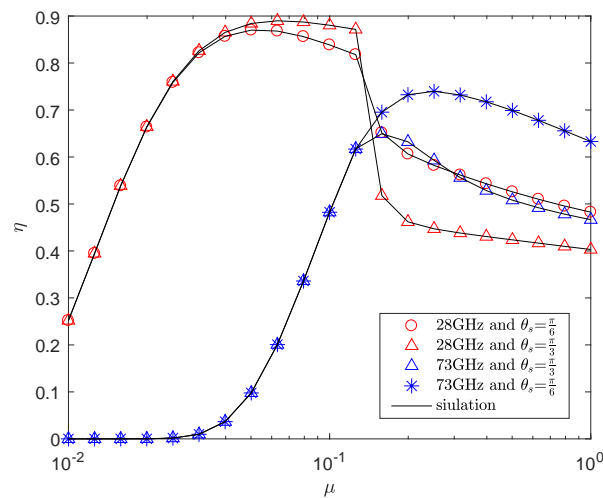


Figure 6. The η versus μ with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $P = 30$ dBm, $\lambda_E = 0.0002$ nodes/m², $r = 50$ m, $m_S = 0.1$ and $M_S = 200$.

Figure 7 presents the effects of the η versus the eavesdropper density λ_E with the different central angle θ_S . We see that, when increasing of λ_E , the secrecy throughput declines. This can be explained by when λ_E is low, the eavesdroppers located in $E \in \Phi_1$ and $E \in \Phi_2$ are indeed harmful for secrecy. However, as λ_E grows large, the secrecy throughput increases. This is because, in this case, the eavesdropper will be in the sector secrecy guard zone, the transmitter emits AN to interfere with the eavesdropper, and the secrecy performance will be improved, which shows that AN can improve the secrecy throughput of the system. If λ_E further increases, the secrecy throughput starts to decrease; the reason is that, as the number of eavesdroppers in the sector secrecy guard zone increases, the wiretapping capability of eavesdroppers increases, which deteriorates the secrecy performance. Obviously, when eavesdroppers exist in the sector secure region, transmitting AN is effective, but there is an appropriate λ_E , which makes the secrecy throughput reach the maximum. This shows that increasing the density of eavesdroppers not always deteriorates the secrecy performance. In this case, the large sector secrecy guard zone is superior to the small one.

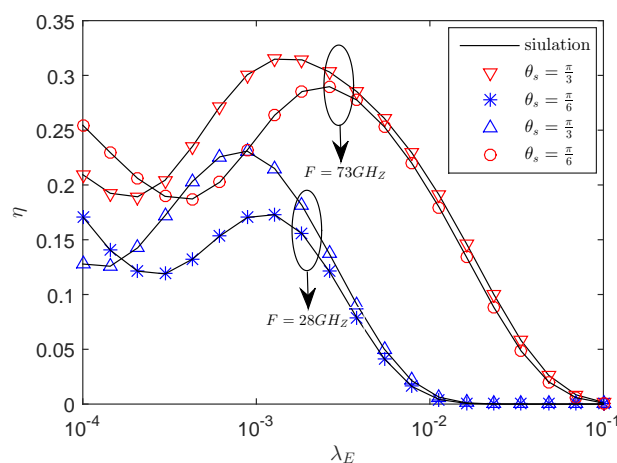


Figure 7. The η versus λ_E with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $P = 35$ dBm, $r = 50$ m, $\mu = 0.4$, $m_S = 0.1$ and $M_S = 200$.

Figure 8 presents the effects of transmit power allocation factor μ and the eavesdropper density λ_E on the secrecy throughput. From the simulation results, it shows that there exists an optimal transmit power allocation factor μ for maximizing the secrecy throughput with the changing λ_E . On the

other hand, when the power allocation factor is smaller, no matter how high λ_E is, the connection is interrupted, and the reliability of the system is not guaranteed. As both μ and λ_E are sufficiently high, the secrecy outage occurs and the security is not guaranteed. It reveals that the power allocation of the information signal and AN need to be properly set depending on different system parameters for increasing the secrecy throughput.

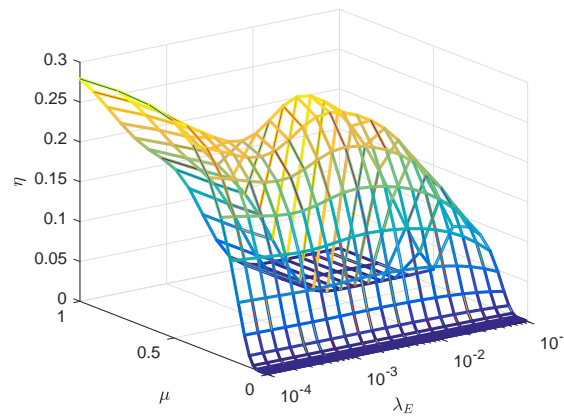


Figure 8. The η versus μ , λ_E with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $P = 30$ dBm, $F = 28$ GHz, $r = 50$ m, $\theta_S = \frac{\pi}{6}$, $m_S = 0.1$ and $M_S = 200$.

Figure 9 presents the effects of the η versus the blockage density β with different r_D . We observe that the secrecy throughput of $r = 80$ m is always superior to that of $r = 60$ m under the same system parameter settings. The reason is that, with the increase of r , if eavesdroppers exist in the sector secrecy guard zone and there is an appropriate λ_E , the transmitter will transmit AN interference to eavesdroppers, so the secrecy performance will be enhanced. In addition, increasing blocking intensity β does not always result in a strict decline in the secrecy throughput of mmwave wiretap networks. This shows that blockage plays an important role in the transmission of mmWave, which can be utilized to improve secrecy performance. From Figure 9, there exists an optimal β for maximizing the secrecy throughput at the different r . It is a meaningful conclusion that choosing sector secrecy guard zone according to the density of physical barriers and the distance of receiver can improve the secrecy throughput. As we improve β to the optimal point, the secrecy throughput attenuates, as NLOS communication dominates mmwave wiretap networks, using the multipath signals at the receiver. However, when the environment is full of physical obstacles, it is highly difficult for the message to reach the receiver, thus the secrecy throughput is gradually declining.

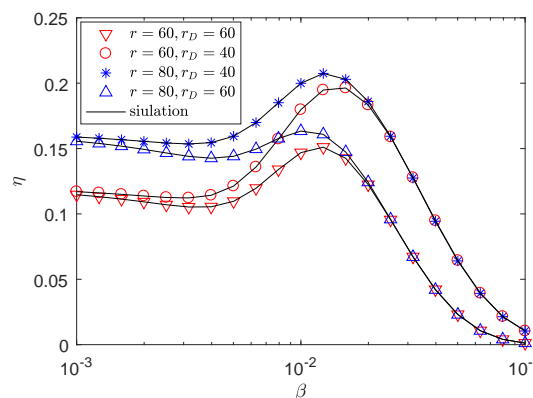


Figure 9. The η versus β , with $R_B = 1.5$ bps/Hz, $R_S = 0.5$ bps/Hz, $P = 35$ dBm, $F = 28$ GHz, $\lambda_E = 0.0002$ nodes/m², $\theta_S = \frac{\pi}{6}$, $\mu = 0.6$, $m_S = 0.1$ and $M_S = 200$.

6. Conclusions

In this paper, we investigated secrecy performance under the Nakagami fading channel in an mmWave wiretap network. Then, an adaptive transmission scheme according to the locations of eavesdroppers is adopted for secrecy transmission, and we derived the SOP, COP and secrecy throughput under stochastic geometry. Specifically, there exists an optimal transmission power for the direct transmission and an optimal power allocation factor for the AN-assisted transmission by maximizing secrecy throughput. When the system parameters are set properly, AN can improve the secrecy throughput of the system. We got a meaningful conclusion that choosing sector secrecy guard zone with a larger radius according to the density of physical barriers and the distance of receiver can improve the secrecy throughput. In addition, it provides an important perception into the interaction among the transmitting power, main-lobe gain and the mmWave frequency. In future works, complex scenarios such as imperfect CSI, base-station (BS) cooperation and nonorthogonal multiple access (NOMA) will be considered. Furthermore, the results presented here can be combined with unmanned aerial vehicle (UAV) to analyze secrecy transmission capability.

Author Contributions: Y.S., W.Y., Z.X., Y.L., and Y.C. conceived of the main proposal of the secure transmission schemes, conducted system modeling, and derived analysis and numerical simulation of the proposed schemes. Y.S. and W.Y. wrote the manuscript. Z.X. and Y.L. provided considerable comments and technique review of the proposed scheme and contributed to the revision of the paper. Y.C. read and approved the final manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant Nos. 61471393 and 61771487.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Pi, Z.; Khan, F. An Introduction to Millimeter-Wave Mobile Broadband Systems. *IEEE Commun. Mag.* **2011**, *49*, 101–107. [[CrossRef](#)]
- Rangan, S.; Rappaport, T.S.; Erkip, E. Millimeter Wave Cellular Wireless Networks: Potentials and Challenges. *Proc. IEEE* **2014**, *102*, 366–385. [[CrossRef](#)]
- Gong, S.; Xing, C.; Fei, Z.; Ma, S. Millimeter-Wave Secrecy Beamforming Designs for Two-Way Amplify-and-Forward MIMO Relaying Networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2059–2071. [[CrossRef](#)]
- Bai, T.; Alkhateeb, A.; Heath, R. Coverage and Capacity of Millimeter-Wave Cellular Networks. *IEEE Commun. Mag.* **2014**, *52*, 70–77.
- Bai, T.; Heath, R.W. Coverage Analysis for Millimeter Wave Cellular Networks with Blockage Effects. In Proceedings of the 2013 IEEE Global Conference on Signal and Information Processing, Austin, TX, USA, 3–5 December 2013; pp.727–730.
- Yang, W.; Tao, L.; Sun, X.; Ma, R.; Cai, Y.; Zhang, T. Secure On-Off Transmission in MmWave Systems with Randomly Distributed Eavesdroppers. *IEEE Access* **2019**, *7*, 32681–32692. [[CrossRef](#)]
- Liu, Y.; Chen, H.; Wang, L. Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 347–376. [[CrossRef](#)]
- Xiang, Z.; Yang, W.; Pan, G.; Cai, Y.; Song, Y. Physical Layer Security in Cognitive Radio Inspired NOMA Network. *IEEE J. Sel. Top. Signal Process.* **2019**, 1–14. [[CrossRef](#)]
- Tang, X.; Cai, Y.; Huang, Y.; Duong, T.; Yang, W. Secrecy Outage Analysis of Buffer-Aided Cooperative MIMO Relaying Systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 2035–2048. [[CrossRef](#)]
- Tang, X.; Cai, Y.; Deng, Y.; Huang, Y.; Yang, W. Energy-Constrained SWIPT Networks: Enhancing Physical Layer Security With FD Self-Jamming. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 212–222. [[CrossRef](#)]
- Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surv. Tuts* **2018**. [[CrossRef](#)]
- Khisti, A.; Wornell, G. Secure Transmission with Multiple Antennas II: The MIMOME Wiretap Channel. *IEEE Trans. Inf. Theory* **2010**, *56*, 3088–3104. [[CrossRef](#)]
- Sun, X.; Yang, W.; Cai, Y.; Tao, L.; Liu, Y.; Huang, Y. Secure Transmissions in Wireless Information and Power Transfer Millimeter Wave Ultra-dense Networks. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1817–1829. [[CrossRef](#)]

14. Xiang, Z.; Yang, W.; Pan, G.; Cai, Y.; Sun, X. Secure Transmission in Non-Orthogonal Multiple Access Networks with an Untrusted Relay. *IEEE Commun. Lett. (Early Access)* **2019**. [[CrossRef](#)]
15. Yang, N.; Yan, S.; Member, S.; Yuan, J.; Member, S.; Malaney, R.; Subramanian, R.; Land, I.; Member, S. Artificial Noise: Transmission Optimization in Multi-Input Single-Output Wiretap Channels. *IEEE Trans. Commun.* **2015**, *63*, 1771–1783. [[CrossRef](#)]
16. Li, W.; Ghogho, M.; Member, S.; Chen, B.; Xiong, C. Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis. *IEEE Commun. Lett.* **2012**, *16*, 1628–1631. [[CrossRef](#)]
17. Romero-zurita, N.; McLernon, D.; Ghogho, M.; Swami, A. PHY Layer Security Based on Protected Zone and Artificial Noise. *IEEE Signal Process. Lett.* **2013**, *20*, 487–490. [[CrossRef](#)]
18. Chae, S.H.; Member, S.; Choi, W.; Member, S.; Lee, J.H.; Quek, T.Q.S.; Member, S. Enhanced Secrecy in Stochastic Wireless Networks: Artificial Noise With Secrecy Protected Zone. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1617–1628. [[CrossRef](#)]
19. Xu, X.; He, B.; Yang, W.; Zhou, X.; Cai, Y. Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 373–387. [[CrossRef](#)]
20. Valliappan, N.; Heath, R.W.; Lozano, A. Antenna Subset Modulation for Secure Millimeter-wave Wireless Communication. *IEEE Trans. Commun.* **2013**, *61*, 3231–3245. [[CrossRef](#)]
21. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Renzo, M.D. Safeguarding 5G Wireless Communication Networks Using Physical Layer Security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [[CrossRef](#)]
22. Barati, C.N.; Hosseini, S.A.; Rangan, S.; Liu, P.; Korakis, T.; Panwar, S.S.; Rappaport, T.S. Directional Cell Discovery in Millimeter Wave Cellular Networks. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 6664–6678. [[CrossRef](#)]
23. Vuppala, S.; Biswas, S.; Ratnarajah, T. An Analysis on Secure Communication in Millimeter/Micro-Wave Hybrid Networks. *IEEE Trans. Commun.* **2016**, *64*, 3507–3519. [[CrossRef](#)]
24. Wang, L.; Elkashlan, M.; Duong, T.Q.; Heath, R.W. Secure Communication in Cellular Networks: The Benefits of Millimeter Wave Mobile Broadband. In Proceedings of the 2014 IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Toronto, ON, Canada, 22–25 June 2014.
25. Wang, C.; Wang, H.-M. Physical Layer Security in Millimeter Wave Cellular Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 5569–5585. [[CrossRef](#)]
26. Zhu, Y.; Wang, L.; Wong, K.-K.; Heath, R.W. Secure Communications in Millimeter Wave Ad Hoc Networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3205–3217. [[CrossRef](#)]
27. Ju, Y.; Wang, H.M.; Zheng, T.X.; Yin, Q. Secure Transmissions in Millimeter Wave Systems. *IEEE Trans. Commun.* **2017**, *65*, 2114–2127. [[CrossRef](#)]
28. Zhang, X.; Zhou, X.; McKay, M.R. Enhancing Secrecy with Multi-Antenna Transmission in Wireless Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1802–1814. [[CrossRef](#)]
29. Andrews, J.G.; Bai, T.; Kulkarni, M.; Alkhateeb, A.; Gupta, A.; Heath, R.W. Modeling and Analyzing Millimeter Wave Cellular Systems. *IEEE Trans. Commun.* **2017**, *65*, 403–430. [[CrossRef](#)]
30. Song, Y.; Yang, W.; Xiang, Z.; Cai, Y. Secure Transmission Design of Millimeter-Wave Wiretap Channel with Guard Zone and Artificial Noise. In Proceedings of the 2018 International Conference on Wireless Communications and Signal Processing (WCSP 2018), Hangzhou, China, 18–20 October 2018; pp. 1–6.
31. Adhikary, A.; Safadi, E.A.; Member, S.; Samimi, M.K.; Wang, R.; Caire, G.; Rappaport, T.S.; Molisch, A.F. Joint Spatial Division and Multiplexing for mm-Wave Channels. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1239–1255. [[CrossRef](#)]
32. Bai, T.; Heath, R.W. Coverage and Rate Analysis for Millimeter Wave Cellular Networks. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 1100–1114. [[CrossRef](#)]
33. Kong, L.; Vuppala, S.; Kaddoum, G. Secrecy Analysis of Random MIMO Wireless Networks Over α - μ Fading Channels. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11654–11666. [[CrossRef](#)]
34. Vuppala, S.; Tolossa, Y.J.; Kaddoum, G.; Abreu, G. On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks. *IEEE Trans. Commun.* **2018**, *66*, 1139–1152. [[CrossRef](#)]
35. Turgut, E.; Gursoy, M.C. Coverage in Heterogeneous Downlink Millimeter Wave Cellular Networks. *IEEE Trans. Commun.* **2017**, *65*, 4463–4477. [[CrossRef](#)]
36. Xu, X.; Yang, W.; Cai, Y.; Jin, S. On the Secure Spectral-Energy Efficiency Tradeoff in Random Cognitive Radio Networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 2706–2722. [[CrossRef](#)]

37. Tang, X.; Liu, R.; Spasojević, P.; Poor, V.H. On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-fading Channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 1575–1591. [[CrossRef](#)]
38. He, B.; Zhou, X.; Swindlehurst, A.L. On Secrecy Metrics for Physical Layer Security Over Quasi-Static Fading Channels. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6913–6924. [[CrossRef](#)]
39. He, B.; She, Y.; Lau, V.K.N. Artificial noise injection for securing single-antenna systems. *IEEE Trans. Veh. Technol.* **2017**, *66*, 9577–9581. [[CrossRef](#)]
40. Qin, H.; Sun, Y.; Chang, T.-H.; Chen, X.; Chi, C.-Y.; Zhao, M.; Wang, J. Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 2717–2729. [[CrossRef](#)]
41. Akitaya, T.; Asano, S.; Saba, T. Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems. In Proceedings of the 2014 IEEE International Conference on Communications Workshops (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 807–812.
42. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Academic Press: New York, NY, USA, 2007.
43. Baccelli, F.; Baszczyszyn, B. *Stochastic Geometry and Wireless Networks, Volume II: Applications*; Now Publishers Inc.: Hanover, MA, USA, 2009.
44. Haenggi, M.; Andrews, J.G.; Baccelli, F.; Dousse, O.; Franceschetti, M. Stochastic Geometry and Random Graphs for the Analysis and Design of Wireless Networks. *IEEE J. Sel. Areas Commun.* **2009**, *27*, 1029–1046. [[CrossRef](#)]
45. MacCartney, G.R.; Rappaport, T.S.; Sun, S.; Deng, S. Indoor Office Wideband Millimeter-wave Propagation Measurements and Channel Models at 28 and 73 GHz for Ultra-Dense 5G Wireless Networks. *IEEE Access* **2015**, *3*, 2388–2424. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).