IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received January 6, 2019, accepted January 18, 2019, date of publication March 13, 2019, date of current version March 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2898180

Secure On-Off Transmission in mmWave Systems With Randomly Distributed Eavesdroppers

WEIWEI YANG[1], (Member, IEEE), LIWEI TAO[1], XIAOLI SUN[1], RUIQIAN MA[1], YUEMING CAI[1], (Senior Member, IEEE), AND TAO ZHANG[2]

[1]College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]Sixty-Third Research Institute, National University of Defense Technology, Nanjing 210007, China

Corresponding author: Liwei Tao (liweitaoo@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61471393, Grant 61771487, and Grant 61801496, in part by the National University of Defense Technology Research Project under Grant ZK17-03-25, and in part by the National Postdoctoral Program for Innovative Talents of China under Grant BX20180374.

ABSTRACT To meet ever-increasing mobile data traffic demands for next-generation wireless communication systems, the plentiful spectrum resources in millimeter wave (mmWave) band have been exploited to improve the system capacity. This paper investigates physical layer security of mmWave systems with different secure on-off transmission strategies in the presence of randomly distributed eavesdroppers, including capacity threshold-based on-off scheme, secrecy guard zone on-off scheme and hybrid on-off scheme. Considering the effect of mmWave channel characteristics, random blockages and directional beamforming antenna gains, new closed-form expressions of system performance for each transmission scheme in terms of transmitting probability and secrecy outage probability have been derived under stochastic geometry framework. Then, the effects of various network parameters on secrecy performance, e.g., the density of eavesdroppers and blocking parameter, and the number of antennas and transmit power are validated. The numerical and analysis results show that the secure on-off schemes can effectively improve the secrecy performance of mmWave systems. Furthermore, for the capacity threshold-based on-off scheme and hybrid on-off transmission scheme, blocking is beneficial for improving secrecy performance significantly.

INDEX TERMS mmWave systems, secure on-off transmission, stochastic geometry.

I. INTRODUCTION

Due to the large available bandwidth in millimeter wave (mmWave) frequencies, it has become one of the key technologies to provide high-speed data rate in next generation wireless networks [1], [2]. A series of research on channel model, blockage model, coverage and rate in mmWave systems has been undertaken in recent years [3]–[5]. On the other hand, the openness of wireless channel results that the security and privacy issues need to be addressed in mmWave communications. Previous research has shown that physical layer security (PLS) technologies provide an effective solution to enhance security [6]–[9], and have great potential in mmWave communications [1], [10], [11].

A. BACKGROUND

Recently, PLS in mmWave systems has attracted widely interest [12]–[17], [19]. In [12], antenna subset modulation was designed to secure point-to-point mmWave communications by introducing randomness in the received constellation to confound the eavesdropper. Two secure transmission schemes based on phased array techniques were designed for mmWave vehicular communication systems in [13]. In order to enhance security, artificial noise and beamforming/precoding techniques have been employed in mmWave systems [14]–[17], [19]. Ramadan *et al.* [14] proposed an artificial noise aided hybrid precoding scheme to enhance PLS of mmWave multiple-input single-output (MISO) systems with partial channel knowledge. Reference [15] investigated secure hybrid precoder design in MISO systems under two types of channel knowledge at the transmitter. Two joint satellite/terrestrial base station digital beamforming schemes were designed for cognitive satellite terrestrial mmWave networks in the presence of one eavesdropper or multiple eavesdroppers in [16]. Three secure transmission schemes, namely maximum ratio transmitting beamforming, artificial noise beamforming and partial

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

maximum ratio transmitting beamforming, were proposed to improve secrecy performance of mmWave multiple-input multiple-output (MIMO) systems in [17]. Considering the application of amplify-and-forward (AF) relay technology [18], secure beamforming design for mmWave two-way AF MIMO relaying networks was investigated in [19].

However, these prior works mainly focus on the scenarios with determinate location and number of the eavesdroppers. In fact, on one hand, considering the eavesdroppers worked in a passive way generally, it is difficult to know the location and number of eavesdroppers. On the other hand, mmWave communications are sensitive to the blockages and experience higher propagation loss, which results that mmWave links are more random compared to that in low frequency band. Recently, stochastic geometry has provided an effective tool to model randomly distributed eavesdroppers, and achieved great success in random networks [20], [21]. In the presence of unknown eavesdroppers, which were modeled as homogeneous poisson point process (PPP), PLS on mmWave cellular networks [22], mmWave ad-hoc networks [23], [24] and hybrid micro/millimeter wave networks [25]–[27] have been studied in recent years. Reference [22] first studied the security of mmWave cellular networks with noise-limited and interference-limited. Especially, the artificial noise scheme was exploited to enhance secrecy performance in interference-limited networks. In mmWave ad-hoc networks, the average secrecy rate performance for artificial noise transmission has been analyzed in [24] and [25]. In addition, the secrecy outage performance of mmWave overlaid micro-wave networks was analyzed, where the intend user always associated to the best base station based on maximum received power association strategies in [25]–[27].

Besides exploiting beamforming/precoding [17], [19], artificial noise [22]–[24], and heterogeneous network architecture [25]–[27], there are also other PLS enhancement technologies, e.g., cooperative transmission, multi-user scheduling, on-off transmission, and so on [8], [9]. Specially, for on-off transmission, it has been proved to be an effective solution to improve secrecy performance in conventional sub-6GHz systems [28]–[32]. According to different sensing capability about channel state information (CSI) and eavesdroppers, various secure on-off transmission schemes were designed in existing literatures. A secure on-off transmission scheme based on signal-to-noise (SNR) of main channel was designed in [28], where the confidential information transmission takes place when the value of instantaneous SNR of main channel exceeds the given SNR threshold. In addition, assuming that the transmitter has the ability of detecting the nearby eavesdroppers, some researchers introduced the idea of secrecy guard zone to secure on-off transmission [29]–[31]. Reference [32] has designed threshold-based on-off scheme and secrecy guard zone on-off scheme to enhance the secrecy performance of cognitive networks. Especially, the hybrid on-off scheme which includes both the secrecy guard zone and the threshold-based on-off transmissions has been proposed in the work of [32], and in the hybrid on-off scheme, the secondary transmitter transmits only when there is no eavesdropper in the secrecy guard zone around the secondary transmitter and the received SNR at secondary receiver is larger than the threshold μ. However, most of above works mainly focused on secure on-off transmission design in conventional sub-6GHz systems.

B. MOTIVATION AND CONTRIBUTION

To the best of authors' knowledge, there are no works on secure on-off transmission design in mmWave systems in the presence of randomly distributed eavesdroppers. Different from the secure on-off schemes in sub-6GHz systems, some new challenges, i.e., blockages, directional transmission, and randomly distributed eavesdroppers, have to be addressed for mmWave secure on-off transmission design. In addition, under these new characteristics of mmWave channels, the secrecy performance need to be re-evaluated and the efficiency of secure on-off transmission technologies should be rechecked as well.

Our prior work [33] investigated capacity threshold-based secure on-off transmission scheme in mmWave systems, which focused on the focuses on secrecy performance differences in cooperative eavesdropping and non-cooperative eavesdropping scenarios. In addition, the recent research [34]exploited a sector secrecy guard zone protocol and a sector secrecy guard zone protocol with artificial noise scheme to enhance the secrecy performance. However, different from [33] and [34], we focus on the design of different secure on-off transmission schemes for improving secrecy performance, and besides capacity threshold-based on-off scheme and secrecy guard zone on-off scheme, we also have designed a hybrid on-off transmission scheme. And the hybrid protocol includes both the secrecy guard zone and the threshold-based transmissions, hence, is expected to have the best performance. Specially, considering that all eavesdroppers may successfully decode confidential information, even if the eavesdropper is located in the transmitter's side-lobe gain area, a full-plane secrecy guard zone on-off transmission scheme have been designed. These motivate us to investigate secure on-off transmission in mmWave systems in the presence of randomly distributed eavesdroppers.

In this paper, we investigate secure on-off transmission in mmWave systems where the transmitter sends confidential information to an intended receiver in the presence of PPP distributed eavesdroppers. According to different assumptions on the channel knowledge of the main channel and the detection capability on the eavesdroppers, three different secure on-off transmission schemes, named capacity threshold-based on-off scheme, secrecy guard zone on-off scheme and hybrid on-off scheme, have been discussed. For comparison, the secrecy performance of the conventional non-on-off transmission scheme is also given as a benchmark. The detail contributions are summarized as follows.

- Considering the effect of mmWave channel characteristics, random blockages, and directional antenna gains, we first investigated secure on-off transmission in mmWave systems in the presence of PPP distributed eavesdroppers and re-evaluated the efficiency of different secure on-off transmission schemes in mmWave frequency bands. Our results show that the secure on-off transmission schemes can effectively improve secrecy performance of mmWave systems.

- With the help of stochastic geometry framework, the novel closed-form expressions of system performance in terms of transmit probability (TP) and secrecy outage probability (SOP) for each on-off transmission scheme have been derived. And the impacts of key parameters such as the density of eavesdroppers and blockages, the number of antennas and the transmit power on secrecy performance are evaluated.
- Numerical and analysis results show that for capacity threshold-based on-off scheme and hybrid on-off transmission scheme, blocking is beneficial for improving secrecy performance significantly. However, increasing the blocking paremeter is harmful for secrecy outage probability in secrecy guard zone on-off scheme. In addition, different from secrecy guard zone on-off scheme, there is an optimal transmit power to achieve better secrecy outage performance in secure capacity threshold-based on-off and hybrid on-off transmission schemes.

The remainder of this paper is organized as follows. Section II gives the system model and performance metrics. Section III introduces three secure on-off transmission schemes, and the performance analysis is given in Sections IV. For comparison, the secrecy performance of conventional non-on-off transmission scheme has also given in Sections IV. Then Section V presents the numerical results. Finally, Section VI concludes the paper. In addition, a list of the fundamental variables is provided in Table I.

II. SYSTEM MODEL AND PERFORMANCE METRIC

A. SYSTEM MODEL

We consider a mmWave system, which consists of a transmitter equipped with directional beamforming antenna arrays of N antennas, a legitimate receiver and a group of randomly distributed eavesdroppers, as shown in Fig. 1, and the legitimate receiver and each eavesdropper are equipped with a single omnidirectional antenna.[1] In addition, the locations of eavesdroppers are modeled to follow an independent homogeneous PPP Φ_e with λ_e.

Similar to [22]–[24], a sectored antenna model of antenna pattern has been used in this paper, i.e.,

$$G_b(\theta) = \begin{cases} M_s, & \mathit{if}\ \theta \le \theta_b \\ m_s, & \mathit{Otherwise} \end{cases} \tag{1}$$

where M_s denotes the main-lobe gain with beamwidth θ_b and m_s denotes the side-lode gain.

TABLE 1. **List of fundamental variables.**

Φ_e	HPPP eavesdroppers
Φ_e^L	The inhomogeneous PPP eavesdroppers with LOS link
Φ_e^N	The inhomogeneous PPP eavesdroppers with NLOS link
$P_L(x)$	The probability of LOS link with distance x
$P_N(x)$	The probability of NLOS link with distance x
r_b	The communication distance between transmitter and legitimate receiver
γ_a	The channel gain at node a
$\lvert h\rvert^2$	The small-scale fading coefficient
$L(x)$	The path loss with distance x
$\Gamma(a,b)$	The upper incomplete Gamma function
N_L, N_N	The Nakagami fading parameter of LOS or NLOS link
C_L, C_N	The standard path-loss of LOS or NLOS link
α_L, α_N	The path-loss exponent of LOS or NLOS link
p_{tx}	The transmit probability
p_{so}	The secrecy outage probability
$1_{(condition)}$	The indicator function
R_S	The target secrecy rate
μ	A given threshold value
r	The radius of secrecy guard zone
$\beta(0,r)$	The secrecy guard zone
${}_2F_1(\alpha,\beta,\gamma,z)$	The Gauss hypergeometric function
$\gamma(a,b)$	The lower incomplete Gamma function

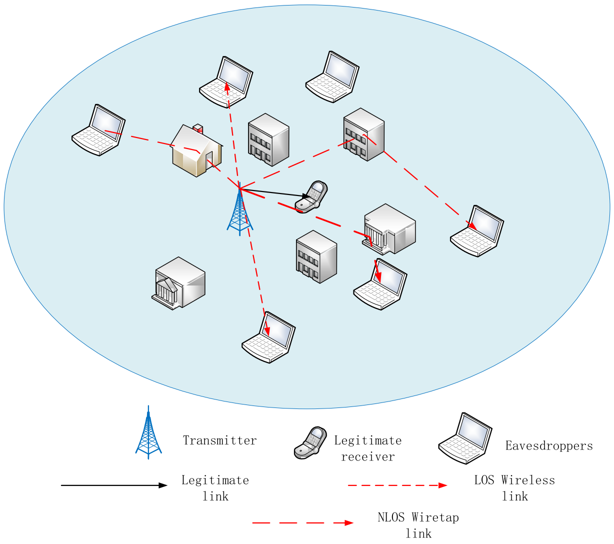


FIGURE 1. **The mmWave systems with randomly distributed multiple eavesdroppers.**

In this paper, we assume the transmitter has perfect CSI of the intended receiver, thus the transmitter can adjust steering orientation to achieve the maximum directivity gain [22]–[24]. In addition, due to the assumption of single omnidirectional antenna at the legitimate receiver and eavesdroppers [22], [37]–[39], so the antenna gains are only accounted for at the transmitter side. With the antenna pattern in (1), the antenna gain G_e seen by the eavesdropper is a Bernoulli random variable, whose probability mass function (PMF) is given by [24]

$$G_e = \begin{cases} M_s, & P(M_s) = \dfrac{\theta_b}{2\pi} \\ m_s, & P(m_s) = \dfrac{2\pi - \theta_b}{2\pi} \end{cases} \tag{2}$$

[1] This assumption has been widely adopted to research the mmWave systems in the existing literatures, e.g., [22], [37]–[39], the obtained analysis methods can be extended to the multiple antennas scenario directly.

In the outdoor mmWave scenario, the communication link may be the line-of-sight (LOS) or the non-line-of-sight (NLOS) link due to the presence of blocking. According to 3GPP standards and the blockage model with random shape theory [5], the probability of a LOS link with a communication distance l is given by $P_L(l) = e^{-\varsigma l}$, and the probability of a NLOS link is $P_N(l) = 1 - e^{-\varsigma l}$, where ς is a constant depending on the density and the average size of blockages.

Considering that the path-loss model presented in [22] and the small-scale fading of each mmWave link follows independent Nakagami-m fading, the channel gain of the intended receiver with the communication distance r_b and the arbitrary eavesdropper e with the communication distance r_e can be expressed as $\gamma_b = M_s|h_b|^2 L(r_b)$ and $\gamma_e = G_e|h_e|^2 L(r_e)$, respectively, where $|h_b|^2$ and $|h_e|^2$ follow independent Gamma distribution. Concretely, $|h_b|^2 \sim \Gamma\left(N_L, \frac{1}{N_L}\right)$ or $|h_e|^2 \sim \Gamma\left(N_N, \frac{1}{N_N}\right)$, where $\Gamma(a, b)$ is the incomplete Gamma function, and N_L/N_N are the Nakagami fading parameters of the LOS/NLOS link. And the path-loss function $L(l) = C_L l^{-\alpha_L}$ or $C_N l^{-\alpha_N}$ with a reference distance l is determined by LOS or NLOS link, respectively, where C_L/C_N and α_L/α_N are the path-loss parameters and path loss exponents in the LOS/NLOS link [5].

In this paper, we consider the passive eavesdropping scenario[2] and the CSI of wiretap channel isn't known by the transmitter. In addition, we focus on the non-cooperative eavesdropping case, where all eavesdroppers decode the information independently. For such case, we consider the most detrimental eavesdropper, which has the worst impact on secrecy performance. Hence, the channel gain at the most detrimental eavesdropper is

$$\gamma_{e^*} = \max_{e \in \Phi_e} \gamma_e \tag{3}$$

B. PERFORMANCE METRIC

In order to measure the system performance, the two important performance metric, which named TP and SOP [28], are exploited in this paper.

1) TRANSMIT PROBABILITY

Different from prior works [22]–[27], the transmitter is not always in the state of transmitting information due to exploiting secure on-off transmission. According to different secure on-off transmission schemes, the transmitter transmits the confidential information when the transmission condition is satisfied. Therefore, there exists a probability of information transmission referred to as TP, which is given by

$$p_{tx} = \mathbb{P}\left(1_{(condition)} = 1\right) \tag{4}$$

where $1_{(condition)}$ is the indicator function determined by different secure on-off transmission schemes, and it returns 1 when the condition holds, and 0 otherwise. For strictly delay-limited systems, $1 - p_{tx}$ represents the probability of a message packet being dropped. For delay-tolerant systems, p_{tx}^{-1} may give an indication of the average delay of transmission [28]. Obviously, the larger of TP, the better of delay performance, and on the contrary, the worse of delay performance.

2) SECRECY OUTAGE PROBABILITY

When the achievable secrecy rate C_S is less than a given target secrecy rate R_S, perfect security can't be guaranteed and the secrecy outage occurs. In particularly, for the secure on-off transmission schemes, the SOP is the probability of such outage events when information transmission occurs, which is defined as

$$\begin{aligned} p_{so} &= \mathbb{P}\left(C_S < R_S |\, 1_{(condition)} = 1\right) \\ &= \mathbb{P}\left([C_B - C_E]^+ < R_S \middle|\, 1_{(condition)} = 1\right) \end{aligned} \tag{5}$$

where $C_B = \log_2(1 + \rho\gamma_b)$, $C_E = \log_2(1 + \rho\gamma_{e^*})$, $\rho = P/\sigma^2$ is the average SNR, P denotes the transmit power, and σ^2 is the noise power. For simplicity, we assume that the legitimate receiver and all eavesdroppers have the same noise power, and the same assumption has also been used in [22]–[27].

III. SECURE ON-OFF TRANSMISSION SCHEMES

For the system described above, the different secure on-off transmission schemes are adopted to enhance secrecy performance in mmWave systems. According to the channel capacity of legitimate link and whether there are eavesdroppers in secrecy guard zone or not, three kinds of secure on-off transmission schemes are designed as follows.

A. CAPACITY THRESHOLD-BASED ON-OFF SCHEME

Assuming that the CSI of the intended receiver is available at the transmitter, the secure on-off transmission scheme can be designed based on the channel capacity of legitimate link. When only the channel capacity of legitimate link is larger than a given threshold μ, the transmitter transmits the confidential information to the intended receiver. It is worth noting that in order to guarantee security, we consider $\mu \geq R_S$ in this paper.

In the capacity threshold-based on-off transmission scheme, the channel gains of the intended receiver and the most detrimental eavesdropper can be expressed as

$$\gamma_b = M_s|h_b|^2 L(r_b)\, 1_{(C_1)} \tag{6}$$

$$\gamma_{e^*} = \max_{e \in \Phi_e} \left(G_e|h_e|^2 L(r_e)\right) 1_{(C_1)} \tag{7}$$

where $\{C_1 : C_B > \mu\}$ indicates the channel capacity C_B of legitimate link larger than the given threshold μ.

[2] Passive eavesdropping refers to malicious nodes try to intercept the security information of legitimate users, and malicious nodes keep silent and does not send any signal during passive eavesdropping, Therefore, it is not easy to be detected by legitimate users, and the security threat is more serious. Future work can trend to consider the smart attack [35], which concluding multiple attack types, such as eavesdropping, jamming and spoofing.

B. SECRECY GUARD ZONE ON-OFF SCHEME

In order to confront eavesdroppers who are closest to the transmitter, some scholars have introduced the idea of secrecy guard zone. That is to say, if the transmitter has ability of detecting the presence of eavesdroppers in a limited area, which can be achieved by metal detection, x-ray detection, enhancing thermal detection, local oscillator signal detection, and so on, the secrecy guard zone strategy can be adopted to enhance security [30]–[32]. The limited area modeled as a secrecy guard zone, which is a circle with center point of the transmitter and a radius of r.

In the secrecy guard zone on-off transmission scheme, the transmitter changes the state of 'off' to 'on' and transmits the confidential information to the intended receiver when there is no eavesdropper in the secrecy guard zone. Thus, the channel gains of the intended receiver and the most detrimental eavesdropper can be showed as

$$\gamma_b = M_s|h_b|^2 L(r_b)\, 1_{(C_2)} \tag{8}$$

$$\gamma_{e^*} = \max_{e\in\Phi_e}\left(G_e|h_e|^2 L(r_e)\right) 1_{(C_2)} \tag{9}$$

where $\{C_2 : r_e > r, \forall e \in \Phi_e\}$, and r_e is the distance between the transmitter and an eavesdropper e. Obviously, the distance between any eavesdropper and the transmitter is larger than the guard zone radius r if there is no eavesdropper in the secrecy guard zone. In addition, on one hand, it is obvious that the larger r can decrease the capacity of wiretap channel, and achieve the better secrecy performance. On the other hand, the large r means more higher complexity, and the transmitter needs to cost more resource to achieve the larger detection range.

C. HYBRID ON-OFF SCHEME

When the transmitter can know the CSI of legitimate link and also detect the presence of eavesdroppers in a limited area, the hybrid secure on-off transmission scheme, which is a joint capacity threshold-based and secrecy guard zone transmission strategy, can be exploited to enhance secrecy performance. The transmitter transmits only when both of the following conditions are satisfied: 1) there is no eavesdropper in the secrecy guard zone; 2) the received channel capacity at the intended receiver is larger than the threshold μ.

Thus, the condition that the transmitter transmits the confidential information to the intended receiver is given by $\{C_1\&C_2 : C_B > \mu \text{ and } r_e > r, \forall e \in \Phi_e\}$. Then, the channel gains of the intended receiver and the most detrimental eavesdropper can be given by

$$\gamma_b = M_s|h_b|^2 L(r_b)\, 1_{(C_1\&C_2)} \tag{10}$$

$$\gamma_{e^*} = \max_{e\in\Phi_e}\left(G_e|h_e|^2 L(r_e)\right) 1_{(C_1\&C_2)} \tag{11}$$

IV. PERFORMANCE ANALYSIS

In this section, we derive closed-form expressions of TP and SOP for above secure on-off transmission schemes in mmWave systems with randomly distributed eavesdroppers, and re-evaluated the efficiency of secure on-off transmission strategy in mmWave frequency bands. For comparison, the secrecy performance of the conventional non-on-off transmission scheme is also given as a benchmark.

A. TRANSMIT PROBABILITY ANALYSIS

1) CAPACITY THRESHOLD-BASED ON-OFF SCHEME

In this scheme, the transmitter transmits information only when the channel capacity of legitimate link is larger than a given threshold $\mu \in [R_S, \infty)$. Consequently, the TP is derived as

$$\begin{aligned} p_{tx}^{cts} &= \mathbb{P}(C_1 : C_B > \mu) \\ &= \mathbb{P}\left(\log_2(1+\rho\gamma_b) > \mu\right) \\ &= \sum_{i\in\{L,N\}} \mathbb{P}\left(|h_b|^2 > \frac{\beta_1}{M_s C_i r_b^{-\alpha_i}} \,|i\right) P_i(r_b) \\ &= \sum_{i\in\{L,N\}} \left(\frac{\Gamma\left(N_i, \frac{\beta_1 N_i}{M_s C_i r_b^{-\alpha_i}}\right)}{\Gamma(N_i)}\right) P_i(r_b) \end{aligned} \tag{12}$$

where $\beta_1 = \frac{2^\mu - 1}{\rho}$, and $P_i(l)$, $i \in \{L, N\}$, denotes the probability of LOS or NLOS link with distance l, respectively.

From (12), it can know that the TP is related to β_1, the communication distance r_b, the main beam gain M_s and the blockage parameter ς. The smaller β_1 can increase TP, which can be achieved by increasing the transmit power P or decreasing the transmission threshold μ. And the smaller r_b also can increase the TP performance. In addition, considering the characteristic of mmWave, the transmitter can configure large-scale antennas to achieve large narrow beam gain M_s, which can also increase TP. However, increasing the blocking parameter ς will decrease TP.

2) SECRECY GUARD ZONE ON-OFF SCHEME

In this scheme, the transmitter transmits only when there is no eavesdropper in the secrecy guard zone. We denote the location of the transmitter as the origin o, and the secrecy guard zone around the transmitter with radius r is denoted by $\beta(0, r)$. Thus, the closed-form expression of the TP can be derived as

$$\begin{aligned} p_{tx}^{sgzs} &= \mathbb{P}(C_2 :\ r_e > r, \forall e \in \Phi_e) \\ &= \mathbb{P}(N_e = 0) \\ &= e^{-\pi\lambda_e r^2} \end{aligned} \tag{13}$$

where N_e is the number of eavesdroppers in the secrecy guard zone $\beta(0, r)$.

It is easily to know that the guard zone radius r and the eavesdrop density λ_e have the significant effect on the TP. Specifically, the larger r and λ_e can decrease the TP performance in secrecy guard zone on-off transmission scheme.

3) HYBRID ON-OFF SCHEME

In this scheme, the transmitter transmits only when the channel capacity of the intended receiver is larger than a given threshold and there is no eavesdropper in the secrecy guard zone simultaneously. Thus, the TP is given by

$$\begin{aligned}p_{tx}^{hs} &= \mathbb{P}\left\{C_1\&C_2 : C_B > \mu \; and \; r_e > r, \forall e \in \Phi_e\right\}\\ &= \mathbb{P}\left(C_B > \mu\right)\mathbb{P}\left(N_e = 0\right)\\ &= e^{-\pi\lambda_e r^2}\sum_{i\in\{L,N\}}\left(\frac{\Gamma\left(N_i, \frac{\beta_1 N_i}{M_s C_i r_b^{-\alpha_i}}\right)}{\Gamma\left(N_i\right)}\right)P_i\left(r_b\right) \qquad (14)\end{aligned}$$

Similar to capacity threshold-based on-off scheme and secrecy guard zone on-off scheme, the TP in hybrid on-off scheme depends on P, μ, r_b, M_s, ς, r and λ_e. It can know that with increasing P and M_s or decreasing μ, r_b, ς, r and λ_e, the TP increases. Therefore, the large-scale antennas can increase the probability of information transmission, and the blocking decreases the probability of information transmission in mmWave systems with hybrid on-off scheme.

B. SECRECY OUTAGE PROBABILITY ANALYSIS

In this subsection, we derive the closed-form expressions of SOP in each transmission scheme, and some asymptotic properties also have been analyzed.

1) CAPACITY THRESHOLD-BASED ON-OFF SCHEME

In this scheme, utilizing the definition of the SOP given in (5), the SOP can be calculated as

$$\begin{aligned}p_{so}^{cts} &= \frac{\mathbb{P}(C_s < R_s, C_B > \mu)}{\mathbb{P}(C_B > \mu)}\\ &= \frac{\mathbb{P}\left(\gamma_{e^*} > \frac{\gamma_b-\beta_2}{T}, \gamma_b > \beta_1\right)}{\mathbb{P}(\gamma_b > \beta_1)}\\ &= \frac{\int_{\beta_1}^{\infty}\left(1 - F_{\gamma_{e^*}}\left(\frac{y-\beta_2}{T}\right)\right)f_{\gamma_b}\left(y\right)dy}{p_{tx}^{cts}} \qquad (15)\end{aligned}$$

where $T = 2^{R_S}$ and $\beta_2 = \frac{2^{R_S}-1}{\rho}$.

Due to the fact $\mu > R_S$, it is obvious that $\beta_1 > \beta_2$. Therefore, after the transformation of integral variable $x = \frac{y-\beta_2}{T}$, the SOP can be derived as

$$p_{so}^{cts} = 1 - \frac{T\int_{\frac{\beta_1-\beta_2}{T}}^{\infty} F_{\gamma_{e^*}}\left(x\right)f_{\gamma_b}\left(Tx+\beta_2\right)dx}{p_{tx}^{cts}} \qquad (16)$$

In order to obtain the closed-form expression of the SOP in (16), we need to derive the probability density function (PDF) of γ_b and the cumulative density function (CDF) of γ_{e^*}.

First, the CDF of γ_b is given as

$$\begin{aligned}F_{\gamma_b}\left(x\right) &= \mathbb{P}\left(\gamma_b < x\right)\\ &= \mathbb{P}\left(|h_b|^2 < \frac{x}{M_s L\left(r_b\right)}\right)\\ &= \sum_{i\in\{L,N\}}\mathbb{P}\left(|h_b|^2 < \frac{x}{M_s C_i r_b^{-\alpha_i}}\,|i\right)P_i\left(r_b\right)\\ &\overset{a}{=} \sum_{i\in\{L,N\}}\left(\frac{\gamma\left(N_i, \frac{xN_i}{M_s C_i r_b^{-\alpha_i}}\right)}{\Gamma\left(N_i\right)}\right)P_i\left(r_b\right) \qquad (17)\end{aligned}$$

where step (a) is based on the fact that $|h_b|^2$ follows Gamma distribution.

During taking the derivative of (17), the PDF of γ_b can be calculated as

$$f_{\gamma_b}\left(x\right) = \sum_{i\in\{L,N\}}P_i\left(r_b\right)\frac{\left(\frac{N_i}{M_s C_i r_b^{-\alpha_i}}\right)^{N_i}}{\Gamma\left(N_i\right)}x^{N_i-1}e^{-\frac{N_i x}{M_s C_i r_b^{-\alpha_i}}} \qquad (18)$$

Next, the CDF of γ_{e^*} can be calculated as follows

$$\begin{aligned}F_{\gamma_{e^*}}\left(x\right) &= \mathbb{P}\left(\gamma_{e^*} < x\right) = \mathbb{P}\left(\max_{e\in\Phi_e}\gamma_e < x\right)\\ &= \mathbb{P}\left(\max_{e\in\Phi_e} G_e|h_e|^2 L\left(r_e\right) < x\right)\\ &\overset{a}{=} \mathbb{P}\left(\max\left(\underset{e\in\Phi_e^L}{G_e|h_e|^2 L\left(r_e\right)}, \underset{e\in\Phi_e^N}{G_e|h_e|^2 L\left(r_e\right)}\right) < x\right)\\ &= \underbrace{\mathbb{P}\left(\max_{e\in\Phi_e^L}\left(G_e|h_e|^2 L\left(r_e\right)\right) < x\right)}_{\Xi_1}\\ &\quad\times\underbrace{\mathbb{P}\left(\max_{e\in\Phi_e^N}\left(G_e|h_e|^2 L\left(r_e\right)\right) < x\right)}_{\Xi_2} \qquad (19)\end{aligned}$$

where step(a) follows that all eavesdroppers can be divided into two independent inhomogeneous PPPs sets due to the blockage, and Φ_e^L and Φ_e^N denote the set of eavesdroppers with LOS and NLOS link, respectively.

Then, according to (7) and using the probability generating functional (PGFL) of the PPP [41], Ξ_1 can be derived as follows.

$$\begin{aligned}\Xi_1 &= \mathbb{P}\left(\max_{e\in\Phi_e^L}\left(G_e|h_e|^2 C_L r_e^{-\alpha_L}\right) < x\right)\\ &= \mathbb{E}\left\{\prod_{e\in\Phi_e^L}\mathbb{P}\left(|h_e|^2 < \frac{x r_e^{\alpha_L}}{G_e C_L}\middle|\Phi_e^L\right)\right\}\\ &= \exp\left(-\lambda_e\int_{R^2}\mathbb{P}\left(|h_e|^2 > \frac{x r_e^{\alpha_L}}{G_e C_L}\right)P_L\left(r_e\right)dR^2\right) \qquad (20)\end{aligned}$$

By relying on polar coordinates, Ξ_1 can be rewritten as

$$\begin{aligned}&\Xi_1\\ &= \exp\left(-\lambda_e\left(\int_{-\frac{\theta_b}{2}}^{\frac{\theta_b}{2}}\int_0^{\infty}\mathbb{P}\left(|h_e|^2 > \frac{x r_e^{\alpha_L}}{M_s C_L}\right)P_L\left(r_e\right)r_e d\theta dr_e\right.\right.\\ &\quad\left.\left.+\int_{\frac{\theta_b}{2}}^{2\pi-\frac{\theta_b}{2}}\int_0^{\infty}\mathbb{P}\left(|h_e|^2 > \frac{x r_e^{\alpha_L}}{m_s C_L}\right)P_L\left(r_e\right)r_e d\theta dr_e\right)\right)\end{aligned}$$

$$= \exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} \int_0^\infty P(V)\left(1-\frac{\gamma\left(N_L, \frac{N_L r_e^{\alpha_L} x}{VC_L}\right)}{\Gamma(N_L)}\right) \times e^{-\varsigma r_e} r_e dr_e\right) \tag{21}$$

where $P(V)$ is the probability mass function given in (2).

By invoking [40, eq.(8.354.1)] and [40, eq.(3.326.2)], we obtain

$$\begin{aligned}\Xi_1 &= exp\left(-2\pi\lambda_e\left(\int_0^\infty e^{-\varsigma r_e} r_e dr_e - \frac{1}{\Gamma(N_L)}\int_0^\infty \sum_{V\in\{M_s,m_s\}} \times \sum_{n=0}^{\infty}\frac{(-1)^n}{n!(N_L+n)}\left(\frac{N_L x}{VC_L r_e^{-\alpha_L}}\right)^{N_L+n} P(V)e^{-\varsigma r_e} r_e dr_e\right)\right)\\ &= \exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)\left(\frac{1}{\varsigma^2}-A_L(V)\right)\right)\end{aligned} \tag{22}$$

where $A_L(V) = \frac{\left(\frac{N_L x}{VC_L}\right)^{N_L}}{\Gamma(N_L)} \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{N_L x}{VC_L}\right)^n \Gamma(\alpha_L(N_L+n)+2)}{n!(N_L+n)\varsigma^{\alpha_L(N_L+n)+2}}$.

Similar to (20)-(22), Ξ_2 can be given by

$$\Xi_2 = \exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)\left(B(V)-\frac{1}{\varsigma^2}+A_N(V)\right)\right) \tag{23}$$

where $B(V) = \frac{\Gamma\left(\frac{2}{\alpha_N}+N_N\right)}{\frac{2}{\alpha_N}\left(\frac{N_N x}{VC_N}\right)^{\frac{2}{\alpha_N}}} {}_2F_1\left(1, \frac{2}{\alpha_N}+N_N, \frac{2}{\alpha_N}+1, 0\right)$, ${}_2F_1(\alpha,\beta,\gamma,z)$ is the Gauss hypergeometric function [40, eq.(9.100)], and

$$A_N(V) = \frac{\left(\frac{N_N x}{VC_N}\right)^{N_N}}{\Gamma(N_N)} \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{N_N x}{VC_N}\right)^n \Gamma(\alpha_N(N_N+n)+2)}{n!(N_N+n)\varsigma^{\alpha_N(N_N+n)+2}}.$$

Substituting Ξ_1 and Ξ_2 into (23), the CDF of γ_{e^*} can be computed as

$$F_{\gamma_{e^*}}(x) = \exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)(B(V)+A_N(V)-A_L(V))\right) \tag{24}$$

Substituting (18), (24) and (12) into (16), the closed-form expression of the SOP for capacity threshold-based on-off scheme can be obtained in (25), as shown at the top of the next page. From (25), it can know that the transmit power P, the eavesdropper density λ_e, the main beam gain M_s and the blockage parameter ς have a significant impact on the SOP.

Remark 1: When $P \to \infty$, it can be known that $p_{tx}^{cts} \to 1$ according to (12). Thus, the SOP $p_{so}^{cts} \to 1 - T\int_0^\infty F_{\gamma_{e^*}}(x) f_{\gamma_b}(Tx)dx$ for $P \to \infty$. This is a constant which has no relation with P and means that increasing P has no improvement on secrecy performance in such case.

2) SECRECY GUARD ZONE ON-OFF SCHEME

Denote $\tilde{\Phi}_e$ as the new location set of the eavesdroppers for the scenario where the transmission happens, i.e., no eavesdropper is inside the secrecy guard zone. The SOP for the secrecy guard zone scheme can be derived by following the similar step of (15), which is given by

$$\begin{aligned}p_{so}^{sgzs} &= \mathbb{P}\left(C_S < R_S \middle| 1_{(C_2)} = 1\right)\\ &= \mathbb{P}\left(C_S < R_S \middle| r_e > r, \forall e \in \tilde{\Phi}_e\right)\\ &= 1 - T\int_0^\infty F_{\tilde{\gamma}_{e^*}}(x) f_{\gamma_b}(Tx+\beta_2)\, dx\end{aligned} \tag{26}$$

where $\tilde{\gamma}_{e^*} = \max_{e^*\in\tilde{\Phi}_e}\left(G_e|h_e|^2 L(r_e)\right)$.

Similar to (19)-(24), all eavesdroppers in $\tilde{\Phi}_e$ also can be divided into two inhomogeneous PPPs due to the blockage. Therefore, the CDF of $\tilde{\gamma}_{e^*}$ can be computed as $F_{\gamma_{e^*}}(x) = \underbrace{\mathbb{P}\left(\max_{e\in\tilde{\Phi}_e^L}\left(\gamma_e^L\right) < x\right)}_{\Xi_3} \underbrace{\mathbb{P}\left(\max_{e\in\tilde{\Phi}_e^N}\left(\gamma_e^N\right) < x\right)}_{\Xi_4}$, where $\tilde{\Phi}_e^L$ and $\tilde{\Phi}_e^N$ are respectively independent homogeneous PPPs of eavesdroppers LOS and NLOS link outside the secrecy guard zone $\beta(0, r)$.

Then, Ξ_3 can be given as

$$\begin{aligned}\Xi_3 &= \mathbb{P}\left(\max_{e\in\tilde{\Phi}_e^L}\left(G_e|h_e|^2 L(r_e)\right) < x\right)\\ &= \mathbb{E}\left\{\prod_{e\in\tilde{\Phi}_e^L} \mathbb{P}\left(|h_e|^2 < \frac{x}{G_e C_L r_e^{-\alpha_L}} \middle| \tilde{\Phi}_e^L\right)\right\}\\ &\overset{a}{=} \exp\left(-\lambda_e \int_{R^2\backslash\beta(0,r)} \sum_{V\in\{M_s,m_s\}} \mathbb{P}\left(|h_e|^2 > \frac{x}{VC_L r_e^{-\alpha_L}} |V\right) \times P(V) P_L(r_e)\, dR^2\right)\\ &= \exp\left(-2\pi\lambda_e \int_r^\infty e^{-\varsigma r_e} r_e d_{r_e} - \frac{1}{\Gamma(N_L)}\int_r^\infty \sum_{V\in\{M_s,m_s\}} \times P(V)\gamma\left(N_L, \frac{xN_L}{VC_L r_e^{-\alpha_L}}\right) e^{-\varsigma r_e} r_e dr_e\right)\\ &\overset{b}{=} \exp\left(-2\pi\lambda_e \int_r^\infty e^{-\varsigma r_e} r_e d_{r_e} - \frac{1}{\Gamma(N_L)}\int_r^\infty \sum_{V\in\{M_s,m_s\}} \times \sum_{n=0}^{\infty}\frac{(-1)^n}{n!(N_L+n)}\left(\frac{N_L x}{VC_L r_e^{-\alpha_L}}\right)^{N_L+n} P(V)e^{-\varsigma r_e} r_e dr_e\right)\Bigg)\\ &\overset{c}{=} exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)\left(\varsigma^{-2}\Gamma(2,\varsigma r) - D_L(V)\right)\right)\end{aligned} \tag{27}$$

$$p_{so}^{ctx} = 1 - \frac{\sum_{i\in\{L,N\}} \left(\frac{\left(\frac{N_i}{M_s C_i r_b^{-\alpha_i}}\right)^{N_i}}{\Gamma(N_i)(TP_i(r_b))^{-1}} \int_{\frac{\beta_1-\beta_2}{T}}^{\infty} \exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)\left(B(V)+A_N(V)-A_L(V)\right)\right)(Tx+\beta_1)^{N_i-1} e^{-\frac{N_i(Tx+\beta_1)}{M_s C_i r_b^{-\alpha_i}}}\, dx \right)}{\sum_{i\in\{L,N\}} \left(\frac{\Gamma\left(N_i, \frac{\beta_1 N_i}{M_s C_i r_b^{-\alpha_i}}\right)}{\Gamma(N_i)} \right) P_i(r_b)} \tag{25}$$

$$\begin{aligned} p_{so}^{sgzs} &= 1 - \sum_{i\in\{L,N\}} \left(\frac{\left(\frac{N_i}{M_s C_i r_b^{-\alpha_i}}\right)^{N_i}}{\Gamma(N_i)(TP_i(r_b))^{-1}} \int_{0}^{\infty} \exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)\left(E(V)+D_N(V)-D_L(V)\right)\right)(Tx+\beta_1)^{N_i-1} e^{-\frac{N_i(Tx+\beta_1)}{M_s C_i r_b^{-\alpha_i}}}\, dx \right) \end{aligned} \tag{30}$$

where $D_L(V) = \sum_{n=0}^{\infty} \frac{(-1)^n \left(\frac{x}{VC_L}\right)^{N_L+n} \Gamma((N_L+n)\alpha_L+2, \varsigma r)}{n!(N_L+n)\varsigma^{(N_L+n)\alpha_L+2}}$, and step (a) follows the probability generating functional (PGFL) of PPP [41], and step (b) and step (c) are derived based on the expressions in [40, eq.(3.326.2)] and [40, eq.(3.515.2)], respectively.

Similarly, Ξ_4 can be given as

$$\begin{aligned} \Xi_4 = exp\Bigg(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)\,[E(V) \\ - \varsigma^{-2}\Gamma(2,\varsigma r) + D_N(V)]\Bigg) \end{aligned} \tag{28}$$

where $E(V) = \sum_{m=0}^{N_N-1} \left(\frac{\Gamma\left(m+\frac{2}{\alpha_N}, \frac{x}{VC_N} r^{\alpha}\right)}{\alpha_N \left(\frac{x}{VC_N}\right)^{\frac{2}{\alpha_N}}} \right)$ and $D_N(V) = \sum_{0}^{\infty} \frac{(-1)^n \left(\frac{x}{VC_N}\right)^{N_N+n}}{n!\Gamma(N_N)} \times \frac{\Gamma((N_N+n)\alpha_N+2, \varsigma r)}{(N_N+n)\varsigma^{(N_N+n)\alpha_N+2}}$.

Therefore, based on (27) and (28), the CDF of $\tilde{\gamma}_{e^*}$ is given by

$$\begin{aligned} F_{\tilde{\gamma}_{e^*}}(x) \\ = exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)[E(V)+D_N(V)-D_L(V)]\right) \end{aligned} \tag{29}$$

Finally, substituting (18) and (29) into (26), the closed-form expression of the SOP in secrecy guard zone on-off scheme can be derived as (30), shown at the top of this page. From (30), it can know that the transmit power P, the eavesdrop density λ_e, the main beam gain M_s and the blockage parameter ς have a significant impact on the SOP.

Remark 2: When $P \to \infty$, the SOP can be derived as $p_{so}^{sgzs} = 1 - T\int_0^{\infty} F_{\tilde{\gamma}_{e^*}}(x) f_{\gamma_b}(Tx)dx$, which also has no relation with P and means that increasing P has no improvement on secrecy performance for high P regime.

3) HYBRID ON-OFF SCHEME

Considering the effect of both channel capacity threshold and secrecy guard zone radius r, the SOP for the hybrid on-off scheme is derived as

$$\begin{aligned} p_{so}^{hs} &= \mathbb{P}\left(C_S < R_S \,\middle|\, 1_{(C_1\&C_2)} = 1\right) \\ &= \frac{\mathbb{P}\left(C_S < R_S, C_b > \mu, \forall e \in \tilde{\Phi}_e,\ r_e > r\right)}{\mathbb{P}\left(C_b > \mu, \forall e \in \tilde{\Phi}_e,\ r_e > r\right)} \\ &\overset{a}{=} 1 - \frac{T\int_{\frac{\beta_1-\beta_2}{T}}^{\infty} F_{\tilde{\gamma}_{e^*}}(x) f_{\gamma_b}(Tx+\beta_2)\, dx}{p_{tx}^{cts}} \end{aligned} \tag{31}$$

where step (a) follows the fact that $\mu > R_S$. According to hybrid on-off scheme, $F_{\tilde{\gamma}_{e^*}}(x)$ is same as (29) in secrecy guard zone on-off scheme, and $f_{\gamma_b}(x)$ is same as (18) in capacity threshold-based on-off scheme, respectively.

Thus, the final expression p_{so}^{hs} can be obtained by using $E(V)$, $D_N(V)$ and $D_L(V)$ to substitute $B(V)$, $A_N(V)$ and $A_L(V)$ in (25), respectively.

Remark 3: It is worth noting that the result in hybrid on-off scheme can degraded into other two secure on-off transmission schemes. When $\mu \to 0$, the result can be degraded into (30) for the secrecy guard zone scheme. If $r \to 0$, the result can be degraded into (25) as the capacity threshold-based scheme. Furthermore, when $\mu \to 0$ and $r \to 0$ simultaneously, $p_{tx}^{hs} \to 1$, the result can be degraded into the result for conventional non-on-off transmission scheme.

C. NON-ON-OFF SCHEME

In order to make a comparison with the proposed secure on-off transmission schemes, we also give the TP and SOP in conventional non-on-off transmission scheme, in which

TABLE 2. Antenna parameters of uniform planar square antenna [43].

Number of antenna elements	N
Half-power beamwidth θ	$\frac{\sqrt{3}}{N}$
Main-lobe gain	N
Side-lobe gain	$\frac{\sqrt{N}-\frac{\sqrt{3}}{2\pi}N\sin\left(\frac{\sqrt{3}}{2\sqrt{N}}\right)}{\sqrt{N}-\frac{\sqrt{3}}{2\pi}\sin\left(\frac{\sqrt{3}}{2\sqrt{N}}\right)}$

the transmitter always transmits the message to the intended receiver whether or not the channel capacity exceeds some given threshold or there are no eavesdroppers in the guard zone. Obviously, the TP in non-on-off transmission scheme is $p_{tx}^{non} = 1$.

In the non-on-off transmission scheme, the SOP is defined as $p_{so} = \mathbb{P}\left([C_B - C_E]^+ < R_S\right)$. Therefore, the SOP in non-on-off transmission scheme can be given as

$$p_{so}^{non} = 1 - T\int_0^\infty F_{\gamma_{e*}}(x) f_{\gamma_b}(Tx+\beta_1)\,dx \tag{32}$$

where $F_{\gamma_{e*}}(x)$ is given by (24) and $f_{\gamma_b}(x)$ is given by (18).

Similar to the derivation process of p_{so}^{ctx}, the SOP in conventional non-on-off transmission scheme can be evaluated as (33), shown at the bottom of this page.

V. SIMULATION RESULTS

In this section, some numerical results are provided to illustrate the effects of the system parameters on the system performance. We assume that the carrier frequency $F_c = 28\ GHz$, the transmission bandwidth $BW = 2\ GHz$, the noise figure $\mathcal{F}_{dB} = 10dB$, and the noise power is $\sigma^2(dBm) = -174 + 10\log 10(BW) + \mathcal{F}_{dB}$. In addition, the Nakagami fading parameter of the LOS (NLOS) link is $N_L = 3$ ($N_N = 2$), and the parameters of path-loss model are $\beta_L = 61.4\ dB$, $\alpha_L = 2$, $C_L = 10^{-\frac{\beta_L}{10}}$, $\beta_N = 72\ dB$, $\alpha_N = 2.92$, and $C_N = 10^{-\frac{\beta_N}{10}}$ [22]. We consider the uniform planar square array (UPA) with the antenna pattern showed in Table 1 [43], and the transmitting node is equipped with N antennas. As can be readily seen from these figures, the analytical results are in exact agreement with the Monte Carlo simulations.

Fig. 2 plots the TP of the capacity threshold-based on-off transmission scheme and hybrid on-off transmission scheme with different communication distance r_b versus the threshold μ. For comparison, the transmit probability of non-on-off transmission scheme also is drawn in Fig. 2. The results illustrate that the transmit probability in non-on-off transmission scheme is always one because the transmitter always transmits the message to the intended receiver. And it is obvious that increasing μ can decrease the transmit probability for capacity threshold-based on-off and hybrid on-off transmission schemes. For a given threshold μ, the transmit probability of the two secure on-off transmission schemes will decrease with increasing the communication distance r_b due to the channel gain γ_b of the intended receiver decreasing.

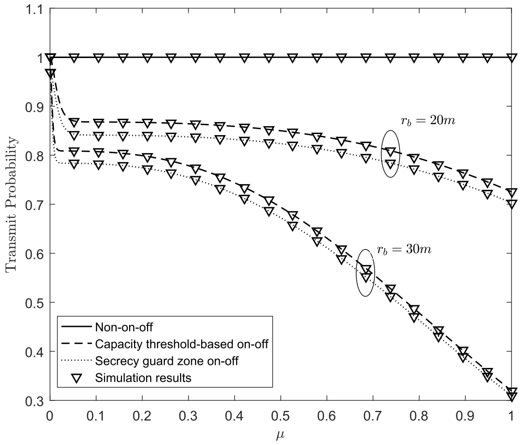


FIGURE 2. The TP as a function of the threshold ($N = 30$, $P = 35dBm$, $\lambda_e = 10^{-3}$, $r = 10m$).

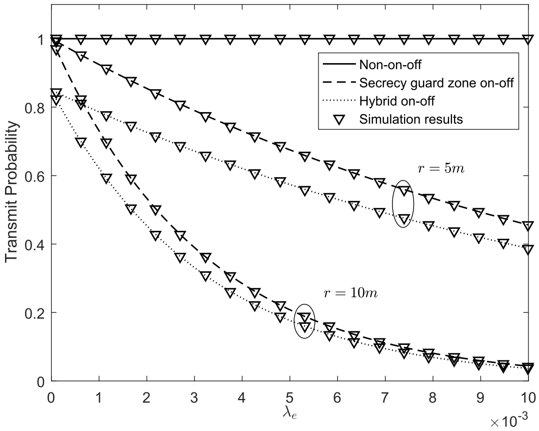


FIGURE 3. The TP as a function of the density of eavesdroppers ($N = 30$, $P = 35dBm$, $r_b = 20m$, $\mu = 0.5$).

Fig. 3 shows the TP of the secrecy guard zone on-off scheme and hybrid on-off transmission scheme with different guard zone radius r versus the eavesdropper density λ_e. It can be observed that increasing λ_e can decrease the transmit probability for a given guard zone radius r. This is because the probability that there is no eavesdropper in this secure guard zone will reduce with increasing of λ_e, which decreases the probability of information transmission. In addition, it is obviously that the transmit probability performance of hybrid

$$p_{so}^{non} = 1 - \sum_{i\in\{L,N\}} \left(\frac{\left(\frac{N_i}{M_s C_i r_b^{-\alpha_i}}\right)^{N_i}}{\Gamma(N_i)(TP_i(r_b))^{-1}} \int_0^\infty \exp\left(-2\pi\lambda_e \sum_{V\in\{M_s,m_s\}} P(V)(B(V)+A_N(V)-A_L(V))\right)(Tx+\beta_1)^{N_i-1} e^{-\frac{N_i(Tx+\beta_1)}{M_s C_i r_b^{-\alpha_i}}}\,dx \right) \tag{33}$$

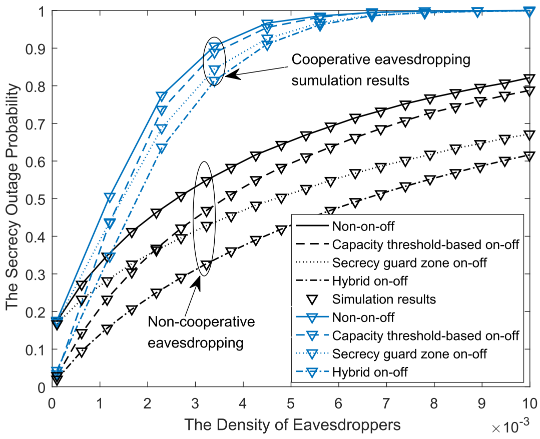


FIGURE 4. The SOP as a function of the density of eavesdroppers ($N = 30$, $P = 35dBm$, $\mu = 0.5$, $r = 10m$, $\varsigma = 1/141.4$).

on-off transmission scheme is the worst because the transmitter transmits only when the channel capacity of the intended receiver is larger than the threshold μ and there is no eavesdropper in the secrecy guard zone simultaneously.

Fig. 4 illustrates the SOP in different transmission schemes versus the eavesdropper density λ_e. Specially, in order to compare the secrecy performance of non-cooperative eavesdropping with that of cooperative eavesdropping scenario, we give the simulation results of cooperative eavesdropping scenario. As can be expected, with the increasing of λ_e, the SOP increases in all schemes. Because the larger λ_e implies that more eavesdroppers intercept the information transmission. The SOP is the worst in non-on-off transmission scheme and the best in hybrid on-off transmission scheme for a fixed λ_e. This shows that the secure on-off transmission scheme can effectively improve the secrecy performance, and the hybrid on-off transmission scheme has the best secrecy outage performance. For the capacity threshold-based on-off and secrecy guard zone on-off transmission schemes, the secrecy outage performance is related to the secrecy threshold μ and the radius of guard zone r, respectively. Therefore, the network parameter can be carefully designed to achieve the secrecy performance. In addition, from the simulation results of cooperative eavesdropping scenario, it can be known that the similar conclusions can be obtained. But the secrecy performance in cooperative eavesdropping scenario is worse, this is because that eavesdroppers in cooperative eavesdropping scenario can share information with each other, which makes eavesdropping more successful. Therefore, it poses a greater threat to the security of the system.

Fig. 5 presents the impact of the density of blockage ς on the SOP of the considered system. With the increase of ς, the SOP performance is improved in the capacity threshold-based on-off and hybrid on-off transmission schemes and is declined in other two schemes. This is because increasing the value of ς, the probability of having LOS propagation paths falls down, and the NLOS communication dominates the mmWave network, exploiting the multipath signals at the receiver. Therefore, on the one hand, increasing the value of ς, the TP will decrease in capacity threshold-based and hybrid on-off transmission schemes, but no influence on non-on-off and secrecy guard zone transmission schemes. On the other hand, the large value of ς decreases the channel capacity of main channel and wiretap channel simultaneously, and in the definition of secrecy outage probability, the change of the SOP determined by how much of the improvement in main channel and wiretap channel capacity. The results illustrate that increasing the blocking parameter is beneficial for improving secrecy outage performance in the capacity threshold-based on-off and hybrid on-off transmission schemes. And the blockage is harmful for the non-on-off transmission and secrecy guard zone on-off schemes. This is a significant conclusion for enhancing secrecy outage performance by adjusting the density and average size of the buildings in the capacity threshold-based on-off and hybrid on-off transmission schemes.

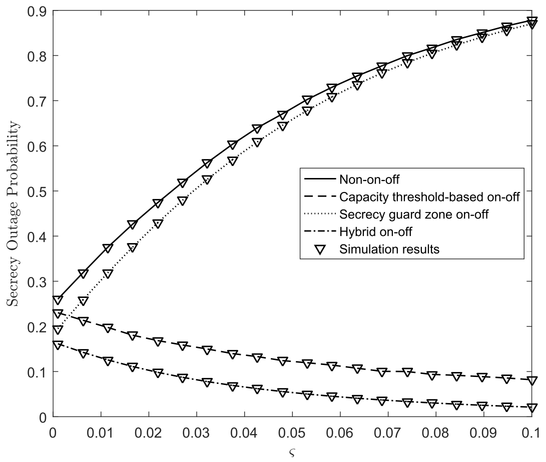


FIGURE 5. The SOP as a function of the blocking parameter ($N = 30$, $P = 35dBm$, $\mu = 0.5$, $r = 10m$, $\lambda_e = 10^{-3}$).

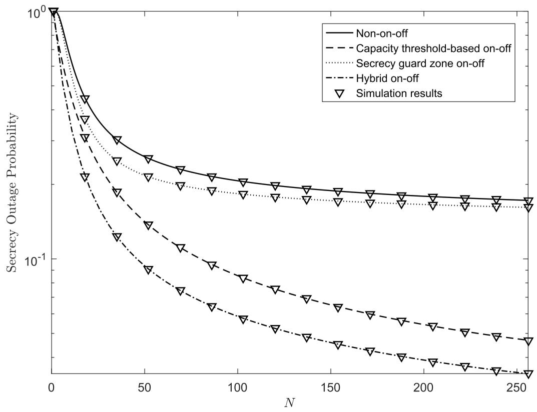


FIGURE 6. The SOP as a function of the number of antennas ($P = 35dBm$, $\mu = 0.5$, $r = 10m$, $\varsigma = 1/141.4$, $\lambda_e = 10^{-3}$).

Fig. 6 shows the SOP of different on-off transmission schemes versus the number of antennas N. With increasing of N, the SOP decreases in all schemes. This is because that more antennas can make a narrower beam to aim at the intended receiver, which would make litter eavesdroppers can

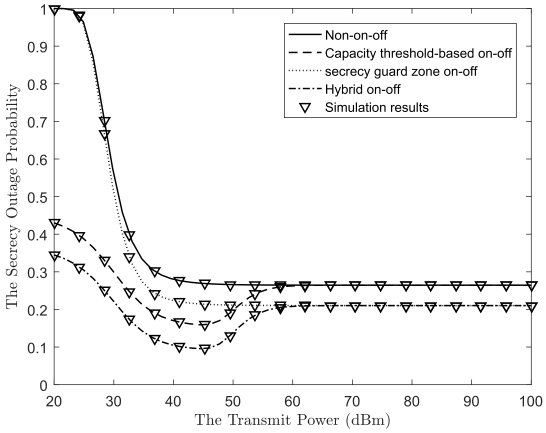


FIGURE 7. **The SOP as a function of the transmit power ($N = 30$, $\mu = 0.5$, $r = 10m$, $\varsigma = 1/141.4$, $\lambda_e = 10^{-3}$).**

fall in the beam. Moreover, the directional antenna gains is larger with the increasing of N. Therefore, we can improve secrecy performance by configuring more antennas.

Fig. 7 shows the effect of the transmit power P on the SOP in the different transmission schemes. In the non-on-off transmission scheme and secrecy guard zone on-off scheme, the SOP keeps decreasing until reaches a constant value. However, It can be observed that for capacity threshold-based on-off and hybrid on-off schemes, increasing P makes the SOP first decreases and then increases, and finally keep constant. This is because increasing P is beneficial for main channel and wiretap channel simultaneously. Especially, the result indicates that there is an optimal P to achieve the best secrecy performance in capacity threshold-based on-off and hybrid on-off schemes.

VI. CONCLUSION

In this paper, we concentrated on the secure on-off transmission in mmWave systems with homogeneous PPP distributed eavesdroppers. The novel expressions of transmit probability and secrecy outage probability are derived under considering the effect of mmWave channel characteristics, random blockages, and directional beamforming antenna gains. Our results show that the secure on-off transmission can effectively enhance the secrecy performance. Another interesting finding is that blocking is beneficial for improving secrecy performance in the capacity threshold-based on-off and hybrid on-off transmission schemes. Furthermore, increasing transmit power P does not always improve the secrecy performance, and the SOP will reach a constant floor when the P is large enough. However, there exists an optimal P to provide the best secrecy performance in the the capacity threshold-based on-off and hybrid on-off transmission schemes.

REFERENCES

[1] 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.

[2] M. Xiao *et al.*, "Millimeter wave communications for future mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 1909–1935, Sep. 2017.

[3] T. Bai and R. W. Heath, Jr., "Coverage analysis for millimeter wave cellular networks with blockage effects," in *Proc. IEEE Global Conf. Signal Inf. Process. (GLobalSIP)*, Dec. 2013, pp. 727–730.

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

[5] J. G. Andrews, T. Bai, M. N. Kulkarni, A. Alkhateeb, A. K. Gupta, and R. W. Heath, Jr., "Modeling and analyzing millimeter wave cellular systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 403–430, Jan. 2017.

[6] W. Yang, W. Mou, X. Xu, W. Yang, and Y. Cai, "Energy efficiency analysis and enhancement for secure transmission in SWIPT systems exploiting full duplex techniques," *IET Commun.*, vol. 10, no. 14, pp. 1712–1720, Sep. 2016.

[7] X. Lai, L. Fan, X. Lei, J. Li, N. Yang, and G. K. Karagiannidis, "Distributed secure switch-and-stay combining over correlated fading channels," *IEEE Trans. Inf. Forensics Security*, to be published.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[9] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[10] 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.

[11] Y. Huang, J. Zhang, and M. Xiao, "Constant envelope hybrid precoding for directional millimeter-wave communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 845–859, Apr. 2018.

[12] N. Valliappan, A. Lozano, and R. W. Heath, Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[13] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, Jr., "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8139–8151, Sep. 2017.

[14] Y. R. Ramadan, H. Minn, and A. S. Ibrahim, "Hybrid analog–digital precoding design for secrecy mmWave MISO-OFDM systems," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 5009–5026, Nov. 2017.

[15] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmWave MISO systems with partial channel knowledge," *IEEE Signal Process. Lett.*, vol. 24, no. 11, pp. 1729–1733, Nov. 2017.

[16] M. Lin, Z. Lin, W.-P. Zhu, and J.-B. Wang, "Joint beamforming for secure communication in cognitive satellite terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 5, pp. 1017–1029, May 2018.

[17] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, May 2017.

[18] L. Fan, N. Zhao, X. Lei, Q. Chen, N. Yang, and G. K. Karagiannidis, "Outage probability and optimal cache placement for multiple amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12373–12378, Dec. 2018.

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

[20] Y. Cai, X. Xu, and W. Yang, "Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise," *IET Commun.*, vol. 10, no. 15, pp. 1904–1913, Oct. 2016.

[21] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706–2722, Oct. 2016.

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

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

[24] Y. Zhu, L. Wang, K. K. 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.

[25] S. Vuppala, S. Biswas, T. Ratnarajah, and M. Sellathurai, "Analysis of secure communication in millimeter wave networks: Are blockages beneficial?" in *Proc. IEEE ICASSP*, Mar. 2016, pp. 2169–2173.

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

[27] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1139–1152, Mar. 2018.

[28] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[29] M. A. Kishk and H. S. Dhillon, "Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 394–397, Jun. 2017.

[30] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[31] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

[32] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 373–387, Feb. 2017.

[33] L. Tao, W. Yang, W. Yang, X. Yang, and C. Cai, "Capacity threshold-based on-off transmission in mmWave systems with randomly distributed eavesdroppers," in *Proc. 10th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Hangzhou, China, 2018, pp. 1–6.

[34] Y. Song, W. Yang, Z. Xiang, and Y. Cai, "Secure transmission design of millimeter-wave wiretap channel with guard zone and artificial noise," in *Proc. 10th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Hangzhou, China, Oct. 2018, pp. 1–6.

[35] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting secure communication under UAV smart attack with imperfect channel estimation," *IEEE Access*, vol. 6, pp. 76395–76401, 2018.

[36] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2018.

[37] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, Jr., "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *Proc. IEEE Signal Process. Adv. Wireless Commun. (SPAWC)*, Toronto, ON, Canada, Jun. 2014, pp. 115–119.

[38] 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.

[39] H. Elshaer, M. N. Kulkarni, F. Boccardi, and J. G. Andrews, "Downlink and uplink cell association with traditional macrocells and millimeter wave small cells," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6244–6258, Sep. 2016.

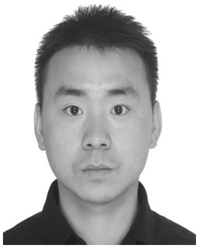
[40] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[41] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[42] 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.

[43] K. Venugopal, M. C. Valenti, and R. W. Heath, Jr., "Device-to-device millimeter wave communications: Interference, coverage, rate, and finite topologies," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6175–6188, Sep. 2016.

WEIWEI YANG (S'08–M'11) received the B.Sc., M.Sc., and Ph.D. degrees in telecommunications from the PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively. He is currently an Associate Professor with the College of Communication Engineering, Army Engineering University of PLA. He has co-authored the book *Handbook of Cognitive Radio* (Springer, 2017). His research interests include cooperative communications, cognitive radio, and physical layer security. He served as a TPC members of WCSP 2011/2014/2017/2018, GC 2016 Workshops, GC 2017 Workshops, and ICC 2016-Workshops. He was a co-recipient of the Best Paper Award from WCSP 2011. He also served as a Publication Co-Chair of WCSP 2015 and a Track Chairs of IEEE CIC ICCC 2017, and WCSP 2015.



LIWEI TAO received the B.S. degree from the University of Electronic Science and Technology of China, in 2016, and the M.S. degree from the Army Engineering University of PLA, in 2017, where he is currently pursuing the Ph.D. degree in communications and information system with the Institute of Communications Engineering. His research interests include physical layer security, cellular networks, and millimeter wave communication.

XIAOLI SUN received the B.S. and M.S. degrees from the PLA University of Science and Technology, in 2014 and 2017, respectively. She is currently pursuing the Ph.D. degree in communications and information system with the Institute of Communications Engineering, Army Engineering University of PLA. Her research interests include physical layer security, relaying networks, millimeter wave communication, and UAV communication.

RUIQIAN MA received the B.S. degree from the University of Electronic Science and Technology of China, in 2017. He is currently pursuing the M.S. degree in communications and information system with the Institute of Communications Engineering, Army Engineering University of PLA. His research interests include physical layer security, relaying networks, and millimeter wave communication.

YUEMING CAI (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982, and the M.S. degree in microelectronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively. His current research interests include MIMO systems, OFDM systems, signal processing in communications, cooperative communications, and wireless sensor networks.

TAO ZHANG received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011 and 2016, respectively. Since 2017, he has been an Engineer with the Sixty-Third Research Institute, National University of Defense Technology, Nanjing. His current research interests include cooperative communications, wireless sensor networks, physical layer security, and cognitive radio systems.