Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 3178335, 14 pages
https://doi.org/10.1155/2023/3178335

Research Article

Analysis of Eavesdropping Region in Hybrid mmWave-Microwave Wireless Systems

Qianyue Qu,[1] **Yuanyu Zhang**,[2,3] **and Shoji Kasahara**[1]

[1]*Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma, Japan*
[2]*School of Computer Science and Technology, Xidian University, Xi'an, China*
[3]*Shannxi Key Laboratory of Network and System Security, Beijing Sunwise Information Technology Ltd, Beijing, China*

Correspondence should be addressed to Yuanyu Zhang; yyuzhang@xidian.edu.cn

Received 5 January 2023; Revised 24 April 2023; Accepted 31 May 2023; Published 2 September 2023

Academic Editor: Kechen Zheng

Hybrid communication systems, where millimeter-wave (mmWave) links coexist with microwave links, have been an essential component in the fifth-generation (5G) wireless networks. Nevertheless, the open feature of the wireless medium makes hybrid systems vulnerable to eavesdropping attacks. Eavesdroppers in hybrid communication systems can enhance their attack performance by opportunistically eavesdropping on mmWave or microwave links. This paper, therefore, aims to answer a natural question: in which region do eavesdroppers prefer the mmWave links? To this end, we first formulate this question as an eavesdropping region characterization problem from the physical layer security perspective, where eavesdroppers select the link to eavesdrop based on the ratio between the security performances of the mmWave and microwave links. To model the security performances of both the mmWave and microwave links, we derive closed-form expressions for the secrecy outage probabilities and lower bounds/exact expressions for the secrecy rates of both links. Finally, we provide numerical results to validate our theoretical analysis and also illustrate the mmWave eavesdropping region under various network parameter settings.

1. Introduction

In the past decade, the number of wireless devices is increasing exponentially, leading to a critical spectrum scarcity issue in current wireless communication systems. One of the promising solutions is to transmit information over the much wider millimeter-wave (mmWave) frequency band for significantly improved capacity and increased data rate in the fifth-generation (5G) wireless networks [1, 2]. Despite the great capacity and high data rate, mmWave communication suffers from high signal attenuation when mmWave signals encounter obstacles [3]. In this case, users may choose to transmit over conventional microwave links. Therefore, hybrid wireless communication systems, where the mmWave links coexist with microwave links, are expected to be a typical component in the ongoing 5G era [4].

However, due to the open nature of the wireless medium, hybrid communication systems are also vulnerable to eavesdropping attacks like other wireless systems [5–7]. Recent research has shown that the emerging physical layer security (PLS) technology can achieve a stronger form of security with less computational cost [8, 9]. The key idea of the PLS technology is to exploit physical layer characteristics of wireless channels (e.g., fading and noise) to ensure that almost no information is leaked to eavesdroppers [10]. Moreover, the PLS technology can be combined with existing cryptographic methods to provide a critical security solution that can combat eavesdropping attacks [11, 12].

Motivated by the benefits of the PLS technology, extensive research efforts have been devoted to the PLS performance analysis and/or PLS scheme design in wireless communication systems [13–23]. For instance, Zhu et al. [15] explored the potential of PLS in mmWave ad hoc networks. Zhang et al. [16] proposed a sight-based cooperative jamming scheme to improve the PLS performance of mmWave ad hoc networks. Zhang et al. [17] examined the problem of mode selection and spectrum partition in cellular networks with inband device-to-device communication. Some authors analyzed the PLS performance of nonorthogonal multiple access networks [18]. In addition, some researchers discussed the joint resource allocation of artificial noise-assisted multiuser wiretap orthogonal frequency division multiplexing channel [20]. The optimization problem of wireless communication systems with intelligent reflecting surfaces was addressed by Chen et al. [21], Makarfi et al. [22], Shen et al. [23].

Recently, the PLS performance analysis of hybrid wireless communication systems has also attracted considerable attention [24–29]. Tokgoz et al. [24] investigated the hybrid free-space optical (FSO) and mmWave wireless system from the perspective of PLS, and different fading channels were considered for FSO and mmWave links, respectively. Vuppala et al. [25, 26] analyzed the performance of mmWave-overlaid microwave cellular networks. They developed a mathematical framework to analyze the connection outage probability, secrecy outage probability (SOP), and achievable secrecy rate of the hybrid mmWave network. Umer et al. [27] proposed a tractable method using stochastic geometry to analyze the SOP and secrecy energy efficiency of a hybrid heterogeneous network (HetNet). They also explored the PLS performance of the hybrid HetNet, where mmWave links coexist with sub-6 GHz (microwave) links. Wang et al. [28] first proposed a secure mobile association policy based on an access threshold and then investigated the connection probability and security probability of a randomly located user based on the proposed policy. The results showed that introducing an appropriate access threshold can significantly improve the security throughput performance of heterogeneous cellular networks. Wang et al. [29] studied the PLS of two-tier HetNets with sub-6 GHz massive multi-input multioutput macrocells and mmWave small cells. In contrast to previous studies, the eavesdroppers of this paper sent pilot signals during the channel training phase to improve the quality of the intercepted signals.

The previous studies investigated the security performance of legitimate transmitters but did not consider the possible behavior of eavesdroppers. Eavesdroppers in hybrid systems behave differently than eavesdroppers in systems with only one link type (i.e., mmWave link or microwave link). They can improve their eavesdropping performance by opportunistically selecting the wave (i.e., mmWave or microwave) to eavesdrop on. For example, eavesdroppers may prefer to eavesdrop on mmWave links when they have better connections to mmWave transmitters than microwave transmitters.

Motivated by the above finding, this paper aims to answer a natural question in hybrid communication systems: in which region do eavesdroppers prefer the mmWave links? Specifically, this paper considers a hybrid communication system with a mmWave communication pair, a microwave communication pair, and an eavesdropper. We focus on characterizing the region where the eavesdropper prefers to eavesdrop on the mmWave link. We first formulate an eavesdropping region characterization problem, where the eavesdropper selects the link to eavesdrop based on the ratio between the security performance of the mmWave and microwave links. To model the security performance of mmWave and microwave links, we derive a closed-form expression for the SOP and lower bound/exact expressions for the secrecy rate of both links. Finally, we provide numerical results to validate our theoretical analysis and also illustrate the millimeter-wave eavesdropping region under various network parameter settings. A preliminary version of this paper can be found by Qu et al. [30], which only focuses on the SOP performance.

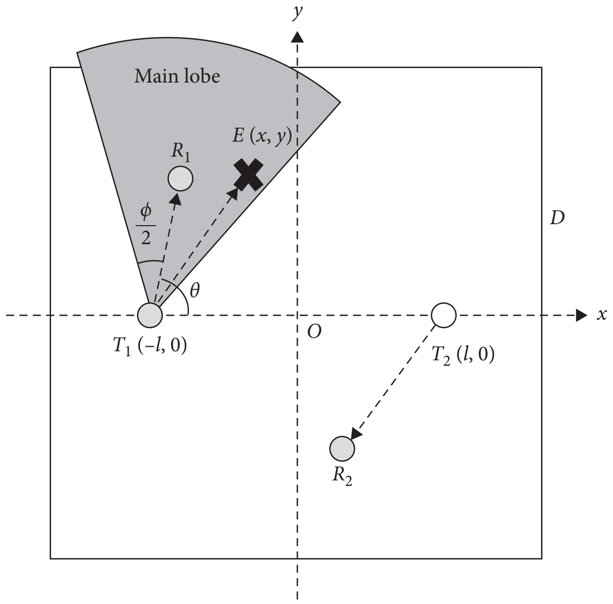

FIGURE 1: System model: one mmWave transmission pair $T_1(-l, 0) \longrightarrow R_1(x_1, y_1)$, one microwave transmission pair $T_2(l, 0) \longrightarrow R_2(x_2, y_2)$, and one eavesdropper $E(x, y)$.

The rest of the paper is structured as follows. Section 2 presents the preliminaries, including the system model and wave selection scheme. In Section 3, we derive the SOPs and secrecy rates of the mmWave link and microwave link and characterize the mmWave eavesdropping regions. We formulate the optimization problem to find the optimal eavesdropping locations in Section 4. Section 5 presents numerical results to validate our theoretical analysis and reveal our findings. Finally, we conclude the paper in Section 6.

2. Preliminaries

In this section, we introduce the preliminaries of this paper, including the system model, antenna model, and blockage and propagation models. In addition, we present the metrics used in this paper and the wave selection scheme of the eavesdropper.

2.1. System Model. Figure 1 shows the system model of this paper, and we consider a square network model with the side length D, which consists of one mmWave transmission pair $T_1 \longrightarrow R_1$, one microwave transmission pair $T_2 \longrightarrow R_2$, and one eavesdropper E which can wiretap on mmWave or microwave link, respectively. We assume the distance between T_1 and T_2 is $2l$ and construct a coordinate system with the origin at the middle point between them. Thus, the coordinate of T_1 and T_2 are $(-l, 0)$ and $(l, 0)$, respectively. In addition, we define the coordinate of R_1 by (x_1, y_1), the coordinate of R_2 by (x_2, y_2), the coordinate of E by (x, y). As shown in Figure 1, the angle between $\overrightarrow{T_1R_1}$ and the x-axis is defined by θ. Note that we use $d_{i,j}$ to denote the distance between nodes i and j.

2.2. Antenna Model. To approximate the antenna patterns of mmWave transmitter T_1, we adopt the sectored antenna model by Bai and Heath [31] and Thornburg et al. [32], where the antenna of T_1 consists of a main lobe and a back lobe. We use ϕ, A_m, and a_m $(A_m > a_m)$ to define the beam width of the main lobe, the main lobe gain, and back lobe gain, respectively. We assume that to obtain the maximum antenna gain, T_1 and T_2 have guided their antennas correctly so that $\overrightarrow{T_1R_1}$ coincides with the aperture of the antenna. Unlike T_1, the microwave transmitter T_2 uses an omnidirectional antenna with an antenna gain of A_u.

To simplify the analysis, we assume that the eavesdropper E uses an omnidirectional antenna with antenna gain of A_E. Note that the effective channel gain G between T_1 and E depends on the location of E. When E is within the main lobe of the antenna of T, G is A_mA_E. Otherwise, G is a_mA_E. We need to compare the angle of $\overrightarrow{T_1R_1}$ with x-axis and the angle between x-axis and $\overrightarrow{T_1E}$ to determine whether E is inside the main lobe of T_1's antenna.

Based on the locations of T_1 and E as well as the angle θ, we have $\overrightarrow{T_1E} = (x + \ell, y)$ and $\overrightarrow{T_1R_1} = (r_0 \cos\theta, r_0 \sin\theta)$, where r_0 denotes the distance between T_1 and R_1. Thus, the angle between $\overrightarrow{T_1R_1}$ and $\overrightarrow{T_1E}$ can given by the following:

$$\vartheta(x, y) = \arccos\left(\frac{(x + \ell)\cos\theta + y \sin\theta}{\sqrt{(x + \ell)^2 + y^2}}\right). \quad (1)$$

If and only if $\vartheta(x, y)$ is smaller than or equal to half of the beamwidth of the main lobe, i.e., $\phi/2$, E is inside the main lobe of T's antenna. Formally, we can give the effective channel gain $\mathcal{G}$ between T_1 and E by the following:

$$G(x, y) = \begin{cases} A_mA_E, & \vartheta(x, y) \le \phi/2, \\ a_mA_E, & \text{otherwise}. \end{cases} \quad (2)$$

2.3. Blockage and Propagation Model. To describe the blockage effect, we use an exponential line-of-sight (LoS) model, where a mmWave link of length r is LoS with a probability

$$p_L(r) = e^{-\beta r}, \quad (3)$$

and is NLoS with probability

$$p_N(r) = 1 - p_L(r), \quad (4)$$

where β represents the blockage density [33]. The blockage effect results in different path losses for LoS and NLoS links, where the exponents are denoted by α_L and α_N, respectively.

In addition, mmWave links are subject to multipath fading, which we characterize with the Nakagami-m fading model. Note that in this paper, we only consider the case where the link $T_1 \longrightarrow R_1$ of the mmWave link transmits information only when the link is LoS. Thus the channel gain of the legitimate channel follows a gamma distribution $\Gamma(N_L, N_L)$ with shape N_L and rate N_L. In contrast, two cases exist for the eavesdropping channel $T_1 \longrightarrow E$. When the link is LoS, it follows a gamma distribution $\Gamma(N_L, N_L)$ with shape N_L and rate N_L, and when the link is NLoS, it follows a gamma distribution $\Gamma(N_N, N_N)$ with shape N_N and rate N_N. Typically, $N_L > N_N$ holds. We use h_{T_1,R_1} to denote the channel gain of the $T_1 \longrightarrow R_1$ link, and $h^L_{T_1,E}$ (resp. $h^N_{T_1,E}$) to denote the channel gain of the $T_1 \longrightarrow E$ link under LoS (resp. NLoS). Thus, the probability density function (PDF) of h_{T_1,R_1} is given by the following:

$$f_{h_{T_1,R_1}}(x) = \frac{N_L^{N_L} x^{N_L-1} e^{-N_L x}}{\Gamma(N_L)}, \quad (5)$$

and the PDF of $h^b_{T_1,E}$ $(b = L, N)$ is given by the following:

$$f_{h^b_{T_1,E}}(x) = \frac{N_b^{N_b} x^{N_b-1} e^{-N_b x}}{\Gamma(N_b)}, \quad (6)$$

where $\Gamma(\cdot)$ is the gamma function.

To describe the fading effect of microwave links, we use a quasi-static Rayleigh fading model. Thus, the legitimate channel gain h_{T_2,R_2} of the link $T_2 \longrightarrow R_2$ and the eavesdropping channel gain $h_{T_2,E}$ of the link $T_2 \longrightarrow E$ follow the exponential distribution with unit mean, e.g., $h_{T_2,E} \sim \text{Exp}(1)$. In addition, the links of $T_2 \longrightarrow R_2$ and $T_2 \longrightarrow E$ are also impaired by the large-scale path loss. We use α_u to denote the path loss of microwave links.

2.4. Metrics. To measure the secrecy performance of the network, we adopt the commonly-used SOP and secrecy rate as the metrics. Note that SOP represents the probability that E succeeds in decoding the transmitted signals. The secrecy rate denotes the difference between the rate of the main communication channel and the rate of the eavesdropping channel.

We use ε_m and ε_u to denote the minimum required signal-to-noise ratios (SNRs) for decoding the signals from T_1 and T_2, respectively. Formally, the SOP when E eavesdropps on the mmWave (i.e., transmitter T_1) is formulated as follows:

$$p^m_{\text{so}} = \mathbb{P}\left(\text{SNR}_{T_1,E} > \varepsilon_m\right), \quad (7)$$

and that when E eavesdropps on the microwave (i.e., transmitter T_2) is formulated as follows:

$$p^u_{\text{so}} = \mathbb{P}\left(\text{SNR}_{T_2,E} > \varepsilon_u\right). \quad (8)$$

According to Barros and Rodrigues [34], Bloch et al. [35], Geraci et al. [36], Ozan Koyluoglu et al. [37], the secrecy rate of mmWave link is formulated as follows:

$$R_s = \left[\log_2\left(1 + \mathrm{SNR}_{T_1,R_1}\right) - \log_2\left(1 + \mathrm{SNR}_{T_1,E}\right)\right]^+, \quad (9)$$

and the secrecy rate of the microwave link is formulated as follows:

$$R_s^u = \left[\log_2\left(1 + \mathrm{SNR}_{T_2,R_2}\right) - \log_2\left(1 + \mathrm{SNR}_{T_2,E}\right)\right]^+, \quad (10)$$

where $[x]^+ = \max\{x, 0\}$.

2.5. Eavesdropping Wave Selection. Based on the SOPs, E chooses between eavesdropping on the mmWave and eavesdropping on the microwave wave. We assume that E uses the ratio between Equations (7) and (8) as the selection criterion and conducts the selection according to the following rule:

(i) If $p_{\mathrm{so}}^m/p_{\mathrm{so}}^u \geq \rho_{\mathrm{sop}}$, E eavesdrops on the mmWave;
(ii) Otherwise, E eavesdrops on the microwave.

Similarly, E chooses to eavesdrop on mmWave links or microwave links, depending on the secrecy rate. We propose to utilize the ratio between Equations (9) and (10) as the selection criterion and develop the selection scheme of eavesdroppers according to the following rules:

(i) If $R_s^u/R_s \geq \rho_{sr}$, E eavesdrops on the mmWave link;
(ii) Otherwise, E eavesdrops on the microwave link.

Here, the parameter ρ_{sop} and ρ_{sr} represent the preference of E. If $\rho_{\mathrm{sop}}\ (\mathrm{resp.}\, \rho_{sr}) = 1$, E treats eavesdropping on the mmWave links and eavesdropping on microwave links as equally important. If $\rho_{\mathrm{sop}}(\mathrm{resp.}\, \rho_{sr}) < 1$, E prefers to eavesdrop on the mmWave links rather than the microwave links, and vice versa.

3. Eavesdropping Region Characterization Modeling

In this section, we characterize the mmWave eavesdropping regions of the eavesdropper, for which we formulate the eavesdropping regions in Section 3.1, derive the SOP p_{so}^m and p_{so}^u in Section 3.2, and derive the average achievable secrecy rate R_s and R_s^u in Section 3.3, respectively.

3.1. Problem Formulation. In this section, we will formulate the eavesdropping regions characterized by SOPs and secrecy rates, respectively.

3.1.1. Eavesdropping Region Characterized by SOP. Note that both p_{so}^m and p_{so}^u vary with the location of E. Thus, the eavesdropping wave of E, i.e., the wave on which E eavesdrops, varies with its location. Therefore, this paper aims to characterize the eavesdropping region, i.e., the *mmWave eavesdropping region* where E eavesdrops on the mmWave based on the proposed wave selection scheme in Section 2.5. We use $\mathscr{R}_m$ to denote the mmWave eavesdropping regions characterized by SOPs, which can be given by the following:

$$\mathscr{R}_m = \left\{(x, y) : p_{\mathrm{so}}^m(x, y)/p_{\mathrm{so}}^u(x, y) \geq \rho_{\mathrm{sop}}\right\}. \quad (11)$$

We can see that, to determine the mmWave eavesdropping region $\mathscr{R}_m$, we need to derive the SOPs $p_{\mathrm{so}}^m(x, y)$ and $p_{\mathrm{so}}^u(x, y)$ when E is located in an arbitrary location (x, y).

3.1.2. Eavesdropping Region Characterized by Secrecy Rate. Similar to SOPs, both R_s and R_s^u vary with the location of E. Therefore, the wave that E chooses to eavesdrop on varies with its location. Thus, we also use the secrecy rates to characterize the mmWave eavesdropping region. We use $\mathscr{M}_m$ to denote the mmWave eavesdropping regions characterized by secrecy rates, which can be given by the following:

$$\mathscr{M}_m = \{(x, y) : R_s^u(x, y)/R_s(x, y) \geq \rho_{sr}\}. \quad (12)$$

It is easy to see that we need to derive the secrecy rate R_s and R_s^u to determine the mmWave eavesdropping region $\mathscr{M}_m$.

3.2. SOP Analysis. In this section, we derive the expression of the SOPs $p_{\mathrm{so}}^m(x, y)$ and $p_{\mathrm{so}}^u(x, y)$ to determine the regions $\mathscr{R}_m$. With the help of the SOPs, we show the mmWave eavesdropping regions characterized by SOPs in Section 5.

3.2.1. SOP of mmWave Link. According to Equation (7), to derive the SOP, we first need to determine the $\mathrm{SNR}_{T_1,E}$. Note that $\mathrm{SNR}_{T_1,E}$ varies depending on whether the link $T_1 \longrightarrow E$ is LoS or NLoS. We use $\mathrm{SNR}_{T_1,E}^L$ (resp. $\mathrm{SNR}_{T_1,E}^N$) to denote the SNR when the link is LoS (resp. NLoS). $\mathrm{SNR}_{T_1,E}^L$ and $\mathrm{SNR}_{T_1,E}^N$ can be given by the followings:

$$\mathrm{SNR}_{T_1,E}^L = \frac{P_m G(x,y) h_{T_1,E}^L d_{T_1,E}^{-\alpha_L}}{\sigma^2}, \quad (13)$$

and

$$\mathrm{SNR}_{T_1,E}^N = \frac{P_m G(x,y) h_{T_1,E}^N d_{T_1,E}^{-\alpha_N}}{\sigma^2}, \quad (14)$$

where P_m represents the transmit power of T_1, $d_{T_1,E}$ denotes the distance between T_1 and E, and σ^2 is the noise power.

Theorem 1. *The SOP $p_{\mathrm{so}}^m(x, y)$ when E eavesdrops on the mmWave link is as follows:*

$$p_{so}^m(x, y) = 1 - e^{-\beta d_{T_1,E}} \frac{\gamma\left(N_L, \frac{N_L \varepsilon_m d_{T_1,E}^{\alpha_L} \sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_L)} - \left(1 - e^{-\beta d_{T_1,E}}\right) \frac{\gamma\left(N_N, \frac{N_N \varepsilon_m d_{T_1,E}^{\alpha_N} \sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_N)}, \quad (15)$$

where $d_{T_1,E} = \sqrt{(x + \ell)^2 + y^2}$ and $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function.

Proof. Applying the law of total probability, we have the following:

$$p_{so}^{m} = p_L\left(d_{T_1,E}\right)\underbrace{\mathbb{P}\left(\mathrm{SNR}_{T_1,E}^{L} > \varepsilon_m\right)}_{Q_L} + p_N\left(d_{T_1,E}\right)\underbrace{\mathbb{P}\left(\mathrm{SNR}_{T_1,E}^{N} > \varepsilon_m\right)}_{Q_N}. \tag{16}$$

Next, we derive Q_L and Q_N. Applying the PDF of gamma random variables, we have the following:

$$\begin{aligned} Q_L &= \mathbb{P}\left(\frac{P_m G(x,y) h_{T_1,E}^{L} d_{T_1,E}^{-\alpha_L}}{\sigma^2} > \varepsilon_m\right) \\ &= \mathbb{P}\left(h_{T_1,E}^{L} > \frac{\varepsilon_m d_{T_1,E}^{\alpha_L}\sigma^2}{P_m G(x,y)}\right) \\ &= 1 - \frac{\gamma\left(N_L, \frac{N_L \varepsilon_m d_{T_1,E}^{\alpha_L}\sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_L)}. \end{aligned} \tag{17}$$

Similarly, we have the following:

$$Q_N = 1 - \frac{\gamma\left(N_N, \frac{N_N \varepsilon_m d_{T_1,E}^{\alpha_N}\sigma^2}{P_m G(x,y)}\right)}{\Gamma(N_N)}. \tag{18}$$

Substituting $p_L\left(d_{T_1,E}\right) = e^{-\beta d_{T_1,E}}$, Equations (17) and (18) into Equation (16) completes the proof. □

3.2.2. SOP of Microwave Link. Likewise, to derive the SOP in this case, we need to determine the SNR $\mathrm{SNR}_{T_2,E}$, which is given by the following:

$$\mathrm{SNR}_{T_2,E} = \frac{P_u A_u A_E h_{T_2,E} d_{T_2,E}^{-\alpha_u}}{\sigma^2}, \tag{19}$$

where $d_{T_2,E}$ is the distance between T_2 and E. Based on $\mathrm{SNR}_{T_2,E}$, we derive the SOP in the following theorem.

Theorem 2. *The SOP $p_{\mathrm{so}}^{u}(x,y)$ when E eavesdrops on the microwave link is as follows:*

$$p_{\mathrm{so}}^{u}(x,y) = \exp\left(-\frac{\varepsilon_u\left((x-\ell)^2+y^2\right)^{\frac{\alpha_u}{2}}\sigma^2}{P_u A_u A_E}\right). \tag{20}$$

Proof. Following the definition of SOP, we have the following:

$$\begin{aligned} p_{so}^{u}(x,y) &= \mathbb{P}\left(\mathrm{SNR}_{T_2,E} > \varepsilon_u\right) \\ &= \mathbb{P}\left(\frac{P_u A_u A_E h_{T_2,E} d_{T_2,E}^{-\alpha_u}}{\sigma^2} > \varepsilon_u\right) \\ &= \mathbb{P}\left(h_{T_2,E} > \frac{\varepsilon_u d_{T_2,E}^{\alpha_u}\sigma^2}{P_u A_u A_E}\right) \\ &= e^{-\frac{\varepsilon_u d_{T_2,E}^{\alpha_u}\sigma^2}{P_u A_u A_E}}. \end{aligned} \tag{21}$$

Substituting $d_{T_2,E} = \sqrt{(x-\ell)^2+y^2}$ in Equation (21) completes the proof. □

Using the SOPs in Theorems 1 and 2, we can determine the mmWave eavesdropping region $\mathscr{R}_m$ based on the definition in Equation (11).

3.3. Secrecy Rate Analysis. In this section, we show the derivation steps of the secrecy rates of the mmWave link and microwave link, respectively. With the help of these two rates, we determine the mmWave eavesdropping region characterized by secrecy rates.

3.3.1. Secrecy Rate of mmWave Link. We analyze the average achievable secrecy rate of mmWave communication networks. Based on Equation (9) and [38–40], the average secrecy rate can be lower bounded by the following:

$$\overline{R}_s = \left[\overline{R} - \overline{R}_e\right]^{+}, \tag{22}$$

where $\overline{R} = \mathbb{E}\left[\log_2\left(1 + \mathrm{SNR}_{T_1,R_1}\right)\right]$ is the average achievable secrecy rate of the channel between the transmitter T_1 and its receiver R_1, and $\overline{R}_e = \mathbb{E}\left[\log_2\left(1 + \mathrm{SNR}_{T_1,E}\right)\right]$ is the average achievable rate of the channel between transmitter T_1 and eavesdropper E.

According to Equation (9), to derive the secrecy rate, we first need to determine the SNR_{T_1,R_1} and $\mathrm{SNR}_{T_1,E}$. As mentioned above, the link $T_1 \longrightarrow R_1$ transmits information only when the link is LoS. Thus, the SNR_{T_1,R_1} is as follows:

$$\mathrm{SNR}_{T_1,R_1} = \underbrace{\frac{P_m G(x_1,y_1) d_{T_1,R_1}^{-\alpha_L}}{\sigma^2}}_{C_1} h_{T_1,R_1}, \tag{23}$$

where (x_1, y_1) denotes the coordinate of R_1 and d_{T_1,R_1} denotes the distance between T_1 and R_1.

The $\mathrm{SNR}_{T_1,E}$ varies depending on whether the link $T_1 \longrightarrow E$ is LoS or NLoS. We use $\mathrm{SNR}_{T_1,E}^{L}$ (resp. $\mathrm{SNR}_{T_1,E}^{N}$) to denote the SNR when the link is LoS (resp. NLoS). Thus, the $\mathrm{SNR}_{T_1,E}^{b}$ $(b = L, N)$ is given by the following:

$$\mathrm{SNR}^{b}_{T_1,E} = \underbrace{\frac{P_m G(x,y) d^{-\alpha_b}_{T_1,E}}{\sigma^2}}_{C_2^b} h^{b}_{T_1,E}. \tag{24}$$

Next, we first derive $\overline{R}$, then show the derivation of $\overline{R}_e$, and finally derive $\overline{R}_s$ based on Equation (22).

Lemma 1. *The average rate of the channel between the transmitter T_1 and its receiver R_1 is as follows:*

$$\overline{R} = \frac{\ln \frac{C_1}{N_L} + \psi_0(N_L)}{\ln 2}, \tag{25}$$

where $C_1 = \frac{P_m G(x_R, y_R) d_{T_1,R_1}}{\sigma^2}$ and $\psi_0(x)$ is Polygamma function.

Proof. To simplify the calculation, we ignore the 1 in $\log_2(1 + \mathrm{SNR}_{T_1,R_1})$. The reason is that we focus on the high SNR regime, i.e., SNR ≫ 1. Then, we have the following:

$$\overline{R} = \mathbb{E}\left[\log_2\left(1 + \mathrm{SNR}_{T_1,R_1}\right)\right] = \mathbb{E}\left[\log_2\left(C_1 \underbrace{h_{T_1,R_1}}_{u}\right)\right]. \tag{26}$$

Applying the PDF of gamma random variables, we have the following:

$$\begin{aligned}\overline{R} &= \frac{1}{\ln 2}\int_0^{\infty} \ln\left(C_1 u\right) d\frac{\gamma(N_L, N_L u)}{\Gamma(N_L)} \\ &\overset{(a)}{=} \frac{\ln\left(C_1 u\right)\frac{\gamma(N_L,N_L u)}{\Gamma(N_L)}}{\ln 2} - \frac{\int_0^{\infty}\sum_{k=0}^{\infty}(-1)^k \frac{(N_L u)^{N_L+k}}{k!(N_L+k)}\frac{1}{u}\, du}{\Gamma(N_L)\ln 2} \\ &= \frac{\left[\ln\left(C_1 u\right)\gamma(N_L, N_L u) - \sum_{k=0}^{\infty}\frac{(-1)^k (N_L u)^{N_L+k}}{k!(N_L+k)^2}\right]\Bigg|_0^{\infty}}{\Gamma(N_L)\ln 2},\end{aligned} \tag{27}$$

where (a) follows the series expansions of the *incomplete gamma function* by Olver et al. [41]. Let

$$D(u) = \ln\left(C_1 u\right)\gamma(N_L, N_L u) - \sum_{k=0}^{\infty}\frac{(-1)^k (N_L u)^{N_L+k}}{k!(N_L+k)^2}. \tag{28}$$

Then, $\overline{R}$ can be rewritten as follows:

$$\overline{R} = \frac{1}{\Gamma(N_L)\ln 2}\left(\lim_{u\longrightarrow\infty} D(u) - \lim_{u\longrightarrow 0} D(u)\right). \tag{29}$$

Next, we derive the limit $\lim_{u\longrightarrow\infty} D(u)$, which is given by the following:

$$\begin{aligned}\lim_{u\longrightarrow\infty} D(u) &= \lim_{u\longrightarrow\infty}\left(\ln C_1\gamma(N_L, N_L u) + \ln u\gamma(N_L, N_L u)\right) \\ &\quad - \lim_{u\longrightarrow\infty}\sum_{k=0}^{\infty}\frac{(-1)^k (N_L u)^{N_L+k}}{k!(N_L+k)^2}.\end{aligned} \tag{30}$$

Based on the series expansions of *lower incomplete gamma function* by Olver et al. [41], we have the following:

$$\begin{aligned}\lim_{u\longrightarrow\infty} D(u) &= \lim_{u\longrightarrow\infty}\sum_{k=0}^{\infty}\frac{(-1)^k (N_L u)^{N_L+k}(\ln u(N_L+k) - 1)}{k!(N_L+k)^2} \\ &\quad + \lim_{u\longrightarrow\infty}\left(\ln C_1\gamma(N_L, N_L u)\right).\end{aligned} \tag{31}$$

Letting $\ln u = \ln \frac{N_L u}{N_L} = \ln N_L u - \ln u$, we have the following:

$$\begin{aligned}\lim_{u\longrightarrow\infty} D(u) &= \lim_{u\longrightarrow\infty}\sum_{k=0}^{\infty}\frac{(-1)^k (N_L u)^{N_L+k}(\ln N_L u(N_L+k) - 1)}{k!(N_L+k)^2} + \lim_{u\longrightarrow\infty}\left(\gamma(N_L, N_L u)\ln\left(\frac{C_1}{N_L}\right)\right) \\ &\overset{(b)}{=} \lim_{u\longrightarrow\infty}\left((\ln(C_1) - \ln(N_L))\gamma(N_L, N_L u)\right) + \lim_{u\longrightarrow\infty}\frac{\partial\gamma(N_L u, N_L)}{\partial N_L} \\ &\overset{(c)}{=} \ln(C_1)\Gamma(N_L) - \ln(N_L)\Gamma(N_L) + \Gamma'(N_L) \\ &= \Gamma(N_L)(\ln(C_1) - \ln(N_L) + \psi_0(N_L)),\end{aligned} \tag{32}$$

where step (b) follows from Equation (33) and step (c) follows the Equation (8.8.13) by Olver et al. [41],

$$
\begin{aligned}
\frac{\partial(\gamma(s,x))}{\partial s} &= \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \frac{x^{s+k}\ln x(s+k) - x^{s+k}}{(s+k)^2} \\
&= \sum_{k=0}^{\infty} \frac{(-1)^k x^{s+k}}{k!(s+k)} \left(\ln x - \frac{1}{s+k}\right).
\end{aligned} \tag{33}
$$

Then, we derive the $\lim_{u\longrightarrow 0} D(u)$, which is given by the following:

$$
\begin{aligned}
\lim_{u\longrightarrow 0} D(u) &= \lim_{u\longrightarrow 0} \ln(C_1 u)\gamma(N_L, N_L u) \\
&- \lim_{u\longrightarrow 0} \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u)^{N_L+k}}{k!(N_L+k)^2} \\
&\overset{(d)}{=} \lim_{u\longrightarrow 0} \sum_{k=0}^{\infty} \left(\frac{(-1)^k {N_L}^{N_L+k}}{k!(N_L+k)} \frac{\ln(C_1 u)}{(u)^{-(N_L+k)}} \right) \\
&\overset{(e)}{=} \sum_{k=0}^{\infty} \lim_{u\longrightarrow 0} \left(\frac{(-1)^k {N_L}^{N_L+k}}{k!(N_L+k)} \frac{u^{N_L+k}}{-(N_L+k)} \right),
\end{aligned} \tag{34}
$$

where step (d) follows from the series expansion of the *lower incomplete gamma function* by Olver et al. [41] and step (e) due to the *L'Hospital's* rule. When $u \longrightarrow 0$, Equation (34) is equal to 0. Substituting Equations (32) and (34) into Equation (29) completes the proof. □

Lemma 2. *The average rate of the channel between the transmitter T_1 and the eavesdropper E is as follows:*

$$
\begin{aligned}
\overline{R}_e &= \frac{1}{\ln 2} \left(p_L(d_{T_1,E}) \left(\ln \frac{C_2^L}{N_L} + \psi_0(N_L) \right) \right. \\
&\left. + p_N(d_{T_1,E}) \left(\ln \frac{C_2^N}{N_N} + \psi_0(N_N) \right) \right),
\end{aligned} \tag{35}
$$

where $C_2^b = \frac{P_m G(x,y) d_{T_1,E}^{-\alpha_b}}{\sigma^2} (b = L, N)$.

Proof. To simplify the calculation, we ignore the 1 in $\log_2(1+\mathrm{SNR}_{T_1,E})$. Following the definition of $\mathrm{SNR}_{T_1,E}$, Equations (3) and (4), and the law of total probability, we have the following:

$$
\begin{aligned}
\overline{R}_e &= \mathbb{E}\left[\log_2\left(1+\mathrm{SNR}_{T_1,E}\right)\right] \\
&= p_L\left(d_{T_1,E}^L\right)\mathbb{E}\left[\log_2\left(C_2{}^L \underbrace{h_{T_1,E}^L}_{u_L}\right)\right] \\
&+ p_N\left(d_{T_1,E}^N\right)\mathbb{E}\left[\log_2\left(C_2^N \underbrace{h_{T_1,E}^N}_{u_N}\right)\right].
\end{aligned} \tag{36}
$$

Applying the PDF of gamma random variables, we have the following:

$$
\overline{R}_e = p_L\left(d_{T_1,E}^L\right) \underbrace{\int_0^{\infty} \log_2(C_2^L u_L) f(u_L) du_L}_{I_L} + p_N\left(d_{T_1,E}^N\right) \underbrace{\int_0^{\infty} \log_2(C_2^N u_N) f(u_N) du_N}_{I_N}. \tag{37}
$$

Next, we derive I_L and I_N,

$$
I_L = \frac{\left. \ln(C_2^L u_L)\gamma(N_L, N_L u_L) - \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u_L)^{N_L+k}}{k!(N_L+k)^2} \right|_0^{\infty}}{\Gamma(N_L)\ln 2}. \tag{38}
$$

Then, we let

$$
D(u_L) = \ln(C_2^L u_L)\gamma(N_L, N_L u_L) - \sum_{k=0}^{\infty} \frac{(-1)^k (N_L u_L)^{N_L+k}}{k!(N_L+k)^2}. \tag{39}
$$

Thus, the I_L can be rewritten as follows:

$$
\begin{aligned}
I_L &= \frac{1}{\Gamma(N_L)\ln 2} \left(\lim_{u_L\longrightarrow\infty} D(u_L) - \lim_{u_L\longrightarrow 0} D(u_L) \right) \\
&\overset{(f)}{=} \frac{\ln(C_2^L) - \ln(N_L) + \psi_0(N_L)}{\ln 2},
\end{aligned} \tag{40}
$$

where step (f) follows after substituting Equations (32) and (34) into $\overline{R}_e$. Similarly, we have the following:

$$
I_N = \frac{\ln(C_2^N) - \ln(N_N) + \psi_0(N_N)}{\ln 2}. \tag{41}
$$

Substituting Equations (40) and (41) to Equation (37), we complete the proof. □

Theorem 3. *Based on Equation (18), Lemma 1 and 2, the average secrecy rate of mmWave link can be lower bounded by the following:*

$$\overline{R}_s = \frac{1}{\ln 2}\left[\ln \tfrac{C_1 N_N}{N_L C_2^N} + \psi_0(N_L) - \psi_0(N_N) - p_L\left(d_{T_1,E}\right)\right. \\ \left.\left(\ln \tfrac{C_2^L N_N}{N_L C_2^N} + \psi_0(N_L) - \psi_0(N_N)\right)\right]^+. \tag{42}$$

Proof. Substituting Equations (3) and (4) to Equation (9) and Equation (4) to Equation (4), we complete the proof. □

3.3.2. Secrecy Rate of Microwave Link. The average achievable secrecy rate of the microwave link is given by the following:

$$\overline{R_s^u} = \mathbb{E}[R_u - R_e^u]^+, \tag{43}$$

where $R_u = \log_2\left(1 + \mathrm{SNR}_{T_2,R_2}\right)$ is the secrecy rate of the channel between the transmitter T_2 and its receiver R_2, and $R_e^u = \log_2\left(1 + \mathrm{SNR}_{T_2,E}\right)$ is the secrecy rate of the channel between transmitter T_2 and eavesdropper E.

According to Equation (10), to derive the secrecy rate of the microwave link, we first need to determine the SNR_{T_2,R_2} and $\mathrm{SNR}_{T_2,E}$. Therefore, the SNR_{T_2,R_2} is as follows:

$$\mathrm{SNR}_{T_2,R_2} = \underbrace{\frac{P_u A_u A_u d_{T_2,R_2}^{-\alpha_u}}{\sigma^2}}_{C_3} h_{T_2,R_2}, \tag{44}$$

and the $\mathrm{SNR}_{T_2,E}$ is as follows:

$$\mathrm{SNR}_{T_2,E} = \underbrace{\frac{P_u A_u A_E d_{T_2,E}^{-\alpha_u}}{\sigma^2}}_{C_4} h_{T_2,E}, \tag{45}$$

where d_{T_2,R_2} denotes the distance between T_2 and R_2, and $d_{T_2,E}$ denotes the distance between T_2 and E.

We then derive the average achievable secrecy rate of the microwave link, which is given by the following theorem.

Theorem 4. *The average secrecy rate of the microwave link is as follows:*

$$\overline{R_s^u} = \ln\left(1 + \frac{A_u d_{T_2,R_2}^{-\alpha_u}}{A_E d_{T_2,E}^{-\alpha_u}}\right). \tag{46}$$

Proof. Using Equations (10), (44), and (45), we have the following:

$$\begin{aligned}\overline{R_s^u} &= \mathbb{E}\left[\log_2\left(C_3 \underbrace{h_{T_2,R_2}}_{u_3}\right) - \log_2\left(C_4 \underbrace{h_{T_2,E}}_{u_4}\right)\right] \\ &= \frac{1}{\ln 2}\mathbb{E}\left[\ln\left(\frac{C_3 u_3}{C_4 u_4}\right)\right] \\ &\overset{(i)}{=} \frac{1}{\ln 2}\mathbb{E}\left[\ln\left(C\frac{u_3}{u_4}\right)\right],\end{aligned} \tag{47}$$

where step (i) follows after letting $C = \frac{C_3}{C_4}$. Then, applying the PDF of exponential distribution, we have the following:

$$\begin{aligned}\overline{R_s^u} &= \int_0^\infty \int_{\frac{u_4}{C}}^\infty \ln\left(C\frac{u_3}{u_4}\right) e^{-u_3} e^{-u_4}\, du_3\, du_4 \\ &= \int_0^\infty \underbrace{\int_{\frac{u_4}{C}}^\infty \ln\left(C\frac{u_3}{u_4}\right) e^{-u_3}\, du_3\, e^{-u_4}\, du_4}_{A}.\end{aligned} \tag{48}$$

We derive A first,

$$\begin{aligned}A &= \int_{\frac{u_4}{C}}^\infty \ln\left(C\frac{u_3}{u_4}\right) e^{-u_3}\, du_3 \\ &= -\ln\left(C\frac{u_3}{u_4}\right) e^{-u_3}\Bigg|_{u_3=\frac{u_4}{C}}^{u_3\longrightarrow\infty} + \int_{\frac{u_4}{C}}^\infty \frac{e^{-u_3}}{u_3}\, du_3 \\ &= \ln(1) e^{-\frac{u_4}{C}} - \lim_{x\longrightarrow\infty} \ln\left(C\frac{u_3}{u_4}\right) e^{-u_3} + \int_{\frac{u_4}{C}}^\infty \frac{e^{-u_3}}{u_3}\, du_3 \\ &= 0 - 0 - E_i\left(-\frac{u_4}{C}\right) \\ &= -E_i\left(-\frac{u_4}{C}\right),\end{aligned} \tag{49}$$

where $E_i(-t) = -\int_t^\infty \frac{e^{-x}}{x}\, dx$ denotes the *Exponential Integral Function* [42]. Hence,

$$\begin{aligned}\overline{R_s^u} &= -\int_0^\infty E_i\left(-\frac{u_4}{C}\right) e^{-u_4}\, du_4 \\ &= -\lim_{t\longrightarrow 0}\int_t^\infty E_i\left(-\frac{u_4}{C}\right) e^{-u_4}\, du_4.\end{aligned} \tag{50}$$

Applying the rule of integral by parts yields,

$$\begin{aligned}\overline{R_s^u} &= \lim_{t\longrightarrow 0} E_i\left(-\left(1 + \frac{1}{C}\right)t\right) - e^{-t} E_i\left(-\frac{t}{C}\right) \\ &= \lim_{t\longrightarrow 0} E_i\left(-\left(1 + \frac{1}{C}\right)t\right) - E_i\left(-\frac{t}{C}\right).\end{aligned} \tag{51}$$

To calculate the above limit, we can use the following expansion of the exponential integral function [42],

$$E_i(t) = \gamma^* + \ln(t) + \sum_{n=1}^{\infty} \frac{t^n}{nn!}, \tag{52}$$

where γ^* is the *Euler constant*. Therefore, Equation (51) can be expressed as follows:

$$\begin{aligned}\overline{R_s^u} &= \lim_{t\longrightarrow 0} \ln\left(-\left(1+\frac{1}{C}\right)t\right) - \ln\left(-\frac{t}{C}\right) \\ &\quad + \sum_{n=1}^{\infty} \frac{\left(-\left(1+\frac{1}{C}\right)t\right)^n - \left(-\frac{t}{C}\right)^n}{nn!} \\ &= \ln(1+C) + \underbrace{\lim_{t\longrightarrow 0} \sum_{n=1}^{\infty} \frac{\left(-\left(1+\frac{1}{C}\right)\right)^n - \left(-\frac{1}{C}\right)^n}{nn!} t^n}_{=0} \\ &= \ln(1+C).\end{aligned} \tag{53}$$

Substituting Equations (44) and (45) into Equation (53) completes the proof. Using the secrecy rates in Theorems 3 and 4, we can determine the mmWave eavesdropping region $\mathscr{M}_m$ characterized by secrecy rates based on the definition in Equation (12). □

4. Optimal Eavesdropping Location Modeling

4.1. Problem Formulation. To better observe the eavesdropping behavior of eavesdroppers, we propose the optimal eavesdropping location problem to investigate the optimal eavesdropping location in the given network. We formulate the optimization problem as follows:

$$(x*, y*) = \underset{x,y\in\left(-\frac{D}{2},\frac{D}{2}\right)}{\arg\max}\ W_m P_{\text{so}}^m(x,y) + (1-W_m)P_{\text{so}}^u(x,y). \tag{54}$$

Due to the complexity of the optimization problem, it is difficult to obtain closed-form solutions. Thus, we use the Arg max function in *Mathematica* to calculate the numerical results [43]. Lastly, we present the numerical results of the optimization problem in the next section.

5. Numerical Results

In this section, we first provide simulation results to validate the expressions of SOPs and secrecy rates for the mmWave link and microwave link, respectively. We then provide the mmWave eavesdropping regions results characterized by different metrics, i.e., SOPs and secrecy rates, and demonstrate the selection behavior of the eavesdropper in the considered hybrid communication scenario under different parameter settings. Finally, we show the numerical results of the optimal eavesdropping location. Table 1 summarizes the parameter settings used in this section.

5.1. Model Validation

5.1.1. SOP Validation. To validate our theoretical analysis, we compare the simulation and theoretical values of the SOPs in mmWave and microwave, respectively. We set the angle between $\overrightarrow{T_1R_1}$ and the x-axis as $\theta = 2\pi/3$, the blockage density as $\beta = 0.1$ and the beam width of the main lobe of T_1's antenna as $\phi = \pi/6$.

We first show in Figure 2 the simulation results and the theoretical values of the SOP of the mmWave transmission pair for three different locations of the eavesdropper E, i.e., $(-20, 20)$, $(-30, 20)$, and $(-40, 20)$. We can see from Figure 2 that the simulation results are consistent with the theoretical ones under all three eavesdropper locations. This indicates the correctness of the SOP expression of the mmWave transmission. We can also see from Figure 2 that the SOP of mmWave decreases as the decoding threshold ε_m increases.

Table 1: Parameter settings.

Parameter	Value
Beamwidth φ of main lobe of T_1	$\pi/6$
Main (back) lobe gain A_m (a_m) of T_1	10 (0.1)
Antenna gain A_u of T_2	1
Antenna gain A_r of T_1	10
Antenna gain A_E of E	5
Path loss exponent α_L (α_N, α_u)	2 (4, 3)
Nakagami-m fading parameter N_L (N_N)	3 (2)
Transmit power P_m (P_u) of T_1 (T_2)	1 (1) (w)
Noise power σ^2	10^{-5} (w)
Distance 2ℓ between T_1 and T_2	80 (m)
The coordinates of mmWave receiver $R_1(x_1, y_1)$	$(40, 20\sqrt{3})$
The coordinates of microwave receiver $R_2(x_2, y_2)$	(60,−40)
Minimum required SNR ε_m for decoding the signals from T_1	0.03
Minimum required SNR ε_u for decoding the signals from T_2	0.1

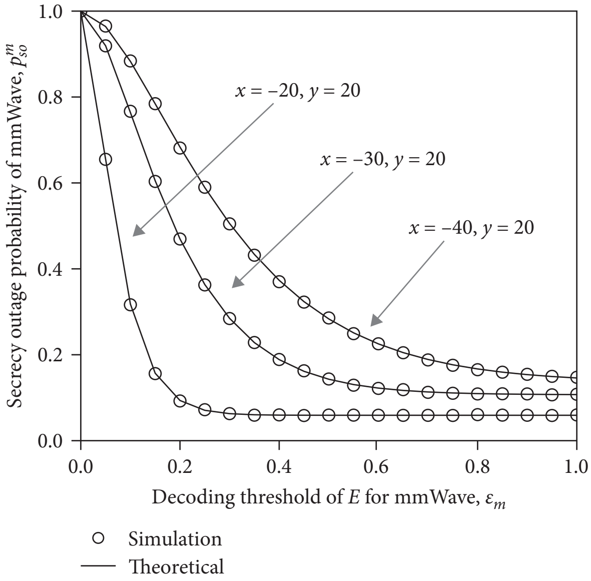

Figure 2: SOP validation of mmWave transmission pair.

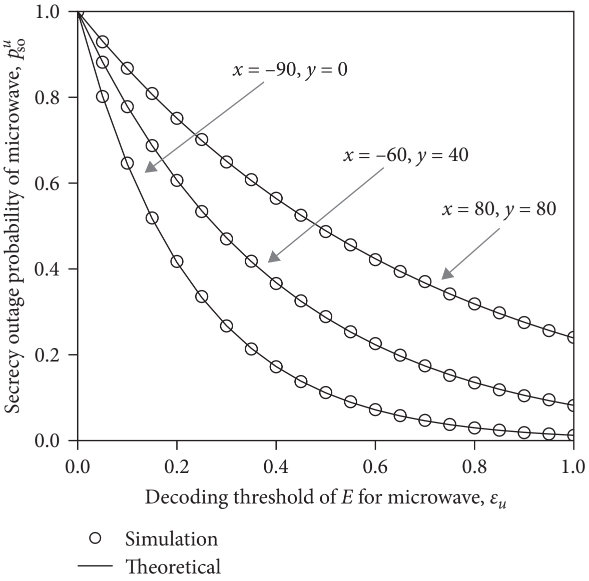

FIGURE 3: SOP validation of microwave transmission pair.

We next show in Figure 3 the simulation results vs. theoretical ones for the SOP of the microwave transmission. We also consider three different locations of E, which are $(-90, 0)$, $(-60, 40)$, and $(80, 80)$. The results in Figure 3 show that the theoretical results match nicely with the simulation ones, demonstrating the correctness of the SOP expression of the microwave transmission. Similar to the SOP of the mmWave transmission, the results show that the SOP of the microwave also decreases as the decoding threshold ε_u increases.

5.1.2. Secrecy Rate Validation. To validate the theoretical analysis in Section 3, we summarize the simulation and theoretical values of the secrecy rate for the mmWave link and microwave link in Figures 4 and 5, respectively. In both figures, we consider three different locations of the eavesdropper E, i.e., $(-40, 20)$, $(-30, 25)$, and $(-40, 30)$ in Figure 4, and $(-20, 20)$, $(0, 40)$, and $(20, -40)$ in Figure 5. We set the antenna gain of E as $A_E = 5$, the coordinates of mmWave receiver $R_1(x_1, y_1)$ and that of microwave receiver as $(40, 20\sqrt{3})$ and $(60, -40)$, respectively.

The results in Figure 4 show that the theoretical results match the simulation results very well, indicating that the lower bound on the secrecy rate of the mmWave link is tight enough to be used as an approximation. Figure 4 also indicates that the secrecy rate of the mmWave link increases as the blockage density β increases. Figure 5 demonstrates the validation of secrecy rate R_s^u for various target antenna gain A_u of microwave transmitter T_1. Notice that the simulation results match nicely with theoretical values, indicating the correctness of the expression of the secrecy rate of the microwave link. The results in Figure 5 also show that the secrecy rate of the microwave transmission increases as the microwave transmitter T_1's antenna gain A_u increases.

5.2. Performance Evaluation. We investigate the impacts of several important parameters on the mmWave eavesdropping region $\mathcal{R}_m$ characterized by the SOPs and that on the mmWave eavesdropping region $\mathcal{M}_m$ characterized by the secrecy rates.

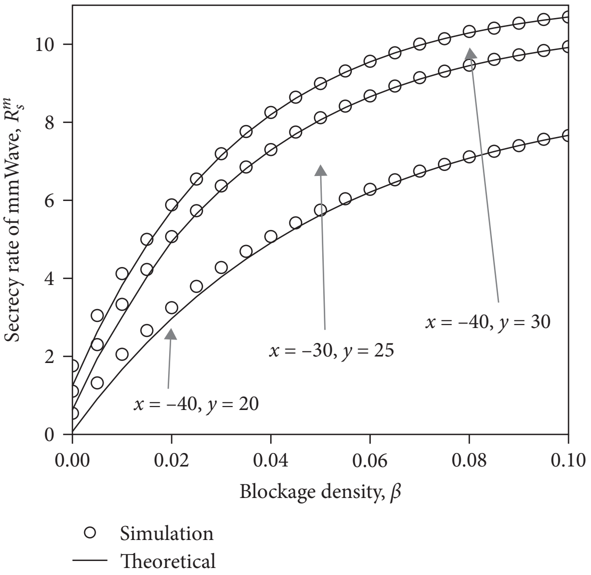

FIGURE 4: Secrecy rate validation of mmWave link.

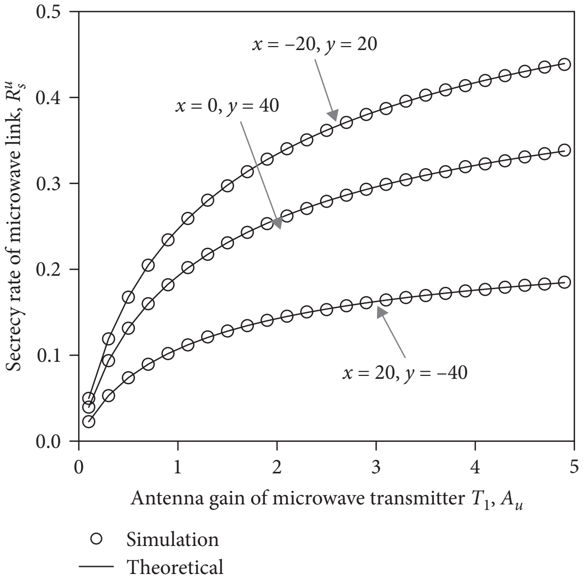

FIGURE 5: Secrecy rate validation of microwave link.

5.2.1. Eavesdropping Region $\mathcal{R}_m$. To understand the impact of the selection parameter ρ_{sop} on the mmWave eavesdropping region $\mathcal{R}_m$, we summarize in Figure 6 the mmWave eavesdropping region $\mathcal{R}_m$ under three different values of ρ_{sop}. Figure 6 shows that $\mathcal{R}_m$ enlarges as the selection parameter ρ_{sop} decreases. Recall that ρ_{sop} represents the selection preference of E. The smaller ρ_{sop} is, the more E prefers the mmWave over the microwave. Thus, for a fixed location, the SOP of the microwave remains unchanged, and as ρ_{sop} decreases, this location is more likely to be included in the mmWave

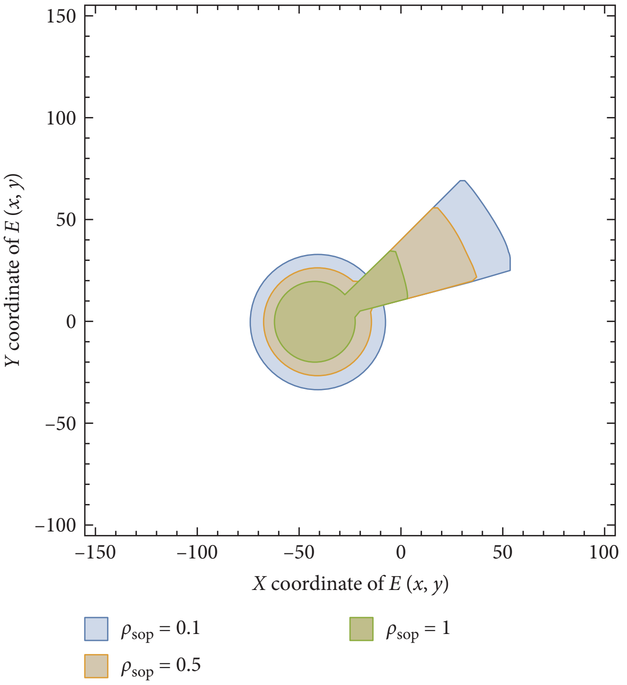

Figure 6: Impact of selection parameter ρ_{sop} on mmWave eavesdropping region (SOP).

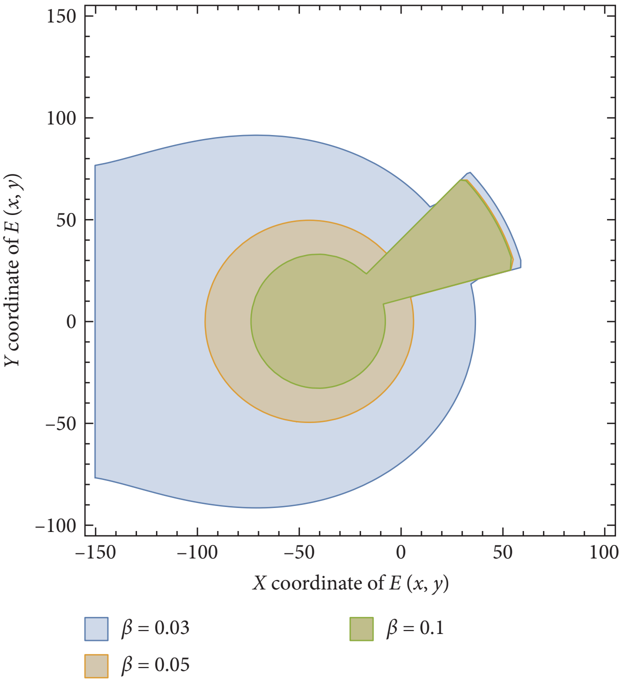

Figure 7: Impact of blockage density β on mmWave eavesdropping region (SOP).

eavesdropping region $\mathscr{R}_m$. As a result, the size of the mmWave eavesdropping region $\mathscr{R}_m$ increases.

Figure 7 shows the impact of the blockage density β on the mmWave eavesdropping region $\mathscr{R}_m$. It can be observed that the size of $\mathscr{R}_m$ decreases as β increases. The major reason for this phenomenon is that the larger β is, the more blockage exists in the network. As a result, the link from T_1 to E is more likely to be NLoS, leading to a smaller SOP. Thus, the possibility of a fixed location being included in $\mathscr{R}_m$ is reduced, resulting in a smaller $\mathscr{R}_m$.

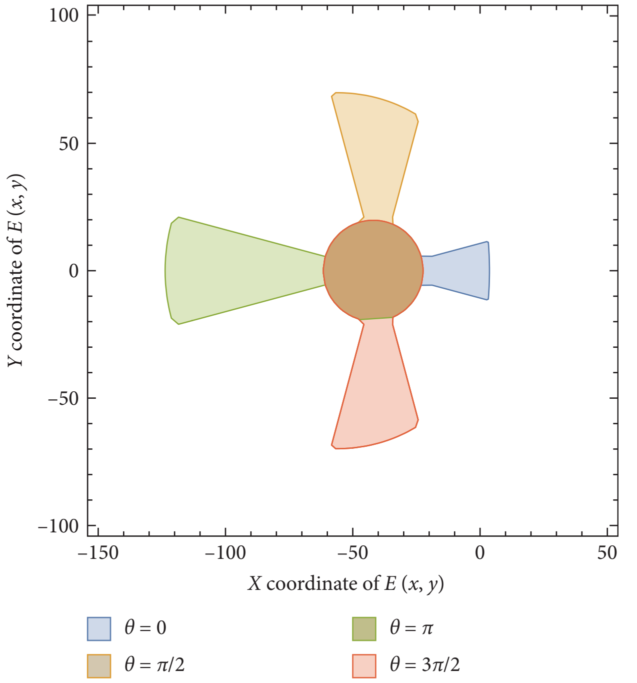

Figure 8: Impact of angle θ on mmWave eavesdropping region (SOP).

Finally, we explore the impact of the angle θ between $\overrightarrow{T_1R_1}$ and the x-axis (i.e., the boresight of the mmWave transmitter's antenna) on the mmWave eavesdropping region $\mathscr{R}_m$. As Figure 8 shows, the size of $\mathscr{R}_m$ changes as the angle θ changes. In general, the region size is minimized when the mmWave transmitter's antenna points toward the microwave transmitter (i.e., the case of $\theta = 0$ in Figure 8), while it is maximized when the mmWave transmitter's antenna points towards the opposite direction of the microwave transmitter (i.e., the case of $\theta = \pi$ in Figure 8). This is intuitive since the closer E is to the microwave transmitter, the larger the SOP under the microwave and, thus, the less likely E prefers the mmWave.

5.2.2. Eavesdropping Region $\mathscr{M}_m$. Figure 9 illustrates the impact of the blocking density β on the mmWave eavesdropping region $\mathscr{M}_m$. We can observe that the size of $\mathscr{M}_m$ decreases as β increases. A larger β means that more blockages exist in the network. Consequently, the link from $T_1 \longrightarrow E$ is more likely to be NLoS, which leads to a larger secrecy rate of the mmWave link. Therefore, the likelihood of any location being included in the mmWave eavesdropping region decreases, which leads to a smaller mmWave eavesdropping region $\mathscr{M}_m$.

We then demonstrate the impact of the selection parameter ρ_{sr} on the mmWave eavesdropping region $\mathscr{M}_m$ in Figure 10. It shows that as the selection parameter ρ_{sr}

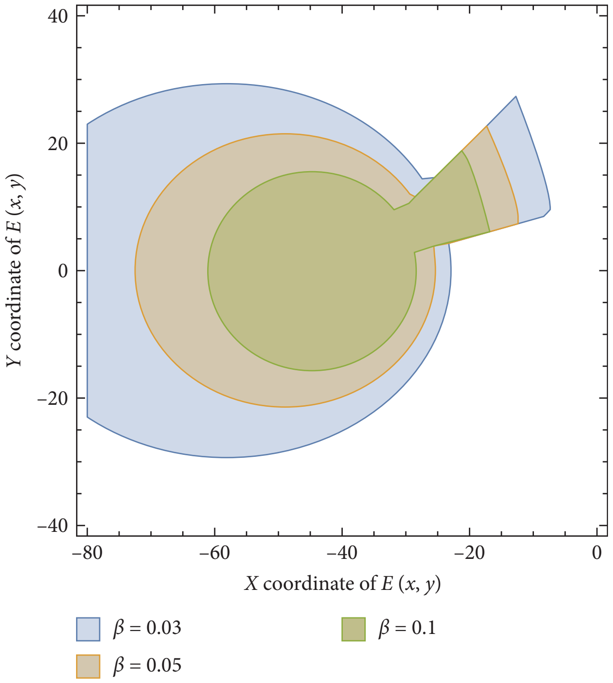

Figure 9: Impact of blockage density β on mmWave eavesdropping region (secrecy rate).

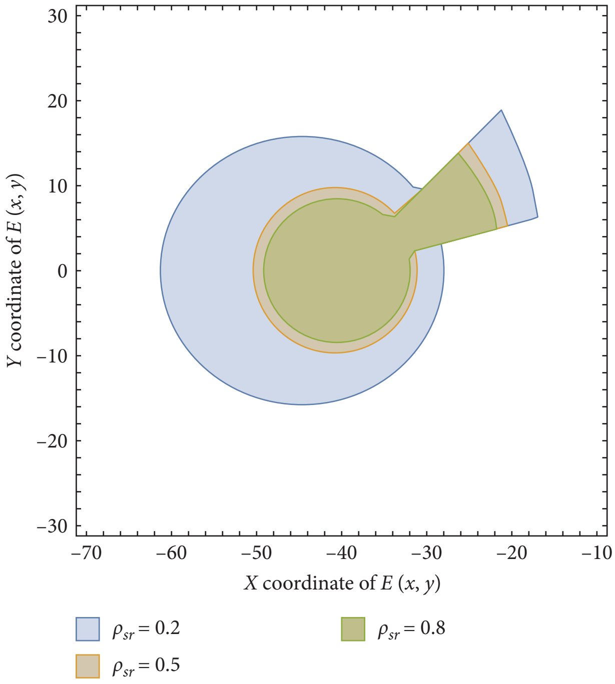

Figure 10: Impact of selection parameter ρ_{sr} on mmWave eavesdropping region (secrecy rate).

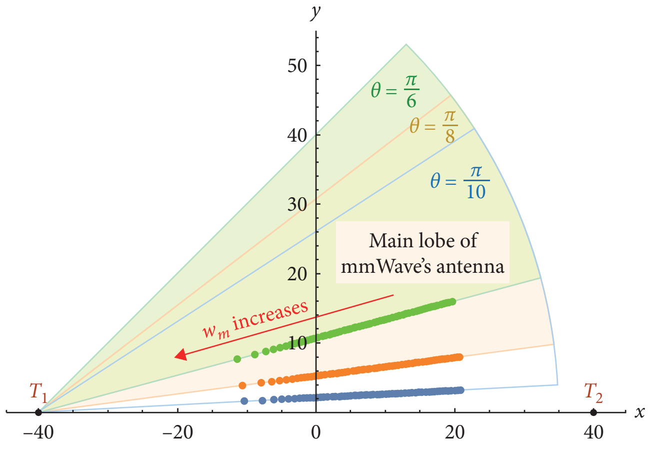

Figure 11: Optimal eavesdropping location.

increases, the size of $\mathscr{M}_m$ decreases. Note that we use ρ_{sr} to represent the selection preference of E in this paper, and a smaller ρ_{sr} means that E prefers mmWave. Since the secrecy rate of the microwave link remains constant, as ρ_{sr} increases, it is more difficult for any fixed location to be included in the mmWave eavesdropping region. Therefore, the mmWave eavesdropping region $\mathscr{M}_m$ becomes smaller.

An interesting phenomenon can be observed from Figure 10, when $\rho_{sr} = 0.5$ or 1, the change of the mmWave eavesdropping region is extremely small. This is because, in this paper, we assume that the eavesdropper E treats eavesdropping on the mmWave link and the microwave link as equally important when $\rho_{sr} = 1$. Also, the transmit power of the mmWave link is much smaller than that of the microwave link. Therefore, when ρ_{sr} is large (i.e., $0.5 < \rho_{sr} < 1$), although the eavesdropper E is in the vicinity of the mmWave transmitter T_1, it still prefers to eavesdrop on the microwave link with stronger transmit power in order to improve their eavesdropping performance.

5.2.3. Optimal Eavesdropping Location. We demonstrate the numerical result of the optimization eavesdropping locations in Section 4. We set the beam width ϕ of the main lobe of T_1 as $\phi = \pi/6$, the blockage density as $\beta = 0.1$ and the antenna gain A_E of E as 5. Moreover, we set the minimum required SNRs ε_m and ε_u as 0.03 and 0.1, respectively.

We illustrate the optimal eavesdropping locations by considering three different angles of θ (the angle between $\overrightarrow{T_1 R_1}$ and x-axis), i.e., $\pi/6$, $\pi/8$, and $\pi/10$. Figure 11 shows the optimal eavesdropping locations of the eavesdropper according to the objective function that we proposed when the angle θ is at three different angles. Note that the sectors represent the main lobe of the mmWave transmitter $T_1(-40, 0)$, $T_2(40, 0)$ represent the microwave transmitter, the three different colors represent three different angles θ, and the continuous dots on the borders denote the optimal eavesdropping locations.

According to Figure 11, we can observe that the optimal eavesdropping location changes as the angle θ changes. Moreover, it is easily seen that the optimal eavesdropping location is always on the lower border of the main lobe of the mmWave transmitter's antenna. As W_m increases, the optimal location is close to mmWave transmitter T_1.

6. Conclusion

This paper investigates the millimeter-wave (mmWave) eavesdropping region characterization problem in hybrid wireless communication systems where mmWave links and microwave links coexist. We first derived the secrecy outage probabilities and secrecy rates of both the mmWave link and microwave link, respectively, based on which we identify the eavesdropping region, where eavesdroppers prefer the mmWave links. We then demonstrate the numerical results of optimization eavesdropping locations. The results in this paper showed that the mmWave eavesdropping region decreases as the selection parameter ρ_{sop} and ρ_{sr} increases. In addition, the eavesdropping region decreases when there are more blockages in the network (i.e., when blockage density β becomes larger).

Data Availability

No underlying data were collected or produced in this study.

Disclosure

This paper was presented in part at the International Conference on Networking and Network Applications (NaNA), Haikou, China, December 2020.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (grant no. 62202354), Qin Chuangyuan Innovation and Entrepreneurship Talent Project of Shaanxi (grant no. QCYRCXM-2022-144), Natural Science Basic Research Program of Shaanxi (program no. 2019JC-17), JST SPRING (grant no. JPMJSP2140) and the Japan Society for the Promotion of Science under Grant-in-Aid for Challenging Research (Exploratory) (grant no. 22K19776).

References

[1] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: potentials and challenges," *Proceedings of the IEEE*, vol. 102, no. 3, pp. 366–385, 2014.

[2] X. Wang, L. Kong, F. Kong et al., "Millimeter wave communication: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1616–1653, 2018.

[3] W. Hong, Z. H. Jiang, C. Yu et al., "The role of millimeter-wave technologies in 5G/6G wireless communications," *IEEE Journal of Microwaves*, vol. 1, no. 1, pp. 101–122, 2021.

[4] M. Shafi, J. Zhang, H. Tataria et al., "Microwave vs. millimeter-wave propagation channels: key differences and impact on 5G cellular systems," *IEEE Communications Magazine*, vol. 56, no. 12, pp. 14–20, 2018.

[5] J. Ma, R. Shrestha, J. Adelberg et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, pp. 89–93, 2018.

[6] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[7] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[8] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[9] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Network*, vol. 36, no. 3, pp. 98–104, 2022.

[10] S. He, Y. Zhang, J. Wang et al., "A survey of millimeter-wave communication: physical-layer technology specifications and enabling transmission technologies," *Proceedings of the IEEE*, vol. 109, no. 10, pp. 1666–1705, 2021.

[11] J. D. V. Sánchez, L. Urquiza-Aguiar, and M. C. P. Paredes, "Physical layer security for 5G wireless networks: a comprehensive survey," in *2019 3rd Cyber Security in Networking Conference (CSNet)*, pp. 122–129, IEEE, 2019.

[12] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli, and J. M. Chuma, "An overview of key technologies in physical layer security," *Entropy*, vol. 22, no. 11, Article ID 1261, 2020.

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

[14] L. Tao, W. Yang, Y. Cai, and D. Chen, "On secrecy outage probability and average secrecy rate of large-scale cellular networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6869189, 14 pages, 2018.

[15] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3205–3217, 2017.

[16] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Secure millimeter-wave ad hoc communications using physical layer security," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 99–114, 2022.

[17] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: a physical layer security perspective," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 623–638, 2019.

[18] S. Huang, M. Xiao, and H. Vincent Poor, "On the physical layer security of millimeter wave noma networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11697–11711, 2020.

[19] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.

[20] L. Fan, B. Tang, Q. Jiang, F. Liu, and C. Yin, "Joint resource allocation for frequency-domain artificial noise assisted multiuser wiretap OFDM channels with finite-alphabet inputs," *Symmetry*, vol. 11, no. 7, Article ID 855, 2019.

[21] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: a programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82599–82612, 2019.

[22] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with

reconfigurable intelligent surfaces," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–6, IEEE, 2020.

[23] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, 2019.

[24] S. C. Tokgoz, S. Althunibat, S. L. Miller, and K. A. Qaraqe, "On the secrecy capacity of hybrid FSO-mmWave links with correlated wiretap channels," *Optics Communications*, vol. 499, Article ID 127252, 2021.

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

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

[27] A. Umer, S. A. Hassan, H. Pervaiz, L. Musavian, Q. Ni, and M. A. Imran, "Secrecy spectrum and energy efficiency analysis in massive MIMO-enabled multi-tier hybrid hetnets," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 1, pp. 246–262, 2020.

[28] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[29] W. Wang, K. C. Teh, S. Luo, and K. H. Li, "Physical layer security in heterogeneous networks with pilot attack: a stochastic geometry approach," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6437–6449, 2018.

[30] Q. Qu, Y. Zhang, and S. Kasahara, "On eavesdropping region characterization in hybrid wireless communications," in *2020 International Conference on Networking and Network Applications (NaNA)*, pp. 29–34, IEEE, 2020.

[31] T. Bai and R. W. Heath, "Coverage and rate analysis for millimeter-wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1100–1114, 2015.

[32] A. Thornburg, T. Bai, and R. W. Heath, "Performance analysis of outdoor mmWave ad hoc networks," *IEEE Transactions on Signal Processing*, vol. 64, no. 15, pp. 4065–4079, 2016.

[33] M. R. Akdeniz, Y. Liu, M. K. Samimi et al., "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1164–1179, 2014.

[34] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, pp. 356–360, IEEE, 2006.

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

[36] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3472–3482, 2012.

[37] O. Ozan Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 3000–3015, 2012.

[38] A. F. Darwesh and A. O. Fapojuwo, "Achievable secrecy rate analysis in mmWave ad hoc networks with multi-array antenna transmission and artificial noise," *IET Communications*, vol. 15, no. 16, pp. 2068–2086, 2021.

[39] S. Iwata, T. Ohtsuki, and P.-Y. Kam, "A lower bound on secrecy capacity for MIMO wiretap channel aided by a cooperative jammer with channel estimation error," *IEEE Access*, vol. 5, pp. 4636–4645, 2017.

[40] C. Liu, J.-Y. Wang, J.-B. Wang, J.-X. Zhu, and M. Chen, "Three lower bounds on secrecy capacity for indoor visible light communications," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, IEEE, 2017.

[41] F. W. J. Olver, A. B. O. Daalhuis, D. W. Lozier et al., 2021, *NIST Digital Library of Mathematical Functions*, http://dlmf.nist.gov/.

[42] M. Abramowitz, *Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*, Dover Publications, Inc., USA, 1974.

[43] W. Research, "ArgMax," 2021, https://reference.wolfram.com/language/ref/ArgMax.html.