Opportunistic Wiretapping/Jamming: A New Attack Model in Millimeter-Wave Wireless Networks

Yuanyu Zhang, Member, IEEE, Zhumeng Zheng, Ji He, Member, IEEE, Shuangrui Zhao, Member, IEEE, Qianyue Qu, Yulong Shen, Member, IEEE, and Xiaohong Jiang, Senior Member, IEEE

Abstract—While the millimeter-wave (mmWave) communication is less susceptible against the conventional wiretapping attack due to its short transmission range and directivity, this paper proposes a new opportunistic wiretapping and jamming (OWJ) attack model in mmWave wireless networks. With OWJ, an attacker can opportunistically conduct wiretapping or jamming to initiate a more hazardous attack based on the instantaneous costs of wiretapping and jamming. We also provide three realizations of the OWJ attack, which are mainly determined by the cost models relevant to distance, path loss, and received power, respectively. To understand the impact of the new attack on mmWave network security, we first develop novel approximation techniques to characterize the irregular distributions of wiretappers, jammers, and interferers under three OWJ realizations. With the help of the results of node distributions, we then derive analytical expressions for the secrecy performance under OWJ. Finally, we provide extensive numerical results to illustrate the effect of OWJ and to demonstrate that the new attack can more significantly degrade the network security performance than the pure wiretapping or jamming attack.

Index Terms—Physical layer security, millimeter-wave ad hoc networks, wiretapping, jamming.

Manuscript received 25 August 2022; revised 20 December 2022, 22 December 2022, and 29 March 2023; accepted 7 May 2023. Date of publication 16 May 2023; date of current version 12 December 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 62251106004, Grant 62202354, Grant 62202355, and Grant 61972308, in part by the Qin Chuangyuan Innovation and Entrepreneurship Talent Project of Shaanxi under Grant QCYRCXM-2022-144, in part by the Major Research Plan of the National Natural Science Foundation of China under Grant 92267204; in part by the Japan Society for the Promotion of Science (JSPS) under Grant 23H03386; and in part by the Japan Science and Technology Agency (JST) Support for Pioneering Research Initiated by the Major Research Plan of the National Natural Science Foundation of China under Grant QCYRCXM-2022-144, in part by the Japan Society for the Promotion of Science (JSPS) under Grant 23H03386; and in part by the Japan Science and Technology Agency (JST) Support for Pioneering Research Initiated by the Next Generation (SPRING) under Grant JPJISP2140. The associate editor coordinating the review of this article and approving it for publication was T. Riihonen. (Corresponding author: Yulong Shen.)

Yuanyu Zhang is with the School of Computer Science and Technology, Xidian University, Xi’an, Shaanxi 710071, China, also with the Shaanxi Key Laboratory of Network and System Security, Xi’an 710071, China, and also with the Beijing Institute of Control Engineering, Beijing Sunwise Information Technology Ltd., Beijing 100190, China (e-mail: yyuzhang@xidian.edu.cn).

Ji He, Shuangrui Zhao, and Yulong Shen are with the School of Computer Science and Technology, Xidian University, Xi’an, Shaanxi 710071, China, and also with the Shaanxi Key Laboratory of Network and System Security, Xi’an 710071, China (e-mail: jihe@xidian.edu.cn; zhaoshuangrui@xidian.edu.cn; yshen@mail.xidian.edu.cn).

Qianyue Qu is with the Division of Information Science, Graduate School of Science and Technology, Nara Institute of Science and Technology, Kofu, Nara 630-0101, Japan (e-mail: qu.qianyue.q2@is.naist.jp).

Shiaohong Jiang is with the School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido 041-8655, Japan, and also with the School of Computer Science and Technology, Xidian University, Xi’an, Shaanxi 710071, China (e-mail: jiang@fun.ac.jp).

Digital Object Identifier 10.1109/TWC.2023.3274808

I. INTRODUCTION

A. Background and Motivation

The past decades have witnessed the explosive growth of wireless devices and the demand for high-speed data traffic, posing a significant challenge to the capacity of wireless systems. To address this challenge, both industry and academia have advocated communications over the millimeter-wave (mmWave) bands between 30 and 300 GHz, where the available bandwidths are orders of magnitude greater than conventional sub-6 bands [1]. In addition, the small wavelength of mmWave signals enables large antenna arrays to be deployed in areas as small as a cellphone or even a chip, achieving significantly high antenna gain for both the transmitting and receiving ends [2]. Thanks to the above benefits, mmWave communication has been regarded as one of the key enabling technologies in future wireless systems like 5G/6G cellular networks [3], unmanned aerial vehicle (UAV) communications [4] and satellite communications [5].

In light of the great potential of mmWave communication, attacks against mmWave signal transmission have drawn considerable attention. Wiretapping and jamming represent two typical attacks in mmWave systems, where the former aims at intercepting valuable information from legitimate transmitters, while the latter aims at radiating jamming signals to impede the normal transmission process of intended transmission pairs. Existing works are mainly from the perspective of network operators to explore the countermeasures against the wiretapping and jamming attacks in various mmWave systems, such as mmWave multiple-input and multiple-output (MIMO) systems [6], [7], [8], [9], [10], [11], [12], [13], mmWave non-orthogonal multiple access (NOMA) systems [14], [15], [16], [17], intelligent reflecting surface (IRS)-aided mmWave systems [18], [19], [20], [21], [22], hybrid mmWave-free space optical (FSO) systems [23], [24], [25], [26] and mmWave ad hoc networks [27], [28], [29], etc.

The above works assumed a simple attack scheme where attackers wiretap/jam brainlessly without caring about the current channel state and antenna pattern for performing the attack. Such attacks are not always effective especially when the attackers are located outside the main lobe of the target transmitter’s/receiver’s antenna, or when the wiretapping and jamming links are blocked by obstacles. Recent real-world measurements on mmWave propagation characteristics indicate that the antenna gains or the condition of the wiretapping and jamming links drop dramatically in such cases [30], [31], [32], [33], thereby greatly degrading the
attack effect. Therefore, from the perspective of attackers, a more effective attack would be opportunistically switching between wiretapping and jamming depending on instantaneous network information (e.g., channel condition and antenna pattern). A practical reason for conducting the opportunistic wiretapping/jamming attack is that such an attack can lead to a more significant attack effect in degrading the network secrecy throughput performance than pure jamming or pure wiretapping, as to be demonstrated by the numerical results in Section V. This serves as the baseline motivation of this work. Another motivation is that, unlike most of the existing works, we aim to provide attack-minded research from the perspective of attackers, discovering more powerful attacks. A few research efforts have also been devoted to this line [34], [35], [36], whereas they only focused on the wiretapping attack.

B. Contribution

By fully exploiting the inherent features of mmWave signal propagation (e.g., high directivity, significant sensitivity to blockages), this paper proposes a more hazardous opportunistic wiretapping and jamming (OWJ) attack model in a mmWave ad hoc network consisting of multiple transmitters, receivers and half-duplex attackers distributed according to Poisson Point Processes (PPPs). With OWJ, an attacker can opportunistically conduct wiretapping or jamming based on the instantaneous costs of conducting wiretapping and jamming, aiming at achieving a more significant attack effect, i.e., reduction of secrecy performance. This paper extends its conference version in [37] by adding more OWJ attack realizations and secrecy performance analysis. The main contributions of this paper are summarized as follows.

- By combining the jamming technique with wiretapping, we propose a new and more hazardous OWJ attack model in mmWave wireless networks, which allows attackers to conduct wiretapping and jamming opportunistically. This model covers conventional wiretapping and jamming attacks as special cases. We also provide three realizations of the OWJ attack, namely distance-based OWJ (DOWJ), loss-based OWJ (LOWJ) and power-based OWJ (POWJ), where the cost of an attacker in wiretapping/jamming is characterized by the distance, path losses and received power, respectively.

- To understand the impact of the OWJ attack on mmWave network security, we first develop novel approximation techniques to characterize the irregular distributions of the wiretappers around a target transmitter, the jammers around a target legitimate receiver and the interferers around a target wiretapper under the three OWJ realizations. With the help of the results of these node distributions, we then derive analytical expressions for the secrecy transmission capacity (STC) to depict the network security performance under the OWJ attack model.

- We finally provide numerical results to illustrate the network STC performance under the OWJ attack model. The results revealed that, in general, the OWJ can more significantly degrade the network security performance than the pure jamming or pure wiretapping attack. In particular, among the three realizations, the POWJ serves as the most hazardous attack, while the DOWJ and LOWJ lead to almost the same attack effect.

C. Related Work

1) Wiretapping and Anti-Wiretapping in mmWave Systems:

Wiretapping represents the most common attack in mmWave systems, while most works focus on the security performance of anti-wiretapping approaches. We divide these works depending on the considered systems.

MIMO is an appealing technology to reap the benefits of mmWave communication, motivating a plethora of work on the security performance of mmWave MIMO systems [6], [7], [8], [9], [10]. For instance, the joint design of the analog and digital precoders of the secondary transmitter (ST) was investigated to maximize the secrecy rates of multiple secondary users (SRs) in the presence of multiple primary users and attackers [6]. The combination of the NOMA technology and mmWave communication for enhanced security has recently been a hot research topic [14], [15], [16], [17]. For example, the authors in [14] proposed two maximum ratio transmission beamforming schemes to enhance the security of the downlink transmission in a mmWave NOMA network. The IRS technology, also known as reconfigurable intelligent surface (RIS), has also been introduced to enhance the security of mmWave communication systems recently [18], [19], [20], [21], [22], [38]. For example, an IRS was introduced in [19] to assist the base station (BS) in securely broadcasting information to multiple users while sending its own information to an IoT device. The precoder at the BS and the beamformer at the IRS were jointly designed to maximize the minimum secrecy rate of the users. The joint design of beamformers at the transmitter and the IRS was also investigated in [21] for a normal mmWave system and in [22] for a mmWave cognitive communication system. For a comprehensive survey on the security of RIS-enhanced mmWave systems, please refer to [38]. As a promising candidate for backhaul solutions of 5G/beyond 5G networks, hybrid communication systems with mmWave links coexisting with FSO links have attracted considerable attention, and so does the security performance therein [23], [24], [25], [26]. For example, the authors in [23] analyzed security performance in a parallel FSO-mmWave system, where the transmitter sends information to the receiver via an FSO link and a mmWave link concurrently. Research efforts have also been devoted to the security performance analysis of mmWave ad hoc networks [27], [28], [29]. For example, the authors in [27] proposed a sight-based cooperative jamming scheme for improved secrecy in a mmWave ad hoc network with transmitters, receivers, potential jammers and attackers distributed according to PPPs.

The above works studied from the perspective of protectors the secrecy capacity under the impacts of the directional antenna pattern, blockage, mobility, user/attacker density, colluding/non-colluding wiretappers, antenna number, etc, while this paper studies from the perspective of attackers the impact of attack strategies on the network secrecy performance. Although a few research efforts have also been devoted to the design of attack schemes in mmWave systems,
they focus only on the wiretapping attack. The authors in [34] demonstrated that although mmWave signals are generally hard to wiretap from outside the signal beam, attackers still can intercept information from the signals reflected by the intentionally-placed small-scale objects within the signal beam. The authors in [35] showed that attackers can exploit the signals leaked from the side lobe to successfully intercept information. The probability of successful wiretapping by a nomadic attacker, which moves around to find a favorable attacking location, was analytically investigated in [36] for 802.11ad mmWave wireless networks.

2) Jamming and Anti-Jamming in mmWave Systems:
Jamming aims to impede the normal process of legitimate transmissions by transmitting high-power signals. The most common case is to degrade the quality of the received signals at intended receivers. For example, in [39], a simple jamming attack towards the femtocell users in a two-tier heterogeneous cellular network was considered and the authors proposed a federated deep reinforcement learning (DRL)-based anti-jamming technique to improve the achievable rates of the femtocell users. The authors in [40] focused on an intelligent jammer that applies Q-learning to choose its jamming power to attack the ground users in a UAV mmWave system. A power control scheme based on dynamic RL was proposed to mitigate the jamming effect. The authors in [11] focused on a jammer that can freely change the jamming power and number of jamming antennas and investigated the robustness of the physical layer network coding against such attacks. Jamming attacks that exploit the vulnerability of the low-resolution analog-to-digital converters of mmWave MIMO BSs were investigated in [12] along with the corresponding anti-jamming strategies, such as beam slicing. In addition to directly degrading the signal quality of legitimate receivers, jamming can also be used to interrupt some critical phases during the access or transmission establishment. For example, the authors in [13] focused on the jamming attack in the beam alignment phase between a user and a BS in a mmWave MIMO system and proposed a random probing-based anti-jamming countermeasure.

3) Attacks Combining Wiretapping and Jamming in Non-mmWave Systems: Attacks combining wiretapping and jamming have also been investigated in non-mmWave systems. In the case of full-duplex attackers, jamming and wiretapping can be conducted simultaneously to launch a more hazardous attack [41], [42], where the jamming degrades the received signals at legitimate receivers, forcing transmitters to raise their transmit powers, which in turn increases the possibility of successful wiretapping. Similar ideas were adopted by legal users to wiretap suspicious communication links with the objective of decreasing the suspicious communication rate while increasing the wiretapping rate. This is termed proactive eavesdropping and has been extensively studied in various scenarios, such as MIMO systems [43], RIS-assisted broadcast systems [44] and wireless information surveillance systems [45]. Research efforts have also been devoted to the hybrid attacks, where wiretappers coexist with jammers, in various system scenarios, such as multi-layer RIS-assisted integrated terrestrial-aerial networks [46], visible light communication systems [47] and device-to-device systems [48].

4) Novelty of Our Work: Compared with the existing works, the main novelty of this work is that we identify a new and more hazardous attack model in mmWave wireless networks. Different from the available attacker models where each attacker can act as only a jammer or wiretapper, in the newly proposed OWJ attack model an attacker can act as both a jammer and a wiretapper in the sense it can opportunistically switch between the roles of wiretapper and jammer to achieve an enhanced attack effect than the traditional pure jamming and pure wiretapping attacks.

The remainder of this paper is organized as follows. We introduce the system model in Section II and conduct theoretical performance analysis in Sections III and IV. Section V presents the numerical results and discussions, and Section VI concludes this paper.

II. SYSTEM MODEL

In this section, we introduce the network, antenna, blockage and propagation models, followed by the proposed OWJ attack model and the performance metrics.

A. Network Model

We consider a Poisson bipolar network comprising a set of mmWave transmitter-receiver pairs, where each receiver is located at a fixed distance \( r_0 \) away from its transmitter but at random orientation. The locations of the transmitters and receivers are modeled by two independent PPPs \( \Phi_T \) and \( \Phi_R \) of the same intensity [49], denoted by \( \lambda \). To simplify the analysis, we neglect the dependence between \( \Phi_T \) and \( \Phi_R \). Also present in the network is a set of half-duplex attackers, whose locations are modeled by another independent and homogenous PPP \( \Phi_E \) of intensity \( \lambda_E \). Each attacker independently conducts the wiretapping or jamming attack based on a certain OWJ strategy, as introduced in Section II-D. We consider wiretapping and jamming as two exclusive attack choices due to the half-duplex constraint at the attackers. The resulting wiretappers and jammers form two independent PPPs, denoted by \( \Phi_W \) and \( \Phi_J \), respectively. Using \( 1_J \) to indicate whether an attacker \( z \) is a jammer (i.e., \( 1_J = 1 \)) or not (i.e., \( 1_J = 0 \)), we have \( \Phi_J = \{ z \in \Phi_E : 1_J = 1 \}, \Phi_W = \{ z \in \Phi_E : 1_J = 0 \} \).

Note that we adopt a relatively simple system model here due to the following reasons. First, this paper represents the first attempt to demonstrate that OWJ serves as a new and more hazardous attack model for mmWave wireless networks, so we adopted a simple system model such that the readers can easily capture the main idea of OWJ. Second, although the concerned system model is simple, it still helps us to understand the fundamental network performance limits. This is why such a model has been widely adopted in the literature for the study of (secrecy) throughput performance of large-scale wireless networks [27], [28], [29]. Third, such a simple system model enables solid theoretical modeling to be conducted for the inhomogeneous distributions of the wiretappers/jammers and thus the system performance under the OWJ attack.

B. Antenna Model

Each node is equipped with a directional antenna characterized by the sectored antenna model in [27], [50], [51].
In [52], [53], and [54], where each antenna consists of a main lobe and a side lobe. The key antenna parameters of different node types are summarized in Table I. Due to the isotropic feature of the PPPs, the effective antenna gain between a transmitting node $a$ of type $t_1 \in \{T, J\}$ ($T$: transmitter, $J$: jammer) and a receiving node $b$ of type $t_2 \in \{R, W\}$ ($R$: receiver, $W$: wiretapper) can be represented by the following random variable

$$G_{a,b}^{t_1 t_2} = \begin{cases} G_{MM}^{t_1 t_2} = G_{M}^{t_1} G_{M}^{t_2}, & \text{w.p. } P_{MM}^{t_1 t_2} = \frac{\theta_1 \theta_2}{(2\pi)^2} \left(2\pi - \theta_1^2 - \theta_2^2\right) \\ G_{MS}^{t_1 t_2} = G_{M}^{t_1} G_{S}^{t_2}, & \text{w.p. } P_{MS}^{t_1 t_2} = \frac{(2\pi - \theta_1)(2\pi - \theta_2)}{(2\pi)^2} \\ G_{SM}^{t_1 t_2} = G_{S}^{t_1} G_{M}^{t_2}, & \text{w.p. } P_{SM}^{t_1 t_2} = \frac{(2\pi - \theta_1)(2\pi - \theta_2)}{(2\pi)^2} \\ G_{SS}^{t_1 t_2} = G_{S}^{t_1} G_{S}^{t_2}, & \text{w.p. } P_{SS}^{t_1 t_2} = \frac{(2\pi - \theta_1)(2\pi - \theta_2)}{(2\pi)^2} \end{cases}$$

(1)

where w.p. stands for with probability. Prior to transmissions, each pair of transmitter and receiver align their antennas to achieve the largest antenna gain $G_{M}^{T} G_{M}^{R}$.

### C. Blockage and Propagation Model

Communication links can be LoS or NLoS due to the existence of blockages. According to the blockage model in [55], a link of length $r$ is LoS with probability $p_L(r) = e^{-\beta r}$ and NLoS with probability $p_N(r) = 1 - p_L(r)$, where $\beta$ denotes the blockage density. We use $S_{a,b}$ to represent the status of the link $a \rightarrow b$ between nodes $a$ and $b$. $S_{a,b} = L$ (resp. $S_{a,b} = N$) means that the link is LoS (resp. NLoS). Links suffer from both large-scale path loss and small-scale fading characterized by the Nakagami fading model. The path loss of the link $a \rightarrow b$ is $d_{a,b}^{\alpha}$, where $d_{a,b}$ denotes the distance between nodes $a$ and $b$, and $\alpha$ is the random path-loss exponent, which equals $\alpha_L$ (resp. $\alpha_N$) if $S_{a,b} = L$ (resp. $S_{a,b} = N$). The corresponding channel gain $h_{a,b}$ follows the gamma distribution with shape $K$ and rate $K$. Here, $K = K_L$ (resp. $K = K_N$) if $S_{a,b} = L$ (resp. $S_{a,b} = N$). Throughout this paper, we assume $\alpha_L < \alpha_N$ and $K_L > K_N$.

### D. OWJ Attack Model

In the OWJ attack, each attacker measures the costs of wiretapping and jamming and chooses to wiretap if cost of wiretapping $< \rho \cdot$ cost of jamming, and chooses to jam otherwise. The bias factor $\rho$ here represents the preference of the attackers for the wiretapping attack. The larger the $\rho$ is, the more likely attackers will wiretap. The OWJ attack reduces to the pure wiretapping (resp. jamming) attack, as $\rho$ tends to $\infty$ (resp. 0). In this paper, we consider the following three representations of the costs of a typical attacker $z \in F_E$, giving rise to three different realizations, i.e., DOWJ, LOWJ, POWJ, respectively. This is motivated by the fact that attackers manage to improve their attack effect with all the available network knowledge.

- **Smallest distances**: We use the smallest distances from $z$ to the transmitters and receivers to represent the costs, which are denoted by $D_T^z = \min_{x \in F_T} d_{x,z}$ (wiretapping) and $D_R^z = \min_{y \in F_R} d_{y,z}$ (jamming), respectively. This applies to the case where only the location information of the transmission pairs is known to the attackers, which can be obtained from auxiliary signals exchanged between a transmitter and a receiver in the beam alignment phase by applying signal feature-based localization approaches, such as time difference of arrival (TDoA), angle of arrival (AoA) and received signal strength (RSS) [56].

- **Smallest path losses**: We use the smallest path losses from $z$ to the transmitters and receivers as the costs, which are given by $L_T^z = \min_{x \in F_T} d_{x,z}^\alpha$ (wiretapping) and $L_R^z = \min_{y \in F_R} d_{y,z}^\alpha$ (jamming), respectively. This applies to the case where both the locations of the transmission pairs and the link status to the transmission pairs are known to the attackers.

- **Smallest reciprocals of power**: We use the smallest reciprocal of the power received by $z$ (resp. receivers) from the transmitters (resp. $z$) as the cost of wiretapping (resp. jamming). The costs are formally given by $P_T^z = \min_{x \in F_T} (P_T z / G_{T}^z)$ (wiretapping) and $P_R^z = \min_{y \in F_R} (P_R z / G_{R}^z)$ (jamming), where $P_T$ and $P_J$ denote the transmit power and jamming power of the transmitters and jammers, respectively. This applies to the case where the information of instantaneous antenna gains to the transmitters and receivers is also available.

MmWave signals experience severe atmospheric absorption, rain attenuation and penetration loss, leading to significantly degraded signal strength as the propagation distance increases or when the signals are blocked by obstacles like human bodies and buildings. To combat signal attenuation, transmitters are equipped with directional antennas with narrow beams, leading to the highly directive propagation of mmWave signal. As a result, attackers will have significantly different attack effects when they are located inside/outside the main lobe of a transmitter (resp. receiver) or when the wiretapping (resp. jamming) link is line-of-sight (LoS)/non-LoS. We fully take such significant differences into consideration when designing the OWJ attack and the three realizations. For example, the POWJ realization exploits both the link and antenna differences to determine the best possible attack strategy. In principle, the proposed OWJ model can be applied to other frequency wireless networks as well, whereas its effectiveness is questionable because the attack effect may have no significant difference under different network circumstances there. In addition, the three OWJ realizations may need to be re-designed to adapt to the target networks. Note that the OWJ attack model associates each attacker with a transmitter and a receiver, which only serve as the reference nodes to help determine the attack strategy rather than the targets of the attack. In fact, each wiretapper (resp. jammer) will attack all the transmitters (resp. receivers).

| Parameters | Transmitter | Receiver | Wiretapper | Jammer |
|------------|-------------|----------|------------|--------|
| ML width   | $2\pi - \theta_r$ | $2\pi - \theta_q$ | $2\pi - \theta_w$ | $2\pi - \theta_v$ |
| ML gain    | $G_M^T$ | $G_M^R$ | $G_M^W$ | $G_M^J$ |
| SL gain    | $G_S^T$ | $G_S^R$ | $G_S^W$ | $G_S^J$ |

**Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.**
E. Performance Metrics

Transmitters adopt the Wyner encoding scheme [27], where each confidential message is encoded into a codeword randomly selected from multiple candidates. Such randomness is used to confuse attackers. This scheme defines two code rates, i.e., the code rate for the codeword $R_s$ and that for the confidential message $R_c$. The difference $R_c = R_t - R_s$ reflects the code rate sacrificed for generating the randomness. $R_t$, $R_s$ and $R_c$ are fixed throughout this paper.

We adopt the STC metric to model the security performance, which defines the average sum rate of transmissions in perfect secrecy per unit area. Formally, the STC is given by

$$\Omega^{T} (\cdot) = \frac{1}{\pi^2} \sum_{k=1}^{K} \frac{K k^{\frac{1}{2}}}{T^2 R_s} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{e^{-\frac{1}{2} \left( \frac{x^2 + y^2}{\alpha^2} \right)}}{\sqrt{x^2 + y^2}} \, dx \, dy$$

where each confidential message is encoded into a codeword $R_c$ of the link status completes the proof.

We can see from (2) that the key terms to determine $p_c$ are the Laplace transforms of the OWJ attack model, while $L_{y_0}^J (\cdot)$ is not. Prior to deriving $L_{y_0}^T (\cdot)$, we present the following functions for any $k \in \{L, N\}$, $i \in \{M, S\}$, $j \in \{M, S\}$, $t_1 \in \{T, J\}$ and $t_2 \in \{R, W\}$, which will be used extensively in this paper.

$$\Omega_{t_1, t_2}^k (s, r) = p_{t_1} t_2 \Omega_{t_1, t_2}^k (r) \left( 1 + \frac{s P_t g_{t_1, t_2} \sigma_k}{K_k r s_k} \right)^{-1}$$

Now, we are ready to derive $L_{y_0}^J (\cdot)$ in the following lemma.

**Lemma 1:** The Laplace transform of $I_{y_0}^T$ under the DOWJ, LOWJ and POWJ attacks is

$$L_{y_0}^T (s) = \exp \left( -2 \pi \lambda \int_{0}^{\infty} \Omega_{T,R}^T (s, r) r \, dr \right)$$

**Proof:** According to the definition, we have

$$L_{y_0}^T (s) = \mathbb{E} \left[ e^{-s I_{y_0}^T} \right] = \mathbb{E} \left[ e^{-s \sum_{k \in \Phi_T} P_k G_{t_1, t_2}^{y_0} \sigma_k} \right]$$

Next, we derive $L_{y_0}^J (\cdot)$ under the three OWJ attacks in the following subsections, respectively.

III. CONNECTION PROBABILITY ANALYSIS

In this section, we first derive a unified expression for the connection probability of a typical transmission pair $x_0 \rightarrow y_0$, which involves a key term, i.e., the Laplace transform of the interference at $y_0$ from the jammers. We then derive this Laplace transform under the DOWJ, LOWJ and POWJ attacks in Sections III-B, III-C and III-D, respectively.

A. Connection Probability

According to the definition, the connection probability is

$$p_c = \mathbb{P} \left( \log \left( \frac{1 + \text{SINR}_{x_0, y_0}}{1} \right) > R_s \right)$$

where $\text{SINR}_{x_0, y_0} = \frac{P_y G_{t_1, t_2}^{x_0, y_0} \sigma_k}{P_x G_{t_1, t_2}^{x_0, y_0} \sigma_k + \sigma^2}$ is the signal-to-interference-plus-noise ratio (SINR) of $y_0$. Here, $\sigma^2$ is the noise power at $y_0$ and $I_{y_0}^T$ (resp. $I_{y_0}^J$) denotes the interference at $y_0$ caused by the transmitters in $\Phi_T$ (resp. jammers in $\Phi_J$). The theorem below gives the unified expression of $p_c$.

**Theorem 1:** The unified connection probability of the typical transmission pair $x_0 \rightarrow y_0$ under the DOWJ, LOWJ and POWJ attacks can be approximated by

$$p_c \approx \sum_{k \in \{L, N\}} \frac{K_k}{t} \left( -1 \right)^{i_1 + \cdots + i_k} \alpha \prod_{i \in \{T, J\}} \mathcal{L}_{y_0}^i (t \mu_k)$$

where $\mu_k = K_k (K_k-1)^{-1/2} (2 R_s - 1) R_s^{t_1} / (P_y G_{t_1, t_2}^{x_0, y_0} \sigma_k)$ and $\mathcal{L}_{y_0}^i (t) (t_1 \in \{T, J\})$ denotes the Laplace transforms of $I_{y_0}^i$.

**Proof:** Suppose $x_0 \rightarrow y_0$ is in status $k$ (i.e., $S_{x_0, y_0} = k$, $k \in \{L, N\}$), $p_c$ is given by

$$p_c \approx \sum_{k \in \{L, N\}} \frac{K_k}{t} \left( -1 \right)^{i_1 + \cdots + i_k} \alpha \prod_{i \in \{T, J\}} \mathcal{L}_{y_0}^i (t \mu_k)$$

Applying the law of total probability in terms of the link status completes the proof.

We can see from (2) that the key terms to determine $p_c$ are the Laplace transforms of the OWJ attack model, while $L_{y_0}^J (\cdot)$ is not. Prior to deriving $L_{y_0}^J (\cdot)$, we present the following functions for any $k \in \{L, N\}$, $i \in \{M, S\}$, $j \in \{M, S\}$, $t_1 \in \{T, J\}$ and $t_2 \in \{R, W\}$, which will be used extensively in this paper.

$$\Omega_{t_1, t_2}^k (s, r) = p_{t_1} t_2 \Omega_{t_1, t_2}^k (r) \left( 1 + \frac{s P_t g_{t_1, t_2} \sigma_k}{K_k r s_k} \right)^{-1}$$

Now, we are ready to derive $L_{y_0}^J (\cdot)$ in the following lemma.

**Lemma 1:** The Laplace transform of $I_{y_0}^T$ under the DOWJ, LOWJ and POWJ attacks is

$$L_{y_0}^T (s) = \exp \left( -2 \pi \lambda \int_{0}^{\infty} \Omega_{T,R}^T (s, r) r \, dr \right)$$

**Proof:** According to the definition, we have

$$L_{y_0}^T (s) = \mathbb{E} \left[ e^{-s I_{y_0}^T} \right] = \mathbb{E} \left[ e^{-s \sum_{k \in \Phi_T} P_k G_{t_1, t_2}^{y_0} \sigma_k} \right]$$

Next, we derive $L_{y_0}^J (\cdot)$ under the three OWJ attacks in the following subsections, respectively.

B. Derivation of $L_{y_0}^J (s)$ Under DOWJ Attack

Before deriving $L_{y_0}^J (s)$, we first establish the following lemma for the probability that an attacker $z$ with distance $v$ to $y_0$ is a jammer (i.e., $I_{y_0}^J = 1$) under the DOWJ attack.

**Lemma 2:** The probability that an attacker $z$ with distance $v$ to the typical receiver $y_0$ is a jammer under the DOWJ attack is

$$\zeta (v) = \frac{1}{\rho^2 + 1} \int_{|v-r_0|}^{\infty} \frac{\rho^2}{\frac{v^2}{\rho^2 + 1}} e^{-\left( \frac{v^2}{\rho^2 + 1} \right) \lambda \pi v^2} du$$

where $c_v = \min \{ \max \{ \rho v, |v-r_0| \}, v+r_0 \}$.

**Proof:** See Appendix A.

Next, we derive $L_{y_0}^J (\cdot)$ under the three OWJ attacks in the following subsections, respectively.

**Lemma 3:** The Laplace transform of $I_{y_0}^J$ under the DOWJ attack can be lower bounded by

$$L_{y_0}^J (s) \geq \exp \left( -2 \pi \lambda E \int_{0}^{\infty} \Omega_{J,R} (s, v) \zeta (v) \, dv \right)$$

where $E$ is the density function of the distance between the typical receiver and a jammer.
Proof: First, we have $I_{y_0} = \sum_{z \in \Phi_E} 1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z} d_{y_0,z}$. Hence,

$$L_{y_0}(s) = \mathbb{E}_{I_{y_0}} e^{-s I_{y_0}} = \mathbb{E}_{\Phi_E} \left[ \prod_{z \in \Phi_E} \mathbb{E}_{h_{y_0,z}} e^{-s \frac{1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z}}{\lambda_w}} \right] = \mathbb{E}_{\Phi_E} \left[ \exp \left( -2\pi \lambda_E \int_0^\infty \right) \left( 1 - \mathbb{E}_{G_{j,R}^{z,y_0},h_{y_0,z}} e^{-s \frac{1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z}}{\lambda_w}} \right) \right] (v)dv}.

(10)

Applying Jensen’s inequality yields

$$L_{y_0}(s) \geq \exp \left( -2\pi \lambda_E \int_0^\infty \right) \left( 1 - \mathbb{E}_{G_{j,R}^{z,y_0},h_{y_0,z}} e^{-s \frac{1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z}}{\lambda_w}} \right) \right) v dv,

$$

C. Derivation of $L_{y_0}(s)$ Under LOWJ Attack

We first establish the following lemma, similar to the analysis in Section III-B.

Lemma 4: The probability that an attacker $z$ with distance $v$ and link status $\tau \in \{L, N\}$ to $y_0$ is a jammer under the LOWJ attack is

$$\zeta_{\tau,n,o}(v) = \int_{|y_0-v|}^{v+\rho \xi_0} \sum_{n \in \{L,N\}} \zeta^*_{\lambda}(u,v)p_n(u) f_{d_{y_0,v}}(u) du,

(12)

$\zeta^*_{\lambda}(u,v)$ is $\zeta^*_{\lambda}(u,v) = \int_0^{\frac{\lambda w}{\lambda w}} e^{-\frac{\lambda (\lambda_w + \lambda_w) \Lambda(\lambda, w) d w}{\lambda w}} du < \rho \alpha \tau$ and is $\zeta^*_{\lambda}(u,v) = 1 - \rho \int_0^{\frac{\lambda w}{\lambda w}} e^{-\frac{\lambda (\lambda_w + \lambda_w) \Lambda(\lambda, w) d w}{\lambda w}} du$ for $u > \alpha \tau$. Let $\Lambda(\lambda, w) = \lambda w - w^{\frac{1}{\alpha}} + \frac{2\pi \lambda^2}{\beta^2} (1 + \beta w^{\frac{1}{\alpha}}) e^{-\beta w^{\frac{1}{\alpha}}} + \frac{2\pi \lambda}{\beta^2} (1 + \beta w^{\frac{1}{\alpha}}) e^{-\beta w^{\frac{1}{\alpha}}}$, and $\Lambda(\lambda, w)$ is the derivative of $\Lambda(\lambda, w)$.

Proof: See Appendix B.

With the help of Lemma 4, we derive the Laplace transform of $I_{y_0}$ under the LOWJ attack in the following lemma.

Lemma 5: The Laplace transform of $I_{y_0}$ under the LOWJ attack can be lower bounded by

$$L_{y_0}(s) \geq \exp \left( -2\pi \lambda_E \int_0^\infty \right) \left( 1 - \mathbb{E}_{G_{j,R}^{z,y_0},h_{y_0,z}} e^{-s \frac{1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z}}{\lambda_w}} \right) \right) v dv}

(13)

where $\Omega_{j,R}(s, v) = k(\tau + \rho \xi_0)$ can be obtained from (4).

Proof: We divide $\Phi_E$ into independent sub-PPPs $\Phi^f_E$ of attackers with link status $\tau \in \{L, N\}$ to $y_0$, i.e., $\Phi_E = \cup_{\tau} \Phi^f_E$. Formally, $\Phi^f_E$ is given by $\Phi_E = \{ z \in \Phi_E : S_{z,y_0} = \tau \}$. Hence, we have $I_{y_0} = \sum_{\tau} I_{y_0}^{\tau}$, where $I_{y_0}^{\tau} = \sum_{z \in \Phi_E} 1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z} d_{y_0,z}$, and thus $L_{y_0}(s) = \prod_{\tau} L_{y_0}^{\tau}(s)$, where $L_{y_0}^{\tau}(s)$ is the Laplace transform of $I_{y_0}^{\tau}$. It follows from Lemma 3 that $L_{y_0}^{\tau}(s) \geq \exp \left( -2\pi \lambda_E \int_0^\infty \right) \left( 1 - \mathbb{E}_{G_{j,R}^{z,y_0},h_{y_0,z}} e^{-s \frac{1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z}}{\lambda_w}} \right) \right) v dv}$, which completes the proof.

D. Derivation of $L_{y_0}(s)$ Under POWJ Attack

The probability of being a jammer also depends on the effective antenna gain to the receiver $y_0$ under the POWJ attack and is given by the following lemma.

Lemma 6: The probability that an attacker $z$ with distance $v$ and link status $\tau \in \{L, N\}$ and effective antenna gain $g_{y_0}^{\tau}(r)$ to $y_0$ is a jammer under the POWJ attack can be approximated by

$$\zeta_{\tau,n,o}(v) \approx \int_{|y_0-v|}^{v+\rho \xi_0} \sum_{n \in \{M,N\}} \zeta^*_{\lambda}(u,v)p_n(u) f_{d_{y_0,v}}(u) du,

(14)

where $u \in \{L, N\}$. In $l \in \{M, S\}$, $m \in \{M, S\}$. $\zeta_{\tau,n,o}(u, v) = \int_0^\infty e^{-\frac{\lambda \Lambda(\lambda, w) + \Lambda(\lambda, w) \Lambda(\lambda, w)}{\lambda w}} d w = \frac{\eta_1}{\rho \eta_2}$ and $\eta_2 = \frac{\eta_1}{\rho \eta_2}$ and is $1 - \rho \int_0^\infty e^{-\frac{\lambda \Lambda(\lambda, w) + \Lambda(\lambda, w) \Lambda(\lambda, w)}{\lambda w}} d w$. Let $\Lambda(\lambda, w) = \sum_{i,j} \Lambda(p_i^{lM} \lambda, p_j^{lM} \lambda) (i \in \{M, S\}, j \in \{M, S\})$, $\Lambda(\lambda, w)$ are the derivatives of $\Lambda(\lambda, w)$.

Proof: See Appendix C.

Note that the approximation in (14) is due to the fact that we neglect the dependence between $G_{j,R}^{z,y_0}$ and $G_{j,R}^{z,y_0}$. Given the probability $\zeta_{\tau,n,o}(v)$, we derive the Laplace transform of $I_{y_0}^{\tau}$ under the POWJ attack as follows.

Lemma 7: The Laplace transform of $I_{y_0}^{\tau}$ under the POWJ attack can be approximated by

$$L_{y_0}^{\tau}(s) \approx \exp \left( -2\pi \lambda_E \int_0^\infty \right) \left( 1 - \mathbb{E}_{G_{j,R}^{z,y_0},h_{y_0,z}} e^{-s \frac{1_j \beta_j G_{j,R}^{z,y_0} h_{y_0,z}}{\lambda_w}} \right) \right) v dv}

(15)

where $\Omega^{\tau,n,o}(s, v) = k(\tau + \rho \xi_0)$ can be obtained from (3).

Proof: Similar to the proof of Lemma 5, $L_{y_0}^{\tau}(s)$ can be rewritten as $L_{y_0}^{\tau}(s) = \prod_{\tau,n,o} L_{y_0}^{\tau,n,o}(s)$, where $L_{y_0}^{\tau,n,o}(s)$ is the Laplace transform of the interference caused by the attackers with link status $\tau$ and effective antenna gain.
Based on Lemma 3, \( L_{x_0, z}^{T, n, o}(s) \) can be given by \( L_{x_0, z}^{T, n, o}(s) \geq \exp \left( -2\pi \lambda E \int_0^{\infty} \Omega_{1, T} \left( t \left( t+1 \right) \right) \right) \), which completes the proof.

IV. Secrecy Probability Analysis

In this section, we focus on the typical link \( x_0 \rightarrow y_0 \) again and derive a unified expression of the secrecy probability. We then analyze the key term involved in the unified expression, i.e., the Laplace transforms of the interference from the transmitters to any attacker under the DOWJ, LOWJ and POWJ attacks in Sections IV-B, IV-C and IV-D, respectively.

A. Secrecy Probability

The secrecy probability is formulated as \( p_s = \mathbb{P} \left( \bigcup_{i,j \in \Phi_{x_0,z}} \{ \log(1 + \text{SINR}_{x_0,z}) \leq R_e \} \right) \), where \( \text{SINR}_{x_0,z} \) denotes the SINR of a wiretapper \( z \in \Phi_{x_0,z} \). We consider an equivalent formulation of \( p_s \) by assuming that all attackers are wiretapping on the typical link. Since jammers actually do not interfere with the transmitters, we remove their impact by setting their interferences to zero. The SINR then becomes equivalent to the best possible SINR.

We divide the PPP \( \Phi_E \) into sub-PPP's \( \Phi_{E, k,l,m} \) of attackers with link status \( k \in \{L, N\} \) and antenna gain \( g_{lm} \) \( (l, m \in \{M, S\}) \) to \( x_0 \). Hence, \( p_s \) can be rewritten as

\[
p_s = \prod_{k,l,m} p_{k,l,m}^{E, k,l,m}
\]

Following the common assumption in [46], [47], and [48], we assume that wiretappers can perfectly suppress interference from jammers. This assumption corresponds to the best-case assumption of attackers. Thus, for any \( z \in \Phi_{E, k,l,m} \), we have \( \text{SINR}_{x_0,z}^{E, k,l,m} = \frac{P_T g_{E, k,l,m}^{x_0,z} \sigma^2 \alpha}{I_z^2 + \sigma^2} \), where \( I_z^2 \) denotes the interference from concurrent transmitters, which equals \( I_z^2 = \sum_{x \in \Phi_E \setminus \Phi_{x_0,z}} P_T G_x^{x_0,z} h_x z_x d_x^{-\alpha} \) for \( 1_j = 0 \) and \( \infty \) for \( 1_j = 1 \). We now derive the secrecy probability based on the above formulations.

**Theorem 2:** The secrecy probability of the typical transmission pair \( x_0 \rightarrow y_0 \) under the DOWJ, LOWJ and POWJ attacks can be approximated by

\[
p_s \approx \exp \left( -2\pi \lambda E \sum_{k,l,m} p_{lm}^{S, k,l,m} \sum_{t=1}^{N_e} \left( N_e \right) \frac{(-1)^{t+1}}{t} \right)
\]

\[
\int_0^{\infty} p_s(u) e^{-u \times T, n, o \cdot} \frac{u^m}{E_{z,n, o}^{T, n, o}(s)} \frac{du}{\nu_k, l, m} \nu_k, l, m, (t \nu_k, l, m, u^\alpha, u) \right),
\]

where \( \nu_k, l, m = \frac{N_e(N_e-1)\cdots(N_e-2)}{P_T g_{lm}} \) and \( L_{z,n, o}^{T, n, o}(s) \) denotes the Laplace transform of \( I_z^2 \) for any attacker \( z \in \Phi_{E, k,l,m} \).

**Proof:** According to (16), we first derive \( p_{k,l,m}^{S, k,l,m} \) as

\[
p_{k,l,m}^{S, k,l,m} = \mathbb{P} \left( \bigcap_{z \in \Phi_{E, k,l,m}} \{ \log(1 + \text{SINR}_{x_0,z}^{E, k,l,m}) \leq R_e \} \right)
\]

\[
\approx \exp \left( -2\pi \lambda E \sum_{t=1}^{N_e} \left( N_e \right) \frac{(-1)^{t+1}}{t} \right)
\]

\[
\int_0^{\infty} p_s(u) e^{-u \times T, n, o \cdot} \frac{u^m}{E_{z,n, o}^{T, n, o}(s)} \frac{du}{\nu_k, l, m} \nu_k, l, m, (t \nu_k, l, m, u^\alpha, u) \right),
\]

following from Theorem 2 in [27]. Substituting (18) into (16) completes the proof.

From (17), we know that the key term involved in \( p_s \) is the Laplace transform \( L_{z,n, o}^{T, n, o}(s) \). In what follows, we will derive the expressions of \( L_{z,n, o}^{T, n, o}(s) \) under the DOWJ, LOWJ and POWJ attacks, respectively. Prior to the derivation, we first give the following functions for any \( k \in \{L, N\}, \ i \in \{M, S\}, \ j \in \{M, S\}, \ l \in \{T, J\} \) and \( z \in \{R, W\} \).

\[
Z_{k,l,m}^{T, k,l,m}(s, \lambda, u) = \exp \left( -2\pi \lambda \int_{\infty}^{\infty} \Omega_{k,l,m}^{T, k,l,m}(t, \lambda, u) \right),
\]

\[
Z_k^{T, k,l,m}(s, \lambda, c) = \prod_{i,j} Z_{k,l,m}^{T, k,l,m}(s, \lambda, c)
\]

\[
= \exp \left( -2\pi \lambda \int_{\infty}^{\infty} \Omega_{k,l,m}^{T, k,l,m}(t, \lambda, c) \right),
\]

where \( \Omega_{k,l,m}^{T, k,l,m}(t, \lambda, u) \) and \( \Omega_{k,l,m}^{T, k,l,m}(t, \lambda, c) \) are given in (3), (4) and (5), respectively.

B. Derivation of \( L_{z,n, o}^{T, n, o}(s, u) \) Under DOWJ Attack

Note that the DOWJ attack is dependent solely on the distances from \( z \) to the transmitters and receivers. Thus, the Laplace transform \( L_{z,n, o}^{T, n, o}(s,u) \) varies with only \( d_{x_0,z} = u \). We rewrite \( L_{z,n, o}^{T, n, o}(s,u) \) as \( L_{z}^{T} \) \( (s,u) \) and derive its expression in the following lemma.

**Lemma 8:** The Laplace transform of the interference caused by the concurrent transmitters at any attacker \( z \in \Phi_{E, k,l,m} \) with distance \( u \) to the typical transmitter \( x_0 \) under the DOWJ attack is

\[
L_{z}^{T}(s,u) = \mathbb{E}_{T, W}(s, \lambda, 0) - \mathbb{E}_{d_{x_0,z}}(c_u)
\]

\[
\int_{0}^{\infty} \mathbb{E}_{T, W}(s, \lambda, \rho \cdot) \pi \lambda \rho \cdot \frac{d\rho}{\rho \cdot} + \mathbb{E}_{d_{x_0,z}}(c_u)
\]

\[
- \int_{0}^{\infty} \mathbb{E}_{T, W}(s, \lambda, \rho \cdot) \pi \lambda \rho \cdot \frac{d\rho}{\rho \cdot} + \mathbb{E}_{d_{x_0,z}}(c_u)
\]

\[
2\pi \lambda \rho \cdot \pi \lambda \rho \cdot \frac{d\rho}{\rho \cdot} + \mathbb{E}_{d_{x_0,z}}(c_u)
\]
where \( c_u = \min \{ \{ u \rho, |u - r_0| \}, u + r_0 \} \), \( \hat{F}_{d_{x_0,z}}(v) = 1 - \frac{1}{\pi} \arccos \left( \frac{\sqrt{r_0^2 + u^2 - v^2}}{2v} \right) \) is the CCDF of \( d_{x_0,z} \) and \( f_{d_{x_0,z}}(v) = \frac{1}{\pi \sqrt{r_0^2 + u^2 - v^2}} \) is the corresponding PDF.

**Proof:** See Appendix D.

### C. Derivation of \( \mathcal{L}_{z,k,l,m}^T(s,u) \) Under LOWJ Attack

Note that the Laplace transform \( \mathcal{L}_{z,k,l,m}^T(s,u) \) under the LOWJ attack varies with \( d_{x_0,z} = u \) and \( S_{x_0,z} = \kappa \). Rewriting \( \mathcal{L}_{z,k,l,m}^T(s,u) \) as \( \mathcal{L}_{z,k}^T(s,u) \), we give the Laplace transform \( \mathcal{L}_{z,k}^T(s,u) \) in the following lemma.

**Lemma 9:** The Laplace transform of the interference caused by the concurrent transmitters at any attacker \( z \in \Phi_E^{k,l,m} \) with distance \( u \) and link status \( \kappa \) to the typical transmitter \( x_0 \) under the LOWJ attack is

\[
\mathcal{L}_{z,k}^T(s,u) = \int_{|u-r_0|}^{u+r_0} \sum_{\tau} \mathcal{L}_{z,k}^{T,\tau}(s,u,v)p_{\tau}(v)f_{d_{x_0,z}}(v)dv,
\]

where \( \mathcal{L}_{z,k}^{T,\tau}(s,u,v) \) is given by

\[
\Xi_{T,W}(s,\lambda,0) - \int_0^{|u-s\alpha|} e^{-\left(\hat{\Lambda}(1,\rho_w\lambda) + \hat{\Lambda}(\lambda,\rho_w)\right)\frac{d}{k}} dw,
\]

for \( u^{\alpha_2} < \rho_u^{\alpha_2} \) and given by

\[
\Xi_{T,W}(s,\lambda,0) - \int_0^{|u-s\alpha|} e^{-\left(\hat{\Lambda}(1,\rho_w\lambda) + \hat{\Lambda}(\lambda,\rho_w)\right)\frac{d}{k}} dw,
\]

for \( u^{\alpha_2} \geq \rho_u^{\alpha_2} \).

**Proof:** See Appendix E.

### D. Derivation of \( \mathcal{L}_{z,k,l,m}^T(s,u) \) Under POWJ Attack

Note that the Laplace transform \( \mathcal{L}_{z,k,l,m}^T(s,u) \) under the POWJ attack varies with \( d_{x_0,z} = u \), \( S_{x_0,z} = \kappa \) and \( \mathcal{G}_{T,W} = g_{TW}^T \). The following lemma summarizes the Laplace transform \( \mathcal{L}_{z,k,l,m}^T(s,u) \) under the POWJ attack.

**Lemma 10:** The Laplace transform of the interference caused by the concurrent transmitters at any attacker \( z \in \Phi_E^{k,l,m} \) with distance \( u \), link status \( \kappa \) and antenna gain \( g_{TW}^T \) to the typical transmitter \( x_0 \) under the POWJ attack can be approximated by

\[
\mathcal{L}_{z,k,l,m}^T(s,u) \approx \int_{|u-r_0|}^{u+r_0} \sum_{\tau,\kappa} \tilde{p}_{\mu} \mathcal{L}_{z,k,l,m}^{T,\tau,\kappa}(s,u,v)p_{\tau}(v)f_{d_{x_0,z}}(v)dv,
\]

where \( \mathcal{L}_{z,k,l,m}^{T,\tau,\kappa}(s,u,v) \) is given by

\[
\Xi_{T,W}(s,\lambda,0) - \int_0^{\frac{u_2}{\rho_w}} e^{-\left(\hat{\Lambda}(1,\rho_w\lambda) + \hat{\Lambda}(\lambda,\rho_w)\right)\frac{d}{k}} dw,
\]

for \( \eta_1 < \rho \eta_2 \) and given by

\[
\Xi_{T,W}(s,\lambda,0) - \int_0^{\frac{u_2}{\rho_w}} e^{-\left(\hat{\Lambda}(1,\rho_w\lambda) + \hat{\Lambda}(\lambda,\rho_w)\right)\frac{d}{k}} dw,
\]

for \( \eta_1 \geq \rho \eta_2 \).

**Proof:** See Appendix F.

**Remark 1:** Although available works also applied PPPs to the secrecy performance study of mmWave systems [27], [28], [29], they are usually based on the common assumption that the locations of jammers and wiretappers can be modeled by a homogeneous PPP. Thus, these works cannot be adopted to model the heterogeneous distribution of the jammers and wiretappers in this paper, which is caused by the location-based opportunistic attack selection.

### E. Optimal \( \rho \)

As \( \rho \) increases, more attackers will choose to wiretap, leading to a decreased secrecy probability \( p_s \) but an increased connection probability \( p_c \). This implies that there would exist an optimal \( \rho \) to minimize the network STC performance from the perspective of the attackers. The optimal \( \rho^* \) can be obtained in a centralized manner, where we assume that one attacker acts as a coordinator to gather the required network information, compute the network STC and conduct an STC minimization problem. The process of obtaining the optimal \( \rho^* \) is as follows.

- **Step 1:** The coordinator gathers the required network parameters (e.g., \( \lambda \) and \( \lambda_E \)) and evaluates the network STC performance based on the parameters and Theorems 1 and 2;
- **Step 2:** The coordinator solves the optimization problem

\[
\rho^* = \arg \min_{\rho \in (0, \infty)} \lambda p_s(\rho)p_c(\rho)(R_s - R_c)
\]

- **Step 3:** The coordinator distributes the optimal \( \rho^* \) to other attackers;
- **Step 4:** Each attacker sets its \( \rho \) to \( \rho^* \), collects required network information, calculates its costs of jamming and wiretapping, and conducts the OWJ attack.

Unfortunately, a closed-form expression for \( \rho^* \) is not available because the secrecy probability and connection probability involve complex integrals with \( \rho \) in the upper limit. Actually, we can see that the optimization problem is just one-dimensional and thus can be easily solved by some one-dimensional search methods like the Golden Section Search and Fibonacci Search.
TABLE II
PARAMETERS USED IN SIMULATIONS

| Parameters           | Value |
|----------------------|-------|
| Carrier frequency    | 28 GHz|
| Link distance $r_0$ | 50[m] |
| Channel bandwidth    | 1 GHz |
| Noise spectral density | $-174$ dBm/Hz |
| Transmit power $P_T$ | 1 W (i.e., 30 dBm) |
| Path loss exponent $\alpha_L$ ($\alpha_N$) | 2 (4) |
| Nakagami fading parameter $K_L$ ($K_N$) | 3 (2) |
| Block density $\beta$ | 1/141.4 |
| ML beam width $\theta_T$, $\theta_R$, $\theta_J$ | $\pi/6$ |
| ML gain $G_T$, $G_R$, $G_J$, $G_M$ | 10 |
| SL gain $G_{R_1}$, $G_{R_2}$, $G_{J_1}$, $G_{J_2}$ | 0.1 |

V. NUMERICAL RESULTS

This section provides simulation results to validate the secrecy and connection probabilities, followed by discussions on the impacts of system parameters on the STC performance. We also compare the attack effect of the three OWJ attacks in terms of the STC performance.

A. Simulation and Validation

A dedicated simulator was developed to simulate the transmission process in a Poisson mmWave bipolar network. Using this simulator, we conducted simulations for the secrecy probability and connection probability of the network under the DOWJ, LOWJ and POWJ attacks with different densities of attackers $\lambda_E$, densities of legitimate transmission pairs $\lambda$, jamming power $P_J$ and bias factor $\rho$. The common parameters are summarized in Table II.

We summarize the simulation results and also the theoretical ones in Figs. 1 and 2 under different settings of $\lambda_E$, $\lambda$, $P_J$ and $\rho$, respectively. We can see that the theoretical results provide good approximations or tight bounds for the secrecy probability $p_s$ and connection probability $p_c$ under all three OWJ attacks, implying the effectiveness of the derived analytical expressions under different system parameters. The above results show that: (1) $p_s$ decreases as $\lambda_E$ and $\rho$ increase while it increases as $\lambda$ increases under all OWJ attacks; (2) $p_s$ under DOWJ and LOWJ are independent of $P_J$, while that of POWJ increases as $P_J$ increases; (3) $p_c$ decreases as $\lambda_E$, $\lambda$ and $P_J$ increase, while it increases as $\rho$ increases under all three OWJ attacks.

B. Attack Effect Evaluation

This subsection investigates the impacts of key system parameters on the attack effect based on the analytical expressions in Sections III and IV. We define the attack effect as the reduction of the network STC with respect to a baseline STC, which is achieved when no attacks are conducted. Since the baseline STC is independent of the attack and is thus identical for DOWJ, LOWJ and POWJ, we use the STC as the criterion instead to measure the attack effect. Obviously, a smaller STC means a larger STC reduction and thus a better attack effect.

1) STC Vs. $\lambda_E$: We first explore the impact of the attacker density $\lambda_E$ on the network STC performance, for which we show in Fig. 3a STC vs. $\lambda_E$ under all the three OWJ attacks. The results show that the STC decreases as $\lambda_E$ increases for a given $\rho$ under all three OWJ attacks, which is due to the more wiretappers and jammers resulting from the increased $\lambda_E$.

2) STC Vs. $\lambda$: Fig. 3b plots the STC vs. $\lambda$ under all three OWJ attacks. We can see from Fig. 3b that, as $\lambda$ increases, the STC first increases and then decreases under all three OWJ attacks. The reason is that the increase of $\lambda$ dominates the trend of the STC for small $\lambda$’s, while as $\lambda$ continues to increase, the secrecy probability remains almost unchanged and the decrease of the connection probability becomes the dominant factor (as shown in Figs. 1b and 2b), leading to the decrease of the STC. The results in Fig. 3b reveal the existence of the optimal density of transmission pairs given a network and its key parameters.

3) STC Vs. $P_J$: Fig. 3c plots STC vs. $P_J$ under all the three OWJ attacks. We can see that, as $P_J$ increases, the STCs under DOWJ and LOWJ decrease while that under POWJ first increases and then decreases. This is because DOWJ and LOWJ are independent of $P_J$ and thus the increase of $P_J$ leads to only the increase of the interference level to the receivers, decreasing the connection probabilities. For POWJ, as $P_J$ increases, the probability of wiretapping decreases while that of jamming increases, leading to increased secrecy probability and decreased connection probability. The STC is dominated by the secrecy probability for small $\rho$’s and dominated by the connection probability for large $\rho$’s.

4) STC Vs. $\rho$: Fig. 4a shows STC vs. $\rho$ under two different settings of $\lambda_E$ (i.e., $\lambda_E = 0.0001$ and $\lambda_E = 0.0002$). We can see that, as $\rho$ increases, the STC first decreases and then increases under all the three OWJ attacks, implying the existence of the optimal $\rho^*$ for attackers to minimize the network STC performance, i.e., maximizing the attack effect. This shows that neither pure jamming (i.e., $\rho \rightarrow 0$) nor pure wiretapping (i.e., $\rho \rightarrow \infty$) is the optimal strategy and the OWJ attacks are more favorable for attackers. Careful observation shows that the optimal $\rho$ decreases as $\lambda_E$ increases, indicating that attackers prefer the jamming attack more as their density increases. To compare the attack effect of the three OWJ attacks, we focus on the worst STC performance they can achieve. Fig. 4a shows that the worst STC achieved by POWJ is the smallest among the three OWJ attacks, while LOWJ and DOWJ achieves almost the same worst STC.

To show the generality of our findings, we also plot STC vs. $\rho$ in Fig. 4b under two different jamming powers and in Fig. 4c under two different densities of transmission pairs. Both figures can observe findings similar to those in Fig. 4a. We can also see from Fig. 4b and Fig. 4c that the optimal $\rho$ decreases as the jamming power $P_J$ and the transmission density $\lambda$ increase, respectively, suggesting that attackers prefer the jamming attack more if they can choose a larger jamming power, or when more transmissions exist in the network.

5) OWJ Model Vs. Pure Wiretapping and Jamming: To investigate the superiority of the proposed OWJ model to the traditional pure wiretapping and jamming attacks, we plot in Fig. 5 the smallest (i.e., optimal from the perspective of attackers) STCs under the DOWJ, LOWJ and POWJ attacks and the STCs under the pure attacks with the jamming power $P_J$ varying from 0 W to 50 W. From the above figures, we can see that: (1) LOWJ has a slightly better attack effect than DOWJ in only a small range of jamming.
In most cases, they have almost the same attack effect; (2) When the jamming power is small, the smallest STCs of DOWJ and LOWJ approach that of pure wiretapping, which is much smaller than that of pure jamming but larger than the smallest STC of POWJ. For a large jamming power, the smallest STCs of DOWJ and LOWJ approach that of pure jamming, which is much smaller than that of pure wiretapping but larger than that of POWJ; (3) POWJ achieves significantly smaller STC than both pure attacks in a large range of jamming power settings (e.g., 0-50 W in the figures), while DOWJ and LOWJ outperform both pure attacks in only a small range of jamming power (10-20 W). To conclude, the superiority of POWJ to both pure attacks is much more significant than DOWJ and LOWJ.
wiretapping is superior to pure jamming when small jamming powers are used, while it is the opposite when large jamming powers are used.

6) **DOWJ Vs. LOWJ Vs. POWJ**: We comprehensively compare DOWJ, LOWJ and POWJ in terms of attack effect, energy consumption and cost of obtaining required information, which is summarized in Table III. Fig. 5 clearly shows that, for a given jamming power (i.e., a certain level of energy consumption), DOWJ achieves the worst attack effect, LOWJ achieves a slightly better attack effect than DOWJ (especially for moderate jamming powers) but a much worse attack effect than POWJ. From the energy consumption perspective, we can see that to achieve the same level of attack effect, POWJ requires the smallest jamming power (i.e., the lowest energy consumption), while DOWJ requires the largest jamming power and LOWJ requires a slightly smaller jamming power than DOWJ. In terms of the cost of obtaining the required information for performing the attack, DOWJ requires only the locations of the transmission pairs, which incurs the lowest cost. LOWJ also requires information of the path losses in addition to the location information, leading to a medium cost. POWJ requires the most amount of information, which includes not only path loss and location but also the transmit power and antenna patterns of the transmission pairs. To summarize, POWJ is the best option when all the required information is available. If not, DOWJ is recommended over LOWJ because the former achieves a slightly worse attack effect with much less information.

### C. Discussions

1) **Impact of Attackers’ Antenna Alignment**: In this paper, we assume that attackers’ antennas are directed randomly. This means that the SL of a wiretapper (resp. jammer) will be directed to the SL of the typical transmitter $x_0$ (resp. receiver $y_0$) in some cases, leading to poor wiretapping (resp. jamming) effect. Attackers are expected to improve their attack effect if they can avoid the SL-SL antenna patterns by properly aligning antennas. However, SL-SL antenna patterns cannot be completely avoided in our work because the attackers target all transmission pairs rather than a particular one. This means that if an attacker aligns its antenna with respect to a reference pair, the SL of its antenna will be directed to the SL of some other pair inevitably.

Despite this fact, it would still be interesting to consider a fictitious attack as the fourth OWJ model, where an attacker can align its antenna somehow to avoid the SL-SL antenna pattern to the typical transmission pair. More specifically, each attacker conducts the OWJ model first to decide its attack strategy (i.e., jamming or wiretapping) and then aligns its antenna according to the following rule: If the SL of $x_0$’s ($y_0$’s) antenna is observed, a wiretapper (jammer) directs its ML to $x_0$ ($y_0$). Otherwise, no alignment is conducted. Thus, the effective antenna gain $g_{SS}^{TW}$ becomes $G_S^T G_M^W$ with probability $p_{SS}^{TW} = \frac{(2\pi - \theta_0)(2\pi - \theta_W)}{(2\pi)^2}$ and $g_{SS}^{JR}$ becomes $G_M^R G_S^L$ with probability $p_{SS}^{JR} = \frac{(2\pi - \theta_J)(2\pi - \theta_R)}{(2\pi)^2}$. We assume that the antenna gains between the attackers and the other pairs still follow the model in (1). Based on the new antenna gains, we can obtain the connection and secrecy probabilities under the OWJ model with antenna alignment (OWJ-AA). Fig. 6 plots the STC performance under the new OWJ-AA model, which significantly outperforms the OWJ models in degrading the network STC.

We can also see from Fig. 6 that while POWJ outperforms DOWJ and LOWJ in the non-AA case, POWJ-AA is noticeably worse than DOWJ-AA and LOWJ-AA. This is mainly due to the following reasons. When applying POWJ to an attacker, it will take the advantage of additional knowledge of antenna gains and power settings (i.e., antenna gains both from the attacker to all receivers and from all transmitters to the attacker, as well as the transmit power of all transmitters and the jamming power of the attacker) to measure both jamming power to all receivers and received power from all transmitters, and make a decision to perform jamming or wiretapping attack based on a comparison between such jamming power and received power. Thus, if an attacker performs a jamming (resp. wiretapping) attack under the POWJ scheme, the attacker is most likely antenna-aligned toward a nearby receiver (resp. nearby transmitter). In this sense, by taking the advantage of additional knowledge of antenna gains and power settings, POWJ achieves a similar effect of adopting AA. Actually, such AA operation can lead to a significant enhancement in attack effects as we can see from Fig. 6. However, when all schemes adopt AA, the POWJ may become less efficient than DOWJ and LOWJ, so the corresponding POWJ-AA scheme may be even worse than DOWJ-AA and LOWJ-AA.

2) **Smaller STC Achieved by DOWJ Than LOWJ**: The network STC generally decreases when more information about the transmission pairs is known to the attackers. However, the results in Figs. 3b, 4b and 4c show that this is not always true and DOWJ achieves smaller STC than LOWJ in some cases. The fundamental reason is that LOWJ cannot achieve both a smaller secrecy probability and a smaller connection probability than DOWJ simultaneously, as can be observed from Figs. 1 and 2. More specifically, the secrecy (resp. connection) probability of LOWJ is smaller (resp. larger) than that of DOWJ for $\rho < 1$, while it is the opposite for $\rho > 1$. This is determined by the probability of selecting the jamming attack (i.e., jamming probability), which leads to a smaller (resp. larger) density of jammers under LOWJ than under DOWJ for $\rho < 1$ (resp. $\rho > 1$) in most cases, and thus a larger (resp. smaller) connection probability and a smaller (resp. larger) secrecy probability. The comparison of the jamming probabilities under both attacks is shown in Fig. 7. Since STC is the product of the secrecy probability and connection probability, the STC under DOWJ is smaller than that under LOWJ when the secrecy probability of DOWJ is smaller (resp. larger) than that of the LOWJ and such relative difference is much larger (resp. smaller) than the relative difference between the connection

| Attack | Attack effect | Energy consumption | Cost of obtaining information |
|--------|--------------|--------------------|-------------------------------|
| DOWJ   | Worst        | Highest            | Lowest                        |
| LOWJ   | $\leq$ DOWJ  | $\leq$ DOWJ        | Medium                        |
| POWJ   | Best         | Lowest             | Highest                       |

TABLE III

**COMPARISON OF DOWJ, LOWJ AND POWJ**

For more detailed analysis and discussions, see the full paper.
probabilities of the two attacks, which corresponds to the cases in Figs. 3b, 4b and 4c.

3) Countermeasures to OWJ Attack: There exist some common approaches to counteracting the OWJ attack. A typical one is artificial noise injection, where each transmitter sends information signals to the intended receiver through its main lobe while radiating artificial noise in the side lobe. In this way, wiretappers will receive more interference than the receivers, thus improving the network’s secrecy performance. Apart from these common approaches, dedicated approaches to counteracting each OWJ realization are also possible. For example, location spoofing (e.g., via software-defined radio equipment USRP and open-source software gps-sdr-sim) can be used to falsify the obtained location information of the attackers [58], directly impeding the attack process of the DOWJ. Pilot contamination can be used to falsify the channel state information obtained by the attackers [59], pushing them to make wrong attack decisions in the LOWJ and POWJ realizations and thus improving network secrecy. Location spoofing and pilot contamination can be combined to further improve network secrecy.

4) STC on mmWave Frequency Vs. STC on Microwave Frequency: We conducted simulations for the STC of microwave networks with/without the proposed OWJ model under the settings of $\lambda = 0.0001$, $\lambda_{E} = 0.0001$, $P_J = 10$. Here, the widely-used Rayleigh fading channel model is adopted (i.e., $K_L = K_N = 1$) and the path loss exponent $\alpha$ is set to a typical value of 4 (i.e., $\alpha_L = \alpha_N = 4$). We summarized in Fig. 8 the simulation results and also the theoretical ones for both mmWave frequency and microwave frequency. We can see from Fig. 8 that the STC performance of the mmWave frequency changes more sharply than that of the microwave frequency, implying that mmWave networks are more sensitive to the proposed OWJ attack. We can also see that the OWJ model achieves a better attack effect than both the pure wiretapping and jamming attack on mmWave frequency, while it only achieves a better attack effect than the wiretapping attack on microwave frequency. In addition, the gap between the STC of the pure jamming/wiretapping attack and the worst STC of the OWJ attack in the mmWave frequency scenario is larger than in the microwave frequency scenario. The above observations indicate that the OWJ attack is more effective for enhancing the attack effect in mmWave networks than that in microwave networks.

The main reason behind the above results lies in the difference of LoS/NLoS transmissions in mmWave networks and microwave networks. We know from the results in the literature [1], [2], [3], [4], [5] that both LoS and NLoS links experience the same path loss in the microwave frequency scenario, while LoS links suffer from less path loss than NLoS.
links in the mmWave frequency scenario. Suppose an attacker is initially designed to operate only in the pure wiretapping mode and it has an NLoS link to $x_0$ but an LoS link to $y_0$. In the mmWave frequency scenario, the proposed OWJ attack model will likely allow the attacker to switch from wiretapping to jamming for improved attack effect since the jamming link to $y_0$ shows an advantage in terms of path loss on mmWave frequency. However, this is not the case for the microwave frequency scenario since both LoS and NLoS links experience the same path loss there. A similar discussion also holds when the attacker is initially designed to operate only in the pure jamming mode and it has an LoS link to $x_0$ but an NLoS link to $y_0$.

VI. CONCLUSION

This paper proposed a new opportunistic wiretapping and jamming (OWJ) attack model for millimeter-wave (mmWave) wireless networks and provided three realizations, namely distance-based OWJ (DOWJ), loss-based OWJ (LOWJ) and power-based OWJ (POWJ), each with a different cost model. Analytical expressions of secrecy transmission capacity (STC) were derived to depict the network security performance under the OWJ attack. The following main conclusions can be drawn from this paper. In general, the proposed OWJ attack can lead to a degraded STC performance than the conventional pure wiretapping or jamming attacks. In particular, the POWJ attack model achieves the best attack effect while the DOWJ and LOWJ models lead to almost the same attack effect. By employing the antenna alignment technique, a new antenna alignment-assisted OWJ model may be devised to further significantly improve the attack effect. Another observation is that under the optimal attack setting, an attacker prefers the jamming attack more when a larger jamming power is allowed, when the density of attackers is high, or when more transmission pairs exist in the network. Some possible future directions should also be considered. First, while this paper focuses on exclusive wiretapping and jamming attacks, one possible future work is to consider the more hazardous non-exclusive wiretapping and jamming attacks. Second, using jammers as helpers to improve the amount of intercepted sensitive data of the wiretappers serves as another interesting attack model, which also deserves dedicated future work. Third, it is interesting to consider the attack model design under a more realistic scenario where wiretappers cannot eliminate interference from nearby jammers.

APPENDIX

A. Proof of Lemma 2

Suppose $d_{x_0,z} = u$ and $\tilde{D}_T = \min_{x \in \Phi_T \setminus \{x_0\}} d_{x,z}$ and $\tilde{D}_L = \min_{y \in \Phi_L \setminus \{y_0\}} d_{y,z}$. We use $A$ (resp. $B$) to denote the event that $x_0$ (resp. $y_0$) is the nearest transmitter (resp. receiver) to $z$, i.e., $A : \tilde{D}_T \geq u$ and $B : \tilde{D}_L \geq v$. The event $1_j^z = 1$ occurs if the following cases happen: (1) $A \cap B \cap \{u \geq v\}$; (2) $A \cap B \cap \{u \geq v\}$; (3) $\tilde{D}_T \geq v$; (4) $\tilde{D}_L \geq v$. Combining the four cases, we have $1_j^z = 1$ if $\tilde{D}_T \geq \rho \tilde{D}_L$, $\tilde{D}_L < \frac{u}{\rho}$ for $u < \rho v$ and if $\tilde{D}_L \geq \rho v$, $\tilde{D}_L \geq v$ or $\tilde{D}_L \geq \rho \tilde{D}_L$, $\tilde{D}_R < v$ for $u \geq \rho v$. Note that $\tilde{D}_L$ (resp. $\tilde{D}_R$) has the same PDF and CDF as those of $D_L$ (resp. $D_R$), with which we obtain the probability of $1_j^z = 1$ conditioned on $d_{x_0,z} = u$ as $\zeta(u,v) = \frac{1}{\rho^2 + \frac{1}{\rho^2}}(1 - e^{-\left(1+\frac{1}{\rho^2}\right) \lambda \pi u^2})$ for $u < \rho v$ and $\zeta(u,v) = \frac{1}{\rho^2 + \frac{1}{\rho^2}} e^{-\left(1+\frac{1}{\rho^2}\right) \lambda \pi v^2}$ for $u \geq \rho v$.

Calculating the expectation of $\zeta(u,v)$ in terms of $d_{x_0,z}$ yields $\zeta(v)$ in (8).

B. Proof of Lemma 4

Suppose $d_{x_0,z} = u$ and $S_{x_0,z} = \kappa \in \{L,N\}$. According to Appendix A, $1_j^z = 1$ if $\tilde{L}_T \geq \rho \tilde{L}_R$, $\tilde{L}_R < \frac{u}{\rho}$ for $u^\kappa < \rho u^\kappa$ and if $\tilde{L}_T \geq \rho u^\kappa$, $\tilde{L}_R \geq v^\kappa$ or $\tilde{L}_T \geq \rho \tilde{L}_R$, $\tilde{L}_R < v^\kappa$ for $u^\kappa \geq \rho v^\kappa$, where $L_T^\kappa = \min_{x \in \Phi_T \setminus \{x_0\}} d_{x,z}$ and $L_R^\kappa = \min_{x \in \Phi_R \setminus \{y_0\}} d_{y,z}$. The PDF of $L_T^\kappa$ is

$$
\mathbb{P}(L_T^\kappa > w) = \mathbb{E}_{\Phi_T} \left[ \prod_{x \in \Phi_T \setminus \{x_0\}} \mathbb{P}(d_{x,z} > w) \right] = \exp \left( -2\pi\lambda \int_0^\infty (1 - \mathbb{P}(r^\kappa > w)) r \, dr \right)
$$

(29)

where (b) follows since $\mathbb{P}(r^\kappa > w) = p_L(r) 1_{r^L \geq w} + p_N(r) 1_{r^N \geq w}$. Since the CDF of $L_T^\kappa$ is identical to that of $L_T$, the PDF of $L_R^\kappa$ is $f_{L_R^\kappa}(w) = e^{-\lambda(\Lambda,w)} \Lambda'(\lambda,w)$. Thus, for $u^\kappa < \rho u^\kappa$, the probability of $1_j^z = 1$ given $d_{x_0,z} = u$ and $S_{x_0,z} = \kappa$ is

$$
\zeta^\kappa(u,v) = \int_0^{u^\kappa} \mathbb{P}(L_T^\kappa \geq \rho w) f_{L_R^\kappa}(w) \, dw = \int_0^{u^\kappa} e^{-(\lambda(\Lambda,\rho w) + \lambda(\Lambda,w))} \Lambda'(\lambda,\rho w) \, dw.
$$

(30)

For $u^\kappa \geq \rho u^\kappa$, the probability is

$$
\zeta^\kappa(u,v) = \mathbb{P}(L_T^\kappa \geq \rho u^\kappa, L_R^\kappa \geq v^\kappa) + \mathbb{P}(L_T^\kappa \geq \rho \tilde{L}_R, L_R^\kappa < v^\kappa) = 1 - \rho \int_0^{v^\kappa} e^{-(\lambda(\Lambda,\rho w) + \lambda(\Lambda,w))} \Lambda'(\lambda,\rho w) \, dw.
$$

(31)

Taking the expectation of $\zeta^\kappa(u,v)$ in terms of $d_{x_0,z}$ and $S_{x_0,z}$ completes the proof.

C. Proof of Lemma 6

Similar to Appendix B, we first derive the probability of $1_j^z = 1$ (denoted by $\zeta_{R,T}^\kappa(u,v)$) conditioned on $d_{x_0,z} = u$, $S_{x_0,z} = \kappa$ and $G_{x_0,T}^W \equiv g_{lm}^{TW}$. The derivation follows the same idea in Appendix B, for which we need to derive the CCDF and PDF of $P_T^\kappa = \min_{x \in \Phi_T \setminus \{x_0\}} d_{x,z}^\kappa / (P_T G_{l,m}^W)$ and $P_R^\kappa = \min_{x \in \Phi_R \setminus \{y_0\}} d_{y,z}^\kappa / (P_R G_{l,m}^R)$. Letting $L_T^\kappa|z$ and $L_R^\kappa|z$ is the PPP of transmitters with
antenna gain $g_{ij}^{TW}$ to $z$, we have
\[
\mathbb{P}(\bar{P}_T^z > w) = \prod_{i \in \{M,S\}, j \in \{M,S\}} e^{-\lambda (p_{ij}^{TW} \lambda_P g_{ij}^{TW} w)} = \exp \left(-\sum_{i,j} \Lambda (p_{ij}^{TW} \lambda_P g_{ij}^{TW} w)\right) = e^{-\lambda z (\lambda, w)}, \tag{32}
\]
where (c) follows from (29). Similarly, we have \(\mathbb{P}(\bar{P}_R^z > w) = e^{-\lambda z (\lambda, w)}\). The PDFs of $\bar{P}_T^z$ and $\bar{P}_R^z$ can be derived accordingly, based on which we can obtain the probability $\zeta_{k,n,o}(u, v)$. Finally, ignoring the dependence between $G_{TU}^{z}$ and $G_{J,R}^{z}$ and taking the expectation of $\zeta_{k,n,o}(u, v)$ in terms of $d_{x,z}$, \(S_{x,z}\), and $G_{T,W}^{z}$ completes the proof.

D. Proof of Lemma 8

We first calculate the Laplace transform of $\tilde{I}_z^T$ conditioned on $d_{y_0,z} = v$, which is given by
\[
\mathcal{L}_{z}^{T}(s, u, v) = \mathbb{E}[e^{-sI_{z}^T}] = e^{-\lambda z (\lambda, w)} I_{z}^T = \mathbb{E}[e^{-sI_{z}^T} | I_{z}^T = 1]\begin{cases} 1 & \text{if } I_{z}^T = 1 \\ 0 & \text{if } I_{z}^T = 0 \end{cases} = e^{-\lambda z (\lambda, w)} (e^{-sI_{z}^T} - e^{-sI_{z}^T} | I_{z}^T = 1). \tag{33}
\]

Following from Lemma 1, $\mathbb{E}[e^{-sI_{z}^T}]$ can be given by $\mathbb{E}[e^{-sI_{z}^T}] = \Xi_{T,W}[s, \lambda, 0]$. According to the conditions of $\zeta_{k,n,o}(u, v)$ for $s_{i}^{z} = 1$, we obtain $\mathbb{E}[e^{-sI_{z}^T} | I_{z}^T = 1] = 1$ can be given by
\[
\int_0^\infty e^{-sT} | \tilde{D}_z^T \geq \rho w| \mathbb{P}(\tilde{D}_z^T \geq \rho w) f_{g_{ij}^{TW}}(w) dw = \int_0^\infty \Xi_{T,W}(s, \lambda, \rho w) 2\pi \lambda w e^{-(\rho^2 + 1)\lambda \pi w^2} dw \tag{34}
\]
for $u < \rho v$, and
\[
\mathbb{E}[e^{-sI_{z}^T} | \tilde{D}_z^T \geq \rho v] \mathbb{P}(\tilde{D}_z^T \geq \rho v) = e^{-\lambda z (\lambda, w)} \Xi_{T,W}(s, \lambda, \rho v) + \int_0^\infty \Xi_{T,W}(s, \lambda, \rho w) 2\pi \lambda w e^{-(\rho^2 + 1)\lambda \pi w^2} dw \tag{35}
\]
for $u \geq \rho v$, taking the expectation of $\mathcal{L}_{z}^{T}(s, u, v)$ in terms of $d_{y_0,z}$ completes the proof.

E. Proof of Lemma 9

Suppose $d_{y_0,z} = v$ and $S_{y_0,z} = \tau$, and rewrite $I_{z}^T$ as $I_{z}^T = \sum_{k \in \{L,N\}} I_{z}^{T,k}$, where $I_{z}^{T,k} = \sum_{x \in \Phi_s \setminus \{x_0\}} P_T G_{x,z}^{T,W} h_{x,z} d_{x,z}^{\alpha_o}$ denotes the interference from the sub-PPP $\Phi_s^{z}$ of transmitters with link status $k$ to $z$. According to (33), defining $\tilde{D}_{z,k}^T = \min_{x \in \Phi_s^{z} \setminus \{x_0\}} d_{x,z}$, we have
\[
\mathcal{L}_{z}^{T,\tau}(s, u, v) = \mathbb{E}[e^{-sI_{z}^T}] - \int_0^u \mathbb{E}[e^{-sI_{z}^T} | \tilde{D}_{z,k}^T \geq (\rho w)^\frac{1}{\alpha_o}] dw \tag{36}
\]
for $u^{\alpha_s} < \rho v^{\alpha_s}$, and
\[
\mathcal{L}_{z,\tau}^{T}(s, u, v) = \mathbb{E}[e^{-sI_{z}^T}] - \mathbb{E}[e^{-sI_{z}^T} | \tilde{D}_{z,k}^T \geq (\rho w)^\frac{1}{\alpha_o}] \| \tilde{D}_{z,k}^T \geq (\rho w)^\frac{1}{\alpha_o} \mathbb{P}(\tilde{D}_z^T \geq \rho w) f_{g_{ij}^{TW}}(w) \tag{37}
\]
for $u^{\alpha_s} \geq \rho v^{\alpha_s}$. After some mathematical manipulations, we obtain (24) and (25). We complete the proof after calculating the expectation of $\mathcal{L}_{z,\tau}^{T}(s, u, v)$ in terms of $d_{y_0,z}$ and $S_{y_0,z}$.

F. Proof of Lemma 10

Similar to Appendix E, we first derive the Laplace transform given $d_{y_0,z} = v$, $S_{y_0,z} = \tau$, and $G_{J,R}^{z} = g_{ij}^{TW}$ (denoted by $\zeta_{T,n,o}(u, v)$). We rewrite $I_{z}^T = \sum_{k \in \{L,N\}} I_{z}^{T,k}$, where $I_{z}^{T,k} = \sum_{x \in \Phi_s^{z} \setminus \{x_0\}} P_T G_{x,z}^{T,W} h_{x,z} d_{x,z}^{\alpha_o}$ denotes the interference from the sub-PPP $\Phi_s^{z}$ of transmitters with link status $k$ and channel gain $g_{ij}^{TW}$ to $z$. Let $\tilde{D}_{z,k,i,j} = \min_{x \in \Phi_s^{z} \setminus \{x_0\}} d_{x,z}$.

For $\eta_1 < \rho v_2$, the Laplace transform $\mathcal{L}_{z,T,n,o}(s, u, v)$ is
\[
\mathbb{E}[e^{-sI_{z}^T}] - \mathbb{E}[e^{-sI_{z}^T} | \tilde{D}_{z,k,i,j} \geq (\rho w)^\frac{1}{\alpha_o}] \mathbb{P}(\tilde{D}_z^T \geq \rho w) f_{g_{ij}^{TW}}(w) \tag{38}
\]
for $u^{\alpha_s} \geq \rho v_2$. We then obtain (27) and (28) after conducting some mathematical manipulations. Calculating the expectation of $\mathcal{L}_{z,T,n,o}(s, u, v)$ in terms of $d_{y_0,z}$, $S_{y_0,z}$, and $G_{J,R}$ completes the proof.

REFERENCES

[1] T. S. Rappaport et al., “Millimeter wave mobile communications for 5G cellular: It will work!” IEEE Access, vol. 1, pp. 335–349, 2013.
[2] S. Rangan, T. S. Rappaport, and E. Erkip, “Millimeter-wave cellular wireless networks: Potentials and challenges," Proc. IEEE, vol. 102, no. 3, pp. 366–385, Mar. 2014.
[3] W. Hong et al., “The role of millimeter-wave technologies in 5G/6G wireless communications,” *IEEE J. Microw.*, vol. 1, no. 1, pp. 101–122, Jan. 2021.

[4] Z. Xiao et al., “A survey on millimeter-wave beamforming enabled UAV communications and networking,” *IEEE Commun. Surveys Tut.*, vol. 24, no. 1, pp. 557–610, 1st Quart., 2022.

[5] Z.-J. Guo, Z.-C. Hao, H.-Y. Yin, D.-M. Sun, and G. Q. Luo, “Planar shared-aperture array antenna with a high isolation for millimeter-wave low earth orbit satellite communication system,” *IEEE Trans. Antennas Propag.*, vol. 69, no. 11, pp. 7582–7592, Nov. 2021.

[6] Z. Kong, J. Song, C. Wang, H. Chen, and L. Hanzo, “Hybrid analog–digital precoder design for securing millimeter wave networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 4019–4034, 2021.

[7] J. Xu, W. Xu, D. W. K. Ng, and A. L. Swindlehurst, “Secure communication for spatially sparse millimeter-wave massive MIMO channels via hybrid precoding,” *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 887–901, Feb. 2020.

[8] W. M. R. Shakir and M.-S. Alouini, “Secrecy performance analysis of hybrid FSO-mmWave wireless communications in presence of correlated wiretap channels,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–7.

[9] S. C. Tokgoz, S. Althunibat, S. Yarka, and K. A. Qaraqe, “Physical layer security of hybrid FSO-mmWave communications,” *IEEE Trans. Veh. Technol.*, vol. 1, no. 1, pp. 101–122, Jan. 2021.

[10] J. Song, B. Lee, J. Park, M.-S. Lee, and J.-H. Lee, “Beamformer design for dual-polarized millimeter wave channels,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12306–12311, Oct. 2020.

[11] I. Castañeda, C. Studer, and G. Marti, “Jammer mitigation via beamforming for millimeter-wave lens antenna array transmission,” *IEEE Trans. Antennas Propag.*, vol. 66, no. 6, pp. 3148–3155, Jun. 2018.

[12] Y. Xiu, J. Zhao, W. Sun, and Z. Zhang, “Secrecy rate maximization for millimeter wave ad hoc communications using physical layer security,” *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 99–114, 2022.

[13] 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.

[14] Y. Zhu, G. Zheng, and M. Fitch, “Secrecy rate analysis of UAV-enabled mmWave networks using Matém hard core point processes,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1397–1409, Jul. 2018.

[15] T. S. Rappaport, Y. Xing, G. R. MacCartney, A. F. Molisch, E. Mellios, and J. Zhang, “Overview of millimeter wave communications for fifth-generation (5G) wireless networks—With a focus on propagation models,” *IEEE Trans. Antennas Propag.*, vol. 65, no. 12, pp. 6213–6230, Dec. 2017.

[16] J. Ma et al., “Security and eavesdropping in terahertz wireless links,” *Nature*, vol. 563, no. 7729, pp. 89–93, Nov. 2018.

[17] I. F. Akyildiz, J. M. Jornet, and C. Han, “Terahertz band: Next frontier for wireless communications,” *Phys. Commun.*, vol. 12, pp. 16–32, Sep. 2014.

[18] J. Xu et al., “Reconfiguring wireless environment via intelligent surfaces,” in *Proc. IEEE Int. Conf. Netw. Netw. Appl. (iWANTA)*, Oct. 2021, pp. 8–14.

[19] Y. Zhu, Y. Tu, B. Wang, J. Cryan, B. Y. Zhao, and H. Zheng, “Wireless side-lobe eavesdropping attacks,” 2018, arXiv:1810.10157.

[20] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, “Modeling and analysis of eavesdropping attack in 802.11ad mmWave wireless networks,” *IEEE Access*, vol. 7, pp. 70355–70370, 2019.

[21] Y. Zhang, J. He, Q. Qu, and Z. Zhang, “Wiretapping or jamming: On eavesdropper attacking strategy in mmWave ad hoc networks,” in *Proc. IEEE Int. Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 335–343.

[22] Y. Zhu, Y. Tu, B. Wang, J. Cryan, B. Y. Zhao, and H. Zheng, “Wireless side-lobe eavesdropping attacks,” 2018, arXiv:1810.10157.

[23] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, “Modeling and analysis of eavesdropping attack in 802.11ad mmWave wireless networks,” *IEEE Access*, vol. 7, pp. 70355–70370, 2019.

[24] Y. Zhang, J. He, Q. Qu, and Z. Zhang, “Wiretapping or jamming: On eavesdropper attacking strategy in mmWave ad hoc networks,” in *Proc. IEEE Int. Conf. Commun. Netw. Appl. (iWANTA)*, Oct. 2021, pp. 8–14.

[25] Y. Zhu et al., “Reconfiguring wireless environment via intelligent surfaces for 6G: Reflection, modulation, and security,” 2022, arXiv:2208.10931.

[26] H. Sharma, N. Kumar, and R. Tekchandani, “Mitigating jamming attack in 5G heterogeneous networks: A federated deep reinforcement learning approach,” *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2439–2452, Feb. 2023.

[27] N. Ma et al., “Reinforcement learning-based dynamic anti-jamming power control in UAV networks: An effective jamming signal strength based approach,” *IEEE Commun. Lett.*, vol. 26, no. 10, pp. 2355–2359, Oct. 2022.

[28] C. Liu, J. Lee, and T. Q. S. Quek, “Safeguarding UAV communications against full-duplex active eavesdropper,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 2919–2931, Jun. 2019.

[29] L. Xiao, S. Hong, S. Xu, H. Yang, and X. Ji, “IRS-aided energy-efficient secure WBAN transmission based on deep reinforcement learning,” *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4162–4174, Jun. 2022.

[30] D. Guo, H. Ding, L. Tang, X. Zhang, L. Yang, and Y.-C. Liang, “A proactive eavesdropping game in MIMO systems based on multiagent deep reinforcement learning,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 8889–8904, Nov. 2022.

[31] G. Hu, J. Si, Y. Cai, and N. Al-Dhahir, “Intelligent reflecting surface-assisted proactive eavesdropping over suspicious broadcasting communication with statistical CSI,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4483–4488, Apr. 2022.

[32] D. Xu and H. Zhu, “Proactive eavesdropping for wireless information surveillance under suspicious communication quality-of-service constraint,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 3220–3234, Feb. 2023.

[33] Y. Sun et al., “Energy-efficient hybrid beamforming for multilayer RIS-assisted secure integrated terrestrial-aerial networks,” *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4189–4210, Jun. 2022.
S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, “Secure and energy-efficient precoding for MIMO two-way untrusted relay systems,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 3371–3386, 2021.

Y. Xu, J. Liu, Y. Shen, X. Jiang, Y. Ji, and N. Shiratori, “QoS-aware secure routing design for wireless networks with selfish jammers,” IEEE Trans. Wireless Commun., vol. 20, no. 8, pp. 4902–4916, Aug. 2021.

S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, “Secure beamforming for full-duplex MIMO two-way untrusted relay systems,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3775–3790, 2020.

J. He, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, “Link selection for security-QoS tradeoffs in buffer-aided relaying networks,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1347–1362, 2020.

A. Thornburg, T. Bui, and R. W. Heath Jr., “Performance analysis of outdoor mmWave ad hoc networks,” IEEE Trans. Signal Process., vol. 64, no. 15, pp. 4065–4079, Aug. 2016.

C. Laoudias, A. Moreira, S. Kim, S. Lee, L. Wirola, and C. Fischione, “A survey of enabling technologies for network localization, tracking, and navigation,” IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 3607–3644, 4th Quart., 2018.

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.

M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection,” Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

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 Trans. Commun., vol. 66, no. 12, pp. 6437–6449, Dec. 2018.

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.