This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

Secure Millimeter-Wave Ad Hoc Communications Using Physical Layer Security

Yuanyu Zhang, *Member, IEEE*, Yulong Shen, *Member, IEEE*, Xiaohong Jiang, *Senior Member, IEEE* and Shoji Kasahara, *Member, IEEE*

***Abstract*—Millimeter-wave (mmWave) communications are highly promising to improve the capacity of modern wireless networks, while the physical layer security (PLS) techniques hold great potential to enhance the critical secrecy performance therein. By carefully exploiting the significant signal difference between the Non-Light-of-Sight (NLoS) and Line-of-Sight (LoS) mmWave links, this paper proposes a Sight-based Cooperative Jamming (SCJ) scheme to improve the PLS performance of mmWave ad hoc communications. In this scheme, each potential jammer that has no LoS link to its nearest receiver but may have LoS links to eavesdroppers is selected with a certain probability to generate artificial noise such that channel advantages at legitimate receivers can be achieved. For performance modeling of the new jamming scheme, novel and efficient theoretical approximation approaches are firstly developed to enable the challenging issue of interference distribution modeling to be tackled, and then a theoretical framework based on stochastic geometry is proposed to capture the secrecy transmission capacity behavior under the SCJ scheme. Finally, extensive numerical results are provided to illustrate the SCJ scheme under various network scenarios.**

***Index Terms*—Physical layer security, millimeter-wave ad hoc communications, cooperative jamming.**

I. Introduction

THE explosive growth of mobile devices in the past decade poses a significant challenge to the capacity of modern wireless networks. To tackle this challenge, the wireless industry has advocated shifting wireless communications from the narrow microwave band below 6 GHz to the extremely wide millimeter-wave (mmWave) band between 30 GHz and 300 GHz [1], [2]. However, like conventional microwave communications, the secrecy issue of mmWave communications caused by eavesdropping attacks has also been regarded as a major concern [3], [4]. Recent research shows that the physical layer security (PLS) technology, which exploits the random physical layer features of wireless channels to achieve information-theoretic security, is highly promising to improve the secrecy of wireless communications [5]–[8]. This paper therefore investigates the PLS issue in mmWave ad hoc communications. In particular, we aim to propose effective PLS schemes for mmWave ad hoc communications and evaluate the PLS performance therein.

Although the PLS performance of microwave communications has been extensively studied (e.g., [9]–[13]), the results cannot be directly applied to the mmWave communications due to the intrinsic physical layer features of mmWave channels [14]–[16]. This motivates researchers to investigate the PLS performance of mmWave communications. The authors in [17] considered a planar mmWave ad hoc network with multiple transmission pairs and eavesdroppers, and evaluated the average achievable secrecy rate of a single pair. In particular, the authors investigated the PLS potentials of an artificial noise (AN)-aided transmission scheme, where each transmitter allocates a fraction of its transmit power for AN transmission, and showed that AN may be ineffective for improving the secrecy rate. Apart from planar ad hoc networks, research efforts have also been devoted to the PLS performance evaluation of other mmWave scenarios, such as 3D ad hoc networks with unmanned aerial vehicles (UAVs) [18], downlink transmissions of cellular networks [19], downlink transmissions of hybrid cellular networks [20], [21], where microwave BSs coexist with mmWave BSs, simultaneous wireless information and power transfer (SWIPT) networks [22] and simple two-hop relay systems with multiple eavesdroppers [23], [24]. Please refer to the Related Work section (Section II) for the detailed introduction of these works.

The above works adopted well-known point processes, like the Poisson Point Processes (PPP) [17], [19]–[22] and Matern Hardcore Point Process (MHPP) [18], to model the locations of nodes, thanks to their ability to enable network-scale performance analysis. However, to retain the mathematical tractability of the point processes, these works applied either no PLS schemes or less effective PLS schemes, like the AN-aided transmission in [17], [19] and cooperative jamming in [18], where part of the transmitters send artificial noise that is *equally detrimental* to legitimate receivers and eavesdroppers. These PLS schemes are based on the design disciplines for microwave communications, while we believe that effective PLS schemes specific to mmWave communications should carefully exploit the distinctive physical layer features of

This work was supported in part by the Japan Society for the Promotion of Science KAKENHI under grants 19K14983 and 18H03235, in part by the National Key Research and Development Program under grants 2018YFE0207600 and 2018YFB2100403, and in part by the National Natural Science Foundation of China under grants 61972308, 61825104 and 61941105. (*Corresponding author*: Yulong Shen)

Y. Zhang is with the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China, and also with the Graduate School of Science and Technology, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, Nara, 630-0192, Japan. Email: yy90zhang@ieee.org.

Y. Shen is with the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China. Email: ylshen@mail.xidian.edu.cn.

X. Jiang is with the School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido, Japan, and also with the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China. Email: jiang@fun.ac.jp.

S. Kasahara is with the Graduate School of Science and Technology, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, Nara, 630-0192, Japan. Email: kasahara@ieee.org

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

mmWave channels. For instance, Non-Line-of-Sight (NLoS) mmWave links suffer from much more severe signal attenuation than LoS mmWave links [14]–[16]. Thus, cooperative jamming schemes can use nodes that have no LoS links (i.e., have NLoS links) to legitimate receivers but have LoS links to eavesdroppers to cause less interference at the former than at the latter, thus improving the PLS performance. Unfortunately, to the best of our knowledge, such appealing idea of designing PLS schemes based on intrinsic physical layer features of mmWave channels (e.g., sensitive to blockage, significantly different attenuation between LoS links and NLoS links) was ignored in previous works. This motivates our PLS scheme design and the corresponding PLS performance evaluation in this paper.

This paper considers an mmWave ad hoc network where the locations of transmission pairs, *potential* jammers and eavesdroppers are modeled by PPPs. The main contributions of this paper can be summarized as follows.

- By carefully exploiting the significant signal difference between NLoS and LoS mmWave links, we propose a novel Sight-based Cooperative Jamming (SCJ) scheme to improve the PLS performance of the transmission pairs. With the aim to achieve channel advantages for the legitimate receivers, in the SCJ scheme, each potential jammer that has no LoS link to its *nearest* receiver but may have LoS links to the eavesdroppers is selected as a jammer with a certain probability to generate artificial noise. To the best of our knowledge, this paper represents the first work that exploits the intrinsic physical layer features of mmWave channels in the design of PLS schemes for mmWave networks. It is expected that this work will shed light on a new approach for the design of secure mmWave communication systems.
- We adopt the secrecy transmission capacity (STC) [25], i.e., the average sum rate of transmissions in perfect secrecy per unit area, as the metric to investigate the PLS performance of the network under the new jamming scheme. Existing works mainly assume that jammers follow homogeneous PPPs, while the jammers in this paper follow Poisson Hole Processes (PHPs) and the resultant regions where jammers reside have irregular shapes, posing a significant challenge to the interference modeling for legitimate receivers and eavesdroppers. To tackle this challenge, we apply region approximation to develop novel and efficient theoretical approaches to approximate the inhomogeneous spatial distribution of the jammers such that the challenging issue of interference distribution modeling can be tackled. With the help of the approximations, we then develop a theoretical framework based on stochastic geometry to derive the connection probability and secrecy probability of transmission pairs, based on which the STC analysis is then conducted. The results in this paper show that our new approach for interference modeling under the PHP enables a more accurate analysis to be conducted for both connection probability and secrecy probability.
- Finally, we provide extensive numerical results to illustrate the effectiveness of the approximations as well as the optimal STC performances of the proposed SCJ scheme under various network scenarios. The results showed that our scheme can improve the network STC performance and outperforms the typical partial jamming scheme in terms of both STC and energy efficiency performances.

The remainder of this paper is organized as follows. Section II introduces the related work and Section III presents the system model as well as the SCJ scheme. To facilitate the theoretical analysis, we consider a simplified scenario with only one transmission pair in Section IV. The theoretical analysis for the general scenario is presented in Section V. We provide numerical results in Section VI and finally conclude the paper in Section VII.

II. Related Work

Extensive research efforts have been devoted to the study of PLS issue in mmWave communications, which can be roughly classified into two categories depending on whether the network model and performance analysis are based on stochastic geometry or not.

In stochastic geometry-based works, the locations of legitimate nodes (e.g., transmitters, BSs, receivers) and eavesdroppers are usually modeled by independent and homogenous PPPs to characterize large-scale network scenarios, like ad hoc networks and cellular networks. The subsequent description of the related works is based on this prerequisite, unless stated otherwise. As introduced in the previous section, the authors in [17] considered a planar ad hoc network with multiple transmission pairs and eavesdroppers, and evaluated the average achievable secrecy rate under a simple AN-based transmission scheme, where each transmitter allocates a fraction of its transmit power to radiate AN. In [18], a 3D ad hoc network was considered, where BS-like UAVs, whose locations are modeled by an MHPP rather than a PPP, transmit to ground receivers in the presence of ground eavesdroppers. The authors then investigated the secrecy rate performance under a simple cooperative jamming scheme, where part of the UAVs generate AN *irrespective of their link conditions to the ground receivers*. Considering the downlink transmission of a cellular network, the authors in [19] analyzed the secure connectivity probability and average number of perfect links per unit area in the noise-limited scenario under both non-colluding and colluding eavesdropping cases. In addition, they also investigated the average number of perfect links per unit area in the interference-limited scenario under only the non-colluding case and a simple AN scheme similar to the one in [17]. A hybrid cellular network, where mmWave BSs coexist with microwave BSs, was considered in [20] and the PLS performances of connection outage probability, secrecy outage probability and secrecy rate were studied. The hybrid cellular network scenario was also considered in [21], while, different from the passive eavesdroppers in [20], the eavesdroppers here send pilot signals during the channel training phase to improve the quality of intercepted signals. Connection and secrecy performances were then investigated under this new attacking scenario. The downlink transmissions of an SWIPT cellular

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

network were examined in [22], where BSs can simultaneously send information and transfer power to user devices. The performances of energy-information coverage probability, secrecy probability and secrecy throughput were also investigated under non-colluding or colluding eavesdropping cases.

Note that the above works adopted either no PLS schemes or ineffective AN and cooperative jamming schemes, where the noise or jamming signals are equally detrimental to both the legitimate receivers and eavesdroppers, failing to create channel advantages for the former. The main reason is to ensure the mathematical tractability of the point processes (e.g., PPPs and MHPPs), since the adopted schemes lead to homogenous point processes of interfering nodes. Differing from these works, this paper proposes an effective SCJ scheme, which carefully exploits the blockage effects between jammers and legitimate receivers to create better legitimate channels. As a result, the point process of the jammers becomes inhomogeneous, and thus new and dedicated theoretical analysis is required to model the interference from the jammers in our scenario.

Apart from the above works, there also exist some other stochastic geometry-based works focusing on multiple-input multiple-output transmissions [23], [26], SWIPT transmissions [24], relaying transmissions [27] and cognitive radio networks [28]. However, different from the above ones, these works considered only one or two source-destination pairs. In addition to the stochastic geometry-based works, some works have also been done in relatively simple scenarios with only a few nodes. For example, the authors in [29] considered a simple network with only one source equipped with multiple antennas, one destination and one eavesdropper, both having a single antenna. The PLS performances of secrecy outage probability and secrecy throughput were evaluated under three beamforming schemes, namely, maximum ratio transmitting (MRT) beamforming, AN beamforming and partial MRT beamforming. This work was partially extended in [30] by adding a multi-antenna relay. In [31], the authors considered the secrecy issue of a secondary transmission pair in a cognitive system, which shares the spectrum of a primary pair while controlling its power to avoid impairing the transmission of the primary pair. For PLS performance evaluation, the authors derived the secrecy outage probability of the secondary pair.

III. System Model and Sight-based Cooperative Jamming Scheme

A. Network Model

We consider an mmWave ad hoc network over $\mathbb{R}^2$, where the locations of transmitters, *potential* jammers and eavesdroppers are modeled by independent and homogenous PPPs Φ_T, Φ_P and Φ_E with densities λ_T, λ_P and λ_E, respectively. Each transmitter has a receiver located at a fixed distance r_0 away but at a random orientation. According to [32], the locations of the receivers can be modeled by another independent and homogenous PPP Φ_R with density $\lambda_R = \lambda_T$. We assume that the locations of the legitimate nodes (i.e., transmitters, receivers and potential jammers) are known, while those of the eavesdroppers are not. We also assume that the eavesdroppers are passive and non-colluding, i.e., decoding messages based on their own observations without sending signals, and the transmitting nodes (i.e., the transmitters and jammers) transmit with the same power P.

B. Antenna Model

To approximate the antenna patterns of the legitimate nodes, we adopt the sectored antenna model [33], [34], where each antenna consists of a main lobe and a back lobe. We define the beam width of the main lobe, the main lobe gain and back lobe gain of the transmitting nodes' antennas by θ_T, G_T and g_T ($G_T > g_T$), and those of the receivers' antennas by θ_R, G_R and g_R ($G_R > g_R$). We assume that the transmitter and receiver of each pair have properly steered their antennas to obtain the maximum antenna gain $G_T G_R$ before transmission. Since the PPPs Φ_T, Φ_R and Φ_P are isotropic, the random effective antenna gain between a transmitting node (i.e., a transmitter or jammer) and a receiver is

$$\mathsf{G} = \begin{cases} G_T G_R, & \text{w.p. } q_{G_T G_R} = \frac{\theta_T}{2\pi}\frac{\theta_R}{2\pi} \\ G_T g_R, & \text{w.p. } q_{G_T g_R} = \frac{\theta_T}{2\pi}\frac{2\pi-\theta_R}{2\pi} \\ g_T G_R, & \text{w.p. } q_{g_T G_R} = \frac{2\pi-\theta_T}{2\pi}\frac{\theta_R}{2\pi} \\ g_T g_R, & \text{w.p. } q_{g_T g_R} = \frac{2\pi-\theta_T}{2\pi}\frac{2\pi-\theta_R}{2\pi} \end{cases}, \tag{1}$$

where q_{g} ($\mathsf{g} \in \{G_T G_R, G_T g_R, g_T G_R, g_T g_R\}$) denotes the probability of $\mathsf{G} = \mathsf{g}$.

Similarly, eavesdropper antennas are also characterized by the sectored antenna model, and the random effective antenna gain between an eavesdropper and a transmitting node is

$$\mathsf{G}_E = \begin{cases} G_T G_E, & \text{w.p. } q_{G_T G_E} = \frac{\theta_T}{2\pi}\frac{\theta_E}{2\pi} \\ G_T g_E, & \text{w.p. } q_{G_T g_E} = \frac{\theta_T}{2\pi}\frac{2\pi-\theta_E}{2\pi} \\ g_T G_E, & \text{w.p. } q_{g_T G_E} = \frac{2\pi-\theta_T}{2\pi}\frac{\theta_E}{2\pi} \\ g_T g_E, & \text{w.p. } q_{g_T g_E} = \frac{2\pi-\theta_T}{2\pi}\frac{2\pi-\theta_E}{2\pi} \end{cases}, \tag{2}$$

where $q_{\hat{\mathsf{g}}}$ ($\hat{\mathsf{g}} \in \{G_T G_E, G_T g_E, g_T G_E, g_T g_E\}$) denotes the probability of $\mathsf{G} = \hat{\mathsf{g}}$, G_E (resp. g_E) denotes the main (resp. back) lobe gain and θ_E denotes the main beam width of eavesdroppers.

C. Blockage and Propagation Model

To depict the blockage effect, we adopt the LoS ball model [19], [34], [35], where a link of length r is LoS (resp. NLoS) with probability p_L (resp. $1-p_L$) if $r \le D$ and with probability 0 (resp. 1) otherwise, i.e., if $r > D$. Here, D denotes the radius of LoS balls. We assume that $r_0 \le D$ and *the links of the transmission pairs are LoS* throughout this paper. The blockage effect results in different path loss for LoS and NLoS links, of which the exponents are denoted by α_L and α_N, respectively. Besides, the mmWave links also suffer from multi-path fading, which is characterized by the Nakagami-m fading model. Thus, the channel gain $h^{\mathsf{b}}_{x,y}$ of a link $x \to y$ follows the gamma distribution $\Gamma(N_{\mathbf{b}}, N_{\mathbf{b}})$ with shape $N_{\mathbf{b}}$ and rate $N_{\mathbf{b}}$, where $\mathbf{b} = L$ (resp. $\mathbf{b} = N$) for LoS (resp. NLoS) links.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

D. Sight-based Cooperative Jamming (SCJ) Scheme

The SCJ scheme aims to select jammers that are expected to generate more interference at the eavesdroppers than at the receivers. Since the locations of eavesdroppers are unknown, the potential jammers cannot measure their interference to the eavesdroppers. Thus, the selection is solely based on the interference to the receivers. To measure such interference, each potential jammer associates itself with the *nearest* receiver and observes the distance d and link l between them. For a potential jammer $y \in \Phi_P$, if $d > D$, then y has no LoS link to any receiver and thus will cause little interference to the receivers. In this case, y chooses to become a jammer. If $d \leq D$ and l is NLoS, y will cause slight interference to its nearest receiver but may cause severe interference to other receivers when y is inside the LoS ball of more than one receiver. To control the interference to other receivers, y chooses to become a jammer with probability $\rho \in [0, 1]$. In other cases, y will cause severe interference to the receivers and thus remains silent.

Note that the association policy is designed to select the associated receiver for a given potential jammer (rather than selecting associated jammer for a given receiver), with the purpose of reducing as much as possible the interference to other legitimate receivers. Thus, a natural association policy is to select the nearest receiver. This is because if a potential jammer causes no or little interference to its nearest receiver, it would also cause no or little interference to other receivers as well. The proposed scheme can be also applied to the mmWave cellular network scenario, since the mmWave cellular networks share some common features with the network scenario considered in this paper. For instance, in the uplink transmission scenarios where BSs serve as receivers, idle mobile devices can be the potential jammers. By applying the proposed scheme to this scenario, the channel advantages can be created for BSs, leading to an enhancement of STC performance therein.

We define the region covered by the LoS balls of all the receivers by $\mathcal{B} = \bigcup_{x \in \Phi_R} B(x, D)$, where $B(x, D) = \{x' \in \mathbb{R}^2 : \|x' - x\| \leq D\}$ denotes the LoS ball of x. According to the SCJ scheme, each potential jammer becomes a jammer with probability ρp_N, where $p_N = 1 - p_L$, if it is inside $\mathcal{B}$, and with probability 1 otherwise. Thus, the locations of jammers can be equivalently modeled by a homogeneous PPP Φ_J with density $\lambda_J = \rho p_N \lambda_P$ plus an independent Poisson Hole Process (PHP) Ψ_J. The process Ψ_J is formed by removing the nodes in $\mathcal{B}$ from another independent and homogenous PPP $\bar{\Phi}_J$ (called baseline PPP) with density $\bar{\lambda}_J = (1 - \rho p_N)\lambda_P$. Formally, Ψ_J can be defined by $\Psi_J = \bar{\Phi}_J \cap \mathcal{B}^c = \{y \in \bar{\Phi}_J : y \notin \mathcal{B}\}$.

E. Performance Metrics

The transmission pairs apply the Wyner encoding scheme [36] to protect their confidential messages. When sending a confidential message, a transmitter x chooses a codeword rate R_s for this message and another codeword rate R_t for the entire transmitted message. The difference $R_e = R_t - R_s$ reflects the cost for confusing the eavesdroppers. We assume R_t and R_s are fixed throughout this paper. Due to the random channel condition, the corresponding receiver y succeeds in decoding the transmitted message with a certain probability. This probability is called **connection probability** [19] and defined by

$$p_c = \mathbb{P}(\mathrm{SINR}_{x,y} \geq 2^{R_t} - 1), \tag{3}$$

where $\mathrm{SINR}_{x,y}$ denotes the Signal-to-Interference-plus-Noise Ratio (SINR) from x to y. Similarly, eavesdroppers fail to obtain any information from the confidential message with a certain probability. This probability is called **secrecy probability** [19] and defined by the probability that no eavesdropper can decode the confidential message, that is,

$$p_s = \mathbb{P}\Big(\bigcap_{z \in \Phi_E} \mathrm{SINR}_{x,z} \leq 2^{R_e} - 1 \Big), \tag{4}$$

where $\mathrm{SINR}_{x,z}$ denotes the SINR from x to an eavesdropper $z \in \Phi_E$. Note that the concrete expressions of $\mathrm{SINR}_{x,y}$ and $\mathrm{SINR}_{x,z}$ will be determined in the subsequent sections where x, y and z are clearly defined. Using these probabilities, we define another metric, called **secrecy transmission capacity** (STC) [25], to characterize the average sum rate of the transmissions in perfect secrecy per unit area. Formally, the STC can be formulated as

$$\bar{R}_s = p_c p_s (R_t - R_e) \lambda_T. \tag{5}$$

This papers uses the STC $\bar{R}_s$ as the metric to evaluate the secrecy performance, for which we need to derive the connection probability p_c and secrecy probability p_s of a typical pair, respectively.

IV. Performance Analysis: Simplified Scenario

To facilitate the STC analysis of the general scenario, we consider a simplified scenario with only one transmission pair and derive the p_c and p_s in Sections IV-A and IV-B, respectively. The simplified scenario provides an intuitive insight into the main idea of the proposed SCJ scheme and makes it easier for readers to see the superiority of the SCJ scheme in terms of STC performance. In addition, by introducing some basic theoretical results in the simplified scenario, we can focus more on the derivations of the key theoretical results in the general scenario, so that the readers can easily understand the main idea of our theoretical analysis without being lost in the cumbersome and tedious mathematical derivations.

A. Connection Probability

We define x_0 and y_0 the transmitter and receiver of the pair, respectively. The SINR of y_0 can be given by

$$\mathrm{SINR}_{x_0,y_0} = \frac{G_T G_R h^L_{x_0,y_0} r_0^{-\alpha_L}}{I^{y_0}_{\Phi_J} + I^{y_0}_{\Psi_J} + \sigma^2/P}, \tag{6}$$

where σ^2 denotes the variance of the noise and $I^{y_0}_{\Phi_J}$ (resp. $I^{y_0}_{\Psi_J}$) is the interference from the jammers in Φ_J (resp. Ψ_J). To obtain the connection probability, we first derive the Laplace transform of $I^{y_0}_{\Phi_J}$ and $I^{y_0}_{\Psi_J}$ in the following lemmas.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

Lemma 1. *The Laplace transform $\mathcal{L}_{I^{y_0}_{\Phi_J}}(s)$ of $I^{y_0}_{\Phi_J}$ in the simplified scenario is*

$$\mathcal{L}_{I^{y_0}_{\Phi_J}}(s) = \exp\Big(-2\pi\lambda_J \sum_{\mathsf{g}} q_{\mathsf{g}} \int_0^\infty F_N(s\mathsf{g}, r) r \mathrm{d}r\Big), \quad (7)$$

where

$$F_{\mathsf{b}}(x, r) = 1 - \Big(1 + \frac{x}{N_{\mathsf{b}} r^{\alpha_{\mathsf{b}}}}\Big)^{-N_{\mathsf{b}}}, \quad (8)$$

$\mathsf{b} \in \{L, N\}$, $\mathsf{g} \in \{G_T G_R, G_T g_R, g_T G_R, g_T g_R\}$ *and* q_{g} *is given in (1).*

Proof: See Appendix A. ■

Lemma 2. *The Laplace transform $\mathcal{L}_{I^{y_0}_{\Psi_J}}(s)$ of $I^{y_0}_{\Psi_J}$ in the simplified scenario is*

$$\mathcal{L}_{I^{y_0}_{\Psi_J}}(s) = \exp\Big(-2\pi\bar{\lambda}_J \sum_{\mathsf{g}} q_{\mathsf{g}} \int_D^\infty F_N(s\mathsf{g}, r) r \mathrm{d}r\Big), \quad (9)$$

where

$$F_N(x, r) = 1 - \Big(1 + \frac{x}{N_N r^{\alpha_N}}\Big)^{-N_N}, \quad (10)$$

$\mathsf{g} \in \{G_T G_R, G_T g_R, g_T G_R, g_T g_R\}$ *and* q_{g} *is given in (1).*

Proof: This proof follows from Lemma 1. ■

Based on Lemmas 1 and 2, we now derive the upper bound on the connection probability of the transmission pair.

Theorem 1. *The connection probability of the transmission pair in the simplified scenario can be upper bounded by*

$$p_c \le \sum_{k=1}^{N_L} \binom{N_L}{k} (-1)^{k+1} e^{-\frac{k\mu\sigma^2}{P}} \mathcal{L}_{I^{y_0}_{\Phi_J}}(k\mu) \mathcal{L}_{I^{y_0}_{\Psi_J}}(k\mu), \quad (11)$$

where $\mu = \frac{\tau_L r_0^{\alpha_L}(2^{R_t}-1)}{G_T G_R}$, $\tau_L = N_L (N_L!)^{-1/N_L}$, $\mathcal{L}_{I^{y_0}_{\Phi_J}}(\cdot)$ *is given by (7) and* $\mathcal{L}_{I^{y_0}_{\Psi_J}}(\cdot)$ *is given by (9).*

Proof: Based on the definition in (3), we have

$$\begin{aligned} p_c &= \mathbb{P}\Big(h^L_{x_0,y_0} \ge \frac{(2^{R_t}-1) r_0^{\alpha_L}}{G_T G_R} (I^{y_0}_{\Phi_J} + I^{y_0}_{\Psi_J} + \sigma^2/P)\Big) \\ &\overset{(a)}{\le} 1 - \mathbb{E}_{I^{y_0}_{\Phi_J}, I^{y_0}_{\Psi_J}}\Big[\Big(1 - e^{-\mu(I^{y_0}_{\Phi_J} + I^{y_0}_{\Psi_J} + \sigma^2/P)}\Big)^{N_L}\Big] \\ &= \sum_{k=1}^{N_L} \binom{N_L}{k} (-1)^{k+1} e^{-k\mu\frac{\sigma^2}{P}} \mathcal{L}_{I^{y_0}_{\Phi_J}}(k\mu) \mathcal{L}_{I^{y_0}_{\Psi_J}}(k\mu), \end{aligned} \quad (12)$$

where (a) follows from the Lemma 1 in [34]. ■

B. Secrecy Probability

The PPP Φ_E inside the LoS ball $B(x_0, D)$ can be divided into independent sub-PPPs $\Phi^{\mathsf{b},\hat{\mathsf{g}}}_{E,I}$ with density $p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \lambda_E$ ($\mathsf{b} \in \{L, N\}$ and $\hat{\mathsf{g}} \in \{G_T G_E, G_T g_E, g_T G_E, g_T g_E\}$) due to the independent thinning by the blockage effect and antenna gains, while the PPP Φ_E outside $B(x_0, D)$ can be divided into sub-PPPs $\Phi^{N,\hat{\mathsf{g}}}_{E,O}$ with density $q_{\hat{\mathsf{g}}} \lambda_E$, because these eavesdroppers have only NLoS links to x_0. Since these sub-PPPs are independent, we can formulate the secrecy probability as

$$\begin{aligned} p_s = &\prod_{\mathsf{b}} \prod_{\hat{\mathsf{g}}} \mathbb{P}\Big(\cap_{z \in \Phi^{\mathsf{b},\hat{\mathsf{g}}}_{E,I}} \mathrm{SINR}^{\mathsf{b},\hat{\mathsf{g}}}_{x_0,z} \le 2^{R_e} - 1\Big) \\ &\times \prod_{\hat{\mathsf{g}}} \mathbb{P}\Big(\cap_{z \in \Phi^{N,\hat{\mathsf{g}}}_{E,O}} \mathrm{SINR}^{N,\hat{\mathsf{g}}}_{x_0,z} \le 2^{R_e} - 1\Big), \end{aligned} \quad (13)$$

where $\mathrm{SINR}^{\mathsf{b},\hat{\mathsf{g}}}_{x_0,z}$ denotes the SINR of an eavesdropper z with link condition b (i.e., LoS or NLoS) and antenna gain $\hat{\mathsf{g}}$ to x_0. Here, $\mathrm{SINR}^{\mathsf{b},\hat{\mathsf{g}}}_{x_0,z}$ is given by

$$\mathrm{SINR}^{\mathsf{b},\hat{\mathsf{g}}}_{x_0,z} = \frac{\hat{\mathsf{g}} h^{\mathsf{b}}_{x_0,z} \|x_0 - z\|^{-\alpha_{\mathsf{b}}}}{\sum_{\varphi \in \{\Phi_J, \Psi_J\}} I^z_\varphi + \sigma^2/P}, \quad (14)$$

where I^z_φ ($\varphi \in \{\Phi_J, \Psi_J\}$) denotes the interference at z from $\varphi \cap B(z, D)$. For $\varphi = \Phi_J$, $\mathcal{L}_{I^z_{\Phi_J}}(s)$ can be obtained based on Lemma 1. We summarize the result in the following lemma.

Lemma 3. *The Laplace transform $\mathcal{L}_{I^z_{\Phi_J}}(s)$ of $I^z_{\Phi_J}$ in the simplified scenario is*

$$\begin{aligned} \mathcal{L}_{I^z_{\Phi_J}}(\lambda_J, s) = &\exp\Big(-2\pi\lambda_J \sum_{\mathsf{b}} \sum_{\hat{\mathsf{g}}} p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \int_0^D F_{\mathsf{b}}(s\hat{\mathsf{g}}, r) r \mathrm{d}r\Big) \\ &\times \exp\Big(-2\pi\lambda_J \sum_{\hat{\mathsf{g}}} q_{\hat{\mathsf{g}}} \int_D^\infty F_N(s\hat{\mathsf{g}}, r) r \mathrm{d}r\Big), \end{aligned} \quad (15)$$

where $F_{\mathsf{b}}(\cdot,\cdot)$ is given by (10).

Proof: The proof is similar to that of Lemma 1 and thus omitted here. ■

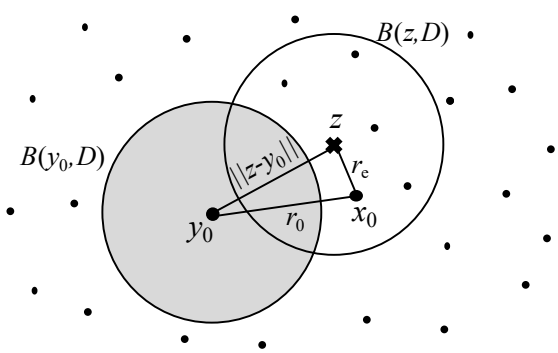


Fig. 1. Illustration of jammers inside $B(z, D)$ removed by $B(y_0, D)$.

Next, we derive the Laplace transform $\mathcal{L}_{I^z_{\Psi_J}}(s)$ of $I^z_{\Psi_J}$. According to the SCJ scheme, some jammers inside the LoS ball $B(z, D)$ of the eavesdropper z will be removed by the LoS ball $B(y_0, D)$ of the receiver y_0 (as shown in Fig. 1), if the distance $\|z - y_0\|$ between z and y_0 is smaller than $2D$. Thus, $\mathcal{L}_{I^z_{\Psi_J}}(s)$ depends on $\|z - y_0\|$ and thus the distance $\|z - x_0\|$ between x_0 and z, because $\|z - y_0\|$ can be expressed by $\|z - x_0\|$ and the link distance r_0 between x_0 and y_0. Denoting $\|z - x_0\|$ as r_e, we rewrite $\mathcal{L}_{I^z_{\Psi_J}}(s)$ as $\mathcal{L}_{I^z_{\Psi_J}}(s, r_e)$ and derive its expression in the following lemma.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

Lemma 4. *The Laplace transform $\mathcal{L}_{I^z_{\Psi_J}}(s, r_e)$ of $I^z_{\Psi_J}$ in the simplified scenario is*

$$\mathcal{L}_{I^z_{\Psi_J}}(s, r_e) = \int_{|r_e - r_0|}^{r_e + r_0} e^{-\bar{\lambda}_J \sum_{\mathsf{b}} \sum_{\mathsf{g}} p_{\mathsf{b}} q_{\hat{\mathsf{g}}} T(s,u)} e^{-\widetilde{\lambda}_J \sum_{\hat{\mathsf{g}}} q_{\hat{\mathsf{g}}} T_2(s,u)} h(u) \mathrm{d}u, \tag{16}$$

where

$$T_1(s,u) = 2\pi \int_{C_1(u)}^{D} F_{\mathsf{b}}(s\hat{\mathsf{g}}, r) r \mathrm{d}r - 2\int_{C_2(u)}^{D} F_{\mathsf{b}}(s\hat{\mathsf{g}}, r) \arccos\left(\frac{u^2 + r^2 - D^2}{2ur}\right) r\mathrm{d}r, \tag{17}$$

$$T_2(s,u) = 2\pi \int_{D}^{\infty} F_N(s\hat{\mathsf{g}}, r) r \mathrm{d}r - 2\int_{C_3(u)}^{u+D} F_N(s\hat{\mathsf{g}}, r) \arccos\left(\frac{u^2 + r^2 - D^2}{2ur}\right) r\mathrm{d}r, \tag{18}$$

$C_1(u) = \min\{D, \max\{0, D-u\}\}$, $C_2(u) = \min\{D, \max\{u - D, D-u\}\}$, $C_3(u) = \max\{D, u-D\}$ *and*

$$h(u) = \frac{2u}{\pi\sqrt{4r_0^2 r_e^2 - (r_0^2 + r_e^2 - u^2)^2}}. \tag{19}$$

Proof: See Appendix B. ■

Based on Lemmas 3 and 4, we derive the lower bound on the secrecy probability in the following theorem.

Theorem 2. *The secrecy probability p_s of the transmission pair in the simplified scenario can be lower bounded by*

$$p_s \geq \exp\Bigg(-2\pi\lambda_E \sum_{\mathsf{b}} \sum_{\hat{\mathsf{g}}} p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \sum_{k=1}^{N_{\mathsf{b}}} \binom{N_{\mathsf{b}}}{k} (-1)^{k+1} \int_0^D e^{-k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}} \frac{\sigma^2}{P}} \mathcal{L}_{I^z_{\Phi_J}}(\lambda_J, k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}) \mathcal{L}_{I^z_{\Psi_J}}(k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}, r_e) r_e \mathrm{d}r_e \Bigg) \times \exp\Bigg(-2\pi\lambda_E \sum_{\hat{\mathsf{g}}} q_{\hat{\mathsf{g}}} \sum_{k=1}^{N_N} \binom{N_N}{k} (-1)^{k+1} \int_D^{\infty} e^{-k\nu_N r_e^{\alpha_N} \frac{\sigma^2}{P}} \mathcal{L}_{I^z_{\Phi_J}}(\lambda_J, k\nu_N r_e^{\alpha_N}) \mathcal{L}_{I^z_{\Psi_J}}(k\nu_N r_e^{\alpha_N}, r_e) r_e \mathrm{d}r_e \Bigg), \tag{20}$$

where $\nu_{\mathsf{b}} = \frac{\tau_{\mathsf{b}}(2^{R_e} - 1)}{\hat{\mathsf{g}}}$, $\tau_{\mathsf{b}} = N_{\mathsf{b}}(N_{\mathsf{b}}!)^{-1/N_{\mathsf{b}}}$, $\mathcal{L}_{I^z_{\Phi_J}}(\cdot)$ is given by Lemma 3 and $\mathcal{L}_{I^z_{\Psi_J}}(\cdot,\cdot)$ by Lemma 4.

Proof: See Appendix C. ■

The bounds in Theorems 1 and 2 are validated by Monte Carlo simulations based on the simulator in [37] under different values of λ_P, λ_E, R_t and R_e. For simulation, we consider an urban environment and summarize in Table I the related environment parameters. Here, the setting of $D = 200$ [m] corresponds to the urban area of Manhattan [38], which provides good fit for real-world scenarios. The simulation results as well as the theoretical ones are shown in Fig. 2, from which we can see that the theoretical results match nicely with the simulation ones, implying that *the bounds are tight enough to be used as approximations*.

TABLE I
PARAMETERS USED IN SIMULATIONS.

Parameters	Value
Link distance r_0	100 m
Channel bandwidth	1 GHz
Noise spectral density	-174 dBm/Hz
Common transmit power P	1 W (i.e., 30 dBm)
Path loss exponent α_L (α_N)	2 (4)
Nakagami fading parameter N_L (N_N)	3 (2)
LoS probability p_L	0.2
LoS ball radius D	200 m
Main lobe beam width θ_T (θ_R)	$\pi/6$ ($\pi/6$)
Main lobe gain G_T (G_R, G_E)	10 (10, 10)
Back lobe gain g_T (g_R, g_E)	0.1 (0.1, 0.1)

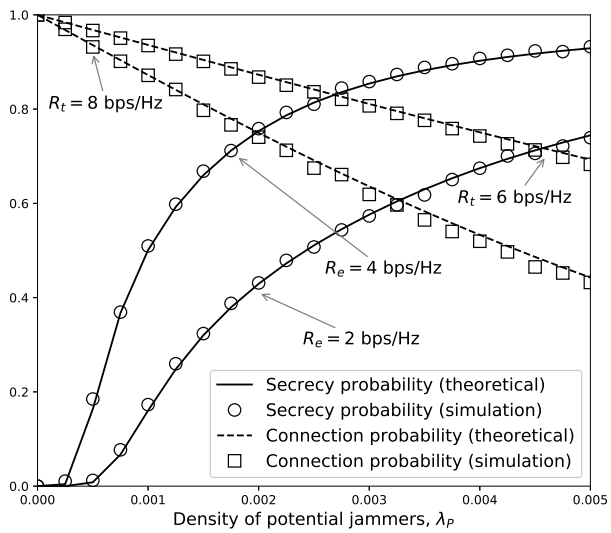


Fig. 2. Validation of the bounds in Theorems 1 and 2 with $\rho = 1.0$ and $\lambda_E = 0.005$ based on Monte Carlo simulation. Simulation setting: a circular network with radius 500 m. Each simulation value is obtained as the arithmetic mean of 10000 simulation outcomes.

V. Performance Analysis: General Scenario

This section derives the connection and secrecy probabilities of the general scenario with multiple transmission pairs. We focus on a typical pair and again define the transmitter and receiver by x_0 and y_0, respectively.

A. Connection Probability

In this scenario, y_0 receives interference from not only the jammers in Φ_J and Ψ_J but also the concurrent transmitters in $\Phi_T \cap B(y_0, D)$. Thus, the SINR of y_0 is given by

$$\mathrm{SINR}_{x_0,y_0} = \frac{G_T G_R h^L_{x_0,y_0} r_0^{-\alpha_L}}{\sum_{\varphi \in \{\Phi_T, \Phi_J, \Psi_J\}} I^{y_0}_{\varphi} + \sigma^2/P}, \tag{21}$$

where $I^{y_0}_{\varphi}$ ($\varphi \in \{\Phi_T, \Phi_J\}$) denotes the interference from $\varphi \cap B(y_0, D)$. Note that the Laplace transform of $I^{y_0}_{\Phi_T}$ can be easily obtained based on Lemma 3, which is given in the following lemma.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

Lemma 5. *The Laplace transform of $I_{\Phi_T}^{y_0}$ is*

$$\mathcal{L}_{I_{\Phi_T}^{y_0}}(\lambda_T, s) = \exp\left(-2\pi\lambda_T \sum_{\mathrm{b}}\sum_{\mathrm{g}} p_{\mathrm{b}} q_{\mathrm{g}} \int_0^D F_{\mathrm{b}}(s\mathrm{g}, r) r \mathrm{d}r\right) \times \exp\left(-2\pi\lambda_T \sum_{\mathrm{g}} q_{\mathrm{g}} \int_D^\infty F_N(s\mathrm{g}, r) r \mathrm{d}r\right), \quad (22)$$

where $F_{\mathrm{b}}(\cdot,\cdot)$ is given by (10).

Proof: The proof follows directly from Lemma 3. ■

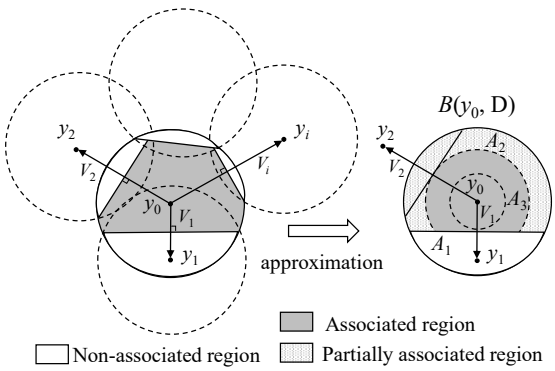


Fig. 3. Approximation of associated region. y_i $(i = 1, 2, \cdots)$: the i-th nearest receiver to y_0; V_i: random distance between y_i and y_0.

Next, we derive the Laplace transform of $I_{\Phi_J}^{y_0}$. According to the SCJ scheme, the LoS ball $B(y_0, D)$ of y_0 may contain jammers that are not associated with y_0, i.e., jammers that are closer to other receivers than y_0. We call these jammers non-associated jammers and the region where they reside non-associated region. Fig. 3 shows an example of the non-associated region, where y_i denotes the $i-$th closest receiver to y_0 and V_i denotes the corresponding random distance. As shown in Fig. 3, the shape of the non-associated region is irregular, making it difficult to derive the exact Laplace transform of $I_{\Phi_J}^{y_0}$. Thus, we resort to a good approximation, which is given in the following lemma.

Lemma 6. *The Laplace transform of $I_{\Phi_J}^{y_0}$ in the general scenario can be approximated by*

$$\mathcal{L}_{I_{\Phi_J}^{y_0}}(s) \approx \exp\left(-2\pi\lambda_J \sum_{\mathrm{g}} q_{\mathrm{g}} \int_0^\infty F_N(s\mathrm{g}, r) r \mathrm{d}r\right) \times \int_0^\infty \int_{v_1}^\infty \exp\left(-2p_L\lambda_J \sum_{\mathrm{g}} q_{\mathrm{g}} Q_1(s, v_1)\right) \exp\left(-2\xi(v_2) p_L \lambda_J \sum_{\mathrm{g}} q_{\mathrm{g}} Q_2(s, v_1, v_2)\right) f_{V_1,V_2}(v_1, v_2) \mathrm{d}v_2 \mathrm{d}v_1, \quad (23)$$

where

$$Q_1(s, v_1) = \int_{\min\{\frac{v_1}{2}, D\}}^D \left(F_L(s\mathrm{g}, r) - F_N(s\mathrm{g}, r)\right) \arccos\left(\frac{v_1}{2r}\right) r \mathrm{d}r, \quad (24)$$

$$Q_2(s, v_1, v_2) = \int_{\min\{\frac{v_2}{2}, D\}}^D \left(F_L(s\mathrm{g}, r) - F_N(s\mathrm{g}, r)\right) \left(\pi - \arccos\left(\frac{v_1}{2r}\right)\right) r \mathrm{d}r, \quad (25)$$

$$\xi(v_2) = \min\left\{\frac{2\lambda_R \int_{v_2}^{2D} A(r) r \mathrm{d}r}{D^2 - (v_2/2)^2}, 1\right\}, \quad (26)$$

$$A(r) = D^2 \arccos\left(\frac{r}{2D}\right) - \frac{r}{2}\sqrt{D^2 - \left(\frac{r}{2}\right)^2}, \quad (27)$$

$$f_{V_1,V_2}(v_1, v_2) = (2\pi\lambda_R)^2 v_1 v_2 \exp\left(-\lambda_R \pi v_2^2\right). \quad (28)$$

Proof: The idea is partitioning the LoS ball $B(y_0, D)$ into three parts as illustrated in Fig. 3, i.e., the *non-associated region* A_1, where the jammers are associated with y_1, the ring-like *partially associated region* A_2, where part of the jammers are associated with the remaining receivers y_i $(i = 2, 3, \cdots)$, and the *associated region* A_3, where the jammers are associated with y_0. According to the SCJ scheme, the locations of the jammers in A_1 and A_3 can be modeled by homogeneous PPPs. The most challenging task is to model the locations of the jammers in A_2, since each receiver y_i $(i = 2, 3, \cdots)$ carves out a sub-non-associated region from A_2 and these sub-non-associated regions may overlap, forming an irregular non-associated region (see Fig. 3). To tackle this challenge, we remove the non-associated region from A_2 and approximate the locations of LoS and NLoS jammers in A_2 by two independent and homogenous PPPs with densities $\xi p_L \lambda_J$ and $(1 - \xi p_L)\lambda_J$ respectively. Here, $\xi \in [0, 1]$ denotes the probability that a jammer in A_2 is located in the non-associated region. For the detailed proof, please refer to Appendix D. ■

Next, we derive the Laplace transform of $I_{\Psi_J}^{y_0}$. Note that Ψ_J is a Poisson Hole Process (PHP), making it challenging to derive the exact $\mathcal{L}_{I_{\Psi_J}^{y_0}}(s)$ due to the difficulty of accurately characterizing the impacts of the holes, i.e., the LoS balls of the receivers. One approach is to consider only the hole $B(y_0, D)$ and neglect all the other holes. This is equivalent to the simplified scenario. Since the interferers in Ψ_J have only NLoS links to y_0 and are far away, this approach yields accurate approximation. Based on this approach, the Laplace transform of $I_{\Psi_J}^{y_0}$ in the generalized scenario can be approximated by that of the simplified scenario in Lemma 2. Based on Lemmas 2, 5 and 6, we derive the connection probability in the following theorem.

Theorem 3. *The connection probability of the transmission pairs in the general scenario is approximated by*

$$p_c \approx \sum_{k=1}^{N_L} \binom{N_L}{k} (-1)^{k+1} e^{-\frac{k\mu\sigma^2}{P}} \mathcal{L}_{I_{\Phi_T}^{y_0}}(\lambda_T, k\mu) \mathcal{L}_{I_{\Phi_J}^{y_0}}(k\mu) \mathcal{L}_{I_{\Psi_J}^{y_0}}(k\mu), \quad (29)$$

where $\mu = \frac{\tau_L r_0^{\alpha_L}(2^{R_t} - 1)}{G_T G_R}$, $\tau_L = N_L (N_L!)^{-1/N_L}$, $\mathcal{L}_{I_{\Phi_T}^{y_0}}(\cdot)$ is given by (22), $\mathcal{L}_{I_{\Phi_J}^{y_0}}(\cdot)$ is given by (23) and $\mathcal{L}_{I_{\Psi_J}^{y_0}}(\cdot)$ is given by (9).

Proof: The proof follows after replacing the inequality in Theorem 1 with approximation. ■

Using the simulator in [37], we also conducted simulations for the connection probability under various settings of λ_T and λ_P to verify the effectiveness of the approximation in Theorem 3. The simulation results as well as the theoretical

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

ones are shown in Fig. 4. These results indicate that the approximation is accurate and the analytical expression in Theorem 3 is effective to model the connection probability of the transmission pairs in the general case.

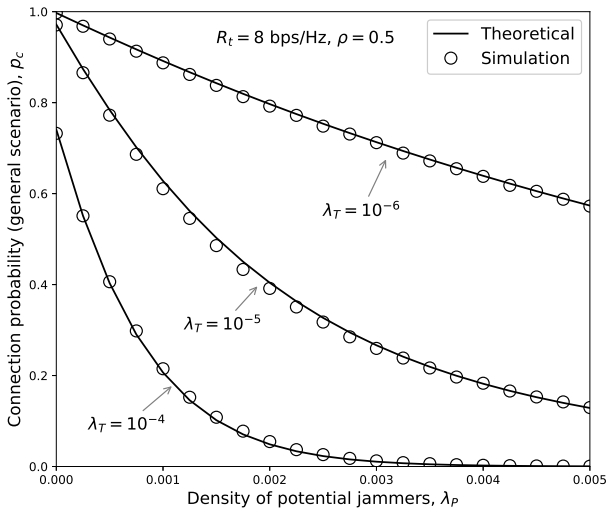


Fig. 4. Validation of the approximation in Theorem 3 based on Monte Carlo simulation. Simulation setting: a circular network with radius 500m. Each simulation value is obtained as the arithmetic mean of 10000 simulation outcomes.

For comparison, we also investigate the connection probabilities of the case with partial jamming (PJ), where, according to the jamming scheme in [18], a fraction ϱ of the potential jammers send artificial noise. This can be interpreted as the case where each potential jammer decides to be a jammer independently with probability ϱ. Thus, the resulting PPP of the jammers is simply an independent thinning of the original PPP Φ_P of the potential jammers. Based on Theorem 3, the connection probability of the PJ scheme can be given by the following corollary.

Corollary 1. *The connection probability of the transmission pairs under the PJ scheme can be given by*

$$p_c^{\mathrm{PJ}} \approx \sum_{k=1}^{N_L} \binom{N_L}{k} (-1)^{k+1} e^{-\frac{k\mu\sigma^2}{P}} \mathcal{L}_{I^{y_0}_{\Phi_T}}(\lambda_T + \varrho\lambda_P, k\mu), \quad (30)$$

where $\mu = \frac{\tau_L r_0^{\alpha_L}(2^{R_t}-1)}{G_T G_R}$, $\tau_L = N_L (N_L!)^{-1/N_L}$ *and* $\mathcal{L}_{I^{y_0}_{\Phi_T}}(\cdot,\cdot)$ *is given by (22).*

Proof. The proof follows directly from Theorem 3. □

B. Secrecy Probability

In the general scenario, the SINR of an eavesdropper z is

$$\mathrm{SINR}^{\mathsf{b},\hat{\mathsf{g}}}_{x_0,z} = \frac{\hat{\mathsf{g}} h^{\mathsf{b}}_{x_0,z} \|x_0 - z\|^{-\alpha_{\mathsf{b}}}}{\sum_{\varphi\in\{\Phi_T,\Phi_J,\Psi_J\}} I^z_\varphi + \sigma^2/P}, \quad (31)$$

where I^z_φ ($\varphi \in \{\Phi_T, \Phi_J, \Psi_J\}$) denotes the interference from the interferers in $\varphi \cap B(z, D)$. Note that the Laplace transform of $I^z_{\Phi_T}$ can be directly given based on that of $I^z_{\Phi_J}$ in Lemma 3. Thus, we have

$$\mathcal{L}_{I^z_{\Phi_T}}(\lambda_T, s) = \mathcal{L}_{I^z_{\Phi_J}}(\lambda_T, s), \quad (32)$$

where $\mathcal{L}_{I^z_{\Phi_J}}(\cdot,\cdot)$ is given by Lemma 3.

Next, we derive the Laplace transform $\mathcal{L}_{I^z_{\Psi_J}}(s)$ of $I^z_{\Psi_J}$, in which we need to deal with the PHP Ψ_J. According to the definition of Ψ_J, each node of the baseline PPP $\bar{\Phi}_J$ is retained (i.e., not removed by the holes) with probability $e^{-\lambda_R \pi D^2}$. Thus, one approach to characterize the impact of holes is to approximate Ψ_J by a homogeneous PPP with density $e^{-\lambda_R \pi D^2}\bar{\lambda}_J$. This approach (say Approach 1) reduces the density of interferers in the neighborhood of z, and may underestimate the interference to some extent and result in an upper bound on the Laplace transform, as shown by the figures (Fig. 7 - Fig. 12) in [39]. Another approach is to neglect the holes, i.e., approximate Ψ_J by a homogeneous PPP with density $\bar{\lambda}_J$. This approach overestimates the interference and thus yields a lower bound. To further improve this lower bound, the authors in [39] considered only the hole closest to z and showed that the new bound is tight enough. However, the typical point z in [39] is assumed to be located outside the holes. As a result, this new approach (say Approach 2) cannot be directly applied in our case, where z can be inside or outside the holes. This paper therefore combines the above three approaches to approximate $\mathcal{L}_{I^z_{\Psi_J}}(s)$. Specifically, we first approximate Ψ_J by a homogeneous $\widetilde{\Phi}_J$ with density

$$\widetilde{\lambda}_J = (\beta e^{-\lambda_R \pi D^2} + (1-\beta))\bar{\lambda}_J, \quad (33)$$

where $\beta \in [0, 1]$, and then carve out the hole closest to z from $\widetilde{\Phi}_J$. The parameter β here is used to adjust the accuracy of the approximation. The approximation of $\mathcal{L}_{I^z_{\Psi}}(s)$ is given in the following lemma.

Lemma 7. *The Laplace transform* $\mathcal{L}_{I^z_{\Psi}}(s)$ *of the general scenario can be approximated by*

$$\mathcal{L}_{I^z_{\Psi_J}}(s, r_e) \approx \int_0^\infty \int_{|r_e - r_0|}^{r_e + r_0} e^{-\widetilde{\lambda}_J \sum_{\mathsf{b}} \sum_{\hat{\mathsf{g}}} p_{\mathsf{b}} q_{\hat{\mathsf{g}}} T_1(s, \min\{u,v\})} e^{-\widetilde{\lambda}_J \sum_{\hat{\mathsf{g}}} q_{\hat{\mathsf{g}}} T_2(s, \min\{u,v\})} h(u) f(v) \mathrm{d}u \mathrm{d}v, \quad (34)$$

where $\widetilde{\lambda}_J$ *is given by (33),* $T_1(\cdot,\cdot)$ *by (17),* $T_2(\cdot,\cdot)$ *by (18),* $h(u)$ *by (19) and* $f(v) = 2\pi\lambda_R v e^{-\lambda_R \pi v^2}$.

Proof: We define the receiver closest to z by $\tilde{y}$. Note that $\tilde{y}$ can be y_0 or the receiver closest to z except y_0 (say y^*). Thus, assuming z is at the origin, we have $\|\tilde{y}\| = \min\{\|y_0\|, \|y^*\|\}$. It follows from Appendix B that

$$\mathcal{L}_{I^z_{\Psi_J}}(s, r_e) \approx \mathbb{E}_{\|\tilde{y}\|}\Big[e^{-\widetilde{\lambda}_J \sum_{\mathsf{b}} \sum_{\hat{\mathsf{g}}} p_{\mathsf{b}} q_{\hat{\mathsf{g}}} T(s, \|\tilde{y}\|)} e^{-\widetilde{\lambda}_J \sum_{\hat{\mathsf{g}}} q_{\hat{\mathsf{g}}} T_2(s, \|\tilde{y}\|)} \Big]. \quad (35)$$

The PDF of $\|y_0\|$ can be given by (19) and that of $\|y^*\|$ by $f(v)$ according to [40]. Substituting $\|\tilde{y}\| = \min\{\|y_0\|, \|y^*\|\}$ into (35) and then taking the expectation in terms of $\|y_0\|$ and $\|y^*\|$ completes the proof. ■

Please note that our analysis can actually cover the two approaches in [39] as special cases. For example, the Laplace transform result of Approach 1 can be obtained by Lemma 3 when setting $\lambda_J = e^{-\lambda_R \pi D^2}\bar{\lambda}_J$ and the Laplace transform result of Approach 2 can be obtained by Lemma 7 when setting $\beta = 0$. Based on Lemmas 3 and 7, we now derive the secrecy probability of the transmission pairs for the general scenario.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

Theorem 4. *The secrecy probability p_s of the transmission pairs in the general scenario can be approximated by*

$$p_s \approx \exp\Bigg(-2\pi\sum_{\mathsf{b}}\sum_{\hat{\mathsf{g}}} p_{\mathsf{b}} q_{\hat{\mathsf{g}}}\lambda_E \sum_{k=1}^{N_{\mathsf{b}}}\binom{N_{\mathsf{b}}}{k}(-1)^{k+1}\int_0^D \mathrm{d}r_e \, e^{-k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}\frac{\sigma^2}{P}}\mathcal{L}_{I^z_{\Phi_J}}(\lambda_T+\lambda_J, k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}})\mathcal{L}_{I^z_{\Psi_J}}(k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}, r_e) r_e\Bigg)$$
$$\times \exp\Bigg(-2\pi\sum_{\hat{\mathsf{g}}} q_{\hat{\mathsf{g}}}\lambda_E\sum_{k=1}^{N_N}\binom{N_N}{k}(-1)^{k+1}\int_D^\infty e^{-k\nu_N r_e^{\alpha_N}\frac{\sigma^2}{P}} \mathcal{L}_{I^z_{\Phi_J}}(\lambda_T+\lambda_J, k\nu_N r_e^{\alpha_N})\mathcal{L}_{I^z_{\Psi_J}}(k\nu_N r_e^{\alpha_N}, r_e) r_e \mathrm{d}r_e\Bigg), \quad (36)$$

where $\nu_{\mathsf{b}} = \frac{\tau_{\mathsf{b}}(2^{R_e}-1)}{\hat{\mathsf{g}}}$, $\tau_{\mathsf{b}} = N_{\mathsf{b}}(N_{\mathsf{b}}!)^{-1/N_{\mathsf{b}}}$, $\mathcal{L}_{I^z_{\Phi_J}}(\cdot,\cdot)$ and $\mathcal{L}_{I^z_{\Psi_J}}(\cdot,\cdot)$ are given by Lemmas 3 and 7, respectively.

Proof: The proof follows after replacing the inequality in Theorem 2 by approximation. ■

Simulations based on the simulator in [37] were also conducted under various settings of λ_T, λ_E and λ_P to demonstrate the effectiveness of the approximated secrecy probability in Theorem 4. The simulation results as well as the corresponding theoretical ones obtained by our approach and the two approaches in [39] are shown in Fig. 5. These results indicate that the approximation in Theorem 4 is effective to model the secrecy probability of the transmission pairs in the general scenario. In addition, the results show that our approach gives more accurate approximation to secrecy probabilities than the above two approaches in [39], especially for small densities of transmitters.

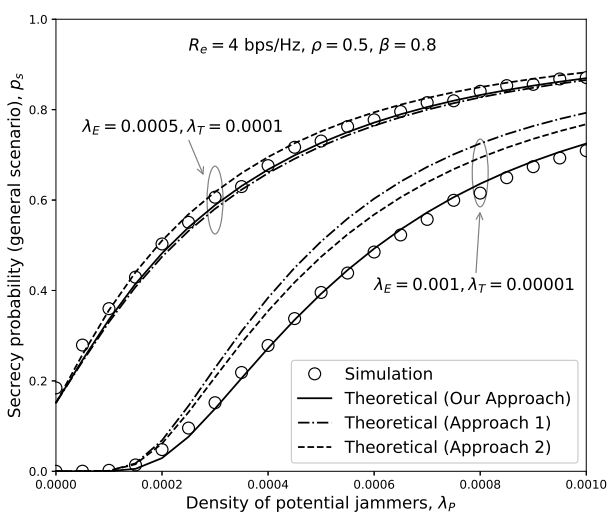


Fig. 5. Validation of the approximation in Theorem 4 based on Monte Carlo simulation. Simulation setting: a circular network with radius 500m. Each simulation value is obtained as the arithmetic mean of 100000 simulation outcomes.

We now justify the superiority of the proposed SCJ scheme in terms of STC performance enhancement.

Lemma 8. *The proposed SCJ scheme improves the network STC under the general scenario.*

Proof: To prove this lemma, we need to show that for any network with legitimate transmission pair density λ_T and eavesdropper density λ_E, we can properly set the parameters λ_P and ρ of the proposed SCJ scheme to achieve a better STC performance than the case without applying the SCJ scheme. Obviously, one such setting is that $\rho = 0$ and λ_P can be any value. In this case, no potential jammers inside the LoS balls of the receivers become jammers. In other words, all the jammers lie outside the LoS balls of the receivers. Thus, we have $\lambda_J = \rho p_N \lambda_P = 0$. For a typical receiver, the jammers have NLoS links to it and are at least distance D away, so their interference can be neglected due to the severe signal attenuation. This is equivalent to the case without the SCJ scheme where there is no interference from jammers. Hence, the connection probability in this case is identical to that of the case without the SCJ scheme. However, this is not the case for eavesdroppers, since the jammers may be inside their LoS balls and have LoS links to them. Thus, the eavesdroppers in this case suffer from more interference than in the case without the SCJ scheme, leading to a greater secrecy probability. As a result, the proposed SCJ scheme improves the network STC performance. ■

The secrecy probabilities for the PJ case is also given in the following corollary based on Theorem 4.

Corollary 2. *The secrecy probability for the transmission pairs under the PJ scheme can be given by*

$$p_s^{\mathrm{PJ}} \approx \exp\Bigg(-2\pi\sum_{\mathsf{b}}\sum_{\hat{\mathsf{g}}} p_{\mathsf{b}} q_{\hat{\mathsf{g}}}\lambda_E \sum_{k=1}^{N_{\mathsf{b}}}\binom{N_{\mathsf{b}}}{k}(-1)^{k+1} \int_0^D e^{-k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}\frac{\sigma^2}{P}}\mathcal{L}_{I^z_{\Phi_J}}(\lambda_T+\varrho\lambda_P, k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}) r_e \mathrm{d}r_e\Bigg)$$
$$\times \exp\Bigg(-2\pi\sum_{\hat{\mathsf{g}}} q_{\hat{\mathsf{g}}}\lambda_E\sum_{k=1}^{N_N}\binom{N_N}{k}(-1)^{k+1} \int_D^\infty e^{-k\nu_N r_e^{\alpha_N}\frac{\sigma^2}{P}}\mathcal{L}_{I^z_{\Phi_J}}(\lambda_T+\varrho\lambda_P, k\nu_N r_e^{\alpha_N}) r_e \mathrm{d}r_e\Bigg), \quad (37)$$

where $\nu_{\mathsf{b}} = \frac{\tau_{\mathsf{b}}(2^{R_e}-1)}{\hat{\mathsf{g}}}$, $\tau_{\mathsf{b}} = N_{\mathsf{b}}(N_{\mathsf{b}}!)^{-1/N_{\mathsf{b}}}$ and $\mathcal{L}_{I^z_{\Phi_J}}(\cdot,\cdot)$ is given by Lemma 3.

Proof: The proof follows directly from Theorem 4. ■

Remark 1. *Note that deriving the accurate results on secrecy probability is extremely challenging, because this involves the complicated interference modeling for legitimate receivers and eavesdroppers under the random point process (in particular the Poisson Hole Process concerned in this paper), which remains a long-lasting open problem by now [32]. That is why the available works (including this work) mainly focus on the efficient approximation for interferences at legitimate receivers and eavesdroppers and thus deriving bounds on the secrecy probability, see, for example, [17], [19]–[22].*

C. Optimal SCJ Parameters

The most important parameter in the proposed SCJ scheme is the interference-control factor ρ, i.e., the jammer selection

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

probability inside the region $\mathcal{B}$ covered by the LoS balls of the receivers. In general, the noise generated by the jammers is helpful to suppress eavesdroppers but harmful to the receivers. Thus, the larger the parameter ρ is, the larger the secrecy probability p_s is but the smaller the connection probability p_c becomes. As a result, there exists an optimal ρ, denoted by ρ^*, that maximizes the STC $\bar{R}_s(\rho)$. Thus, we can formulate the following optimization problem to find the ρ^*, provided all the other system parameters (e.g., λ_T, λ_E and λ_P) are given.

$$\mathbf{P1}: \ \rho^* = \arg\max_{\rho\in[0,1]} p_c(\rho)p_s(\rho)(R_t - R_e)\lambda_T. \quad (38)$$

Similarly, there also exists an optimal ϱ, denoted by ϱ^*, to maximize the STC under the PJ scheme. The ϱ^* can be obtained by solving the following optimization problem.

$$\mathbf{P2}: \ \varrho^* = \arg\max_{\varrho\in[0,1]} p_c^{\mathrm{PJ}}(\varrho)p_s^{\mathrm{PJ}}(\varrho)(R_t - R_e)\lambda_T. \quad (39)$$

Network designers may be also interested in the optimal network STC performance under a constraint ε on the total density of legitimate nodes (i.e., legitimate pairs and potential jammers). Thus, we also formulate the following two optimization problems to facilitate network design.

$$\mathbf{P3}: \max_{\rho\in[0,1],\lambda_T+\lambda_P\in[0,\varepsilon]} p_c(\rho)p_s(\rho)(R_t - R_e)\lambda_T, \quad (40)$$

$$\mathbf{P4}: \max_{\varrho\in[0,1],\lambda_T+\lambda_P\in[0,\varepsilon]} p_c^{\mathrm{PJ}}(\varrho)p_s^{\mathrm{PJ}}(\varrho)(R_t - R_e)\lambda_T. \quad (41)$$

Although closed-form solutions to these four optimization problems may not be available, they can be numerically solved.

VI. Numerical Results

This section provides numerical results to evaluate the optimal STC performance achieved by the proposed SCJ scheme. We adopt the parameter settings in Table I unless stated otherwise, and also set the codeword rates as $R_t = 8$ bps/Hz, $R_e = 4$ bps/Hz and the factor β as $\beta = 0.8$ for all the figures. All results are obtained by numerically solving the optimization problems in Section V-C.

A. Optimal STC vs. Density of Potential Jammers λ_P

Fig. 6 shows the impacts of the density of potential jammers λ_P on the optimal STC under both the SCJ and PJ schemes. In this figure, we fix λ_T as 0.00007 and consider two cases with different density of eavesdroppers λ_E, i.e., ($\lambda_E = 0.0001$ and $\lambda_E = 0.0001$). We can see from Fig. 6 that, for the SCJ scheme scheme, the optimal STC first increases as λ_P increases and finally remains unchanged. This implies that the proposed SCJ scheme can can improve the network STC performance by deploying more jammers The reason for the finally unchanged optimal STC under the SCJ scheme is that, when λ_P exceeds some threshold, the optimal jamming parameter ρ^* decreases to 0. This means that all the jammers are outside the LoS balls, i.e., the region $\mathcal{B}$, and thus generate interference only to the eavesdroppers. As a result, as λ_P further increases from the threshold, the connection probability

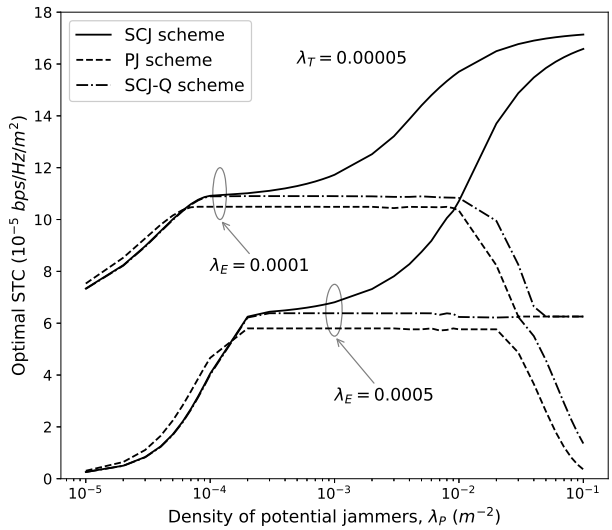


Fig. 6. Optimal STC vs. density of potential jammers λ_P.

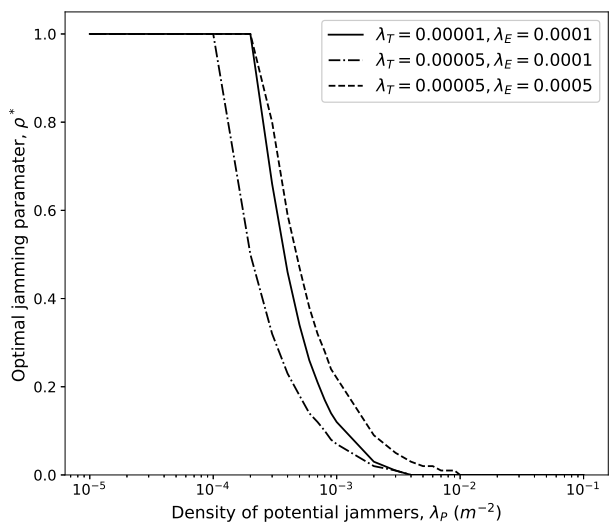


Fig. 7. Optimal jamming parameter ρ^* vs. density of potential jammers λ_P.

remains constant, while the secrecy probability will finally increase to one and stay unchanged, leading to a constant STC. Different from the SCJ scheme, as λ_P keeps increasing, the optimal STC of the PJ scheme further decreases and finally remains constant. The differences between the behaviors of the two schemes show the benefits of the jammers outside the LoS balls of legitimate receivers (i.e., the jammers in Ψ_J) in improving the STC performance. To demonstrate this expectation, we consider a variant SCJ scheme, named SCJ-Q scheme, where the jammers in Ψ_J remain quiet, i.e., $\bar{\lambda}_J$ denotes the density of quiet jammers. We compare the SCJ-Q scheme and the SCJ scheme in terms of the optimal STC performance in Fig. 6. We can observe from Fig. 6 that the proposed SCJ scheme achieves better STC performance than the SCJ-Q scheme, implying that the jammers in Ψ_J have a significant impact on the STC performance enhancement.

A careful observation in Fig. 6 indicates that when λ_P is smaller than some value (about 0.00009 in Fig. 6), the

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

optimal STC achieved by the SCJ scheme is slightly smaller than that achieved by the PJ scheme. However, when λ_P is larger than this value, the SCJ scheme achieves better STC performance than the PJ scheme, and the gap between these two schemes increases significantly as λ_P increases. This implies that the proposed SCJ scheme can greatly improve the STC performance achieved by the PJ scheme by deploying a large number of potential jammers, showing the effectiveness of the SCJ scheme in ensuring the secrecy of transmissions at the physical layer.

Fig. 7 shows the optimal parameter ρ^* of the SCJ scheme versus λ_P under the three cases considered in Fig. 6. We can observe from Fig. 7 that ρ^* decreases as λ_P increases, and finally decreases to 0. This observation explains the reason for the finally unchanged STC in Fig. 6, and also serve as a guideline for setting the value of the jamming parameter ρ to achieve the optimal STC. Another careful observation from Fig. 7 indicates that ρ^* decreases as λ_T increases while increases as λ_E increases.

B. Optimal STC vs. Density of Transmission Pairs λ_T

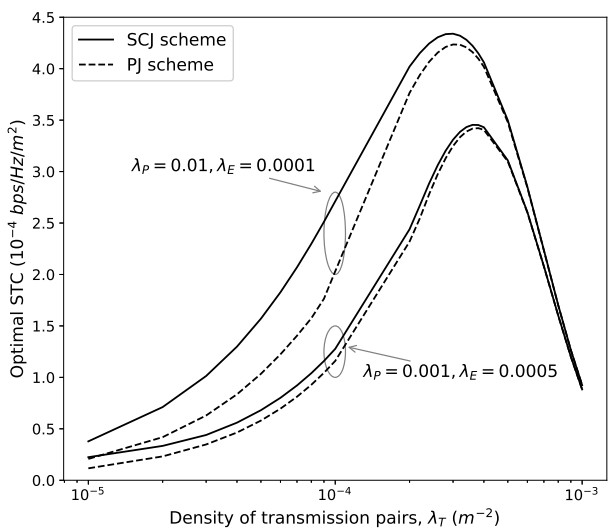


Fig. 8. Optimal STC vs. density of transmission pairs λ_T.

To investigate the impacts of λ_T on the optimal STC performance, we show in Fig. 8 the optimal STC versus λ_T under two cases with different values of λ_P and λ_E, i.e., ($\lambda_P = 0.01$, $\lambda_E = 0.0001$) and ($\lambda_P = 0.001$, $\lambda_E = 0.0005$). We can see from Fig. 8 that as λ_T increases, the optimal STC first increases, then drastically decreases and will finally vanish. This is because when λ_T is small, the change of λ_T dominates the trend of the optimal STC more than the changes of secrecy probability and connection probability do. However, when λ_T is large, the network becomes dense and the interference from concurrent transmitters leads to significantly decreased connection probability. In this case, the decrease of the connection probability dominates the trend of the optimal STC more than the increase of the λ_T does.

Another observation from Fig. 8 suggests that the STC gap between the SCJ scheme and the PJ scheme is large when λ_T is small, and this gap vanishes as λ_T increases. This is because smaller λ_T yields smaller LoS ball region $\mathcal{B}$ and thus more jammers that are outside the $\mathcal{B}$. In addition, smaller λ_T yields larger associated regions (as shown in Fig. 3) inside the LoS balls of legitimate receivers. As a result, the jamming signals from the jammers are more detrimental to the eavesdroppers than to the legitimate receivers. Thus, the SCJ scheme outperforms the PJ scheme in this case. However, as λ_T increases, the region $\mathcal{B}$ becomes larger and will finally cover the whole network region. In this case, the associated region inside the LoS ball of each legitimate receiver vanishes. Thus, the SCJ scheme is equivalent to the PJ scheme and thus achieves the same STC performance. The large gap between the SCJ and PJ schemes for small λ_T indicates that the SCJ scheme is more effective when the density of transmission pairs is low.

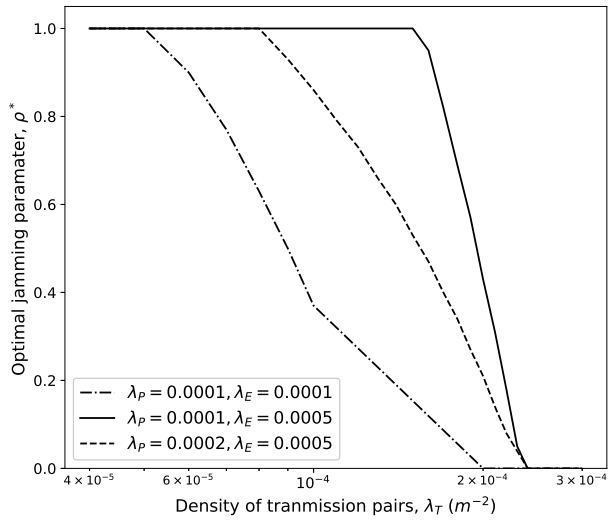


Fig. 9. Optimal jamming parameter ρ^* vs. density of transmission pairs λ_T.

Fig. 9 shows the behavior of the optimal jamming parameter ρ^* versus λ_T under three cases, i.e., ($\lambda_P = 0.0001$, $\lambda_E = 0.0001$), ($\lambda_P = 0.0001$, $\lambda_E = 0.0005$) and ($\lambda_P = 0.0002$, $\lambda_E = 0.0005$). It can be seen from Fig. 9 that the ρ^* decreases as λ_T increases, which is consistent with the observation from Fig. 7. This can also help us determine the optimal settings of the jamming parameter ρ during the system design.

C. Optimal STC and Energy Efficiency vs. Total Density Constraint ε

This subsection explores the impacts of the total density constraint ε on the optimal STC performance. By solving optimization problems P3 and P4, we show in Fig. 10 the optimal STC versus ε under two cases of $\lambda_E = 0.0001$ and $\lambda_E = 0.0005$. The results show that the optimal STC increases as ε increases for both the proposed SCJ scheme and the PJ scheme. A careful observation indicates that the optimal STC of the PJ scheme finally remains unchanged, while that of the proposed SCJ scheme keeps increasing, yielding an increasingly large STC gap. This suggests that the proposed SCJ scheme outperforms the PJ scheme in terms

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

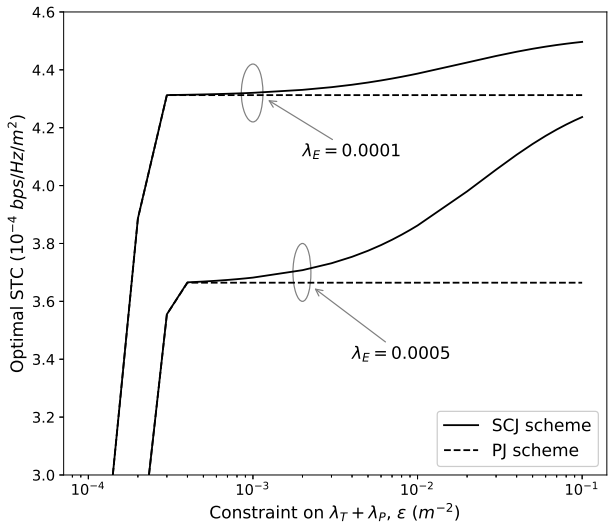


Fig. 10. Optimal STC vs. total density constraint ε.

of the STC performance under the total density constraint, and the performance gap between these two schemes enlarges as the constraint ε increases.

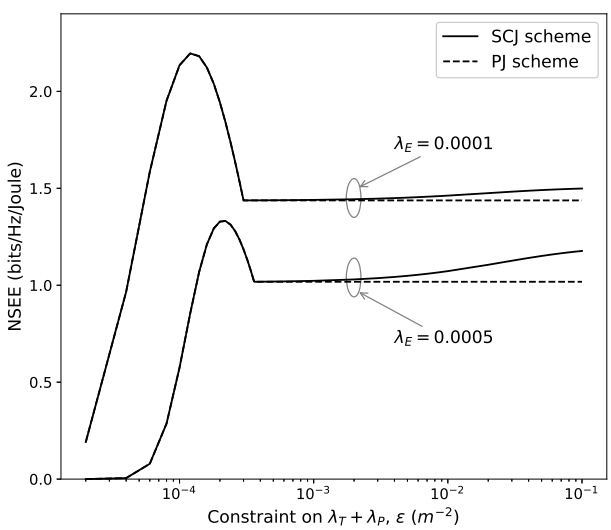


Fig. 11. NSEE vs. total density constraint ε.

The better STC performance of the SCJ is achieved by deploying more potential jammers, which may consume more energy. Thus, we need to compare the energy efficiency of both schemes. To do this, we adopt the metric of network-wide energy efficiency (NSEE) from [41], which can be formulated as

$$NSEE = \frac{\bar{R}_s}{(\lambda_T + \lambda_J + e^{-\lambda_R \pi D^2} \bar{\lambda}_J)P}, \tag{42}$$

where $\bar{R}_s$ denotes the STC and the denominator denotes the average power per unit area, including that of the legitimate transmitters, jammers in Φ_J and jammers in Ψ_J. The unit of the NSEE is $bits/Hz/Joule$. For NSEE comparison, we consider the case in Fig. 10 where both schemes achieve the optimal STC under the total constraint ε. Fig. 11 shows the NSEE of both schemes versus ε under two cases of $\lambda_E = 0.0001$ and $\lambda_E = 0.0005$. The results show that the NSEEs of both schemes first increase and then decrease as ε increases. Similar to the STC, the NSEE of the PJ scheme finally remains unchanged, while that of the SCJ scheme continues increasing. This indicates that the SCJ scheme also outperforms the PJ scheme in terms of the NSEE performance and the performance gap between these two schemes enlarges as the constraint ε increases. The results in this subsection show the superiority of the proposed SCJ scheme over the PJ scheme in terms of not only the STC performance but also energy efficiency.

D. Optimal STC vs. Density of Eavesdroppers λ_E

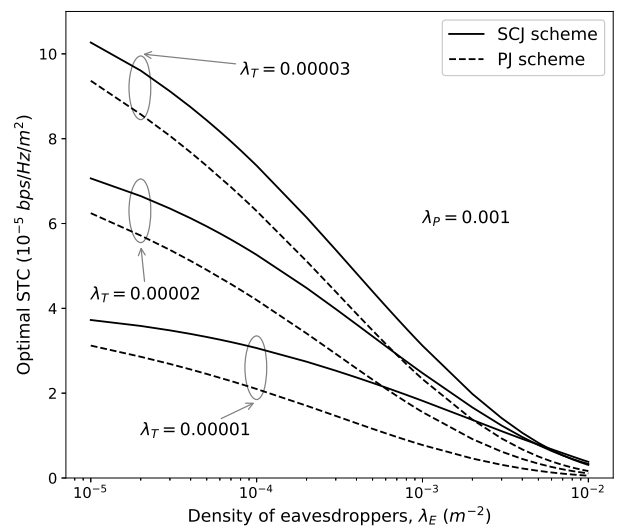


Fig. 12. Optimal STC vs. density of eavesdroppers λ_E.

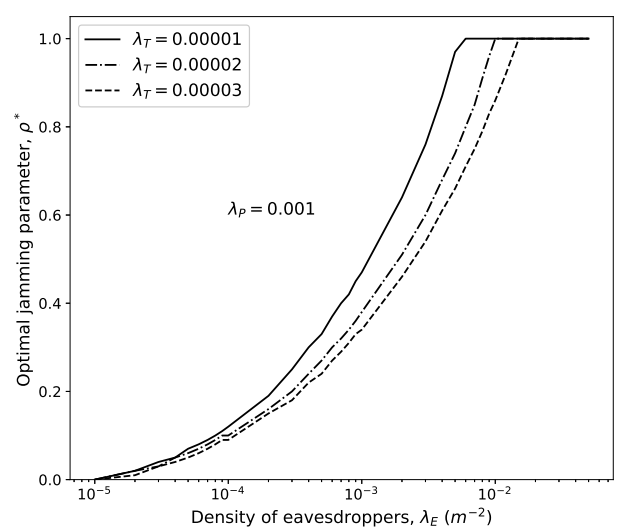


Fig. 13. Optimal jamming parameter ρ^* vs. density of eavesdroppers λ_E.

To explore the impacts of density of eavesdroppers λ_E on the STC performance, we show the optimal STC versus λ_E in Fig. 12 under the setting of $\lambda_P = 0.001$. Three cases of

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

λ_T are considered, which are $\lambda_T = 0.00001$, $\lambda_T = 0.00002$ and $\lambda_T = 0.00003$. We can observe from Fig. 12 that the optimal STC decreases as λ_E increases. This is intuitive since more eavesdroppers leads to lower secrecy probability and thus smaller STC. The superiority of the SCJ scheme over the PJ scheme in terms of the STC performance can also be seen from the figure. Fig. 13 illustrates the behavior of the optimal jamming parameter ρ^* versus λ_E under the same settings of λ_T and λ_P as adopted in Fig. 12. As seen from the figure, the ρ^* increases as λ_E increases. This implies that when there exists more eavesdroppers in the network, we need to adopt a larger jamming parameter ρ to achieve the optimal STC performance.

VII. Conclusions

A Sight-based Cooperative Jamming (SCJ) scheme was proposed in this paper to improve the physical layer security performance in millimeter-wave (mmWave) ad hoc networks, and the related theoretical framework was also developed to model the secrecy transmission capacity (STC) achievable from adopting the jamming scheme. The results in this paper indicate that the proposed jamming scheme can significantly improve the STC of mmWave ad hoc networks, especially for networks with low density of transmission pairs. For an SCJ-based ad hoc network with given densities of transmission pairs, potential jammers and eavesdroppers, our theoretical framework can serve as a guideline on the proper settings of jamming parameter such that the optimal STC performance of the network can be achieved. Although this paper considers the "nearest receiver" association policy, other policies are also possible, like the "smallest average received power" policy. Thus, an interesting topic is the design of optimal association policy, which serves as one future work.

Appendix A
Proof of Lemma 1

Due to the independent thinning by the antenna gains between the jammers and y_0, the jammers in Φ_J seen from y_0 can be modeled by independent sub-PPPs Φ_J^{g} with density $q_{\mathsf{g}}\lambda_J$, where $\mathsf{g} \in \{G_T G_R, G_T g_R, g_T G_R, g_T g_R\}$ denotes the antenna gain. Thus, we have $I_{\Phi_J}^{y_0} = \sum_{\mathsf{g}} I_{\Phi_J^{\mathsf{g}}}^{y_0}$, where

$$I_{\Phi_J^{\mathsf{g}}}^{y_0} = \sum_{x \in \Phi_J^{\mathsf{g}}} \mathsf{g} h_{x,y_0}^N \|x - y_0\|^{-\alpha_N}. \tag{43}$$

Since the sub-PPPs Φ_J^{g} are independent, we have

$$\mathcal{L}_{I_{\Phi_J}^{y_0}}(s) = \prod_{\mathsf{g}} \mathcal{L}_{I_{\Phi_J^{\mathsf{g}}}^{y_0}}(s). \tag{44}$$

Placing y_0 at the origin (i.e., $y_0 = o$) yields

$$\begin{aligned}
\mathcal{L}_{I_{\Phi_J^{\mathsf{g}}}^{y_0}}(s) &= \mathbb{E}\Big[\exp\Big(-s \sum_{x \in \Phi_J^{\mathsf{g}}} \mathsf{g} h_{x,o}^N \|x\|^{-\alpha_N}\Big)\Big] \\
&\overset{(a)}{=} \mathbb{E}_{\Phi_J^{\mathsf{g}}}\Big[\prod_{x \in \Phi_J^{\mathsf{g}}} \mathbb{E}_{h_{x,o}^N}\Big[e^{-s\mathsf{g} h_{x,o}^N \|x\|^{-\alpha_N}}\Big]\Big] \\
&\overset{(b)}{=} \mathbb{E}_{\Phi_J^{\mathsf{g}}}\Big[\prod_{x \in \Phi_J^{\mathsf{g}}} \Big(1 + \frac{s\mathsf{g}}{N_N \|x\|^{\alpha_N}}\Big)^{-N_N}\Big] \\
&\overset{(c)}{=} \exp\Big(-q_{\mathsf{g}}\lambda_J \int_{\mathbb{R}^2} F_N(s\mathsf{g}, \|x\|)\mathrm{d}x\Big) \\
&\overset{(d)}{=} \exp\Big(-2\pi q_{\mathsf{g}}\lambda_J \int_0^\infty F_N(s\mathsf{g}, r) r \mathrm{d}r\Big),
\end{aligned} \tag{45}$$

where $F_{\mathsf{b}}(\cdot,\cdot)$ is given by (10), (a) follows since $h_{x,o}^N$ are i.i.d., (b) follows from the moment generating function (MGF) of the gamma random variable $h_{x,o}^N$, (c) follows after applying the probability generating functional (PGF) of the PPP [40] and (d) follows after changing to the polar coordinates. Substituting (45) into (44) completes the proof.

Appendix B
Proof of Lemma 4

We divide Ψ_J into sub-point processes inside and outside the LoS ball $B(z, D)$ based on the independent thinning by link condition and antenna gains. Thus, we have

$$\mathcal{L}_{I_{\Psi_J}^z}(s, r_e) = \prod_{\mathsf{b}} \prod_{\hat{\mathsf{g}}} \mathcal{L}_{I_{\Psi_{J,I}^{\mathsf{b},\hat{\mathsf{g}}}}^z}(s, r_e) \prod_{\hat{\mathsf{g}}} \mathcal{L}_{I_{\Psi_{J,O}^{N,\hat{\mathsf{g}}}}^z}(s, r_e), \tag{46}$$

where $\Psi_{J,I}^{\mathsf{b},\hat{\mathsf{g}}}$ (resp. $\Psi_{J,O}^{N,\hat{\mathsf{g}}}$) denotes the sub-PPPs inside (resp. outside) $B(z, D)$. Note that $\Psi_{J,I}^{\mathsf{b},\hat{\mathsf{g}}}$ is equivalent to $\bar{\Phi}_{J,I}^{\mathsf{b},\hat{\mathsf{g}}} \cap B^c(y_0, D)$, where $\bar{\Phi}_{J,I}^{\mathsf{b},\hat{\mathsf{g}}}$ is the homogeneous baseline PPP with density $p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \bar{\lambda}_J$ inside $B(z, D)$. Assuming that the eavesdropper z is located at the origin and defining $\Xi_I = B^c(y_0, D) \cap B(z, D)$ and $\Xi_O = B^c(y_0, D) \cap B^c(z, D)$, we have

$$\begin{aligned}
\mathcal{L}_{I_{\Psi_{J,I}^{\mathsf{b},\hat{\mathsf{g}}}}^z}(s, r_e) &= \mathbb{E}\Big[\exp\Big(-s \sum_{x \in \bar{\Phi}_J^{\mathsf{b},\hat{\mathsf{g}}}} \hat{\mathsf{g}} h_{x,o}^{\mathsf{b}} \|x\|^{-\alpha_{\mathsf{b}}}\Big)\Big] \\
&= \exp\Big(-p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \bar{\lambda}_J \underbrace{\int_{\Xi_I} F_{\mathsf{b}}(s\hat{\mathsf{g}}, \|x\|)\mathrm{d}x}_{T_1}\Big),
\end{aligned} \tag{47}$$

$$\begin{aligned}
\mathcal{L}_{I_{\Psi_{J,O}^{N,\hat{\mathsf{g}}}}^z}(s, r_e) &= \mathbb{E}\Big[\exp\Big(-s \sum_{x \in \bar{\Phi}_{J,O}^{N,\hat{\mathsf{g}}}} \hat{\mathsf{g}} h_{x,o}^N \|x\|^{-\alpha_N}\Big)\Big] \\
&= \exp\Big(-q_{\hat{\mathsf{g}}} \bar{\lambda}_J \underbrace{\int_{\Xi_O} F_N(s\hat{\mathsf{g}}, \|x\|)\mathrm{d}x}_{T_2}\Big),
\end{aligned} \tag{48}$$

We can see that T_1 and T_2 depend on the distance $\|y_0\|$ between y_0 and $z = o$. If $\|y_0\| \in [0, D)$, T_1 and T_2 can be given by

$$T_1 = 2\int_{D-\|y_0\|}^{D} F_{\mathsf{b}}(s\hat{\mathsf{g}}, r)\Big(\pi - \arccos\Big(\frac{\|y_0\|^2 + r^2 - D^2}{2\|y_0\| r}\Big)\Big) r \mathrm{d}r, \tag{49}$$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

$$T_2 = 2\pi \int_D^{\infty} F_N(s\hat{\mathsf{g}}, r) r \mathrm{d}r \quad (50)$$
$$-2 \int_D^{\|y_0\|+D} F_N(s\hat{\mathsf{g}}, r) \arccos\Big(\frac{\|y_0\|^2+r^2-D^2}{2\|y_0\|r}\Big) r \mathrm{d}r.$$

If $\|y_0\| \in [D, 2D)$, T_1 can be given by

$$T_1 = 2\pi \int_0^{D} F_{\mathsf{b}}(s\hat{\mathsf{g}}, r) r \mathrm{d}r \quad (51)$$
$$-2 \int_{\|y_0\|-D}^{D} F_{\mathsf{b}}(s\hat{\mathsf{g}}, r) \arccos\Big(\frac{\|y_0\|^2+r^2-D^2}{2\|y_0\|r}\Big) r \mathrm{d}r,$$

T_2 is identical to that of the case of $\|y_0\| \in [0, D)$. If $\|y_0\| \in [2D, \infty)$, T_1 and T_2 can be given by

$$T_1 = 2\pi \int_0^{D} F_{\mathsf{b}}(s\hat{\mathsf{g}}, r) r \mathrm{d}r, \quad (52)$$

$$T_2 = 2\pi \int_D^{\infty} F_N(s\hat{\mathsf{g}}, r) r \mathrm{d}r \quad (53)$$
$$-2 \int_{\|y_0\|-D}^{\|y_0\|+D} F_N(s\hat{\mathsf{g}}, r) \arccos\Big(\frac{\|y_0\|^2+r^2-D^2}{2\|y_0\|r}\Big) r \mathrm{d}r$$

Summarizing (49), (51) and (52) yields the $T_1(s, \|y_0\|)$ in (17), and summarizing (50) and (53) yields the $T_2(s, \|y_0\|)$ in (18). Note that $\|y_0\| \in [|r_e - r_0|, r_e + r_0]$ and the probability density function (PDF) of $\|y_0\|$ can be given by (19). Thus, substituting (47) and (48) into (46) and then taking the expectation of (46) in terms of $\|y_0\|$ completes the proof.

Appendix C
Proof of Theorem 2

Assuming x_0 is located at the origin, we have

$$\mathbb{P}\Big(\cap_{z \in \Phi_{E,I}^{\mathsf{b},\hat{\mathsf{g}}}} \mathrm{SINR}_{x_0,z}^{\mathsf{b},\hat{\mathsf{g}}} \le 2^{R_e} - 1 \Big) \quad (54)$$
$$\overset{(a)}{=} \mathbb{E}\Big[\prod_{z \in \Phi_{E,I}^{\mathsf{b},\hat{\mathsf{g}}}} \mathbb{P}\Big(h_{o,z}^{\mathsf{b}} \le (2^{R_e}-1)\|z\|^{\alpha_{\mathsf{b}}} \big(\sum_{\varphi} I_{\varphi}^{z} + \frac{\sigma^2}{P}\big)/\hat{\mathsf{g}} \Big) \Big]$$
$$\overset{(b)}{\ge} \mathbb{E}_{\{\varphi\}, \Phi_{E,I}^{\mathsf{b},\hat{\mathsf{g}}}} \Big[\prod_{z \in \Phi_{E,I}^{\mathsf{b},\hat{\mathsf{g}}}} \Big(1 - e^{-\nu_{\mathsf{b}} \|z\|^{\alpha_{\mathsf{b}}} (\sum_{\varphi} I_{\varphi}^{z} + \frac{\sigma^2}{P})} \Big)^{N_{\mathsf{b}}} \Big]$$
$$\overset{(c)}{=} \mathbb{E}_{\{\varphi\}} \Big[\exp\Big(-2\pi p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \lambda_E$$
$$\int_0^D \Big[1 - \Big(1 - e^{-\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}} (\sum_{\varphi} I_{\varphi}^{z} + \frac{\sigma^2}{P})} \Big)^{N_{\mathsf{b}}} \Big] r_e \mathrm{d}r_e \Big) \Big]$$
$$\overset{(d)}{\ge} \exp\Big(-2\pi p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \lambda_E \sum_{k=1}^{N_{\mathsf{b}}} \binom{N_{\mathsf{b}}}{k} (-1)^{k+1}$$
$$\int_0^D e^{-k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}} \frac{\sigma^2}{P}} \prod_{\varphi} \mathbb{E}_{\varphi}[e^{-k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}} I_{\varphi}^{z}}] r_e \mathrm{d}r_e \Big)$$
$$= \exp\Big(-2\pi p_{\mathsf{b}} q_{\hat{\mathsf{g}}} \lambda_E \sum_{k=1}^{N_{\mathsf{b}}} \binom{N_{\mathsf{b}}}{k} (-1)^{k+1} \int_0^D \mathrm{d}r_e$$
$$e^{-k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}} \frac{\sigma^2}{P}} \mathcal{L}_{I_{\Phi_J}^{z}}(k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}) \mathcal{L}_{I_{\Psi_J}^{z}}(k\nu_{\mathsf{b}} r_e^{\alpha_{\mathsf{b}}}, r_e) r_e \Big),$$

where (a) follows since $h_{o,z}^{\mathsf{b}}$ are i.i.d., (b) follows from the Lemma 1 in [34], (c) follows after applying the PGF of the PPP and (d) follows from the binomial theorem and the Jensen's inequality. Similarly, we can prove that

$$\mathbb{P}\Big(\cap_{z \in \Phi_{E,O}^{N,\hat{\mathsf{g}}}} \mathrm{SINR}_{x_0,z}^{N,\hat{\mathsf{g}}} \le 2^{R_e} - 1 \Big) \quad (55)$$
$$\ge \exp\Big(-2\pi q_{\hat{\mathsf{g}}} \lambda_E \sum_{k=1}^{N_N} \binom{N_N}{k} (-1)^{k+1} \int_D^{\infty} \mathrm{d}r_e$$
$$e^{-k\nu_N r_e^{\alpha_N} \frac{\sigma^2}{P}} \mathcal{L}_{I_{\Phi_J}^{z}}(k\nu_N r_e^{\alpha_N}) \mathcal{L}_{I_{\Psi_J}^{z}}(k\nu_N r_e^{\alpha_N}, r_e) r_e \Big).$$

Substituting (54) and (55) into (13) completes the proof.

Appendix D
Proof of Lemma 6

We first calculate ξ as the ratio of the expected area of the non-associated region inside A_2 to the area of A_2. Note that the non-associated region in A_2 is the union of many sub-non-associated regions, each formed by a D2D receiver located in the region $\Xi = B(y_0, 2D) \backslash B(y_0, V_2)$. To simplify the calculation, we ignore the overlaps of the sub-non-associated regions and calculate the area of the non-associated region as the sum of the areas of the sub-non-associated regions. Assuming $y_0 = o$, the area of the sub-non-associated region formed by a D2D receiver $y \in \Xi$ is $A(\|y\|)$, where $A(\cdot)$ is given by (27). Thus, the area of the non-associated region in A_2 is $\sum_{y \in \Phi_R \cap \Xi} A(\|y\|)$. Applying the Campbell theorem [40], we obtain the expected area

$$\mathbb{E}_{\Phi_R}\Big[\sum_{y \in \Phi_R \cap \Xi} A(\|y\|) \Big] = 2\pi\lambda_R \int_{V_2}^{2D} A(r) r \mathrm{d}r. \quad (56)$$

Since the area of the non-associated region must be no larger than that of A_2, which is $\pi(D^2 - (V_2/2)^2)$, ξ can be given by the $\xi(V_2)$ in (26).

Next, we calculate the Laplace transform of the interference from the three regions A_1, A_2 and A_3. Based on Lemma 1, we can derive the three Laplace transforms as

$$\mathcal{L}_{A_1} = \exp\Big(-\lambda_J \sum_{\mathsf{b}} \sum_{\mathsf{g}} p_{\mathsf{b}} q_{\mathsf{g}} \int_{A_1} F_{\mathsf{b}}(s\mathsf{g}, \|x\|) \mathrm{d}x \Big), \quad (57)$$

$$\mathcal{L}_{A_2} \approx \exp\Big(-\xi(V_2) p_L \lambda_J \sum_{\mathsf{g}} q_{\mathsf{g}} \int_{A_2} F_L(s\mathsf{g}, \|x\|) \mathrm{d}x \Big) \quad (58)$$
$$\times \exp\Big(-(1-\xi(V_2) p_L) \lambda_J \sum_{\mathsf{g}} q_{\mathsf{g}} \int_{A_2} F_N(s\mathsf{g}, \|x\|) \mathrm{d}x \Big),$$

and

$$\mathcal{L}_{A_3} = \exp\Big(-\lambda_J \sum_{\mathsf{g}} q_{\mathsf{g}} \int_{B(y_0,D)\backslash(A_1 \cup A_2)} F_N(s\mathsf{g}, \|x\|) \mathrm{d}x \Big) \quad (59)$$

Also, we need to calculate the Laplace transform of the interference from outside $B(y_0, D)$, which is

$$\mathcal{L}_{A_4} = \exp\Big(-\lambda_J \sum_{\mathsf{g}} q_{\mathsf{g}} \int_{B^c(y_0,D)} F_N(s\mathsf{g}, \|x\|) \mathrm{d}x \Big). \quad (60)$$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

Calculating the integrals in (57), (58) and (59) in polar coordinates and then multiplying them yields

$$\begin{aligned}\mathcal{L}_{I_{\Phi_J}^{y_0}} &= \mathcal{L}_{A_1}\cdot\mathcal{L}_{A_2}\cdot\mathcal{L}_{A_3}\cdot\mathcal{L}_{A_4} \qquad (61)\\ &\approx \exp\Big(-2\pi\lambda_J\sum_{q_{\mathrm{g}}} q_{\mathrm{g}}\int_0^\infty F_N(s\mathrm{g},r)r\mathrm{d}r\Big)\\ &\quad\times\exp\Big(-p_L\lambda_J\sum_{q_{\mathrm{g}}} q_{\mathrm{g}}Q_1(s,V_1)\Big)\\ &\quad\times\exp\Big(-\xi(V_2)p_L\lambda_J\sum_{q_{\mathrm{g}}} q_{\mathrm{g}}Q_2(s,V_1,V_2)\Big),\end{aligned}$$

where $Q1$ and $Q2$ are given by (24) and (25), respectively. Note that the joint PDFs of V_1 and V_2 can be given by (28) according to [42]. Finally, taking the expectation of $\mathcal{L}_{I_{\Psi_J}^{y_0}}$ in (61) in terms of V_1 and V_2 completes the proof.

References

[1] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5g cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[2] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, and G. Chen, "Millimeter wave communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1616–1653, thirdquarter 2018.

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

[4] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018.

[5] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

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

[7] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, Early Access, 2018.

[8] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5g wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, 2018.

[9] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, 2015.

[10] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan 2016.

[11] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug 2016.

[12] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for device-to-device communication: A physical layer security perspective," *IEEE J. Sel. Areas Commun.*, Early Access, 2018.

[13] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for d2d inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan 2019.

[14] 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, 2017.

[15] S. Sun, T. S. Rappaport, M. Shafi, P. Tang, J. Zhang, and P. J. Smith, "Propagation models and performance evaluation for 5g millimeter-wave bands," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8422–8439, Sep. 2018.

[16] M. Shafi, J. Zhang, H. Tataria, A. F. Molisch, S. Sun, T. S. Rappaport, F. Tufvesson, S. Wu, and K. Kitao, "Microwave vs. millimeter-wave propagation channels: Key differences and impact on 5g cellular systems," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 14–20, December 2018.

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

[18] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of uav-enabled mmwave networks using matern hardcore point processes," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1397–1409, 2018.

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

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

[21] 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, 2018.

[22] X. Sun, W. Yang, Y. Cai, L. Tao, Y. Liu, and Y. Huang, "Secure transmissions in wireless information and power transfer millimeter-wave ultra-dense networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1817–1829, July 2019.

[23] Y. Ju, H. Wang, T. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2675–2689, April 2018.

[24] X. Sun, W. Yang, Y. Cai, Z. Xiang, and X. Tang, "Secure transmissions in millimeter wave swipt uav-based relay networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 785–788, June 2019.

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

[26] W. Yang, L. Tao, X. Sun, R. Ma, Y. Cai, and T. Zhang, "Secure on-off transmission in mmwave systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 32 681–32 692, 2019.

[27] R. Ma, W. Yang, X. Sun, L. Tao, and T. Zhang, "Secure communication in millimeter wave relaying networks," *IEEE Access*, vol. 7, pp. 31 218–31 232, 2019.

[28] Y. Song, W. Yang, X. Yang, Z. Xiang, and B. Wang, "Physical layer security in cognitive millimeter wave networks," *IEEE Access*, vol. 7, pp. 109 162–109 180, 2019.

[29] Y. Ju, H. Wang, T. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2114–2127, May 2017.

[30] Y. Ju, H. Wang, Q. Pei, and H. Wang, "Physical layer security in millimeter wave df relay systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 12, pp. 5719–5733, Dec 2019.

[31] H. Zhao, J. Zhang, L. Yang, G. Pan, and M. Alouini, "Secure mmwave communications in cognitive radio networks," *IEEE Wireless Communications Letters*, vol. 8, no. 4, pp. 1171–1174, Aug 2019.

[32] M. Haenggi, *Stochastic geometry for wireless networks*. Cambridge University Press, 2012.

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

[34] A. Thornburg, T. Bai, and R. W. Heath, "Performance analysis of outdoor mmwave ad hoc networks," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4065–4079, 2016.

[35] N. Deng and M. Haenggi, "A fine-grained analysis of millimeter-wave device-to-device networks," *IEEE Trans. Wireless Commun.*, vol. 65, no. 11, pp. 4940–4954, Nov 2017.

[36] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[37] Monte carlo simulator used in cooperative jamming for secure mmwave ad hoc communications. [Online]. Available: https://github.com/yy90zhang/SimulatorForMmWaveCJPaper

[38] S. Singh, M. N. Kulkarni, A. Ghosh, and J. G. Andrews, "Tractable model for rate in self-backhauled millimeter wave cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2196–2211, 2015.

[39] Z. Yazdanshenasan, H. S. Dhillon, M. Afshang, and P. H. J. Chong, "Poisson hole process: Theory and applications to wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7531–7546, Nov 2016.

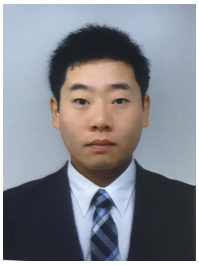
[40] S. Chiu, D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 3rd ed. Wiley, 2013.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2021.3054507, IEEE Transactions on Information Forensics and Security

[41] T. Zheng, H. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. on Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, 2017.

[42] D. Moltchanov, "Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146 – 1166, 2012.



Yuanyu Zhang (S'17–A'17–M'18) received the B.S. and M.S. degrees from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree from Future University Hakodate, Hakodate, Hokkaido, Japan in 2017. He is currently an Assistant Professor of the Graduate School of Science and Technology, Nara Institute of Science and Technology, Ikoma, Japan, and also a guest Associate Professor of the School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China. His research interests include physical layer security, distributed ledger technology and the performance modeling and evaluation of wireless networks.

Yulong Shen (M'09) received the B.S. and M.S. degrees in computer science and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. He is currently a Professor with the School of Computer Science and Technology, Xidian University, where he is also an Associate Director of the Shaanxi Key Laboratory of Network and System Security and a member of the State Key Laboratory of Integrated Services Networks. His research interests include wireless network security and cloud computing security. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS, and SOWN.

Xiaohong Jiang (M'03–SM'09) received his B.S., M.S. and Ph.D degrees in 1989, 1992, and 1999 respectively, all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Before joining Future University, Dr. Jiang was an Associate professor, Tohoku University, from Feb. 2005 to Mar. 2010. Dr. Jiang's research interests include computer communications networks, mainly wireless networks and optical networks, network security, routers/switches design, etc. He has published over 300 technical papers at premium international journals and conferences, which include over 70 papers published in top IEEE journals and top IEEE conferences, like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, IEEE Transactions on Parallel and Distributed Systems, IEEE INFOCOM.

Shoji Kasahara (A'94–M'98) received the B. Eng., M. Eng., and Dr. Eng. degrees from Kyoto University, Kyoto, Japan, in 1989, 1991, and 1996, respectively. Currently, he is a Professor of Graduate School of Information Science, Nara Institute of Science and Technology, Nara, Japan. His research interests include stochastic modeling and analytics of large-scale complex systems based on computer/communication networks.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/