On the Physical Layer Security of Untrusted Millimeter Wave Relaying Networks: A Stochastic Geometry Approach

Mohammad Ragheb, S. Mostafa Safavi Hemami, Ali Kuhestani, *Member, IEEE,*
Derrick Wing Kwan Ng, *Fellow, IEEE* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—The physical layer security (PLS) of millimeter wave (mmWave) communication systems is investigated, where the secure source-to-destination communication is assisted by an untrusted relay selected from a group of them and there are also several passive eavesdroppers (Eves) in the network. In the considered system model, while the distributions of the untrusted relays and Eves follow a homogeneous Poisson Point Process (PPP). To maximize the instantaneous secrecy rate, a novel joint relay selection and power allocation (JRP) method is developed where the destination and source aim for jamming the reception of both the untrusted relays and passive Eves. New expressions of the optimal power allocation (OPA) are derived for both non-colluding Eves (NCE) and colluding Eves (CE). Subsequently, by considering the impact of potential blockages, new closed-form equations are derived for analyzing the system's ergodic secrecy rate (ESR) and secrecy outage probability (SOP) for transmission over fading mmWave channels. Finally, numerical examples are provided for demonstrating the superiority of our proposed JRP method over the relevant benchmarks found in the literature. Interestingly, the ESR increases with the density of untrusted relays for both the NCE and CE scenarios, which is a benefit of the improved probability of selecting a relay with a stronger second-hop channel. Furthermore, in the low transmit power regime, employing relatively low mmWave frequencies achieves better ESR, while in the high transmit power regime, high mmWave frequencies provide higher ESR.**

I. Introduction

The wireless data traffic is expected to escalate further into the foreseeable future due to the ever-growing popularity of video-networks and the Internet-of-Things (IoT) [2]. Unfortunately, traditional sub-6 GHz communications cannot support these data rates due to its limited licensed bandwidth. As a result, researchers have turned their attention to the abundant unlicensed spectral resources in the millimeter wave (mmWave) frequency band (30-300 GHz) for mitigating the impending spectrum crunch [3]. However, mmWave systems suffer from high propagation losses, sensitivity to blockage, and time-varying statistics. As a remedy, highly directional beamforming techniques have been proposed for mitigating the path loss of mmWave systems [4]. The authors of [5] have designed a hybrid secure precoder for boosting the physical layer security (PLS) of a cognitive mmWave wiretap channel, where the channel-state-information (CSI) of multiple eavesdroppers (Eves) is imperfectly known. A range of popular spatial statistical models of the mmWave channel were presented in [6] and [7]. To be specific, the authors of [6] have highlighted the presence of line-of-sight (LoS) and non-line-of-sight (NLoS) links in the system model.

Although increasing the number of base station (BS) antennas results in a high directional beam, the cells still have to be relatively small. A promising technique of overcoming this problem is to allow intermediate relay nodes to forward traffic from a BS to a user equipment (UE), which has poor links to nearby BSs. Due to its promising potential to route around blockages, using two-hop relaying is capable of improving the mmWave communication coverage [8]- [9]. Recently, several papers have studied the system coverage as well as the average ergodic rate of cooperative cellular systems under the stochastic geometry framework [8]- [9]. The authors of [9] quantified both the coverage probability and the capacity of mmWave systems, which are often influenced by blockages. In particular, the results of [9] reveal that the system performance can be significantly improved with the assistance of intermediate relays. Furthermore, the coverage probability of spatially random decode-and-forward (DF) relays was investigated both for direct transmission and for relay-aided links in [10] to highlight the performance gains brought about by relaying. By investigating a full-duplex mmWave multi-relay system, Cai *et al.* [11] proposed an innovative two-timescale analog-digital hybrid beamforming scheme, based on low-dimensional effective matrices for maximizing the sum rate. The authors of [12] also investigated the potential advantages of utilizing two-way amplify-and-forward (AF) relays to assist the bidirectional exchange of data between two nodes in a mmWave system. In mmWave systems, although directional antennas were adopted for improving the communication security, they still remained vulnerable to eavesdropping attacks, when the Eves were located within the focus of the signal beams. Clearly, the security of mmWave communications has to be further improved.

As a potential remedy, PLS is capable of safeguarding the confidential information from interception by exploiting the randomness inherent in wireless channels [13]–[20], hence it has drawn significant research attention in the past few years. For instance, the authors of [16] focused their attention on

Part of this paper was presented at the 28th Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, Aug. 2020 [1]. This work was supported by the Iran National Science Foundation (INSF) under Grant 99028262.

M. Ragheb and S. M. Safavi Hemami are with the Electrical Engineering Department, Amirkabir University of Technology, Tehran, Iran (email: mohammad_ragheb@aut.ac.ir; safavi@aut.ac.ir)

A. Kuhestani is with the Communications and Electronics Department, Faculty of Electrical and Computer Engineering, Qom University of Technology, Qom 3716146611, Iran (e-mail: kuhestani@qut.ac.ir).

D. W. K. Ng is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Australia (e-mail: w.k.ng@unsw.edu.au).

L. Hanzo is with the University of Southampton, Southampton SO17 1BJ, U.K, (e-mail: hanzo@soton.ac.uk).

Corresponding author: S. Mostafa Safavi Hemami

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/P034284/1 and EP/P003990/1 (COALESCE) as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028)

the PLS analysis of mmWave cellular systems. In particular, a mathematical framework was established for investigating the secrecy performance of hybrid mmWave systems in the face of both fading and blockages. Furthermore, the authors of [17] studied secure mmWave systems, where the positions of Eves are modeled as an independent homogeneous Poisson Point Process (PPP). They found artificial noise (AN) beamforming has more beneficial than conventional maximal ratio combining (MRT) aided beamforming, especially in the face of numerous eavesdroppers, who would benefit from a high transmit power. Additionally, in [18], Zhu *et al.* analyzed the PLS of large-scale mmWave *ad-hoc* networks without the assistance of relaying, where the Eves were randomly located. Based on relays as collaborators, the authors of [19] have proposed a physical-layer secret key generation relying on a technique they termed as channel quality indicator-mapped spatial modulation for enhancing the PLS of multi-hop IoT networks. Furthermore, Gong *et al.* [20] have studied the secrecy beamforming design of mmWave two-way AF relaying networks, where the transmit and receive beamformers of two source nodes and the relay beamforming matrix were jointly optimized for further reducing the amount of information that was potentially recoverable by Eve. We note that a relay node can either be deployed by an operator, using a so-called infrastructure relay in long term evolution (LTE) terminology, or can be an idle UE that is used opportunistically. This latter scenario is indeed attractive, because it does not drastically change the network topology or infrastructure requirements. Since a UE serving as a relay connects to a destination UE via a device-to-device (D2D) link, it is often referred as a D2D relay. Despite its benefits, there is paucity of contributions on D2D relay-assisted mmWave cellular communications [21], [22]. Note that since in D2D relaying, no information is available about authenticity of relays, therefore, it is vitally important to study the untrusted relaying scenario in mmWave communication systems, which has not been addressed in the literature.

Amidst various PLS methods, cooperative relaying, cooperative jamming (CJ), cooperative beamforming, and a combination of these methods have gained a lot attention in the context of both conventional microwave [23], [24] and mmWave cellular networks [7], [13], [25]. Additionally, a hybrid cooperative relaying and jamming can be implemented for secrecy enhancement using the available knowledge of the main and wiretap links [24]. Note that cooperative jamming (CJ) methods can be exploited for security improvement by transmitting jamming signals to degrade the received signal quality at Eves [26], [27]. Inspired by this, various innovative techniques such as source-based jamming [7], [26], friendly jammer-based AN transmission [28], or destination-based CJ (DBCJ) [27], [29] have been proposed for designing effective resource allocation policies, while meeting the secrecy requirements. In practice, DBCJ may be realized by applying self-interference cancellation at the destination to remove the interference caused by jamming upon exploiting any prior knowledge about the jamming noise. As such, numerous contributions have adopted the DBCJ technique for secure communications in conventional untrusted relaying networks [23], [27], [30]–[33]. For instance, Saedi *et al.* [31] studied an untrusted relaying network in the presence of an active malicious jammer. Furthermore, Sun *et al.* [32], [33] demonstrated that increasing the number of untrusted relays would substantially reduce the ergodic secrecy rate (ESR) - a trend, which is fundamentally different from the scenario of trusted relays. Additionally, Kuhestani *et al.* [34] developed a joint relay selection and power allocation (JRP) technique for security enhancement in untrusted relaying networks under the scenarios of both non-colluding Eves (NCE) and colluding Eves (CE). Wang *et al.* [35] studied a secure cooperative communication scenario relying on decode-and-forward relays, when only the cumulative distribution information (CDF) of the Eves is available. Based on the security scheme of [35], one of the relays is selected from the set of candidates for forwarding the confidential messages, while the rest are harnessed for generating jamming in order to confuse the Eves. In [36], the relays and jammers acting as helper nodes are exploited by taking into account their positions and their degrees of social trust with the source node. Deng *et al.* [37] investigated the problem of secure communications for a system model consisting of one source, one destination, one Eve and one helper. The authors studied a part of specific scenarios, where the helper node either transmits AN, or plays the role of a relay. By defining the metric of distance-normalized signal to noise ratio (DN-SNR), the authors of [37] analytically derived the OPA and highlighted that depending on the Eve's position, either direct transmission or relaying provides better secrecy performance. By considering practical hardware imperfections and channel estimation errors, the authors of [38] studied the secrecy performance of a multi-hop cooperative network with untrusted relays. Furthermore, Forouzesh *et al.* [39] investigated joint covert communication and secure transmission in untrusted relaying aided *microwave* cellular systems, where multiple non-colluding and colluding wardens[1] overhear the communications.

In contrast to the above mentioned contributions focusing on the microwave band (sub-6 GHz), Ju *et al.* [7] comprehensively studied secure transmission in mmWave DF relaying systems under three different wiretapping scenarios. They highlighted the efficiency of AN-aided transmission by evaluating the secrecy outage probability (SOP). Furthermore, secure communication under randomize-and-forward relaying was investigated by Ma *et al.* [13], for both NCE and CE scenarios. In contrast to the aforementioned treatises [7], [10], [13], in our previous work [25], we have proposed a secure scheme for transmission over mmWave channels and designed a new optimal power allocation (OPA) arrangement for untrusted AF relaying systems operating in the face of randomly positioned Eves, while only the LoS link participates in data transmission.

As a further development, the author teams of [34] and [40] have studied OPA in the presence of multiple-untrusted relays and passive Eves in *a conventional microwave cellular network*. Additionally, in [25] an OPA scheme was designed

[1] The warden is an adversary node that only tries to detect the presence of communication, while Eve represents a more curious node that tries to extract the data exchanged between two nodes [39].

for mmWave untrusted relaying networks by only considering the LoS component. Furthermore, Ragheb *et al.* [1] optimized the power allocation for increasing the ESR in the presence of shadow fading in a mmWave network, when a BS transmits confidential messages to a mobile user with the aid of an untrusted relay in the presence of NCEs and obstacles. However, the impact of OPA on a mmWave cellular network relying on multiple untrusted relays and considering both LoS/NLoS effects has not been reported in the open literature. To fill this gap, this treatise considers a range of practical assumptions related to secure mmWave communications by shedding light on untrusted mmWave relaying. Accordingly, we focus our attention on enhancing the PLS of a cooperative mmWave system, where a large-scale antenna-array (LSAA) aided source communicates with a destination relying on a LSAA in the presence of multiple non-colluding untrusted AF relays and NCE [25], [34]. A specific worst-case scenario is considered, where multiple passive Eves cooperate for increasing the equivalent SNR in a scenario reminiscent of [25].

In our system model, the distributions of both the relays and passive Eves are modeled by independent PPPs, which allows us to employ powerful mathematical tools for stochastic geometry. In our analysis, the effect of blockages is also taken into account for characterizing both LoS and NLoS links. To improve the information security in the above-mentioned two scenarios, the JRP approach is pursued. To design robust secure transmission, the message leakage to Eves is considered during both the first and second phases of communication. As a benchmark, we use the conventional direct transmission (DT) ignoring the relays' presence to compare with our proposal. We note that in contrast to [17] where only passive Eves are in the system model, untrusted relays acting as potential Eves also exist in our system model. As a result the security analysis of even the conventional scheme is more complicated than that in [17]. We also notice that compared to [29][2] and its extension in [34], in our work besides the destination, we have proposed the injection of noise by the source, and accordingly, we have faced with a more complex power allocation problem. We note that the absence of source's injection noise at work [34] causes information leakage to the Eves and therefore, the proposed secure transmission scheme in [34] suffers from a security weakness. Additionally, in contrast to [34], where the Eves are distributed near the relay, and the relays are placed in deterministic positions, in our work, both the Eves and relays are distributed based on PPP distributions with different densities. Accordingly, the issue of power allocation and relay selection is totally different. To expound a little further, Wang *et al.* [41] proposed a successive relaying scheme for a secure AF relaying network operating in the face of multiple untrusted nodes, where the detrimental the inter-relay interference is turned into a beneficial source of noise used for confusing the untrusted relays. To reduce the information leakage, the authors used zero-forcing beamforming at the source combined with a new relay selection policy for minimizing the SOP. In contrast to [41] where only untrusted relays exist in the system model, in our work, we additionally consider external Eves that operate under either the NCE or CE policy, a situation further aggravated by the presence of untrusted relays.

The main contributions of this paper are boldly and explicitly contrasted to the relevant literature in Table I, which are summarized in more detail as follows:

- We develop a JRP technique for maximizing the instantaneous secrecy rate in both NCE and CE scenarios. We take into account both the LoS and NLoS paths along with the impact of both the main-lobes and side-lobes generated by multiple antennas, which is a more realistic scenario than that of [25].
- Based on the proposed JRP technique, a compact closed-form expression is derived for characterizing the ESR performance in a single untrusted relay scenario by using the Laplace transform and incomplete Gamma function integration. These expressions provide important engineering insights into the impact of the key system parameters, such as the antenna gain, mmWave frequency as well as the relaying node and Eve densities on the system performance.
- For the multiple untrusted relays scenario, we derive a new closed-form expression for the cumulative distribution function (CDF) for the received signal at the destination, and then analyze the ESR and SOP performances. Our numerical examples illustrate that the proposed JRP technique significantly improves the ESR compared to its counterpart relying on a single untrusted relay.
- For the conventional DT scheme with MRT beamforming [13], [17], we derive closed-form expressions for the ESR and SOP performance metrics, including both NCE and CE scenarios. Through simulations, we illustrate that the DT scheme experiences the saturation state and therefore, cannot provide any desirable secrecy performance.

The rest of this paper is organized as follows. In Section II, we present our system model and the mmWave channel characteristics. In Section III, we focus our attention on the relay selection criterion and on the related OPA for both the NCE and CE scenarios. In Section IV, we calculate new expressions for the ESR and SOP, followed by our simulation results in Section V. Finally, we conclude in Section VI.

The following notations are used in this work: Bold uppercase (lowercase) letters represent matrices (vectors), while $|\cdot|$, $\|\cdot\|$, and $(\cdot)^{\mathrm{H}}$ stand for the absolute value, the Euclidean norm, and the conjugate transpose operator, respectively; $\mathbb{E}_{\mathrm{X}}\{\cdot\}$ represents the expectation over the random variable (r.v.) X; $pr_{\mathrm{X}}(\cdot)$ denotes the probability; $f_{\mathrm{X}}(\cdot)$ and $F_{\mathrm{X}}(\cdot)$ stand for the probability density function (PDF) and CDF, respectively; $x \sim CN(\mu, \sigma^2)$ and $y \sim \Gamma(N, \lambda)$ denote a circularly symmetric complex Gaussian r.v. with a mean of μ, and variance σ^2 and a gamma distribution with shape N and scale λ, respectively; $\mathbb{R}^2$ and $\mathbb{Z}^+$ denote two-dimensional real number domain and positive integer domain; $\mathrm{E_i}(x)$ is the exponential integral $\mathrm{E_i}(x) = -\int_{-\mathrm{x}}^{+\infty} \frac{e^{-\mathrm{t}}}{t} dt$ with $x > 0$ [42, Sec. (8.21)]; $[x]^+ = \max\{0, x\}$ and $L_{\mathrm{X}}(s)$ denotes the

[2] In [29], only one untrusted relay is present in the system model and no passive Eve exists in communication area. To extend the work in [29], the authors of [34] generalized the system model by considering both multiple relays and multiple passive Eves.

TABLE I: Comparison between our contributions with the state-of-the-art.

Contributions	This work	[7]	[10]	[12]	[13]	[16]	[17]	Our previous work [25]
Cooperation with Untrusted relay	✓							✓
Multiple relays with PPP distribution	✓		✓	✓				
Multiple Eves with PPP distribution	✓				✓	✓	✓	✓
Joint relay selection and power allocation strategy	✓							
NCE and CE scenarios	✓				✓		✓	✓
Blockage effects	✓	✓	✓	✓	✓	✓		

Laplace transform of X, i.e. $L_{\mathrm{X}}(s) = \mathbb{E}_{\mathrm{X}}\{e^{-\mathrm{sx}}\} = \mathbb{E}\{e^{-\mathrm{sx}}\}$.

II. System Model

We consider a cooperative mmWave network having a source and destination node, S and D, respectively, where both are equipped with an LSAA, respectively, for directional beamforming [4], [10]. We assume that several single-antenna-aided untrusted AF relays and passive single-antenna assisted Eves are distributed in an $\mathbb{R}^2$ space obeying homogeneous PPPs Φ_{r} and Φ_{e} with the densities of λ_{r} and λ_{e}, respectively. More especially, the relays are assumed to be trusted at the service level, but untrusted at the data level, implying that the relays assist in exchanging messages between S and D, but they have access to the data symbols, i.e., to the confidential information extracted from their received signals [27], [34]. For simplicity, we denote the r^{th} relay by R_{r} and the e^{th} Eve by E_{e}. The e^{th} Eve has a distance, r_{e}, from the source node. Furthermore, untrusted relays are employed for mitigating the end-to-end path-loss in our mmWave network [8]. The confidential information transmission from S to D can be intercepted by the untrusted relays and passive Eves, as shown in Fig. 1. However, due to the high path loss of mmWave carriers, we consider only the nodes that are placed within a circle centered at D as a reference point with a radius of r_{d} [10]. We also assume that all the passive Eves conceal their existence in the network and that all the nodes operate in half-duplex mode. We use the time division duplexing (TDD) protocol where the source acquires the downlink channel state information (CSI) of legitimate nodes by assuming that it is identical to the uplink CSI, which is perfectly estimated by exploiting the uplink training [17], [18], [43]. Then the CSI acquired is utilized for LSAA steering for achieving the maximum possible directionality gain [10], [43] at the intended legitimate nodes. Note that in our system model, the Eves are totally passive, hence, their instantaneous CSIs are generally unknown to the system.

Remark 1: In practice, it is not possible to acquire the CSI of passive Eves. In this situation, we take into account a scenario in which only the second order statistics of the Eves are accessible. This assumption is popularly explored in the literature, e.g. [28], [34].

We assume that the untrusted relays decode the received message individually, while the Eves may rely on one of the following scenarios for information extraction [34]:

1) **Non-colluding eavesdroppers scenario***:* Each passive Eve intercepts the received signal without sharing its wire-tapped signal with other Eves.

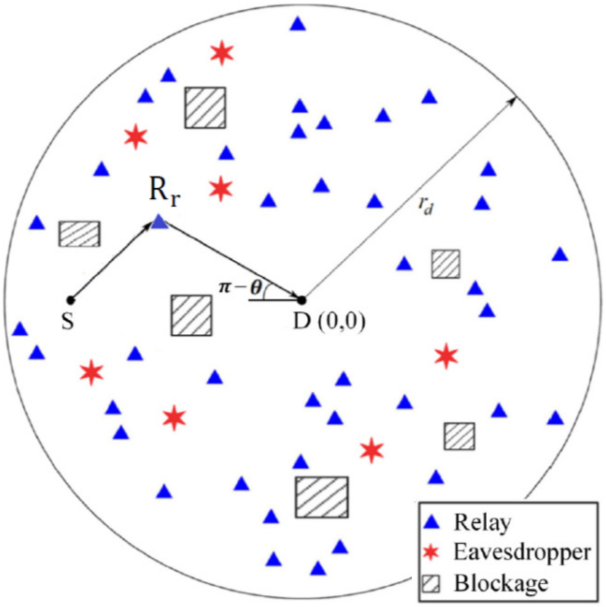

Fig. 1: Secure communication in a cooperative mmWave system model in the presence of multiple untrusted relays and multiple passive Eves. By adopting the destination-and-source-based cooperative jamming (DSBCJ) method, R_{r} is chosen to retransmit the source's confidential message.

2) **Colluding eavesdroppers scenario***:* In this scenario, all the passive Eves share their information for joint eavesdropping.

A. Directivity, Blockage, Path-Loss and Small-Scale Fading Models

As mentioned earlier, mmWave systems suffer from high propagation losses and it is important to consider the impact of blockage, which results in weak signal reception behind the obstacles at mmWave frequencies [6], [10]. To this end, highly directional beamforming techniques can be adopted for extending the transmission distance of mmWave systems. In the following, we describe our directional beamforming solution and our channel model including the blockage model, path loss model, and small-scale fading model.

1) Directional beamforming: The nodes adopt directional beamforming for compensating the signal attenuation caused by path loss. We model the directivity as a function of the main lobe with beamwidth θ_{i}, $i \in \{S, R_{\mathrm{r}}, D\}$, and the antenna has the gain of $G_{\mathrm{i}}^{\mathrm{M}}$ for $|\theta| \leq \theta_{\mathrm{i}}$, and $G_{\mathrm{i}}^{\mathrm{m}}$ in other directions [4],

[8], [13], i.e., the beam pattern is defined as

$$G_{\mathrm{i}}^{\mathrm{l}}(\theta)=\begin{cases}G_{\mathrm{i}}^{\mathrm{M}}, & \text{if } |\theta|\leq\theta_{\mathrm{i}}\\ G_{\mathrm{i}}^{\mathrm{m}}, & \text{if } |\theta|>\theta_{\mathrm{i}}\end{cases}, i\in\{S,R_{\mathrm{r}},D\},\ \ l\in\{m,M\}, \tag{1}$$

where $\theta\in[0,2\pi)$ is the angle of boresight direction which $G_{\mathrm{i}}^{\mathrm{M}}$ and $G_{\mathrm{i}}^{\mathrm{m}}$ represent the array gains of the main and side lobes. For simplicity, it is assumed that the antenna beams are perfectly centered on the relays by using initial beam training, employing the full pilot reuse procedure of [44], again to compensate for the mmWave path-loss in the spirit of [4], [10], [16]. Given the short wave-length of mmWave carriers, compact LSAAs can be used.

After the training phase, the beam patterns of the legitimate nodes are perfectly aligned with each other, but the Eves may be misaligned with S or R_{r} due to gleaming insufficient training. Accordingly, the array gains of the Eves may be expressed as

$$G_{\mathrm{ie}}^{\mathrm{lk}}=\begin{cases}G_{\mathrm{i}}^{\mathrm{M}}G_{\mathrm{e}}^{\mathrm{M}}, & \text{if } pr_{\mathrm{MM}}=\frac{\theta_{\mathrm{i}}\theta_{\mathrm{e}}}{(2\pi)^2}\\ G_{\mathrm{i}}^{\mathrm{M}}G_{\mathrm{e}}^{\mathrm{m}}, & \text{if } pr_{\mathrm{Mm}}=\frac{\theta_{\mathrm{i}}(2\pi-\theta_{\mathrm{e}})}{(2\pi)^2}\\ G_{\mathrm{i}}^{\mathrm{m}}G_{\mathrm{e}}^{\mathrm{M}}, & \text{if } pr_{\mathrm{mM}}=\frac{(2\pi-\theta_{\mathrm{i}})\theta_{\mathrm{e}}}{(2\pi)^2}\\ G_{\mathrm{i}}^{\mathrm{m}}G_{\mathrm{e}}^{\mathrm{m}}, & \text{if } pr_{\mathrm{mm}}=\frac{(2\pi-\theta_{\mathrm{i}})(2\pi-\theta_{\mathrm{e}})}{(2\pi)^2}\end{cases}, i\in\{S,R_{\mathrm{r}}\}, \tag{2}$$

where $pr_{\mathrm{lk}}(l,k\in\{M,m\})$ describes the probability that the antenna gain, $G_{\mathrm{i}}^{\mathrm{l}}G_{\mathrm{e}}^{\mathrm{k}}(l,k\in\{M,m\})$, is achieved. The variables $G_{\mathrm{e}}^{\mathrm{M}}$ and $G_{\mathrm{e}}^{\mathrm{m}}$ represent the array gains of the main- and side- lobes related to each Eve, respectively.

Remark 2: We note that, for simplicity, instead of displaying the notations E_{e} and R_{r} in the subscripts, we have used the lower case letters e and r, respectively. For example, instead of $G_{\mathrm{E_e}}^{\mathrm{M}}$ we use $G_{\mathrm{e}}^{\mathrm{M}}$.

2) Blockage modeling: The blockages are assumed to be in random directions and we opt for the fixed LoS probability model of [8], [9], [12], [45]. Applying this blockage model, a two-state statistical model is considered for each link, which can be either LoS or NLoS. Let the LoS area within a circular ball of radius r_{D} be centered around the reference point. Then if the LoS link is of length r, the probability of the link to be LoS is given by a constant probability p_{L} if $r<r_{\mathrm{D}}$ and 0, otherwise. Similarly, the NLoS probability is represented by p_{N}. Note that r and r_{D} depend on the propagation environment and may be derived from geographic data [9], [45].

3) Path-loss model: Similar to [6], the LoS and NLoS links have different path-loss exponents. For a given link with length r, the related path-loss is given by [6]

$$\begin{aligned}L(r)&=\begin{cases}C_{\mathrm{L}}r^{-\alpha_{\mathrm{L}}}, & \text{if the link is LoS}\\ C_{\mathrm{N}}r^{-\alpha_{\mathrm{N}}}, & \text{if the link is NLoS}\end{cases}\\ &=10^{-0.1\beta_{\mathrm{n}}}|a-b|^{-\alpha_{\mathrm{n}}}, n\in\{L,N\},\end{aligned} \tag{3}$$

where $|a-b|$ represents the distance between the points of a, b, $n\in\{L,N\}$, indicating the LoS and NLoS conditions, which α_{L} and α_{N} are the LoS as well as NLoS path-loss exponents, and $C_{\mathrm{L}}=10^{\frac{-\beta_{\mathrm{L}}}{10}}$, $C_{\mathrm{N}}=10^{\frac{-\beta_{\mathrm{N}}}{10}}$. Note that β_{L} and β_{N} represent the path-loss at a fixed small reference distance for the LoS and NLoS links, respectively, and they are frequency dependent constant parameters [6], [45]. We use this interpretation in our analysis. Typical values of α_{n} and β_{n}, $n\in\{L,N\}$, are available in [6, Table I].

4) Small-scale fading model: In this paper, in contrast to [6], [8], [12], [46], we aim for capturing the main properties of generalized propagation environments. To this end, it is assumed that the small-scale fading of each link obeys an independent Nakagami distribution. We note that the Nakagami-*m* distribution is regarded as a general formula for modeling the random variations of the signal amplitude, when propagating in a wireless medium, including mmWave channels [10], [13], [16], [44]. Following the geometric channel model of [44], the channel $\mathbf{h}_{\mathrm{ij}}$ can be formulated as

$$\mathbf{h}_{\mathrm{ij}}=\sqrt{L(r_{\mathrm{ij}})}\beta_{\mathrm{ij}}\mathbf{a}_{\mathrm{ij}}(\theta), i,j\in\{S,R_{\mathrm{r}},D,E_{\mathrm{e}}\}, \tag{4}$$

where $L(r_{\mathrm{ij}})$ is the path-loss between node i and node j as defined in (3). The small-scale fading is modeled by the complex coefficient β_{ij}. Furthermore, the small-scale channel gain between S and R_{r}, S and E_{e}, R_{r} and D, and R_{r} and Eve are represented by $|\beta_{\mathrm{sr}}|^2$, $|\beta_{\mathrm{se}}|^2$, $|\beta_{\mathrm{rd}}|^2$, and $|\beta_{\mathrm{re}}|^2$, respectively. Accordingly, for Nakagami fading, the r.v.s $|\beta_{\mathrm{sr}}|^2$, $|\beta_{\mathrm{se}}|^2$, $|\beta_{\mathrm{rd}}|^2$, and $|\beta_{\mathrm{re}}|^2$, obey the normalized Gamma distribution [7], [13], [17]. For a LoS link, the small-scale channel gain follows $|\beta_{\mathrm{sr}}|^2\sim\Gamma(N_{\mathrm{L}},1)$, and for a NLoS link we have $|\beta_{\mathrm{sr}}|^2\sim\Gamma(N_{\mathrm{N}},1)$. The notation $N_{\mathrm{L}}(N_{\mathrm{N}})$ is used to state the fading parameter of the LoS (NLoS) channel. For simplicity, we assume that both N_{L} and N_{N} are positive integers. The rest of the r.v.s can be similarly defined. The angle θ denotes the angle of departure/arrival (AoD/AoA) at the transmitter/receiver. We assume that θ is uniformly distributed over $[0,2\pi]$, and $\mathbf{a}_{\mathrm{ij}}(\theta)$ is the array response vector at the transmitter/receiver, for the angle θ. Finally, we mention that for the passive Eves, only the distribution of $|\beta_{\mathrm{se}}|^2$, $E_{\mathrm{e}}\in\Phi_{\mathrm{e}}$ is known for the system.

B. SNR Modeling

Recent research on mmWave systems [6], [8], [45], and [46] illustrates that mmWave communications in urban environments is generally noise limited, which is different from the conventional sub-6 GHz cellular networks. This is because in the presence of blockages, the signals arriving from unintended transmitters are nearly negligible. In these densely blocked zones, the SNR can be adapted for clearly approximating the received signal-to-interference-and-noise ratio (SINR) in directional mmWave systems. Therefore, the interference received at the destination may be ignored. Assuming that the r^{th} relay as the selected one for forwarding the signal, the SNR of the node i- to-node j link is formulated as

$$\gamma_{\mathrm{ij}}^{\mathrm{lk}}=\rho G_{\mathrm{i}}^{\mathrm{l}}G_{\mathrm{j}}^{\mathrm{k}}L(r_{\mathrm{ij}})|\beta_{\mathrm{ij}}|^2, l,k\in\{m,M\}, \tag{5}$$

where γ_{ij} incorporates the impact of path-loss, blockage, and beamforming gain at the transmitter and receiver. Additionally, we have defined $\rho=\frac{P}{N_0}$, where N_0 is the noise power at receiving nodes.

The assumptions and definitions made in this paper are as follows:

- The TDD channels obey the reciprocity, i.e., $\mathbf{h}_{\mathrm{ij}}=\mathbf{h}_{\mathrm{ji}}$ [32], [33], and [34].

- The additive white Gaussian noise (AWGN) at each receiver, $n_{\rm m}, m \in \{R_{\rm r}, E_{\rm e}, D\}$, is a zero-mean complex Gaussian r.v. with variance N_0.
- Similar to [23], the total transmit power during the first phase is limited by $2P$ and for the second phase is limited by P.
- $\gamma_{\rm sr} = \rho G^{\rm M}_{\rm s,S} G^{\rm M}_{\rm r} L(r_{\rm sr})|\beta_{\rm sr}|^2$, $\gamma_{\rm rd} = \rho G^{\rm M}_{\rm D} G^{\rm M}_{\rm r} L(r_{\rm rd})|\beta_{\rm rd}|^2 = \rho G^{\rm MM}_{\rm Dr} L(r_{\rm rd})|\beta_{\rm rd}|^2$, $\gamma^{\rm lk}_{\rm re} = \rho G^{\rm l}_{\rm r} G^{\rm k}_{\rm e} L(r_{\rm re})|\beta_{\rm re}|^2$, $\gamma^{\rm lk}_{\rm de} = \rho G^{\rm l}_{\rm D} G^{\rm k}_{\rm e} L(r_{\rm de})|\beta_{\rm de}|^2$.
- $\gamma^{\rm lk}_{\rm se,S} = \rho G^{\rm l}_{\rm s,S} G^{\rm k}_{\rm e} L(r_{\rm se})|\beta_{\rm se}\mathbf{a}^{\rm H}_{\rm se}(\phi)\mathbf{a}_{\rm sr}(\theta)|^2$, and $\gamma^{\rm lk}_{\rm se,A} = \rho G^{\rm l}_{\rm s,A} G^{\rm k}_{\rm e} L(r_{\rm se})\|\beta_{\rm se}\mathbf{a}^{\rm H}_{\rm se}(\phi)\mathbf{a}_{\rm se}(\phi)\|^2$, where under the Nakagami fading distribution, the new r.v.s., $u = |\beta_{\rm se}\mathbf{a}^{\rm H}_{\rm se}(\phi)\mathbf{a}_{\rm sr}(\theta)|^2$ and $x_{\rm e} = \|\beta_{\rm se}\mathbf{a}^{\rm H}_{\rm se}(\phi)\mathbf{a}_{\rm se}(\phi)\|^2$ have an exponential distribution [17], [43], [47] and normalized Gamma distribution, respectively. Moreover, we have $G^{\rm lk}_{\rm se,S} = G^{\rm l}_{\rm s,S} G^{\rm k}_{\rm e}$, and $G^{\rm lk}_{\rm se,A} = G^{\rm l}_{\rm s,A} G^{\rm k}_{\rm e}$, where $l, k \in \{m, M\}$. We note that $\gamma^{\rm lk}_{\rm se,S}$ and $\gamma^{\rm lk}_{\rm se,A}$ are the message signal and the AN received by each Eve, respectively, and $G^{\rm l}_{\rm s,S}$ and $G^{\rm l}_{\rm s,A}$ describe the main/side-lobe gains of the signal and the AN, respectively.

C. Destination and Source Based Cooperative Jamming (DSBCJ)

In this paper, we propose a DSBCJ method relaying on AN aided beamforming employed for confusing the untrusted relays and passive Eves, where a broadcast phase and a relaying phase is used. During the broadcasting phase, S transmits its message at a power of λP and concurrently radiates AN to confuse the Eves at a power of $(1-\lambda)P$, where $\lambda \in (0,1]$. Simultaneously, the destination radiates another type of AN at power ηP, where $\eta \in [0,1]$ is the power allocation factor of D. The AN generated by the source is transmitted in the null space of the selected relay's channel to avoid contaminating the desired channel [1], [17], [25], and [26]. This method is particularly beneficial, when the Eve's instantaneous CSI is unknown. During the second phase of relaying, the chosen relay forwards the received message at a power P. Eventually, D extracts the source message by subtracting the self-interference imposed by the AN.

Let us denote $x_{\rm s}$, $\mathbf{x}_{\rm j_s}$, and $x_{\rm j_d}$ as the message signal, the jamming signal vector of S, and the jamming signal of D respectively, where $\mathbb{E}\{|x_{\rm n}|^2\} = 1$, $n \in \{S, j_{\rm d}\}$, and $\mathbb{E}\{\|\mathbf{x}_{j_{\rm s}}\|^2\} = 1$. Based on the proposed DSBCJ method, the message received by the relay after applying beamforming can be described as

$$\begin{aligned} y_{\rm r} = {} & \sqrt{\lambda P}\sqrt{L(r_{\rm sr})}\beta_{\rm sr}\mathbf{a}^{\rm H}_{\rm sr}(\theta)\mathbf{W}_{\rm s}x_{\rm s} \\ & + \sqrt{\eta P}\sqrt{L(r_{\rm rd})}\beta_{\rm rd}\mathbf{a}^{\rm H}_{\rm rd}(\varphi)\mathbf{W}_{\rm d}x_{\rm j_d} + n_{\rm r}, \end{aligned} \tag{6}$$

where $R_{\rm r} \in \Phi_{\rm r}$ is the selected relay, which $\mathbf{W}_{\rm s} = \sqrt{G^{\rm M}_{\rm s,S} G^{\rm M}_{\rm r}}\mathbf{a}_{\rm sr}(\theta)$, and $\mathbf{W}_{\rm d} = \sqrt{G^{\rm M}_{\rm D} G^{M}_{\rm r}}\mathbf{a}_{\rm rd}(\varphi)$. We mention that because the AN injected by S is in the null-space channel of the selected relay link, the AN is not received at the selected relay.

The signal received at the malicious node $E_{\rm e}$, ($E_{\rm e} \in \Phi_{\rm e}$), during the first phase can be expressed as

$$\begin{aligned} y^{(1)}_{\rm e,l,k} = {} & \sqrt{\lambda P}\sqrt{L(r_{\rm se})}\beta_{\rm se}\mathbf{a}^{\rm H}_{\rm se}(\phi)\mathbf{W}_{\rm s}x_{\rm s} \\ & + \sqrt{(1-\lambda)P}\sqrt{L(r_{\rm se})}\beta_{\rm se}\mathbf{a}^{\rm H}_{\rm se}(\phi)\mathbf{W}_2\mathbf{x}_{\rm j_s} + n_{\rm e}, \end{aligned} \tag{7}$$

where $\mathbf{W}_2 = \sqrt{G^{\rm lk}_{\rm se,A}}\mathbf{a}_{\rm se}(\phi)$ as defined before. Recall that to degrade the received signal quality at the Eves, AN is injected by S in the null- space of the desired channel between S and the selected relay. The AN beamforming matrix $\mathbf{W}_2$ was proposed in [17]. We note that for simplifying our analysis, we ignore the AN generated by D which is received by the Eves. Note that this assumption is beneficial from the secrecy perspective due to canceling the received AN interference at the passive Eve. During the relaying phase, the relay forwards its received message by adopting the amplification factor $G = \sqrt{\frac{P}{\lambda P G^{\rm M}_{\rm s,S} G^{\rm M}_{\rm r} L(r_{\rm sr})|\beta_{\rm sr}|^2 + \eta P G^{\rm M}_{\rm D} G^{\rm M}_{\rm r} L(r_{\rm rd})|\beta_{\rm rd}|^2 + \sigma^2_{\rm n}}}$ and broadcasts the message as $x_{\rm r} = G y_{\rm r}$. During this phase, all the eavesdropping nodes receive the signal forwarded by the relay. As such, the signal received by the eavesdropping node e is expressed as

$$y^{(2)}_{\rm e,l,k} = G\sqrt{G^{\rm l}_{\rm r} G^{\rm k}_{\rm e} L(r_{\rm rd})}\beta_{\rm re} y_{\rm r} + n_{\rm e}. \tag{8}$$

Additionally, at the destination, after implementing self-interference cancellation, we obtain

$$\begin{aligned} \mathbf{y}_{\rm D} = {} & G\sqrt{\lambda P}\sqrt{G^{\rm M}_{\rm s,S} G^{\rm M}_{\rm r} L(r_{\rm sr})}\beta_{\rm sr}\sqrt{G^{\rm M}_{\rm D} G^{\rm M}_{\rm r} L(r_{\rm rd})}\beta_{\rm rd}\mathbf{a}_{\rm rd}x_{\rm s} \\ & + G\sqrt{G^{\rm M}_{\rm D} G^{\rm M}_{\rm r} L(r_{\rm rd})}\beta_{\rm rd} n_{\rm r}\mathbf{a}_{\rm rd} + \mathbf{n}_{\rm D}. \end{aligned} \tag{9}$$

Based on (6) and (7), the SINRs at $R_{\rm r}$ and at $E_{\rm e}$ during the first phase are formulated respectively, by

$$\gamma_{\rm r} = \frac{\lambda\gamma_{\rm sr}}{\eta\gamma_{\rm rd} + 1}, \tag{10}$$

$$\gamma^{(1)}_{\rm e,l,k} = \frac{\lambda\gamma^{\rm lk}_{\rm se,S}}{(1-\lambda)\gamma^{\rm lk}_{\rm se,A} + 1}, l, k \in \{M, m\}. \tag{11}$$

Up on substituting (6) and the above mentioned relay gain into (8), the SINR at Eve during the second phase is given by

$$\gamma^{(2)}_{\rm e,l,k} = \frac{\lambda\gamma_{\rm sr}\gamma^{\rm lk}_{\rm re}}{\lambda\gamma_{\rm sr} + (\eta\gamma_{\rm rd})\left(\gamma^{\rm lk}_{\rm re} + 1\right)}, l, k \in \{M, m\}. \tag{12}$$

Additionally, by invoking (9), the end-to-end SNR $\gamma_{\rm D,r}$ is expressed as

$$\gamma_{\rm D,r} = \frac{\lambda\gamma_{\rm sr}\gamma_{\rm rd}}{\lambda\gamma_{\rm sr} + (1+\eta)\gamma_{\rm rd} + 1}. \tag{13}$$

The instantaneous ESR is expressed as $R^{\rm r}_{\rm s} = \frac{1}{2}[\log_2(1+\gamma_{\rm D,r}) - \log_2(1+\gamma_{\rm E,r})]^+$ [27], where $\gamma_{\rm E,r}$ is the equivalent SINR at the Eves, depending on the scenario. For the scenario of NCE, this leakage is formulated as [34]

$$\gamma^{NCE}_{\rm E,r} = \max_{E_{\rm e}\in\Phi_{\rm e}, R_{\rm r}\in\Phi_{\rm r}, E_{\rm e}\neq R_{\rm r}} \{\gamma_{\rm r}, \gamma^{(1)}_{\rm e}, \gamma^{(2)}_{\rm e}\}. \tag{14}$$

Remark 3: When a relay is chosen for retransmitting the message signal, the rest of the relays may act as Eves in the second phase of message transmission.

For the scenario of CE, the quantity of message leakage to

Eves is given by [34]

$$\begin{aligned}\gamma_{\mathrm{E,r}}^{CE} = \max\{&\underbrace{\max_{E_{\mathrm{e}}\in\Phi_{\mathrm{e}},R_{\mathrm{r}}\in\Phi_{\mathrm{r}},E_{\mathrm{e}}\neq R_{\mathrm{r}}}(\gamma_{\mathrm{r}},\gamma_{\mathrm{e}}^{(1)},\gamma_{\mathrm{e}}^{(2)})}_{\text{Message leakage 1}}\\ &,\underbrace{\sum_{E_{\mathrm{e}}\in\Phi_{\mathrm{e}}}(\gamma_{\mathrm{e}}^{(1)}+\gamma_{\mathrm{e}}^{(2)})}_{\text{Message leakage 2}}\},\end{aligned} \tag{15}$$

where message leakages 1 and 2 represent the leakages to the untrusted relay and passive Eves, respectively.

III. Joint Relay Selection and Power Allocation

Again, the LSAA S transmits its message via a specifically chosen untrusted relay to the multi-antenna D. Let r^* represents the index of the best selected relay. Hence, influenced by the LSAA of [34], our power allocation technique proposed for both NCE and CE scenarios is as follows

$$(\mu^*,\lambda^*) = \arg\max_{0\leq\mu\leq 1,\ 0<\lambda\leq 1} R_{\mathrm{s}}^{\mathrm{r}}. \tag{16}$$

Then the optimal relay that maximizes the instantaneous secrecy rate is chosen according to

$$r^* = \arg\max_{R_{\mathrm{r}}\in\Phi_{\mathrm{r}}} R_{\mathrm{s}}^{\mathrm{r}}. \tag{17}$$

The relay selection metric of (17) requires the CSI of both hops and of all inter-relay links. Hence, it is challenging to implement (17) in practice, especially when a large number of relays are present in the network. To address this challenge, and inspired by using a LSAA at S, we utilize a simple relay selection metric for both the NCE and CE scenarios.

A. NCE Scenario

For this scenario, according to (14), we have to find the maximum SINR at the eavesdropping nodes. Since we use a LSAA at S, upon applying the Cauchy-Schwarz inequality, $\gamma_{\mathrm{e,l,k}}^{(1)}$ in (11) is upper bounded by γ_{r^*} [25]. Now, we show that $\gamma_{\mathrm{e}}^{(1)}$ is also upper bounded by

$$\begin{aligned}\gamma_{\mathrm{e}}^{(1)} &= \sum_{l,k\in\{M,m\}} \frac{\lambda_{\mathrm{NCE}}\gamma_{\mathrm{se,S}}^{\mathrm{lk}}}{(1-\lambda_{\mathrm{NCE}})\gamma_{\mathrm{se,A}}^{\mathrm{lk}}+\eta_{\mathrm{NCE}}\gamma_{\mathrm{de,A}}+1}pr_{\mathrm{lk}}\\ &< \sum_{l,k\in\{M,m\}} \gamma_{\mathrm{r}^*}pr_{\mathrm{lk}} = \gamma_{\mathrm{r}^*},\end{aligned} \tag{18}$$

where λ_{NCE} is the power allocation factor of the NCE scenario. Additionally, by taking into account (12) and (18) as well as by referring to [25], $\gamma_{\mathrm{e}}^{(2)}$ in (14) and (15) can be upper bounded by

$$\gamma_{\mathrm{e}}^{(2)} < \gamma_{\mathrm{r}^*}. \tag{19}$$

As such, the instantaneous secrecy rate which is defined in Section II-C, can be reformulated as

$$R_{\mathrm{s}}^{\mathrm{r}^*}(\mu^*,\lambda^*) = \frac{1}{2}\log_2\left[\frac{1+\gamma_{\mathrm{D,r}^*}}{1+\gamma_{\mathrm{r}^*}}\right]. \tag{20}$$

If we have $\Phi = \frac{1+\gamma_{\mathrm{D,r}}}{1+\gamma_{\mathrm{r}}}|_{\lambda_{\mathrm{NCE}}=0} \geq 1$, then $\Phi(\lambda_{\mathrm{NCE}}^*) \geq 1$, where λ_{NCE}^* is the OPA factor of the NCE scenario. Therefore, in (20) the operator $[\cdot]^+$ is omitted.

Proposition 1: The function $\Phi = \frac{1+\gamma_{\mathrm{D,r}^*}}{1+\gamma_{\mathrm{r}^*}}$ monotonically grows with η_{NCE} in the domain of $\eta_{\mathrm{NCE}} \in [0,1]$ and the maximum Φ is achievable at $\eta_{\mathrm{NCE}} = 1$. Then in the following, we set $\eta_{\mathrm{NCE}} = 1$ [25].

Remark 4: In more general cooperative networks in which there are both trusted and untrusted relays, if the selected relay is untrusted, the network can implement the DSBCJ method and the D transmits with its full power. By contrast, when the selected relay is a trusted one, the destination does not have to transmit AN, and thus, the network can save part of its power. We note that the same node should distinguish between the trusted relays and the untrusted ones with the aid of the physical layer authentication techniques [34].

Proposition 2: For an LSAA at S, the function $\Phi(\lambda_{\mathrm{NCE}})$ is a quasi-concave function of λ_{NCE} in the feasible set and the optimal solution is given by

$$\lambda_{\mathrm{NCE}}^* = \sqrt{2}v, v = \frac{\gamma_{\mathrm{r}^*\mathrm{d}}}{\gamma_{\mathrm{sr}^*}}, \tag{21}$$

which can be obtained using a straightforward approach similar to [25]. By using the result in ***Proposition 1*** and substituting (18) and (19) into (14), and substituting (21) into (13), then upon applying an LSAA at both S and D, i.e., $\gamma_{\mathrm{sr}^*} \gg \gamma_{\mathrm{r}^*\mathrm{d}} \gg 1$, we obtain

$$\gamma_{\mathrm{D,r}^*}^{\mathrm{NCE}} = \frac{\gamma_{\mathrm{r}^*\mathrm{d}}}{1+\sqrt{2}}, \gamma_{\mathrm{E,r}^*}^{\mathrm{NCE}} \approx \gamma_{\mathrm{r}^*}. \tag{22}$$

Then, by exploiting (22), the instantaneous secrecy rate in (20) is given by

$$R_{\mathrm{s}}^{\mathrm{r}^*} = \frac{1}{2}\log_2\left[\frac{1+\frac{\gamma_{\mathrm{r}^*\mathrm{d}}}{1+\sqrt{2}}}{1+\sqrt{2}}\right]. \tag{23}$$

The interesting result in (23) suggests that the instantaneous secrecy rate is only related to the transmit SNR and to the relay-to-destination link. As a consequence, the sophisticated relay selection criterion in (17) can be simplified to

$$r^* = \arg\max_{R_{\mathrm{r}}\in\Phi_{\mathrm{r}}} \gamma_{\mathrm{D,r}}^{\mathrm{NCE}} = \arg\max_{R_{\mathrm{r}}\in\Phi_{\mathrm{r}}} \|\mathbf{h}_{\mathrm{rd}}\|^2. \tag{24}$$

The above relay selection criterion in (24) only depends on the relays-to-destination channel quality, hence it has a low complexity. It is also important to note that for the NCE scenario we have highlighted in (18) and (19) that the selected untrusted relay obtains the most information, hence there is no need for acquiring the CSI of the passive Eves for network design and optimization.

B. CE Scenario

For CE, the passive Eves cooperate for acquiring the message signal based on the MRC technique. To counteract this attain, more power should be dedicated to S for distracting the cooperation of the Eves and less power should be assigned to forwarding the message signal, compared to λ_{NCE}^* in (21). Based on this, we have $\lambda_{\mathrm{CE}}^* < \lambda_{\mathrm{NCE}}^* \ll 1$, where λ_{CE}^* represent the OPA factor of the CE scenario. As such, $\gamma_{\mathrm{e}}^{(2)}$ may be approximated as

$$\gamma_{\mathrm{e}}^{(2)} \approx \frac{\lambda_{\mathrm{CE}}\gamma_{\mathrm{sr}^*}}{\eta_{\mathrm{CE}}\gamma_{\mathrm{r}^*\mathrm{d}}+1} = \gamma_{\mathrm{r}^*}. \tag{25}$$

Eq. (25) can be proved by following a similar approach to that when driving (18). The observation in (25) represents that the quantity of message leakage to the Eves in the second phase of transmission is approximately equal to the quantity of the message leaked to the selected untrusted relay in the first phase. Based on this statement and on the fact that the signal received by the Eves in the second phase is a degraded copy of the signal forwarded by the selected relay, $\gamma^{CE}_{\mathrm{E,r*}}$ in (15) can be expressed as

$$\gamma^{CE}_{\mathrm{E,r^*}} = \gamma_{\mathrm{r^*}} + \sum_{l,k\in\{M,m\}} \sum_{e\in\Phi_{\mathrm{e}}} \gamma^{(1)}_{\mathrm{e,l,k}} pr_{\mathrm{lk}}. \tag{26}$$

Proposition 3: For the CE scenario, the function Φ monotonically increases with η_{CE} in $\eta_{\mathrm{CE}} \in [0,1]$, and the maximum of Φ is achieved at $\eta_{\mathrm{CE}} = 1$. Accordingly, in the following, we set $\eta_{\mathrm{CE}} = 1$. This proposition can be proved following similar arguments to those in [25].

For the sake of tractability, according to ***Proposition 3*** and to the fact that $\lambda_{\mathrm{CE}} \ll 1$, $\gamma_{\mathrm{r^*}}$ and $\gamma^{(1)}_{\mathrm{e}}$ in (10) and (11) can be rewritten as

$$\gamma_{\mathrm{r^*}} = \frac{\lambda_{\mathrm{CE}}\gamma_{\mathrm{sr^*}}}{(1-\lambda_{\mathrm{CE}})(\gamma_{\mathrm{r^*d+1}})}, \tag{27}$$

$$\gamma^{(1)}_{\mathrm{e,l,k}} = \left(\frac{\lambda_{\mathrm{CE}}}{1-\lambda_{\mathrm{CE}}}\right)\left(\frac{\gamma^{\mathrm{lk}}_{\mathrm{se,S}}}{\gamma^{\mathrm{lk}}_{\mathrm{se,A}} + \gamma_{\mathrm{de,A}} + 1}\right). \tag{28}$$

Then, upon substituting (27) into (26), we have

$$\gamma^{CE}_{\mathrm{E,r*}} = \frac{\lambda_{\mathrm{CE}}\Delta}{1-\lambda_{\mathrm{CE}}}, \tag{29}$$

where $\Delta = \frac{\gamma_{\mathrm{sr^*}}}{\gamma_{\mathrm{r^*d}}+1} + \sum_{\mathrm{l,k}\in\{\mathrm{M,m}\}} \sum_{\mathrm{e}\in\Phi_{\mathrm{e}}} \frac{\gamma^{lk}_{\mathrm{se,S}}}{\gamma^{lk}_{\mathrm{se,A}}+\gamma_{\mathrm{de,A}}+1}$.

Similar to the approach in Proposition 2, the OPA factor of the CE scenario is calculated as

$$\lambda^{*}_{\mathrm{CE}} = \sqrt{\frac{2v}{\Delta}}, v = \frac{\gamma_{\mathrm{r^*d}}}{\gamma_{\mathrm{sr^*}}}. \tag{30}$$

We can deduce from (30) that as the number of Eves or the density λ_{e} grows, much of the total power is allocated to the source for jamming. By substituting (30) into (13) and (29), we arrive at

$$\gamma^{\mathrm{CE}}_{\mathrm{D,r^*}} = \frac{\gamma_{\mathrm{r^*d}}}{1+\sqrt{2v\Delta}}, \gamma^{\mathrm{CE}}_{\mathrm{E,r^*}} = \sqrt{2v\Delta}. \tag{31}$$

By substituting $\gamma^{\mathrm{CE}}_{\mathrm{D,r^*}}$ and $\gamma^{CE}_{\mathrm{E,r^*}}$ in (31) into (20), the instantaneous secrecy rate is calculated.

We define $\xi = \sum_{\mathrm{l,k}\in\{\mathrm{M,m}\}} \sum_{\mathrm{e}\in\Phi_{\mathrm{e}}} \frac{\gamma^{\mathrm{lk}}_{\mathrm{se,S}}}{\gamma^{\mathrm{lk}}_{\mathrm{se,A}}+\gamma_{\mathrm{de,A}}+1}$. From (29), it may be readily shown that $\Delta \approx \frac{1}{v} + \xi$. Then by substituting this into (31), we arrive at

$$\gamma^{\mathrm{CE}}_{\mathrm{D,r^*}} = \frac{\gamma_{\mathrm{r^*d}}}{1+\sqrt{2(1+v\xi)}}, \gamma^{\mathrm{CE}}_{\mathrm{E,r^*}} = \sqrt{2(1+v\xi)}. \tag{32}$$

We can conclude from (32) that $\gamma^{\mathrm{CE}}_{\mathrm{E,r*}}$ grows upon increasing the density of Eves. Upon comparing (22) for NCE and (32) for CE, we may introduce the new parameter $C = v\xi$ for unifying the performance study of NCE and CE scenarios. According to this definition, we have

$$\gamma_{\mathrm{D,r^*}} = \frac{\gamma_{\mathrm{r^*d}}}{1+\sqrt{2(1+C)}}, \gamma_{\mathrm{E,r^*}} = I_{\mathrm{e}} = \sqrt{2(1+C)}, \tag{33}$$

where $C = 0$ for NCE and $C = v\xi$ for CE.

we should mention that the solution proposed for NCE in Eq. (24) is optimal. However, for the CE scenario, a suboptimal solution is proposed. This is because the optimal solution for CE becomes excessively complex and thus, the computational complexity and the spectral overhead imposed on the network will be very high. In this case, the CSIs of all links - including that of the relay to source, relay to destination links and the CSIs of all Eves - are necessary. By contrast, in the proposed design, only the CSI of the second hop is required. Therefore, the required bandwidth, power consumption, and the delay of communication are remarkably reduced.

Let us now use a simple relay selection metric for both NCE and CE scenarios. For a given realization of a PPP associated with $\mathcal{R}$ relay nodes, the SINR at D used for our proposed relay selection criterion in either NCE or CE is obtained as

$$\gamma_{\mathrm{D,r^*}} = \begin{cases} \max\{\gamma_{\mathrm{rd_1}}, \gamma_{\mathrm{rd_2}}, ..., \gamma_{\mathrm{rd}_{\mathcal{R}}}\}, & \text{if } \mathcal{R} \neq 0 \\ 0, & \text{if } \mathcal{R} = 0 \end{cases}, \tag{34}$$

where r^* denotes the selected relay. For simplicity, we replace $\gamma_{\mathrm{rd_i}}$ by γ_{z} to represent an arbitrary node in Φ_{r}. From the features of PPP, given $\mathcal{R} > 0$, the location of z follows a uniform distribution in the space, and γ_{z}s are independent r.v.s. Additionally, we replace $\gamma_{\mathrm{D,r^*}}$ by γ_{best}. Accordingly, regarding (34), we can calculate $F_{\gamma_{\mathrm{best}}}(x)$ as

$$\begin{aligned} F_{\gamma_{\mathrm{best}}}(x) &= \Pr(\gamma_{\mathrm{best}} \leq x) \\ &= \Pr(\max\{\gamma_{\mathrm{rd_1}}, \gamma_{\mathrm{rd_2}}, ..., \gamma_{\mathrm{rd}_{\mathcal{R}}}\} \leq x) \\ &= \mathbb{E}_{\Phi_{\mathrm{r}}} \prod_{r\in\Phi_{\mathrm{r}}} \Pr(\gamma_{\mathrm{rd}} \leq x). \end{aligned} \tag{35}$$

Since that the optimal relay selection criterion related to the maximum achievable ESR suffers from excessive implementation overhead, we propose to use the simple suboptimal relay selection criterion of (34). Remarkably, since the second hop has a major effect on the SNR at D, the relay selection criterion in (34) can be regarded as a near optimal one.

IV. Performance Analysis

In this section, we present new expressions for the ESR and SOP for both the proposed DSBCJ and the DT schemes. The analysis include both the NCE and CE scenarios.

A. *Ergodic Secrecy Rate*

The ESR is a popular secrecy metric, which given by the average of the instantaneous rate difference between the legitimate and the wiretap channel. In this section, we first present a new expression for the ESR of our system model in the presence of a single untrusted relay. Then we extend the results to multiple untrusted relays. Finally, we derive new expressions for the ESR of DT scenario.

A . 1. DSBCJ Scheme:

***Lemma 1**:* Let us assume that X, I_{l}, Y, and I_{e} are independent r.v.s, Therefore, we have

$$\mathbb{E}\left\{\ln\left(1+\frac{X}{I_{\mathrm{l}}+1}\right)\right\}-\mathbb{E}\left\{\ln\left(1+\frac{Y}{I_{\mathrm{e}}+1}\right)\right\}\\ =\int_0^{+\infty}[L_{\mathrm{I_l}}(s)(1-L_{\mathrm{X}}(s))]\frac{e^{-s}}{s}ds\\ -\int_0^{+\infty}[L_{\mathrm{I_e}}(s)(1-L_{\mathrm{Y}}(s))]\frac{e^{-s}}{s}ds, \tag{36}$$

where $L_{\mathrm{X}}(s)$, $L_{\mathrm{I_l}}(s)$, $L_{\mathrm{Y}}(s)$, and $L_{\mathrm{I_e}}(s)$ denotes the Laplace transform of X, I_{l}, Y, I_{e}, respectively.

Proof: Please refer to [48] for a detailed proof.

By using ***Lemma 1***, the ESR of DSBCJ can be written as

$$\bar{R}_{\mathrm{s}}=\frac{1}{2\ln 2}\int_0^{+\infty}[L_{\mathrm{I_e}}(s)\left(2-L_{\mathrm{Y}}(s)\right)-1]\frac{e^{-s}}{s}ds, \tag{37}$$

where we have $I_{\mathrm{e}}=\sqrt{2(1+C)}$ and for a single untrusted relay $Y=\gamma_{\mathrm{rd}}$. Now, we derive the Laplace transform of I_{e} as

$$L_{\mathrm{I_e}}(s)=\mathbb{E}\left\{e^{-sI_{\mathrm{e}}}\right\}=\mathbb{E}\left\{e^{-s\sqrt{2(1+C)}}\right\}\overset{(a)}{\geq}e^{-s\sqrt{2(1+\mathbb{E}\{C\})}}\\ \overset{(b)}{=}e^{-s\sqrt{2(1+\mathbb{E}\{v\}\mathbb{E}\{\xi\})}}. \tag{38}$$

Since $\psi=e^{-s\sqrt{2(1+C)}}$ is convex on C (one can readily find that $\frac{\partial^2\psi}{\partial C^2}>0$), therefore, based on Jensen's inequality, we have (a). In (38), (b) follows from the fact that the two-hops are independent. To derive (b), we should calculate $\mathbb{E}\{v\}$ and $\mathbb{E}\{\xi\}$. Let us now consider the case of numerous relays. Based on the laws of large numbers and on the total expectation theorem, $\frac{\gamma_{\mathrm{r^*d}}}{\gamma_{\mathrm{sr^*}}}$ can be written as follows upon adopting the well-known minimum mean square error (MMSE) estimator along with the proposed relay selection criterion of (24), and with the LSAA at S, we arrive at

$$\frac{\gamma_{\mathrm{r^*d}}}{\gamma_{\mathrm{sr^*}}}\approx\mathbb{E}_{\Phi_{\mathrm{r}},\mathrm{h}}\{\frac{\gamma_{\mathrm{r^*d}}}{\gamma_{\mathrm{sr^*}}}\}\overset{(a)}{=}\mathbb{E}_{\Phi_{\mathrm{r}}}\{\mathbb{E}_{\mathrm{h}}\{\gamma_{\mathrm{r^*d}}\}\mathbb{E}_{\mathrm{h}}\{\frac{1}{\gamma_{\mathrm{sr^*}}}\}\}\\ \overset{(b)}{=}\mathbb{E}_{\phi_{\mathrm{r}}}\\ \{\sum_{n\in\{L,N\}}\mathbb{E}_{\mathrm{h}}\{\gamma_{\mathrm{r^*d}}|\mathbf{h}_{\mathrm{r^*d}},n\}p_{\mathrm{n}}\sum_{m\in\{L,N\}}\mathbb{E}_{\mathrm{h}}\{\frac{1}{\gamma_{\mathrm{sr^*}}}|\mathbf{h}_{\mathrm{sr^*}},m\}p_{\mathrm{m}}\}\\ \overset{(c)}{=}\frac{G_{\mathrm{r^*d}}}{G_{\mathrm{sr^*}}}\sum_{n\in\{L,N\}}\sum_{m\in\{L,N\}}\frac{C_{\mathrm{n}}}{C_{\mathrm{m}}}\frac{N_{\mathrm{n}}}{N_{\mathrm{m}-1}}\mathbb{E}_{\Phi_{\mathrm{r}}}\{\frac{r_{\mathrm{rd}}^{-\alpha_{\mathrm{n}}}}{r_{\mathrm{sr}}^{-\alpha_{\mathrm{m}}}}\}p_{\mathrm{n}}p_{\mathrm{m}}, \tag{39}$$

where (a) follows from the fact that the two-hops are independent, (b) is obtained according to the law of total probability, and (c) follows from evaluating $\sum_{n\in\{L,N\}}\mathbb{E}_{\mathrm{h}}\{\gamma_{\mathrm{r^*d}}|h_{\mathrm{r^*d}},n\}$ and $\sum_{m\in\{L,N\}}\mathbb{E}_{\mathrm{h}}\{\frac{1}{\gamma_{\mathrm{sr^*}}}|h_{\mathrm{sr^*}},m\}$. As such, $\mathbb{E}_{\Phi_{\mathrm{r}}}\{\frac{r^{-\alpha_{\mathrm{n}}}}{r_{\mathrm{sr}}^{-\alpha_{\mathrm{m}}}}\}$ is given by

$$\mathbb{E}_{\Phi_{\mathrm{r}}}\{\frac{r_{\mathrm{rd}}^{-\alpha_{\mathrm{n}}}}{r_{\mathrm{sr}}^{-\alpha_{\mathrm{m}}}}\}=\frac{1}{\pi{r_{\mathrm{d}}}^2}\int_0^{2\pi}\int_0^{r_{\mathrm{d}}}\frac{r^{-\alpha_{\mathrm{n}}}}{r_{\mathrm{sr}}^{-\alpha_{\mathrm{m}}}}rdrd\theta\\ =\frac{1}{\pi{r_{\mathrm{d}}}^2}\int_0^{2\pi}\int_0^{r_{\mathrm{d}}}\frac{r^{-\alpha_{\mathrm{n}}}}{(r^2+A^2+2rA\cos\theta)^{-\alpha_{\mathrm{m}}/2}}rdrd\theta. \tag{40}$$

where A and r_{d} are the distance between S and D, as well as the radius of the disk, respectively.

Upon substituting the result in (40) into (39), we have $\frac{\gamma_{\mathrm{r^*d}}}{\gamma_{\mathrm{sr^*}}}$. For a special system model associated with only a single untrusted relay, we arrive at

$$\frac{\gamma_{\mathrm{rd}}}{\gamma_{\mathrm{sr}}}\approx\mathbb{E}_{\mathrm{h}}\left\{\frac{\gamma_{\mathrm{rd}}}{\gamma_{\mathrm{sr}}}\right\}\\ =\frac{G_{\mathrm{rd}}}{G_{\mathrm{sr}}}\sum_{n\in\{L,N\}}\sum_{m\in\{L,N\}}\frac{C_{\mathrm{n}}}{C_{\mathrm{m}}}\frac{N_{\mathrm{n}}}{N_{\mathrm{m}-1}}\frac{r_{\mathrm{rd}}^{-\alpha_{\mathrm{n}}}}{r_{\mathrm{sr}}^{-\alpha_{\mathrm{m}}}}p_{\mathrm{n}}p_{m}. \tag{41}$$

Let us now return to (38) to derive $\mathbb{E}\{\xi\}$. In this case, we have the stages mentioned in (42). In (42), $\varrho_{\mathrm{n}}^{\mathrm{lk}}=\rho G_{\mathrm{se,A}}^{\mathrm{lk}}C_{\mathrm{n}}$. We note that $(\mathbf{a})$ in (42) follows from the fact that $\gamma_{\mathrm{de,A}}$ can be neglected compared to $\gamma_{\mathrm{se,A}}^{\mathrm{lk}}$. This is because in the first phase of communication, D injects AN with in the angular scope of its main-lobe to distract the selected relay. As such, a small amount of AN is received by the passive Eves, which could be neglected. Note that the r.v. u in (42) obeys an exponential distribution as mentioned in Section II. Upon substituting $\gamma_{\mathrm{se,S}}^{\mathrm{lk}}$ and $\gamma_{\mathrm{se,A}}^{lk}$ into (a) of (42) and also considering both the LoS and NLoS effects, $(\mathbf{b})$ and $(\mathbf{c})$ of (42) are reached. In (42), $(\mathbf{d})$ follows from the fact that the two variables are independent. To determine the distribution of the r.v. $x_{\mathrm{e}}=\|\mathbf{h}_{\mathrm{se}}W_2\|^2$, which is related to the amount of noise received by the e^{th} Eve in the null space of the selected relay, we can state that since the beamwidth of the signal transmitted by the source to the selected relay is narrow, the AN is approximately propagated in all directions. Accordingly, the amount of AN received by the e^{th} Eve is reduced and an upper band is obtained for $\mathbb{E}\{\xi\}$ in conjunction with $W_2=1$. As a consequence, x_{e} is equivalent to $\|\mathbf{h}_{\mathrm{se}}\|^2$ with an acceptable approximation, which has a gamma distribution formulated as $x_{\mathrm{e}}\sim\Gamma(N_{\mathrm{n}},1)$. Additionally, based on the stochastic geometry framework and on Campbell's theorem [4] over PPP, and using $r_{\mathrm{se}}^2=r_{\mathrm{e}}^2+A^2+2r_{\mathrm{e}}Acos\theta_{\mathrm{e,D}}$, after applying [41,Eq.(3.383.10)], the equation (e) of (42) holds.

For calculating $L_{\mathrm{Y}}(s)$, we have to calculate $F_{\mathrm{Y}}(x)$ as [13]

$$F_{\mathrm{Y}}(x)=\sum_{n\in\{L,N\}}\frac{\gamma\left(N_{\mathrm{n}},\frac{x}{\rho G_{\mathrm{r}}^{\mathrm{M}}G_{\mathrm{D}}^{\mathrm{M}}C_{\mathrm{n}}{r_{\mathrm{rd}}}^{-\alpha_{\mathrm{n}}}}\right)}{\Gamma(N_{\mathrm{n}})}p_{\mathrm{n}}, \tag{43}$$

where we have $Y=\gamma_{\mathrm{rd}}$ and $\gamma(s,x)$ is the lower incomplete gamma function.

Although (43) is exact, we present an approximate expression as follows. By using the binomial expansion [42, Eq.(1.111)] and then applying Alzer's lemma [7, Sec. (III)], [13, Sec. (IV)], we can derive the following approximate expression for $F_{\gamma_{\mathrm{rd}}}(x)$

$$F_{\gamma_{\mathrm{rd}}}(x)=\sum_{n\in\{L,N\}}\sum_{m=0}^{N_{\mathrm{n}}}(-1)^m\binom{N_{\mathrm{n}}}{m}e^{-\frac{\kappa_{\mathrm{n}}\mathrm{xm}}{\rho\mathrm{G_r^M G_D^M C_n r_{rd}}^{-\alpha_{\mathrm{n}}}}}p_{\mathrm{n}}, \tag{44}$$

where $\kappa_{\mathrm{n}}=(N_{\mathrm{n}}!)^{-\frac{1}{N_{\mathrm{n}}}}$, $n\in\{L,N\}$. $L_{\mathrm{Y}}(s)$ can also be

$$\begin{aligned}\mathbb{E}\{\xi\} &\overset{(a)}{=} \mathbb{E}_{\mathrm{e}}\left\{\sum_{e\in\Phi_{\mathrm{e}}}\sum_{l,k\in\{m,M\}}\frac{\gamma_{\mathrm{se,S}}^{\mathrm{lk}}}{\gamma_{\mathrm{se,A}}^{\mathrm{lk}}+1}pr_{\mathrm{lk}}\right\} \overset{(\mathbf{b})}{=} \mathbb{E}_{\mathrm{u,x_e,e}}\left\{\sum_{e\in\Phi_{\mathrm{e}}}\sum_{l,k\in\{m,M\}}\frac{\rho G_{\mathrm{se,S}}^{\mathrm{lk}}L(r_{\mathrm{se}})u}{\rho G_{\mathrm{se,A}}^{\mathrm{lk}}L(r_{\mathrm{se}})x_{\mathrm{e}}+1}pr_{\mathrm{lk}}\right\}\\
&\overset{(\mathbf{c})}{=} \sum_{l,k\in\{m,M\}}\mathbb{E}_{\mathrm{u,x_e,e}}\left\{\sum_{e\in\Phi_{\mathrm{e}}}\sum_{n\in\{L,N\}}\frac{\rho G_{\mathrm{s,S}}^{\mathrm{l}}G_{\mathrm{e}}^{\mathrm{k}}C_{\mathrm{n}}r_{\mathrm{se}}^{-\alpha_{\mathrm{n}}}u}{\rho G_{\mathrm{s,A}}^{\mathrm{l}}G_{\mathrm{e}}^{\mathrm{k}}C_{\mathrm{n}}r_{\mathrm{se}}^{-\alpha_{\mathrm{n}}}x_{\mathrm{e}}+1}p_{\mathrm{n}}\right\}pr_{\mathrm{lk}}\\
&\overset{(\mathbf{d})}{=} \sum_{l,k\in\{m,M\}}\frac{G_{\mathrm{s,S}}^{\mathrm{l}}}{G_{\mathrm{s,A}}^{\mathrm{l}}}\mathbb{E}_{\mathrm{e}}\left\{\sum_{e\in\Phi_{\mathrm{e}}}\sum_{n\in\{L,N\}}E\{u\}E\{\frac{1}{x_{\mathrm{e}}+\frac{r_{\mathrm{se}}^{\alpha_{\mathrm{n}}}}{\varrho_{\mathrm{n}}^{\mathrm{lk}}}}\}p_{\mathrm{n}}\right\}pr_{\mathrm{lk}}\\
&\overset{(\mathbf{e})}{=} \sum_{l,k\in\{m,M\}}\frac{G_{\mathrm{s,S}}^{\mathrm{l}}}{G_{\mathrm{s,A}}^{\mathrm{l}}}\mathbb{E}_{\mathrm{e}}\{\sum_{e\in\Phi_{\mathrm{e}}}\sum_{n\in\{L,N\}}\int_{0}^{+\infty}\frac{1}{x+\frac{r_{\mathrm{se}}^{\alpha_{\mathrm{n}}}}{\varrho_{\mathrm{n}}^{\mathrm{lk}}}}\frac{x^{\mathrm{N_n}-1}e^{-\mathrm{x}}}{\Gamma(N_{\mathrm{n}})}\,dxp_{\mathrm{n}}\}pr_{\mathrm{lk}}\\
&\overset{(\mathbf{f})}{=} \lambda_{\mathrm{e}}\sum_{l,\bar{l},k\in\{m,M\},l\neq\bar{l}}\frac{G_{\mathrm{s,S}}^{\mathrm{l}}}{G_{\mathrm{s,A}}^{\bar{\mathrm{l}}}}\left\{\sum_{n\in\{L,N\}}p_{\mathrm{n}}\int_{\theta_{e,D}=0}^{2\pi}\int_{r_{\mathrm{e}}=0}^{r_{\mathrm{d}}}(\frac{r_{\mathrm{se}}^{\alpha_{\mathrm{n}}}}{\varrho_{\mathrm{n}}^{\mathrm{lk}}})^{\mathrm{N_n}-1}e^{\frac{\mathrm{r_{se}^{\alpha_n}}}{\varrho_{\mathrm{n}}^{\mathrm{lk}}}}\Gamma(1-N_{\mathrm{n}},\frac{r_{\mathrm{se}}^{\alpha_{\mathrm{n}}}}{\varrho_{\mathrm{n}}^{\mathrm{lk}}})r\,dr_{\mathrm{e}}\,d\theta_{\mathrm{e,D}}\right\}pr_{\mathrm{lk}}.\end{aligned} \tag{42}$$

evaluated as

$$\begin{aligned}L_{\mathrm{Y}}(s) &= \mathbb{E}\{e^{-\mathrm{sY}}\} \overset{(a)}{=} s\int_{0}^{+\infty}F_{\mathrm{Y}}(x)e^{-\mathrm{sx}}dx\\
&= \sum_{n\in\{L,N\}}p_{\mathrm{n}}(1+s\rho G_{\mathrm{r}}^{\mathrm{M}}G_{\mathrm{D}}^{\mathrm{M}}C_{\mathrm{n}}r_{\mathrm{rd}}{}^{-\alpha_{\mathrm{n}}})^{-\mathrm{N_n}}.\end{aligned} \tag{45}$$

Up on substituting $\mathbb{E}\{\xi\}$ in (42) and $\mathbb{E}\{v\}$ in (41) into (38), and then by substituting (38), and $L_{\mathrm{Y}}(s)$ of (45) into (37), a new closed-form expression is formulated for the ESR of our system model for a single untrusted relay which is given as

$$\begin{aligned}\bar{R}_{\mathrm{s}}^{\mathrm{Single-relay}} &= \frac{1}{2\ln 2}\sum_{n\in\{L,N\}}e^{\frac{a_{\mathrm{n}}+1}{b_{\mathrm{n}}}}\\
\times&\left[-\mathrm{E_i}\left(-\tfrac{a_{\mathrm{n}}+1}{b_{\mathrm{n}}}\right)+\textstyle\sum_{l=1}^{N_{\mathrm{n}}-1}\left(\tfrac{a_{\mathrm{n}}+1}{b_{\mathrm{n}}}\right)^{N_{\mathrm{n}}-l}\Gamma\left(-(N_{\mathrm{n}}-l),\tfrac{a_{\mathrm{n}}+1}{b_{\mathrm{n}}}\right)\right]p_{\mathrm{n}},\end{aligned} \tag{46}$$

where $a_{\mathrm{n}} = \sqrt{2(1+\mathbb{E}\{C\})}$, $b_{\mathrm{n}} = \rho G_{\mathrm{r}}^{\mathrm{M}}G_{\mathrm{D}}^{\mathrm{M}}C_{\mathrm{n}}r_{\mathrm{rd}}{}^{-\alpha_{\mathrm{n}}}$ and $E_{\mathrm{i}}(.)$ is defined as in section I.

We note that for the NCE scenario we have to substitute $C = 0$ into (38) and (46). We note that the ESR in (46) is determined by the transmit power of the network, the antenna gains of the source, destination and untrusted relay, the mmWave carrier frequency, the parameters related to the environment including blockage, path-loss and small scale fading, as well as the parameters related to the Eves, including the density and antenna gains' of Eves. Now, we calculate a closed-form expression for the relay selection policy in (34) as

$$\begin{aligned}F_{\gamma_{\mathrm{best}}}(x) &= \mathbb{E}_{\Phi_{\mathrm{r}}}\prod_{r\in\Phi_{\mathrm{r}}}\Pr(\gamma_{\mathrm{rd}}\leq x) \overset{(a)}{=} e^{-\lambda_{\mathrm{r}}\pi\mathrm{r_d}^2(1-\mathrm{v(x)})} \qquad (47)\\
&= \exp\{2\pi\lambda_{\mathrm{r}}\sum_{n\in\{L,N\}}\frac{p_{\mathrm{n}}}{\alpha_{\mathrm{n}}}\sum_{m=1}^{N_{\mathrm{n}}}(-1)^{m}\binom{N_{\mathrm{n}}}{m}\left(\frac{\kappa_{\mathrm{n}}xm}{\rho G_{\mathrm{r}}^{\mathrm{M}}G_{\mathrm{D}}^{\mathrm{M}}C_{\mathrm{n}}}\right)^{-\frac{2}{\alpha_{\mathrm{n}}}}\\
&\times\gamma\left(\frac{2}{\alpha_{\mathrm{n}}},\frac{\kappa_{\mathrm{n}}xm}{\rho G_{\mathrm{r}}^{\mathrm{M}}G_{\mathrm{D}}^{\mathrm{M}}C_{\mathrm{n}}}r_{\mathrm{d}}{}^{\alpha_{\mathrm{n}}}\right)\},\end{aligned}$$

where in (47, (a)), we have

$$\begin{aligned}v(x) &= \frac{1}{\pi r_{\mathrm{d}}{}^2}\int_{0}^{2\pi}\int_{0}^{r_d}F_{\gamma_{\mathrm{rd}}}(x)rdrd\theta\\
&= 1+\frac{2}{r_{\mathrm{d}}{}^2}\sum_{n\in\{L,N\}}\frac{p_{\mathrm{n}}}{\alpha_{\mathrm{n}}}\sum_{m=1}^{N_{\mathrm{n}}}(-1)^{m}\binom{N_{\mathrm{n}}}{m}\left(\frac{\kappa_{\mathrm{n}}xm}{\rho G_{\mathrm{r}}^{\mathrm{M}}G_{\mathrm{D}}^{\mathrm{M}}C_{\mathrm{n}}}\right)^{-\frac{2}{\alpha_{\mathrm{n}}}}\\
&\times\gamma\left(\frac{2}{\alpha_{\mathrm{n}}},\frac{\kappa_{\mathrm{n}}xm}{\rho G_{\mathrm{r}}^{\mathrm{M}}G_{\mathrm{D}}^{\mathrm{M}}C_{\mathrm{n}}}r_{\mathrm{d}}{}^{\alpha_{\mathrm{n}}}\right).\end{aligned} \tag{48}$$

We note that (47) holds which can be shown by using a similar approach to that in [12, Eq. (8)]. However, in this work, we consider the case in which there may be no relays in the network. By using $F_{\mathrm{Y}}(x)$ in (44), and using [42, Eq. (3.381.1)], $v(x)$ in (48) is derived. According to Eqs. (37), (45, (a)), (47), (48), we can find that $F_{\gamma_{\mathrm{best}}}(x)$ and consequently, $\bar{R}_{\mathrm{s}}$ depends on the statistical characteristics of the second hop, the main lobe gains of the destination and the selected relay's antennas, the carrier frequency, the path-loss, the obstacles and the amount of leakage.

Then $\bar{R}_{\mathrm{s}}^{\mathrm{Multi-relay}}$ can be expressed as

$$\bar{R}_{\mathrm{s}}^{\mathrm{Multi-relay}} = \frac{1}{2\ln 2}\int_{0}^{+\infty}[L_{\mathrm{I_e}}(s)(2-L_{\gamma_{\mathrm{best}}}(s))-1]\frac{e^{-s}}{s}ds. \tag{49}$$

To drive (49), the following steps should be followed. Upon applying $F_{\gamma_{\mathrm{best}}}(x)$ in (47) and (48), and then substituting $Y = \gamma_{\mathrm{best}}$ into (45, (a)), $L_{\gamma_{\mathrm{best}}}(s)$ is formulated. For driving $L_{\mathrm{I_e}}(s)$ in (38), we need $\mathbb{E}\{\xi\}$ and $\mathbb{E}\{\frac{\gamma_{\mathrm{r*d}}}{\gamma_{\mathrm{sr*}}}\}$, where $\mathbb{E}\{\xi\}$ is given in (42), and there is no difference between the single-relay and multi-relay cases. Finally, to express $\mathbb{E}\{\frac{\gamma_{\mathrm{r*d}}}{\gamma_{\mathrm{sr*}}}\}$ for the multi-relay case, we have to rely on using (39).

A. 2. DT Scheme: We now study a scenario that the source transmits the message signal directly to the destination with MRT beamforming ($\lambda = 1$). In this condition, all the untrusted relays (as internal Eves) and passive Eves (as external Eves) listen to the communications. As such, the received signal at the destination can be represented by

$$\gamma_{\mathrm{D}}^{\mathrm{DT}} = \sum_{n\in\{L,N\}} \rho G_{s,S}^{M} G_{D}^{M} \|\mathbf{h}_{\mathrm{sd}}\|^2 p_{\mathrm{n}}$$
$$\overset{(a)}{\approx} \sum_{n\in\{L,N\}} \rho G_{\mathrm{s,S}}^{\mathrm{M}} G_{\mathrm{D}}^{\mathrm{M}} C_{\mathrm{n}} r_{\mathrm{sd}}^{-\mathrm{a_n}} N_{\mathrm{n}} p_{\mathrm{n}} = \sum_{n\in\{L,N\}} \bar{\gamma}_{\mathrm{sd}} N_{\mathrm{n}} p_{\mathrm{n}}, \quad (50)$$

where (a) follows from the law of large numbers due to the LSAA and $\bar{\gamma}_{\mathrm{sd}} = \rho G_{\mathrm{s,S}}^{\mathrm{M}} G_{\mathrm{D}}^{\mathrm{M}} C_{\mathrm{n}} r_{\mathrm{sd}}^{-\mathrm{a_n}}$. Here, for mathematical simplicity, we assume that all relays and Eves receive the message signal in their main lob antennas. This assumption is a worst-case scenario from the security perspective.

In the following, we investigate the DT scheme for NCE and CE scenarios, separately.

1) DT with NCE: For NCE scenario, the message leakage is expressed as

$$\gamma_{\mathrm{E}}^{\mathrm{DT,NCE}} = \max_{\mathrm{r}\in\Phi_{\mathrm{r}},\mathrm{e}\in\Phi_{\mathrm{e}}} \{\gamma_{\mathrm{r}}, \gamma_{\mathrm{e}}\}. \quad (51)$$

To calculate the average wiretap rate, we need to obtain the CDF of the message leakage as

$$F_{\gamma_{\mathrm{E}}^{\mathrm{DT,NCE}}}(x) = \Pr(\max_{\mathrm{r}\in\Phi_{\mathrm{r}},\mathrm{e}\in\Phi_{\mathrm{e}}} \{\gamma_{\mathrm{r}}, \gamma_{\mathrm{e}}\} < x) \quad (52)$$
$$= \prod_{\mathrm{i}\in\{\mathrm{r,e}\}} e^{-\lambda_{\mathrm{i}} \pi r_{\mathrm{d}}^2 (1 - v_{\mathrm{i}}^{\mathrm{DT,NCE}}(x))},$$

where for $i \in \{r, e\}$, $v_{\mathrm{i}}^{\mathrm{DT,NCE}}(x) = \sum_{n\in\{L,N\}} \frac{1}{\pi r_{\mathrm{d}}^2}$ $\times \int_0^{r_{\mathrm{d}}} \left(1 - e^{\frac{-x}{\rho G_{\mathrm{s,S}}^{m} G_{\mathrm{i}}^{\mathrm{M}} C_{\mathrm{n}} \left(r^2 + A^2 + 2rAcos(\theta)\right)^{-\frac{a_{\mathrm{n}}}{2}}}}\right) r d_{\mathrm{r}} d_{\theta}$. In (52), we have $\gamma_{\mathrm{i}} = \rho G_{\mathrm{s,S}}^{m} G_{\mathrm{i}}^{\mathrm{M}} L(r_{\mathrm{si}}) |\beta_{\mathrm{si}} \mathbf{a}_{\mathrm{si}}^{\mathrm{H}} \mathbf{a}_{\mathrm{sd}}|^2, i \in \{r, e\}$, where as mentioned earlier $|\beta_{\mathrm{si}} \mathbf{a}_{\mathrm{si}}^{H} \mathbf{a}_{\mathrm{sd}}|^2 \sim \exp(1)$. In (52), we proceed the trend similar to those applied in (35) and (47).

By substituting $F_{\gamma_{\mathrm{E}}^{\mathrm{DT,NCE}}}(x)$ in (52) and $\gamma_{\mathrm{D}}^{\mathrm{DT}}$ in (50) into the ESR formula [34], we get

$$\bar{R}_{\mathrm{s}}^{\mathrm{DT,NCE}} = \frac{1}{\ln 2} \sum_{n\in\{L,N\}} \left\{ \ln(1 - \bar{\gamma}_{\mathrm{sd}} N_{\mathrm{n}}) - \int_0^{+\infty} \frac{1 - F_{\gamma_{\mathrm{E}}^{\mathrm{DT,NCE}}}}{1+x} d_{\mathrm{x}} \right\}. \quad (53)$$

2) DT with CE: For CE scenario, the message leakage can be given by

$$\gamma_{\mathrm{E}}^{\mathrm{DT,CE}} = \max_{\mathrm{r}\in\Phi_{\mathrm{r}}} \{\gamma_{\mathrm{r}}, \sum_{\mathrm{e}\in\phi_{\mathrm{e}}} \gamma_{\mathrm{e}}\}. \quad (54)$$

In the following, we present a new expression for the CDF of $\gamma_{\mathrm{E}}^{\mathrm{DT,CE}}$. To do so, we first need to calculate the laplace transform of $\gamma_{\mathrm{E}}^{\mathrm{Eve}} = \sum_{n\in\{L,N\}} \sum_{\mathrm{e}\in\Phi_{\mathrm{e}}} \rho G_{\mathrm{s,S}}^{\mathrm{m}} G_{\mathrm{e}}^{\mathrm{M}} C_{\mathrm{n}} r_{\mathrm{se}}^{-\alpha_{\mathrm{n}}} |\beta_{\mathrm{se}} \mathbf{a}_{\mathrm{se}}^{\mathrm{H}} \mathbf{a}_{\mathrm{sd}}|^2$ as

$$L_{\gamma_{\mathrm{E}}^{\mathrm{Eve}}}(s) = \mathbb{E}_{\Phi_{\mathrm{e}}} \left\{ e^{-s \sum_{n\in\{L,N\}} \sum_{\mathrm{e}\in\Phi_{\mathrm{e}}} \rho G_{\mathrm{s,S}}^{m} G_{\mathrm{e}}^{\mathrm{M}} C_{\mathrm{n}} r_{\mathrm{se}}^{-\alpha_{\mathrm{n}}} |\beta_{\mathrm{se}} \mathbf{a}_{\mathrm{se}}^{H} \mathbf{a}_{\mathrm{sd}}|^2} \right\}$$
$$\overset{(a)}{=} e^{-\lambda_{\mathrm{e}} \pi r_{\mathrm{d}}^2 (1 - v_{e}^{\mathrm{DT,CE}}(s))} \quad (55)$$

where $v_{\mathrm{e}}^{\mathrm{DT,CE}}(s) = \frac{1}{\pi r_{\mathrm{d}}^2} \sum_{n\in\{L,N\}} p_{\mathrm{n}}$ $\times \int_0^{\mathrm{r_d}} \left(e^{-s\rho G_{\mathrm{s,S}}^{m} G_{\mathrm{e}}^{\mathrm{M}} C_{\mathrm{n}} \left(r^2 + A^2 + 2rAcos(\theta)\right)^{-\frac{\mathrm{a_n}}{2}}} \right) r d_{\mathrm{r}} d_{\theta}$, and (a) holds by adopting the similar approach used in [12, Eq. (8)]. As such, the SOP performance related to the passive Eves can be expressed as

$$P_{\mathrm{so},\gamma_{\mathrm{E}}^{\mathrm{Eve}}} = \Pr\left(\log_2 \left(\frac{1 + \gamma_{\mathrm{D}}^{\mathrm{DT}}}{1 + \gamma_{\mathrm{E}}^{\mathrm{Eve}}}\right) < R_t \right)$$
$$= \Pr\left(\gamma_{\mathrm{E}}^{\mathrm{Eve}} > 2^{-2R_t} (1 + \bar{\gamma}_{\mathrm{sd}} N_{\mathrm{n}}) - 1 \right) = 1 - F_{\gamma_{\mathrm{E}}^{\mathrm{Eve}}}(\tilde{R}_t), \quad (56)$$

where R_{t} is the target transmission rate and $\tilde{R}_t \triangleq 2^{-2R_t}(1 + \bar{\gamma}_{\mathrm{sd}} N_{\mathrm{n}}) - 1$. Based on Lemma 1 in [17] and (55), we can express $P_{\mathrm{so},\gamma_{\mathrm{E}}^{\mathrm{Eve}}}$ as

$$P_{\mathrm{so},\gamma_{\mathrm{E}}^{\mathrm{Eve}}} = \sum_{m=0}^{N} (-1)^m \binom{N}{m} e^{-\lambda_{\mathrm{e}} \pi r_{\mathrm{d}}^2 (1 - v_{\mathrm{e}}^{\mathrm{DT,CE}}(\frac{\kappa m}{\tilde{R}_t}))}, \quad (57)$$

where $\kappa = (N!)^{-\frac{1}{N}}$, and N is the number of terms utilized in the approximation. According to (56) and (57), $F_{\gamma_{\mathrm{E}}^{\mathrm{Eve}}}(x)$ is given by

$$F_{\gamma_{\mathrm{E}}^{\mathrm{Eve}}}(x) = \sum_{m=1}^{N} (-1)^{m+1} \binom{N}{m} e^{-\lambda_{\mathrm{e}} \pi r_{\mathrm{d}}^2 (1 - v_{\mathrm{e}}^{\mathrm{DT,CE}}(\frac{\kappa m}{x}))}. \quad (58)$$

Following the trends mentioned earlier, we can calculate $F\gamma_{\mathrm{E}}^{\mathrm{DT,CE}}(x)$ as

$$F\gamma_{\mathrm{E}}^{\mathrm{DT,CE}}(x) = F\gamma_{\mathrm{E}}^{\mathrm{r}}(x) F\gamma_{\mathrm{E}}^{\mathrm{Eve}}(x). \quad (59)$$

By substituting $F\gamma_{\mathrm{E}}^{\mathrm{DT,CE}}(x)$ in (59) and $\gamma_{\mathrm{D}}^{\mathrm{DT}}$ in (50) into $\bar{R}_{\mathrm{s}}^{\mathrm{DT,CE}} = \frac{1}{\ln 2} \{\mathbb{E}\left\{\ln(1 + \gamma_{\mathrm{D}}^{\mathrm{DT}})\right\} - \mathbb{E}\left\{\ln(1 + \gamma_{\mathrm{E}}^{\mathrm{DT,CE}})\right\}$, one can obtain

$$\bar{R}_{\mathrm{s}}^{\mathrm{DT,CE}} = \frac{1}{\ln 2} \left\{ \sum_{n\in\{L,N\}} p_{\mathrm{n}} \ln(1 - \bar{\gamma}_{\mathrm{sd}} N_{\mathrm{n}}) \right\} - \int_0^{+\infty} \frac{1 - F_{\gamma_{\mathrm{E}}^{\mathrm{DT,CE}}}(x)}{1+x} d_{\mathrm{x}}. \quad (60)$$

B. Secrecy Outage Probability

B.1. DSBCJ Scheme: According to the definition [34], the SOP is defined as $P_{\mathrm{so}} = \Pr(R_{\mathrm{s}} < R_{\mathrm{t}})$, where R_{t} is the target transmission rate. To evaluate this popular metric for our proposed JRP method, by substituting (33) into the SOP definition, we obtain $P_{\mathrm{so}}^{\mathrm{DSBCJ}} = \Pr(\gamma_{r^*d} < \tilde{R}_{\mathrm{t}}) = F_{\gamma_{\mathrm{r}^*\mathrm{d}}}(\tilde{R}_{\mathrm{t}})$, where $\tilde{R}_{\mathrm{t}} = \left(1 + \sqrt{2(1+C)}\right)\left(2^{2R_{\mathrm{t}}}(1 + \sqrt{2(1+C)}) - 1\right)$. Note that for NCE, we have $C = 0$. By substituting $\tilde{R}_{\mathrm{t}}$ into (47) and (48), the new closed-form expression for the SOP of the optimized mmWave multiple-untrusted relaying network is represented by

$$P_{\mathrm{so}}^{\mathrm{DSBCJ}}$$
$$= \exp\{2\pi\lambda_{\mathrm{r}} \sum_{n\in\{L,N\}} \frac{p_{\mathrm{n}}}{\alpha_{\mathrm{n}}} \sum_{m=1}^{N_{\mathrm{n}}} (-1)^m \binom{N_{\mathrm{n}}}{m} \left(\frac{\kappa_{\mathrm{n}} \tilde{R}_{\mathrm{t}} m}{\rho G_{\mathrm{r}}^{\mathrm{M}} G_{\mathrm{D}}^{\mathrm{M}} C_{\mathrm{n}}}\right)^{-\frac{2}{\alpha_{\mathrm{n}}}} \quad (61)$$
$$\times \gamma\left(\frac{2}{\alpha_{\mathrm{n}}}, \frac{\kappa_{\mathrm{n}} \tilde{R}_{\mathrm{t}} m}{\rho G_{\mathrm{r}}^{\mathrm{M}} G_{\mathrm{D}}^{\mathrm{M}} C_{\mathrm{n}}} {r_{\mathrm{d}}}^{\alpha_{\mathrm{n}}}\right)\}.$$

Additionally, for a single-relay mmWave networks relying on the DSBCJ policy, we arrive at

$$P_{\mathrm{so}}^{\mathrm{DSBCJ}} = \sum\nolimits_{n\in\{L,N\}} \frac{\gamma\left(N_{\mathrm{n}}, \frac{\tilde{R}_{\mathrm{t}}}{\rho G_{\mathrm{r}}^{\mathrm{M}} G_{\mathrm{D}}^{\mathrm{M}} C_{\mathrm{n}} r_{\mathrm{rd}}{}^{-\alpha_{\mathrm{n}}}}\right)}{\Gamma(N_{\mathrm{n}})} p_{\mathrm{n}}.$$

B. 2. DT Scheme: By exploiting a similar method to that used in (58) and by using (52), we derive the SOP for the DT scheme under the NCE and CE scenarios as follows

$$p_{\mathrm{so}}^{\mathrm{DT,NCE}} = 1 - F_{\gamma_{\mathrm{E}}^{\mathrm{DT,NCE}}}(\tilde{R}_{\mathrm{t}}), \tag{62}$$

$$p_{\mathrm{so}}^{\mathrm{DT,CE}} = 1 - F_{\gamma_{\mathrm{E}}^{\mathrm{DT,CE}}}(\tilde{R}_{\mathrm{t}}), \tag{63}$$

where in (62) and (63), we have $\tilde{R}_{\mathrm{t}} \triangleq 2^{-2\mathrm{R}_{\mathrm{t}}}(1 + \bar{\gamma}_{\mathrm{sd}} N_{\mathrm{n}}) - 1$.

V. Simulations and Discussions

In this section, our ESR and SOP results are presented for a carrier frequency of 28 GHz. Our simulation parameters are listed in Table II [6]. In all numerical results, we assume that each passive Eve has a single directional antenna gain with main and side lobes of 5 dB and -5 dB gains, respectively.

Fig. 2 and Fig. 3 illustrate the ESR versus the transmit power P for a single-relay scenario, including both NCE and CE, and for different blockage densities. Our observations from Fig. 2 and Fig. 3 are summarized as follows:

1) The ESR performance of our proposed model is a monotonically increasing function of the transmit power P. We also mention that the ESR of the OPA is not satisfactory for low P.
2) The ESR performance of the proposed DSBCJ increases as p_{L} grows. This is because when the blockage density in the second hop is reduced, the probability of having a LoS link is increased, which can be exploited for increasing the system's ESR. It can also be found that when the LoS probability is reduced, more transmit power should be dedicated for compensating the ESR reduction and this reduces the power efficiency of the network.
3) The analytical curves in Fig. 2, obtained from (46) with $C = 0$ represent that the ESR is independent of the density of the Eves. This is because the ESR is essentially limited by the untrusted relay, not by the NCE.
4) In contrast to Fig. 2, the analytical curves in Fig. 3, obtained from (46) with $C > 0$ and represent that the ESR is reduced by increasing the density of Eves. This is because when the density of CEs is increased, the Eves collude more with each other, which leads to an ESR reduction. For example, for a ten-fold increase in the density of Eves, the ESR in the CE scenario is reduced by about 80%.
5) Bearing in mind equations (37), (43), (45), and considering Fig. 2 and Fig. 3, we can observe that in the OPA mode, when the gain of the second hop's antennas is improved, $L_{\mathrm{Y}}(s)$ is decreased which leads to an ESR increment. For example, for a mmWave carrier of 28 GHz when the transmit power P is 30 dBm and $p_{\mathrm{L}} = 0.7$, a 5dB increase in the second hop antenna gain increases the ESR for the NCE scenario by about 35% and for the CE scenario by about 20%. An increase in the carrier frequency increases the term $L_{\mathrm{Y}}(s)$ in (37) and consequently reduces the ESR. Furthermore, as observe in Fig. 3, for a beamforming gain of 15 dB at the second hop, that the ESR of the NCE and CE scenarios decreases by 45% and 55%, respectively, when the frequency increases from 28 GHz to 73 GHz.
6) As such, when the AN transmit power of S is reduced by 5 dBm, the ESR of the CE scenario is reduced by about 15%. The reason is that regarding (29) and (30), less AN provides an advantages for the Eves, which in turn reduces the ESR. This means that AN tends to improve the ESR. Finally, as we can see in both Fig. 2 and Fig. 3, the blockage plays a significant role in reducing the ESR.

TABLE II: Simulation Parameters.

Type	Value
Antenna gain	$G_{\mathrm{s,S}}^{\mathrm{M}}$ =18 dB, $G_{\mathrm{s,S}}^{\mathrm{m}} = -3$ dB $G_{\mathrm{s,A}}^{\mathrm{M}} = 15$ dB, $G_{\mathrm{s,A}}^{\mathrm{m}} = -3$ dB $G_{\mathrm{r}}^{\mathrm{M}} = 10$ dB, $G_{\mathrm{r}}^{\mathrm{m}} = -5$ dB $G_{\mathrm{D}}^{\mathrm{M}} = G_{\mathrm{e}}^{\mathrm{M}} = 5$ dB, $G_{\mathrm{D}}^{\mathrm{m}} = G_{\mathrm{e}}^{\mathrm{m}} = -5$ dB
Main-lobe beamwidth	$\theta_{\mathrm{S}} = \theta_{\mathrm{r}} = \theta_{\mathrm{D}} = \theta_{\mathrm{e}} = 10°$
Blockage	p_{L}
Path-loss (for 28 GHz)	$\alpha_{\mathrm{L}} = 2$, $\beta_{\mathrm{L}} = 61.4$ $\alpha_{\mathrm{N}} = 2.92$, $\beta_{\mathrm{N}} = 72$
Path-loss (for 73 GHz)	$\alpha_{\mathrm{L}} = 2$, $\beta_{\mathrm{L}} = 69.8$ $\alpha_{\mathrm{N}} = 2.69$, $\beta_{\mathrm{N}} = 82.7$
Small scale fading	$N_{\mathrm{L}} = 3$, $N_{\mathrm{N}} = 2$
Noise figure (NF)	10 dB
Bandwidth (BW)	2 GHz
Noise power (N_0)	-174 dBm/Hz$+10\log_{10}(BW) + NF$

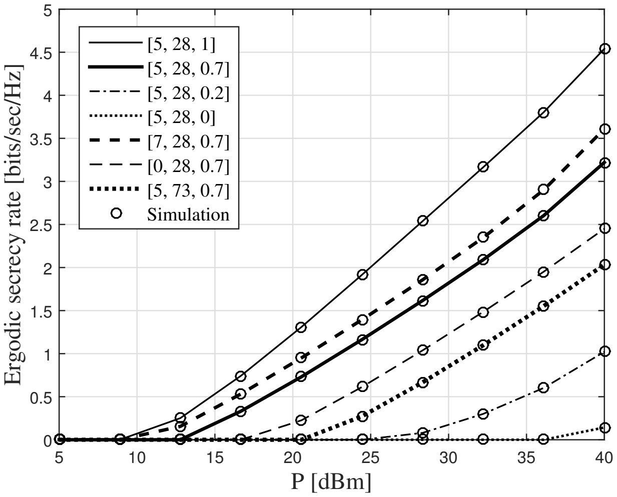

Fig. 2: ESR versus P for a single relay NCE scenario and for different density of blockages using the proposed OPA. The elements in the vector [a, b, c] are respectively represented as $a = G_{\mathrm{D}}^{\mathrm{M}}$ [dB], $b = f_{\mathrm{c}}$ GHz and $c = p_{\mathrm{L}}$. The circles represent the Monte-Carlo simulations.

Fig. 4 also shows the ESR versus transmit power P, for different power allocation strategies. The curves are obtained from (46) with $C = 0$. As it can be seen, when the transmitter allocates the optimal power to the message signal the ESR is improved about 0.3 bits/sec/Hz compared to the case with half power allocation ($\lambda = 0.5$), for the single relay scenario

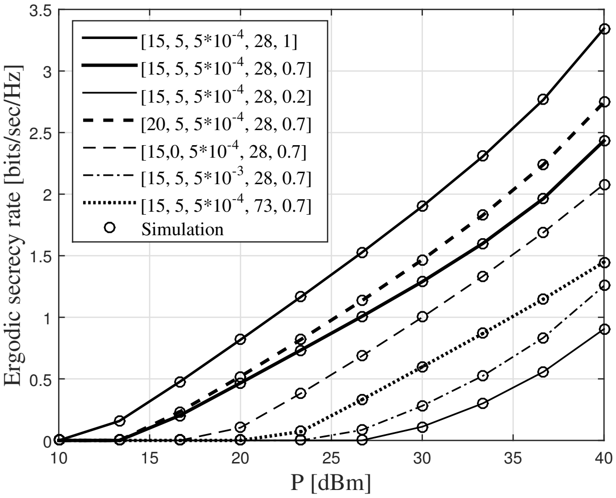

Fig. 3: ESR versus P for a single relay CE scenario and different density of blockages, using the proposed OPA. The elements in the vector [a, b, c, d, e] are respectively described as $a = G^{\rm M}_{\rm s,A}$ [dB], $b = G^{\rm M}_{\rm D}$ [dB], $c = \lambda_{\rm e}$ $(1/m^2)$, $d = f_{\rm c}$ GHz and $e = p_{\rm L}$. The circles represent the Monte-Carlo simulations.

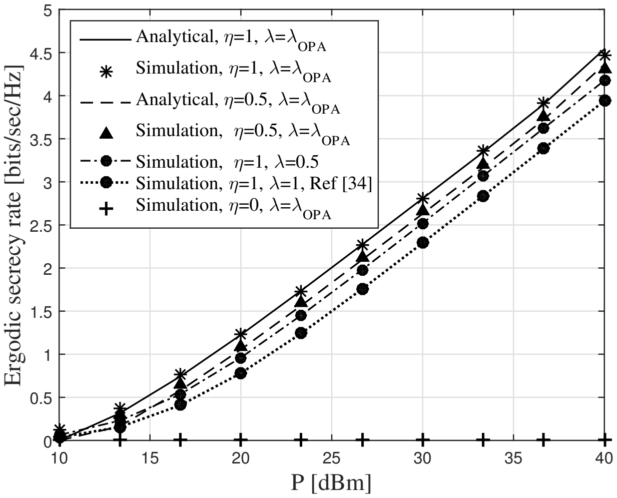

Fig. 4: ESR versus P for a single relay NCE scenario with $p_{\rm L} = 0.7$, and for different power allocation strategies.

with $P = 30$ dBm. Again, AN improves the ESR upon using OPA. Additionally, we observe from Fig. 4 that the optimal AN power allocation for D ($\eta = 1$), has a significant role in increasing the ESR i.e., by increasing η from $\eta = 0$ to $\eta = 1$, the ESR increases approximately 2.8 bits/sec/Hz for $P = 30$ dBm. Similar secrecy performance behavior can be observed for CE scenario, and due to space limitations, we omit the corresponding curves here. Depending on the required secrecy rate, the user can adjust its jamming power. Note that as observed in Fig. 4, for the case of $\eta = 0$, confidentiality is not achieved and as a result, the secrecy rate becomes zero. Furthermore, as observed in Fig. 4, by decreasing the jamming power from $\eta = 1$ to $\eta = 0.5$ for the single relay and NCE scenario, if we save 50% of the destination (jamming) power, about 5% ESR erosion is experienced at high power consumption.

Fig. 5 portrays the effect of P on the ESR of a network operating in the face of multiple-untrusted relays in both NCE and CE scenarios, when $p_{\rm L} = 0.7$, $f = 28$ GHz, $G^{\rm M}_{\rm s,S} = 18$ dB, $G^{\rm M}_{\rm s,A} = 15$ dB, and $\lambda_{\rm r} = 5 \times 10^{-4}$. The analytical curves achieved are plotted using (49). The ESR of our proposed JRP method exhibits a monotonically increasing nature vs. P in both the NCE and CE scenarios, NCE scenario provides a higher ESR than the CE scenario. The effect of increasing gain of D ($G^{\rm M}_{\rm D}$), on increasing the ESR curve is quite obvious and the corresponding curve is plotted for NCE. We also mention that the ESR of the OPA is reduced by approximately 0.8 bits/sec/Hz for both scenarios, when the relay gain reduces by 5 dB. In the high P regime, the ESR is no longer increased upon increasing P. This is because for NCE, the ESR depends on the received SNR in the second hop and maximum information leakage to the relays, but for high P, it depends on the ratio of them, so it is not a function of P and saturates. For CE, we observe that at a high P, the ESR gradually stats to saturate, because the Eves trend to receive more power, which leads to increased leakage and reduced ESR. Increasing the density of NCE does not affect the ESR, whereas in the case of the CE the ESR decreases. For example at $P = 30$ dBm, this reduction is about 1.3 bits/sec/Hz upon increasing the density of the Eves by about of 10 times. It can also be deduced from Fig. 5 that the Eves cannot increase their eavesdropping capability by increasing their antenna gains. The reason for this is that for the NCE scenario, as mentioned in Section III-A, the amount of message leakage depends on the selected relay's link and not on the passive Eves' links. By contrast, for the CE scenario the amount of captured information increases by boosting the antenna gains of Eves, but the amount of AN they receive is also increased. As a result, increasing the antenna gains of colluding Eves has no impact on increasing their eavesdropping capability. This result confirms the importance of AN injection for the security of mmWave networks.

Fig. 6 portrays the ESR versus untrusted relay density for $p_{\rm L} = 0$, 0.5 and 1. We utilize the mmWave carrier frequency of 28 GHz. The analytical curves are plotted using (49). Our observations are summarized as follows

- The ESR increases as the density of untrusted relays increases. This is because upon increasing the number of relays and intelligently injecting AN, the probability of having a stronger link in the second hop increases, hence increasing the ESR. However, the ESR tends to saturate in the high relay density regime, because the non-selected untrusted relays act as interferers and hence the network becomes interference-limited.
- The JRP proposed for the NCE scenario offers a superior ESR approaching, that of the CE scenario. Furthermore, although having more relays increases the probability of selecting a better helper, it also increases the amount of information leakage, and the latter results in gradual ESR-saturation. We can also conclude from Fig. 6 that as the blockage density increases, the ESR is reduced.

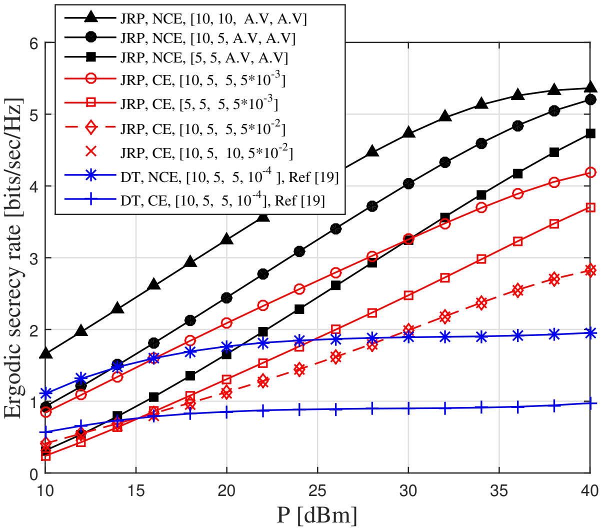

Fig. 5: The effect of P on the ESR in multiple-untrusted relaying network for both NCE and CE scenarios when $p_{\rm L} = 0.7$ and $\lambda_{\rm r} = 5 \times 10^{-4}$. The elements in the vector [a, b, c, d] respectively express $a = G_{\rm r}^{\rm M}$ [dB], $b = G_{\rm D}^{\rm M}$ [dB], $c = G_{\rm e}^{\rm M}$ [dB], $d = \lambda_{\rm e}$ $(1/m^2)$. The notation ‘A.V’ states any value for the density of Eves.

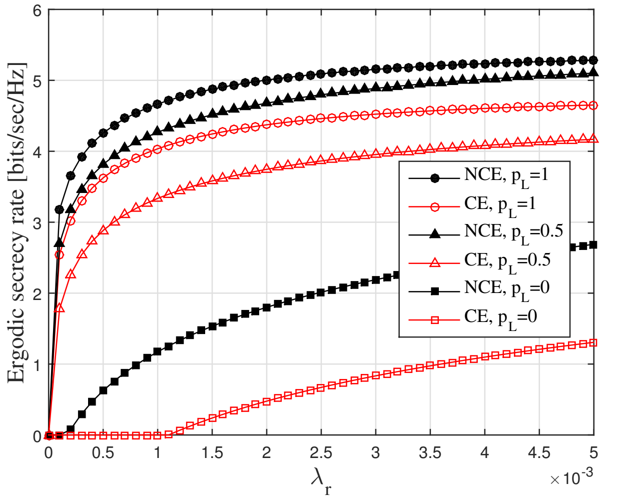

Fig. 6: ESR versus the relay density $\lambda_{\rm r}$ for $f_{\rm c} = 28$ GHz and $P = 30$ dBm, and for different values of $p_{\rm L}$.

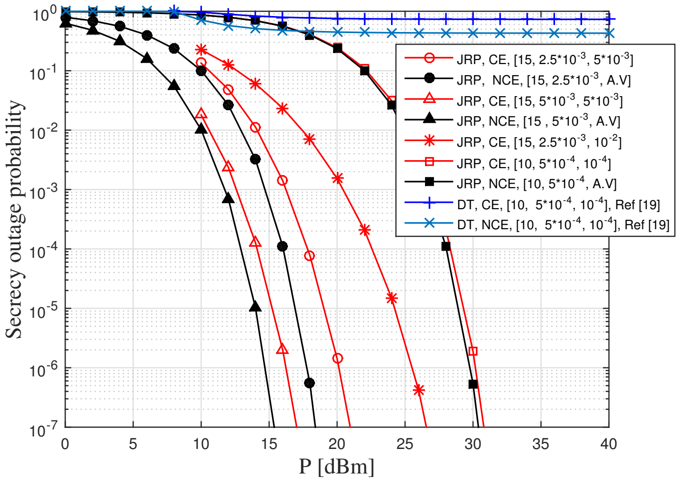

Fig. 7: The effect of P on the SOP in multiple-untrusted relaying network when $p_{\rm L} = 0.7$. The elements in the vector [a, b, c] respectively express $a = G_{\rm rd}$ [dB], $b = \lambda_{\rm r}$ $(1/m^2)$, $c = \lambda_{\rm e}$ $(1/m^2)$. The notation ‘A.V’ states any value for the density of Eves.

- By increasing the density of relays $\lambda_{\rm r}$, the ESR performance grows for both the NCE and CE scenarios. This is because as the number of relays increases, the communication network gets more chance to select a relay with stronger second hop channel. We can further examine the effect of $\lambda_{\rm r}$ on the ESR by considering large $\lambda_{\rm r}$. Fig. 6 depicts that the ESR performance curves tends to saturation for larger $\lambda_{\rm r}$. This is because increasing $\lambda_{\rm r}$ causes $F_{\gamma_{\rm best}}(x)$ to decrease in (47), such that for very large $\lambda_{\rm r}$, $F_{\gamma_{\rm best}}(x) \to 0$, and consequently, we get $L_{{\rm F}_{\gamma_{\rm best}}({\rm x})}(s) \to 1$. Therefore, according to (49), the ESR will depend only on $L_{I_{\rm e}}(s)$ which is not depend on the density of relays. This states that for very large $\lambda_{\rm r}$, only the density of Eves has impact on the ESR performance.
- As the LoS probability $p_{\rm L}$ grows, the ESR performance improves. For example, when we consider $\lambda_{\rm r} = 10^{-3}$ and $f_{\rm c} = 28$ GHz for both the NCE and CE scenarios, by increasing the LoS probability from $p_{\rm L} = 0$ to $p_{\rm L} = 0.5$, the network enjoys from 3.2 bits/s/Hz secrecy rate enhancement. This observation reveals the remarkable importance of deploying relay nodes in mmWave communications.

Fig. 7 describes the SOP versus P for both the NCE and CE scenarios. We consider the outage threshold of $R_{\rm t} = 1$ bit/channel use for the secrecy rate calculation and set the gains of antennas as shown in Table II. As concluded from Fig. 7, the performance of NCE scenario is more comparable to the CE scenario. This figure also illustrates that the SOP significantly reduces as $\lambda_{\rm r}$ increases. This is because as $\lambda_{\rm r}$ becomes higher, the probability of selecting the best channel increases and thus, the SOP decreases. Finally, we can observe from Fig. 7 that the SOP substantially degrades upon increasing $\lambda_{\rm e}$. The reason for this observation is that as the number of Eves increases, more confidential information is captured by the Eves. As can be readily seen from this figure, unlike DT scheme that the SOP performance converges to a nonzero constant at high P, the SOP of the proposed JRP scheme for both NCE and CE scenarios reaches zero at high P regime.

In Fig. 8, we plot the ESR versus the OPA factor λ for a single-relay network at $P = 30$ dBm and $p_{\rm L} = 1$. For the CE scenario, two densities of Eves, i.e., $\lambda_{\rm e} = 2.5 \times 10^{-4}$ and $\lambda_{\rm e} = 5 \times 10^{-3}$ are considered. As shown in Fig. 8, each curve has an extreme point which maximizes the ESR. It can also be observed that the CE curves are lower than the NCE ones which is due to the eavesdropping attacks of the passive Eves in the CE scenario. Fig. 8 also states that as $\lambda_{\rm e}$ increases the extreme point of the CE scenario moves toward zero. This is because as the number of passive Eves grows, more AN power must be allocated by the source for protecting the message signal. This means the power allocation factor λ

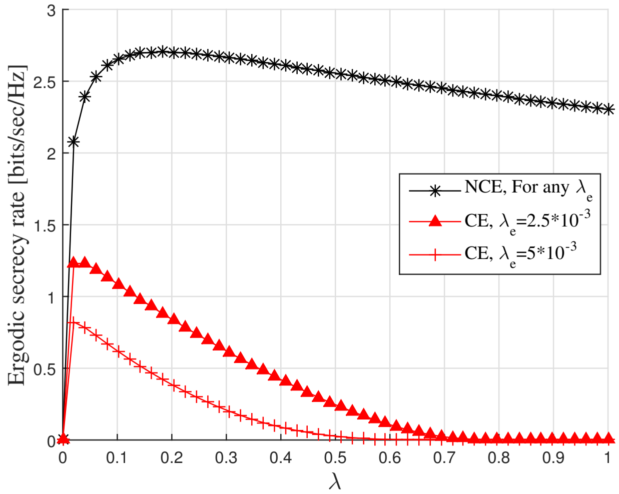

Fig. 8: The effect of the source's power allocation factor λ on the ESR in single-untrusted relaying network for both NCE and CE scenarios when $p_{\mathrm{L}} = 1$.

that determines the ratio of power dedicated to information signal approaches zero.

VI. Conclusions

Secure AF relaying was investigated in the presence of multiple untrusted relays, blockages and small-scale fading. The positions of relays and passive Eves were modeled by homogeneous PPPs, and the best relay was chosen for secure communications. A new JRP technique was proposed for security enhancement in both NCE and CE scenarios and new closed-form expressions were derived for the ESR and SOP as security metrics. It was shown that the optimal sharing of the transmit power between the message signal and AN beneficially improves the ESR. The results highlighted the impact of different mmWave carrier frequencies, transmit powers, node densities and antenna gains on the secrecy performance.

References

[1] M. Ragheb and S. M. Safavi Hemami, "Secure communication for millimeter-wave systems with randomly located non-colluding eavesdroppers," in *Proc. 28th Iranian Conference on Electrical Engineering (ICEE)*. Tabriz: IEEE, Aug. 2020, pp. 1–6.

[2] K. L.-M. Ang and J. K. P. Seng, "Application specific Internet of Things (ASIoTs): Taxonomy, applications, use case and future directions," *IEEE Access*, vol. 7, pp. 56 577–56 590, May 2019.

[3] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *in Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

[4] Y. Zhu, L. Wang, K.-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, May 2017.

[5] Z. Kong, J. Song, C. Wang, H. Chen, and L. Hanzo, "Hybrid analog-digital precoder design for securing cognitive millimeter wave networks," *IEEE Trans. Inf. Forens. Sec.*

[6] M. Riza Akdeniz, Y. Liu, M. K. Samimi, S. Sun, S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 164–1179, Jun. 2014.

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

[8] S. Biswas, S. Vuppala, J. Xue, and T. Ratnarajah, "On the performance of relay aided millimeter wave networks," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 576–588, Apr. 2016.

[9] ——, "An analysis on relay assisted millimeter wave networks," in *in Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[10] K. Belbase, Z. Zhang, H. Jiang, and C. Tellambura, "Coverage analysis of millimeter wave decode-and-forward networks with best relay selection," *IEEE Access*, vol. 6, pp. 22 670–22 683, Apr. 2018.

[11] Y. Cai, K. Xu, A. Liu, M. Zhao, B. Champagne, and L. Hanzo, "Two-Timescale Hybrid Analog-Digital Beamforming for mmWave Full-Duplex MIMO Multiple-Relay Aided Systems," *IEEE J. Sel. Commun.*, vol. 38, no. 9, pp. 2086–2103, Sept. 2020.

[12] K. Belbase, C. Tellambura, and H. Jiang, "Two-way relay selection for millimeter wave networks," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 201–204, Jan. 2018.

[13] 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, Mar. 2019.

[14] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, Mar. 2017.

[15] Z. Yulong, J. Z. Xianbin Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *in Proc. IEEE*, vol. 104, no. 9, p. 1765—1727, Sept. 2016.

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

[17] Y. Ju, H.-M. Wang, T.-X. 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, Apr. 2018.

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

[19] Y. Yang, M. Ma, S. A¨ıssa, and L. Hanzo, "Physical-layer secret key generation via CQI-mapped spatial modulation in multi-hop wiretap Ad-Hoc networks," *IEEE Trans. Inf. Forens. and Security*, vol. 16, pp. 1322–1334, Oct. 2021.

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

[21] S. Wu, R. Atat, N. Mastronarde, and L. Liu, "Improving the Coverage and Spectral Efficiency of Millimeter-Wave Cellular Networks Using Device-to-Device Relays," *IEEE Trans. Wireless Commun.*, vol. 66, no. 5, pp. 2251–2265, May 2018.

[22] ——, "Coverage analysis of D2D relay-assisted millimeter-wave cellular networks," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*. San Francisco, CA, USA: IEEE, Mar. 2017, pp. 1–6.

[23] A. Kuhestani, P. L. Yeoh, and A. Mohammadi, "Optimal power allocation and secrecy sum rate in two-way untrusted relaying," in *in Proc. IEEE Global Communications Conference*. IEEE, Dec. 2017, pp. 1–6.

[24] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[25] M. Ragheb and S. M. Safavi Hemami, "Secure transmission in large-scale cooperative millimeter-wave systems with passive eavesdroppers," *IET Commun*, vol. 14, no. 1, pp. 37–46, Jan. 2020.

[26] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[27] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *in Proc. IEEE Global Telecommunications Conference*. New Orleans, LA: IEEE, Dec. 2008, pp. 1–5.

[28] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[29] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE wireless commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jan. 2014.

[30] M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jamming-resilient frequency hopping-aided secure communication for Internet-

of-Things in the presence of an untrusted relay," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6771–6785, Oct. 2020.

[31] H. Saedi, A. Mohammadi, and A. Kuhestani, "Characterization of untrusted relaying networks in the presence of an adversary jammer," *Wireless Networks*, vol. 26, no. 3, pp. 2113–2124, Jun. 2019.

[32] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 463–466, Mar. 2015.

[33] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[34] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," *IEEE Trans. Inf. Forens. and Security*, vol. 13, no. 2, pp. 341–355, Feb. 2017.

[35] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid Opportunistic Relaying and Jamming With Power Allocation for Secure Cooperative Networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[36] H.-M. Wang, Y. Xu, K.-W. Huang, Z. Han, and T. A. Tsiftsis, "Cooperative Secure Transmission by Exploiting Social Ties in Random Networks," *IEEE Trans. Wireless Commun.*, vol. 66, no. 8, pp. 3610–3622, Aug. 2018.

[37] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy Transmission With a Helper: To Relay or to Jam," *IEEE Trans. Inf. Forens. and Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[38] M. Letafati, A. Kuhestani, and H. Behroozi, "Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things," *IEEE Trans. Inf. Forens. and Security*, vol. 15, pp. 2856–2868, Mar. 2020.

[39] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Trans. Commun.*, Mar. 2020.

[40] M. Moradikia, H. Bastami, A. Kuhestani, H. Behroozi, and L. Hanzo, "Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments," *IEEE Access*, vol. 7, pp. 116 942–116 964, Aug. 2019.

[41] W. Wang, T. Kah Chan, and K. H. Li, "Relay Selection for Secure Successive AF Relaying Networks With Untrusted Nodes," *IEEE Trans. Inf. Forens. and Security*, vol. 11, no. 11, pp. 2466–2476, Nov. 2016.

[42] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. New York, NY: Elsevier, 2007.

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

[44] A. Alkhateeb, Y.-H. Nam, M. S. Rahman, J. C. Zhang, and R. W. Heath Jr., "Initial beam association in millimeter wave cellular systems: analysis and design insights," *IEEE trans. Wireless Commun.*, vol. 16, no. 5, pp. 2807–2821, May. 2017.

[45] 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. Commun.*, vol. 33, no. 10, pp. 2196–2211, Oct. 2015.

[46] A. Ghosh, T. A. Thomas, M. C. Cudak, R. Ratasuk, P. Moorut, F. W. Vook, T. S. Rappaport, G. R. MacCartney, S. Sun, and S. Nie, "Millimeter-wave enhanced local area systems: A high-data-rate approach for future wireless networks," *IEEE J. Sel. Commun.*, vol. 32, no. 6, pp. 1152–1163, Jun. 2014.

[47] T. Zheng, H. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, Jun. 2014.

[48] K. A. Hamdi, "A useful lemma for capacity analysis of fading interference channels," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 411–416, Feb. 2010.