IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 10, 2019, accepted July 27, 2019, date of publication August 5, 2019, date of current version September 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2933231

Secure mmWave Communication Using UAV-Enabled Relay and Cooperative Jammer

RUIQIAN MA[1], WEIWEI YANG[1], (Member, IEEE), YU ZHANG[1,2], JUE LIU[1,3], AND HUI SHI[1]

[1]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]Sixty-third Research Institute, National University of Defense Technology, Nanjing 210007, China
[3]College of Information Science and Engineering, Nanjing Audit University Jinshen College, Nanjing 210023, China

Corresponding author: Weiwei Yang (wwyang1981@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 61471393 and Grant 61771487.

ABSTRACT Communication assisted by unmanned aerial vehicles (UAVs) has been regarded as an effective technique for reliability improvement in both military and civilian domains, whereas it also makes the information vulnerable to passive eavesdropping due to its wide broadcast. In this paper, we investigate the secure millimeter wave (mmWave) communication assisted by multiple UAV-enabled relays and jammers, where exist multiple randomly distributed eavesdroppers on the ground. Leveraging the models of 3D-antenna gain and stochastic geometry, new closed-form expressions of secrecy outage probability are derived on the basis of the opportunistic relay selection scheme involving the characteristics of air-to-ground channel, and the secrecy improvement is demonstrated when the relay density increases. In addition, a cooperative jamming scheme, where a part of UAVs transmit the jamming signals, is designed to degrade the qualities of eavesdropping channels and further enhance physical layer security. The simulation results show the impacts of different system parameters on secrecy outage probability and verify our analysis. It's also revealed that there exist the optimal attitude of UAVs, jamming power and density of jammers for achieving the best secrecy performance.

INDEX TERMS UAV, millimeter wave, relay, physical layer security, secrecy outage probability.

I. INTRODUCTION

Recently, with the explosive growth of wireless data traffic, it has been becoming an emergency to develop the high data-rate transmission in wireless communication systems. As a consequence, millimeter wave (mmWave) technique has been emerging as an important solution to improve the data rate of wireless networks due to its sufficient frequency resources [1], [2]. However, because of the high path-loss and the sensitivity to blockages, mmWave communication links may be interrupted, especially in a complex and dynamic environment [3], [4]. To this end, operating an unmanned aerial vehicle (UAV) as relay in the air has been studied for disconnection recovery and system performance improvement in mmWave communication networks [5]–[7].

Although there are such advantages by adopting UAV-enabled relays in mmWave networks, it also makes the signals prone to passive eavesdropping attack due to its wide coverage and the broadcast nature of wireless channels. Meanwhile, taking into account the prevalence of sensitive and confidential information in wireless networks, it's one of the top priorities to provide a secure service in UAV-enabled relaying networks. Conventional upper-layer security method mainly based on computational complexity by using encryption protocols [8]. As a supplement of conventional cryptographic techniques, physical layer security has emerged as a powerful measure to protect confidential information from wiretapping by exploiting the randomness of wireless channel and its impairments, e.g., noise and interference [9]. There are kinds of techniques, including directional antenna [10], cooperative jamming [11] and relay [12], having been used to improve the secrecy performance in wireless communication networks. However, the researches of physical layer security in UAV-enabled mmWave relaying networks are few, and there still exist many problems waiting to be solved. For example, if the cooperative jamming can enhance the physical layer security in UAV-enabled mmWave relaying networks and how can we improve it?

The associate editor coordinating the review of this article and approving it for publication was Tiago Cruz.

A. RELATED WORK AND MOTIVATION

At present, there have been a significant amount of works focusing on mmWave relaying networks on the ground, and the performance analysis and optimization of them have been investigated [13]–[18]. More specifically, considering a relaying network where the sources and relays have been modeled as two independent Possion point processes (PPPs), the coverage probability and transmission capacity have been analyzed for both best path and relay selection schemes [13]. Meanwhile, applying energy harvesting technology to the relays, the coverage probability constrained with harvesting power has been also examined in [14]. Additionally, using directional antenna at relay can enhance the reliability of mmWave networks, and the impact of directional antenna's beamwidth and self-interference on maximum achievable rate has been demonstrated in [15]. In [16], taking into account the co-channel interferences at the relays with directional antennas, the outage performance of mmWave relaying systems has been examined. On the other hand, [17] has considered the decode-and-forward relaying systems at mmWave band, and has provided a low-complexity resource allocation algorithm, which can optimize the average outage probability. Xue *et al*. [18] has investigated the hybrid precoding design in a mmWave relaying system for improving the secrecy rate.

Recently, due to the low cost, high mobility and flexible deployment of UAV, deploying UAV-enabled relays in wireless communication networks has emerged as an effective method for performance improvement [19]–[22]. To be specific, the channel model of multi-hop UAV-enabled relaying systems at sub-6GHz band have been studied in [19], and the communication performances such as outage probability, average channel capacity and bit error rate have been examined. Considering a cognitive radio system where the primary and secondary users communicate to the base station via the same UAV-enabled relay, the achievable rates have been analyzed in [21]. In [22], the authors have compared the outage probability of UAV-enabled relaying networks for multi-hop single link and multiple dual-hop links schemes. However, all above mentioned works only have investigated the system performances without security consideration.

Physical layer security can protect confidential information with lower computation complexity, and an increasing attention has been paid to the application of physical layer security in UAV-enabled relaying networks [10], [23]–[25]. Specifically, in [23], the secrecy outage probability in microwave communication networks with several UAV-enabled relays and eavesdroppers has been examined. Considering a microwave communication system, the average secrecy rate for mobile relaying scheme has been investigated in [24]. Recently, the physical layer security also has been investigated in mmWave networks. Sun *et al.* [25] has investigated the physical layer security of the mmWave communication networks containing one fixed UAV relay with the directional antenna. In addition, transmitting jamming has been regarded as an effective method for secrecy enhancement in mmWave networks, and it's worth mentioning that the UAVs can be used not only for relaying message signals, but also for sending jamming. In [10], considering a mmWave communication network, the UAVs are deployed as jammers to confound the eavesdroppers on the ground, and the average secrecy rate in the considered network has been analyzed.

Contrasting to the existing works, the secure communication in the mmWave networks assisted by multiple UAV-enabled relays and jammers is still an open issue. First, by considering the characteristics of UAV communication channels, the opportunistic relay selection scheme subjected to the channel quality of the air-to-ground link between source and relay still waits to be investigated. In addition, how to enhance the secrecy performance in the UAV-enabled mmWave networks by using cooperative jamming is a challenging work.

B. CONTRIBUTION

In this paper, we investigate the secure mmWave communication using UAV-enabled relay and cooperative jammer. Our main contributions are summarized as follows:

- Considering a ground mmWave network assisted by multiple UAV-enabled relays in the presence of multiple randomly distributed eavesdroppers on the ground, the effect of cooperative jamming on secrecy performance are first investigated. Specifically, the locations of relaying UAVs, jamming UAVs and ground eavesdroppers are modeled as independent PPPs. Then, the opportunistic relay selection scheme are investigated by considering the characteristics of air-to-ground channels for decode-and-forward relay strategy. Furthermore, the jamming UAVs are adopted to send jamming signals for degrading the qualities of eavesdropping channels.
- The closed-form expression of secrecy outage probability is derived in the considered networks without cooperative jamming. Furthermore, by using the tools of numerical inversion of Laplace transforms and Euler summation, a tight approximated expression of secrecy outage probability for cooperative jamming scheme is derived. The Monte Carlo simulations are presented to verify our derivations and reveal that secrecy performance has obvious positive correlation with the relay density, the antenna number and the transmitting power of message signals.
- Analyzing the simulation results, we find that the secrecy outage probability can be improved by adopting higher UAV attitude when the relay density is small, and the result is opposite in large relay density situations. Additionally, the enhancement of physical layer security is testified for cooperative jamming scheme. Furthermore, there exist the optimal attitude of UAVs, jamming power and density of jamming UAVs for achieving the best secrecy outage probability.

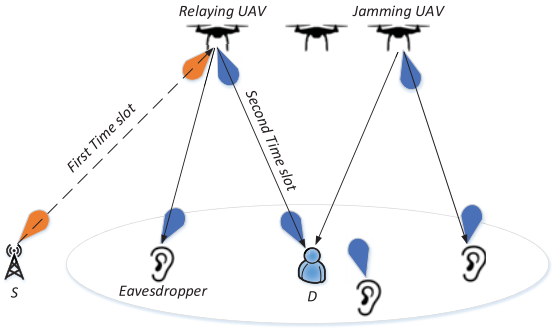


FIGURE 1. System model.

The remainder of this article is organized as follows. The system model is introduced in Section II. In Section III and Section IV, we examine the secrecy outage probability in the considered system without and with cooperative jamming. Then, the simulation results are presented in Section V. Finally, the concluding remarks are provided in Section VI.

II. SYSTEM MODEL

We consider secure communication in the UAV-enabled mmWave relaying networks, as depicted in Fig. 1. The direct link from source (S) to destination (D) is disconnected and the communication occurs via a selected UAV-enabled relay, which is denoted as R. The half-duplex mode is adopted at R. Specifically, S first transmits the messages to R, and then R forwards its received signals to D by using decode-and-forward strategy. Meanwhile, there are multiple ground eavesdroppers distributing around D and locating out of the coverage area of S, meaning that the eavesdroppers only wiretap the information from R, similar to [26]–[28]. The distribution of all UAVs follows a homogeneous PPP Φ_U with density λ_U, and the locations of eavesdroppers are modeled as an independent PPP Φ_E with density λ_E. We assume that each node equips multi-antenna, which is modeled by the 3D antenna pattern. Moreover, all UAVs are deployed inside a circular disc of radius $\mathcal{X}$ and at the same altitude H [10]. Both the transmission schemes without and with cooperative jamming are considered. For the first scheme, the UAVs can only forward the signals received from S to D. For the second scheme, we divide the PPP Φ_U into two independent PPPs Φ_U^R and Φ_U^I with densities $\lambda_R = \varepsilon\lambda_U$ and $\lambda_I = (1-\varepsilon)\lambda_U$, where ε is the cooperative jamming factor. The UAVs in Φ_U^R are only used to relay message signals while the UAVs in Φ_U^I only transmit jamming signals. In the following, we will further describe the model of this paper in detail.

A. 3D ANTENNA GAIN

We assume that R equips with N_R antennas, and each ground node has N_l antennas, where $l \in \{S, D, E\}$ denotes S, D and eavesdroppers. We adopt a 3D sectored model by considering the UAVs' altitude [10], [25]. In particular, the directional antenna gain and the associated probability of R and ground nodes (D or eavesdropper) can be given as

$$G_i^R = \begin{cases} G_M^R, & P_M^R = \dfrac{\theta_a^R}{\theta_{\max}} \cdot \dfrac{\theta_d^R}{\theta_{\max}} \\ G_m^R, & P_m^R = 1 - \dfrac{\theta_a^R}{\theta_{\max}} \cdot \dfrac{\theta_d^R}{\theta_{\max}}, \end{cases} \tag{1}$$

and

$$G_i^l = \begin{cases} G_M^l, & P_M^l = \dfrac{\theta_a^l}{\pi} \cdot \dfrac{\theta_d^l}{\pi - \theta_d^l} \\ G_m^l, & P_m^l = 1 - \dfrac{\theta_a^l}{\pi} \cdot \dfrac{\theta_d^l}{\pi - \theta_d^l} \end{cases}, l \in \{D, E\}, \tag{2}$$

where $\theta_a^R\left(\theta_a^l\right)$ is the half-power beamwidth in the azimuth, $\theta_d^R\left(\theta_d^l\right)$ is the half-power beamwidth in the elevation and $\theta_{\max} = 2 \cdot \arctan\left(\mathcal{X}/H\right)$ is the max turning angle of R's antenna beam.

Similar to [29], [30], we assume perfect beam alignment between the legitimate transmitter and receiver, so the antenna gains of $S \to R$ and $R \to D$ links are $G_{SR} = G_M^S G_M^R$ and $G_{RD} = G_M^R G_M^D$ respectively. At the same time, the antenna gain of the link between R and the most malicious eavesdropper are given as

$$G_{RE} = \begin{cases} G_M^R G_M^E, & P_{MM}^{RE} = P_M^R P_M^E \\ G_M^R G_m^E, & P_{Mm}^{RE} = P_M^R P_m^E \\ G_m^R G_M^E, & P_{mM}^{RE} = P_m^R P_M^E \\ G_m^R G_m^E, & P_{mm}^{RE} = P_m^R P_m^E, \end{cases} \tag{3}$$

where P_{ij}^{RE} denotes the probability that the antenna gain $G_i^R G_j^E$ $(i, j \in \{m, M\})$ occurs.

B. BLOCKAGE MODEL

It's necessary to take into account the effect of blockage in mmWave networks. Considering the blockage effect of air-to-ground links, the occurrence probabilities of line-of-sight (LOS) and non-line-of-sight (NLOS) links are given respectively as [31]

$$p_L(r) = \frac{1}{1 + a\exp\left(-b\left(\arctan(\frac{H}{r}) - a\right)\right)}, \tag{4}$$

and

$$p_N(r) = 1 - p_L(r), \tag{5}$$

where r is the horizontal distance from the UAV node to the ground receiver, and a and b are the constant parameters depend on the environment.

C. PATH-LOSS MODEL

Just as [32] and [33], we use different path-loss laws for LOS link and NLOS link. Let the link be of length d, we can calculate its path-loss as

$$L(d) = \begin{cases} C_L d^{-\alpha_L}, & \text{if the link is LOS} \\ C_N d^{-\alpha_N}, & \text{if the link is NLOS,} \end{cases} \tag{6}$$

where $C_L = 10^{-\frac{\zeta_L}{10}}$ and $C_N = 10^{-\frac{\zeta_N}{10}}$ can be regarded as the intercepts of LOS and NLOS links, α_L and α_N are the LOS

and NLOS path-loss exponents. Specifically, the parameters C_j and α_j ($j \in \{L, N\}$) are determined with the frequency of carrier wave.

D. SMALL-SCALE FADING

We assume that the small-scale fading for each link follows independent Nakagami-m fading, which has been regarded as a general model of intensity distribution for rapid fading [34]–[36]. After that, the small-scale fading powers between S and R, R and D and R and eavesdropper are expressed as $|h_{SR}|^2$, $|h_{RD}|^2$ and $|h_{RE}|^2$. Under the Nakagami-m fading assumption, $\left|h_{ij}\right|^2$ ($i, j \in \{S, R, E\}$) follows normalized Gamma random variable. We use N_L and N_N to represent the fading parameters of LOS and NLOS link respectively. Then, if a link is LOS, the small-scale channel gain is $\left|h_{ij}\right|^2 \sim \Gamma(N_L, 1)$, and for a NLOS link, $\left|h_{ij}\right|^2 \sim \Gamma(N_N, 1)$.

E. RELAY SELECTION SCHEME

For a potential UAV-enabled relay, it must successfully decode the signals received from S. Therefor, we consider an opportunistic relay selection scheme with two stages: 1) We select a set of UAV-enabled relays that the channel capacities of the links from S are above the threshold C_{th1}, and denote the set as $\hat{\Phi}\left(\hat{\Phi} \in \Phi_U\right)$. Each node in $\hat{\Phi}$ can successfully decode the S's messages and forward the decoding messages to D. It's obvious that the density of available relays depends on the distance from S and whether the communication link is LOS or NLOS. 2) Then, we select an UAV-enabled relay which can offer the lowest path-loss to D from the decoding set $\hat{\Phi}$. According to the blockage and path-loss model, the selected relay provides the minimum length of LOS or NLOS link to D.

In this paper, we use polar coordinate system to facilitate the analysis. Then, we set the coordinate origin at D, and S locate at $(d_{SD}, \pi, 0)$. After that, for an UAV-enabled relay locate at (r, θ, H), the distance from R to D can be calculated by $d_{RD} = \sqrt{r^2 + H^2}$, and the length of the link between S and R can be written as $d_{SR} = \sqrt{r^2 + d_{SD}^2 - 2rd_{SD}\cos(\theta - \pi) + H^2}$.

III. SECRECY PERFORMANCE WITHOUT COOPERATIVE JAMMING

In this section, we select an UAV to relay the signals received from S and the other UAVs keep silent. On the basis of the above assumptions on the antenna gain, the relay deployment and the air-to-ground channel model, the received signal to noise (SNR) at a legitimate receiver can be given as

$$\gamma_{ij} = \frac{P_t G_{ij} L\left(d_{ij}\right)\left|h_{ij}\right|^2}{N_0}, \quad i \in \{S, R_x\}, \ j \in \{R_x, D\}, \tag{7}$$

where R_x denotes the available relay at location x, P_t is the transmit power of both S and R_x, d_{ij} is the length of the link between two legitimate nodes, and N_0 is the noise power.

According to the system model in Section II, the eavesdroppers are out of the coverage area of S and only eavesdrop the information from relay. In addition, we assume that all eavesdroppers are independent and cannot exchange information with each other [25]. Then, the SNR at the most malicious eavesdropper can be written as

$$\gamma_E = \max_{e \in \Phi_E}\left\{\frac{P_t G_{RE_e} L\left(d_{RE_e}\right)\left|h_{RE_e}\right|^2}{N_0}\right\}, \tag{8}$$

where G_{RE_e} is the antenna gain between R and the eavesdropper e, which can be obtained by (3), and d_{RE_e} and $\left|h_{RE_e}\right|^2$ are the distance and small-scale fading gain of the link from R to the eavesdropper e.

A. PRELIMINARY ANALYSIS

Prior of the secrecy evaluation, we first give the mathematical preliminaries of the opportunistic relay selection scheme, and the decoding set of UAV-enabled relay is defined as

$$\hat{\Phi} = \left\{x \in \Phi_U, \log_2\left(1 + \gamma_{SR_x}\right) > C_{th1}\right\}, \tag{9}$$

where γ_{SR_x} is the received SNR of the available relay located at x. No doubt, γ_{SR_x} is a function of the distance between S and R_x, and the probability of containing in $\hat{\Phi}$ also depends on the location of the relay R_x. Particularly, the nodes are more likely to be included in $\hat{\Phi}$ if they are closed to S. Also due to the fact that the channels between S and different R_x are independent, the available relay set $\hat{\Phi}$ is an independent thinning of the initial process Φ_U. Thus, $\hat{\Phi}$ is an inhomogeneous PPP which the node density is location dependent [37]. Furthermore, we can derive the density of the point process as

$$\begin{aligned}
\hat{\lambda}(x) &= \lambda_U \Pr\left(\log_2\left(1 + \gamma_{SR_x}\right) > C_{th1}\right) \\
&= \lambda_U \Pr\left(\frac{P_t G_{SR_x}\left|h_{SR_x}\right|^2 L\left(d_{SR_x}\right)}{N_0} > 2^{C_{th1}} - 1\right) \\
&= \lambda_U \Pr\left(\left|h_{SR_x}\right|^2 > \frac{N_0\left(2^{C_{th1}} - 1\right)}{P_t G_{SR_x} L\left(d_{SR_x}\right)}\right) \\
&\overset{a}{=} \lambda_U \sum_{j \in (L,N)} p_j(r) \frac{\Gamma\left(N_j, \frac{N_0\left(2^{C_{th1}} - 1\right) d_{SR_x}^{\alpha_j}}{P_t G_{SR_x} C_j}\right)}{\Gamma\left(N_j\right)},
\end{aligned} \tag{10}$$

where step (a) is due to $|h_{SR}|^2 \sim \Gamma\left(N_j, 1\right)$ for $j \in \{L, N\}$, r is the horizontal distance between R_x and the origin S, and d_{SR_x} is the distance between S and R_x.

In order to maximize the receiving signal quality of D, we assume that D associates with the UAV-enabled relay offering the smallest path loss to D. This means that the selected relay is the nearest one in Φ_L or Φ_N, where Φ_j is the LOS/NLOS available relay point process with density of $p_j(r)\,\hat{\lambda}(x)$ ($j \in \{L, N\}$).

Lemma 1: Denoting the horizontal distance between D and the nearest UAV-enabled relay in Φ_j as r_j ($j \in \{L, N\}$), the probability distribution functions (PDF) of r_j is given as

$$f_{r_j}(y) = W \sum_{k=1}^{T} y p_j(y)\,\hat{\lambda}(y, \theta_k)\, e^{v_j(y)} \sqrt{\theta_k\left(2\pi - \theta_k\right)}, \tag{11}$$

$$A_L = W \sum_{i=0}^{T} e^{\nu_N\left(\max\left(0,\sqrt{\left(\frac{C_N}{C_L}\right)^{\frac{2}{\alpha_N}}\left(y_i{}^2+H^2\right)^{\frac{\alpha_L}{\alpha_N}}-H^2}\right)\right)} f_{r_L}(y_i)\sqrt{y_i(\chi-y_i)}, \tag{14}$$

where $\theta_k = \pi\left(1+\cos\frac{(2k-1)\pi}{2T}\right)$, and $\nu_j(y)$ is given as

$$\nu_j(y) = -W^2 \sum_{h=1}^{T} p_j(r_h)\, r_h^{\frac{3}{2}} \sqrt{y-r_h} \times \sum_{i=1}^{T} \hat{\lambda}(r_h,\theta_i)\sqrt{\theta_i(2\pi-\theta_i)}, \tag{12}$$

where $W = \frac{\pi}{T}$, $\theta_i = \pi\left(1+\cos\frac{(2i-1)\pi}{2T}\right)$, $r_h = \frac{y}{2}\left(1+\cos\frac{(2h-1)\pi}{2T}\right)$, and T is the number of the cumulative times by using Gauss-Chebyshev integration.

Proof: See Appendix A.

Lemma 2: Giving that D associates with a LOS UAV-enabled relay, the conditional PDF of r_L is

$$g_{r_L}(y) = \frac{f_{r_L}(y)}{A_L} e^{\nu_N\left(\max\left(0,\sqrt{\left(\frac{C_N}{C_L}\right)^{\frac{2}{\alpha_N}}\left(y^2+H^2\right)^{\frac{\alpha_L}{\alpha_N}}-H^2}\right)\right)}, \tag{13}$$

where A_L is the probability that D associates with a LOS relay given as (14) at the top of the this page, and $y_i = \frac{\chi}{2}\left(1+\cos\frac{(2i-1)\pi}{2T}\right)$.

Proof: See Appendix B.

Accordingly, given that D observes at least one NLOS UAV-enabled relay, the conditional PDF of r_N is

$$g_{r_N}(y) = \frac{f_{r_N}(y)}{A_N} e^{\nu_L\left(\min\left(\chi,\sqrt{\left(\frac{C_L}{C_N}\right)^{\frac{2}{\alpha_L}}\left(y^2+H^2\right)^{\frac{\alpha_N}{\alpha_L}}-H^2}\right)\right)}, \tag{15}$$

where $A_N = 1 - A_L$ is the probability that an NLOS relay is selected.

B. SECRECY OUTAGE PROBABILITY

In this subsection, we investigate the secrecy outage probability of the UAV-enabled mmWave relaying networks by considering the effect of the most malicious eavesdropper on the ground. Specifically, the selected UAV-enabled relay R provides the lowest path-loss to D, which means that R is the closest LOS or NLOS relay from D. And the PDF of the horizontal distance between R and D is derived detailly in above Subsection III-A *Preliminary Analysis*.

Then, according to aforementioned system model, the eavesdroppers only can wiretap information from the UAV-enabled relay. The secrecy outage probability can be derived as

$$\begin{aligned} p_{out} &= 1 - \Pr\left(\log_2(1+\gamma_{RD}) - \log_2(1+\gamma_E) > C_{th2}\right) \\ &= 1 - W \sum_{j\in\{L,N\}} A_j \int_0^{\chi} g_{r_j}(r) \\ &\quad \times \int_0^{\infty}\int_{\beta(x)}^{\infty} f_{\gamma_{RD,j}}(y) f_{\gamma_E}(x)\,dy\,dx \\ &= 1 - W \sum_{j\in\{L,N\}} A_j \sum_{i=1}^{T} g_{r_j}(r_i)\sqrt{r_i(\chi-r_i)} \\ &\quad \times \int_0^{\infty} F_{\gamma_E}(x) f_{\gamma_{RD,j}}(\beta(x))\beta'(x)\,dx \\ &\overset{b}{\approx} 1 - W^2 \sum_{j\in\{L,N\}} A_j \sum_{i=1}^{T} g_{r_j}(r_i)\sqrt{r_i(\chi-r_i)} \\ &\quad \times \sum_{k=1}^{T} \sqrt{x_k(\mu-x_k)} F_{\gamma_E}(x_k) f_{\gamma_{RD,j}}(\beta(x_k))\beta'(x_k), \end{aligned} \tag{16}$$

where $F_{\gamma_E}(\cdot)$ is the cumulative probability function (CDF) of γ_E, $f_{\gamma_{RD,j}}(\cdot)$ is the PDF of γ_{RD} for LOS or NLOS $R \to D$ link, $r_i = \frac{\chi}{2}\left(1+\cos\frac{(2i-1)\pi}{2T}\right)$, $x_k = \frac{\mu}{2}\left(1+\cos\frac{(2k-1)\pi}{2T}\right)$, $\beta(x) = 2^{C_{th2}}(x+1)-1$, step (b) is due to that the maximal SNR at the most malicious eavesdropper is approximated as $\mu = \frac{5P_t N_j G_M^R G_M^E L(H)}{N_0}$, and $j \in \{L, N\}$ represents that the LOS or NOLS relay is selected.

In order to calculate the secrecy outage probability, we need to obtain the distributions of the received SNRs at D and the most malicious eavesdropper. The PDF of $\gamma_{RD,j}$ is derived as

$$\begin{aligned} f_{\gamma_{RD,j}}(x) &= \left[\Pr\left(|h_{RD}|^2 < \frac{N_0 x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)\right]' \\ &= \frac{1}{\Gamma(N_j)}\left(\gamma\left(N_j, \frac{N_0 x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)\right)' \\ &\overset{c}{=} e^{-\frac{N_0 x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}} \left(\sum_{m=1}^{N_j-1} \frac{x^{m-1}}{m!}\left(\frac{N_0 d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)^m \right. \\ &\quad \left. \times \left(\frac{N_0 x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j} - m\right) + \frac{N_0 d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right), \end{aligned} \tag{17}$$

where step (c) is due to [38, eq.(8.352.1)].

Without loss of generality, we only take into account the eavesdroppers inside a circular area, and for simplicity, the radius is also set as χ. Then, the CDF of γ_E can be given by

$$\begin{aligned} &F_{\gamma_E}(x) \\ &= \Pr\left(\max_{e\in\Phi_E} \gamma_{E_e} < x\right) \\ &= E_{\Phi_E}\left[\prod_{e\in\Phi_E} \Pr\left(\gamma_{E_e} < x\right)\right] \end{aligned}$$

$$\varpi_j(V,x) = \int_0^{\chi} p_j(r)\Pr\left(\gamma_{e,j} \geq x \,|\, \Phi_{E,j}\right) rdr = \int_0^{\chi} \left(\frac{\Gamma\left(N_j, \frac{N_0 x d_{RE}^{\alpha_L}}{P_t V C_j}\right)}{\Gamma\left(N_j\right)}\right) p_j(r)\, rdr$$
$$= \frac{1}{\Gamma\left(N_j\right)} \sum_{i=0}^{T} W p_j(r_i) \Gamma\left(N_j, \frac{N_0 x\left(r_i^2+H^2\right)^{\frac{\alpha_j}{2}}}{P_t V C_j}\right) r_i \sqrt{r_i(\chi - r_i)}. \quad (19)$$

$$\stackrel{d}{=} \exp\left(-\lambda_E \int_{\mathcal{R}^2} 1 - \Pr\left(\gamma_{E_e} < x\right) de\right)$$
$$= \exp\left(-2\pi\lambda_E \sum_{G_{RE}} \Pr\left(G_{RE} = V\right) \sum_{j\in\{L,N\}} \varpi_j(V,x)\right), \quad (18)$$

where step (d) is due to the generation function of PPP Φ_E [39], and $\varpi_j(V,x)$ is given by (19), as shown at the top of the next page.

Finally, we can obtain the secrecy outage probability in UAV-enabled mmWave relaying networks by substituting (17) and (18) into (16).

Remark 1: According to (16), we know that the secrecy outage probability is affected by the distributions of the closest horizontal distance between S and legitimate receiver r_L/r_N, the received SNR at legitimate destination γ_{RD} and the received SNR at the most malicious eavesdropper γ_E. From (13) and (15), we find that the mean value of r_L/r_N becomes small as λ_U increases. Then, D has more chance of receiving stronger signals from R, which causes the decline of secrecy outage probability. Additionally, from (17) and (18), we find that the effect of UAV attitude H on the distributions of γ_{RD} and γ_E are different. To be specific, for a given λ_U which is much smaller than λ_E, the received SNR of the most malicious eavesdropper is more sensitive to H than that of D when H is small, and the result is opposite when H becomes large. Thus, there exist an optimal H that provides the best secrecy performance.

IV. SECRECY PERFORMANCE WITH COOPERATIVE JAMMING

In this section, we further use a part of UAVs to transmit jamming signals for achieving the enhancement of physical layer security in the UAV-enabled mmWave relaying system.

Different from (7), the jamming signals create the interferences at D, and the signal to interference plus noise ratio (SINR) seen from D is written as

$$\gamma_{RD}^J = \frac{P_t G_{RD} L\left(d_{RD}\right) |h_{RD}|^2}{N_0 + I_D}, \quad (20)$$

where $I_D = \sum_{y\in\Phi_I} P_I G_{ID} \left|h_{I_y D}\right|^2 L\left(d_{I_y D}\right)$ is the jamming signals at D. The power of jamming signals is P_I, and $G_{ID} = G_m^R G_l^D$ for $l \in \{M, m\}$ is the antenna gain between the UAV jammers and D. Specifically, we assume that the jamming UAVs know partial D's channel state information, and in order to alleviate the jamming at D, the UAV jammers adjust the antenna steering orientation to misalign D [40].

The SINR at the most malicious eavesdropper can be described as

$$\gamma_E^J = \max_{e\in\Phi_E} \left\{\frac{P_t G_{RE_e} L\left(d_{RE_e}\right) \left|h_{RE_e}\right|^2}{N_0 + I_E}\right\}, \quad (21)$$

where $I_E = \sum_{i\in\Phi_I} P_I G_{IE} L\left(d_{ie}\right) |h_{ie}|^2$ is the jamming signals received from jamming UAVs, where $G_{IE} = G_l^R G_k^E$ for $l, k \in \{M, m\}$.

Similar to (16), the secrecy outage probability of UAV-enabled mmWave relaying networks with cooperative jamming can be derived as

$$p_{out}^J = 1 - \Pr\left(\log_2\left(1+\gamma_{RD}^J\right) - \log_2\left(1+\gamma_E^J\right) > C_{th2}\right)$$
$$= 1 - W \sum_{j\in\{L,N\}} A_j \sum_{i=1}^{T} g_{r_j}(r_i)\sqrt{r_i(\chi - r_i)}$$
$$\times \left(1 - \int_0^{\infty} F_{\gamma_{RD,j}}^J\left(\beta(x)\right) f_{\gamma_E}^J(x) dx\right)$$
$$= W \sum_{j\in\{L,N\}} A_j \sum_{i=1}^{T} g_{r_j}(r_i)\sqrt{r_i(\chi - r_i)}$$
$$\times \int_0^{\infty} F_{\gamma_{RD,j}}^J\left(\beta(x)\right) f_{\gamma_E}^J(x) dx$$
$$\approx W^2 \sum_{j\in\{L,N\}} A_j \sum_{i=1}^{T} g_{r_j}(r_i)\sqrt{r_i(\chi - r_i)}$$
$$\times \sum_{k=1}^{T} \sqrt{x_k(\mu - x_k)} F_{\gamma_{RD,j}}^J\left(\beta(x_k)\right) f_{\gamma_E}^J(x_k), \quad (22)$$

where $g_{r_j}(\cdot)$ is given as (13) and (15) in Section III but replacing λ_U with λ_R, $F_{\gamma_{RD,j}}^J(\cdot)$ is the CDF of γ_{RD}^J for LOS or NLOS $R \to D$ link, $f_{\gamma_E}^J(\cdot)$ is the PDF of γ_E^J.

In the following, we need to characterize the distributions of the SINRs at D and the most harmful eavesdropper.

Lemma 3: The CDF of the SINR at D for associating with a LOS/NLOS relay is given by

$$F_{\gamma_{RD,j}}^J(x) = 1 - e^{-\frac{N_0 x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}} \sum_{m=0}^{N_L-1} \frac{1}{m!}\left(\frac{x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)^m$$
$$\times \sum_{l=0}^{m} \binom{m}{l} N_0^{m-l} (-1)^l \mathcal{L}_{I_D}^{(l)}\left(e^{\frac{x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}}\right), \quad (23)$$

where $\mathcal{L}_{I_D}(s)$ denotes the Laplace transform of the random variable I_D and is written as (24) at the bottom of this page.

Proof: See Appendix C.

Lemma 4: The PDF of the SINR at the most malicious eavesdropper γ_E^J is written as

$$f_{\gamma_E}^J(x) = \int_0^\infty f_{I_E}(\tau) \exp\left(-2\pi\lambda_E \sum_{G_{RE}} \Pr(G_{RE} = V) \times \sum_{j\in\{L,N\}} \varpi_j^J(V,x,\tau)\right) \sum_{j\in\{L,N\}} \varphi_j(V,x,\tau) d\tau, \quad (25)$$

where $\varpi_j^J(V,x,\tau)$ and $\varphi_j(V,x,\tau)$ are given by (26) and (27) at the bottom of this page respectively, and the PDF of I_E can be obtain as

$$f_{I_E}(\tau) \approx \frac{2^{-B}e^{\frac{A}{2}}}{\tau} \sum_{b=0}^{B} \binom{B}{b} \sum_{c=0}^{C+b} \frac{(-1)^c}{D_c} Re\left\{\mathcal{L}_{I_E}(s)\right\}, \quad (28)$$

where D_c equal to 2 or 1 with the condition of $c = 0$ or $c = 1, 2, \ldots, s = \frac{(A+i2\pi c)}{2\tau}$, $Re\{y\}$ represents the real part of y, and the Laplace transform of I_E is given by (29) at the bottom of next page. The estimation accuracy depends on the selection of the values for A, B and C, which are set as $A = 8, \ln 10$, $B = 11$ and $C = 14$, and achieving the accuracy of 10^{-8}.

Proof: See Appendix D.

Finally, substituting (23) and (25) into (22), we can calculate the secrecy outage probability in the UAV-enabled mmWave relaying networks with cooperative jamming.

Remark 2: According to (23) and (25), we find that the jamming signals degrade the channels of both the legitimate link and the eavesdropping links. When the jamming power P_I increases, the secrecy outage probability first decreases and then increases. It can be explained that the received SINRs at eavesdroppers decrease as P_I becomes large, meanwhile, the effect of jamming signals on the SINR at D is smaller due to the weak side-lobe gains of jammers. But if P_I is large enough, the channel qualities of eavesdroppers are too poor, and D is more sensitive to the jamming signals than eavesdroppers. Furthermore, the secrecy outage probability (22) is not a monotonous function of cooperative jamming factor ε. The reason is that there would be more chance to select a better relay to assist the communication when ε starts to increases. But if ε is too large, the jamming signals are not strong enough to degrade the message signals at eavesdroppers. From the above analysis, the lowest secrecy outage probability can be obtained by properly designing P_I and ε.

TABLE 1. 3D Antenna parameters [41].

Number of antenna elements	N
Main-lobe Beamwidth $\theta_a = \theta_d$	$\sqrt{\frac{N}{3}}$
Main-lobe Gain G_M	N
Side-lobe Gain G_m	$\frac{\sqrt{N}-\frac{\sqrt{3}}{2\pi}N\sin\left(\frac{\sqrt{3}}{2\sqrt{N}}\right)}{\sqrt{N}-\frac{\sqrt{3}}{2\pi}\sin\left(\frac{\sqrt{3}}{2\sqrt{N}}\right)}$

TABLE 2. Simulation parameters.

Type	Values
Number of antenna elements	$N_S = 16$, $N_D = N_E = 4$
Blockage parameters	$a = 9.6$, $b = 0.28$
Path-loss	$\alpha_L = 2$, $\zeta_L = 61.4$ $\alpha_N = 2.92$, $\zeta_N = 72$
Small-scale fading	$N_L = 3$, $N_N = 2$
Radius of UAV-relay area	$\chi = 200m$
Distance between S and D	400m
Noise power	$N_0 = -174 + 10\lg(BW) + F_{dB}$
Noise figure	$F_{dB} = 10$ dB
Bandwidth	BW = 1 GHz

V. SIMULATION RESULTS

In this section, the simulation results are provided to show the secrecy performance of the mmWave networks assisted by UAV-enabled relays and jammers. We consider the mmWave communication operating at carrier frequency 28GHz. The parameters used in the performance are given in Table 1. In general, we present the Monte Carlo simulations in each figure, which are used to validate our analytical results.

Fig. 2 shows the effect of UAV-enabled relay density on the secrecy outage probability when N_R and H are different.

$$\mathcal{L}_{I_D}(s) = \exp\left(-2\pi s P_I \lambda_I \sum_{G_{ID}} \Pr(G_{ID} = V) \sum_{j\in(L,N)} \sum_{m=0}^{N_j-1} \sum_{i=0}^{T} W \frac{p_j(r_i) V C_j \left(r_i^2 + H^2\right)^{\frac{m\alpha_j}{2}} r_i \sqrt{r_i(\chi - r_i)}}{\left(\left(r_i^2 + H^2\right)^{\frac{\alpha_j}{2}} + P_I s V C_j\right)^{m+1}}\right). \quad (24)$$

$$\varpi_j^J(V,x,\tau) = \frac{1}{\Gamma(N_j)} \sum_{i=0}^{T} W p_j(r_i) \Gamma\left(N_j, \frac{(N_0+\tau)x\left(r_i^2+H^2\right)^{\frac{\alpha_j}{2}}}{P_t V C_j}\right) r_i\sqrt{r_i(\chi - r_i)}. \quad (26)$$

$$\varphi_j(V,x,\tau) = 2\pi\lambda_E \frac{x^{N_j-1}}{\Gamma(N_j)} \sum_{G_{IE}} \Pr(G_{IE} = V) \left(\frac{N_0+\tau}{P_t V C_j}\right)^{N_j} \sum_{i=0}^{T} W p_j(r_i) e^{-\frac{(N_0+\tau)x\left(r_i^2+H^2\right)^{\frac{\alpha_j}{2}}}{P_t V C_j}} \left(r_i^2 + H^2\right)^{\frac{N_j\alpha_j}{2}} r_i\sqrt{r_i(\chi - r_i)}. \quad (27)$$

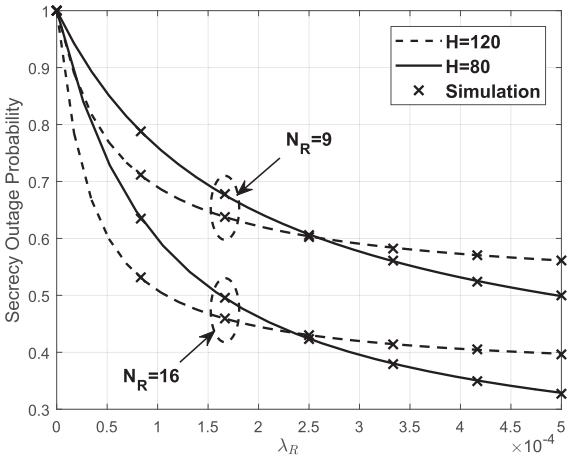


FIGURE 2. Secrecy outage probability versus the UAV-enabled relay densities when $P_t = 30dBm$, $C_{th1} = 5$, $C_{th2} = 1$, and $\lambda_E = 1.5 \times 10^{-3}$.

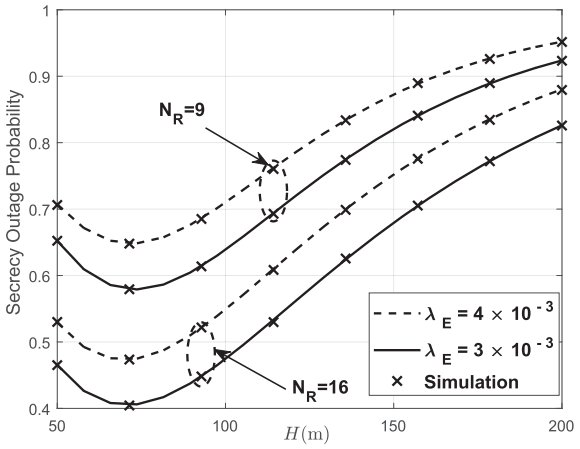


FIGURE 3. Secrecy outage probability versus the attitude of UAV-enabled relays when $P_t = 30dBm$, $C_{th1} = 5$, $C_{th2} = 1$, and $\lambda_U = 1 \times 10^{-3}$.

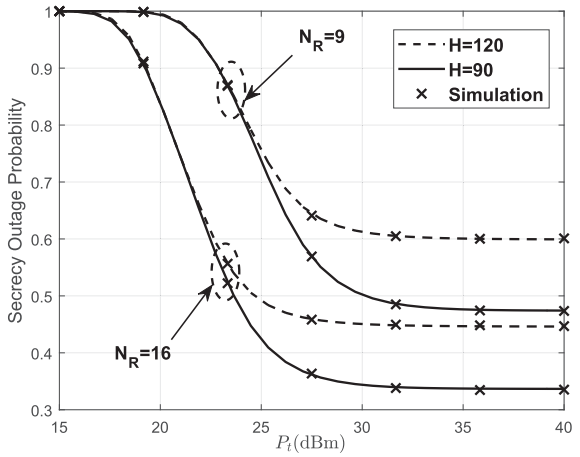


FIGURE 4. Secrecy outage probability versus the transmitting power when $C_{th1} = 5$, $C_{th2} = 1$, $\lambda_R = 1 \times 10^{-3}$ and $\lambda_E = 1.5 \times 10^{-3}$.

We observe that: 1) For a given λ_E, the secrecy outage probability decreases as the density of relays λ_R increases. This is due to the fact that D has more chances to associate with a better relay when λ_R increases, which means that D can receive stronger signals. 2) In the low relay density regime, better secrecy outage probability is obtained for $H = 120m$, and smaller secrecy outage probability can be achieved for $H = 80m$ as λ_R becomes large. This reason is that due to the random distribution of eavesdroppers, when λ_R is small, the quality of the most malicious eavesdropper channel benefits more from small H, which is opposite when λ_R becomes large. 3) The secrecy outage probability can be improved dramatically when N_R increases from 9 to 16. The reason is that we can obtain larger main-lobe gain and smaller side-lobe gain by adopting more antenna elements, then the gap between the qualities of legitimate and eavesdropper links expands. As a consequence, we can enhance the secrecy performance by using the directional antenna with more antenna elements.

In Fig. 3, we plot the secrecy outage probability as a function of H for different N_R and λ_E. The results show that: 1) The secrecy outage probability first decreases and then increases as H becomes large. This is because the quality of the most malicious eavesdropper channel is more sensitive to H than legitimate channel in the low H regime, and it's opposite when H becomes large. 2) When N_R reduces from 16 to 9, the secrecy outage probability deteriorates dramatically. The reason is that the antenna gain of legitimate link weakens severely when adopting less antenna elements. 3) The secrecy outage probability is worse for high λ_E. This is due to the fact that for higher λ_E, the most malicious eavesdropper can obtain better wiretapping channel as the legitimate channel remains stable. From the above-mentioned, we can properly design H to achieve the best secrecy performance.

Fig. 4 illustrates the effect of P_t on the secrecy outage probability by setting different N_R and H. Several observations can be drawn as follows: 1) When P_t is small, the secrecy outage probability decreases as P_t increases. In addition, in the high P_t regime, the secrecy outage probability remain unchanged when P_t increases. This is because when P_t becomes large, the gap between the capacities of legitimate and eavesdropper channels expands. But when P_t is large enough, the channel capacities is mainly determined

$$\mathcal{L}_{I_E}(s) = \exp\left(-2\pi s P_I \lambda_I \sum_{G_{IE}} \Pr(G_{IE} = V) \sum_{j\in(L,N)} \sum_{m=0}^{N_j-1} \sum_{i=0}^{T} W \frac{p_j(r_i)\, V C_j \left(r_i^2 + H^2\right)^{\frac{m\alpha_j}{2}} r_i \sqrt{r_i(\chi - r_i)}}{\left(\left(r_i^2 + H^2\right)^{\frac{\alpha_j}{2}} + P_I s V C_j\right)^{m+1}}\right). \quad (29)$$

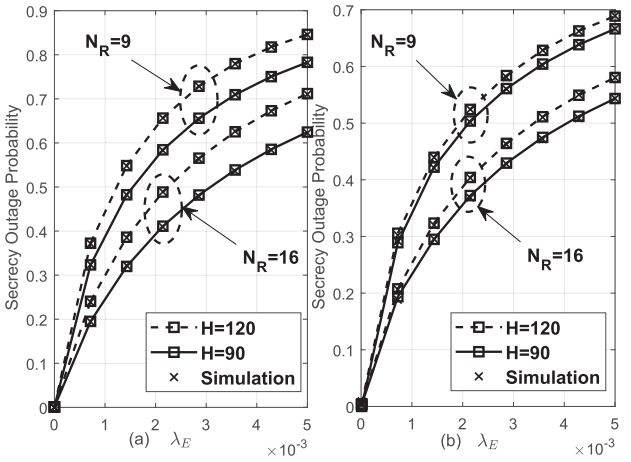


FIGURE 5. The secrecy outage probability versus the eavesdropper density λ_E when $P_t = 30dBm$, $C_{th1} = 5$, $C_{th2} = 1$, $\lambda_U = 1 \times 10^{-3}$.

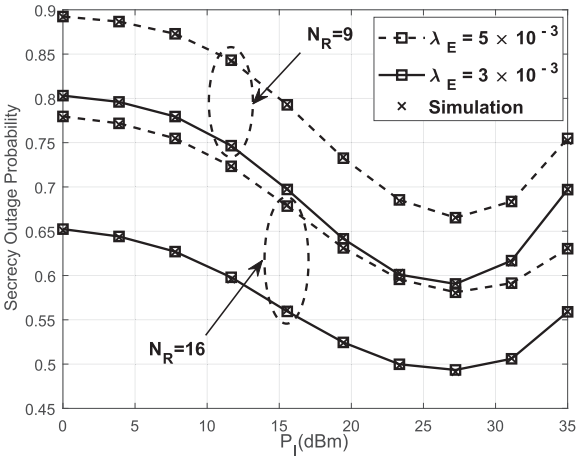


FIGURE 6. The secrecy outage probability versus the jamming power P_I when $H = 140m$, $C_{th1} = 5$, $C_{th2} = 1$, $\lambda_U = 5 \times 10^{-4}$ and $\varepsilon = 0.8$.

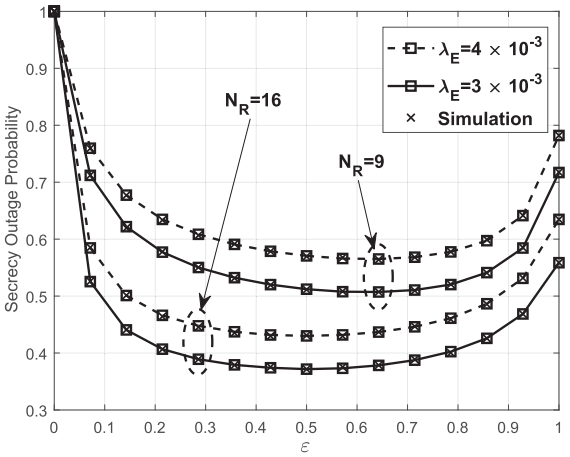


FIGURE 7. The secrecy outage probability versus the cooperative jamming factor ε when $P_t = 30dBm$, $P_I = 20dBm$, $C_{th1} = 5$, $C_t h2 = 1$ and $\lambda_U = 1 \times 10^{-3}$.

with P_t for both legitimate and eavesdropper channel, which means the gap of their channel capacities changes to stable. 2) By adopting more antennas elements, the secrecy outage probability will become low due to the high antenna gain of legitimate link. 3) The secrecy outage probability changes for different H. The reason is that the sensitivities to H are different for the legitimate and eavesdropper channels.

Fig. 5 illustrates the secrecy outage probability versus λ_E. The sub-graph (a) describes the secrecy performance without cooperative jamming. To gain more insight, we also give the sub-graph (b) which depicts the secrecy performance with cooperative jamming for $P_I = 20dBm$ and $\varepsilon = 0.8$. We can observe that: 1) The secrecy outage probability can be improved by adopting cooperative jamming. This is because the channel quality of eavesdropper can be deteriorated by transmitting jamming signals, at the same time, the effect of jamming on D is slight due to the weak side-lobe gain of jamming UAVs. 2) The secrecy outage probability increases as λ_E becomes large due to the fact that there are more eavesdroppers distributing around D when λ_E increases, and the channel quality of the most malicious eavesdropper may be better. 3) Using more antennas can enhance the main-lobe gain and restrain the side-lobe gain of UAVs to improve the secrecy outage probability.

In Fig. 6, we show the secrecy outage probability versus P_I for different N_R and λ_E. The simulation results show that: 1) The secrecy outage probability is not monotonous versus P_I. This is because when P_I increases, the jamming signals received by D are weaker than eavesdroppers due to that the main-lobes of jamming UAVs don't align D. But if P_I is large enough, the channel quality of eavesdropper is too poor, and D is more sensitive to jamming signals than eavesdroppers. 2) The secrecy outage probability can be improved when N_R increases from 9 to 16. The reason is that we can obtain better antenna gain for legitimate link by adopting more antennas. 3) The secrecy outage probability becomes large when λ_E increases. The reason is that the channel quality of the most malicious eavesdropper will be better if λ_E increases. In addition, the lowest secrecy outage probability can be obtained by optimizing P_I.

Fig.7 shows the effect of ε on secrecy outage probability. Several observations can be drawn as follows: 1) As ε increases, the secrecy outage probability first decreases and following increases. This is because when ε increases, the better UAV can be selected to forward messages to D, and the jamming signals wouldn't be too strong. But if ε is too large, the jamming signals are not strong enough to suppress the confidential signals received by eavesdroppers. 2) We can employ more antennas to restrain the leakage of signals and then the secrecy outage probability can be improved. 3) The secrecy outage probability are different when λ_E changes. The reason is that different λ_E means different channel of the most malicious eavesdropper. Obviously, the best secrecy performance can be achieved by properly designing ε.

VI. CONCLUSION

This paper investigated secure mmWave communication by using UAV-enabled relay and cooperative jammer. Considering the opportunistic relay selection scheme, we

$$
\begin{aligned}
A_L &= \Pr\left(C_L d_L^{-\alpha_L} > C_N d_N^{-\alpha_N}\right) \\
&= \int_0^{\chi} \bar{F}_{r_N}\left(\max\left(0, \sqrt{\left(\frac{C_N}{C_L}\right)^{\frac{2}{\alpha_N}}\left(y^2+H^2\right)^{\frac{\alpha_L}{\alpha_N}} - H^2}\right)\right) f_{r_L}(y)\, dy \\
&= W\sum_{i=0}^{T} e^{\nu_N\left(\max\left(0,\sqrt{\left(\frac{C_N}{C_L}\right)^{\frac{2}{\alpha_N}}\left(y_i{}^2+H^2\right)^{\frac{\alpha_L}{\alpha_N}} - H^2}\right)\right)} f_{r_L}(y_i)\sqrt{y_i(\chi - y_i)}. \qquad (34)
\end{aligned}
$$

$$
\begin{aligned}
\bar{G}_{r_L}(y) &= \Pr\left(r_L > y \,\middle|\, r_N > \max\left(0, \sqrt{\left(\frac{C_N}{C_L}\right)^{\frac{2}{\alpha_N}}\left(y^2+H^2\right)^{\frac{\alpha_L}{\alpha_N}} - H^2}\right)\right) \\
&= \frac{\int_y^{\infty} \Pr\left(r_N > \max\left(0, \sqrt{\left(\frac{C_N}{C_L}\right)^{\frac{2}{\alpha_N}}\left(z^2+H^2\right)^{\frac{\alpha_L}{\alpha_N}} - H^2}\right) | r_L > z\right) f_{r_L}(z)dz}{A_L}. \qquad (35)
\end{aligned}
$$

analyzed the distribution of the available UAV-enabled relays which follows an inhomogeneous PPP. In addition, we took into account that a part of UAVs are used to transmit the jamming signals to improve the secrecy performance. The simulation results show that the secrecy outage probability decreases when the density of relays, antenna number and message signal power increase or the density of eavesdroppers decreases. It's worth mentioning that the secrecy outage probability can be improved by adopting higher UAV attitude in low relay density situations, and the result is opposite when the relay density is large. Furthermore, our analysis shows that optimizing the attitude of UAVs, jamming signal power and density of jamming UAVs can indeed improve the secrecy outage probability. In the future, it's worth to study the optimization design in the UAV-enabled mmWave relaying networks, e.g., the power allocation between relay and jammer.

APPENDIX A
PROOF OF LEMMA 1

In order to obtain the PDF of r_L/r_N, which is the horizontal distance between D and the nearest LOS/NLOS UAV-enabled relay, we first derive the complimentary cumulative distribution function (CCDF) of r_L as

$$
\begin{aligned}
\bar{F}_{r_L}(y) &= \Pr(r_L > y) \\
&= \Pr(\textit{no LOS relay is closer than } y) \\
&\overset{e}{=} \exp\left(-\Lambda_L(0,y)\right), \qquad (30)
\end{aligned}
$$

where step (e) is due to PPP's void probability, and $\Lambda_L(0,y)$ is the mean number of LOS relays which are closer than y, then the expression is derived as

$$
\begin{aligned}
\Lambda_L(0,y) &= \int_{\mathcal{R}^2} \Pr\left(z \in \Phi_R\left(\mathcal{B}(0,y)\right) \textit{ is LOS}\right)dz \\
&= \int_0^{y}\int_0^{2\pi} p_L(r)\,\hat{\lambda}(r,\theta) r d\theta dr, \qquad (31)
\end{aligned}
$$

and we can calculate $\bar{F}_{r_L}(y)$ by substituting (31) into (30).

Then, because $f_{r_L}(y) = -\frac{d\bar{F}_{r_L}(y)}{dy}$, the PDF $f_{r_L}(y)$ can be derived as

$$
\begin{aligned}
f_{r_L}(y) &= -\left(\exp\left(-\Lambda_L(0,y)\right)\right)' \\
&= y p_L(y)\int_0^{2\pi}\hat{\lambda}(y,\theta)d\theta e^{\nu_L(y)} \\
&\overset{f}{=} W\sum_{k=0}^{T} y p_L(y)\,\hat{\lambda}(y,\theta_k)\, e^{\nu_L(y)}\sqrt{\theta_k(2\pi-\theta_k)}, \qquad (32)
\end{aligned}
$$

where step (f) follows the Gauss-Chebyshev integration, $W = \frac{\pi}{T}$, $\theta_k = \pi\left(1+\cos\frac{(2k-1)\pi}{2T}\right)$, T is the number of the cumulative times, and $\nu_L(y)$ can be derived as

$$
\begin{aligned}
\nu_L(y) &= -\int_0^{y}\int_0^{2\pi} p_L(r)\,\hat{\lambda}(r,\theta) r d\theta dr \\
&= -\int_0^{y}\sum_{i=0}^{T} W p_L(r)\,\hat{\lambda}(r,\theta_i)\, r\sqrt{\theta_i(2\pi-\theta_i)}dr \\
&= -W^2\sum_{h=0}^{T} p_L(r_h)\, r_h^{\frac{3}{2}}\sqrt{y-r_h} \\
&\quad\times\sum_{i=0}^{T}\hat{\lambda}(r_h,\theta_i)\sqrt{\theta_i(2\pi-\theta_i)}, \qquad (33)
\end{aligned}
$$

where $\theta_i = \pi\left(1+\cos\frac{(2i-1)\pi}{2T}\right)$, $r_h = \frac{y}{2}\left(1+\cos\frac{(2h-1)\pi}{2T}\right)$, and the derivation is due to the Gauss-Chebyshev integration.

Similarly, we can obtain the PDF of r_N as (11) for $j = N$.

APPENDIX B
PROOF OF LEMMA 2

We first derive the probability that the nearest LOS UAV-enabled relay is selected, and the detailed derivation is given as (34) at the top of this page. Then, we can easily get $A_N = 1 - A_L$.

In the following, we derive the conditional CCDF of the distance between D and the nearest LOS relay by giving that

$$\Lambda_y(0,t) = \lambda_I \int_{\mathcal{R}^2} \Pr\left(\frac{1}{G_{ID} L\left(d_{I_yD}\right)\left|h_{I_yD}\right|^2} \in [0,t]\right) = 2\pi\lambda_I \sum_{j\in(L,N)} \int_0^{\chi} \Pr\left(\left|h_{I_yD}\right|^2 \geq \frac{d_{ID}^{\alpha_j}}{G_{ID} C_j t}\right) p_j(r)\, r dr$$

$$= 2\pi\lambda_I \sum_{G_{ID}} \Pr(G_{ID} = V) \sum_{j\in(L,N)} \frac{1}{\Gamma(N_j)} \sum_{i=0}^{T} w p_j(r_i)\, \Gamma\left(N_j, \frac{\left(r_i^2 + H^2\right)^{\frac{\alpha_j}{2}}}{V C_j t}\right) r_i \sqrt{r_i(\chi - r_i)}. \tag{38}$$

$$K = -2\pi s P_I \lambda_I \sum_{G_{ID}} \Pr(G_{ID} = V) \sum_{j\in(L,N)} \frac{1}{\Gamma(N_j)} \sum_{i=0}^{T} W p_j(r) r_i \sqrt{r_i(\chi - r_i)} \int_0^{\infty} \Gamma\left(N_j, \frac{z\left(r_i^2 + H^2\right)^{\frac{\alpha_j}{2}}}{V C_j}\right) e^{-P_I s z} dz$$

$$\stackrel{o}{=} -2\pi s P_I \lambda_I \sum_{G_{ID}} \Pr(G_{ID} = V) \sum_{j\in(L,N)} \sum_{m=0}^{N_j-1} \sum_{i=0}^{T} W \frac{p_j(r_i) V C_j \left(r_i^2 + H^2\right)^{\frac{m\alpha_j}{2}} r_i \sqrt{r_i(\chi - r_i)}}{\left(\left(r_i^2 + H^2\right)^{\frac{\alpha_j}{2}} + P_I s V C_j\right)^{m+1}}. \tag{39}$$

$$F_{\gamma_E}^{J}(x) = \Pr\left(\max_{e\in\Phi_E} \frac{P_t G_{RE_e} \left|h_{RE_e}\right|^2 L\left(d_{RE_e}\right)}{N_0 + I_E} < x\right) = E_{\Phi_E, I_E}\left[\prod_{e\in\Phi_E} \Pr\left(\frac{P_t G_{RE_e} \left|h_{RE_e}\right|^2 L\left(d_{RE_e}\right)}{N_0 + I_E} < x\right)\right]$$

$$= E_{I_D}\left[\exp\left(-\lambda_E \sum_{G_{RE}} \Pr(G_{RE} = V) \sum_{j\in\{L,N\}} \int_{\mathcal{R}^2} p_j(r) \Pr\left(\left|h_{RE_e}\right|^2 < \frac{(N_0 + I_D)\, x d_{RE_e}^{\alpha_j}}{P_t G_{RE_e} C_j}\right)\right)\right]$$

$$= \int_0^{\infty} f_{I_E}(\tau) \exp\left(-2\pi\lambda_E \sum_{G_{RE}} \Pr(G_{RE} = V) \sum_{j\in\{L,N\}} \varpi_j^J(V, x, \tau)\right) d\tau. \tag{40}$$

a LOS UAV-enabled relay is selected, and the expression is given by (35) at the top of previous page.

Then we can derive the PDF $g_{r_L}(y) = -\frac{d\tilde{G}_{r_L}(y)}{dy}$ as (13). Similarly, we can obtain the PDF g_{r_N} as (15).

APPENDIX C
PROOF OF LEMMA 3

In the following, we detail the derivation of $F_{\gamma_{RD,j}}^{J}(x)$, i.e.,

$$F_{\gamma_{RD,j}}^{J}(x) = \Pr\left(|h_{RD}|^2 \leq \frac{x(N_0 + I_D) d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)$$

$$= 1 - e^{-\frac{(N_0+I_D) x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}} \sum_{m=0}^{N_L-1} \frac{1}{m!}\left(\frac{x(N_0 + I_D) d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)^m$$

$$= 1 - e^{-\frac{N_0 x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}} \sum_{m=0}^{N_L-1} \frac{1}{m!}\left(\frac{x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)^m$$

$$\times \sum_{l=0}^{m} \binom{m}{l} N_0^{m-l} E_{I_D}\left[I_D^l e^{-\frac{I_D x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}}\right]$$

$$\stackrel{g}{=} 1 - e^{-\frac{N_0 x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}} \sum_{m=0}^{N_L-1} \frac{1}{m!}\left(\frac{x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}\right)^m$$

$$\times \sum_{l=0}^{m} \binom{m}{l} N_0^{m-l} (-1)^l \mathcal{L}_{I_D}^{(l)}\left(e^{\frac{x d_{RD}^{\alpha_j}}{P_t G_{RD} C_j}}\right), \tag{36}$$

where step (g) follows the Laplace transform property $t^n f(t) \overset{\mathcal{L}}{\leftrightarrow} (-1)^n \frac{d^n}{ds^n} \mathcal{L}_{f(t)}(s)$, and $\mathcal{L}_{I_D}(s)$ can be derived as

$$\mathcal{L}_{I_D}(s) = E\left(e^{-sP_I \sum\limits_{y\in\Phi_I} G_{ID} L\left(d_{I_yD}\right)\left|h_{I_yD}\right|^2}\right)$$

$$= \exp\left(\int_0^{\infty}\left(e^{-\frac{sP_I}{x}} - 1\right)\Lambda_y(0, dx)\right)$$

$$= \exp\left(-\int_0^{\infty} \Lambda_y(0, x) \frac{sP_I}{x^2} e^{-\frac{sP_I}{x}} dx\right)$$

$$= exp\left(\underbrace{-\int_0^{\infty} \Lambda_y\left(0, \frac{1}{z}\right) sP_I e^{-szP_I} dz}_{K}\right), \tag{37}$$

where $\Lambda_y(0,t)$ is derived as (38) at the top of this page, then we can obtain K as (39), and the step (o) is due to [38, eq.(8.352.2)] and [38, eq.(3.381.4)].

Finally, we can obtain the Laplace transform $\mathcal{L}_{I_D}(s)$ as (24) by substituting (38) and (39) into (37).

APPENDIX D
PROOF OF LEMMA 4

In order to calculate the PDF of γ_E^J, which is the SINR at the most malicious eavesdropper, we need to clarify the distribution of the cooperative jamming signals. In general, the value of $f_{I_E}(\tau)$ cannot be calculated directly. Thus, we use numerical inversion of Laplace transform to obtain $f_{I_E}(\tau)$, and the

relationship is described as $f_{I_E}(\tau) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} \mathcal{L}_{I_E}(s)\, e^{s\tau} ds$. Then we can discretize the integral as a finite series by using Euler summation [42], and we can approximate $f_{I_E}(\tau)$ as (28). The Laplace transform $\mathcal{L}_{I_E}$ is given by (29), and the derivation is similar to Appendix B. In addition, according to the well builded guidelines in [43], we can achieve the accuracy of $10^{-\varsigma}$ when A, B and C at least equal $\varsigma \ln 10$, $1.243\varsigma - 1$ and 1.467ς. For example, we set $A = 8 \ln 10$, $B = 11$ and $C = 14$ and achieve an estimation error of 10^{-8}.

In the following, we first derive the CDF of γ_E^J as (40) at the top of previous page. Then the PDF $f_{\gamma_E}^J(x) = \frac{dF_{\gamma_E}^J(x)}{dx}$ can be derived as (25), where $\varphi_j(V, x, \tau)$ is given by (27), and the derivation is due to [38, eq.(0.410)] and [38, eq.(8.350.2)].

REFERENCES

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

[2] M. Xiao, S. Mumtaz, Y. Huang, L. Dai, Y. Li, M. Matthaiou, G. K. Karagiannidis, E. Björnson, K. Yang, C.-L. I, and A. Ghosh, "Millimeter wave communications for future mobile networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 1909–1935, Sep. 2017.

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

[4] T. Bai, R. Vaze, and R. W. Heath, Jr., "Analysis of blockage effects on urban cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 5070–5083, Sep. 2014.

[5] M. Gapeyenko, V. Petrov, D. Moltchanov, S. Andreev, N. Himayat, and Y. Koucheryavy, "Flexible and reliable UAV-assisted backhaul operation in 5G mmWave cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 11, pp. 2486–2496, Nov. 2018.

[6] H. Baek and J. Lim, "Design of future UAV-relay tactical data link for reliable UAV control and situational awareness," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 144–150, Oct. 2018.

[7] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.

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

[9] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8653906/

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

[11] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 181–184, Feb. 2019.

[12] R. Ma, W. Yang, X. Sun, L. Tao, and T. Zhang, "Secure communication in millimeter wave relaying networks," *IEEE Access*, vol. 7, pp. 31218–31232, 2019.

[13] 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.

[14] S. Biswas, S. Vuppala, and T. Ratnarajah, "On the performance of mmWave networks aided by wirelessly powered relays," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1522–1537, Dec. 2016.

[15] G. Yang and M. Xiao, "Performance analysis of millimeter-wave relaying: Impacts of beamwidth and self-interference," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 589–600, Feb. 2018.

[16] Z. Lin, X. Peng, F. Chin, and W. Feng, "Outage performance of relaying with directional antennas in the presence of co-channel interferences at relays," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 288–291, Aug. 2012.

[17] Z. Wei, X. Zhu, S. Sun, and Y. Huang, "Energy-efficiency-oriented cross-layer resource allocation for multiuser full-duplex decode-and-forward indoor relay systems at 60 GHz," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3366–3379, Dec. 2016.

[18] X. Xue, Y. Wang, L. Dai, and C. Masouros, "Relay hybrid precoding design in millimeter-wave massive MIMO systems," *IEEE Trans. Signal Process.*, vol. 66, no. 8, pp. 2011–2026, Apr. 2018.

[19] X. Chen, X. Hu, Q. Zhu, W. Zhong, and B. Chen, "Channel modeling and performance analysis for UAV relay systems," *China Commun.*, vol. 15, no. 12, pp. 89–97, Dec. 2018.

[20] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.

[21] L. Sboui, H. Ghazzai, Z. Rezki, and M.-S. Alouini, "Achievable rates of UAV-relayed cooperative cognitive radio MIMO systems," *IEEE Access*, vol. 5, pp. 5190–5204, 2017.

[22] Y. Chen, N. Zhao, Z. Ding, and M.-S. Alouini, "Multiple UAVs as relays: Multi-hop single link versus multiple dual-hop links," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6348–6359, Sep. 2018.

[23] H. Liu, S.-J. Yoo, and K. S. Kwak, "Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers," *J. Commun. Netw.*, vol. 20, no. 5, pp. 496–508, Oct. 2018.

[24] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, Jun. 2017.

[25] X. Sun, W. Yang, Y. Cai, R. Ma, and L. Tao, "Physical layer security in millimeter wave SWIPT UAV-based relay networks," *IEEE Access*, vol. 7, pp. 35851–35862, 2019.

[26] 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.

[27] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[28] S. Jia, J. Zhang, H. Zhao, Y. Lou, and Y. Xu, "Relay selection for improved physical layer security in cognitive relay networks using artificial noise," *IEEE Access*, vol. 6, pp. 64836–64846, 2018.

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

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

[31] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 569–572, Dec. 2014.

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

[33] W. Yang, L. Tao, X. Sun, R. Ma, Y. Cai, and T. Zhang, "Secure on-off transmission in mmWave systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 32681–32692, 2019.

[34] F. J. Lopez-Martinez, D. Morales-Jimenez, E. Martos-Naya, and J. F. Paris, "On the bivariate Nakagami-*m* cumulative distribution function: Closed-form expression and applications," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1404–1414, Apr. 2013.

[35] R. Zhao, Y. Yuan, L. Fan, and Y.-C. He, "Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-*m* fading channels," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 549–563, Feb. 2017.

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

[37] 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. 22670–22683, 2018.

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

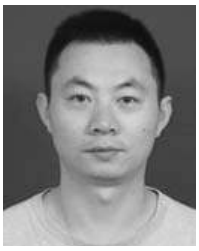
[39] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706–2722, Oct. 2016.

[40] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2016.
[41] K. Venugopal, M. C. Valenti, and R. W. Heath, Jr., "Device-to-device millimeter wave communications: Interference, coverage, rate, and finite topologies," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6175–6188, Sep. 2016.
[42] C. A. O'cinneide, "Euler summation for Fourier series and Laplace transform inversion," *Commun. Statist. Stochastic Models*, vol. 13, no. 2, pp. 315–337, Jan. 1997.
[43] J. Abate and W. Whitt "Numerical inversion of Laplace transforms of probability distributions," *ORSA J. Comput.*, vol. 7, no. 1, pp. 36–43, 1995.

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

WEIWEI YANG (S'08–M'12) received the B.Sc., M.Sc., and Ph.D. degrees in telecommunications from the PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively.

He is currently an Associate Professor with the College of Communication Engineering, Army Engineering University of PLA. He is also a coauthor of the book *"Handbook of Cognitive Radio"* (Springer, 2017). His research interests include cooperative communications, cognitive radio, and physical layer security. He is also a co-recipient of Best Paper Award from WCSP 2011. He also served as a publication Co-Chair for WCSP 2015, a track chairs for IEEE CIC ICCC 2017 and WCSP 2015, and TPC members for WCSP 2011/2014/2017/2018, GC 2016 Workshops, and GC 2017 Workshops and ICC 2016-Workshops.



YU ZHANG received the B.S. and M.S. degrees from the PLA University of Science and Technology, Nanjing, China, in 2006 and 2008, respectively. He is currently pursuing the Ph.D. degree in communications and information system with the College of Communications Engineering, Army Engineering University of PLA. He is currently an Associate Researcher with the Sixty-third Research Institute, National University of Defense Technology. His research interests include electromagnetic spectrum management, cooperative communications, cognitive radio, and physical layer security.

JUE LIU received the B.S. degree in computer science and technology from the School of Computer Science and Technology, Soochow University, Suzhou, China, in 2007. She is currently pursuing the Ph.D. degree in information and communications engineering with the College of Communications Engineering, Army Engineering University of PLA, Nanjing, China. She is currently an Associate Professor with the College of Information Science and Engineering, Nanjing Audit University Jinshen College, Nanjing, China. Her current research interests include physical layer security and UAV communication.

HUI SHI received the M.S. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2007. She is currently pursuing the Ph.D. degree in information and communications engineering with the College of Communications Engineering, Army Engineering University of PLA, Nanjing. Her current research interests include cooperative communications, wireless sensor networks, the Internet of things, physical layer security, SWIPT, and cognitive radio systems.