Secrecy Analysis of UAV-Based mmWave Relaying Networks

Xiaowei Pang, Mingqian Liu, *Member, IEEE*, Nan Zhao, *Senior Member, IEEE*, Yunfei Chen, *Senior Member, IEEE,* Yonghui Li, *Fellow, IEEE,* and F. Richard Yu, *Fellow, IEEE*

***Abstract*—Employing unmanned aerial vehicles (UAVs) in millimeter-wave (mmWave) networks as relays has emerged as an appealing solution to assist remote or blocked communication nodes. In this case, the network security becomes a great challenge due to the presence of malicious eavesdroppers. In this paper, we perform a secrecy analysis for a UAV-based mmWave relaying network. We first investigate the relaying scheme without jamming where the UAV decodes and forwards the information from the source to the destination with malicious eavesdropping. Furthermore, to enhance the secrecy performance, we propose a cooperative jamming scheme via utilizing the destination and an external UAV to cooperatively disrupt the eavesdroppers at the two stages of relaying, respectively. Using the probability of line-of-sight (LoS) between the UAV and ground nodes, the three-dimensional (3D) antenna gain, and the Nakagami-m small-scale fading model, the secrecy outage probability (SOP) of the two schemes with and without jamming is analyzed. Closed-form expressions for the SOP of the two schemes are obtained by employing the Gauss-Chebyshev quadrature. Simulation results are presented to validate the theoretical expressions of SOP and to show the effectiveness of the proposed schemes.**

***Index Terms*—Cooperative jamming, millimeter-wave, physical layer security, relay, secrecy outage probability, unmanned aerial vehicle**

I. Introduction

Unmanned aerial vehicles (UAVs) have been deployed at an astounding pace in wireless communication systems over the past decade, thanks to their high mobility, on-demand deployment and enhanced line-of-sight (LoS) probability [1]. UAVs have been extensively applied in multifarious scenarios for different purposes, such as seamless coverage [2], relaying [3], data gathering [4], and internet of things (IoT) applications [5]. On the standpoint of service provision, UAVs can be employed as an aerial platform to enhance the communication quality of existing terrestrial wireless systems [6]. Furthermore, UAVs can also be integrated into cellular networks as aerial users to ensure ultra-reliable wireless links, as cellular-connected UAV communication [7], [8].

Manuscript received August 27, 2020; revised December 29, 2020; accepted March 03, 2021. The work was supported by the National Natural Science Foundation of China (NSFC) under Grant 62071364 and 61871065. The associate editor coordinating the review of this paper and approving it for publication was J. Zhang. *(Corresponding author: Mingqian Liu and Nan Zhao.)*

As other communication devices, UAVs have to deal with the growing data rate as well as the overcrowding spectrum. In this regard, millimeter-wave (mmWave) communication offers much wider bandwidth and is a promising technique to be utilized in UAV networks to enable much higher capacity [9]. The short wavelength of mmWave allows massive antennas to be packed on a small UAV so that beamforming can be carefully designed to overcome the drawbacks of mmWave such as severe path loss and blocking. Moreover, UAVs can flexibly change their locations to avoid blockages and thus are suitable for the mmWave transmission [10]. For example, a novel channel tracking method based on the flight control was proposed by Zhao *et al.* in [11], where the three-dimensional (3D) geometry channel model was formulated as a function of the UAV movement and the channel gain. A novel hardware-efficient implementation for mmWave hybrid precoding was proposed in [12], and hybrid precoding can also be employed in mmWave UAV networks. Particularly, hybrid precoding was jointly optimized with the UAV placement and power allocation in [13] to maximize the energy efficiency of mmWave UAV networks.

An increasingly interesting application of UAVs is relaying network, where UAVs act as relays to assist the transmission between two terrestrial terminals without reliable direct links due to obstacles or a long distance [14]. One of the challenges for practical applications is to find the optimal location for a static relay or the trajectory for a mobile relay. Particularly, the optimum altitude of the UAV as a relaying station for maximum reliability was investigated by Chen *et al.* in [15], with both static and mobile UAVs considered. Moreover, Chen *et al.* designed an algorithm to find the optimal UAV position to establish the best wireless relay link in [16]. To effectively minimize the decoding error probability subject to the latency requirement for UAV-enabled relaying systems, the UAV location and blocklength were jointly optimized in [17]. and the UAV location and power allocation were jointly optimized in [18], respectively. To achieve the full potential of UAVs, the mobility of UAV was utilized by Zhang *et al.* in [19], where the trajectory and transmit power are jointly optimized to minimize the outage probability of the relay network. Furthermore, Kong *et al.* in [20] proposed a novel UAV-relaying method for mmWave communications, where the UAV gradually adjusts its path to approach the optimal location in an accurate and efficient way. In [21], Zhu *et al.* jointly optimized the UAV position, analog beamforming, and power control to maximize the achievable rate in a full-duplex UAV relaying network. However, none of them has considered the security aspect of UAV relaying networks.

Despite the advantages of UAV-enabled relaying networks, the broadcast nature and the LoS of UAVs channels pose great threats to the network security. Thus, it is important to study physical layer security problem to provide secure transmission by leveraging the imperfections of the communication medium [22]. Aiming at maximizing the secrecy rate, Wang *et al.* proposed a mobile relaying scheme in a four-node senario including a source, a destination, a UAV relay, and an eavesdropper [23]. In [24], a joint precoding scheme was proposed for UAV-aided networks to achieve simultaneous wireless information and power transfer (SWIPT) while guaranteeing the secure transmission for passive receivers. In [25], the secrecy performance of a mmWave SWIPT UAV-based relaying system was analyzed, with both amplify-and-forward (AF) and decode-and-forward (DF) protocols considered. Particularly, cooperative jamming has been regarded as an effective enabler for secure communication by imposing interference to eavesdroppers [26]. The resource allocation and trajectory design were investigated by Li *et al.* in [27] for secure UAV-enabled systems, where UAVs can provide communications or serve as jammers. To ensure energy-efficient secure UAV communication, the trajectory and resource allocation were jointly optimized by Cai *et al.* in [28] with the assistance of a multi-antenna jamming UAV. In [29], Chen *et al.* proposed a new joint relay and jammer selection scheme and maximized the secrecy rate via power allocation. Employing UAVs as jammmers, the secrecy performance of UAV-enabled mmWave networks was analyzed in [30] by Zhu *et al.*, with the practical constraints of UAV deployment and unique propagation characteristics. However, none of them has considered jointly employing the UAV and ground nodes as jammers to disturb eavesdropping in mmWave UAV-based relaying systems.

Motivated by these observations, we consider a UAV-based mmWave relaying network in this paper, where a UAV is employed to assist the communication between the ground source and destination. We propose two UAV relaying schemes with and without jamming, and analyze the secrecy performance by deriving the secrecy outage probability (SOP). To the best of our knowledge, this is the first work that utilizes the destination and the UAV to cooperatively transmit jamming signals in UAV-based mmWave relaying networks. The main contributions of this paper are summarized as follows.

- A UAV-based mmWave relaying network is studied to help forward confidential information from the ground source to the destination in the presence of multiple eavesdroppers that are assumed to be deployed according to a homogeneous Poisson point process (HPPP) distribution. We consider both the probabilities of LoS and non-line-of-sight (NLoS) links when modeling mmWave UAV-to-ground channels with Nakagami-m fading. In addition, we employ the 3D antenna gain model to characterize the mmWave directional transmission.
- We first investigate the secrecy performance of the UAV-based mmWave relaying network without jamming, where the transmission is divided into two time slots. Specifically, the relaying UAV and eavesdroppers receive the confidential information from the source in the first time slot. In the second slot, the UAV forwards the messages to the destination in the presence of eavesdropping. For a given secrecy rate threshold, the theoretical SOP of the scheme is derived to evaluate the secrecy performance by employing the Gauss-Chebyshev quadrature.
- To further guarantee the secure transmission, we develop a cooperative jamming scheme exploiting the destination and a jamming UAV to disturb the eavesdropping in the two time slots, respectively. In contrast to the existing studies on UAV-based relaying networks without jamming or only using UAVs as jammers, we not only employ a jamming UAV but also exploit the destination to send jamming signals at its spare time to promote the secure performance. The theoretical SOP of the scheme with cooperative jamming is derived by adopting a two-layer Gauss-Chebyshev quadrature.

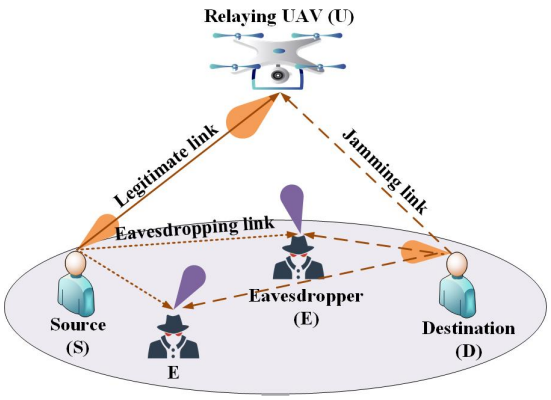
The remainder of this paper is organized as follows. In Section II, the system model is introduced. The secrecy performance of the UAV-based mmWave relaying networks without and with cooperative jamming is investigated in Section III and Section IV, respectively. In Section V, numerical results are provided to validate the derived SOP performance, followed by the conclusions in Section VI.

II. System Model

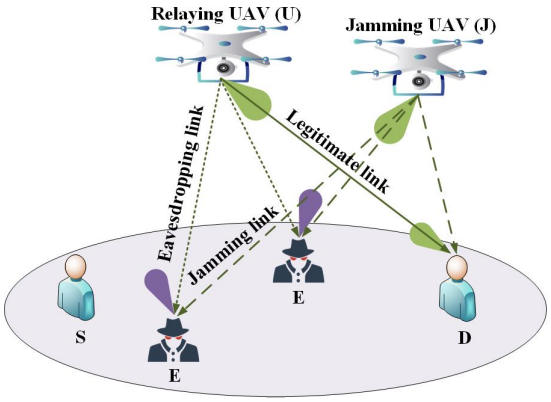
Consider a UAV-based mmWave relaying network as illustrated in Fig. 1, where a UAV (U) is employed as a relay to assist the transmission from the source (S) to the destination (D). Note that there is no direct link between S and D due to the severe path loss or blockage. Assume that the relaying UAV works in half-duplex using the DF strategy. The total transmission is divided into two time slots. In the first time slot, S transmits signals to U in the first time slot, and in the second time slot, U forwards the signals to D. Meanwhile, multiple eavesdroppers on the ground intend to wiretap the confidential information in both two slots. The distribution of eavesdroppers is modeled as an HPPP Φ_E with density λ_E, and we use E to denote the eavesdroppers with $E \in \Phi_E$. Considering the small size of mmWave antennas, all the nodes are assumed to be equipped with multiple antennas.

Two transmission schemes without and with cooperative jamming are investigated in this paper. The scheme without jamming includes the legitimate transmission from S to U and from U to D with malicious eavesdropping, and its transmission process can be referred to Fig. 1 by removing the jamming links. For the scheme with cooperative jamming, D is utilized to interfere the eavesdropping in the first time slot by sending jamming signals[1] as shown in Fig. 1(a). In the second time slot, an external UAV is employed as a jammer to combat the eavesdropping as shown in Fig. 1(b). The relaying UAV and jamming UAV are assumed to be deployed at the same altitude H, while the vertical heights of terrestrial nodes S, D, and E are negligible compared with H.

[1]It is assumed that the antennas equipped at D can be used for either transmitting or receiving signals at a specific time slot.



(a) First Time Slot



(b) Second Time Slot

Fig. 1. Illustration of the mmWave UAV-based relaying scheme with cooperative jamming. (a) Transmissions in the first time slot. (b) Transmissions in the second time slot.

A. Channel Model

It is known that the air-to-ground channels can be LoS or NLOS links due to the blockage effect [31]. According to [32], the occurrence probability of LoS links is given as

$$P_L(r) = \frac{1}{1 + A\exp(-B(\arctan(\frac{H}{r}) - A))}, \tag{1}$$

where r denotes the horizontal distance between the UAV and a ground node. A and B are constants relying on the environment. Accordingly, the probability of NLoS links is calculated as $P_N(r) = 1 - P_L(r)$.

With the 3D distance of a LoS or NLoS link denoted by d, the path loss model can be expressed as

$$L(d) = \begin{cases} \beta_L d^{-\alpha_L}, & \text{LoS links}, \\ \beta_N d^{-\alpha_N}, & \text{NLoS links}, \end{cases} \tag{2}$$

where α_L and α_N denote the path loss exponents for LoS and NLoS links, respectively. β_L and β_N can be considered as intercepts of the LOS and NLOS path loss formulas, respectively.

In the following sections, we use d_{ij} and r_{ij} to denote the 3D distance and the horizontal distance between nodes i and j, respectively, where $i, j \in \{S, D, E, U, J\}$. Without loss of generality, we assume that each link experiences independent Nakagami$-m$ fading. Particularly, the small-scale fading power between the ith and jth nodes is denoted as h_{ij}, which is a Gamma random variable. We have $h_{ij} \sim \Gamma(N_L, 1/N_L)$ for a LoS link and $h_{ij} \sim \Gamma(N_N, 1/N_N)$ for a NLoS link, where N_L and N_N are integers and denote the Nakagami fading parameters for LoS links and NLoS links, respectively.

B. 3D Antenna Gain

Assume that the relaying UAV (U) and jamming UAV (J) are equipped with N_U and N_J antennas, respectively. For a ground node $g \in \{S, D, E\}$, the number of antennas is denoted as N_g. Similar to [25], we adopt a 3D sectorized antenna model taking into account the directional mmWave transmission and the UAV's altitude. For each node $j \in \{S, D, E, U, J\}$, the main-lobe gain and side-lobe gain are expressed as G_M^j with probability p_M^j and G_m^j with probability p_m^j, respectively.

Thus, the directional antenna gain and the corresponding probability can be written as [25]

$$G_i^a = \begin{cases} G_M^a, & p_M^a = \dfrac{\psi_a}{\pi}\dfrac{\theta_a}{\pi} \\ G_m^a, & p_m^a = 1 - \dfrac{\psi_a}{\pi}\dfrac{\theta_a}{\pi} \end{cases}, a \in \{U, J\}, \tag{3}$$

$$G_i^g = \begin{cases} G_M^g, & p_M^g = \dfrac{\psi_g}{\pi}\dfrac{\theta_g}{\pi - \theta_g} \\ G_m^g, & p_m^g = 1 - \dfrac{\psi_g}{\pi}\dfrac{\theta_g}{\pi - \theta_g} \end{cases}, g \in \{S, D, E\}, \tag{4}$$

where ψ_a (ψ_g) and θ_a (θ_g) denote the half-power beamwidth in the azimuth and the elevation, respectively. Particularly, we consider the worst case for the elevation angle at ground nodes similar to [30], and accordingly the elevation angle of ground nodes is uniformly distributed in the range of $[\theta_g/2, \pi - \theta_g/2]$.

Assume perfect beam alignment for the legitimate links between S (D) and U, and the misalignment caused by UAV jittering is supposed to be well mitigated by existing techniques [33]. Thus, the antenna gains from S to U and from U to D can be given by $G_{SU} = G_M^S G_M^U$ and $G_{UD} = G_M^U G_M^D$, respectively. In contrast, the antenna gain of an eavesdropping link (from U to E) or a jamming link (from J to E) can be obtained as

$$G_{aE} = \begin{cases} G_M^a G_M^E, & p_1 = p_M^a p_M^E \\ G_M^a G_m^E, & p_2 = p_M^a p_m^E \\ G_m^a G_M^E, & p_3 = p_m^a p_M^E \\ G_m^a G_m^E, & p_4 = p_m^a p_m^E \end{cases}, a \in \{U, J\}. \tag{5}$$

III. Secrecy Analysis Without Jamming

In this section, we analyze the secrecy performance of a UAV-based relaying network without jamming. Using DF, the signal-to-noise ratio (SNR) at the destination can be expressed as

$$\gamma_D = \min\left(\frac{P_S G_{SU} L(d_{SU}) h_{SU}}{\sigma_U^2}, \frac{P_U G_{UD} L(d_{UD}) h_{UD}}{\sigma_D^2}\right), \tag{6}$$

where P_S (P_U) is the transmit power of S (U), and σ_U^2 (σ_D^2) denotes the power of the additive white Gaussian noise (AWGN) at U (D).

In addition, we suppose that the eavesdroppers are independent and use the selection combining scheme to decode the received signals from the source and the UAV. Thus, the highest eavesdropping SNR among all the eavesdroppers can be given as

$$\gamma_E = \max\left(\max_{E\in\Phi_E}\gamma_{SE}, \max_{E\in\Phi_E}\gamma_{UE}\right), \tag{7}$$

where the SNR at each eavesdropper for decoding signals from S and from U can be written as

$$\gamma_{SE} = \frac{P_S G_{SE} L(d_{SE}) h_{SE}}{\sigma_E^2}, \tag{8}$$

$$\gamma_{UE} = \frac{P_U G_{UE} L(d_{UE}) h_{UE}}{\sigma_E^2}, \tag{9}$$

and σ_E^2 is the noise power at eavesdroppers.

The achievable secrecy rate is

$$R_s = \frac{1}{2}\left[\log_2(1+\gamma_D) - \log_2(1+\gamma_E)\right]^+, \tag{10}$$

where $[x]^+ \triangleq \max(x, 0)$. We set the threshold of secrecy rate at the desired receiver D as R_{th}, and thus, the secrecy outage occurs when the secrecy rate is lower than R_{th}. Specifically, the secrecy outage probability of D can be derived as

$$\begin{aligned}
P_{sop} &= Pr\left\{R_s < R_{th}\right\} \\
&= Pr\left\{\frac{1}{2}\log_2(1+\gamma_D) - \frac{1}{2}\log_2(1+\gamma_E) < R_{th}\right\} \\
&= Pr\left\{\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) < 2R_{th}\right\} \\
&= Pr\left\{1+\gamma_E > (1+\gamma_D)2^{-2R_{th}}\right\} \\
&= 1 - \int_0^\infty F_{\gamma_E}\left((1+y)2^{-2R_{th}} - 1\right) f_{\gamma_D}(y)dy,
\end{aligned} \tag{11}$$

where $F_{\gamma_E}(\cdot)$ is the cumulative probability function (CDF) of γ_E and $f_{\gamma_D}(\cdot)$ is the probability distribution function (PDF) of γ_D.

To derive the secrecy outage probability, the distributions of the SNR at D as well as the highest eavesdropping SNR at all the eavesdroppers are derived in Theorem 1.

Theorem 1: The CDF and PDF of γ_D can be given as (12a) and (12b) respectively at the top of the next page.

Proof: For the Gamma random variable $h_{ij} \sim \Gamma(N_i, 1/N_i), i \in \{L, N\}$, the PDF and CDF of h_{ij} can be written as

$$f_h(x) = N_i^{N_i}\frac{x^{N_i-1}}{\Gamma(N_i)}e^{-N_i x}, \tag{13}$$

$$F_h(x) = 1 - \sum_{n=0}^{N_i-1}(N_i x)^n \frac{1}{n!}e^{-N_i x}. \tag{14}$$

Therefore, we can derive the CDF of γ_D as

$$\begin{aligned}
F_{\gamma_D}(\gamma) &= \Pr\left\{\min\left(\frac{P_S G_{SU} L(d_{SU}) h_{SU}}{\sigma_U^2}, \frac{P_U G_{UD} L(d_{UD}) h_{UD}}{\sigma_D^2}\right) < \gamma\right\} \\
&= 1 - \Pr\left\{\frac{P_S G_{SU} L(d_{SU}) h_{SU}}{\sigma_U^2} > \gamma\right\}\Pr\left\{\frac{P_U G_{UD} L(d_{UD}) h_{UD}}{\sigma_D^2} > \gamma\right\} \\
&= 1 - \Pr\left\{h_{SU} > \frac{\sigma_U^2\gamma}{P_S G_{SU} L(d_{SU})}\right\}\Pr\left\{h_{UD} > \frac{\sigma_D^2\gamma}{P_U G_{UD} L(d_{UD})}\right\} \\
&\overset{(a)}{=} 1 - \sum_{i\in\{L,N\}} P_i(r_{SU}) \sum_{n_1=0}^{N_i-1}\left(\frac{N_i\gamma\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}\right)^{n_1}\frac{1}{n_1!}e^{-\frac{N_i\gamma\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}} \\
&\times \sum_{j\in\{L,N\}} P_j(r_{UD}) \sum_{n_2=0}^{N_j-1}\left(\frac{N_j\gamma\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}\right)^{n_2}\frac{1}{n_2!}e^{-\frac{N_j\gamma\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}} \\
&= (12a).
\end{aligned} \tag{15}$$

Step (a) is derived using the complementary cumulative distribution function (CCDF) of h_{ij} by $1 - F_h(x)$. Taking the derivative of $F_{\gamma_D}(\gamma)$, we can easily obtain the PDF of γ_D as (12b). ■

The CDF of γ_E can be expressed as

$$\begin{aligned}
F_{\gamma_E}(\gamma) &= \Pr\left\{\max\left(\max_{E\in\Phi_E}\gamma_{SE}, \max_{E\in\Phi_E}\gamma_{UE}\right) < \gamma\right\} \\
&= \underbrace{\mathbb{E}\left[\prod_{E\in\Phi_E}\Pr\{\gamma_{SE} < \gamma\}\right]}_{\mathcal{F}_1(\gamma)}\underbrace{\mathbb{E}\left[\prod_{E\in\Phi_E}\Pr\{\gamma_{UE} < \gamma\}\right]}_{\mathcal{F}_2(\gamma)}.
\end{aligned} \tag{16}$$

Based on this, We will calculate $F_{\gamma_E}(\gamma)$ in Theorem 2 by deriving $\mathcal{F}_1(\gamma)$ and $\mathcal{F}_2(\gamma)$ separately.

Theorem 2: The CDF of γ_E can be given as (17) at the top of the next page, where $x_j = \cos(\frac{2j-1}{2J}\pi)$, $v_j = \frac{R_U}{2}(x_j+1)$, and J denotes the number of nodes in the Chebyshev-Gauss approximation. In addition, R_U is the maximum connection distance in the horizontal plane between U and a specific eavesdropper, and r_0 (R_0) denotes the minimum (maximum) connection distance between S and E.

Proof: First, define $\mathcal{F}_1(\gamma) = \mathbb{E}\left[\prod_{E\in\Phi_E}\Pr\{\gamma_{SE} < \gamma\}\right]$. Then, according to the generation function of the PPP [34], we have

$$\begin{aligned}
\mathcal{F}_1(\gamma) &= \exp\left\{-2\pi\lambda_E \times \int_{r_0}^{R_0}\Pr\{\gamma_{SE} > \gamma\}rdr\right\} \\
&= \exp\left\{-2\pi\lambda_E \times \sum_{i\in\{M,m\}} p_i^E \int_{r_0}^{R_0}\Pr\left\{h_{SE} > \frac{\gamma\sigma_E^2 r^{\alpha_N}}{P_S G_{SE}\beta_N}\right\}rdr\right\}.
\end{aligned} \tag{18}$$

Particularly, the integral term in (18) can be calculated as

$$\begin{aligned}
&\int_{r_0}^{R_0}\Pr\left\{h_{SE} > \frac{\gamma\sigma_E^2 r^{\alpha_N}}{P_S G_{SE}\beta_N}\right\}rdr \\
&\overset{(b)}{=} \sum_{n=0}^{N_N-1}\int_{r_0}^{R_0}\left(\frac{N_N\gamma\sigma_E^2 r^{\alpha_N}}{P_S G_{SE}\beta_N}\right)^n\frac{1}{n!}e^{-\frac{N_N\gamma\sigma_E^2 r^{\alpha_N}}{P_S G_{SE}\beta_N}}rdr \\
&\overset{(c)}{=} \sum_{n=0}^{N_N-1}\frac{\Gamma\left(\frac{\alpha_N n+2}{\alpha_N}, \frac{N_N\gamma\sigma_E^2 r_0^{\alpha_N}}{P_S G_{SE}\beta_N}\right) - \Gamma\left(\frac{\alpha_N n+2}{\alpha_N}, \frac{N_N\gamma\sigma_E^2 R_0^{\alpha_N}}{P_S G_{SE}\beta_N}\right)}{n!\alpha_N\left(\frac{N_N\gamma\sigma_E^2}{P_S G_{SE}\beta_N}\right)^{\frac{2}{\alpha_N}}},
\end{aligned} \tag{19}$$

$$F_{\gamma_D}(\gamma)=1-\sum_{i,j\in\{L,N\}}\sum_{n_1=0}^{N_i-1}\sum_{n_2=0}^{N_j-1}P_i(r_{SU})P_j(r_{UD})\frac{\gamma^{n_1+n_2}}{n_1!n_2!}\left(\frac{N_i\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}\right)^{n_1}\left(\frac{N_j\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}\right)^{n_2} e^{-\gamma\left(\frac{N_i\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}+\frac{N_j\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}\right)}, \quad (12a)$$

$$f_{\gamma_D}(\gamma)=-\sum_{i\in\{L,N\}}\sum_{j\in\{L,N\}}\sum_{n_1=0}^{N_i-1}\sum_{n_2=0}^{N_j-1}P_i(r_{SU})P_j(r_{UD})\frac{1}{n_1!n_2!}\left(\frac{N_i\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}\right)^{n_1}\left(\frac{N_j\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}\right)^{n_2}$$
$$\times\left[(n_1+n_2)\gamma^{n_1+n_2-1}e^{-\gamma\left(\frac{N_i\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}+\frac{N_j\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}\right)}-\left(\frac{N_i\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}+\frac{N_j\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}\right)e^{-\gamma\left(\frac{N_i\sigma_U^2 d_{SU}^{\alpha_i}}{P_S G_{SU}\beta_i}+\frac{N_j\sigma_D^2 d_{UD}^{\alpha_j}}{P_U G_{UD}\beta_j}\right)}\gamma^{n_1+n_2}\right]. \quad (12b)$$

$$F_{\gamma_E}(y)=\exp\left\{-2\pi\lambda_E\times\left[\sum_{i\in\{M,m\}}p_i^E\sum_{n=0}^{N_N-1}\frac{\Gamma\left(\frac{\alpha_N n+2}{\alpha_N},\frac{N_N\gamma\sigma_E^2 r_0^{\alpha_N}}{P_S G_m^S G_i^E\beta_N}\right)-\Gamma\left(\frac{\alpha_N n+2}{\alpha_N},\frac{N_N\gamma\sigma_E^2 R_0^{\alpha_N}}{P_S G_m^S G_i^E\beta_N}\right)}{n!\alpha_N\left(\frac{N_N\gamma\sigma_E^2}{P_S G_m^S G_i^E\beta_N}\right)^{\frac{2}{\alpha_N}}}\right.\right.$$
$$\left.\left.+\sum_{q\in\{L,N\}}\sum_{i,t\in\{M,m\}}p_i^U p_t^E\sum_{n=0}^{N_q-1}\sum_{c=1}^{C}\frac{\pi R_U}{2Cn!}\sqrt{1-x_c^2}\times\left(\frac{N_q\gamma\sigma_E^2(v_j^2+H^2)^{\frac{\alpha_q}{2}}}{P_U G_i^U G_t^E\beta_q}\right)^n e^{-\frac{N_q\gamma\sigma_E^2(v_c^2+H^2)^{\frac{\alpha_q}{2}}}{P_U G_i^U G_t^E\beta_q}}P_q(v_c)v_c\right]\right\}. \quad (17)$$

where step (b) is based on (14) and step (c) is obtained according to Eq. (3.381.9) in [35], . Substituting (19) into (18), we can derive $\mathcal{F}_1(\gamma)$. As the beam transmitted from S is aligned with the direction from S to U, we have $G_{SE}=G_m^S G_i^E, i\in\{M,m\}$.

For convenience, let $\mathcal{F}_2(\gamma)=\mathbb{E}\left[\prod_{E\in\Phi_E}\Pr\{\gamma_{UE}<\gamma\}\right]$. Using thinning theorem in the point process, the eavesdroppers can be divided into a LoS PPP Φ_E^L with density $\lambda_E P_L(r)$ and a NLoS PPP Φ_E^N with density $\lambda_E P_N(r)$, respectively. Therefore, $\mathcal{F}_2(\gamma)$ can be further expressed as

$$\mathcal{F}_2(\gamma)=\mathbb{E}\left[\prod_{E\in\Phi_E^L}\Pr\{\gamma_{UE}^L<\gamma\}\right]\mathbb{E}\left[\prod_{E\in\Phi_E^N}\Pr\{\gamma_{UE}^N<\gamma\}\right]. \quad (20)$$

Similar to (18), we can get

$$\mathbb{E}\left[\prod_{E\in\Phi_E^L}\Pr\{\gamma_{UE}^L<\gamma\}\right]=\exp\left\{-2\pi\lambda_E\times\sum_{i,t\in\{M,m\}}p_i^U p_t^E\right.$$
$$\left.\times\int_0^{R_U}\Pr\left\{h_{UE}>\frac{\gamma\sigma_E^2(r^2+H^2)^{\frac{\alpha_L}{2}}}{P_U G_{UE}\beta_L}\right\}P_L(r)rdr\right\}. \quad (21)$$

Denoting $d=\sqrt{r^2+H^2}$, we have

$$\int_0^{R_U}\Pr\left\{h_{UE}>\frac{\gamma\sigma_E^2(r^2+H^2)^{\frac{\alpha_L}{2}}}{P_U G_{UE}\beta_L}\right\}P_L(r)rdr$$
$$=\sum_{n=0}^{N_L-1}\int_0^{R_U}\left(\frac{N_L\gamma\sigma_E^2 d^{\alpha_L}}{P_U G_{UE}\beta_L}\right)^n\frac{1}{n!}e^{-\frac{N_L\gamma\sigma_E^2 d^{\alpha_L}}{P_U G_{UE}\beta_L}}P_L(r)rdr$$
$$\overset{(d)}{=}\sum_{n=0}^{N_L-1}\sum_{c=1}^{C}\frac{\pi R_U}{2Cn!}\sqrt{1-x_c^2}\left(\frac{N_L\gamma\sigma_E^2(v_c^2+H^2)^{\frac{\alpha_L}{2}}}{P_U G_{UE}\beta_L}\right)^n$$
$$\times e^{-\frac{N_L\gamma\sigma_E^2(v_c^2+H^2)^{\frac{\alpha_L}{2}}}{P_U G_{UE}\beta_L}}P_L(v_c)v_c. \quad (22)$$

Step (d) is computed by using Gauss-Chebyshev integration [36], with $x_c=\cos(\frac{2c-1}{2C}\pi)$ and $v_c=\frac{R_U}{2}(x_c+1)$. C denotes the number of the cumulative times.

In the same way, $\mathbb{E}\left[\prod_{E\in\Phi_E^N}\Pr\{\gamma_{UE}^N<\gamma\}\right]$ can be derived as

$$\mathbb{E}\left[\prod_{E\in\Phi_E^N}\Pr\left\{\gamma_{UE}^N<\gamma\right\}\right]$$
$$=\exp\left\{-2\pi\lambda_E\sum_{i,t\in\{M,m\}}p_i^U p_t^E\sum_{n=0}^{N_N-1}\sum_{c=1}^{C}\frac{\pi R_U}{2Cn!}\sqrt{1-x_c^2}\right.$$
$$\left.\times\left(\frac{N_N\gamma\sigma_E^2(v_c^2+H^2)^{\frac{\alpha_N}{2}}}{P_U G_{UE}\beta_N}\right)^n e^{-\frac{N_N\gamma\sigma_E^2(v_c^2+H^2)^{\frac{\alpha_N}{2}}}{P_U G_{UE}\beta_N}}P_N(v_c)v_c\right\}. \quad (23)$$

By substituting (21), (22) and (23) into (20), we can obtain $\mathcal{F}_2(\gamma)$. Finally, $F_{\gamma_E}(\gamma)$ can be given as (17) by multiplying $\mathcal{F}_1(\gamma)$ with $\mathcal{F}_2(\gamma)$. ■

Using (12b) and (17), P_{sop} can be calculated according to (11). However, the integral does not have a closed-form expression due to the complicated expressions in (12b) and (17). Hence, Gauss-Chebyshev quadrature is exploited to achieve a close approximation. Particularly, it should satisfy $(1+y)2^{-2R_{th}}-1>0$ in (11), and accordingly the lower limit of the integral is changed into $y_0=2^{2R_{th}}-1$. By means of variable substitution, i.e., $y=y_0+\tan t$, we can approximate P_{sop} as

$$P_{sop}=1-\int_{y_0}^{\infty}F_{\gamma_E}\left((1+y)2^{-2R_{th}}-1\right)f_{\gamma_D}(y)dy$$
$$=1-\int_0^{\frac{\pi}{2}}F_{\gamma_E}\left((1+y_0+\tan t)2^{-2R_{th}}-1\right)f_{\gamma_D}(y_0+\tan t)\sec^2 t dt$$
$$\approx 1-\frac{\pi^2}{4C}\sum_{c=1}^{C}\sqrt{1-u_c^2}F_{\gamma_E}\left((1+y_0+\tan\frac{\pi}{4}(u_c+1))2^{-2R_{th}}-1\right)$$
$$\times f_{\gamma_D}(y_0+\tan\frac{\pi}{4}(u_c+1))\sec^2\frac{\pi}{4}(u_c+1), \quad (24)$$

where $u_c=\cos(\frac{2c-1}{2C}\pi)$ and C denotes the number of

$$\mathcal{L}1(\gamma)=\sum_{i,j\in\{L,N\}}P_i(r_{SU})P_j(r_{UD})(P_DG_{DU}L(d_{DU}))^{-N_j}\frac{N_j^{N_j}}{\Gamma(N_j)}e^{-\frac{N_i\gamma\sigma_U^2}{P_SG_{SU}L(d_{SU})}}\sum_{n=0}^{N_i-1}\frac{(N_i\gamma)^n}{n!(P_SG_{SU}L(d_{SU}))^n}$$
$$\times\sum_{k=0}^{n}C_n^k\sigma_U^{2(n-k)}(N_j-1+k)!\left(\frac{N_i\gamma}{P_SG_{SU}L(d_{SU})}+\frac{N_j}{P_DG_{DU}L(d_{DU})}\right)^{-k-N_j}, \tag{33a}$$

$$\mathcal{L}2(\gamma)=\sum_{i,j\in\{L,N\}}P_i(r_{UD})P_j(r_{JD})(P_JG_{JD}L(d_{JD}))^{-N_j}\frac{N_j^{N_j}}{\Gamma(N_j)}e^{-\frac{N_i\gamma\sigma_D^2}{P_UG_{UD}L(d_{UD})}}\sum_{n=0}^{N_i-1}\frac{(N_i\gamma)^n}{n!(P_UG_{UD}L(d_{UD}))^n}$$
$$\times\sum_{k=0}^{n}C_n^k\sigma_U^{2(n-k)}(N_j-1+k)!\left(\frac{N_i\gamma}{P_UG_{UD}L(d_{UD})}+\frac{N_j}{P_JG_{JD}L(d_{JD})}\right)^{-k-N_j}. \tag{33b}$$

Gauss-Chebyshev nodes. Thus, for any given R_{th}, we can calculate P_{sop} in the UAV-based mmWave relaying network by substituting (12b) and (17) into (24).

Remark 1: According to (12b), (17) and (24), the SOP will increase with R_{th} and is determined by the UAV altitude H, the transmit power P_S and P_U, and the density λ_E. We can easily find that the SOP monotonically increases with λ_E. It is known that the communication quality of LoS links outperforms that of NLoS links under the same transmission distance. As the altitude of UAV increases, the LoS probabilities $P_L(r_{SU})$ and $P_L(r_{UD})$ increase, while the communication distances d_{SU} and d_{UD} will also increase. This indicates that the altitude of UAV should be moderately designed to reach a lower path loss of legitimate transmission. The approximation error of the Gauss-Chebyshev quadrature can be reduced by increasing the number of nodes.

IV. Secrecy Analysis With Cooperative Jamming

In this section, we consider the secrecy performance of the UAV-based relaying network with cooperative jamming. During the first time slot, S sends signals to U and D transmits jamming signals at the same time to degrade the eavesdropping channels as shown in Fig. 1(a). In the second time slot, the jamming UAV J as a friendly jammer transmits jamming signals to enhance the secrecy performance as shown in Fig. 1(b). To alleviate the jamming at U in the first time slot, we assume that D adjusts the beamforming randomly but only transmits jamming signals in horizontal directions. Similarly, J adjusts the antenna steering orientation to misalign D with the partial channel state information of D in the second time slot. Therefore, we consider the antenna gains of jamming signals from D to U and from J to D as $G_{DU}=G_m^DG_m^U$ and $G_{JD}=G_m^JG_m^D$, respectively. In addition, $G_{DE}=G_i^DG_j^E, i,j\in\{M,m\}$ denotes the antenna gain between D and E with probability $\tilde{p}_i^Dp_j^E$, and $G_{JE}=G_i^JG_j^E, i,j\in\{M,m\}$ with probability $p_i^Jp_j^E$ is the antenna gain between J and E. Specifically, p_i^J (G_i^J) and p_j^E (G_j^E) follow (3) and (4), respectively. $\tilde{p}_M^D=\frac{\psi_D}{2\pi}$ and $\tilde{p}_m^D=1-\frac{\psi_D}{2\pi}$.

With the jamming signal as the interference, the signal-to-interference-plus-noise ratio (SINR) at D can be written as

$$\gamma_D^J=\min\left(\gamma_{SU}^J,\gamma_{UD}^J\right), \tag{25}$$

where

$$\gamma_{SU}^J=\frac{P_SG_{SU}L(d_{SU})h_{SU}}{P_DG_{DU}L(d_{DU})h_{DU}+\sigma_U^2}, \tag{26}$$
$$\gamma_{UD}^J=\frac{P_UG_{UD}L(d_{UD})h_{UD}}{P_JG_{JD}L(d_{JD})h_{JD}+\sigma_D^2}. \tag{27}$$

The highest eavesdropping SINR among all the eavesdroppers can be expressed as

$$\gamma_E^J=\max\left(\max_{E\in\Phi_E}\gamma_{SE}^J,\max_{E\in\Phi_E}\gamma_{UE}^J\right), \tag{28}$$

where

$$\gamma_{SE}^J=\frac{P_SG_{SE}L(d_{SE})h_{SE}}{P_DG_{DE}L(d_{DE})h_{DE}+\sigma_E^2}, \tag{29}$$
$$\gamma_{UE}^J=\frac{P_UG_{UE}L(d_{UE})h_{UE}}{P_JG_{JE}L(d_{JE})h_{JE}+\sigma_E^2}. \tag{30}$$

Similar to (11), when the threshold of secrecy rate is set as R_{th}, the SOP of the UAV-based relaying network utilizing cooperative jamming can be derived as

$$P_{sop}^J=Pr\left\{\frac{1}{2}\log_2(1+\gamma_D^J)-\frac{1}{2}\log_2(1+\gamma_E^J)<R_{th}\right\}$$
$$=1-\int_0^\infty F_{\gamma_E}^J\left((1+y)2^{-2R_{th}}-1\right)f_{\gamma_D}^J(y)dy, \tag{31}$$

where $F_{\gamma_E}^J(\cdot)$ is the CDF of γ_E^J and $f_{\gamma_D}^J(\cdot)$ is the PDF of γ_D^J in the cooperative jamming scheme. Thus, we need to find the distributions of the SINR at D as well as at the eavesdropper with the highest eavesdropping SINR in the following.

Theorem 3: The CDF of γ_D^J can be obtain as

$$F_{\gamma_D^J}(\gamma)=\Pr\left\{\min\left(\gamma_{SU}^J,\gamma_{UD}^J\right)<\gamma\right\}$$
$$=1-\underbrace{\Pr\left\{\gamma_{SU}^J>\gamma\right\}}_{\mathcal{L}1(\gamma)}\underbrace{\Pr\left\{\gamma_{UD}^J>\gamma\right\}}_{\mathcal{L}2(\gamma)}, \tag{32}$$

where $\mathcal{L}1(\gamma)$ and $\mathcal{L}2(\gamma)$ are given in (33a) and (33b) at the top of this page.

Proof: Let $Y_1=P_SG_{SU}L(d_{SU})h_{SU}$ and $Y_2=P_UG_{UD}L(d_{UD})h_{UD}$, and we have

$$\mathcal{L}1(\gamma)=\Pr\left\{\gamma_{SU}^{J}>\gamma\right\}=\Pr\left\{\frac{Y_1}{Y_2+\sigma_U^2}>\gamma\right\}$$
$$=1-\Pr\left\{Y_1<\gamma(Y_2+\sigma_U^2)\right\}$$
$$=1-\int_0^{\infty}F_{Y_1}\left(\gamma(y_2+\sigma_U^2)\right)f_{Y_2}(y_2)dy_2. \quad (34)$$

According to (13) and (14), the CDF $F_{Y_1}(y_1)$ and the PDF $f_{Y_2}(y_2)$ can be given as

$$F_{Y_1}(y_1)=1-\sum_{n=0}^{N_i-1}\left(\frac{N_i y_1}{P_S G_{SU} L(d_{SU})}\right)^n\frac{1}{n!}e^{-\frac{N_i y_1}{P_S G_{SU} L(d_{SU})}}, \quad (35a)$$

$$f_{Y_2}(y_2)=\left(\frac{N_i}{P_D G_{DU} L(d_{DU})}\right)^{N_i}\frac{y_2^{N_i-1}}{\Gamma(N_i)}e^{-\frac{N_i y_2}{P_D G_{DU} L(d_{DU})}}. \quad (35b)$$

Using (35a) and (35b), $\mathcal{L}1(\gamma)$ is derived as (36) at the top of this page, and step (e) exploits Eq. (3.351-3) in [35]. Similarly, we can obtain the expression of $\mathcal{L}2(\gamma)$ as presented in (33b). ■

Furthermore, the derivation of (32) gives the PDF of γ_D^J as

$$f_{\gamma_D}^{J}(\gamma)=\frac{\partial F_{\gamma_D^J}(\gamma)}{\partial\gamma}=-\frac{\partial\mathcal{L}1(\gamma)}{\partial\gamma}\mathcal{L}2(\gamma)-\frac{\partial\mathcal{L}2(\gamma)}{\partial\gamma}\mathcal{L}1(\gamma), \quad (37)$$

where the derivatives of $\mathcal{L}1$ and $\mathcal{L}2$ are calculated as (38a) and (38b) at the top of the next page, respectively. As a result, the PDF of γ_D with cooperative jamming can be obtained by substituting (33a), (33b), (38a) and (38b) into (37).

In the following, we will derive the CDF of the highest eavesdropping SINR among all the eavesdroppers to calculate P_{sop}^{J}. To this end, the theoretical expressions of $\Pr\{\gamma_{SE}^{J}>\gamma\}$ and $\Pr\{\gamma_{UE}^{J}>\gamma\}$ are derived in the following theorem.

Theorem 4: For convenience, we define the functions $F_{E,1}(r,\theta)$ and $F_{E,2}(r,\theta)$ that are related to a distance variable and an angle variable to represent $\Pr\{\gamma_{SE}^{J}>\gamma\}$ and $\Pr\{\gamma_{UE}^{J}>\gamma\}$, respectively. The expressions are given by (39a) and (39b) on the next page. Particularly, in (39b), $r_{JE}=\sqrt{r^2+r_{UJ}^2-2rr_{UJ}\cos\theta}$ denotes the horizonal distance between J and E.

Proof: Comparing the expressions in (26) and (29), we can observe that γ_{SE}^{J} has a similar form with γ_{SU}^{J}. Similar to the proof of Theorem 3, $\Pr\{\gamma_{SE}^{J}>\gamma\}$ can be derived based on the expression of $\Pr\{\gamma_{SU}^{J}>\gamma\}$, as

$$\Pr\left\{\gamma_{SE}^{J}>\gamma\right\}=\Pr\left\{\frac{P_S G_{SE} L(d_{SE})h_{SE}}{P_D G_{DE} L(d_{DE})h_{DE}+\sigma_E^2}>\gamma\right\}$$
$$=\sum_{i,j,g\in\{M,m\}}p_i^E p_j^E \tilde{p}_g^D\sum_{n=0}^{N_N-1}\frac{N_N^{N_N}}{\Gamma(N_N)}(P_D G_g^D G_j^E\beta_N r_{DE}^{-\alpha_N})^{-N_N}$$
$$\times e^{-\frac{N_N\gamma\sigma_E^2 r_{SE}^{\alpha_N}}{P_S G_m^S G_i^E\beta_N}}\sum_{n=0}^{N_N-1}\frac{(N_N\gamma r_{SE}^{\alpha_N})^n}{n!(P_S G_m^S G_i^E\beta_N)^n}\sum_{k=0}^{n}C_n^k\sigma_U^{2(n-k)}$$
$$(N_N-1+k)!\left(\frac{N_N\gamma r_{SE}^{\alpha_N}}{P_S G_m^S G_i^E\beta_N}+\frac{N_N r_{DE}^{\alpha_N}}{P_D G_g^D G_j^E\beta_N}\right)^{-k-N_N}. \quad (40)$$

Since the distribution of eavesdroppers follows the PPP, r_{SE} and r_{DE} are variables depending on the location of E. Define $r=r_{SE}$, with $r_0\le r\le R_0$ and $\theta\in[0,2\pi]$ that are random variables denoting the distance from S to E and the angle between connecting lines SE and SD, respectively. Therefore, we have $r_{DE}=\sqrt{r^2+r_{SD}^2-2rr_{SD}\cos\theta}$ based on the law of cosines. Furthermore, $\Pr\{\gamma_{SE}^{J}>\gamma\}$ is replaced with the function $F_{E,1}(r,\theta)$ related to the two variables, i.e., r and θ. In this case, the expression of $F_{E,1}(r,\theta)$ can be obtained as (39a) by applying corresponding variable substitutions to (40).

Let $F_{E,2}(r,\theta)=\Pr\{\gamma_{UE}^{J}>\gamma\}$, where $r=r_{UE}$ represents the horizontal distance between U and E, and θ denotes the angle between connecting lines UE and UJ. After that, the horizontal distance from D to E can be calculated as $r_{DE}=\sqrt{r^2+r_{UJ}^2-2rr_{UJ}\cos\theta}$, where r_{UJ}^2 is the horizontal distance between J and U. With the UAV altitude H considered, the lengths of the two links between U and E and J and E can be written as $d_{UE}=\sqrt{r^2+H^2}$ and $d_{JE}=\sqrt{r_{JE}^2+H^2}$, respectively. Through the similar procedure of obtaining $F_{E,1}(r,\theta)$, we can derive $F_{E,2}(r,\theta)$ taking into consideration that the links from U (J) to eavesdroppers can be LoS or NLoS as

$$F_{E,2}(r,\theta)=\Pr\left\{\frac{P_U G_{UE} L(d_{UE})h_{UE}}{P_J G_{JE} L(d_{JE})h_{JE}+\sigma_E^2}>\gamma\right\}$$
$$=\sum_{q,v\in\{L,N\}}P_q(r_{UE})P_v(r_{JE})\sum_{i,j,g,w\in\{M,m\}}\frac{p_i^U p_j^E p_g^J p_w^E}{(P_J G_g^J G_w^E L(d_{JE}))^{N_v}}$$
$$\times\frac{N_v^{N_v}}{\Gamma(N_v)}e^{-\frac{N_q\gamma\sigma_E^2}{P_U G_i^U G_j^E L(d_{UE})}}\sum_{n=0}^{N_q-1}\frac{(N_q\gamma)^n}{n!(P_U G_i^U G_j^E L(d_{UE}))^n}$$
$$\times\sum_{k=0}^{n}\left(\frac{N_q\gamma}{P_U G_i^U G_j^E L(d_{UE})}+\frac{N_v}{P_J G_g^J G_w^E L(d_{JE})}\right)^{-k-N_v}$$
$$\times C_n^k\sigma_E^{2(n-k)}(N_v-1+k)! \quad \triangleq \quad (39b). \quad (41)$$

Similarly, the equality in (41) holds by applying corresponding variable substitutions. ■

Based on Theorem 4, we can obtain the CDF of the highest eavesdropping SINR among all the eavesdroppers when cooperative jamming is considered, which can be written as

$$F_{\gamma_E}^{J}(\gamma)=\underbrace{\mathbb{E}\left[\prod_{E\in\Phi_E}\Pr\{\gamma_{SE}^{J}<\gamma\}\right]}_{\mathcal{F}_1^J(\gamma)}\underbrace{\mathbb{E}\left[\prod_{E\in\Phi_E}\Pr\{\gamma_{UE}^{J}<\gamma\}\right]}_{\mathcal{F}_2^J(\gamma)}. \quad (42)$$

Particularly, by utilizing the probability generating function of PPP and a two-layer Gauss-Chebyshev quadrature equation, $F_{\gamma_E}^{J}(\gamma)$ can be derived as

$$\mathcal{F}_1^J(\gamma)=\exp\left\{\lambda_E\int_0^{2\pi}\int_{r_0}^{R_0}\Pr\{\gamma_{SE}^{J}>\gamma\}rdrd\theta\right\}$$
$$=\exp\left\{\lambda_E\int_0^{2\pi}\int_{r_0}^{R_0}F_{E,1}(r,\theta)rdrd\theta\right\}$$
$$\approx\exp\left(-\lambda_E\sum_{l=1}^{L}\sum_{t=1}^{T}\sqrt{1-x_l^2}\sqrt{1-y_t^2}\left(\frac{R_0-r_0}{2}y_t+\frac{R_0+r_0}{2}\right)\right.$$
$$\left.\times\frac{\pi^3(R_0-r_0)}{2TL}F_{E,1}\left(\frac{R_0-r_0}{2}y_t+\frac{R_0+r_0}{2},\pi(x_l+1)\right)\right), \quad (43)$$

$$\mathcal{L}1(\gamma)=1-\int_0^{\infty} f_{Y_2}(y_2)\left[1-\sum_{n=0}^{N_i-1}\left(\frac{N_i\gamma(y_2+\sigma_U^2)}{P_S G_{SU} L(d_{SU})}\right)^n \frac{1}{n!} e^{-\frac{N_i\gamma(y_2+\sigma_U^2)}{P_S G_{SU} L(d_{SU})}}\right] dy_2$$

$$=\int_0^{\infty} f_{Y_2}(y_2)\sum_{n=0}^{N_i-1}\left(\frac{N_i\gamma(y_2+\sigma_U^2)}{P_S G_{SU} L(d_{SU})}\right)^n \frac{1}{n!} e^{-\frac{N_i\gamma(y_2+\sigma_U^2)}{P_S G_{SU} L(d_{SU})}} dy_2$$

$$=\sum_{i,j\in\{L,N\}} P_i(r_{SU})P_j(r_{UD})\int_0^{\infty}\left(\frac{N_j}{P_D G_{DU} L(d_{DU})}\right)^{N_j}\frac{y_2^{N_j-1}}{\Gamma(N_j)} e^{-\frac{N_j y_2}{P_D G_{DU} L(d_{DU})}}\sum_{n=0}^{N_i-1}\left(\frac{N_i\gamma(y_2+\sigma_U^2)}{P_S G_{SU} L(d_{SU})}\right)^n \frac{1}{n!} e^{-\frac{N_i\gamma(y_2+\sigma_U^2)}{P_S G_{SU} L(d_{SU})}} dy_2$$

$$=\sum_{i,j\in\{L,N\}} P_i(r_{SU})P_j(r_{UD})\sum_{n=0}^{N_i-1}\frac{N_j^{N_j}(N_i\gamma)^n}{\Gamma(N_j)n!} e^{-\frac{N_i\gamma\sigma_U^2}{P_S G_{SU} L(d_{SU})}}\frac{(P_S G_{SU} L(d_{SU}))^{-n}}{(P_D G_{DU} L(d_{DU}))^{N_j}}\int_0^{\infty} y_2^{N_j-1}(y_2+\sigma_U^2)^n e^{-y_2\left(\frac{N_i\gamma}{P_S G_{SU} L(d_{SU})}+\frac{N_j}{P_D G_{DU} L(d_{DU})}\right)} dy_2$$

$$=\sum_{i,j\in\{L,N\}} P_i(r_{SU})P_j(r_{UD})\sum_{n=0}^{N_i-1}\frac{(P_S G_{SU} L(d_{SU}))^{-n}}{(P_D G_{DU} L(d_{DU}))^{N_j}}\frac{N_j^{N_j}(N_i\gamma)^n}{\Gamma(N_j)n!} e^{-\frac{N_i\gamma\sigma_U^2}{P_S G_{SU} L(d_{SU})}}\sum_{k=0}^{n} C_n^k \sigma_U^{2(n-k)}\int_0^{\infty} y_2^{N_j-1+k} e^{-y_2\left(\frac{N_i\gamma}{P_S G_{SU} L(d_{SU})}+\frac{N_j}{P_D G_{DU} L(d_{DU})}\right)} dy_2$$

$$\overset{(e)}{=}\sum_{i,j\in\{L,N\}} P_i(r_{SU})P_j(r_{UD})(P_D G_{DU} L(d_{DU}))^{-N_j}\frac{N_j^{N_j}}{\Gamma(N_j)} e^{-\frac{N_i\gamma\sigma_U^2}{P_S G_{SU} L(d_{SU})}}\sum_{n=0}^{N_i-1}\frac{(N_i\gamma)^n}{n!(P_S G_{SU} L(d_{SU}))^n}$$
$$\times\sum_{k=0}^{n} C_n^k \sigma_U^{2(n-k)}(N_j-1+k)!\left(\frac{N_i\gamma}{P_S G_{SU} L(d_{SU})}+\frac{N_j}{P_D G_{DU} L(d_{DU})}\right)^{-k-N_j}. \tag{36}$$

$$\frac{\partial\mathcal{L}1(\gamma)}{\partial\gamma}=\sum_{i,j\in\{L,N\}}\frac{P_i(r_{SU})P_j(r_{UD})}{(P_D G_{DU} L(d_{DU}))^{N_j}}\frac{N_j^{N_j}}{\Gamma(N_j)}\sum_{n=0}^{N_i-1}\sum_{k=0}^{n}\frac{(N_i)^n C_n^k \sigma_U^{2(n-k)}(N_j-1+k)!}{n!(P_S G_{SU} L(d_{SU}))^n}\left(\frac{N_i\gamma}{P_S G_{SU} L(d_{SU})}+\frac{N_j}{P_D G_{DU} L(d_{DU})}\right)^{-k-N_j}$$
$$\times\gamma^n e^{-\frac{N_i\gamma\sigma_U^2}{P_S G_{SU} L(d_{SU})}}\left[n\gamma^{-1}-\frac{N_i\sigma_U^2}{P_S G_{SU} L(d_{SU})}-\frac{N_i(k+N_j)}{(P_S G_{SU} L(d_{SU}))^n}\left(\frac{N_i\gamma}{P_S G_{SU} L(d_{SU})}+\frac{N_j}{P_D G_{DU} L(d_{DU})}\right)^{-1}\right], \tag{38a}$$

$$\frac{\partial\mathcal{L}2(\gamma)}{\partial\gamma}=\sum_{i,j\in\{L,N\}}\frac{P_i(r_{UD})P_j(r_{JD})}{(P_J G_{JD} L(d_{JD}))^{N_j}}\frac{N_j^{N_j}}{\Gamma(N_j)}\sum_{n=0}^{N_i-1}\sum_{k=0}^{n}\frac{(N_i)^n C_n^k \sigma_D^{2(n-k)}(N_j-1+k)!}{n!(P_U G_{UD} L(d_{UD}))^n}\left(\frac{N_i\gamma}{P_U G_{UD} L(d_{UD})}+\frac{N_j}{P_J G_{JD} L(d_{JD})}\right)^{-k-N_j}$$
$$\times\gamma^n e^{-\frac{N_i\gamma\sigma_U^2}{P_U G_{UD} L(d_{UD})}}\left[n\gamma^{-1}-\frac{N_i\sigma_U^2}{P_U G_{UD} L(d_{UD})}-\frac{N_i(k+N_j)}{(P_U G_{UD} L(d_{UD}))^n}\left(\frac{N_i\gamma}{P_U G_{UD} L(d_{UD})}+\frac{N_j}{P_J G_{JD} L(d_{JD})}\right)^{-1}\right]. \tag{38b}$$

$$F_{E,1}(r,\theta)=\sum_{i,j,g\in\{M,m\}} p_i^E p_j^E \tilde{p}_g^D \frac{N_N^{N_N}}{\Gamma(N_N)}(P_D G_g^D G_j^E \beta_N)^{-N_N}(r^2+r_{SD}^2-2rr_{SD}\cos\theta)^{\frac{\alpha_N N_N}{2}} e^{-\frac{N_N\gamma\sigma_E^2 r^{\alpha_N}}{P_S G_m^S G_i^E \beta_N}},$$
$$\times\sum_{n=0}^{N_N-1}\frac{(N_N\gamma)^n r^{\alpha_N n}}{n!(P_S G_m^S G_i^E \beta_N)^n}\sum_{k=0}^{n} C_n^k \sigma_U^{2(n-k)}(N_N-1+k)!\left(\frac{N_N\gamma r^{\alpha_N}}{P_S G_m^S G_i^E \beta_N}+\frac{N_N(r^2+r_{SD}^2-2rr_{SD}\cos\theta)^{\frac{\alpha_N}{2}}}{P_D G_g^D G_j^E \beta_N}\right)^{-k-N_N}, \tag{39a}$$

$$F_{E,2}(r,\theta)=\sum_{q,v\in\{L,N\}} P_i(r)P_j(r_{JE})\sum_{i,j,g,w\in\{M,m\}} p_i^U p_j^E p_g^J p_w^E \frac{N_v^{N_v}}{\Gamma(N_v)}(P_J G_g^J G_w^E \beta_v)^{-N_v}(r_{JE}^2+H^2)^{\frac{\alpha_v N_v}{2}} e^{-\frac{N_q\gamma\sigma_E^2(r^2+H^2)^{\frac{\alpha_q}{2}}}{P_U G_i^U G_j^E \beta_q}}$$
$$\times\sum_{n=0}^{N_q-1}\frac{(N_q\gamma)^n(r^2+H^2)^{\frac{\alpha_q n}{2}}}{n!(P_U G_i^U G_j^E \beta_q)^n}\sum_{k=0}^{n} C_n^k \sigma_E^{2(n-k)}(N_v-1+k)!\left(\frac{N_q\gamma(r^2+H^2)^{\frac{\alpha_q}{2}}}{P_U G_i^U G_j^E \beta_q}+\frac{N_v(r_{JE}^2+H^2)^{\frac{\alpha_v}{2}}}{P_J G_g^J G_w^E \beta_v}\right)^{-k-N_v}. \tag{39b}$$

TABLE I
SIMULATION PARAMETERS

Constant values in the Urban Environment	$a = 9.6$, $b = 0.28$
Nakagami fading parameters	$N_L = 3$, $N_N = 2$
Path loss parameters	$\alpha_L = 2$, $\beta_L = 10^{-6.4}$, $\alpha_N = 2.92$, $\beta_N = 10^{-7.2}$
Transmission bandwidth	$BW = 1$ GHz
Noise figure	$NF = 10$ dB
Noise power	$-174 + 10\lg(BW) + NF$ dBm
The density of eavesdroppers	$\lambda_E = 10^{-4}/\text{m}^2$
Minimum/maximum connection distance from S to E	$r_0 = 20$ m, $R_0 = 500$ m
The number of Gauss-Chebyshev nodes	$C = L = T = 100$
Number of antennas	$N = 16$
Half-power beamwidth	$\psi_j = \theta_j = \sqrt{\frac{3}{N}}$
Main-lobe gain	$G_M^j = N$
Side-lobe gain	$G_m^j = \frac{\sqrt{N} - \frac{\sqrt{3}}{2\pi} N \sin(\frac{\sqrt{3}}{2\sqrt{N}})}{\sqrt{N} - \frac{\sqrt{3}}{2\pi} \sin(\frac{\sqrt{3}}{2\sqrt{N}})}$

where $x_l = \cos(\frac{2l-1}{2L}\pi)$ and $y_t = \cos(\frac{2t-1}{2T}\pi)$ are Gauss-Chebyshev nodes corresponding to θ and r, respectively. Similarly, we can obtain $\mathcal{F}_2^J(\gamma)$ as

$$\mathcal{F}_2^J(\gamma) = \exp\left(- \lambda_E \frac{\pi^3 R_U}{2TL} \sum_{l=1}^{L} \sum_{t=1}^{T} \sqrt{1-x_l^2}\sqrt{1-y_t^2} \times F_{E,2}\left(\frac{R_U}{2}(y_t+1), \pi(x_l+1)\right) \frac{R_U}{2}(y_t+1)\right). \quad (44)$$

As a result, $F_{\gamma_E}^J(\gamma)$ can be calculated by substituting (43) and (44) into (42).

Similar to (24), the analytical expression for SOP in the UAV-based relaying network with cooperative jamming can be given as

$$P_{sop}^J \approx 1 - \frac{\pi^2}{4C} \sum_{c=1}^{C} \sqrt{1-u_c^2} f_{\gamma_D}^J(y_0 + \tan\frac{\pi}{4}(u_c+1)) \times F_{\gamma_E}^J\left((1+y_0+\tan\frac{\pi}{4}(u_c+1))2^{-2R_{th}}-1\right)\sec^2\frac{\pi}{4}(u_c+1), \quad (45)$$

where $y_0 = 2^{2R_{th}} - 1$ and $u_c = \cos(\frac{2c-1}{2C}\pi)$. Finally, with $f_{\gamma_D}^J(\gamma)$ and $F_{\gamma_E}^J(\gamma)$ derived above, we can calculate the SOP by substituting them into (45).

Remark 2: A lot of system parameters can affect the secrecy performance. The impacts of H and λ_E are similar to what is in Remark 1. Also, the jamming transmit power is important. It is not necessarily true that the larger the jamming power is, the lower the SOP will be. This is because the jamming signals not only degrade the eavesdropping channels but also interfere with the legitimate transmission. Note that the SOP expression in (45) specializes to the one without jamming by setting $P_J = P_D = 0$.

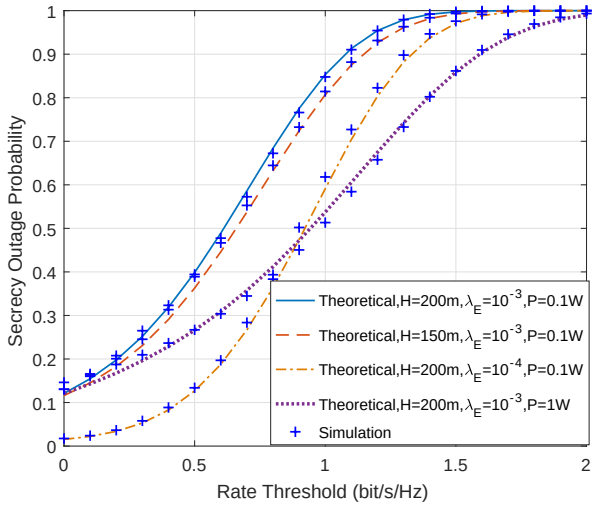


Fig. 2. The secrecy outage probability without jamming, with $P_S = P_U = P$.

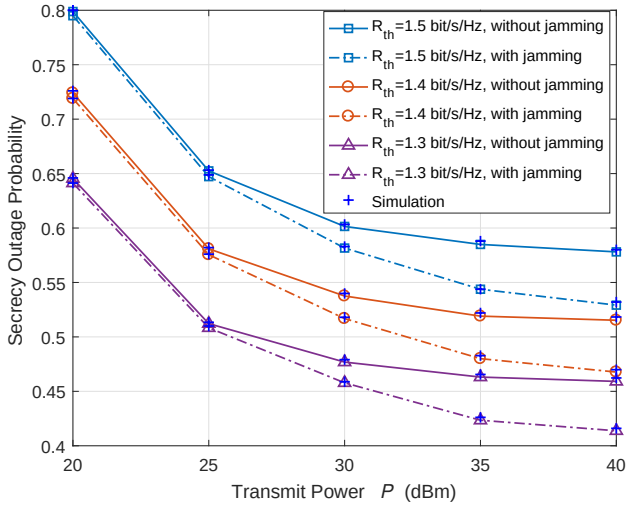


Fig. 3. The secrecy outage probability versus the transmit power P, with $H = 200$ m, $N = 32$ and $\lambda_E = 5 \times 10^{-3}/\text{m}^2$.

V. SIMULATION RESULTS AND DISCUSSIONS

In this section, numerical results are presented to demonstrate the secrecy performance of the UAV-based mmWave relaying network. Unless otherwise stated, the simulation parameters are listed in Table I. Without loss of generality, we set $N_j = N, j \in \{S, D, E, U, J\}$ and the main-lobe beamwidth, main-lobe and side-lobe gains are shown in Table I. In addition, Monte Carlo simulations are conducted to validate the theoretical results.

Without loss of generality, we consider a Cartesian coordinate, where S is placed at the origin with the coordinate $\mathbf{W}_S = [0, 0]$, the coordinate of D is assumed as $\mathbf{W}_D = [400, 0]$, and the location of U projected on the ground is $\mathbf{W}_U = [200, 0]$. First, we evaluate the secrecy performance of the network without jamming for different system parameters in Fig. 2. It can be observed that the theoretical results match

well with the Monte-Carlo simulation. The results show that the SOP increases with the rate threshold R_{th}, as expected. In addition, better secrecy outage probability can be obtained for $H = 150$ m than $H = 200$ m, but there is only a narrow gap between the two curves. When the density of eavesdroppers λ_E decreases from $10^{-3}/\text{m}^2$ to $10^{-4}/\text{m}^2$, a significant improvement of secrecy performance can be achieved. Comparing the two curves of different transmit power P, we can see a wide gap between them, which implies that the SOP can be dramatically decreased by increasing the transmit power. As analyzed in Remark 1, the results in Fig. 2 demonstrate that the system parameters, such as the UAV altitude, the density of eavesdroppers and the transmit power, can affect the secrecy performance.

In Fig. 3, we plot the SOP versus the transmit power P with the two proposed schemes, where $P_S = P_U = P$ and $P_D = P_J = P/2$. For the cooperative jamming scheme, the location of the jamming UAV is set as $\mathbf{W}_J = [200, 50]$. In both schemes, one can see that the SOP decreases as P increases and finally approaches a lower limit. This is because the gap of qualities between the wiretapping channels and legitimate channels expands as the transmit power increases. However, when P is large enough, the gap of their channel capacities becomes constant. The effect of cooperative jamming on the secrecy outage probability is illustrated by comparing the curves with and without jamming. More specifically, the gap of SOP between the two schemes enlarges when P increases, which indicates that the performance improvement of SOP by employing cooperative jamming is more significant when higher transmit power is available. Therefore, we should employ cooperative jamming and properly improve the transmit power to effectively enhance the secrecy performance in practice. In the following, we will focus on evaluating the secrecy performance of the UAV-based relaying network with cooperative jamming.

In Fig. 4, we investigate the effect of λ_E on the SOP with cooperative jamming when adopting different number of antennas and rate thresholds. We set $P_S = P_U = 0.1$ W, $P_D = P_J = 0.05$ W and $H = 200$ m. The SOP increases with the increase of λ_E, due to the fact that there are more potential eavesdroppers around S and D trying to wiretap the confidential information and the channel quality with the highest eavesdropping SINR will be better. In the case of $N = 16$, the SOP is equal to 1 when $R_{th} = 2$ bit/s/Hz and is very close to 1 when $R_{th} = 1.5$ bit/s/Hz. The SOP can be significantly reduced by increasing the number of antennas. This is because equipping more antennas can enhance the main-lobe gain and meanwhile suppressing the side-lobe gain with narrower half-power beamwidth, which encourages the utilization of massive antennas in practical system designs.

Adopting the same power parameters as Fig. 4, Fig. 5 plots the SOP versus the height of UAVs H for the cooperative jamming scheme, with a step size of 50 m. It is seen that the SOP first decreases as H becomes higher and then increases with H. As a result, there exists an optimal value of H which achieves the optimal SOP. This is due to the tradeoff between the path-loss distance and the LoS probability when H varies. Also, the legitimate channel benefits more than the

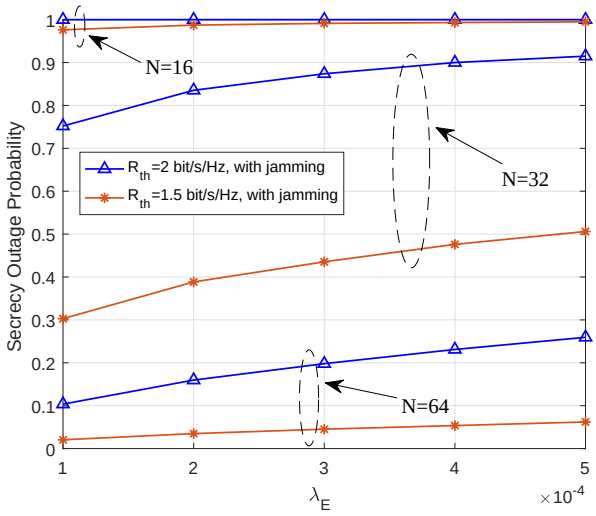


Fig. 4. The secrecy outage probability versus the eavesdropper density λ_E, with $P_S = P_U = 0.1$ W, $P_D = P_J = 0.05$ W and $H = 200$ m.

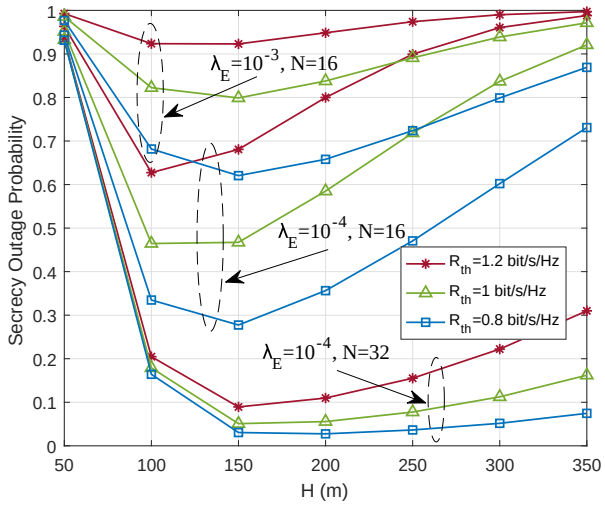


Fig. 5. The secrecy outage probability versus the height of the UAVs with cooperative jamming. $P_S = P_U = 0.1$ W and $P_D = P_J = 0.05$ W.

eavesdropping channel with the highest SINR in the low H regime, while the opposite is the case with higher H. We can also see that for the case $\lambda_E = 10^{-4}, N = 32$, the SOP first decreases much more dramatically but then grows at a very slow pace when H increases. This is because the quality of channels in this case is much more sensitive to H than that of the other two cases with higher density of eavesdroppers and smaller number of antennas. The results in Fig. 5 motivate us to find an optimal height of UAV to achieve the optimal secrecy performance for practical systems in the future.

To gain more insights, we investigate the impact of the power of jamming signals on the SOP in Figs. 6-9. Particularly, we set $\mathbf{W}_J = [200, 50]$, $P_S = P_U = 1$ W, $\lambda_E = 10^{-4}$ and $H = 100$ m in Fig. 6 and Fig. 7. By setting $P_D = 0$ W, we plot the SOP versus the transmit power of J in Fig. 6. As we can see, the SOP decreases almost linearly with P_J due to the fact that the jamming signals received at D is much weaker

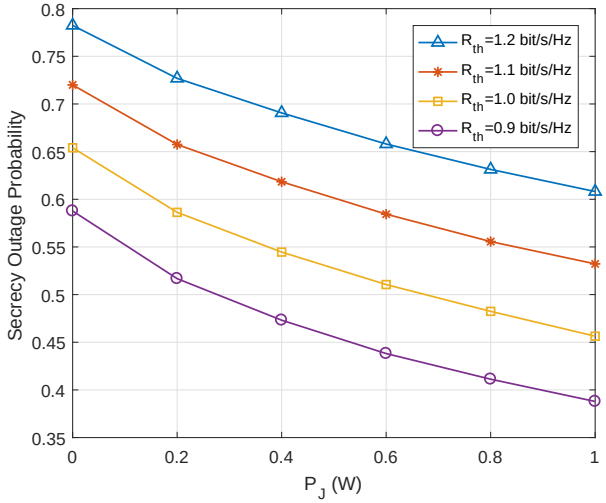


Fig. 6. The secrecy outage probability versus the transmit power of J with cooperative jamming. $P_D = 0$ W.

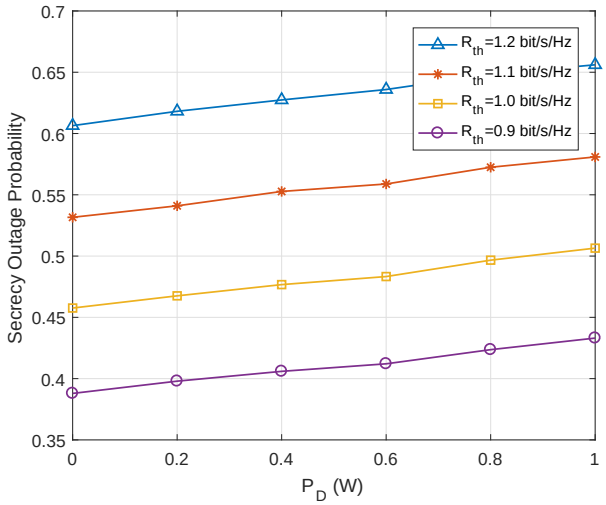


Fig. 7. The secrecy outage probability versus the jamming power of D with cooperative jamming. $P_J = 1$ W.

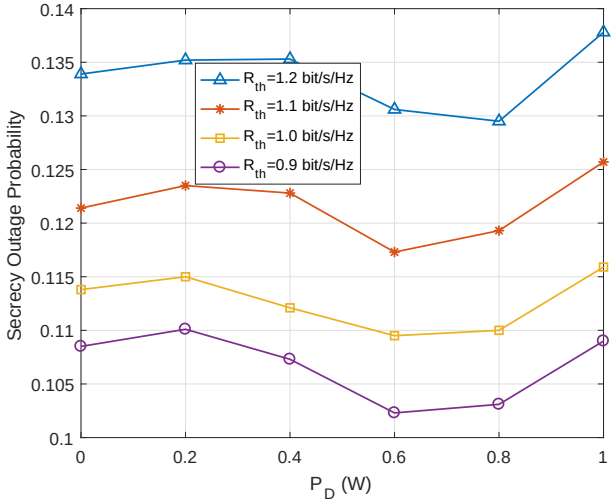


Fig. 8. The secrecy outage probability versus the jamming power of D with cooperative jamming. $P_J = 0$ W.

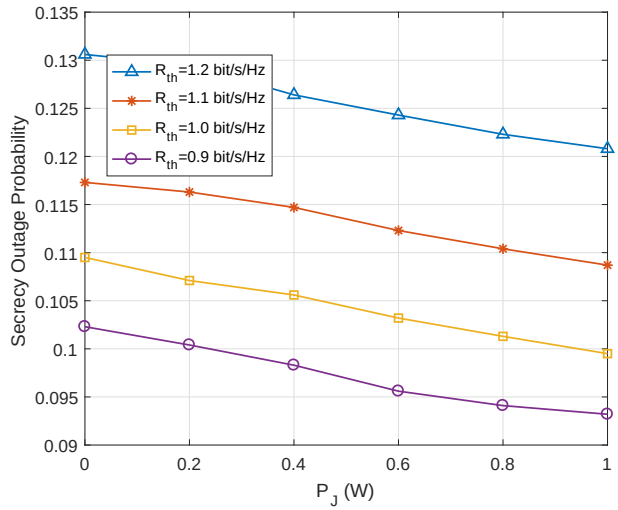


Fig. 9. The secrecy outage probability versus the transmit power of J with cooperative jamming. $P_D = 0.6$ W.

than eavesdroppers. This can be explained by the fact that the beam direction of J is set not to align D. In this context, it is reasonable for us to choose $P_J = 1$ W when the transmit power of J is limited by the maximum value 1 W. Setting $P_J = 1$ W, Fig. 7 depicts the SOP versus the jamming power of D, P_D. By comparison, the SOP increases with P_D. This is because in this condition, the performance loss of U caused by the jamming from D is larger than that of the eavesdropper with the highest eavesdropping SINR. Thus, we can conclude that it is better to adopt $P_J = 1$ W and $P_D = 0$ W to achieve high secrecy performance in the considered cases.

Furthermore, we change some of the parameters as $\mathbf{W}_J = [150, 0]$, $\mathbf{W}_D = [450, 0]$, $\lambda_E = 5 \times 10^{-3}$ and $H = 500$ m, and analyze the SOP affected by the jamming power. In Fig. 8, one can see that the SOP is not monotonic with P_D and there is an optimal jamming power of D to minimize the SOP. The reason for this is that the rate performance of U is more sensitive to the jamming power of D as the channel between D and U is dominated by LoS in this case. When P_D is small, the receiving jamming power at U may be much weaker compared with its legitimate receiving signals while the jamming signals can degrade the SINR at eavesdroppers. However, as P_D gets large enough, the rate loss of U results from the jamming signals will be more severe than that of eavesdroppers. With $P_D = 0.6$ W, Fig. 9 shows the similar performance as in Fig. 6, and thus, we will not go into details here. As a result, under this case, it is preferable to set $P_J = 1$ W and $P_D = 0.6$ W to lower the SOP. The results shown in Figs. 6-9 reveal that there are the optimal values of P_J and P_D to achieve the optimal secrecy performance. Thus, we should jointly design the jamming power in the two time slots according to the practical system topologies and parameters.

VI. Conclusions and Future Work

In this paper, we have studied the secure transmission in UAV-based mmWave relaying networks, where Nakagami fading for LoS and NLoS links, and 3D directional transmissions are considered. Specifically, two transmission schemes have been proposed. The SOP of the proposed schemes have been analyzed. In both schemes, the CDF of the highest eavesdropping SINR among all the eavesdroppers and the PDF of the SINR at the destination have been derived to calculate the SOP. Simulation results have shown the effectiveness of the proposed schemes in guaranteeing the security of UAV-based mmWave relaying networks. In the future work, we will further improve the secrecy performance of UAV-based relaying networks via the mobility of UAVs.

References

[1] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[2] P. K. Sharma and D. I. Kim, "Coverage probability of 3-D mobile UAV networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 97–100, Feb. 2019.

[3] Y. Chen, N. Zhao, Z. Ding, and M. 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.

[4] C. You and R. Zhang, "3D trajectory optimization in Rician fading for UAV-enabled data harvesting," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3192–3207, Jun. 2019.

[5] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives," *IEEE Internet of Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.

[6] N. Zhao, X. Pang, Z. Li, Y. Chen, F. Li, Z. Ding, and M. Alouini, "Joint trajectory and precoding optimization for UAV-assisted NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3723–3735, May 2019.

[7] Y. Zeng, J. Lyu, and R. Zhang, "Cellular-connected UAV: Potential, challenges, and promising technologies," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 120–127, Feb. 2019.

[8] X. Pang, G. Gui, N. Zhao, W. Zhang, Y. Chen, Z. Ding, and F. Adachi, "Uplink precoding optimization for NOMA cellular-connected UAV networks," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 1271–1283, Feb. 2020.

[9] C. Zhang, W. Zhang, W. Wang, L. Yang, and W. Zhang, "Research challenges and opportunities of UAV millimeter-wave communications," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 58–62, Feb. 2019.

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

[11] J. Zhao, F. Gao, L. Kuang, Q. Wu, and W. Jia, "Channel tracking with flight control system for UAV mmwave MIMO communications," *IEEE Commun. Lett.*, vol. 22, no. 6, pp. 1224–1227, Jun. 2018.

[12] X. Yu, J. Zhang, and K. B. Letaief, "A hardware-efficient analog network structure for hybrid precoding in millimeter wave systems," *IEEE J. Sel. Topics in Signal Process.*, vol. 12, no. 2, pp. 282–297, May, 2018.

[13] X. Pang, J. Tang, N. Zhao, X. Zhang, and Y. Qian, "Energy-efficient design for mmWave-enabled NOMA-UAV networks," *Sci. China Inf. Sci.*, vol. 64, no. 4: 140303, Apr. 2021.

[14] 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.

[15] Y. Chen, W. Feng, and G. Zheng, "Optimum placement of UAV as relays," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 248–251, Feb. 2018.

[16] J. Chen and D. Gesbert, "Optimal positioning of flying relays for wireless networks: A LoS map approach," in *Proc. IEEE ICC'17*, pp. 1–6, Paris, France, May 2017.

[17] C. Pan, H. Ren, Y. Deng, M. Elkashlan, and A. Nallanathan, "Joint blocklength and location optimization for URLLC-enabled UAV relay systems," *IEEE Commun. Lett.*, vol. 23, no. 3, pp. 498–501, Mar. 2019.

[18] H. Ren, C. Pan, K. Wang, W. Xu, M. Elkashlan, and A. Nallanathan, "Joint transmit power and placement optimization for URLLC-enabled UAV relay systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 8003–8007, Jul. 2020.

[19] S. Zhang, H. Zhang, Q. He, K. Bian, and L. Song, "Joint trajectory and power optimization for UAV relay networks," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 161–164, Jan. 2018.

[20] L. Kong, L. Ye, F. Wu, M. Tao, G. Chen, and A. V. Vasilakos, "Autonomous relay for millimeter-wave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 9, pp. 2127–2136, Sep. 2017.

[21] L. Zhu, J. Zhang, Z. Xiao, X. Cao, X. Xia, and R. Schober, "Millimeter-wave full-duplex UAV relay: Joint positioning, beamforming, and power control," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 9, pp. 2057–2073, Sept. 2020.

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

[23] 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.

[24] W. Wang, J. Tang, N. Zhao, X. Liu, X. Y. Zhang, Y. Chen, and Y. Qian, "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, Aug. 2020.

[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] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R. Liao, "Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108–2117, Mar. 2018.

[27] R. Li, Z. Wei, L. Yang, D. W. K. Ng, J. Yuan, and J. An, "Resource allocation for secure multi-UAV communication systems with multi-eavesdropper," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4490–4506, Jul. 2020.

[28] Y. Cai, Z. Wei, R. Li, D. W. K. Ng, and J. Yuan, "Joint trajectory and resource allocation design for energy-efficient secure UAV communication systems," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4536–4553, Jul. 2020.

[29] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

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

[31] Z. Xiao, L. Zhu, and X. G. Xia, "UAV communications with millimeter-wave beamforming: Potentials, scenarios, and challenges," *China Commun.*, vol. 17, no. 9, pp. 147–166, Sept. 2020.

[32] 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.

[33] W. Yuan, C. Liu, F. Liu, S. Li, and D. W. K. Ng, "Learning-based predictive beamforming for UAV communications with jittering," *IEEE Wireless Commun. Lett.*, vol. 9, no. 11, pp. 1970–1974, Nov. 2020.

[34] 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.

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

[36] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 938–953, Apr. 2016.