Manuscript version: Author’s Accepted Manuscript
The version presented in WRAP is the author’s accepted manuscript and may differ from the published version or Version of Record.

Persistent WRAP URL:
http://wrap.warwick.ac.uk/150078

How to cite:
Please refer to published version for the most recent bibliographic citation information. If a published version is known of, the repository item page linked to above, will contain details on accessing it.

Copyright and reuse:
The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher’s statement:
Please refer to the repository item page, publisher’s statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk.
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].

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 scenario 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 jammers, 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 UA V and ground nodes as jammers to disturb eavesdropping in mmWave UAV-based relaying systems.

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 $\Phi_E$ with density $\lambda_E$, 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.
the path loss model can be expressed as

\[ A \text{ and } B \text{ and a ground node.} \]

where \( d \) is 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

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

where \( \alpha_L \) and \( \alpha_N \) denote the path loss exponents for LoS and NLoS links, respectively. \( \beta_L \) and \( \beta_N \) 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 Nakagami-\( m \) fading. Particularly, the small-scale fading power between the \( i \)th and \( j \)th 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. Channel Model**

In the following sections, we use \( S; D; E; U; J \) to denote the \( i \)th and \( j \)th nodes. Without loss of generality, we assume that each link experiences Nakagami-\( m \) fading. Particularly, the small-scale fading power between the \( i \)th and \( j \)th 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]

\[
G_a^j = \begin{cases} 
G_M^j, & p_M^j = \psi_g \frac{\theta_a}{\pi}, \quad a \in \{ U, J \}, \\
G_m^j, & p_m^j = 1 - \psi_g \frac{\theta_a}{\pi}, \quad a \in \{ U, J \},
\end{cases}
\]

where \( \psi_g \) and \( \theta_a \) denote the half-power beamwidth in the azimuth and the elevation, respectively.

Assume perfect beam alignment for the legitimate links between \( S \) and \( D \), 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 \( U \) 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 \( E \)) can be obtained as

\[
G_{aE} = \begin{cases} 
G_M^a G_M^E, & p_1 = \psi_M^a \psi_M^E, \\
G_m^a G_m^E, & p_2 = \psi_m^a \psi_m^E, \\
G_M^a G_m^E, & p_3 = \psi_m^a \psi_M^E, \\
G_m^a G_m^E, & p_4 = \psi_m^a \psi_m^E, \quad a \in \{ U, J \},
\end{cases}
\]

**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

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

where \( P_S \) (\( P_U \)) is the transmit power of \( S \) (\( U \)), and \( \sigma_U^2 \) (\( \sigma_D^2 \)) 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
\[
\gamma = \max \left( \max_{E \in \Phi} \gamma_E, \max_{E \in \Xi} \gamma_U \right),
\] where the SNR at each eavesdropper for decoding signals from and from \(U\) can be written as
\[
\gamma_E = \frac{P_S G_{SE} L(d_{SE}) h_{SE}}{\sigma_E^2}, \quad \gamma_U = \frac{P_U G_{UE} L(d_{UE}) h_{UE}}{\sigma_E^2},
\] and \(\sigma_E^2\) is the noise power at eavesdroppers.

The achievable secrecy rate is
\[
R_s = \frac{1}{2} \left[ \log_2(1 + \gamma_D) - \log_2(1 + \gamma_E) \right]^+, \quad (10)
\] where \([x]^+ = \max(x, 0)\). 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
\[
P_{sop} = \Pr \{ R_s < R_{th} \}
= \Pr \{ \frac{1}{2} \log_2(1 + \gamma_D) - \frac{1}{2} \log_2(1 + \gamma_E) < R_{th} \}
= \Pr \{ \log_2 \left( \frac{1 + \gamma_D}{1 + \gamma_E} \right) < 2R_{th} \}
= \Pr \{ 1 + \gamma_E > (1 + \gamma_D)2^{-2R_{th}} \}
= 1 - \int_0^\infty F_{\gamma_E} ((1 + y)2^{-2R_{th}} - 1) f_{\gamma_D}(y)dy,
\] where \(F_{\gamma_E}(\cdot)\) is the cumulative probability function (CDF) of \(\gamma_E\) and \(f_{\gamma_D}(\cdot)\) is the probability distribution function (PDF) of \(\gamma_D\).

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 \(\gamma_D\) 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
\[
f_{h}(x) = N_i^{N_i} x^{N_i-1} \frac{e^{-N_i x}}{\Gamma(N_i)}, \quad (13)
\]
\[
F_{h}(x) = 1 - \sum_{n=0}^{N_i-1} (N_i x)^n \frac{1}{n!} e^{-N_i x}. \quad (14)
\]
Therefore, we can derive the CDF of \(\gamma_D\) as
\[
F_{\gamma_D}(\gamma) = \Pr \left\{ \min \left( \frac{P_S G_{SU} L(d_{SU}) h_{SU}}{\sigma_D^2}, \frac{P_S G_{UD} L(d_{UD}) h_{UD}}{\sigma_D^2} \right) < \gamma \right\}
= 1 - \Pr \left\{ \frac{P_S G_{SU} L(d_{SU}) h_{SU}}{\sigma_D^2} > \gamma \right\} \Pr \left\{ \frac{P_S G_{UD} L(d_{UD}) h_{UD}}{\sigma_D^2} > \gamma \right\}
= 1 - \Pr \left\{ h_{SU} > \frac{\sigma_D^2 \gamma}{P_S G_{SU} L(d_{SU})} \right\} \Pr \left\{ h_{UD} > \frac{\sigma_D^2 \gamma}{P_S G_{UD} L(d_{UD})} \right\}
= 1 - \sum_{i \in \{L, N\}} \Pr \left\{ r_{SU} > \frac{N_i \gamma \sigma_D^2}{P_S G_{SU} \beta_i} \right\} \sum_{n_1=0}^{N_i-1} \frac{1}{n_1!} \left( -\frac{N_i \gamma \sigma_D^2}{P_S G_{SU} \beta_i} \right)^{n_1}
\times \sum_{j \in \{L, N\}} \Pr \left\{ r_{UD} > \frac{N_j \sigma_D^2 \gamma}{P_U G_{UD} \beta_j} \right\} \sum_{n_2=0}^{N_j-1} \frac{1}{n_2!} \left( -\frac{N_j \sigma_D^2 \gamma}{P_U G_{UD} \beta_j} \right)^{n_2}
= \left(12a\right).
\]
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 \(\gamma_D\) as (12b).

The CDF of \(\gamma_E\) can be expressed as
\[
F_{\gamma_E}(\gamma) = \Pr \left\{ \max \left( \max_{E \in \Phi_E} \gamma_E, \max_{E \in \Xi} \gamma_U \right) < \gamma \right\}
= \prod_{E \in \Phi_E} \Pr \{ \gamma_E < \gamma \} \prod_{E \in \Xi} \Pr \{ \gamma_U < \gamma \}. \quad (16)
\]
Based on this, We will calculate \(F_{\gamma_E}(\gamma)\) in Theorem 2 by deriving \(F_1(\gamma)\) and \(F_2(\gamma)\) separately.

**Theorem 2:** The CDF of \(\gamma_E\) can be given as (17) at the top of the next page, where \(x_j = \cos(2\pi j/2M+1), y_j = \sin(\pi j/2M+1), j\) 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 \(F_1(\gamma) = \mathbb{E} \left[ \prod_{E \in \Phi_E} \Pr \{ \gamma_E < \gamma \} \right]\). Then, according to the generation function of the PPP [34], we have
\[
F_1(\gamma) = \exp \left\{ -2\pi \lambda_E \times \int_{r_0}^{R_0} \Pr \{ \gamma_E > \gamma \} rdr \right\}
= \exp \left\{ -2\pi \lambda_E \times \sum_{i \in \{M, m\}} \int_{r_0}^{R_0} \Pr \{ h_{SE} > \gamma \} \frac{\sigma_D^2 \gamma \alpha_N}{P_S G_{SE} \beta_N} rdr \right\}. \quad (18)
\]
Particularly, the integral term in (18) can be calculated as
\[
\int_{r_0}^{R_0} \Pr \{ h_{SE} > \gamma \} \frac{\sigma_D^2 \gamma \alpha_N}{P_S G_{SE} \beta_N} rdr
\]
\[
= \sum_{n=0}^{N_N-1} \Gamma \left( \frac{\alpha_{NN} + 2}{\alpha_N}, \frac{N_N \gamma \sigma_D^2 \gamma \alpha_N}{P_S G_{SE} \beta_N}, \frac{R_0}{\alpha_N} \right) \Gamma \left( \frac{\alpha_{NN} + 2}{\alpha_N}, \frac{N_N \gamma \sigma_D^2 \gamma \alpha_N}{P_S G_{SE} \beta_N}, \frac{R_0}{\alpha_N} \right). \quad (19)
\]
\[ F_{\gamma D}(\gamma) = 1 - \sum_{i,j \in \{L,N\}} \sum_{n_1=0}^{N-L-1} \sum_{n_2=0}^{N-N-L-1} P_i(r_{SU}) P_j(r_{UD}) \frac{\gamma^{n_1+n_2}}{n_1! n_2!} \left( \frac{N_i \sigma^2_D d_{SU}^2}{P_S G_{SU i}} \right)^{n_1} \left( \frac{N_j \sigma^2_D d_{SD}^2}{P_U G_{UD j}} \right)^{n_2} e^{- \left( \frac{N_i \sigma^2_D d_{SU}^2}{P_S G_{SU i}} + \frac{N_j \sigma^2_D d_{SD}^2}{P_U G_{UD j}} \right) \gamma} \] (12a)

\[ f_{\gamma D}(\gamma) = - \sum_{i,j \in \{L,N\}} \sum_{n_1=0}^{N-L-1} \sum_{n_2=0}^{N-N-L-1} P_i(r_{SU}) P_j(r_{UD}) \frac{1}{n_1! n_2!} \left( \frac{N_i \sigma^2_D d_{SU}^2}{P_S G_{SU i}} \right)^{n_1} \left( \frac{N_j \sigma^2_D d_{SD}^2}{P_U G_{UD j}} \right)^{n_2} e^{- \left( \frac{N_i \sigma^2_D d_{SU}^2}{P_S G_{SU i}} + \frac{N_j \sigma^2_D d_{SD}^2}{P_U G_{UD j}} \right) \gamma} \left( \frac{N_i \sigma^2_D d_{SU}^2}{P_S G_{SU i}} + \frac{N_j \sigma^2_D d_{SD}^2}{P_U G_{UD j}} \right) \gamma^{n_1+n_2} \] (12b)

\[ F_{\gamma E}(y) = \exp \left\{ -2\pi \lambda_E \times \left[ \sum_{i \in \{M,m\}} p_i^E \sum_{n=0}^{N-1} \frac{\gamma^{n+1}}{n!} \left( \frac{N_i \gamma^2 \sigma^2_E}{P_S G_{UE i}^\beta} \right)^n \right] \right\} \]

\[ + \sum_{q \in \{L,N\}} \sum_{i \in \{M,m\}} p_i^U p_i^E \sum_{n=0}^{N-1} C_n \pi \frac{\gamma^{n+1}}{n!} \left( \frac{N_q \gamma^2 \sigma^2_E}{P_U G_{UE q}^\beta} \right)^n e^{- \frac{N_q \gamma^2 \sigma^2_E}{P_U G_{UE q}^\beta} \gamma} \] (17)

where step (b) is based on (14) and step (c) is obtained according to Eq. (3.81.9) in [35]. Substituting (19) into (18), we can derive \( F_1(\gamma) \). As the beam transmitted from \( S \) is aligned with the direction from \( S \) to \( U \), we have \( G_{SE} = G_{SM}^G G_{LM}^G \).

For convenience, let \( F_2(\gamma) = E \left[ \prod_{\gamma \in \Phi_k} \Pr \{ \gamma_U < \gamma \} \right] \). Using thinning theorem in the point process, the eavesdroppers can be divided into a LoS PPP \( \Phi_k^L \) with density \( \lambda_L P_L(r) \) and a NLoS PPP \( \Phi_k^N \) with density \( \lambda_N P_N(r) \), respectively. Therefore, \( F_2(\gamma) \) can be further expressed as

\[ F_2(\gamma) = E \left[ \prod_{\gamma \in \Phi_k^L} \Pr \{ \gamma_U < \gamma \} \right] E \left[ \prod_{\gamma \in \Phi_k^N} \Pr \{ \gamma_U < \gamma \} \right] \] (20)

Similar to (18), we can get

\[ E \left[ \prod_{\gamma \in \Phi_k^L} \Pr \{ \gamma_U < \gamma \} \right] = \exp \left\{ -2\pi \lambda_L \sum_{i \in \{M,m\}} p_i^L \frac{\gamma^{n+1}}{n!} \left( \frac{\gamma^2 \sigma^2_E}{P_L G_{UE i}^\beta L} \right)^n \right\} \]

\[ \int_0^{R_U} \Pr \left\{ h_{UE} > \frac{\gamma^2 \sigma^2_E (r^2 + H^2)^{\frac{\alpha}{2}}}{P_U G_{UE i}^\beta L} \right\} P_L(r) rdr \} \] (21)

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

\[ \int_0^{R_U} \Pr \left\{ h_{UE} > \frac{\gamma^2 \sigma^2_E (r^2 + H^2)^{\frac{\alpha}{2}}}{P_U G_{UE i}^\beta L} \right\} P_L(r) rdr \] = \[ \sum_{n=0}^{N-1} \int_0^{R_U} \left( \frac{N_L \gamma^2 \sigma^2_E}{P_U G_{UE i}^\beta L} \right)^n e^{- \frac{N_L \gamma^2 \sigma^2_E}{P_U G_{UE i}^\beta L} \gamma} \frac{\gamma^{n+1}}{n!} \] \[ \frac{\gamma^{n+1}}{n!} \left( \frac{\gamma^2 \sigma^2_E}{P_L G_{UE i}^\beta L} \right)^n \] \[ \times e^{- \frac{\gamma^2 \sigma^2_E}{P_L G_{UE i}^\beta L} \gamma} P_L(v_c) v_c. \] (22)

Step (d) is computed by using Gauss-Chebyshev integration [36], with \( x_c = \cos \left( \frac{2\pi}{20} \right) \) and \( v_c = \frac{\gamma_j}{\gamma} (x_c + 1) \). \( C \) denotes the number of the cumulative times.

In the same way, \( E \left[ \prod_{\gamma \in \Phi_k^N} \Pr \{ \gamma_U < \gamma \} \right] \) can be derived as

\[ E \left[ \prod_{\gamma \in \Phi_k^N} \Pr \{ \gamma_U < \gamma \} \right] = \exp \left\{ -2\pi \lambda_N \sum_{i \in \{M,m\}} p_i^L \frac{\gamma^{n+1}}{n!} \left( \frac{\gamma^2 \sigma^2_E}{P_N G_{UE i}^\beta N} \right)^n G_{UE i}^\beta N \right\} \]

\[ \exp \left\{ -2\pi \lambda_N \sum_{i \in \{M,m\}} p_i^L \frac{\gamma^{n+1}}{n!} \left( \frac{\gamma^2 \sigma^2_E}{P_N G_{UE i}^\beta N} \right)^n \right\} \times e^{- \frac{\gamma^2 \sigma^2_E}{P_N G_{UE i}^\beta N} \gamma} \frac{\gamma^{n+1}}{n!} \left( \frac{\gamma^2 \sigma^2_E}{P_N G_{UE i}^\beta N} \right)^n \] \[ \times e^{- \frac{\gamma^2 \sigma^2_E}{P_N G_{UE i}^\beta N} \gamma} P_N(v_c) v_c. \] (23)

By substituting (21), (22) and (23) into (20), we can obtain \( F_2(\gamma) \). Finally, \( F_{\gamma E}(\gamma) \) can be given as (17) by multiplying \( F_1(\gamma) \) with \( F_2(\gamma) \).}

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 \( (1+y)^{2-2Rc} - 1 \geq 0 \) in (11), and accordingly the lower limit of the integral is changed into \( y_0 = 2^{2Rc} - 1 \). By means of variable substitution, i.e., \( y = y_0 + \tan t \), we can approximate \( P_{sop} \) as

\[ P_{sop} = 1 - \int_{y_0}^{\infty} F_{\gamma E} \left( (1+y)^{2-2Rc} - 1 \right) f_{\gamma D}(y) dy \]

\[ = 1 - \int_0^\pi F_{\gamma E} \left( (1+y_0 + \tan t)^{2-2Rc} - 1 \right) \frac{\gamma_{\gamma D}(y_0 + \tan t) \sec^2 t dt}{4} \]

\[ \approx 1 - \frac{\pi}{4C} \sum_{c=1}^{C} \sqrt{1-u_c^2} F_{\gamma E} \left[ (1+y_0 + \tan \frac{\pi}{4} (u_c + 1)^2 - 2^{2Rc} - 1) \right] \]

\[ \times f_{\gamma D}(y_0 + \tan \frac{\pi}{4} (u_c + 1)) \sec^2 \pi (u_c + 1), \] (24)

where \( u_c = \cos \left( \frac{2\pi}{20} \right) \) and \( C \) denotes the number of
\[ \mathcal{L}_1(\gamma) = \sum_{i,j \in [L, N]} P_i(r_{SU}) P_j(r_{UD}) (P_{DG}G_{DL}(d_{DL}))^{-N_j} \frac{N_j^{N_j}}{\Gamma(N_j)} e^{-\frac{N_j}{P_{DG}G_{DL}(d_{DL})}} \frac{N_j}{P_{DG}G_{DL}(d_{DL})} - N_j \sum_{n=0}^{N_j-1} \frac{(N_j)^n}{n!} \left( \frac{P_{DG}G_{DL}(d_{DL})}{P_{DG}G_{DL}(d_{DL})} \right)^n \]
\[ \mathcal{L}_2(\gamma) = \sum_{i,j \in [L, N]} P_i(r_{UD}) P_j(r_{JD}) (P_{JG}G_{JD}(d_{JD}))^{-N_j} \frac{N_j^{N_j}}{\Gamma(N_j)} e^{-\frac{N_j}{P_{JG}G_{JD}(d_{JD})}} \frac{N_j}{P_{JG}G_{JD}(d_{JD})} - N_j \sum_{n=0}^{N_j-1} \frac{(N_j)^n}{n!} \left( \frac{P_{JG}G_{JD}(d_{JD})}{P_{JG}G_{JD}(d_{JD})} \right)^n \]

where
\[ \gamma^j_{SU} = \frac{P_{DG}G_{SU}(d_{SU})}{P_{DG}G_{SU}(d_{SU})} \mathcal{L}_1(\gamma) + \mathcal{L}_2(\gamma) \]
\[ \gamma^j_{UD} = \frac{P_{DG}G_{UD}(d_{UD})}{P_{DG}G_{UD}(d_{UD})} \mathcal{L}_1(\gamma) + \mathcal{L}_2(\gamma) \]

The highest eavesdropping SINR among all the eavesdroppers can be expressed as
\[ \gamma^j_E = \max \left( \max_{i \in [M, m]} \gamma^j_{SU}, \max_{i \in [M, m]} \gamma^j_{UD} \right) \]

where
\[ \gamma^j_{SE} = \frac{P_{DG}G_{SE}(d_{SE})}{P_{DG}G_{SE}(d_{SE})} \mathcal{L}_1(\gamma) + \mathcal{L}_2(\gamma) \]
\[ \gamma^j_{UE} = \frac{P_{DG}G_{UE}(d_{UE})}{P_{DG}G_{UE}(d_{UE})} \mathcal{L}_1(\gamma) + \mathcal{L}_2(\gamma) \]

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
\[ P_{sop}^j = P_r \left\{ \frac{1}{2} \log_2(1 + \frac{1}{\gamma^j_D}) - \frac{1}{2} \log_2(1 + \frac{1}{\gamma^j_E}) < R_{th} \right\} \]
\[ = 1 - \int_0^{\gamma^j_{SU}} F_{\gamma_{SE}} \left( 1 + (1 + y)2^{-2R_{th}} - 1 \right) f_{\gamma_{SE}}(\gamma_E) d\gamma_E, \]

where \( F_{\gamma_{SE}}(\cdot) \) is the CDF of \( \gamma^j_{SU} \) and \( f_{\gamma_{SE}}(\cdot) \) is the PDF of \( \gamma^j_{SE} \) 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 \( \gamma^j_{SU} \) can be obtained as
\[ F_{\gamma_{SU}}(\gamma) = \Pr \left\{ \min \left( \gamma^j_{SU}, \gamma^j_{UD} \right) < \gamma \right\} \]
\[ = 1 - \Pr \left\{ \gamma^j_{SU} > \gamma \right\} \Pr \left\{ \gamma^j_{UD} > \gamma \right\} \]

where \( \mathcal{L}_1(\gamma) \) and \( \mathcal{L}_2(\gamma) \) are given in (33a) and (33b) at the top of this page.

**Proof:** Let \( Y_1 = P_{DG}G_{SU}(d_{SU}) \) and \( Y_2 = P_{DG}G_{UD}(d_{UD}) \), and we have
\[ L_1(\gamma) = \Pr \{ \gamma_{SE}^J > \gamma \} = \Pr \left\{ \frac{Y_1}{Y_2 + \sigma_U^2} > \gamma \right\} \]
\[ = 1 - \Pr \{ Y_1 < \gamma (Y_2 + \sigma_U^2) \} \]
\[ = 1 - \int_{-\infty}^{\infty} f_{Y_1}(\gamma_2 + \sigma_U^2) d\gamma_2. \]  

(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

\[ F_{Y_1}(y_1) = 1 - \sum_{n=0}^{N-1} \frac{N y_1}{P_S G_{SU}(d_{SU})} \frac{1}{n!} e^{-\frac{N y_1}{P_S G_{SU}(d_{SU})}}, \]  

(35a)

\[ f_{Y_2}(y_2) = \left( \frac{P_D G_{DL}(d_{DL})}{P_{SU} G_{SU}(d_{SU})} \right) \frac{y_2^{N-1} \Gamma(N)}{\Gamma(N)} e^{-\frac{P_D G_{DL}(d_{DL}) y_2}{P_{SU} G_{SU}(d_{SU})}}. \]

(35b)

Using (35a) and (35b), \( L_1(\gamma) \) is derived as (36) at the top of this page, and step (e) exploits Eq. (3.51-3) in [35]. Similarly, we can obtain the expression of \( L_2(\gamma) \) as presented in (33b).

Furthermore, the derivation of (32) provides the PDF of \( \gamma_{DE}^J \) as

\[ f_{\gamma_{DE}^J}(\gamma) = \frac{\partial L_1(\gamma)}{\partial \gamma} - \frac{\partial L_2(\gamma)}{\partial \gamma} L_1(\gamma), \]  

(37)

where the derivatives of \( L_1 \) and \( L_2 \) are calculated as (38a) and (38b) at the top of the next page, respectively. As a result, the PDF of \( \gamma_{DE}^J \) 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 \( P_{\text{sep}} \). To this end, the theoretical expressions of \( \Pr \{ \gamma_{SE}^J > \gamma \} \) and \( \Pr \{ \gamma_{DE}^J > \gamma \} \) 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 \( \Pr \{ \gamma_{DE}^J > \gamma \} \), respectively. The expressions are given by (39a) and (39b) on the next page. Particularly, in (39b), \( r_{DE} = \sqrt{r^2 + r_{UJ}^2} - 2r_{UJ} \cos \theta \) denotes 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 \( d_{JE} = \sqrt{r_{DE}^2 + H^2} \), respectively. Through the similar procedure of deriving \( F_{E,1}(r, \theta) \), we can derive \( F_{E,2}(r, \theta) \) taking into consideration that the links from \( U \) to \( J \) or \( E \) to eavesdroppers can be LoS or NLoS as

\[ F_{E,2}(r, \theta) = \Pr \left\{ \frac{P_{U} G_{UE}(d_{UE})}{P_{J} G_{JE}(d_{JE})} > \gamma \right\} \]

\[ = \sum_{q, e \in \{U, N\}} \sum_{i,j,g,w \in \{M,m\}} \frac{P_{U} G_{UE}(d_{UE})}{P_{J} G_{JE}(d_{JE})} \left( \frac{P_{U} G_{UE}(d_{UE})}{P_{J} G_{JE}(d_{JE})} \right)^n \times \frac{N_{\gamma}}{n!} \prod_{k=0}^{n} \left( 1 + \frac{1}{n} \right) \left( \frac{P_{U} G_{UE}(d_{UE})}{P_{J} G_{JE}(d_{JE})} \right)^{n-k} \times C_n^k \gamma_{DE}^{2(n-k)} \gamma_{DE}^{n-k} \]  

(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

\[ F_{E,2}^J(\gamma) = \left[ \prod_{E \in \Phi_E} \Pr \{ \gamma_{SE}^J < \gamma \} \right] \left[ \prod_{E \in \Phi_E} \Pr \{ \gamma_{DE}^J < \gamma \} \right]. \]  

(42)

Particularly, by utilizing the probability generating function of PPP and a two-layer Gauss-Chebyshev quadrature equation, \( F_{E,2}^J(\gamma) \) can be derived as

\[ F_{E,2}^J(\gamma) = \exp \left\{ \lambda_E \int_0^{2\pi} \int_0^{R_0} \Pr \{ \gamma_{SE}^J > \gamma \} r dr d\theta \right\} \approx \exp \left\{ \lambda_E \int_0^{2\pi} \int_0^{R_0} F_{E,1}(r, \theta) r dr d\theta \right\} \]

\[ = \lambda_E \int_0^{2\pi} \int_0^{R_0} F_{E,1} \left( r, \theta \right) r dr d\theta \]

\[ \approx \exp \left\{ \lambda_E \sum_{t=1}^{T} \sum_{i=1}^{L_i} \left( \frac{1 - x_i^2}{1 - y_i^2} \frac{R_0 - r_0}{2} \frac{y_i + r_0 + r_0}{2} \pi (x_i + 1) \right) \right\}. \]  

(43)
\[L(\gamma) = 1 - \int_0^\infty f_{Y_2}(y_2) \left[ 1 - \sum_{n=0}^{N-1} \left( \frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)} \right)^n \frac{1}{n!} e^{-\frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)}} \right] dy_2\]

\[= \sum_{i,j \in \{L,N\}} \frac{P_i(rSU)P_j(rUD)}{P_{D G DU} L(dDU)} \frac{N_j}{\Gamma(N_j)} \int_0^\infty \left( \frac{y_2}{2} \right)^{N_j-1} e^{-\frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)}} \sum_{n=0}^{N-1} \left( \frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)} \right)^n \frac{1}{n!} e^{-\frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)}} dy_2\]

\[= \sum_{i,j \in \{L,N\}} \frac{P_i(rSU)P_j(rUD)}{P_{D G DU} L(dDU)} \frac{N_j}{\Gamma(N_j)} \int_0^\infty \left( \frac{y_2}{2} \right)^{N_j-1} e^{-\frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)}} \sum_{n=0}^{N-1} \left( \frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)} \right)^n \frac{1}{n!} e^{-\frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)}} dy_2\]

\[= \left( \sum_{i,j \in \{L,N\}} \frac{P_i(rSU)P_j(rUD)}{P_{D G DU} L(dDU)} \frac{N_j}{\Gamma(N_j)} \int_0^\infty \left( \frac{y_2}{2} \right)^{N_j-1} e^{-\frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)}} \sum_{n=0}^{N-1} \left( \frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)} \right)^n \frac{1}{n!} e^{-\frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)}} dy_2\right)\]

\[\times \sum_{j=0}^n \frac{C_k^j (n-k)}{(N_j - 1 + k)!} \left( \frac{N_i \gamma (y_2 + \sigma_U^2)}{P_{D G SU} L(dSU)} + \frac{N_j}{P_{D G DU} L(dDU)} \right)^{-k-N_j}.\] (36)
where \( x_i = \cos(\frac{2i-1}{2L}\pi) \) and \( y_t = \cos(\frac{2t-1}{2T}\pi) \) are Gauss-Chebyshev nodes corresponding to \( \theta \) and \( r \), respectively. Similarly, we can obtain \( F_2^J(\gamma) \) as

\[
F_2^J(\gamma) = \exp\left( -\lambda_E \frac{\pi^3 R_{UL}}{2TL} \sum_{l=1}^{L} \sum_{t=1}^{T} \sqrt{1-x_i^2} \sqrt{1-y_t^2} \right. \\
\times F_{E,2}\left( \frac{R_{UL}}{2}(y_t+1), \pi(x_l+1), \frac{R_{UL}}{2}(y_t+1) \right) .
\]

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

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

where \( y_0 = 2^{2R_{UL}}-1 \) 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 \( \lambda_E \) 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 \( P_S = P_U = P \).](image)

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

**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 $\lambda_E$ decreases from $10^{-3}$/m$^2$ to $10^{-4}$/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 $W_J = [200, 50]$. 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 $\lambda_E$ 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 $\lambda_E$, 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 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 $W_J = [200, 50]$, $P_S = P_U = 1$ 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...
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 $P_J = 1 \text{ W}$ when the transmit power of $J$ is limited by the maximum value 1 W. Setting $P_J = 1 \text{ W}$, 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 $P_J = 1 \text{ W}$ and $P_D = 0 \text{ W}$ to achieve high secrecy performance in the considered cases.

Furthermore, we change some of the parameters as $W_J = [150, 0], W_D = [450, 0], \lambda_E = 5 \times 10^{-3}$ 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 $P_D = 0.6 \text{ W}$, 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 $P_J = 1 \text{ W}$ and $P_D = 0.6 \text{ W}$ 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.
will further improve the secrecy performance of UA V-based wireless networks. 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