Hindawi
Security and Communication Networks
Volume 2022, Article ID 7452014, 17 pages
https://doi.org/10.1155/2022/7452014

Research Article

Secure Transmission of mmWave NOMA UAV-Assisted Relay System against Randomly Located Eavesdroppers

Danyu Diao,[1] **Buhong Wang**,[1] **Kunrui Cao**,[2,3] **Runze Dong**,[1] **and Tianhao Cheng**[1]

[1]*School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China*
[2]*School of Information and Communications, National University of Defense Technology, Wuhan 430035, China*
[3]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Buhong Wang; hongwks@aliyun.com and Kunrui Cao; krcao@nudt.edu.cn

Received 9 May 2022; Revised 17 July 2022; Accepted 1 August 2022; Published 10 October 2022

Academic Editor: Chien Ming Chen

UAV wireless communication has been regarded as a promising technology in the fifth-generation (5G) networks. In this paper, we consider the security of the mmWave NOMA UAV-assisted relay system, where a ground source transmits messages to two types of authorized users assisted by a UAV relay in the presence of multiple eavesdroppers. A practical probabilistic line-of-sight (LoS) channel model with Nakagami-*m* small-scale fading and three-dimensional (3D) antenna gain is established to describe the mmWave air-to-ground channel. In addition, to improve the security of the system, cooperative jamming and protected zone strategies are introduced. The analytical expressions of connection outage probability (COP), secrecy outage probability (SOP), and effective secrecy throughput (EST) under the NOMA scheme and cooperative jamming NOMA scheme are derived. Also, the asymptotic SOP and EST are analyzed to gain further insights. The theoretic analysis and simulation results show the effectiveness of the proposed schemes. As the transmitting power of the source and UAV relay increases, the SOP depends only on the location distribution and density of eavesdroppers and the ESTs under different schemes converge to the same floor.

1. Introduction

To support long-range connectivity, massive access, and explosive traffic growth in 5G networks, unmanned aerial vehicles (UAVs) have rekindled strong interest of both industry and academia in wireless connectivity owing to enhanced channel quality and flexible dynamic deployment [1–3]. In emergencies such as natural disasters or military activities, UAVs can be deployed as temporary base stations, mobile relays, and cooperative jammers. For example, the urgent deployment of Wing Loong UAV provided stable access to residents affected by the storm that disrupted communications. There has been numerous research on UAV wireless communication systems recently [4–25]. In order to improve the reliability of UAV communications, the trajectory and transmitting power of UAV relay were jointly optimized to minimize the connection outage probability (COP) in [4]. By considering the propulsion energy limitations of UAVs, the authors of [5] investigated the maximization of energy efficiency and transmission rate, where the UAV was deployed to support uplink communications. To further solve the problem, energy harvesting technology was applied in the UAV-assisted relay communication networks to enhance the flight endurance in [6].

Nevertheless, owing to the strong line-of-sight (LoS) components over air-to-ground (A2G) links, it is extremely arduous to investigate the security of UAV communication systems. Physical layer security technology can exploit the randomness of wireless fading channels to secure wireless communications from the perspective of information theory, which is a good complement to conventional cryptography technology [26–28]. The authors of [7] employed UAVs as an aerial base station and cooperative jammer to defend against eavesdropping exploiting the controllable mobility. By designing neural networks, [8] proposed a dynamic beamforming technique to maximize the average

secrecy rate in the UAV wireless communication system. Considering the scenario of full-duplex active eavesdropping, [9] maximized the secrecy rate of the system by optimizing the trajectory and transmitting power. Unlike [7–13] focused on the performance analysis of secure UAV communications. Reference [10] studied the secrecy performance of a UAV-assisted relay system. Ji et al. and coauthor proposed a novel UAV cognitive network to achieve higher-spectrum efficiency [11]. Artificial noise (AN) was used to improve the secrecy performance of the UAV system in [12]. The authors of [13] investigated the secrecy performance of UAV systems from the perspective of three-dimensional (3D) space.

Due to its widely available spectrum resources, integrating millimeter wave (mmWave) technique into UAV networks has been a potential solution to address the spectrum crunch [14–18]. The 3D mmWave antenna gain from UAV to ground nodes is first proposed in [16]. The authors of [17] investigated the secrecy performance of mmWave communications assisted by multiple UAV-enabled relays and jammers. Furthermore, the on–off transmission strategy was designed in [18] to evaluate the performance under the effect of beam alignment error.

Meanwhile, with the explosive growth of traffic demand, nonorthogonal multiple access (NOMA) has been viewed as a promising candidate for 5G networks [29–31]. It is noteworthy investigating the transmission scheme of UAV-assisted NOMA systems to obtain important insights on performance improvement [19–21, 32]. A UAV-assisted NOMA network was proposed in [22] to achieve secure simultaneous wireless information and power transfer (SWIPT) transmission, while the inherent mobility of UAV was not considered. As a further advance, the authors of [23] proposed an aerial cooperative jamming strategy to secure terrestrial NOMA communications and optimized the position of the UAV. Moreover, the authors of [24] achieved secure transmission by jointly designing user scheduling, trajectory, and power allocation from the perspective of secure users. Pang et al. [25] considered the energy-constrained UAV mmWave NOMA network and maximized the energy efficiency. Introducing NOMA into UAV mmWave communication system can further improve system performance and satisfy the different communication needs of users. Despite such research progress, none of them considered the security topic of UAV-assisted relay mmWave NOMA system, and corresponding secrecy transmission scheme designing and the impact of key system parameters are not reported yet, which motivates this work.

In this work, we consider the physical layer security of a mmWave NOMA UAV-assisted relay system, where a UAV is deployed as a relay to enhance the communication quality of the system while another UAV is deployed as a friendly jammer to send AN for enhancing the security of the system. This is in stark contrast to the existing work which is without taking into account the security [33], OMA transmission mode [17, 34], and simplified LoS channel [35]. The contributions of the work are summarized as follows:

We model a mmWave NOMA UAV-assisted relay network in the presence of randomly distributed eavesdroppers. Due to the blockage or long distance, a UAV relay is employed to decode-and-forward (DF) signals from the terrestrial source to NOMA users. Based on different service requirements, the authorized users are classified into high-security required users and common users. The distribution of users and eavesdroppers is modeled as homogeneous Poisson point processes (HPPPs). We take into account a practical probabilistic line-of-sight (LoS) and nonline-of-sight (NLoS) A2G channel model based on the elevation. Moreover, the 3D antenna gain model is established to characterize the mmWave transmission:

In order to study the reliability and security of the system and reveal the effects of key parameters on the system, we derive the closed-form expressions of connection outage probability (COP), secrecy outage probability (SOP), and effective secrecy throughput (EST) under the NOMA scheme. To further improve the secrecy performance of the system, the cooperative aerial jamming scheme is proposed to degrade the quality of wiretapping. Based on the proposed scheme, the COP, SOP, and EST are obtained by utilizing Gauss–Chebyshev quadrature. Furthermore, the asymptotic SOP and EST are derived to gain valuable insights.

The numerical results show that (1) the proposed NOMA scheme with cooperative jamming outperforms benchmark schemes. (2) Increasing the number of antennas equipped at each node can improve the security of the system due to the increased main lobe gain. The improvement is more obvious when the jamming power is relatively large. (3) The asymptotic SOP is independent of the transmitting power of the source and UAV relay, while it is influenced by the size of protected zone and the density of eavesdroppers. (4) With the increase of jamming power, the EST of cooperative jamming scheme converges to a performance floor, which is independent of the size of the protected zone.

The remainder of the paper is organized as follows: In Section 2, we describe the system and channel models. The COP, SOP, and EST of UAV-assisted mmWave relay system are investigated in Section 3. With cooperative jamming, the expressions are derived in Section 4. In Section 5, numerical results are presented to validate the theoretical analysis. Finally, the conclusions are provided in Section 6.

2. System Model

We consider a secure mmWave NOMA UAV-assisted communication system as illustrated in Figure 1, where a source (S) sends the confidential message to two NOMA users (D_1 and D_2) via a UAV-based relay (U) in the presence of randomly distributed eavesdroppers (E). Since NOMA users use the same frequency and spread spectrum coding at the same time, the interference between users will be relatively strong. In general, it is impractical for all users to jointly perform NOMA due to high complexity and high decoding latency [36]. A promising alternative is to split the user into multiple orthogonal pairs and perform NOMA in each pair [37]. In our work, a NOMA pair is taken as an example. (Since NOMA users use the same

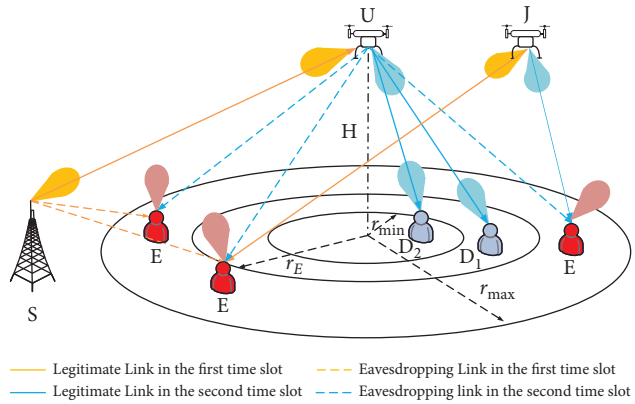

Figure 1: System model.

frequency and spread spectrum coding at the same time, the interference between users will be relatively strong. In general, it is impractical for all users to jointly perform NOMA due to high-complexity and high-decoding latency [36]. A promising alternative is to split the user into multiple orthogonal pairs and perform NOMA in each pair [37]. In our work, a NOMA pair is taken as an example) The communication can be divided into two time slots. In the first slot, S sends a superimposed signal to U, and in the second slot, U decodes the signal and sends it to the users on the ground. Due to the obstruction on the ground, the source and the users cannot communicate directly. Without loss of generality, one of the users D_2 is high-security required user and the other user D_1 is a common user with only rate requirements. This makes sense in many practical applications for the Internet of Things (IoT) era [24], such as the transmission of private information or military secrets may require a higher-security priority, while information such as weather forecasts has low or no security requirements. Eavesdroppers denoted by Φ_e follow HPPPs with density λ_e. A sector protected zone method is introduced to enhance security. Particularly, we model the finite range around U as the sector protected zone with radius r_E and central angle θ_s considering the sector-protected zone in a sector beam. D_2 is randomly located in a circle with center O and radius $r_{\min}$. D_1 is randomly located at the external sector ring spanning the radius from $r_{\min}$ to $r_{\max}$. We denote $n_i \in \mathrm{CN}(0, \sigma_i^2)$ as the additive white Gaussian noise (AWGN) at the receiver i, $i \in \{U, D_1, D_2, E\}$.

2.1. Directional Beamforming. In order to compensate for the loss of mmWave, each node is equipped with multiple pint-sized antennas. 3D antenna gain model is established, where G_M and G_m represent the main-lobe gain and side-lobe gain. θ_a and θ_d are denoted as the beamwidth in azimuth and depression/elevation directions, respectively. The 3D beamforming's horizontal projection shows the range of azimuth angle is $[-\pi, \pi]$. The worst-case scenario is considered as [16] that the range of depression/elevation angle is $[(\theta_d/2), \pi - (\theta_d/2)]$ for the node l, $l \in \{S, D1, D2, E\}$ and $[-\pi, 0]$ for the UAV. Thus, the directional antenna gain and the corresponding probability in the system can be written as follows:

$$G_i^l = \begin{cases} G_M^l, & p_M^l = \dfrac{\theta_a^l}{2\pi} \cdot \dfrac{\theta_d^l}{\pi - \theta_d^l}, \\ G_m^l, & p_m^l = 1 - \dfrac{\theta_a^l}{2\pi} \cdot \dfrac{\theta_d^l}{\pi - \theta_d^l}, \end{cases}$$

$$G_i^U = \begin{cases} G_M^U, & p_M^U = \dfrac{\theta_a^U}{2\pi} \cdot \dfrac{\theta_d^U}{\pi}, \\ G_m^U, & p_m^U = 1 - \dfrac{\theta_a^U}{2\pi} \cdot \dfrac{\theta_d^U}{\pi}. \end{cases} \tag{1}$$

In the training phase, we consider perfect beam alignment for A2G legitimate communication links. In addition, lack of training information makes it difficult for eavesdroppers to align to aerial nodes. Specifically, the antenna gain between legitimate nodes can be given by $G_{SU} = G_M^S G_M^U$, $G_{UD_1} = G_M^U G_M^{D_1}$, $G_{UD_2} = G_M^U G_M^{D_2}$. Since the transmitting beam of S is aligned with U, the gain of the terrestrial eavesdropping link can be obtained as $G_{\mathrm{SE}} = G_m^S G_i^E$, where $i \in \{m, M\}$. The gain of $U - E$ link can be formulated as follows:

$$G_{UE} = \begin{cases} G_m^U G_m^E, & p1 = p_m^U p_m^E, \\ G_m^U G_M^E, & p2 = p_m^U p_M^E, \\ G_M^U G_m^E, & p3 = p_M^U p_m^E, \\ G_m^U G_m^E, & p4 = p_M^U p_M^E. \end{cases} \tag{2}$$

2.2. Channel Model

2.2.1. Line-of-Sight (LoS) Probability. For the A2G link between U and l, we model it as a channel with a given LoS probability, which is determined by the environment and elevation angle [38]. The LoS probability is given by

$$P_L(r_{Ul}) = \frac{1}{1 + \varphi \exp\left[-\omega\left(\arctan\left(H/r_{Ul}\right) - \varphi\right)\right]}, \tag{3}$$

where r_{Ul} denotes the horizontal distance between U and l. H is the minimum flying height of U without colliding with obstacles on the ground. φ and ω are constants associated with the environment. Then the NLoS probability of the A2G channel can be formulated as $P_N(r_{Ul}) = 1 - P_L(r_{Ul})$.

2.2.2. Path Loss. Similar to [39], the path loss for the A2G channel with distance d_{Ul} under LoS and NLoS links can be expressed as follows:

$$L(d_{Ul}) = \begin{cases} d_{Ul}^{-\tau}\eta_L, & \text{LoS links}, \\ d_{Ul}^{-\tau}\eta_N, & \text{NLoS links}, \end{cases} \tag{4}$$

where $d_{Ul} = \sqrt{r_{Ul}^2 + H^2}$ and τ denotes the path loss factor. η_L and η_N depend on environment. For the ground-to-ground (G2G) channel, the path loss is calculated as $L(d_{\mathrm{SE}}) = d_{\mathrm{SE}}^{-\tau}\eta_N$.

2.2.3. Small-Scale Fading. We assume all communication links experience independent Nakagami-m fading [11, 34], where different parameters represent LoS and NLoS links, respectively. To be specific, the small-scale fading between i and j satisfies $h_{ij} \sim \Gamma(N_L, 1/N_L)$ for the LoS links and $h_{ij} \sim \Gamma(N_N, 1/N_L)$ for the NLoS links, $i, j \in \{S, U, D_1, D_2, E\}$. Denoting Gamma random variable $Z = |h_{ij}|^2$, the probability density function (PDF) and cumulative distribution function (CDF) are, respectively, denoted as follows:

$$\begin{aligned} f_Z(z) &= N_k^{N_k} \frac{z^{N_k - 1}}{\Gamma(N_k)} e^{-N_k z}, \\ F_Z(z) &= 1 - \sum_{n=0}^{N_k - 1} (N_k z)^n \frac{1}{n!} e^{-N_k z}, \end{aligned} \tag{5}$$

where $k \in \{L, N\}$.

3. Performance Analysis Without Jamming

In this section, we consider the reliability and security performance of the mmWave NOMA UAV-assisted relay system in terms of COP, SOP, and EST.

In the first time slot, S transmits superimposed signal $x = \sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2$ to U, where P_s denotes the transmitting power. $\alpha_j\,(j \in \{1, 2\})$ denotes the power allocation factor for the user D_j, $\alpha_1 \geq \alpha_2$ and $\alpha_1 + \alpha_2 = 1$. Following the principle of downlink NOMA, U first decodes x_1, then removes x_1 from the signal, and decodes x_2 without interference. Hence, the signal-to-interference-plus-noise ratio (SINR) and signal-to-noise ratio (SNR) for x_1 and x_2 at U can be, respectively, expressed as follows:

$$\begin{aligned} \gamma_{SU}^{x_1} &= \frac{\alpha_1 G_{SU} P_s |h_{SU}|^2 L(d_{SU})}{\alpha_2 G_{SU} P_s |h_{SU}|^2 L(d_{SU}) + \sigma_U^2}, \\ \gamma_{SU}^{x_2} &= \frac{\alpha_2 G_{SU} P_s |h_{SU}|^2 L(d_{SU})}{\sigma_U^2}. \end{aligned} \tag{6}$$

The worst-case scenario is considered where the eavesdropper owns the multiuser detection capacity to detect signals of users with high-security requirements [40]. Besides, we consider noncolluding eavesdroppers, which mean the instantaneous SNR for eavesdropping on the information of D_2 is determined by the most detrimental eavesdropper. Therefore, the SNR for eavesdroppers to decode x_2 from S can be calculated as follows:

$$\gamma_{\mathrm{SE}} = \max_{E \in \Phi_e} \frac{\alpha_2 G_{\mathrm{SE}} P_s |h_{\mathrm{SE}}|^2 L(d_{\mathrm{SE}})}{\sigma_E^2}. \tag{7}$$

In the second time slot, U works in DF mode to decode and reforward the signal. After receiving the signal from U, D_1 decodes x_1 by interpreting x_2 as interference. The SINR at D_1 can be written as follows:

$$\gamma_{\mathrm{UD}_1}^{x_1} = \frac{\alpha_1 G_{\mathrm{UD}_1} P_u \left|h_{\mathrm{UD}_1}\right|^2 L\left(d_{\mathrm{UD}_1}\right)}{\alpha_2 G_{\mathrm{UD}_1} P_u \left|h_{\mathrm{UD}_1}\right|^2 L\left(d_{\mathrm{UD}_1}\right) + \sigma_{D_1}^2}, \tag{8}$$

where P_u denotes the transmitting power of U. The user D_2 utilizes successive interference cancellation (SIC) to decode the message x_1 before decoding its own message. The SINR at D_2 to decode x_1 can be written as follows:

$$\gamma_{\mathrm{UD}_2}^{x_1} = \frac{\alpha_1 G_{\mathrm{UD}_2} P_u \left|h_{\mathrm{UD}_2}\right|^2 L\left(d_{\mathrm{UD}_2}\right)}{\alpha_2 G_{\mathrm{UD}_2} P_u \left|h_{\mathrm{UD}_2}\right|^2 L\left(d_{\mathrm{UD}_2}\right) + \sigma_{D_2}^2}. \tag{9}$$

After subtracting the signal x_1, D_2 decodes its own message and the SNR can be expressed as follows:

$$\gamma_{\mathrm{UD}_2}^{x_2} = \frac{\alpha_2 G_{\mathrm{UD}_2} P_u \left|h_{\mathrm{UD}_2}\right|^2 L\left(d_{\mathrm{UD}_2}\right)}{\sigma_{D_2}^2}. \tag{10}$$

In the second time slot, the SNR for eavesdropping x_2 from U at the most detrimental eavesdropper is given by

$$\gamma_{UE} = \max_{E \in \Phi_e} \frac{\alpha_2 G_{\mathrm{UE}} P_u \left|h_{\mathrm{UE}}\right|^2 L\left(d_{\mathrm{UE}}\right)}{\sigma_E^2}. \tag{11}$$

3.1. COP of D_1 and D_2 for NOMA Scheme. The connection outage probability (COP) is defined as the probability that the system will be interrupted when the instantaneous

transmission rate of the system is less than a given target rate. As such, we present the COP of D_1 in the following theorem.

Theorem 1. *For the reliable communication of D_1, S-U, and U-D_1 links must satisfy the target rate R_1 simultaneously. The COP of D_1 can be derived as (15), where $r(v_l) = r_{max}(v_l + 1)/2$, $v_l = cos(2l - 1/2L\pi)$, $r(v_t) = r_{min}(v_t + 1)/2$, $v_t = cos(2t - 1/2L\pi)$, and L denotes the number of Gauss–Chebyshev nodes.*

$$P_{\text{cop}}^{D1} = 1 - \sum_{k_1=\{L,N\}} P_{k_1}(r_{\text{SU}}) \sum_{n=0}^{N_{k_1}-1} \left(N_{k_1} \frac{\epsilon_1 \sigma_U^2 \left(r_{SU}^2 + H^2\right)^{(\tau/2)} \eta_k}{(\alpha_1 - \epsilon_1\alpha_2) G_{SU} P_s} \right)^n \frac{1}{n!} e^{-N_k \left(\epsilon_1 \sigma_U^2 \left(r_{SU}^2 + H^2\right)^{-(\tau/2)} \eta_k / (\alpha_1 - \epsilon_1\alpha_2) G_{\text{SU}} P_s\right)} \sum_{k_2=\{L,N\}} \frac{2}{r_{\max^2} - r_{\min^2}}$$

$$\times \left(\frac{r_{\max}\pi}{2L} \sum_{l=1}^{L} \sum_{n=0}^{N_{k_2}-1} \sqrt{1 - v_l^2}\, P_{k_2}(r(v_l)) \left(N_{k_2} \frac{\epsilon_1 \sigma_{D_1}^2 \left(r(v_l)^2 + H^2\right)^{(\tau/2)} \eta_k}{(\alpha_1 - \epsilon_1\alpha_2) G_{\text{UD}_1} P_u} \right)^n \frac{r(v_l)}{n!} e^{-N_{k_2}\left(\epsilon_1 \sigma_{D_1}^2 \left(r(v_l)^2 + H^2\right)^{(\tau/2)} \eta_k / (\alpha_1 - \epsilon_1\alpha_2) G_{\text{UD}_1} P_u\right)} \right.$$

$$\left. - \frac{r_{\min}\pi}{2T} \sum_{t=1}^{T} \sum_{n=0}^{N_{k_2}-1} \sqrt{1 - v_t^2}\, P_{k_2}(r(v_t)) \left(N_{k_2} \frac{\epsilon_1 \sigma_{D_1}^2 \left(r(v_t)^2 + H^2\right)^{(\tau/2)} \eta_k}{(\alpha_1 - \epsilon_1\alpha_2) G_{\text{UD}_1} P_u} \right)^n \frac{r(v_t)}{n!} e^{-N_{k_2}\left(\epsilon_1 \sigma_{D_1}^2 \left(r(v_t)^2 + H^2\right)^{(\tau/2)} \eta_k / (\alpha_1 - \epsilon_1\alpha_2) G_{\text{UD}_1} P_u\right)} \right), \tag{12}$$

Proof. According to the definition of COP, we have

$$\begin{aligned} P_{\text{cop}}^{D1} &= 1 - \Pr\left\{\frac{1}{2}\log_2\left(1 + \gamma_{\text{SU}}^{x_1}\right) > R_1, \frac{1}{2}\log_2\left(1 + \gamma_{\text{UD}_1}^{x_1}\right) > R_1\right\} \\ &= 1 - \Pr\left\{\gamma_{\text{SU}}^{x_1} > 2^{2R_1} - 1, \gamma_{\text{UD}_1}^{x_1} > 2^{2R_1} - 1\right\} \\ &= 1 - \underbrace{\Pr\left\{\left|h_{\text{SU}}\right|^2 > \frac{\epsilon_1 \sigma_U^2}{(\alpha_1 - \epsilon_1\alpha_2) G_{\text{SU}} P_s L(d_{\text{SU}})}\right\}}_{\mathscr{K}_1} \\ &\quad \times \underbrace{\Pr\left\{\left|h_{\text{UD}_1}\right|^2 > \frac{\epsilon_1 \sigma_{D_1}^2}{(\alpha_1 - \epsilon_1\alpha_2) G_{\text{UD}_1} P_u L\left(d_{\text{UD}_1}\right)}\right\}}_{\mathscr{K}_2}, \end{aligned} \tag{13}$$

where $\epsilon_1 = 2^{2R_1} - 1$. According to (5), $\mathscr{K}_1$ can be given by

$$\mathscr{K}_1 = \sum_{k=\{L,N\}} P_k(r_{\text{SU}}) \sum_{n=0}^{N_k-1} \left(N_k \xi_1\right)^n \frac{1}{n!} e^{-N_k \xi_1}, \tag{14}$$

where $d_{\text{SU}} = \sqrt{r_{\text{SU}}^2 + H^2}$ and $\xi_1 = \epsilon_1 \sigma_U^2 \left(r_{\text{SU}}^2 + H^2\right)^{\tau/2} \eta_k / (\alpha_1 - \epsilon_1\alpha_2) G_{\text{SU}} P_s$. By applying the polar coordinates and the probability generating functional (PGFL) of PPP, $\mathscr{K}_2$ can be derived as follows:

$$\begin{aligned} \mathscr{K}_2 &= \Pr\left\{\left|h_{\text{UD}_1}\right|^2 > \frac{\epsilon_1 \sigma_{D_1}^2}{(\alpha_1 - \epsilon_1\alpha_2) G_{\text{UD}_1} P_u L\left(d_{\text{UD}_1}\right)}\right\} \\ &= \sum_{k=\{L,N\}} \frac{2}{r_{\max^2} - r_{\min^2}} \int_{r_{\min}}^{r_{\max}} P_k(r) \\ &\quad \times \Pr\left\{\left|h_{\text{UD}_1}\right|^2 > \xi_2\right\} \text{rdr} \\ &= \sum_{k=\{L,N\}} \frac{2}{r_{\max^2} - r_{\min^2}} \left(\int_0^{r_{\max}} P_k(r) \times \Pr\left\{\left|h_{UD_1}\right|^2 > \xi_2\right\} \text{rdr} - \int_0^{r_{\min}} P_k((r)) \times \Pr\left\{\left|h_{\text{UD}_1}\right|^2 > \xi_2\right\} \text{rdr} \right) \\ &= \sum_{k=\{L,N\}} \frac{2}{r_{\max^2} - r_{\min^2}} \left(\int_0^{r_{\max}} P_k(r) \times \sum_{n=0}^{N_k-1} \left(N_k \xi_2\right)^n \frac{1}{n!} e^{-N_k \xi_2} \text{rdr} - \int_0^{r_{\min}} P_k(r) \times \sum_{n=0}^{N_k-1} \left(N_k \xi_2\right)^n \frac{1}{n!} e^{-N_k \xi_2} \text{rdr} \right), \end{aligned} \tag{15}$$

where $\xi_2 = \epsilon_1\sigma_{D_1}^2(r^2+H^2)^{\tau/2}\eta_k/(\alpha_1-\epsilon_1\alpha_2)G_{\mathrm{UD}_1}P_u$. It is difficult to obtain the closed-form expression of (15), so the Gaussian–Chebyshev quadrature is applied to yield a close approximation with $r(v_l) = r_{\max}(v_l+1)/2$, $v_l = \cos(2l-1/2L\pi)$, $r(v_t) = r_{\min}(v_t+1)/2$, and $v_t = \cos(2t-1/2L\pi)$. By substituting (14) and (15) into (13), the closed-form expression can be obtained as (12).

In the following, we investigate the reliable transmission of D_2 for the NOMA scheme. □

Theorem 2. *Since D_2 decodes x_1 first and then decodes its own information x_2, $\gamma_{SU}^{x_1} > 2^{R_1}-1$, $\gamma_{SU}^{x_2} > 2^{R_2}-1$, $\gamma_{UD_2}^{x_1} > 2^{R_1}-1$ and $\gamma_{UD_2}^{x_2} > 2^{R_2}-1$ must be satisfied simultaneously for the reliable communications. The closed-form expression of COP can be derived as (19).*

$$P_{\mathrm{cop}}^{D2} = 1 - \sum_{k_1=\{L,N\}} P_{k_1}(r_{\mathrm{SU}}) \sum_{n=0}^{N_{k_1}-1} \left(N_k\xi_3\left(r_{\mathrm{SU}}^2+H^2\right)^{(\tau/2)}\right)^n \frac{1}{n!} e^{-N_k\xi_3\left(r_{\mathrm{SU}}^2+H^2\right)^{(\tau/2)}} \sum_{k_2=\{L,N\}} \frac{2}{r_{\min^2}} \times \sum_{l=1}^{L}\sum_{n=0}^{N_{k_2}-1} \sqrt{1-g_l^2}\,P_{k_2}(r(g_l)) \frac{\left(N_k\xi_4\left(r((g_l))^2+H^2\right)^{(\tau/2)}\right)^n}{n!} e^{-N_k\xi_4\left(r((g_l))^2+H^2\right)^{\tau/2}} r(g_l). \tag{16}$$

Proof. The COP of D_2 can be given by

$$\begin{aligned} P_{\mathrm{cop}}^{D2} &= 1 - \Pr\left\{\gamma_{\mathrm{SU}}^{x_1} > 2^{2R_1}-1, \gamma_{\mathrm{SU}}^{x_2} > 2^{2R_2}-1\right\} \times \Pr\left\{\gamma_{\mathrm{UD}_2}^{x_1} > 2^{2R_1}-1, \gamma_{\mathrm{UD}_2}^{x_2} > 2^{2R_2}-1\right\} \\ &= 1 - \underbrace{\Pr\left\{\left|h_{\mathrm{SU}}\right|^2 > \xi_3\left(r_{\mathrm{SU}}^2+H^2\right)^{(\tau/2)}\right\}}_{\mathscr{K}_3} \times \underbrace{\Pr\left\{\left|h_{\mathrm{UD}_2}\right|^2 > \xi_4\left(r_{\mathrm{UD}_2}^2+H^2\right)^{(\tau/2)}\right\}}_{\mathscr{K}_4}, \end{aligned} \tag{17}$$

where
$\xi_3 = \max\left\{\epsilon_2\sigma_U^2\eta_k/\alpha_2G_{SU}P_s, \epsilon_1\sigma_U^2\eta_k/(\alpha_1-\epsilon_1\alpha_2)G_{\mathrm{SU}}P_s\right\}$,
$\xi_4 = \max\left\{\epsilon_2\sigma_{D_2}^2\eta_k/\alpha_2G_{\mathrm{UD}_2}P_u, \epsilon_1\sigma_{D_2}^2\eta_k/(\alpha_1-\epsilon_1\alpha_2)G_{\mathrm{UD}_2}P_u\right\}$

and $\epsilon_2 = 2^{2R_2}-1$. Similar to (17), $\mathscr{K}_3$ can be obtained as follows:

$$\mathscr{K}_3 = \sum_{k=\{L,N\}} P_k(r_{\mathrm{SU}}) \sum_{n=0}^{N_k-1} \left(N_k\xi_3\left(r_{\mathrm{SU}}^2+H^2\right)^{\tau/2}\right)^n \times \frac{1}{n!} e^{-N_k\xi_3\left(r_{\mathrm{SU}}^2+H^2\right)^{(\tau/2)}}. \tag{18}$$

Since D_2 is randomly located in a circle of radius $r_{\min}$, $\mathscr{K}_4$ can be obtained as follows:

$$\begin{aligned} \mathscr{K}_4 &= \Pr\left\{\left|h_{\mathrm{UD}_2}\right|^2 > \xi_4\left(r_{\mathrm{UD}_2}^2+H^2\right)^{(\tau/2)}\right\} \\ &= \sum_{k=\{L,N\}} \frac{2}{r_{\min^2}} \int_0^{r_{\min}} P_k(r) \times \Pr\left\{\left|h_{\mathrm{UD}_1}\right|^2 > \xi_4\left(r_{\mathrm{UD}_2}^2+H^2\right)^{(\tau/2)}\right\} \mathrm{rdr} \\ &= \sum_{k=\{L,N\}} \frac{2}{r_{\min^2}} \int_0^{r_{\min}} P_k(r) \times \sum_{n=0}^{N_k-1} \frac{\left(N_k\xi_4\left(r^2+H^2\right)^{(\tau/2)}\right)^n}{n!} e^{-N_k\xi_4\left(r^2+H^2\right)^{\tau/2}} \mathrm{rdr}. \end{aligned} \tag{19}$$

By exploiting the Gaussian–Chebyshev quadrature and substituting $r(g_l) = r_{\min}(g_l+1)/2$, $g_l = \cos(2l-1/2L\pi)$, $\mathscr{K}_4$ can be rewritten as follows:

$$\mathcal{K}_4 = \sum_{k=\{L,N\}} \frac{\pi}{r_{\min} L} \sum_{l=1}^{L} \sum_{n=0}^{N_k-1} \sqrt{1-g_l^2} P_k(r(g_l)) \times \frac{\left(N_k \xi_4 \left(r(g_l)^2 + H^2\right)^{(\tau/2)}\right)^n}{n!} e^{-N_k \xi_4 \left(r(g_l)^2 + H^2\right)^{(\tau/2)}} r(g_l). \tag{20}$$

According to (18) and (20), the COP of D_2 can be derived as (16). □

Remark 1. It can be observed from Theorems 1 and 2 that the COPs of D_1 and D_2 decrease with the increase of source transmitting power P_s and P_u. Besides, reducing the zone radius of external sector ring $r_{\max}$ and $r_{\min}$ can decrease the COPs of D_1 and D_2, which implies a smaller user area or one closer to the UAV relay can improve the reliability of the system.

Proposition 1. *The asymptotic COPs of D_1 and D_2 can be respectively expressed as follows:*

$$P_{\text{cop,asy}}^{D_1} = 1 - \frac{2}{r_{\max^2} - r_{\min^2}} \sum_{k_1=\{L,N\}} \sum_{k_2=\{L,N\}} P_{k_1}(r_{\text{SU}}) \times \int_{r_{\min}}^{r_{\max}} P_{k_2}(r) \text{rdr}, \tag{21}$$

and

$$P_{\text{cop,asy}}^{D_2} = 1 - \frac{2}{r_{\min^2}} \sum_{k_1=\{L,N\}} \sum_{k_2=\{L,N\}} P_{k_1}(r_{\text{SU}}) \times \int_{0}^{r_{\min}} P_{k_2}(r) \text{rdr}. \tag{22}$$

Proof. As the transmitting power P_s and P_u approach infinity, by exploiting $e^{-x} = 1 - x$ for small x, we have

$$\begin{aligned} \sum_{n=0}^{N_k-1} (N_k \xi_1)^n \frac{1}{n!} e^{-N_k \xi_1} &\approx \sum_{n=0}^{N_k-1} (N_k \xi_1)^n \frac{1}{n!} (1 - N_k \xi_1) \\ &\approx \sum_{n=0}^{N_k-1} (N_k \xi_1)^n \frac{1}{n!}. \end{aligned} \tag{23}$$

In (23), the term corresponding to $n = 0$ is larger than the summation of other terms owing to the presence of ξ_1^n and ξ_2^n when P_s and P_u go to infinity. Hence, $P_{\text{cop,asy}}^{D_1}$ can be approximated as the term corresponding to $n = 0$. After some mathematical manipulation, $P_{\text{cop,asy}}^{D_1}$ can be rewritten as (21). Similarly, the expression of $P_{\text{cop,asy}}^{D_2}$ can be obtained as (22). The proof is completed. □

3.2. SOP of D_2 for NOMA Scheme. Since D_2 is a high-security required user, we analyze the secrecy performance of D_2 in terms of SOP. According to Wyner's wiretap code theory, the SOP is defined as the probability which the wiretap channel capacity is larger than the redundancy rate of wiretap code [26]. For the proposed protected zone method, we consider the case that the eavesdroppers are located inside the circle of radius (r_E, $r_{\max}$) with angle θ_s. Particularly, by denoting r as the horizontal distance between U and E, the distance d_{SE} can be expressed as $d_{\text{SE}} = \sqrt{r^2 + r_{\text{SU}}^2 - 2 r r_{\text{SU}} \cos(\pi - \theta)}$ with $r_E \le r \le r_{\max}$ and $\theta \in [-\theta_s/2, \theta_s/2]$.

Lemma 1. *Denoting R_s as the target secrecy rate of D_2, we define the function $F_1(r, \theta)$ and $F_2(r)$ in polar coordinates to describe the probability $\Pr\{\gamma_{SE} > 2^{2(R_2 - R_s)} - 1\}$ and $\Pr\{\gamma_{UE} > 2^{2(R_2 - R_s)} - 1\}$. By considering $S - E$ channel as the NLoS link, while $U - E$ channel is composed of NLoS link and LoS link, and $F_1(r, \theta)$ and $F_2(r)$ can be expressed as follows:*

$$\begin{aligned} F_1(r, \theta) &= \Pr\left\{\gamma_{\text{SE}} > 2^{2(R_2 - R_s)} - 1\right\} \\ &= \Pr\left\{|h_{\text{SE}}|^2 > \frac{\varepsilon_s \sigma_E^2}{\alpha_2 G_{SE} P_s L(d_{\text{SE}})}\right\} \\ &= \sum_{i \in \{m,M\}} p_i^E \Pr\left\{|h_{\text{SE}}|^2 > \xi_5 \left(r^2 + r_{\text{SU}}^2 - 2 r r_{\text{SU}} \cos(\pi - \theta)\right)^{(\tau/2)}\right\}, \end{aligned} \tag{24}$$

and

$$\begin{aligned} F_2(r) &= \Pr\left\{\gamma_{\text{UE}} > 2^{R_2 - R_s} - 1\right\} \\ &= \Pr\left\{|h_{\text{UE}}|^2 > \frac{\epsilon_s \sigma_E^2}{\alpha_2 G_{\text{UE}} P_s L(d_{\text{UE}})}\right\} \\ &= \sum_{w=\{L,N\}} \sum_{i,j \in \{m,M\}} p_i^U p_j^E P_w(r) \Pr\left\{|h_{\text{UE}}|^2 > \xi_6 \left(r^2 + H^2\right)^{(\tau/2)}\right\}, \end{aligned} \tag{25}$$

where $\epsilon_s = 2^{2(R_2 - R_s)} - 1$, $\xi_5 = (\epsilon_s \sigma_E^2 / \alpha_2 G_S^m G_E^i P_s)$ and $\xi_6 = \epsilon_s \sigma_E^2 \eta_w / \alpha_2 G_U^i G_E^j P_u$.

Based on Lemma 1, the SOP of D_2 is given in the following theorem:

Theorem 3. *In light of the HPPPs distribution for E, the SOP of D_2 under protected zone method is given by*

$$\begin{aligned} P_{\text{sop}}^{D_2} &= \Pr\left\{\max\left(\max_{E \in \Phi_e} \gamma_{\text{SE}}, \max_{E \in \Phi_e} \gamma_{\text{UE}}\right) > \epsilon_s\right\} \\ &= 1 - \underbrace{\mathbb{E}\left[\prod_{E \in \Phi_e} \Pr\{\gamma_{\text{SE}} < \epsilon_s\}\right]}_{\mathcal{K}_5} \underbrace{\mathbb{E}\left[\prod_{E \in \Phi_e} \Pr\{\gamma_{UE} < \epsilon_s\}\right]}_{\mathcal{K}_6}, \end{aligned} \tag{26}$$

where $\mathscr{K}_5$ and $\mathscr{K}_6$ are given in (27) and (28

$$\begin{aligned}\mathscr{K}_5 = \exp\Bigg\{ & -\frac{\theta_s^3\lambda_E}{64\mathrm{TL}} \sum_{i\in\{m,M\}} \sum_{l=1}^{L}\sum_{t=1}^{T}\sum_{n=0}^{N_N-1} \frac{p_i^E}{n!}\sqrt{1-a_l^2}\,\sqrt{1-b_t^2}\left(\frac{r_{\max}-r_E}{2}b_t+\frac{r_{\max}+r_E}{2}\right) \\ & \times\left(\frac{N_N\epsilon_s\sigma_E^2}{\alpha_2 G_S^m G_E^i P_s}\left(\left(\frac{r_{\max}-r_E}{2}b_t+\frac{r_{\max}+r_E}{2}\right)^2+r_{SU}^2+2\left(\frac{r_{\max}-r_E}{2}b_t+\frac{r_{\max}+r_E}{2}\right)r_{SU}\cos\theta\right)^{(\tau/2)}\right)^n \\ & \times e^{-\left(N_N\epsilon_s\sigma_E^2/\alpha_2 G_S^m G_E^i P_s\right)\left(\left(r_{\max}-r_E/2b_t+r_{\max}+r_E/2\right)^2+r_{\mathrm{SU}}^2+2\left(\left(r_{\max}-r_E/2b_t+r_{\max}+r_E/2\right)\right)r_{\mathrm{SU}}\cos\theta\right)^{\tau/2}}\Bigg\},\end{aligned} \tag{27}$$

$$\begin{aligned}\mathscr{K}_6 = \exp\Bigg\{ & -\lambda_E\theta_s \sum_{i,j\in\{m,M\}} p_i^U p_j^E \left(\frac{\pi r_{\max} r(c_l)}{2L}\sum_{w=\{L,N\}}\sum_{l=1}^{L}\sum_{n=0}^{N_w-1}\frac{\sqrt{1-c_l^2}\,P_w(r(c_l))}{n!}\left(\frac{N_w\epsilon_s\sigma_E^2\left(r^2(c_l)+H^2\right)^{(\tau/2)}}{\alpha_2 G_U^i G_E^j P_u}\right)^n\right. \\ & \times e^{-\left(N_w\epsilon_s\sigma_E^2\left(r^2(c_l)+H^2\right)^{\tau/2}/\alpha_2 G_U^i G_E^j P_u\right)} - \frac{\pi r_E r(d_t)}{2L}\sum_{w=\{L,N\}}\sum_{l=1}^{L}\sum_{n=0}^{N_w-1}\frac{\sqrt{1-d_t^2}\,P_w(r(d_t))}{n!} \\ & \left.\cdot\left(\frac{N_w\epsilon_s\sigma_E^2\left(r^2(d_t)+H^2\right)^{(\tau/2)}}{\alpha_2 G_U^i G_E^j P_u}\right)^n e^{-\left(N_w\epsilon_s\sigma_E^2\left(r^2(d_t)+H^2\right)^{(\tau/2)}/\alpha_2 G_U^i G_E^j P_u\right)}\right)\Bigg\}.\end{aligned} \tag{28}$$

Proof. Following the PGFL of PPP, we can obtain

$$\begin{aligned}\mathscr{K}_5 &= \exp\left\{-\lambda_E\int_{-(\theta_s/2)}^{(\theta_s/2)}\int_{r_E}^{r_{\max}}\Pr\{\gamma_{\mathrm{SE}}>\epsilon_s\}r\mathrm{d}r\mathrm{d}\theta\right\} \\ &= \exp\left\{-2\lambda_E\int_{0}^{(\theta_s/2)}\int_{r_E}^{r_{\max}}F_1(r,\theta)r\mathrm{d}r\mathrm{d}\theta\right\} \\ &\overset{(a)}{\approx} \exp\left\{-\frac{\theta_s^3\lambda_E}{64}\sum_{l=1}^{L}\sum_{t=1}^{T}\sqrt{1-a_l^2}\,\sqrt{1-b_t^2}\times\frac{1}{\mathrm{TL}}\left(\frac{r_{\max}-r_E}{2}b_t+\frac{r_{\max}+r_E}{2}\right)\times F_1\left(\frac{r_{\max}-r_E}{2}b_t+\frac{r_{\max}+r_E}{2},\frac{\theta_s}{4}(a_l+1)\right)\right\},\end{aligned} \tag{29}$$

$$\begin{aligned}\mathscr{K}_6 &= \exp\left\{-\lambda_E\theta_s\int_{r_E}^{r_{\max}}\Pr\{\gamma_{\mathrm{UE}}>\epsilon_s\}r\mathrm{d}r\right\} \\ &= \exp\left\{-\lambda_E\theta_s\int_{r_E}^{r_{\max}}F_2(r)r\mathrm{d}r\right\} \\ &\overset{(b)}{\approx} \exp\left\{-\lambda_E\theta_s\left(\frac{\pi r_{\max}}{2L}\sum_{l=1}^{L}\sqrt{1-c_l^2}\,F_2(r(c_l))r(c_l)-\frac{\pi r_E}{2T}\sum_{t=1}^{T}\sqrt{1-d_t^2}\,F_2(r(d_t))r(d_t)\right)\right\}.\end{aligned}$$

Step (a) is computed by a two-layer Gauss–Chebyshev integration related to r and θ, where $a_l = \cos(2l - 1/2L\pi)$ and $b_t = \cos(2t - 1/2T\pi)$. Step (b) is calculated through the similar procedure of deriving $\mathscr{K}_2$ with $c_l = \cos(2l - 1/2L\pi)$, $d_t = \cos(2t - 1/2T\pi)$, $r(c_l) = r_{\max}(c_l + 1)/2$ and $r(d_t) = r_E \quad (d_t + 1)/2$. Substituting (5) into (24) and (25), equation $\mathscr{K}_5$ and $\mathscr{K}_6$ are expressed as (27) and (28), respectively. The proof is completed. □

Remark 2. From Theorem 3, we can observe that the SOP of D_2 is influenced by the transmitting power P_s and P_u, the target codeword rate R_2, the confidential codeword rate R_s, the power allocation factor α_2, and the distribution of eavesdroppers Φ_e. To be specific, the SOP decreases with the reduction of eavesdroppers' density λ_E and the increase of r_E. The SOP increases with the enlargement of P_s and P_u, which means the enhancement of reliability leads to more information at the risk of eavesdropping.

To proceed forward, we derive the asymptotic expression of the SOP to gain more insights. When the transmitting power P_s and P_u are sufficiently large, the asymptotic SOP under the NOMA scheme is shown in the following:

Proposition 2. *The asymptotic SOP under the NOMA scheme can be calculated as follows:*

$$P_{\text{sop-asy}}^{D_2} = 1 - \exp\left(-\theta_s \lambda_E \left(r_{\max^2} - r_E^2\right)\right). \tag{30}$$

Proof. For sufficiently large P_s, $\mathscr{K}_5$ can be calculated as follows:

$$\begin{aligned}\mathscr{K}_5 &= \exp\left\{-\lambda_E \int_{-(\theta_s/2)}^{(\theta_s/2)} \int_{r_E}^{r_{\max}} \Pr\{\gamma_{\text{SE}} > \epsilon_s\} r \mathrm{d}r \mathrm{d}\theta\right\} \\ &= \exp\left\{-\lambda_E \int_{-(\theta_s/2)}^{(\theta_s/2)} \int_{r_E}^{r_{\max}} \sum_{i\in\{m,M\}} p_i^E \times \sum_{n=0}^{N_N-1} \left(N_N \frac{\Omega}{P_s}\right)^n \frac{1}{n!} e^{-N_N \Omega/P_s} r \mathrm{d}r \mathrm{d}\theta\right\},\end{aligned} \tag{31}$$

where $\Omega = \epsilon_s \sigma_E^2 (r^2 + r_{SU}^2 - 2rr_{SU}\cos(\pi - \theta))^{\tau/2}/\alpha_2 G_S^m G_E^i$. When $P_s \longrightarrow \infty$, by utilizing the approximation of $e^{-x} \approx 1 - x$ for small x, we have

$$\begin{aligned}\sum_{n=0}^{N_N-1} \left(N_N \frac{\Omega}{P_s}\right)^n \frac{1}{n!} e^{-N_N(\Omega/P_s)} &\approx \sum_{n=0}^{N_N-1} \left(N_N \frac{\Omega}{P_s}\right)^n \frac{1}{n!} \left(1 - N_N \frac{\Omega}{P_s}\right) \\ &\approx \sum_{n=0}^{N_N-1} \left(N_N \frac{\Omega}{P_s}\right)^n \frac{1}{n!}.\end{aligned} \tag{32}$$

In (32), the term corresponding to $n = 0$ is larger than the summation of other terms owing to the presence of $(\Omega/P_s)^n$ when P_s goes to infinity. Hence, $\mathscr{K}_5$ can be approximated as the term corresponding to $n = 0$, and it can be rewritten as follows:

$$\mathscr{K}_5 = \exp\left(-\frac{\theta_s \lambda_E}{2}\left(r_{\max^2} - r_E^2\right)\right). \tag{33}$$

Similarly, we can derive $\mathscr{K}_6 = \mathscr{K}_5$. After some calculations, the proof of $P_{\text{sop-asy}}^{D_2}$ is completed. □

Remark 3. It can be observed from Proposition 2 that the asymptotic SOP is influenced by the density of eavesdroppers and the size of the protected zone when P_s and P_u are considerably large.

3.3. EST of D_2 for NOMA Scheme. The reliability and security of the system are investigated above. However, it is necessary to use a unified framework to integrate security and reliability considerations. To holistically characterize the performance of the system, we derive the effective secrecy throughput (EST) of the system, which is defined as the secrecy rate multiplied by the reliable-and-secure probability of D_2.

Theorem 4. *The EST of D_2 for NOMA scheme can be written as follows:*

$$T_{\text{EST}}^{D_2} = R_s\left(1 - P_{\text{cop}}^{D_2}\right)\left(1 - P_{\text{sop}}^{D_2}\right), \tag{34}$$

where $P_{cop}^{D_2}$ and $P_{sop}^{D_2}$ are shown in (16) and (26), respectively.

Proof. Due to the independence of the channels, $P_{\text{cop}}^{D_2}$ and $P_{\text{sop}}^{D_2}$ are independent of each other. As a result, we can derive

$$\begin{aligned}T_{\text{EST}}^{D_2} &= R_s \Pr\left\{\gamma_{\text{SU}}^{x_2} > \epsilon_2, \gamma_{\text{UD}_2}^{x_1} > \epsilon_1, \gamma_{\text{UD}_2}^{x_2}\right. \\ &\quad \left. > \epsilon_2, \max\left(\max_{E\in\Phi_e} \gamma_{\text{SE}}, \max_{E\in\Phi_e} \gamma_{\text{UE}}\right) < \epsilon_s\right\} \\ &= R_s\left(1 - P_{\text{cop}}^{D_2}\right)\left(1 - P_{\text{sop}}^{D_2}\right).\end{aligned} \tag{35}$$

The proof is completed. □

Remark 4. From Theorem 4, we can observe that the reliability is improved while the security is degraded with the increase of P_s and P_u. It means there exists a trade-off between reliability and security. By selecting the optimal transmitting power, the system's reliability-security performance index can be maximized.

Next, we analyze the system performance for the OMA transmission scheme to make a fair comparison. By considering one of the OMA transmissions, that is, the TDMA scheme, the communication progress is evenly divided into four time slots. In the first time slot, S sends signal x_1 to U. U decodes and forwards x_1 to D_1 at the next time slots. Similarly, S sends signal x_2 to D_2 by relay U in the next two time slots.

The COPs of D_1 and D_2 for OMA scheme can be expressed as follows:

$$\begin{aligned}P_{\text{cop}}^{\text{OMA}_{D_1}} &= 1 - \Pr\left\{\gamma_{\text{SU}}^{x_1} > 2^{4R_1} - 1, \gamma_{\text{UD}_1}^{x_1} > 2^{4R_1} - 1\right\} \\ &= 1 - \Pr\left\{|h_{\text{SU}}|^2 > \frac{\epsilon_1' \sigma_u^2}{L(d_{\text{SU}})P_s}\right\} \times \Pr\left\{|h_{\text{UD}_1}|^2 > \frac{\epsilon_1' \sigma_{D_1}^2}{L(d_{\text{UD}_1})P_u}\right\}, \\ P_{\text{cop}}^{\text{OMA}_{D_2}} &= 1 - \Pr\left\{\gamma_{\text{SU}}^{x_2} > 2^{4R_2} - 1, \gamma_{\text{UD}_1}^{x_2} > 2^{4R_2} - 1\right\} \\ &= 1 - \Pr\left\{|h_{\text{SU}}|^2 > \frac{\epsilon_2' \sigma_u^2}{L(d_{\text{SU}})P_s}\right\} \times \Pr\left\{|h_{\text{UD}_2}|^2 > \frac{\epsilon_2' \sigma_{D_2}^2}{L(d_{\text{UD}_2})P_u}\right\},\end{aligned} \tag{36}$$

where $\epsilon_1' = 2^{4R_1} - 1$ and $\epsilon_2' = 2^{4R_2} - 1$. The SOP of D_2 for OMA scheme can be expressed as follows:

$$P_{\text{sop}}^{\text{OMA}_{D_2}} = 1 - \Pr\left\{\max_{E\in\Phi_e}\gamma_{\text{SE}} < 2^{4(R_2-R_s)} - 1\right\} \times \Pr\left\{\max_{E\in\Phi_e}\gamma_{\text{UE}} < 2^{4(R_2-R_s)} - 1\right\}$$
$$= 1 - \mathbb{E}\left[\prod_{E\in\Phi_e}\Pr\left\{|h_{\text{SE}}|^2 < \frac{\epsilon_s'\sigma_E^2}{P_s L(d_{\text{SE}})}\right\}\right] \times \mathbb{E}\left[\prod_{E\in\Phi_e}\Pr\left\{|h_{\text{UE}}|^2 < \frac{\epsilon_s'\sigma_E^2}{P_u L(d_{\text{UE}})}\right\}\right], \tag{37}$$

where $\epsilon_s' = 2^{4(R_2-R_s)} - 1$.

4. Performance Analysis with Jamming

In this section, we propose a cooperative jamming strategy to improve the secrecy performance of the system. Specifically, a friendly aerial jammer J is introduced to interfere with the eavesdroppers by sending AN. As illustrated in [41], the AN is designed by the pseudorandom sequence method, which is known to legitimate nodes but unknown to eavesdroppers. Therefore, the AN can be canceled at the legitimate nodes and only deteriorate the channel quality of the eavesdroppers. It is worth noting that the pseudorandom sequence can be realized by channel estimation-assisted physical layer key generation and agreement without presharing as in traditional cryptography [42–44]. Without loss of generality, we assume the jammer UAV is hovering at the same altitude as the relay UAV. Under this method, the COP of D_1 and D_2 is the same as (12) and (16). In the following, we analyze the SOP and EST of the cooperative jamming strategy.

4.1. SOP of D_2 for NOMA Scheme with Cooperative Jamming. The SINR for eavesdroppers to decode x_2 from S and U can be calculated as follows:

$$\gamma_{\text{SE}}^J = \max_{E\in\Phi_e}\frac{\alpha_2 G_{\text{SE}} P_s |h_{\text{SE}}|^2 L(d_{\text{SE}})}{\sigma_E^2 + G_{\text{JE}} P_j |h_{JE}|^2 L(d_{\text{JE}})},$$
$$\gamma_{\text{UE}}^J = \max_{E\in\Phi_e}\frac{\alpha_2 G_{\text{UE}} P_u |h_{UE}|^2 L(d_{\text{UE}})}{\sigma_E^2 + G_{\text{JE}} P_j |h_{\text{JE}}|^2 L(d_{\text{JE}})}. \tag{38}$$

Lemma 2. *For the NOMA scheme with cooperative jamming, we set the polar function $F_3(r,\theta)$ and $F_4(r,\theta)$ to denote $\Pr\{\gamma_{SE}^J > 2^{2(R_2-R_s)} - 1\}$ and $\Pr\{\gamma_{UE}^J > 2^{2(R_2-R_s)} - 1\}$. $F_3(r,\theta)$ and $F_4(r,\theta)$ are, respectively, written as (40) and (41).*

Proof. By denoting $z = |h_{JE}|^2$, $F_3(r,\theta)$ can be derived as

$$F_3(r,\theta) = \Pr\left\{\frac{\alpha_2 G_{\text{SE}} P_s |h_{\text{SE}}|^2 L(d_{\text{SE}})}{\sigma_E^2 + G_{\text{JE}} P_j |h_{\text{JE}}|^2 L(d_{\text{JE}})} > \epsilon_s\right\}$$
$$= \Pr\left\{|h_{\text{SE}}|^2 > \frac{\epsilon_s\left(\sigma_E^2 + G_{\text{JE}} P_j |h_{JE}|^2 L(d_{\text{JE}})\right)}{\alpha_2 G_{\text{SE}} P_s L(d_{\text{SE}})}\right\}$$
$$= \sum_{w=\{L,N\}}\sum_{i,j\in\{m,M\}} p_i^{\text{SE}} p_j^{\text{JE}} P_w(r_{\text{JE}}) \times \Pr\left\{|h_{\text{SE}}|^2 > \frac{\epsilon_s\left(\sigma_E^2 + G_J^M G_E^j P_j |h_{\text{JE}}|^2 L(d_{\text{JE}})\right)}{\alpha_2 G_S^m G_E^i P_s L(d_{\text{SE}})}\right\}$$
$$= \sum_{w=\{L,N\}}\sum_{i,j\in\{m,M\}} p_i^{\text{SE}} p_j^{JE} P_w(r_{JE}) \times \int_0^\infty \left(1 - F_{|h_{\text{SE}}|^2}\left(\frac{\epsilon_s\left(\sigma_E^2 + zG_J^M G_E^j P_j L(d_{\text{JE}})\right)}{\alpha_2 G_S^m G_E^i P_s L(d_{\text{SE}})}\right)\right) f_Z(z)\mathrm{d}z. \tag{39}$$

Utilizing (6) and (7), $F_3(r,\theta)$ can be further derived as (40) according to Eq. (3.381.4) in [45], where $r_{\text{JE}} = \sqrt{r^2 + r_{\text{UJ}}^2 - 2rr_{\text{UJ}}\cos\theta}$, $d_{\text{JE}} = \sqrt{H^2 + r_{\text{JE}}^2}$ and r_{UJ} denotes the horizontal distance between U and J. Similarly, $F_4(r,\theta)$ can be calculated as (41). Lemma 2 is proved.

$$F_3(r,\theta) = \sum_{w=\{L,N\}}\sum_{i,j\in\{m,M\}} e^{-\left(N_N\epsilon_s\sigma_E^2/\alpha_2 G_S^m G_E^i P_s L(d_{\text{SE}})\right)} \frac{p_i^{\text{SE}} p_j^J p_e^E P_w(r_{\text{JE}}) N_w^{N_w}}{\Gamma(N_w)} \sum_{n=0}^{N_N-1}\frac{1}{n!}\left(\frac{N_N\epsilon_s}{\alpha_2 G_S^m G_E^i P_s L(d_{\text{SE}})}\right)^n$$
$$\times \sum_{k=0}^{n}\sigma_E^{2(n-k)}\left(G_J^j G_E^e P_j L(d_{\text{JE}})\right)^k (k+N_w-1)!\left(\frac{N_N\epsilon_s G_J^j G_E^e P_j L(d_{\text{JE}})}{\alpha_2 G_S^m G_E^i P_s L(d_{\text{SE}})} + N_w\right)^{-k-N_w}, \tag{40}$$

$$F_4(r,\theta) = \sum_{w,q=\{L,N\}}\sum_{i,j\in\{m,M\}} p_i^U p_j^E P_q(r) P_w(r_{JE}) e^{-N_q\epsilon_s\sigma_E^2/\alpha_2 G_U^i G_E^j P_u L(d_{\text{UE}})} \frac{N_w^{N_w}}{\Gamma(N_w)} \sum_{n=0}^{N_q-1}\frac{1}{n!}\left(\frac{N_q\epsilon_s}{\alpha_2 G_U^i G_E^j P_u L(d_{\text{UE}})}\right)^n$$
$$\times \sum_{k=0}^{n}\sigma_E^{2(n-k)}\left(G_J^j G_E^e P_j L(d_{\text{JE}})\right)^k (k+N_w-1)!\left(\frac{N_N\epsilon_s G_J^j G_E^e P_j L(d_{\text{JE}})}{\alpha_2 G_U^i G_E^j P_s L(d_{\text{UE}})} + N_w\right)^{-k-N_w}. \tag{41}$$

□

Theorem 5. *Similar to the above section, the SOP of D_2 under the proposed cooperative jamming scheme can be expressed as follows:*

$$P_{\text{sop}}^{J} = 1 - \underbrace{\mathbb{E}\left[\prod_{E \in \Phi_e} \Pr\left\{\gamma_{\text{SE}}^{J} < \epsilon_s\right\}\right]}_{\mathscr{K}_7} \underbrace{\mathbb{E}\left[\prod_{E \in \Phi_e} \Pr\left\{\gamma_{\text{UE}}^{J} < \epsilon_s\right\}\right]}_{\mathscr{K}_8}, \tag{42}$$

where

$$\mathscr{K}_7 \approx \exp\left\{-\frac{\theta_s^3 \lambda_E}{64} \sum_{l=1}^{L} \sum_{t=1}^{T} \sqrt{1-a_l^2}\sqrt{1-b_t^2} \times \frac{1}{\text{TL}}\left(\frac{r_{\max}-r_E}{2} b_t + \frac{r_{\max}+r_E}{2}\right) \times F_3\left(\frac{r_{\max}-r_E}{2} b_t + \frac{r_{\max}+r_E}{2}, \frac{\theta_s}{4}(a_l+1)\right)\right\},$$
$$\mathscr{K}_8 \approx \exp\left\{-\frac{\theta_s^3 \lambda_E}{64} \sum_{l=1}^{L} \sum_{t=1}^{T} \sqrt{1-a_l^2}\sqrt{1-b_t^2} \times \frac{1}{\text{TL}}\left(\frac{r_{\max}-r_E}{2} b_t + \frac{r_{\max}+r_E}{2}\right) \times F_4\left(\frac{r_{\max}-r_E}{2} b_t + \frac{r_{\max}+r_E}{2}, \frac{\theta_s}{4}(a_l+1)\right)\right\}. \tag{43}$$

Proof. Following similar steps as in the proof of Theorem 3, then Theorem 5 can be proved by exploiting a two-layer Gauss–Chebyshev quadrature equation. □

Remark 5. As can be seen from Theorem 5, the SOP of D_2 under the proposed cooperative jamming scheme is affected by many factors, among which jamming power plays an important role. By designing AN, the noise will not affect the SNR of legitimate users and the SOP monotonically decreases with the increase of P_j.

4.2. EST of D_2 for NOMA Scheme with Cooperative Jamming. Similar to the previous process of proving Theorem 4, the EST of D_2 under cooperative jamming scheme can be expressed as follows:

$$T_{\text{EST}}^{J} = R_s\left(1 - P_{\text{cop}}^{D_2}\right)\left(1 - P_{\text{sop}}^{J}\right), \tag{44}$$

where $P_{\text{cop}}^{D_2}$ and P_{sop}^{J} are shown in (16) and (42). To gain more insights, we analyze the performance when P_j is sufficiently large.

Proposition 3. *The asymptotic EST achieved by the cooperative jamming scheme can be calculated as follows:*

$$T_{\text{EST-asy}}^{J} = R_s\left(1 - P_{\text{cop}}^{D_2}\right). \tag{45}$$

Proof. As P_j goes to infinity, $\mathscr{K}_7$ and $\mathscr{K}_8$ approximately equals 1. Hence, the asymptotic EST under the cooperative jamming scheme can be rewritten as equation (45). The proof is completed. □

Remark 6. As can be observed from Proposition 3, in the case of high SNR of P_j, the EST of D_2 is mainly determined by COP and the influence of SOP on the system can be ignored. It is noted that the increase of power allocation factor α_2 improves the performance of the system in the high-SNR region. It can also be found that the asymptotic EST is independent of the jamming power, which means that the EST of the proposed cooperative jamming scheme converges to a floor with the increasing P_j.

5. Simulation Results and Discussions

In this section, numerical results are presented to illustrate the reliable and secure performance of the mmWave NOMA UAV-assisted relay system. Without loss of generality, the parameters are set as shown in Table 1. We assume that all nodes are equipped with N antennas. The transmitting power from the source and relay satisfies $P_s = P_u = P$. The unit of transmission rate is BPCU. The simulation results are obtained through 10^6 different Monte Carlo simulations.

In Figure 2, we investigate the reliability of D_1 versus R_1 under NOMA scheme for different parameters α_1 and N. It can be observed that the theoretical analysis agrees well with the simulation, which verifies the correctness of the theoretical derivation. Furthermore, the COP of D_1 increases with the target transmission rate R_1. It can also be found that the COP of D_1 decreases with the increase of P and α_1 because more power assigned to D_1 results in higher reliability of D_1. At the same time, more antennas deployed on UAVs can lead to greater main-lobe gain and thus improve the reliability, which encourages us to equip UAV with more antennas.

Figure 3 illustrates the COP of D_1 versus H for different target transmission rate R_1 and user zone. The analytical curves precisely match the simulations and the correctness of the derivation can be verified. As shown in Figure 3, the COP increases with the increase of flight height H, which demonstrates that longer distance leads to more path loss and impairs the reception quality of the signal. However, the higher LoS link probability caused by the increase of H is relatively negligible. In addition, the OMA scheme outperforms the NOMA scheme when $\alpha_1 = 0.7$ because the interference from the message of D_2 weakens the performance of D_1. The NOMA scheme performs better when α_1 continues to increase. Furthermore, reducing COP can be

Table 1: Simulation parameters.

Number of antennas	$N = 16$
Environment parameters	$\varphi = 9.6,\ \omega = 0.28$
Half-power beamwidth	$\theta_a = \theta_d = \sqrt{3/N}$
Main-lobe gain	$G_M = N$
Side-lobe gain	$G_m = \sqrt{N} - \sqrt{3}/2\pi N \sin(\sqrt{3}/2\sqrt{N})/\sqrt{N} - \sqrt{3}/2\pi \sin(\sqrt{3}/2\sqrt{N})$
The distance between ground nodes	$r_{\min} = 20$ m, $r_{\max} = 80$ m, $r_E = 30$ m
Path loss parameters	$\tau = 2,\ \eta_L = 1$ dB, $\eta_N = 20$ dB
Noise power	$-174 + 10\lg(BW) + NF$ dBm
The number of Gauss–Chebyshev nodes	$L = T = 20$
Nakagami-m fading parameters	$N_N = 2,\ N_L = 3$
The angle of protected zone	$\theta_s = \pi/3$
The flight altitude of UAVs	$H = 50$ m
The density of eavesdroppers	$0.0005/m^2$
Transmission bandwidth	$BW = 1$ GHz
Noise parameters	$NF = 10$ dB
The horizontal distance between S and U	$r_{SU} = 50$ m
The horizontal distance between U and J	$r_{UJ} = 30$ m

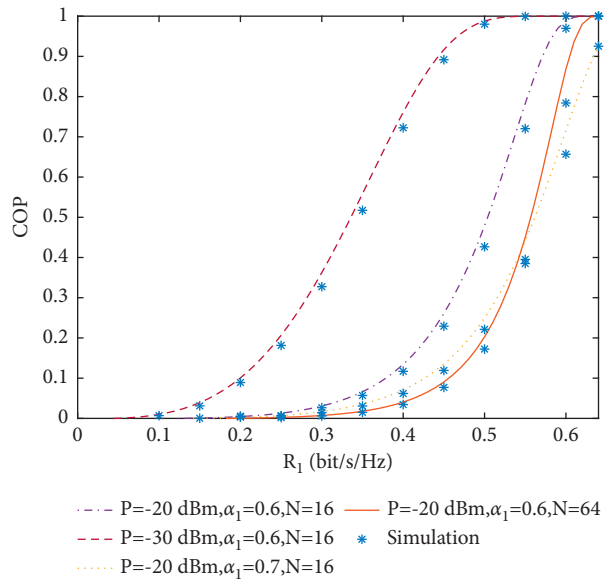

Figure 2: The COP of D_1 versus R_1 under NOMA scheme.

achieved by decreasing the user zone. It is due to the fact that in the case of random distribution, there are closer users in a smaller user area, which reduces the path loss.

Figure 4 shows the effect of P and R_2 on the reliability of D_2 under OMA and NOMA schemes. Observations can be drawn that the COP is reduced by increasing P. In addition, the asymptotic COP is in good agreement with the simulated value, which verifies the correctness of the analysis. For the COP of D_2, we note that the transmitting power demanded a small target rate R_2 is also small and vice versa. By comparing the COP under NOMA and OMA schemes, it is easy to find that the NOMA scheme outperforms the OMA scheme when R_2 is large. It is due to the fact that D_2 is difficult to achieve reliable transmission under the OMA scheme in half the time of the NOMA scheme. However, transmission in OMA mode is better for the system performance when R_2 is small, which encourages us to select the appropriate transmission mode according to different target transmission rates.

In Figure 5, we plot the SOP of D_2 as the function of λ_E under the NOMA scheme for different P_j and the number of antennas N. We can find that the secrecy performance can be improved by adopting the aerial cooperative jamming strategy. It can be explained that the channel quality of eavesdroppers can be deteriorated by jamming, while the channel quality of the legitimate user remains unchanged. Furthermore, it is obvious that the SOP of D_2 increases with the increase of λ_E. This is because the more the eavesdroppers distributed around S and U, the better the channel quality of the eavesdropper with the best eavesdropping SINR. It can also be seen that increasing the number of antennas can improve the security of the system, and it is more obvious when the jamming power increases. This is because increasing the number of antennas will suppress

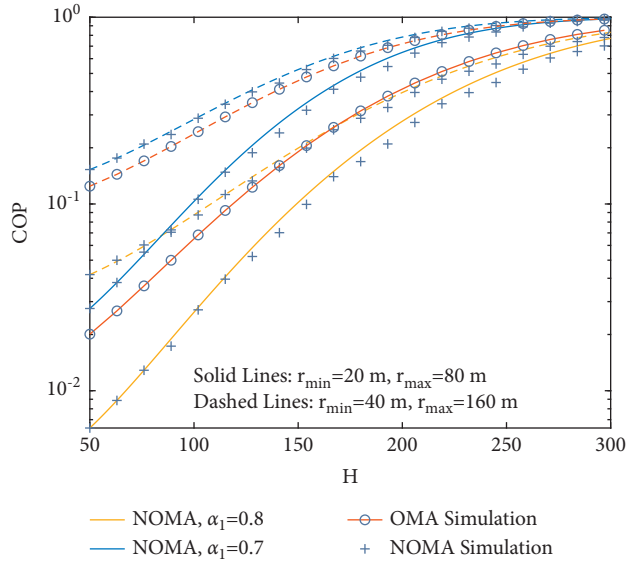

Figure 3: The COP of D_1 versus H under NOMA and OMA scheme for user zone radius and α_1, where $P = -20$ dBm and $R_1 = 0.6$.

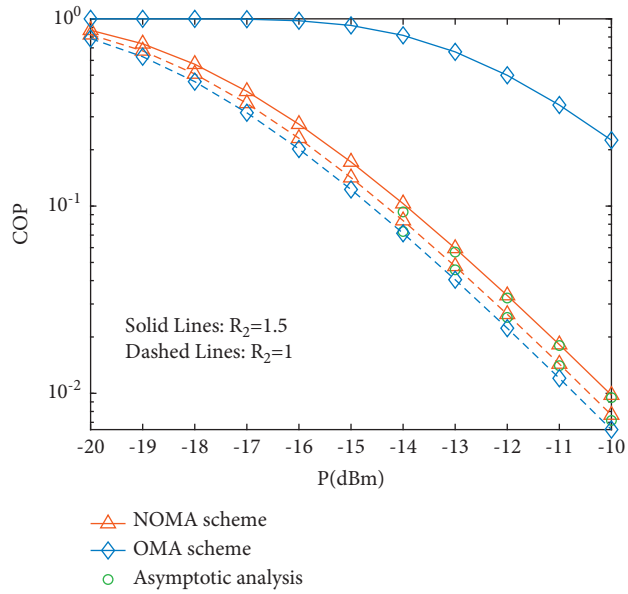

Figure 4: The COP of D_2 versus P under the NOMA and OMA scheme, where $R_1 = 0.6$, $R_s = 1$ and $\alpha_1 = 0.6$.

side-lobe gain and increase the main-lobe gain. It is noted that employing a large number of antennas is useful for the practical secure UAV system.

Figure 6 compares the EST of D_2 versus P under three schemes. It can be observed that the EST of D_2 increases to a peak value with the increase of P and then decreases to a stable value. There exists an optimal P to maximize EST. It is because the reliability is dominant when P is small, and the security is dominant when P is large. Increasing P reduces the probability of connection outage while making the signal more susceptible to eavesdropping, which is consistent with Figure 4. When P is considerably large, the SO is a dominant factor affecting the EST because COP tends to zero in that case. Note that the NOMA scheme with cooperative jamming outperforms the other two schemes. This is because the reliability of the NOMA scheme is better than the OMA scheme and the cooperative jamming strategy improves the security of the system.

Figure 7 plots the EST of D_2 versus P_j under three schemes. As shown in the figure, the EST of D_2 increases with the increase of P_j under the NOMA scheme with cooperative jamming. It can be explained by the fact that increasing P_j results in more interference on the channel of eavesdroppers, which deteriorates the quality of wire-tapping. The smaller the location distribution of eavesdroppers, the higher the EST of D_2 is. When P_j goes to infinity, the ESTs of D_2 with different protected zones converge to the same value, which verifies the result of

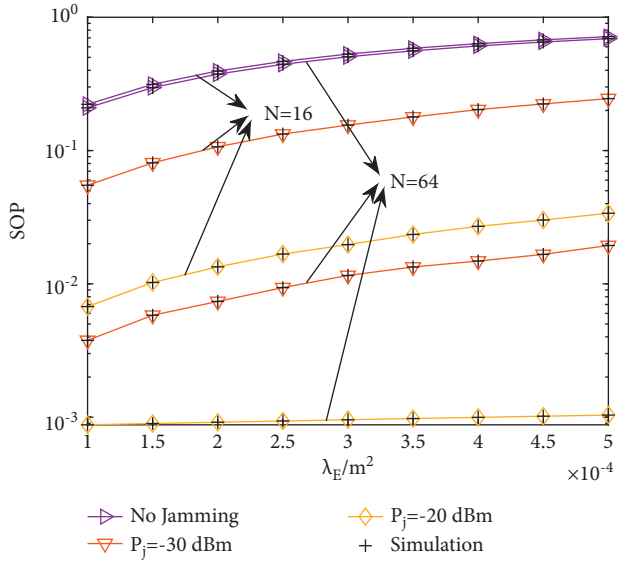

Figure 5: The SOP of D_2 versus λ_E under NOMA scheme, where $R_1 = 0.6, R_2 = 1.5, R_s = 1, \alpha_1 = 0.6, P = -30$ dBm.

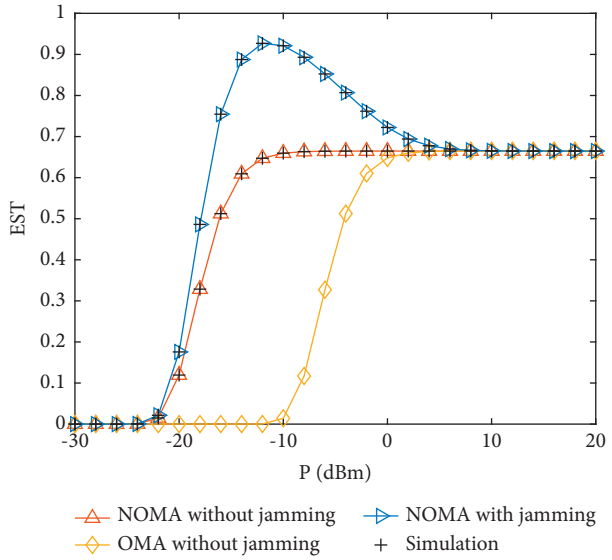

Figure 6: The EST of D_2 versus P under different schemes, where $R_1 = 0.6, R_2 = 2, R_s = 1, \alpha_1 = 0.6, P_j = -20$ dBm.

Proposition 3. Note that, increasing the jamming power within a reasonable range is meaningful for the practical system design. Meanwhile, the EST of the system without cooperative jamming strategy does not change with P_j. Obviously, the NOMA scheme outperforms the OMA scheme owing to the improvement of reliability under the NOMA scheme. As a result, it shows the superiority of the proposed NOMA scheme with cooperative jamming.

Figure 8 shows the EST of D_2 versus different P and P_j under the NOMA scheme with cooperative jamming. It is observed that the higher jamming power is beneficial to the EST of the system. When the transmitting power of P increases, the EST of D_2 increases initially and decreases afterward. However, when P_j is fairly large or fairly small, the EST remains constant after enlargement as P increases. The figure also shows that there is an optimal $[P, P_j]$ point, which can minimize the consumption of resources and obtain good reliability and security performance. It provides the theoretical basis and reference for the practical design of the UAV mmWave NOMA system.

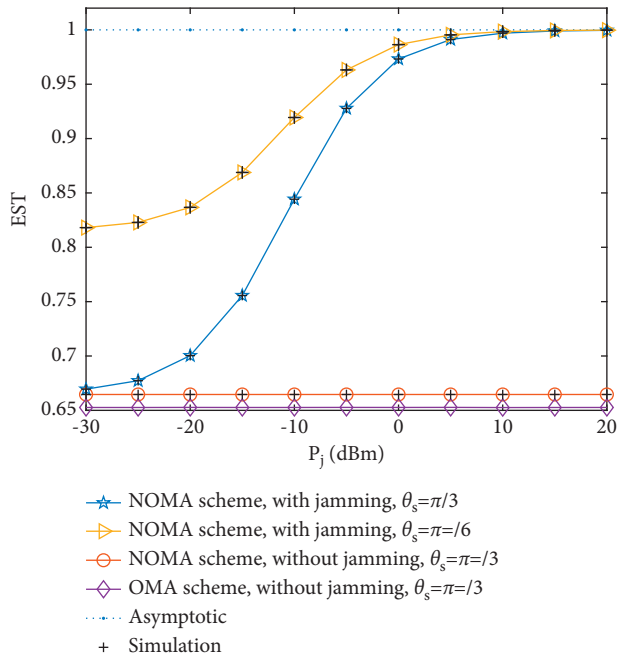

Figure 7: The EST of D_2 versus P_j under different schemes, where $R_1 = 0.6, R_2 = 2, R_s = 1, \alpha_1 = 0.6, P = 0$ dBm.

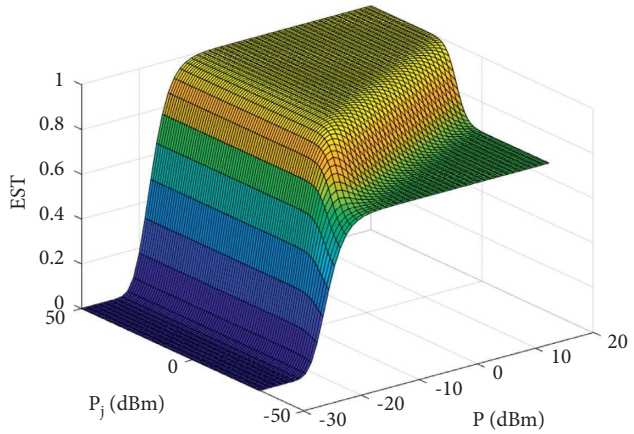

Figure 8: The EST of D_2 versus P and P_j under NOMA scheme with cooperative jamming, where $R_1 = 0.6, R_2 = 2, R_s = 1, \alpha_1 = 0.6$.

6. Conclusion

In this paper, we have studied the downlink mmWave NOMA UAV-assisted relay system in the presence of randomly distributed eavesdroppers and users with different levels of security requirements. The distribution of users and eavesdroppers was characterized as independent HPPPs. Two transmission schemes without or with cooperative jamming were proposed. Based on the two schemes, the COP, SOP, and EST expressions of the users were derived to measure the reliability and security. The simulation results show that the reliability and security performance of NOMA scheme with cooperative jamming outperforms other schemes. However, when the transmitting power of the source and UAV relay is large, SOP depends on the shape of the protected zone and the density of eavesdroppers. With the increase of jamming power, the EST of the cooperative jamming scheme converges to a performance floor, which is independent of the size of the protected zone. In the future, it is worth investigating the performance of the system by exploiting the mobility of UAVs.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China, under Grants 62101560 and

61671465, Natural Science Basic Research Program of Shaanxi, under Grant 2022JQ-619, open research fund of the State Key Laboratory of ISN, under Grant ISN23-04, and National University of Defense Technology Research Fund, under Grant ZK21-44.

References

[1] M. Mozaffari, W. Saad, M. Bennis, Y. H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: applications, challenges, and open problems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2334–2360, 2019.

[2] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2016.

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

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

[5] S. Eom, H. Lee, J. Park, and I. Lee, "UAV-aided wireless communication designs with propulsion energy limitations," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 651–662, 2020.

[6] L. Yang, J. Chen, M. O. Hasna, and H. C. Yang, "Outage performance of UAV-assisted relaying systems with RF energy harvesting," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2471–2474, 2018.

[7] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Communications Letters*, vol. 23, no. 2, pp. 286–289, 2019.

[8] R. Dong, B. Wang, and K. Cao, "Deep learning driven 3D robust beamforming for secure communication of UAV systems," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1643–1647, 2021.

[9] B. Duo, J. Luo, Y. Li, H. Hu, and Z. Wang, "Joint trajectory and power optimization for securing UAV communications against active eavesdropping," *China Communications*, vol. 18, no. 1, pp. 88–99, 2021.

[10] T. Bao, H.-C. Yang, and M. O. Hasna, "Secrecy performance analysis of UAV-assisted relaying communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 1122–1126, 2020.

[11] B. Ji, Y. Li, D. Cao, C. Li, S. Mumtaz, and D. Wang, "Secrecy performance analysis of UAV assisted relay transmission for cognitive network with energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7404–7415, 2020.

[12] H. Lei, D. Wang, K.-H. Park et al., "Safeguarding UAV iot communication systems against randomly located eavesdroppers," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1230–1244, 2020.

[13] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, "Secure UAV-to-UAV systems with spatially random UAVs," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 564–567, 2019.

[14] Z. Xiao, L. Zhu, Y. Liu et al., "A survey on millimeter-wave beamforming enabled UAV communications and networking," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 557–610, 2022.

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

[16] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmwave networks using matérn hardcore point processes," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1397–1409, 2018.

[17] R. Ma, W. Yang, Y. Zhang, J. Liu, and H. Shi, "Secure mmwave communication using UAV-enabled relay and cooperative jammer," *IEEE Access*, vol. 7, Article ID 119729, 2019.

[18] R. Ma, W. Yang, Y. Zhang, and S. Wang, "Secure on-off transmission in UAV relay-assisted mmwave networks," *Applied Sciences*, vol. 9, no. 19, p. 4138, 10 2019.

[19] A. Akbar, S. Jangsher, and F. A. Bhatti, "Noma and 5G emerging technologies: a survey on issues and solution techniques," *Computer Networks*, vol. 190, Article ID 107950, 2021.

[20] T. Hou, Y. Liu, Z. Song, X. Sun, and Y. Chen, "Exploiting NOMA for UAV communications in large-scale cellular networks," *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 6897–6911, 2019.

[21] Y. Liu, Z. Qin, Y. Cai, Y. Gao, G. Y. Li, and A. Nallanathan, "UAV communications based on non-orthogonal multiple access," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 52–57, 2019.

[22] W. Wang, J. Tang, N. Zhao et al., "Joint precoding optimization for secure swipt in UAV-aided NOMA networks," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 5028–5040, 2020.

[23] Y. . Chen, Z. Zhang, and B. Li, "Enhancing physical layer security via a UA V friendly jammer for NOMA-based IoT systems with imperfect CSI," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 3, Article ID e4175, 2021.

[24] H.-M. Wang and X. Zhang, "UAV secure downlink NOMA transmissions: a secure users oriented perspective," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5732–5746, 2020.

[25] X. Pang, J. Tang, N. Zhao, X. Zhang, and Y. Qian, "Energy-efficient design for mmwave-enabled NOMA-UAV networks," *Science China Information Sciences*, vol. 64, Article ID 140303, 2021.

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

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

[28] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[29] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, 2017.

[30] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-s. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 721–742, 2017.

[31] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5747–5763, 2020.

[32] Diao, B. Wang, K. Cao, R. Dong, and T. Cheng, "Enhancing reliability and security of UAV-enabled NOMA communications with power allocation and aerial jamming," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 8, pp. 8662–8674, 2022.

[33] Q. Wang, X. Li, S. Bhatia et al., "UAV-enabled non-orthogonal multiple access networks for ground-air-ground communications," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1340–1354, 2022.

[34] X. Pang, M. Liu, N. Zhao, Y. Chen, Y. Li, and F. R. Yu, "Secrecy analysis of UAV-based mmwave relaying networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 8, pp. 4990–5002, 2021.

[35] X. Sun, W. Yang, and Y. Cai, "Secure communication in NOMA-assisted millimeter-wave swipt UAV networks," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1884–1897, 2020.

[36] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6010–6023, 2016.

[37] K. Janghel and S. Prakriya, "Performance of adaptive oma/cooperative-NOMA scheme with user selection," *IEEE Communications Letters*, vol. 22, no. 10, pp. 2092–2095, 2018.

[38] R. I. Bor-Yaliniz, A. El-Keyi, and H. Yanikomeroglu, "Efficient 3-D placement of an aerial base station in next generation cellular networks," in *Proceedings of the 2016 IEEE International Conference on Communications (ICC)*, pp. 1–5, Kuala Lumpur, Malaysia, May 2016.

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

[40] K. Cao, B. Wang, H. Ding et al., "Improving physical layer security of uplink NOMA via energy harvesting jammers," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 786–799, 2021.

[41] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1319–1329, 2017.

[42] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in af multi-antenna multi-relay networks," *IEEE Transactions on Signal Processing*, vol. 63, no. 1, pp. 206–220, 2015.

[43] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[44] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.

[45] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, Cambridge, Massachusetts, USA, 2007.