Security Enhancement for NOMA-UAV Networks

***Abstract*—Owing to its distinctive merits, non-orthogonal multiple access (NOMA) techniques have been utilized in unmanned aerial vehicle (UAV) enabled wireless base stations to provide effective coverage for terrestrial users. However, the security of NOMA-UAV systems remains a challenge due to the line-of-sight air-to-ground channels and higher transmission power of weaker users in NOMA. In this paper, we propose two schemes to guarantee the secure transmission in UAV-NOMA networks. When only one user requires secure transmission, we derive the hovering position for the UAV and the power allocation to meet rate threshold of the secure user while maximizing the sum rate of remaining users. This disrupts the eavesdropping towards the secure user effectively. When multiple users require secure transmission, we further take the advantage of beamforming via multiple antennas at the UAV to guarantee their secure transmission. Due to the non-convexity of this problem, we convert it into a convex one for an iterative solution by using the second order cone programming. Finally, simulation results are provided to show the effectiveness of the proposed scheme.**

***Index Terms*—Beamforming optimization, non-orthogonal multiple access, physical layer security, power allocation, unmanned aerial vehicle.**

I. Introduction

Unmanned aerial vehicles (UAVs) could be used as a platform to provide cost-effective wireless communications for terrestrial users [2]–[4]. Under these solutions, the unobstructed air-to-ground channels can be modeled as high-quality line-of-sight (LoS) links [5]. Meanwhile, due to their flexibility and mobility, UAV-based transmitters have a wider wireless coverage in both urban and rural areas [6], [7]. Thus, recent research advances have made it possible to improve the performance of UAV networks significantly [8]–[16]. In [8], Zeng *et al*. exploited a mobile relay mounted on the UAV to maximize the network throughput via optimizing the transmit power and the trajectory of the UAV relay. A novel sense-and-send scheme for cooperative UAVs was designed by Zhang *et al*. to enable the UAV-to-X transmission in [9], with the sub-channel allocation and the UAV speed jointly optimized to maximize the sum rate. In [10], Fan *et al*. proposed a UAV relaying network, in which the transmit power, bandwidth, rate and the location of the UAV were jointly optimized to maximize the network throughput. The transceiver was designed and the multihop device-to-device links were established by Liu *et al*. in [11], to guarantee the reliable transmission with extended coverage in disasters. In [12], Zhang *et al*. optimized the trajectory of UAV to minimize its mission completion time in cellular-connected UAV networks. Zeng *et al*. proposed an effective algorithm to jointly optimize the hovering locations, durations and flying trajectory in [13], to minimize the energy consumption of the UAVs. In [14], Zhang *et al*. proposed an effective scheme to minimize the energy consumption in UAV-assisted mobile edge computing systems. In [15], Yang *et al*. made a fundamental energy tradeoff in UAV wireless networks by considering both the circular and straight trajectories. Tang *et al*. proposed a channel assignment algorithm in the wireless network combining both UAV and D2D [16]. However, the high-quality LoS links make the information easily to be eavesdropped in UAV communications [17]–[20]. In [18], the trajectory and scheduling were jointly optimized in a dual-UAV network by Cai *et al*., to guarantee the secure transmission for ground users effectively. In [19], the secure transmission of the UAV relaying system was ensured by Cheng *et al.* via the edge caching and trajectory optimization. Xiao *et al*. maximized the secrecy energy efficiency of the UAV relay with the uncertain location of eavesdropper considered in [20].

On the other hand, non-orthogonal multiple access (NOMA) is becoming an important technique for future wireless networks, due to its low latency, high reliability, massive connectivity and high throughput [21]–[23]. In the power-domain NOMA scheme, the base station (BS) performs power allocation (PA) according to the quality of channels [24]. Then, the high-power signals from other NOMA users can be decoded and removed by successive interference cancellation (SIC) at each user before decoding its own. Due to its superior performance, NOMA has received great attention in both academia and industry [25]–[28]. In [25], Cui *et al*. proposed a PA scheme for downlink NOMA networks under outage constraints with a single antenna at the BS. The performance of capacity and sum rate in NOMA relaying systems with massive multiple-input multiple-output (MIMO)

Manuscript received September 22, 2019; revised December 3, 2019; accepted February 5, 2020. The work was supported by the National Natural Science Foundation of China (NSFC) under Grant 61871065, 61871455 and 61871348. Part of this work is published in preliminary form in the Proceedings of IEEE VTC'19-Spring [1]. The associate editor coordinating the review of this paper and approving it for publication was F. Tang. *(Corresponding author: Jingjing Wang.)*

was analyzed by Zhang *et al.* in [26]. In [27], the PA and time switching control were jointly optimized by Tang *et al.* to effectively maximize the energy efficiency in NOMA networks with simultaneous wireless information and power transfer. Two effective relay selection schemes for cooperative downlink NOMA networks were proposed by Xu *et al.* in [28]. However, the security in NOMA networks is greatly threatened due to the higher transmit power for the weaker users, which makes the information for these users easy to be eavesdropped [29]. Some preliminary works have been done to improve the security of NOMA [30]–[32]. In [30], Li *et al*. optimized the PA and beamforming to maximize the sum secrecy rate of central users in downlink multiple-input single-output (MISO) NOMA networks. The privacy of a specific user was guaranteed by Cao *et al*. via joint beamforming optimization at the BS to prevent eavesdropping inside the NOMA network [31]. In [32], Zheng *et al*. proposed to exploit the artificial noise and full duplex relay to ensure the secure transmission for NOMA networks with two-way relaying in the presence of eavesdroppers. In [33], artificial jamming was generated together with the NOMA information by the BS via beamforming optimization to disrupt the adversarial eavesdropping without affecting the legitimate transmission.

To leverage the advantages of both techniques, UAV and NOMA have been combined [34]–[38]. In [34], some fundamental work was done by Liu *et al*. to establish a novel framework of UAV communications based on NOMA. In [35], Liu *et al*. proposed a multi-objective resource allocation scheme in UAV-assisted networks for disasters. A novel UAV-aided NOMA scheme was proposed by Hou *et al*. in [36] to provide wireless transmission for ground users. In [37], Zhao *et al*. proposed a UAV-aided NOMA scheme, and the sum rate can be maximized by jointly optimizing the precoding of NOMA at BS and the UAV trajectory. NOMA was applied to cellular-connected UAV networks by Mei and Zhang in [38], to avoid severe uplink interference from the UAV to cellular BSs. Nevertheless, the security of NOMA-UAV networks is largely ignored in the existing works. Thus, in this paper, we propose two schemes to enhance the security of NOMA-UAV networks via PA and beamforming optimization, respectively. The main motivations and contributions of this paper can be summarized as follows.

- In NOMA-UAV wireless networks, the security remains as a challenging issue, due to the LoS air-to-ground links and higher transmit power of weaker users in NOMA. To the best of our knowledge, this important aspect has been largely ignored in existing research. Thus, in this paper, we propose two schemes via PA and beamforming to improve the performance of secure transmission for NOMA-UAV networks.
- First, we assume that one of the ground users requires secure transmission from the single-antenna UAV. The optimal location of the UAV is derived and the optimal PA among users is performed at the UAV to guarantee the security of the private user. The PA optimization problem is converted into convex ones, and its closed-form solution is derived.

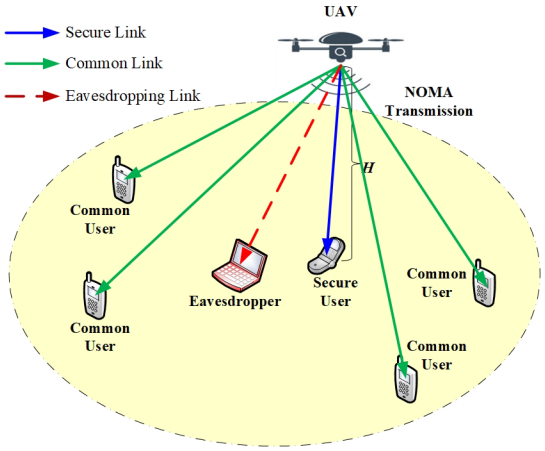

Fig. 1. A NOMA-UAV network with one secure user, several common users and one eavesdropper.

- Then, we consider the case when multiple users require secure transmission simultaneously. We fully exploit the antenna resource at the UAV, and perform beamforming optimization to guarantee the secure transmission for these users in NOMA-UAV networks. The problem is non-convex, and we use the first-order Taylor expansion to transform it into a second-order cone programming (SOCP) problem, which can be solved by iteratively.

The rest of this paper is organized as follows. In Section II, the system model is presented. The secure transmission scheme for single-antenna NOMA-UAV networks is proposed in Section III. In Section IV, the beamforming optimization at the UAV for multiple secure users is studied. Simulation results are discussed in Section V, followed by the conclusion in Section VI.

Notation: $\|\mathbf{h}\|$ and $\mathbf{h}^{\dagger}$ denote the Euclidean norm and Hermitian transpose of $\mathbf{h}$. $\mathbb{C}^{M\times N}$ is the space of $M \times N$ complex matrices. $\mathcal{CN}(\mathbf{h}, \mathbf{H})$ is the complex Gaussian distribution with mean $\mathbf{h}$ and covariance $\mathbf{H}$. $Re(a)$ represents the real part of a complex number a.

II. System Model

Consider the downlink transmission in a NOMA wireless network as shown in Fig. 1, where a UAV serves K single-antenna ground users. There exists a ground eavesdropper aiming to intercept the private information of a specific user. Denote the ith user as U_i, $i = 1, ..., K$. U_s is assumed to be the secure user that requires privacy from the UAV, while the other users only require the public information. Define d_i as the distance between the UAV and U_i. Without loss of generality, we assume that

$$d_1 \leq d_2 \leq ... \leq d_K. \tag{1}$$

NOMA is adopted to send the superimposed information to the K users. The transmitted signal by the UAV can be expressed as

$$x = \sum_{i=1}^{K} \sqrt{p_i} s_i, \tag{2}$$

where p_i represents the transmit power of U_i, satisfying

$$\sum_{i=1}^{K} p_i = P_{sum}, \tag{3}$$

and s_i is the information for U_i with $\mathbb{E}\left\{|s_i|^2\right\} = 1$. The received signal at U_i can be expressed as

$$y_i = h_i\sqrt{p_i}s_i + \sum_{j=1,j\neq i}^{K} h_i\sqrt{p_j}s_j + n_i, \tag{4}$$

where $h_i = \sqrt{\rho d_i^{-\alpha}}$ represents the channel coefficient from the UAV to U_i in LoS, $n_i \sim \mathcal{CN}(0, \sigma_i^2)$ is the additive white Gaussian noise (AWGN) at U_i with zero mean and variance σ_i^2, ρ is a parameter of channel gain at the reference distance $d_0 = 1$ m, and d_i is the distance between the UAV and U_i. α is the path-loss exponent, which is equal to 2 due to the air-to-ground LoS channels.

According to NOMA, the decoding order is related to the distance, i.e., the information of farther users from the UAV should be first decoded. Before decoding the message of U_s, we adopt SIC to decode and eliminate the information from U_{s+1} to U_K, and the received signal-to-interference-plus-noise-ratio (SINR) at U_s can be denoted as

$$\text{SINR}_s^s = \frac{h_s^2 p_s}{h_s^2 \sum\limits_{m=1}^{s-1} p_m + \sigma^2}. \tag{5}$$

Thus, the transmission rate of U_s can be written as

$$R_t^s = \log_2\left(1 + \text{SINR}_s^s\right). \tag{6}$$

The eavesdropping SINR towards U_s at the eavesdropper can be expressed as

$$\text{SINR}_e^s = \frac{h_e^2 p_s}{h_e^2 \sum\limits_{i=1,i\neq s}^{K} p_i + \sigma^2}, \tag{7}$$

where h_e indicates the channel power gain between the UAV and the eavesdropper. Thus, the eavesdropping rate can be denoted as

$$R_e^s = \log_2\left(1 + \text{SINR}_e^s\right). \tag{8}$$

Accordingly, the secrecy rate of U_j can be given by

$$R_s^s = \left(R_t^s - R_e^s\right)^+, \tag{9}$$

where $(.)^+$ means that if $R_t^s > R_e^s$, $R_s^s = R_t^s - R_e^s$, otherwise, $R_s^s = 0$.

From (7) and (9), we can conclude that when U_s is far away from the UAV, its transmit power is quite high and it is easy to be eavesdropped. Therefore, a PA scheme is proposed in the next section to guarantee the secure transmission of U_s while satisfying the QoS requirements of other users.

III. Secure Transmission for Single-Antenna NOMA-UAV Networks

In this section, the hovering position of UAV is discussed and the PA is optimized to guarantee the security for the secure user. Then, the case of two secure users in the network is briefly discussed.

A. A Single Secure User

According to NOMA, farther users from the UAV will be allocated with higher transmit power, and hence their security is in danger. Thus, the UAV should just hover above the secure user to minimize its transmit power when there is only one user requires private transmission.

Proposition 1: In order to minimize the transmit power for the secure user U_s, the UAV should hover above it.

Proof: According to (7), in order to minimize the eavesdropping SINR towards U_s, p_s should be minimized and $\sum_{i=1,i\neq s}^{K} p_i$ should be maximized. According to NOMA, U_s should be nearer from the UAV than other users. Thus, in this case, the secure user can be defined as U_1, i.e., $U_1 \triangleq U_s$. Assume that the horizontal position of the UAV is $\mathbf{Q}_0(x_0, y_0)$, and the location of U_1 is $\mathbf{W}_1(x_1, y_1)$. Hence, the channel coefficient between them can be denoted as

$$h_1 = \sqrt{\frac{\rho}{H^2 + \|\mathbf{Q}_0 - \mathbf{W}_1\|^2}}, \tag{10}$$

where H represents the height of UAV. Accordingly, the transmission rate of U_1 can be expressed as

$$R_1 = \log_2\left(1 + \frac{h_1^2 p_1}{\sigma^2}\right) \geq r_1, \tag{11}$$

where r_1 is the threshold of achievable rate. From (11), we have

$$p_1 \geq \frac{(2^{r_1} - 1)\sigma^2}{h_1^2}. \tag{12}$$

Obviously, p_1 can achieve the minimum value when h_1^2 is maximum. In this case, according to (10), the denominator should take the minimum value, i.e., $\mathbf{Q}_0 = \mathbf{W}_1$. Hence, it can be concluded that the UAV should hover above U_1 to minimize its transmit power. ■

Thus, we assume that U_1 is the secure user with (13) and (14) limited to $\sum_{i=1}^{K} p_i = P_{sum}$.

$$h_1 \geq h_2 \geq ... \geq h_K. \tag{13}$$

$$0 \leq p_1 \leq p_2 \leq ... \leq p_K. \tag{14}$$

To maximize the sum rate of other users while guaranteeing the secure transmission of U_1, the optimization problem can be formulated as

$$\max_{p_2,p_3,...,p_K} \sum_{i=2}^{K} R_i \tag{15a}$$

$$s.t. \quad R_i \geq r_i, i = 1, ..., K, \tag{15b}$$

$$0 \leq p_1 \leq p_2 \leq ... \leq p_K, \tag{15c}$$

$$\sum_{i=1}^{K} p_i = P_{sum}, \tag{15d}$$

with $p_1 = \frac{(2^{r_1}-1)\sigma^2}{h_1^2}$.

To determine whether (15) is convex, we first define α_i as

$$\alpha_i = \frac{h_i^2}{\sigma^2}, \tag{16}$$

and R_i can be transformed into

$$\begin{aligned} R_i &= \log_2\left(1+\frac{h_i^2 p_i}{|h_i|^2\sum_{j=1}^{i-1}p_j+\sigma^2}\right) \\ &= \log_2\left(1+\frac{\alpha_i p_i}{\alpha_i\sum_{j=1}^{i-1}p_j+1}\right). \end{aligned} \tag{17}$$

Then, we define

$$q_i = \sum_{j=1}^{i} p_i, i = 1, 2, ..., K, \tag{18}$$

$$q_K = P_{sum}. \tag{19}$$

It can be derived that

$$p_i = q_i - q_{i-1}, i = 2, ..., K, \tag{20}$$

and (17) can be further written as

$$\begin{aligned} R_i &= \log_2\left(1+\frac{\alpha_i(q_i-q_{i-1})}{\alpha_i q_{i-1}+1}\right) \\ &= \log_2\left(\frac{1+\alpha_i q_i}{1+\alpha_i q_{i-1}}\right) \\ &= \log_2\left(1+\alpha_i q_i\right) - \log_2(1+\alpha_i q_{i-1}). \end{aligned} \tag{21}$$

Thus, the condition (15b) can be changed into

$$R_i = \log_2\frac{1+\alpha_i q_i}{1+\alpha_i q_{i-1}} \geq r_i, \tag{22}$$

$$\Rightarrow \frac{1+\alpha_i q_i}{1+\alpha_i q_{i-1}} \geq 2^{r_i} = \frac{1}{\eta_i}, \tag{23}$$

$$\Rightarrow \eta_i + \eta_i\alpha_i q_i \geq 1 + \alpha_i q_{i-1}, \tag{24}$$

$$\Rightarrow q_{i-1} \leq \frac{\eta_i - 1}{\alpha_i} + \eta_i q_i, \tag{25}$$

$$\Rightarrow q_{i-1} \leq \eta_i q_i - \beta_i, \tag{26}$$

for $i = 2, ..., K$, where η_i and β_i satisfy

$$\eta_i = 2^{-r_i}, \tag{27}$$

$$\beta_i = \frac{1-\eta_i}{\alpha_i}. \tag{28}$$

Similarly, $0 \leq p_1 \leq p_2 \leq ... \leq p_K$ is equivalent to $q_2 - q_1 \leq q_3 - q_2 \leq ... \leq q_K - q_{K-1}$.

Define $f_1(q_1)$ and $f_i(q_i)$ as

$$f_1(q_1) = \log_2(1+\alpha_1 q_1), i = 1, \tag{29}$$

$$f_i(q_i) = \log_2\frac{1+\alpha_i q_i}{1+\alpha_{i-1} q_i}, i = 2, ..., K, \tag{30}$$

and the sum rate of common users can be expressed as

$$\sum_{i=2}^{K} R_i = \sum_{i=2}^{K} f_i(q_i). \tag{31}$$

Thus, the problem (15) can be changed into

$$\begin{aligned} \max_{q_i}\ & \sum_{i=2}^{K} f_i(q_i) \\ s.t.\ & q_{i-1} \leq \eta_i q_i - \beta_i,\ i = 2, ..., K-1, \\ & q_2 - q_1 \leq q_3 - q_2 \leq ... \leq q_K - q_{K-1}, \\ & q_1 = p_1, \\ & q_K = P_{sum}. \end{aligned} \tag{32}$$

Lemma 1: The problem (32) is convex.

Proof: The first-order derivative of $f_i(q_i)$, for $i = 1, ..., K$, can be expressed as

$$f_i'(q_i) = \begin{cases} \dfrac{1}{\ln 2\left(\frac{1}{\alpha_1}+q_1\right)}, & i = 1, \\ \dfrac{\frac{1}{\alpha_{i-1}} - \frac{1}{\alpha_1}}{\ln 2\left(\frac{1}{\alpha_i}+q_i\right)\left(\frac{1}{\alpha_{i-1}}+q_i\right)}, & i = 2, ..., K. \end{cases} \tag{33}$$

Since $\alpha_i \geq \alpha_{i-1} \geq 0$ and $q_i \geq 0$, we have $f_i'(q_i) \geq 0$, for $i = 1, 2, ..., K$.

The second-order derivative of $f_i(q_i)$ can be derived as

$$f_i''(q_i) = \begin{cases} -\dfrac{1}{\ln 2\left(\frac{1}{\alpha_1}+q_1\right)^2}, & i = 1, \\ \dfrac{\left(\frac{1}{\alpha_i}+q_i\right)^2 - \left(\frac{1}{\alpha_{i-1}}+q_i\right)^2}{\ln 2\left(\frac{1}{\alpha_i-1}+q_i\right)^2\left(\frac{1}{\alpha_i}+q_i\right)^2}, & i = 2, ..., K. \end{cases} \tag{34}$$

Obviously, we have $f_i''(q_i) \leq 0$. As a result, all the conditions in (32) are linear. Thus, the problem (32) is convex. ■

Based on Lemma 1, we can derive the solution to the PA problem in (32) by Proposition 2.

Proposition 2: The solution to (15) can be obtained as

$$\hat{p}_i = \begin{cases} p_1, & i = 1, \\ (1-\eta_i)\hat{q}_i + \beta_i, & i = 2, ..., K-1, \\ P_{sum} - p_1 - ... - p_{K-1}, & i = K. \end{cases} \tag{35}$$

Proof: According to (26), when $i = 2, ..., K-1$, we can conclude that

$$q_i \leq \eta_{i+1}\hat{q}_{i+1} - \beta_{i+1}, i = 2, ..., K-1. \tag{36}$$

By means of (18), when $i = 1$, we have $q_1 = p_1$. Similarly, when $i = K$, $q_K = P_{sum}$. As a result, we can obtain the solution to (32) as

$$\hat{q}_i = \begin{cases} p_1, & i = 1, \\ \eta_{i+1}\hat{q}_{i+1} - \beta_{i+1}, & i = 2, ..., K-1, \\ P_{sum}, & i = K. \end{cases} \tag{37}$$

Due to $p_i = q_i - q_{i-1}$, the solution to (15) can be expressed as (35). ■

Based on (35), the transmission rate of U_1 can be calculated as

$$R_t^1 = \log_2\left(1+\text{SINR}_1^1\right) = \log_2\left(1+\frac{h_1^2 p_1}{\sigma^2}\right). \tag{38}$$

Assume that the position of eavesdropper is $\mathbf{E}_e(x_e, y_e)$, and the eavesdropping channel can be expressed as $h_e = \sqrt{\rho d_e^{-\alpha}}$, where d_e is the distance between the UAV and eavesdropper. We have the channel coefficient from the UAV to the eavesdropper as

$$h_e = \frac{\rho_0}{\sqrt{H^2 + \|\mathbf{Q}_0 - \mathbf{E}_e\|^2}}. \tag{39}$$

Thus, the eavesdropping SINR towards the secure user U_1 can be expressed as

$$\text{SINR}_e^1 = \frac{h_e^2 p_1}{h_e^2 \sum\limits_{i=2}^{K} p_i + \sigma^2}. \tag{40}$$

Accordingly, we can derive the eavesdropping rate towards U_1 as

$$R_e^1 = \log_2\left(1 + \frac{h_e^2 p_1}{h_e^2 \sum_{i=2}^{K} p_i + \sigma^2}\right). \tag{41}$$

Based on (38) and (41), we can obtain the secrecy rate of U_1 as

$$\begin{aligned} R_s^1 &= R_t^1 - R_e^1 \\ &= \log_2\left(1+\frac{h_1^2 p_1}{\sigma^2}\right) - \log_2\left(1+\frac{h_e^2 p_1}{h_e^2 \sum_{i=2}^{K} p_i + \sigma^2}\right). \end{aligned} \tag{42}$$

Remark 1: From (41), we can conclude that R_e^1 is close to 0, because $p_2, ..., p_K$ are much higher than p_1. In other words, the signal of U_1 can be hidden in the high-power signals of other users to guarantee its secure transmission.

B. Two Secure Users

We assume that two users, U_m and U_n, both require secure transmission, with their coordinates as $\mathbf{W}_m(x_m, y_m)$ and $\mathbf{W}_n(x_n, y_n)$. U_m has a higher secure priority than U_n. Without loss of generality, we assume

$$d_1 < ... < d_m < ... < d_n < ... < d_K. \tag{43}$$

To guarantee the secure transmission, the eavesdropping rate towards them should be as low as possible. Thus, we should maximize the sum rate of other common users while guaranteeing the QoS requirements of secure users. The problem can be expressed as

$$\begin{aligned} \max_{p_1,p_2,...p_K} \quad & \sum_{i=1, i\neq m, i\neq n}^{K} R_i \\ s.t. \quad & R_i \geq r_i, i = 1, ..., K, \\ & 0 < p_1 <, ..., < p_m <, ..., < p_n <, ..., < p_K, \\ & \sum_{i=1}^{K} p_i = P_{sum}. \end{aligned} \tag{44}$$

When the secure users U_m and U_n are close to each other compared with common users, e.g., $U_m = U_1$, $U_n = U_2$, (44) can be solved in the same way as (15). The transmission rate of U_1 and U_2 can be expressed as

$$\begin{aligned} R_1 &= \log_2\left(1 + \frac{h_1^2 p_1}{\sigma^2}\right) \geq r_1, \\ R_2 &= \log_2\left(1 + \frac{h_2^2 p_2}{h_2^2 p_1 + \sigma^2}\right) \geq r_2. \end{aligned} \tag{45}$$

Thus, p_1 and p_2 can be calculated as

$$\begin{aligned} p_1 &= \frac{(2^{r_1} - 1)\sigma^2}{h_1^2}, \\ p_2 &= \frac{(2^{r_2} - 1)(h_2^2 p_1 + \sigma^2)}{h_2^2}. \end{aligned} \tag{46}$$

Accordingly, the solution to (44) is similar to (15), and we have

$$p_i = \begin{cases} p_1, & i = 1, \\ p_2, & i = 2, \\ (1 - \eta_i) q_i + \beta_i, & i = 3, ..., K. \end{cases} \tag{47}$$

However, when U_1 and U_2 are not next to each other, it is difficult to satisfy

$$\max(d_1, d_2) < \max(d_3, ..., d_K), \tag{48}$$

no matter where the UAV hovers. Thus, (44) has no solution in this case.

In addition, if there are more than three secure users, it becomes even more difficult to solve (44) with a single antenna at the UAV. Thus, we will solve the secure transmission problem with several secure users by exploiting multiple antennas at the UAV in the following section.

IV. Beamforming Optimization for Multiple Secure Users

In this section, we take advantage of multiple antennas at UAV via beamforming to improve the secure performance of these users, where a UAV with M antennas transmits information to K single-antenna users.

A. Problem Formulation

We assume that there exist S secure users, i.e., $U_1, ..., U_S$, and $U_{S+1}, ..., U_K$ are common ones. Without loss of generality, we define the distance for the secure users as

$$d_1 \leq d_2 \leq ... \leq d_S, \tag{49}$$

and the distance for the common users as

$$d_{S+1} \leq d_{S+2} \leq ... \leq d_K. \tag{50}$$

The security priority is $U_1 > U_2 > ... > U_S$.

The transmitted signal by the UAV can be expressed as

$$\mathbf{x} = \sum_{i=1}^{K} \mathbf{v}_i s_i, \tag{51}$$

where $\mathbf{v}_i \in \mathbb{C}^{M\times 1}$ is the precoding vector for U_i, with $\|\mathbf{v}_i\|^2 = p_i, i = 1, ..., K$.

Thus, the received signal at U_i can be denoted as

$$y_i = \mathbf{h}_i^\dagger \mathbf{v}_i s_i + \sum_{j\neq i}^{K} \mathbf{h}_i^\dagger \mathbf{v}_j s_i + n_i, i = 1, ..., K, \tag{52}$$

where $\mathbf{h}_i = \sqrt{\rho d_i^{-\alpha}}\ \mathbf{g}_i \in \mathbb{C}^{M\times 1}$ is the channel gain vector from the UAV to U_i, and $\mathbf{g}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ represents the corresponding Rayleigh fading vector. The channel vector from the UAV to the eavesdropper can be expressed as

$$\mathbf{h}_e = \sqrt{\frac{\rho}{H^2 + \|\mathbf{Q} - \mathbf{E}\|^2}}\mathbf{g}_e, \tag{53}$$

where $\mathbf{g}_e \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is the corresponding Rayleigh fading vector from the UAV to the eavesdropper.

Due to the existence of S secure users, the decoding order should be expressed as $K \to \cdots \to S \to \cdots \to 2 \to 1$. Accordingly, the PA constraints should follow

$$\begin{cases} \left|\mathbf{h}_1^\dagger \mathbf{v}_1\right|^2 \le \left|\mathbf{h}_1^\dagger \mathbf{v}_2\right|^2 ... \le \left|\mathbf{h}_1^\dagger \mathbf{v}_S\right|^2 ... \le \left|\mathbf{h}_1^\dagger \mathbf{v}_K\right|^2, \\ ..... \\ \left|\mathbf{h}_S^\dagger \mathbf{v}_1\right|^2 \le \left|\mathbf{h}_S^\dagger \mathbf{v}_2\right|^2 ... \le \left|\mathbf{h}_S^\dagger \mathbf{v}_S\right|^2 ... \le \left|\mathbf{h}_S^\dagger \mathbf{v}_K\right|^2, \\ \left|\mathbf{h}_{S+1}^\dagger \mathbf{v}_1\right|^2 \le \left|\mathbf{h}_{S+1}^\dagger \mathbf{v}_2\right|^2 ... \le \left|\mathbf{h}_{S+1}^\dagger \mathbf{v}_S\right|^2 ... \le \left|\mathbf{h}_{S+1}^\dagger \mathbf{v}_K\right|^2, \\ ..... \\ \left|\mathbf{h}_K^\dagger \mathbf{v}_1\right|^2 \le \left|\mathbf{h}_K^\dagger \mathbf{v}_2\right|^2 ... \le \left|\mathbf{h}_K^\dagger \mathbf{v}_S\right|^2 ... \le \left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2, \end{cases} \tag{54}$$

which is beneficial to improve the SINR and fulfill the desired decoding order at NOMA users.

Thus, according to NOMA, the achievable SINR to decode the signal for U_i at U_j can be denoted as

$$\text{SINR}_j^i = \frac{\left|\mathbf{h}_j^\dagger \mathbf{v}_i\right|^2}{\sum\limits_{m=1}^{i-1} \left|\mathbf{h}_j^\dagger \mathbf{v}_m\right|^2 + \sigma^2}, \quad j \le i. \tag{55}$$

In order to protect the privacy of secure users, we should maximize the sum rate of common users with the rate thresholds of secure users guaranteed. Thus, the low-power signals of the secure users can be hidden in the signals of other common users with higher power. The optimization problem can be expressed as

$$\begin{aligned} \max_{\mathbf{v}_i} \quad & \sum_{i=S+1}^{K} R_t^i \\ s.t. \quad & R_t^j \ge r_j, j = 1, 2, ..., K, \\ & \sum_{i=1}^{K} \|\mathbf{v}_i\|^2 \le P_{sum} \text{ and (54)}, \end{aligned} \tag{56}$$

where r_j represents the threshold of transmission rate for U_j, and P_{sum} is the total transmit power. The transmission rate for U_j can be denoted as

$$R_t^j = \log_2\left(1 + \min\left(\text{SINR}_b^j\right)\right), \quad b \le j. \tag{57}$$

B. Approximate Transformations

Due to the fact that (56) is non-convex, we need to convert it into a convex one before solving it. We first introduce auxiliary variables $t_w, w = S+1, S+2, ..., K$. Thus, the optimization problem (56) can be converted to

$$\max_{\mathbf{v}_i, t_w} \quad \log_2(t_{S+1} t_{S+2} ... t_K) \tag{58a}$$

$$s.t. \ 1 + \min\{\text{SINR}_a^w, \text{SINR}_w^w\} \ge t_w, a = 1, 2, ..., w-1, \tag{58b}$$

$$R_t^j \ge r_j, j = 1, 2, ..., K, \tag{58c}$$

$$\sum_{i=1}^{K} \|\mathbf{v}_i\|^2 \le P_{sum} \text{ and (54)}. \tag{58d}$$

The logarithmic function in (58a) is non-decreasing, and it is equivalent to maximize $\left(\prod\limits_{w=S+1}^{K} t_w\right)^{\frac{1}{K}}$, which is convex, increasing, and easy to solve. Thus, the convex problem (58) can be changed into

$$\max_{\mathbf{v}_i, t_w} \quad \left(\prod_{w=S+1}^{K} t_w\right)^{\frac{1}{K}} \tag{59a}$$

$$s.t. \ \sum_{m=1}^{w-1} |\mathbf{h}_a^\dagger \mathbf{v}_m|^2 + \sigma^2 \le \frac{|\mathbf{h}_a^\dagger \mathbf{v}_w|^2}{t_w - 1}, \tag{59b}$$

$$w = S+1, ..., K, \ a = 1, ..., w-1,$$

$$\sum_{m=1}^{w-1} |\mathbf{h}_w^\dagger \mathbf{v}_m|^2 + \sigma^2 \le \frac{|\mathbf{h}_w^\dagger \mathbf{v}_w|^2}{t_w - 1}, \tag{59c}$$

$$\sum_{m=1}^{j-1} |\mathbf{h}_j^\dagger \mathbf{v}_m|^2 + \sigma^2 \le \frac{|\mathbf{h}_j^\dagger \mathbf{v}_j|^2}{2^{r_j} - 1}, \ j = 1, 2, ..., K, \tag{59d}$$

$$\sum_{i=1}^{K} \|\mathbf{v}_i\|^2 \le P_{sum} \text{ and (54)}. \tag{59e}$$

We can observe that the objective function (59a) is convex with t_w. However, the constraints are not convex except the last one. Thus, it needs to be further transformed into a convex one.

Proposition 3: Define expressions of $\mathbf{v}_w$ and t_w as

$$F_1(\mathbf{v}_w, t_w) = \frac{\left|\mathbf{h}_a^\dagger \mathbf{v}_w\right|^2}{t_w - 1}, \ w = S+1, S+2, ..., K, \tag{60a}$$

$$F_2(\mathbf{v}_u) = \frac{\left|\mathbf{h}_u^\dagger \mathbf{v}_u\right|^2}{2^{r_u} - 1}, \ u = 1, ..., K. \tag{60b}$$

The relationship between the above two functions and their approximate functions at certain points of $(\overline{\mathbf{v}}_w, \overline{t}_w)$ and $\overline{\mathbf{v}}_u$ can be denoted as (61a) and (61b), respectively.

$$F_1(\mathbf{v}_w, t_w) \ge \mathcal{L}_1(\mathbf{v}_w, t_w, \overline{\mathbf{v}}_w, \overline{t}_w), \tag{61a}$$

$$F_2(\mathbf{v}_u) \ge \mathcal{L}_2(\mathbf{v}_u, \overline{\mathbf{v}}_u). \tag{61b}$$

The Taylor approximate expansions of the above two functions at these points can be expressed as

$$\begin{aligned} \mathcal{L}_1(\mathbf{v}_w, t_w, \overline{\mathbf{v}}_w, \overline{t}_w) = & \frac{2Re\left(\mathbf{h}_a^\dagger \mathbf{v}_w \overline{\mathbf{v}}_w^\dagger \mathbf{h}_a\right)}{\overline{t}_w - 1} \\ & - \frac{Re\left(\mathbf{h}_a^\dagger \overline{\mathbf{v}}_w \overline{\mathbf{v}}_w^\dagger \mathbf{h}_a\right)}{(\overline{t}_w - 1)^2}(t_w - 1), \end{aligned} \tag{62a}$$

$$\mathcal{L}_2(\mathbf{v}_u, \overline{\mathbf{v}}_u) = \frac{2Re\left(\mathbf{h}_u^\dagger \mathbf{v}_u \overline{\mathbf{v}}_u^\dagger \mathbf{h}_u\right) - Re\left(\mathbf{h}_u^\dagger \overline{\mathbf{v}}_u \overline{\mathbf{v}}_u^\dagger \mathbf{h}_u\right)}{2^{r_u} - 1}. \tag{62b}$$

Proof: (60a) is a convex function of $\mathbf{v}_w$ and t_w. Thus, applying the first order Taylor expansion at $(\overline{\mathbf{v}}_w, \overline{t}_w)$, we can derive

$$\begin{aligned} F_1(\mathbf{v}_w, t_w) \ge & F_1\left(\overline{\mathbf{v}}_w, \overline{t}_w\right) + \frac{\partial F_1\left(\overline{\mathbf{v}}_w, \overline{t}_w\right)}{\partial t_w}\left(t_w - \overline{t}_w\right) \\ & + 2Re\left\{\frac{\partial F_1\left(\overline{\mathbf{v}}_w, \overline{t}_w\right)}{\partial \mathbf{v}_w}\left(\mathbf{v}_w - \overline{\mathbf{v}}_w\right)\right\} \\ = & \frac{2Re\left(\mathbf{h}_a^\dagger \mathbf{v}_w \overline{\mathbf{v}}_w^\dagger \mathbf{h}_a\right)}{t_w - 1} - \frac{Re\left(\mathbf{h}_a^\dagger \overline{\mathbf{v}}_w \overline{\mathbf{v}}_w^\dagger \mathbf{h}_a\right)}{(t_w - 1)^2}(t_w - 1) \\ = & \mathcal{L}_1\left(\mathbf{v}_w, t_w, \overline{\mathbf{v}}_w, \overline{t}_w\right), \end{aligned} \tag{63}$$

where $\mathbf{h}_a^\dagger \mathbf{v}_w \bar{\mathbf{v}}_w^\dagger \mathbf{h}_a$ can be approximated as $Re(\mathbf{h}_a^\dagger \mathbf{v}_w \bar{\mathbf{v}}_w^\dagger \mathbf{h}_a)$, and $\mathbf{h}_a^\dagger \bar{\mathbf{v}}_w \bar{\mathbf{v}}_w^\dagger \mathbf{h}_a$ can be approximated as $Re(\mathbf{h}_a^\dagger \bar{\mathbf{v}}_w \bar{\mathbf{v}}_w^\dagger \mathbf{h}_a)$. Similarly, the first order Taylor expansion of (60b) at $\bar{\mathbf{v}}_u$ can be derived as

$$\begin{aligned} F_2(\mathbf{v}_u) &\geq F_2(\bar{\mathbf{v}}_u) + \frac{\partial F_2(\bar{\mathbf{v}}_u)}{\partial \mathbf{v}_u}(\mathbf{v}_u - \bar{\mathbf{v}}_u) \\ &= \frac{2Re\left(\mathbf{h}_u^\dagger \bar{\mathbf{v}}_u \bar{\mathbf{v}}_u^\dagger \mathbf{h}_u\right) - Re\left(\mathbf{h}_u^\dagger \bar{\mathbf{v}}_u \bar{\mathbf{v}}_u^\dagger \mathbf{h}_u\right)}{2^{r_u} - 1} \\ &= \mathcal{L}_2\left(\mathbf{v}_u, \bar{\mathbf{v}}_u\right). \end{aligned} \tag{64}$$

■

Then, we can perform the first-order Taylor approximation at a specific point on (59). As a result, (59b), (59c), (59d), and (59e) can be transformed into convex ones. Similarly, the decoding conditions (54) can be also converted to

$$S_k = \begin{cases} \left|\mathbf{h}_1^\dagger \mathbf{v}_1\right|^2 \leq ... \leq \min\left(\left|\mathbf{h}_1^\dagger \mathbf{v}_2\right|^2, ..., \left|\mathbf{h}_1^\dagger \mathbf{v}_K\right|^2\right), \\ \ldots, \\ \left|\mathbf{h}_S^\dagger \mathbf{v}_1\right|^2 \leq ... \leq \min\left(\left|\mathbf{h}_S^\dagger \mathbf{v}_2\right|^2, ..., \left|\mathbf{h}_S^\dagger \mathbf{v}_K\right|^2\right), \\ \left|\mathbf{h}_{S+1}^\dagger \mathbf{v}_1\right|^2 \leq ... \leq \min\left(\left|\mathbf{h}_{S+1}^\dagger \mathbf{v}_2\right|^2, ..., \left|\mathbf{h}_{S+1}^\dagger \mathbf{v}_K\right|^2\right), \\ \ldots, \\ \left|\mathbf{h}_K^\dagger \mathbf{v}_1\right|^2 \leq ... \leq \min\left(\left|\mathbf{h}_K^\dagger \mathbf{v}_2\right|^2, ... \left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2\right). \end{cases} \tag{65}$$

Therefore, all the restrictions in (59) have been converted to convex, and the problem can be modified into a SOCP, where the hyperbolic constraint $t^2 \leq xy$ $(x \geq 0, y \geq 0)$ can be changed into

$$\|[2t, x-y]^\dagger\| \leq x + y. \tag{66}$$

In addition, (59b), (59c), (59d), and (59e) can also be changed into SOC constraints, and we can obtain the corresponding optimization problem in (67) at the top of next page. In (67), $\mathcal{H} = \lceil \log_2 K \rceil$, which denotes a ceiling function.

C. Proposed Algorithm

(67) is a convex SOCP problem, which can be solved iteratively via CVX to obtain the solution to the original problem (56). The iterative algorithm is summarized as Algorithm 1.

Algorithm 1 Iterative algorithm for (56)

1: Randomly generate initial values $(\mathbf{v}_w^0, t_w^0)$ for (67). Set the initial number of iterations $n = 1$.
2: **repeat**
3: Calculate the optimization value of (67) by the point $(\mathbf{v}_w^n, t_w^n)$.
4: Update the current value of $(\mathbf{v}_w^{n+1}, t_w^{n+1}) = (\bar{\mathbf{v}}_w^n, \bar{t}_w^n)$.
5: Update: $n = n + 1$.
6: **until** $n = N$.

In Algorithm 1, the SOCP is solved in each iteration, and only the variables are updated. Thus, in order to derive the computational complexity, we can estimate the complexity of the worst case for the SOCP in (67). It is known that the complexity of the interior-point method for SOCP depends on the number of constraints, variables and the dimensions of all the SOC constraints [39]. The total number of constraints in (67) can be calculated as $0.5K^3 - 0.5K^2 + 4K - 2 + C_1$, where C_1 represents the non-negative integer constants generated due to the equivalent SOC representations of the geometric means in the objective functions. Thus, the number of iterations to reduce the duality gap to a constant fraction of itself is upper bounded by

$$\mathcal{I} = \mathcal{O}\sqrt{0.5K^3 - 0.5K^2 + 4K - 2 + C_1} \tag{68}$$

for (67). Furthermore, the amount of calculation per iteration can be expressed as

$$\mathcal{Q} = \mathcal{O}\Big((2KM+K-1)^2\big(1.5K^3 - 1.5K^2 + 8K + KM + 2C_1\big)\Big). \tag{69}$$

Based on (68) and (69), we can derive the computational complexity of Algorithm 1 by (70) .

After performing Algorithm 1, the eavesdropping rate towards the secure users can be calculated as

$$R_e^i = \log\left(1 + \frac{|\mathbf{h}_e \mathbf{v}_i|^2}{\sum_{m=1, m\neq i}^K |\mathbf{h}_e \mathbf{v}_m|^2 + \sigma^2}\right),\ i = 1, \ldots, S, \tag{71}$$

which is close to 0, due to the fact that the transmit power of the common users becomes higher to maximize their transmission rate, which can disrupted the eavesdropping towards the secure users effectively.

Thus, the privacy of the secure users can be guaranteed, and their secrecy rate can be denoted as

$$R_s^i = R_t^i - R_e^i,\ i = 1, \ldots, S, \tag{72}$$

where R_t^i and R_e^i are given by (57) and (71), respectively.

V. Simulation Results and Discussion

In this section, the performance of the proposed scheme for the single-antenna UAV is first presented. Then, the case for the multi-antenna UAV with multiple secure users is discussed. The altitude of the UAV is fixed at 50 m in the simulation. The pass-loss exponent α is set to 2 and the channel power gain at the reference distance ρ is equal to 10^{-4}. The noise power σ^2 is set to -110 dBm.

A. Single-Antenna UAV

First, we consider the case of 3 ground users, and one of them requires secure transmission, i.e., $K = 3$ and $S = 1$. The threshold of transmission rate is set to $r = r_1 = r_2 = r_3 =$0.5 bit/s/Hz. The locations of the three ground users are (0, 0, 0), (60, -30, 0) and (110, 40, 0) in meters, respectively. U_1 is the secure user.

To verify the optimal hovering position of the UAV, the transmission rate and secrecy rate of U_1 are compared in Fig. 2 for different locations of the UAV, i.e., above the secure user (0, 0, 0), above the farthest user (110, 40, 0) and above the horizontal center of the three users (56.67, 3.33, 0). From the results, we can see that the transmission rate of U_1 with these UAV positions can all achieve the rate threshold 0.5 bit/s/Hz, according to the optimization problem (14). For the secrecy

$$\max_{\mathbf{v}_i, t_w} \; t^0 \tag{67a}$$

$$s.t. \;\; \|[2t_m^{\mathcal{H}-1}, (t_{2m-1}^{\mathcal{H}} - t_{2m}^{\mathcal{H}})]^\dagger\| \leq t_{2m-1}^{\mathcal{H}} + t_{2m}^{\mathcal{H}}, \; m = 1, 2, ...2^{\mathcal{H}-1}, \tag{67b}$$

$$\|[2t_m^{\mathcal{H}-2}, (t_{2m-1}^{\mathcal{H}-1} - t_{2m}^{\mathcal{H}-1})]^\dagger\| \leq t_{2m-1}^{\mathcal{H}-1} + t_{2m}^{\mathcal{H}-1}, \; m = 1, 2, ...2^{\mathcal{H}-2}, \tag{67c}$$

$$..... \tag{67d}$$

$$\|[2t_1^0, (t_1^1 - t_2^1)]^\dagger\| \leq t_1^1 + t_2^1, \; m = 1,$$

$$\|[2\mathbf{h}_w^\dagger \mathbf{v}_1, 2\mathbf{h}_w^\dagger \mathbf{v}_2 ... 2\mathbf{h}_w^\dagger \mathbf{v}_w, 2\sigma, (\mathcal{L}_1 - 1)]^\dagger\| \leq \mathcal{L}_1 + 1, \; w = S+1, ...K, \tag{67e}$$

$$\|[2\mathbf{h}_u^\dagger \mathbf{v}_1, 2\mathbf{h}_u^\dagger \mathbf{v}_2 ... 2\mathbf{h}_u^\dagger \mathbf{v}_u, 2\sigma, (\mathcal{L}_2 - 1)]^\dagger\| \leq \mathcal{L}_2 + 1, \; u = 1, ...K, \tag{67f}$$

$$\|[\mathbf{v}_1, \mathbf{v}_2 ... \mathbf{v}_K]^\dagger\| \leq \sqrt{P_{sum}}, \text{and } (65). \tag{67g}$$

$$\mathcal{C} = \mathcal{O}\left(\sqrt{0.5K^3 - 0.5K^2 + 4K - 2 + C_1}\left(2KM + K - 1\right)^2 \left(1.5K^3 - 1.5K^2 + 8K + KM + 2C_1\right)\right). \tag{70}$$

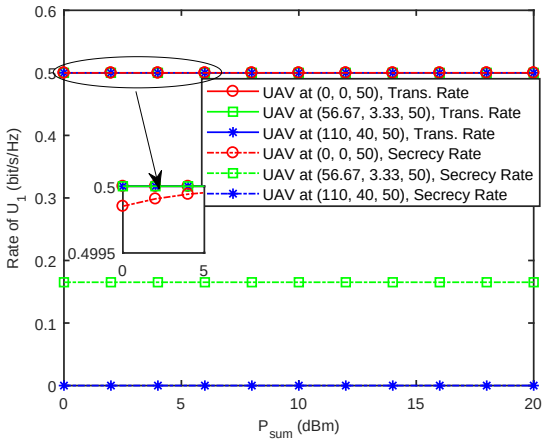

Fig. 2. Comparison of transmission rate and secrecy rate of U_1 with different hovering positions of the UAV.

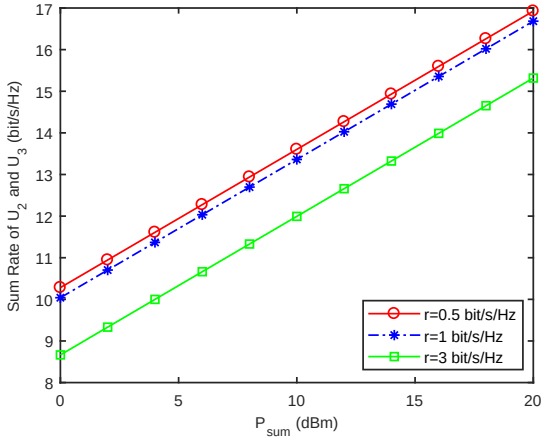

Fig. 3. Comparison of sum rate of U_2 and U_3 with different values of P_{sum} and the threshold r.

rate of U_1, it is close to the transmission rate when the UAV hovers above U_1, due to the fact that its transmit power is the lowest, and it can be hidden in the high-power signals of other users. However, when the UAV hovers above the farthest user or above the horizontal center of the three users, the secrecy rate becomes lower or even close to 0 according to (71). In this case, the transmit power for U_1 becomes higher when U_1 is far from the UAV, and thus, the eavesdropping rate towards U_s tends to be higher.

Then, the sum rate of U_2 and U_3 is compared in Fig. 3, with different values of P_{sum} and the threshold r. The UAV is located at (0, 0, 50). From the results, we can see that the sum rate of U_2 and U_3 becomes higher with larger P_{sum} and lower r. This is because the the lowest transmit power is allocated to U_1 to satisfy its rate threshold r and guarantee its security, and the remaining power is allocated to U_2 and U_3 to maximize their sum rate. Therefore, lower r results in higher sum rate of U_2 and U_3 due to higher transmit power allocated to them. In addition, the eavesdropping rate and secrecy rate of U_1 are compared in Fig. 4, with different values of P_{sum} and the threshold r. The UAV is located at (0, 0, 50). From

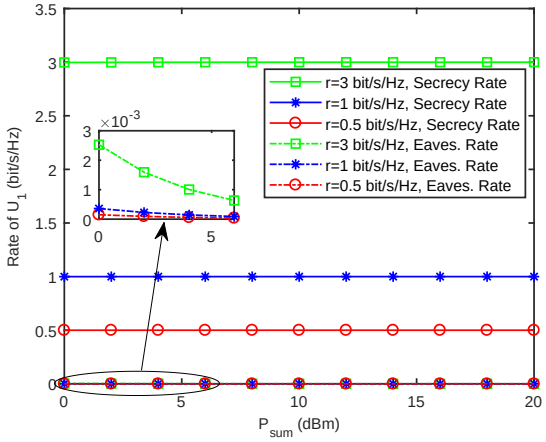

Fig. 4. Comparison of eavesdropping rate and secrecy rate of U_1 with different values of P_{sum} and the threshold r.

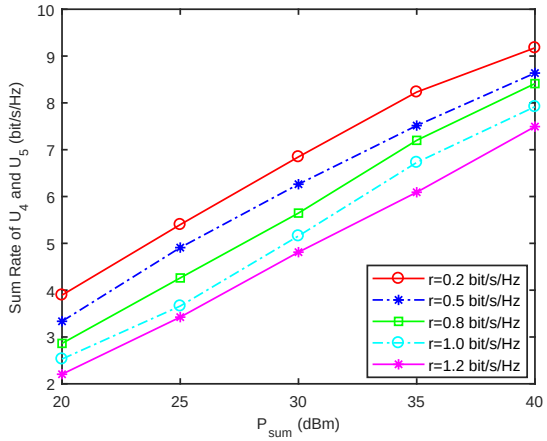

Fig. 5. Comparison of the sum rate of U_4 and U_5 with different values of P_{sum} and the threshold r. $M = 5$.

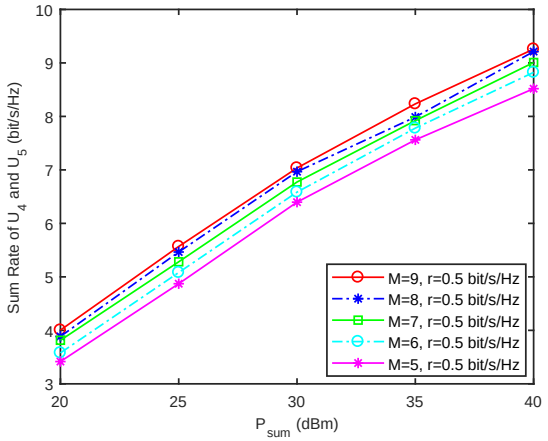

Fig. 6. Comparison of the sum rate of U_4 and U_5 with different values of P_{sum} and M. $r = 0.5$ bit/s/Hz.

the results, we can see that the secrecy rate of U_1 is close to the threshold r, especially when P_{sum} is high and r is small, which is due to the fact that more transmit power can be allocated to U_2 and U_3 to disrupt the eavesdropping towards U_1 in this case. On the other hand, we can also find that the eavesdropping rate towards U_1 is a little higher when P_{sum} is low and r is large. This is because lower power can be allocated to U_2 and U_3 to disrupt the eavesdropping, in order to achieve higher r for U_1.

B. Multi-Antenna UAV

For the multi-antenna UAV, we assume that $S = 3$ and $K = 5$, i.e., 3 out of 5 users are secure users. U_1, U_2 and U_3 are secure users, and U_4 and U_5 are common users. The five users are located at (0, 0, 0), (8, -18, 0), (40, 32, 0), (-8, 10, 0) and (15, 25, 0) in meters, while the UAV is at (0, 0, 50). Thus, the distances between the UAV and these users can be expressed as $d_1 < d_4 < d_2 < d_5 < d_3$.

First, the sum rate of U_4 and U_5 is compared in Fig. 5, with different values of P_{sum} and the threshold r. $M = 5$ antennas are equipped at the UAV. From the results, we can see that the sum rate of U_4 and U_5 increases with higher P_{sum} and smaller r. This is because when r becomes smaller or P_{sum} becomes higher, more transmit power can be allocated to the common users, which makes the small signals of the secure users hidden in the larger signals of the common users. Thus, the security of the secure users can be guaranteed. The sum rate of U_4 and U_5 is compared in Fig. 6, with different values of P_{sum} and M. $r = 0.5$ bit/s/Hz. From the results, we can see that the sum rate of U_4 and U_5 increases with P_{sum} and M, which is natural due to the fact that more antennas at the UAV can improve the performance of the beamforming effectively.

Then, the eavesdropping rate towards the secure users is compared in Fig. 7, with different values of P_{sum} and M. $r = 0.5$ bit/s/Hz. From the results, we can observe that the eavesdropping rate decreases with P_{sum} and M. This is because more power and antenna resource will make the proposed more effectively to disrupt the eavesdropping. In addition, we can also find that the eavesdropping rate of U_1

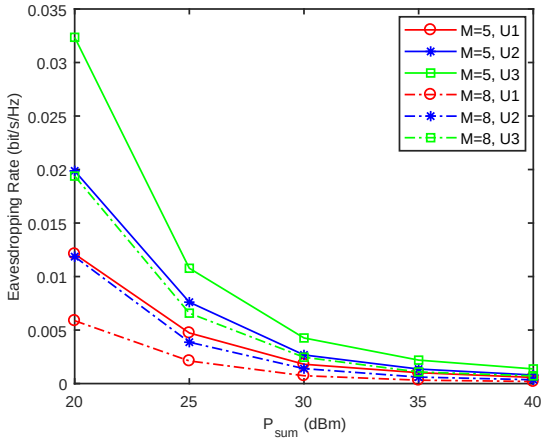

Fig. 7. Comparison of the eavesdropping rate towards the secure users with different values of P_{sum} and M. $r = 0.5$ bit/s/Hz.

is lower than that of U_2, and the eavesdropping rate of U_2 is lower than that of U_3. This is due to the fact that the transmit power of U_1 is the lowest and the transmit power of U_3 is the highest among the three secure users according to NOMA based on their distances from the UAV, i.e., $d_1 < d_2 < d_3$. The secrecy rate of the secure users is compared in Fig. 8, with different values of P_{sum} and M. $r = 0.5$ bit/s/Hz. From the results, we can observe that the secrecy rate of the secure users increase with P_{sum} and M, due to the fact that more resource can be utilized in the beamforming to disrupt the eavesdropping more effectively. Besides, the secrecy rate of U_1 is higher than that of U_2, and the secrecy rate of U_2 is higher than that of U_3. This is because shorter distance from the UAV to a specific user will make its transmit power much lower, and thus, its secure performance becomes better.

Finally, the secrecy rate of the secure users is compared in the proposed scheme and the conventional scheme in Fig. 9, with different values of P_{sum}. $r = 0.5$ bit/s/Hz. In the conventional NOMA scheme, the decoding order is determined by the distances of the users from the UAV, i.e., $3 \to 5 \to 2 \to 4 \to 1$. From the results, we can observe that the secrecy rate of U_1 in both of these two schemes is almost the same, due to

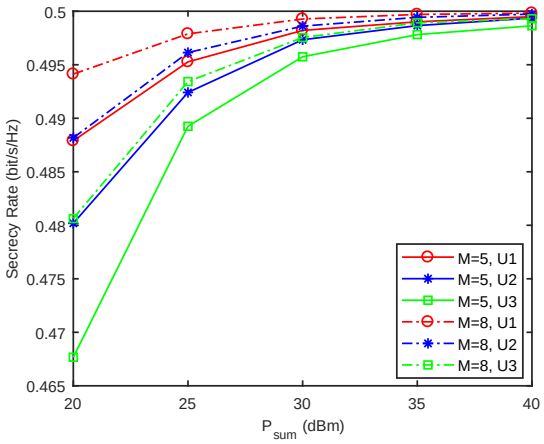

Fig. 8. Comparison of the secrecy rate of the secure users with different values of P_{sum} and M. $r = 0.5$ bit/s/Hz.

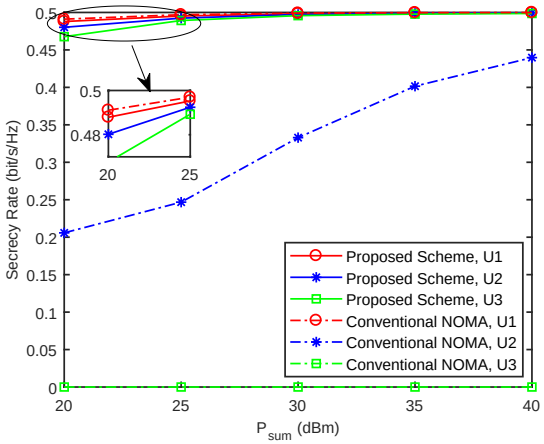

Fig. 9. Comparison of the secrecy rate in the proposed scheme and the conventional NOMA scheme with different values of P_{sum}. $r = 0.5$ bit/s/Hz. $M = 5$.

the fact that the signal from U_1 is last decoded with the lowest power. However, the secrecy rate of U_2 and U_3 in the proposed scheme is much higher than that in the conventional NOMA scheme. This is because the signals of these two users in the proposed scheme is decoded later with lower power than those in the conventional NOMA scheme, which can guarantee their security effectively.

VI. Conclusions

In this paper, we have proposed two schemes to enhance the security of NOMA-UAV networks via PA and beamforming, respectively. First, when only one user requires secure transmission, the optimal position is derived for the UAV and the PA problem is performed to maximize the sum rate of common users with the secure transmission for the private user guaranteed. However, when several users require secure transmission simultaneously, it becomes difficult or even impossible to achieve the secure transmission with a single antenna at the UAV. Thus, the antenna resource at the UAV is fully utilized to guarantee the secure transmission of these users via beamforming optimization. The problem is non-convex, and we transform it into a SOCP problem, which can be solved iteratively. Simulation results are presented to show the effectiveness of the proposed scheme in enhancing the security of NOMA-UAV networks.

References

[1] Y. Li, F. Jiang, N. Zhao, S. Zhang, Y. Chen, W. Lu, and X. Wang, "Security enhancement for NOMA-UAV networks," in *Proc. IEEE VTC'20-Spring*, pp. 1–6, Antwerp, Belgium, May 2020.

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

[3] N. Zhao, W. Lu, M. Sheng, Y. Chen, J. Tang, F. R. Yu, and K. Wong, "UAV-assisted emergency networks in disasters," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 45–51, Feb. 2019.

[4] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network towards 6G: Machine learning approaches," *Proc. IEEE*, DOI: 10.1109/JPROC.2019.2954595.

[5] A. A. Khuwaja, Y. Chen, N. Zhao, M. Alouini, and P. Dobbins, "A survey of channel modeling for UAV communications," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2804–2821, 4th Quart. 2018.

[6] F. Tang, Z. M. Fadlullah, B. Mao, N. Kato, F. Ono, and R. Miura, "On a novel adaptive UAV-mounted cloudlet-aided recommendation system for LBSNs," *IEEE Trans. Emerg. Top. Comput.*, DOI: 10.1109/TETC.2018.2792051.

[7] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 73–82, Sept. 2017.

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

[9] S. Zhang, H. Zhang, B. Di, and L. Song, "Cellular UAV-to-X communications: Design and optimization for Multi-UAV networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1346–1359, Feb. 2019.

[10] R. Fan, J. Cui, S. Jin, K. Yang, and J. An, "Optimal node placement and resource allocation for UAV relaying network," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 808–811, Apr. 2018.

[11] X. Liu, Z. Li, N. Zhao, W. Meng, G. Gui, Y. Chen, and F. Adachi, "Transceiver design and multihop D2D for UAV IoT coverage in disasters," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1803–1815, Apr. 2019.

[12] S. Zhang, Y. Zeng, and R. Zhang, "Cellular-enabled UAV communication: A connectivity-constrained trajectory optimization perspective," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2580–2604, Mar. 2019.

[13] Y. Zeng, J. Xu, and R. Zhang, "Energy minimization for wireless communication with rotary-wing UAV," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2329–2345, Apr. 2019.

[14] T. Zhang, Y. Xu, J. Loo, D. Yang, and L. Xiao, "Joint computation and communication design for UAV-assisted mobile edge computing in IoT," *IEEE Trans. Ind. Informat.*, DOI: 10.1109/TII.2019.2948406.

[15] D. Yang, Q. Wu, Y. Zeng, and R. Zhang, "Energy tradeoff in ground-to-UAV communication via trajectory design," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6721–6726, 2018. Jul.

[16] F. Tang, Z. M. Fadlullah, N. Kato, F. Ono, and R. Miura, "AC-POCA: Anticoordination game based partially overlapping channels assignment in combined UAV and D2D-based networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1672–1683, Feb. 2018.

[17] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, 2013. Nov.

[18] Y. Cai, F. Cui, Q. Shi, M. Zhao, and G. Y. Li, "Dual-UAV-enabled secure communications: Joint trajectory design and user scheduling," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1972–1985, Sept. 2018.

[19] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV-relaying-assisted secure transmission with caching," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3140–3153, May 2019.

[20] L. Xiao, Y. Xu, D. Yang, and Y. Zeng, "Secrecy energy efficiency maximization for UAV-enabled mobile relaying," *IEEE Trans. Green Commun. Netw.*, DOI: 10.1109/TGCN.2019.2949802.

[21] 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 J. Select. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[22] G. Gui, H. Huang, Y. Song, and H. Sari, "Deep learning for an effective nonorthogonal multiple access scheme," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8440–8450, Sept. 2018.

[23] Y. Lin, S. Wang, X. Bu, C. Xing, and J. An, "NOMA-based calibration for large-scale spaceborne antenna arrays," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2231–2242, Mar. 2018.

[24] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts*, vol. 19, no. 2, pp. 721–742, 2nd Quart. 2017.

[25] J. Cui, Z. Ding, and P. Fan, "A novel power allocation scheme under outage constraints in NOMA systems," *IEEE Signal Processing Lett.*, vol. 23, no. 9, pp. 1226–1230, Sept. 2016.

[26] D. Zhang, Y. Liu, Z. Ding, Z. Zhou, A. Nallanathan, and T. Sato, "Performance analysis of non-regenerative massive-MIMO-NOMA relay systems for 5G," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4777–4790, Nov. 2017.

[27] J. Tang, J. Luo, M. Liu, D. K. C. So, E. Alsusa, G. Chen, K. Wong, and J. A. Chambers, "Energy efficiency optimization for NOMA with SWIPT," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 452–466, Jun. 2019.

[28] P. Xu, Z. Yang, Z. Ding, and Z. Zhang, "Optimal relay selection schemes for cooperative NOMA," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7851–7855, Aug. 2018.

[29] Y. Cao, N. Zhao, Y. Chen, M. Jin, Z. Ding, Y. Li, and F. R. Yu, "Secure transmission via beamforming optimization for NOMA networks," *IEEE Wireless Commun.*, Online. DOI: 10.1109/MWC.001.1900159.

[30] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7563–7567, Aug,2017.

[31] Y. Cao, N. Zhao, Y. Chen, M. Jin, L. Fan, Z. Ding, and F. R. Yu, "Privacy preservation via beamforming for NOMA," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3599–3612, Jul. 2019.

[32] B. Zheng, M. Wen, C. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[33] N. Zhao, W. Wang, J. Wang, Y. Chen, Y. Lin, Z. Ding, and N. C. Beaulieu, "Joint beamforming and jamming optimization for secure transmission in MISO-NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2294–2305, Mar. 2019.

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

[35] M. Liu, J. Yang, and G. Gui, "DSF-NOMA: UAV-assisted emergency communication technology in a heterogeneous internet of things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5508–5519, Jun. 2019.

[36] T. Hou, Y. Liu, Z. Song, X. Sun, and Y. Chen, "Multiple antenna aided NOMA in UAV networks: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1031–1044, Feb. 2019.

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

[38] W. Mei and R. Zhang, "Uplink cooperative NOMA for cellular-connected UAV," *IEEE J. Sel. Topics Signal Proc.*, vol. 13, no. 3, pp. 644–656, Jun. 2019.

[39] M. S. Lobo, L. Vandenberghe, S. P. Boyd, and H. Lebret, "Applications of second-order cone programming," *Linear Algebra Appl.*, vol. 284, no. 1-3, pp. 193–228, Nov. 1998.