Enhance Secrecy Performance of the Cooperative NOMA/UAV Network Applying NSGA-II Algorithm

Anh Le-Thi[1(✉)], Thuc Kieu-Xuan[1], Hong Nguyen-Thi[2], and Nhung Tran-Phuong[1]

[1] Hanoi University of Industry, Hanoi, Vietnam
{leanh,thuckx,nhungtp}@haui.edu.vn
[2] Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

Abstract. In this paper, we propose and analyze the security performance of cooperative power-domain non-orthogonal multiple access systems (NOMA) for multiple users with the assistance of UAV over Rice fading channels. In the proposed system, multi-destination users are allocated various powers and communicate with the transmitter (Tx) via the UAV relaying node. UAV acts as an intermediate node that transmits the signal to the user through the amplification and forward (AF) protocol. A friendly jammer node interferes with the received signals at eavesdroppers to enhance the system's security. In addition, in order to increase the security quality of the system through both secrecy capacity, in this paper, a multi-objective optimization technique NSGA-II is applied to maximize the secrecy capacity at the valid users and minimize the received signal's quality at the eavesdropping node. Finally, we analyze the influence of critical system parameters on secrecy performance, such as transmit power, distance of UAV from the ground, and distance between friendly jammer and base station.

Keywords: Power-domain NOMA · rice fading · multi-objective optimization · NSGA-II

1 Introduction

With the rapid development of wireless techniques, communication with the assistance of drones or unmanned aerial vehicles (UAVs) has been seen as a promising solution for current and future network infrastructure deployments [1,2]. With high mobility, flexible deployment, and low cost, UAVs can be deployed as relaying stations or aerial base stations to help establish temporary communication infrastructure in emergencies. For example, UAV communication can be set up for disaster-affected areas, reducing the load on areas with dense

Supported by Hanoi University of Industry.

N. Thi Dieu Linh et al. (Eds.): ADHOCNETS 2023, LNICST 558, pp. 137–149, 2024.
https://doi.org/10.1007/978-3-031-55993-8_11

equipment density. Besides, the NOMA technique is also considered a potential candidate for future mobile networks because of its high spectrum efficiency, low latency, and serving many users [3,4]. Recently, due to the benefits of the NOMA technique and UAV communication, the combination of NOMA-UAV has been an interesting topic. Some publications [5–7] have studied the NOMA cooperative communication network with the help of UAVs.

Security is a critical aspect of future wireless networks that the research community focuses on now. Developing techniques for enhancing secure transmission in the wireless medium is an intricate problem that needs to be focused on research. Because of the principle of broadcasting radio communication, signals on wireless channels can be overheard by eavesdroppers. One of the methods against eavesdropping attract is exploiting jamming signals [8,9]. Some publications investigated the secrecy performance of NOMA and UAV communication [10–12]. However, no studies have been published on improving the security of NOMA/UAV systems using multi-objective optimization techniques, applying variations of genetic algorithms such as the Non-dominated Sorting Genetic Algorithm (NSGA-II) [13]. Thus, in this paper, we propose a new power-domain NOMA network with the help of a UAV relaying station and apply NSGA-II to improve the secrecy capacity and reduce the effect of the eavesdropper.

2 Communication Model and Phases

2.1 Communication Model

Figure 1 presents our proposed communication scheme of multi-NOMA users and a base station with the assistance of an intermediate node as a UAV applying AF protocol in the presence of an eavesdropper and a friendly jammer. Because of the working principle of PD-NOMA, the node operating on the poor channel is allocated higher power; conversely, the node undergoing the better link is assigned lower power. In our model, the first user (U_1)is assumed to be furthest from the base station, followed by the second user (U_2), and the user closest to the source node is the L^{th} user (U_L). Thus, (U_1) is allocated the highest level of transmitted power, and a second power level is assigned to (U_2), and the lowest power is assigned to (U_L). The source signal (x_s) is a superimposed signal of L users x_1, x_2,..., and x_L. Moreover, the UAV relaying node forwards the received signal from the ground source node to NOMA users. The ground-air link is a BS-UAV connection, and air-ground links are UAV-user connections that undergo Rice fading channels. NOMA-user applies the successive interference cancellation (SIC) to detect the desired user signal.

In this design, we denote h_0, h_l with $l = 1, 2, \ldots, L$, h_E, and $h_{UAV,Jl,JE}$ are the channel coefficients of the ground-air link BS-UAV, the air-ground links UAV-U_l, the air-ground link UAV-Eavesdropper, and friendly jammer - UAV, jammer-users, jammer-eavesdropper links respectively. The distances of BS-UAV, UAV-U_l, UAV-Jammer, UAV-E and Jammer-U_l, Jammer-E links are d_0, d_l, d_J, d_E, and d_{Jl} respectively.

The ground-air links are communications connections from the BS and friendly jammer to the UAV, and air-ground links are from the UAV to the users and eavesdroppers. These links are Rician fading channels which include two components that are line-of-sight propagation (direct path) and non-line-of-sight propagation (NLoS), and can be expressed as $h = \sqrt{\frac{K_h}{K_h+1}}h^{LoS} + \sqrt{\frac{1}{K_h+1}}h^{NLoS}$.

With $h \in H = \{g_{km}, g_{mj}\}, j = \{1, 2\}$ where K_h, h^{LoS}, and h^{NLoS} are the Rician factor, Los components, and NLoS components of channel h, respectively. The NLoS parts hNLoS are i.i.d. complex Gaussian distributed with zero mean and unit variance.

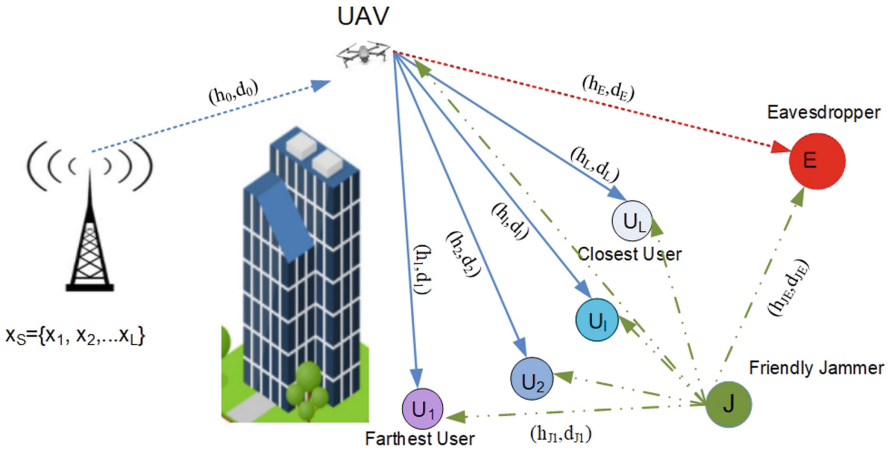

Fig. 1. The proposed network model

In addition, we assume that (1) the ground-air and air-ground connections of BS-UAV, J-UAV, and UAV-users, UAV-E suffer Rician fading channels; (2) there is no direct path between BS and NOMA users, BS and Eavesdropper, BS and jammer; (3) the local channel state information (CSI) is assumed at the relay, and the global CSI is presumed at BS and the users.

2.2 The First Communication Phase

BS transmits the source signal of multiple NOMA-users to the intermediate node UAV. This signal is represented mathematically as follows:

$$x_S = \sum_{l=1}^{L} \sqrt{P_l \alpha_l} s_l, \tag{1}$$

where x_l (l=1,2,..., L) is denoted as the signal to user l, and P_l is denoted as the power allocation level corresponding to the l^{th} user which satisfies the condition $\sum_{l=1}^{L} P_l = P_S$ and $P_1 \geq P_2 \geq ... \geq P_l \geq ... \geq P_L$.

Then, the received signal at UAV relaying node is composed of the signal from BS and the friendly Jammer. Thus, the received signal at UAV can be expressed ass

$$y_{UAV} = \sum_{l=1}^{L} \sqrt{P_l} s_l h_0 + \sqrt{P_J} s_J h_J + n_{UAV}^{[a]} \tag{2}$$

Here, the channel coefficients of the link BS - UAV, friendly jammer-UAV are denoted by h_0, and h_J respectively; and $n_{UAV}^{[a]} \sim CN\left(0, \sigma_{\text{aR}}^2\right)$ is antenna white Gaussian noise (AWGN).

2.3 The Second Communication Phase

After receiving the superimposed signal from the BS, the UAV will apply the AF protocol to amplify this signal before forwarding it to the destination users. Denoting G as an amplified factor of AF protocol, G is calculated as $G = \left(\sum_{l=1}^{L} \sqrt{P_l}|h_0|^2 + P_J|h_J|^2 + \sigma_{UAV}^2\right)^{-1}$. Moreover, in this phase, a friendly jammer also transmits the jamming signal to all destination users and eavesdroppers.

Because of the propagation characteristics of the wireless environment, the signals from UAV and Jammer will broadcast to legitimate NOMA users and eavesdroppers. Hence, the received signals at L destinations users and the eavesdropper can be written as follows:

$$\begin{aligned} y_{U_l} = &\sum_{l=1}^{L} \sqrt{GP_rP_l} s_l h_0 h_l + \sqrt{GP_r} n_{UAV} h_l + n_{U_l} \\ &+ \underbrace{\sqrt{GP_rP_J} s_J h_l h_J + \sqrt{P_J} s_J h_{Jl}}_{\text{Totaljammingsignals}}. \end{aligned} \tag{3}$$

and,

$$\begin{aligned} y_E = &\sum_{l=1}^{L} \sqrt{GP_rP} s_l h_0 h_E + \sqrt{GP_r} n_{UAV} h_E + n_E \\ &+ \underbrace{\sqrt{GP_rP_J} s_J h_E h_J + \sqrt{P_J} s_J h_{JE}}_{\text{Totaljammingsignals}} \end{aligned} \tag{4}$$

Here, n_{U_l} and n_E are the AWGN at U_l and E respectively; P_r is transmitted power at UAV relaying node.

Because the legitimate users can eliminate the jamming signals from the Friendly Jammer and due to the SIC at the NOMA receiver of each user, the SINRs at any user (User l) can be expressed as,

$$\gamma_{1l} = \frac{|h_0|^2|h_l|^2}{\frac{\sum_{l=2}^{L} P_l}{P_1}|h_0|^2|h_l|^2 + \frac{\sigma_{UAV}^2}{P_1}|h_l|^2 + \frac{\sigma_{U_l}^2 \sum_{l=1}^{L} P_l}{P_r P_1}|h_0|^2 + \frac{P_J \sigma_{U_l}^2}{P_r P_1}|h_J|^2 + \frac{\sigma_{U_l}^2 \sigma_{UAV}^2}{P_r P_1}} \tag{5}$$

We can see that $\sigma_{U_l}^2\sigma_{UAV}^2 << P_rP_1$, thus $\frac{\sigma_{U_l}^2\sigma_{UAV}^2}{P_rP_1} \to 0$, then Eq.(5) can be rewritten as

$$\gamma_{1l} = \frac{|h_0|^2|h_l|^2}{\frac{\sum_{l=2}^{L} P_l}{P_1}|h_0|^2|h_l|^2 + \frac{\sigma_{UAV}^2}{P_1}|h_l|^2 + \frac{\sigma_{U_l}^2\sum_{l=1}^{L} P_l}{P_rP_1}|h_0|^2 + \frac{P_J\sigma_{U_l}^2}{P_rP_1}|h_J|^2} \tag{6}$$

Similarly, we have:

$$\gamma_{2l} = \frac{|h_0|^2|h_l|^2}{\frac{\sum_{l=3}^{L} P_l}{P_2}|h_0|^2|h_l|^2 + \frac{1}{P_2}\sigma_{UAV}^2|h_l|^2 + \frac{\sum_{l=1}^{L} P_l}{P_rP_2}|h_0|^2\sigma_{U_l}^2 + \frac{P_J}{P_rP_2}|h_J|^2\sigma_{U_l}^2} \tag{7}$$

...
...
...

$$\gamma_{ll} = \frac{|h_0|^2|h_l|^2}{\frac{\sum_{j=l+1}^{L} P_l}{P_l}|h_0|^2|h_l|^2 + \frac{1}{P_l}\sigma_{UAV}^2|h_l|^2 + \frac{\sum_{l=1}^{L} P_l}{P_rP_l}|h_0|^2\sigma_{U_l}^2 + \frac{P_J}{P_rP_l}|h_J|^2\sigma_{U_l}^2} \tag{8}$$

...
...
...

$$\gamma_{Ll} = \frac{|h_0|^2|h_l|^2}{\frac{\sigma_{UAV}^2}{P_L}|h_l|^2 + \frac{\sigma_{U_l}^2\sum_{l=1}^{L} P_l}{P_rP_L}|h_0|^2 + \frac{P_J\sigma_{U_l}^2}{P_rP_L}|h_J|^2} \tag{9}$$

At Eavesdropper, in this paper, we consider the worst-case scenario: applying the parallel interference cancellation to guarantee the capacity of best decoding [14]. This means E can eliminate the interference of x_2,..., x_L when decoding x_1, similar to other cases. Moreover, E cannot eliminate the jamming signal from the friendly jammer. Thus, the SINRs of user signals at E can be expressed as follows:

$$\gamma_{1E} = \frac{|h_0|^2|h_E|^2}{\left(\begin{array}{l}\frac{P_J}{P_1}|h_E|^2|h_J|^2 + \frac{\sigma_{UAV}^2}{P_1}|h_E|^2 + \frac{P_J\sum_{l=1}^{L}\sqrt{P_l}}{P_rP_1}|h_0|^2|h_{JE}|^2 + \\ \frac{P_J^2}{P_rP_1}|h_J|^2|h_{JE}|^2 + \frac{P_J\sigma_{UAV}^2}{P_rP_1}|h_{JE}|^2 + \frac{\sum_{l=1}^{L}\sqrt{P_l}\sigma_E^2}{P_rP_1}|h_0|^2 + \frac{P_J\sigma_E^2}{P_rP_1}|h_J|^2\end{array}\right)} \tag{10}$$

...
...

$$\gamma_{lE} = \frac{|h_0|^2|h_E|^2}{\left(\begin{array}{l}\frac{P_J}{P_l}|h_E|^2|h_J|^2 + \frac{\sigma^2_{UAV}}{P_l}|h_E|^2 + \frac{P_J\sum\limits_{l=1}^{L}\sqrt{P_l}}{P_rP_l}|h_0|^2|h_{JE}|^2 \\ +\frac{P_J^2}{P_rP_l}|h_J|^2|h_{JE}|^2 + \frac{P_J\sigma^2_{UAV}}{P_rP_l}|h_{JE}|^2 + \frac{\sum\limits_{l=1}^{L}\sqrt{P_l}\sigma^2_E}{P_rP_l}|h_0|^2 + \frac{P_J\sigma^2_E}{P_rP_l}|h_J|^2\end{array}\right)} \tag{11}$$

...

...

$$\gamma_{LE} = \frac{|h_0|^2|h_E|^2}{\left(\begin{array}{l}\frac{P_J}{P_L}|h_E|^2|h_J|^2 + \frac{\sigma^2_{UAV}}{P_L}|h_E|^2 + \frac{P_J\sum\limits_{l=1}^{L}\sqrt{P_l}}{P_rP_L}|h_0|^2|h_{JE}|^2 \\ +\frac{P_J^2}{P_rP_L}|h_J|^2|h_{JE}|^2 + \frac{P_J\sigma^2_{UAV}}{P_rP_L}|h_{JE}|^2 + \frac{\sum\limits_{l=1}^{L}\sqrt{P_l}\sigma^2_E}{P_rP_L}|h_0|^2 + \frac{P_J\sigma^2_E}{P_rP_L}|h_J|^2\end{array}\right)} \tag{12}$$

3 Secrecy Performance Analysis

In this part, we investigate the secrecy performance of our PD-NOMA/UAV model. To enhance the secrecy capacity of this system and interference with the eavesdropping links, we apply the multi-objective optimization technique as NSGA-II. Remarkably, the problem is the maximization of the sum of the secrecy capacity of NOMA users and the minimization of the capacity of the eavesdropper.

The secrecy capacity at any node is defined as follows

$$C^l_{\text{sec}} = \left[R^{U_l}_{s_l} - R^E_{s_l}\right]^+. \tag{13}$$

Here, according to Shannon capacity, $R^{U_l}_{s_l} = \log_2(1+\gamma_{ll})$ as data rate at user l^{th}, with $l = 1, 2, ..., L$, and $R^E_{s_l} = \log_2(1+\gamma_{lE})$ as data rate at the eavesdropper.

Due to the NOMA principle, user l^{th} has to decode the successfully stronger signals and then detect its desired signal. The data rate at user l^{th} can be expressed as $R^{U_l}_{s_l} = \log_2\left(1 + \min\limits_{l=1,..,L}\{\gamma_{ll}\}\right)$. Thus, secrecy capacity at user l^{th} can be formulated as follows

$$C^l_{\text{sec}} = \left[\log_2\left(1 + \min_{l=1,..,L}\{\gamma_{ll}\}\right) - \log_2(1+\gamma_{lE})\right]^+ \tag{14}$$

The sum of the secrecy capacity (SSC) of our proposed system can be expressed as

$$C_{\text{sec}} = \sum_{l=1}^{L} C^l_{\text{sec}} \tag{15}$$

The problem is defined as how to maximize the SSC and minimize the capacity at Eavesdropper. And this problem can be formulated as follows

$$\max_{P_1,..,P_l,..,P_L} C_{\text{sec}} = \sum_{l=1}^{L} \left[\log_2 \left(1 + \min_{l=1,..,L} \{\gamma_{ll}\} \right) - \log_2 (1 + \gamma_{lE}) \right]^+ \text{and}$$

$$\min_{P_1,..,P_l,..,P_L} R_l^E = \log_2 (1 + \gamma_{lE}) \quad (16)$$

$$\text{subjectto} : \min_{j,l=\{1,2,...,L\}} \gamma_{jl} \geq \gamma_0 \quad (16.1)$$

$$\sum_{l=1}^{L} P_l \leq P_S^{\max} \quad (16.2)$$

$$P_1 \geq P_2 \geq ... \geq P_l \geq ... \geq P_L investigatestheinfluenceP_r \geq e_0 \quad (16.3)$$

Here γ_0 is a threshold at which the user signal can be decoded, and e_0 is the threshold power, which means the minimum power to transmit the signal from the relaying UAV node.

To solve the problem of two objectives in Eq. 16 under multiple constraint conditions (16.1), (16.2), (16.3) and (16.4), we apply Non-Dominated Sorting Genetic Algorithm II (NSGA-II). NSGA II is a well-known application to solve multi-objective optimization problems [15]. It is an elitist non-dominated sorting genetic algorithm. To put it another way, the best solutions of the previous iteration are kept unchanged in the current one. In addition, it adopts an elite preservation strategy and uses an explicit diversity preservation technique. Firstly, the offspring population is created from the parent population, which is initialized. Before using non-dominated to classify, both populations are combined. Then, the assignment of rank 1 for the best non-dominated font is to obtain a new filled population. This continues for successive fronts with the assignment of ranks. The crowding distance sorting is also utilized to obtain the greater diversity of the Pareto front. The crowding distance sorting is also utilized to obtain the greater diversity of the Pareto front. Crowding distance implies the closeness of a solution to its neighbors, so the greater the distance, the better the diversity of the Pareto front. It means a more suitable solution for the problem. The offspring population is created from the parent population using crowded tournament selection, crossover, and mutation operators. This whole operation iterates until it meets a termination criterion. Fig. 2 show the flow-chart of NSGA-II procedure.

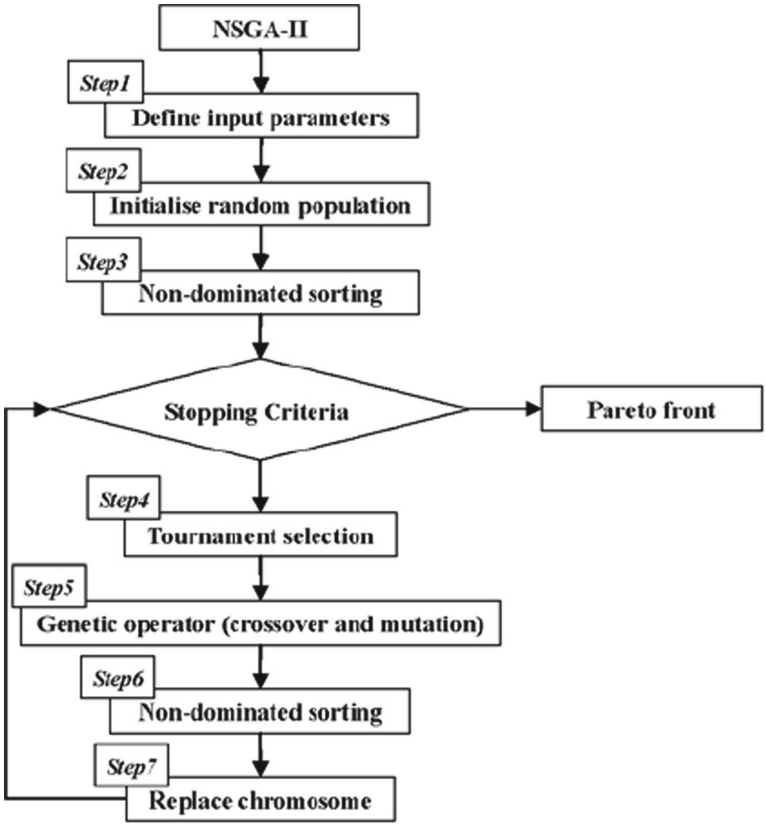

Fig. 2. The flow-chart of the NGSA-II procedure

4 Simulation Results and Discussions

In this section, we present simulation results for problems in Eq.(16) to investigate the secrecy capacity sum of our proposed PD-NOMA/UAV network in the presence of an eavesdropper. Without loss of general, we do experiments for two NOMA users. All of the simulation results are performed in Python language.

To be more detail, the parameters used in this model are the UAV's coverage radius $r = 30m$, height from ground to UAV as $h_{uav} = 50m$, the transmitted power from the UAV as $P_r = 30dBm$, the target secrecy rate R_1 and R_2 in range $[0, 3.5]$ (bits/s/Hz), the signal-decoded threshold at users γ_0 belongs to $[0, 4]$ (dB), path-loss exponent $m = 3$, and Rice coefficient $K = 13$. By applying NSGA-II to address the problem (16), we set up the NSGA-II multi-objective Python program, including maximizing the function of the secrecy capacity sum of the system and minimizing the function of the user's data rate at the eavesdropper.

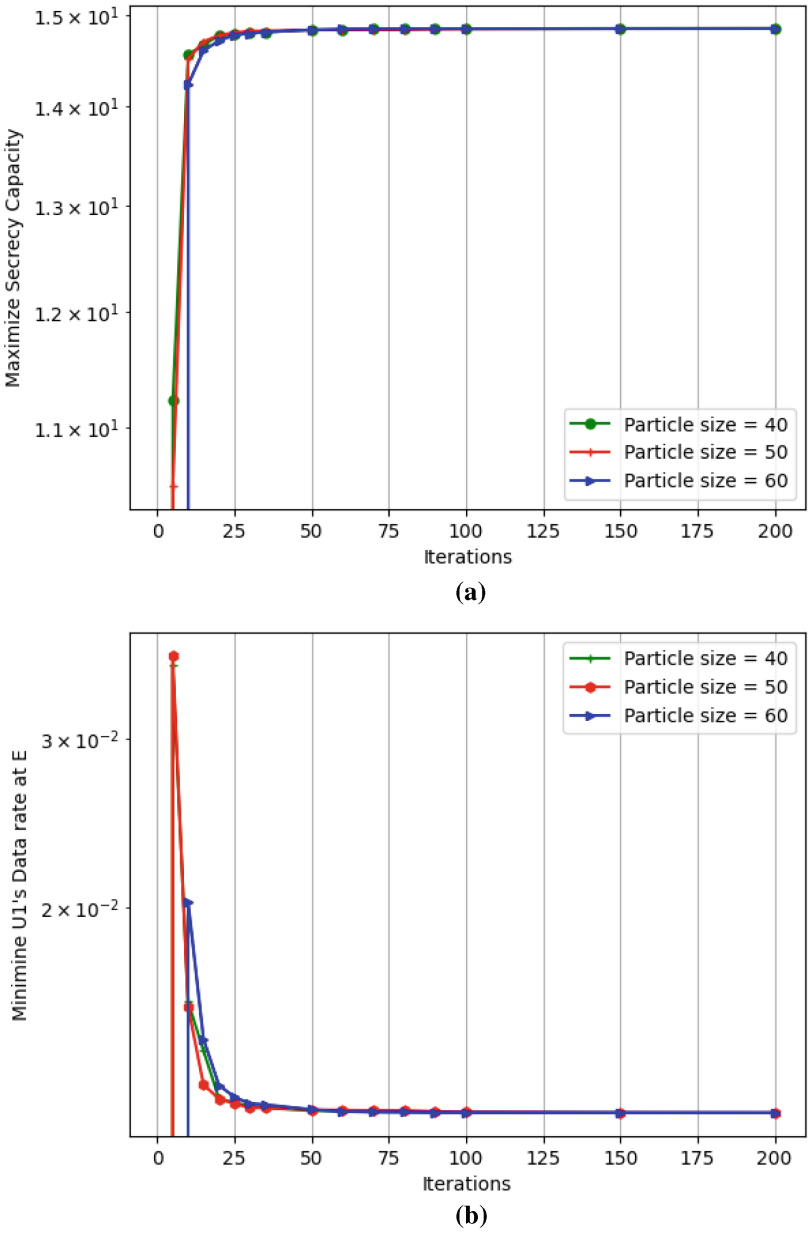

Fig. 3. NSGA-II Convergence behavior

Figure 3 shows the NSGA-II algorithm's convergence behavior of our proposed system model for two objectives: maximization of the secrecy capacity (Fig. 3a) and minimization of user signal at E (Fig. 3b). These figures illustrate

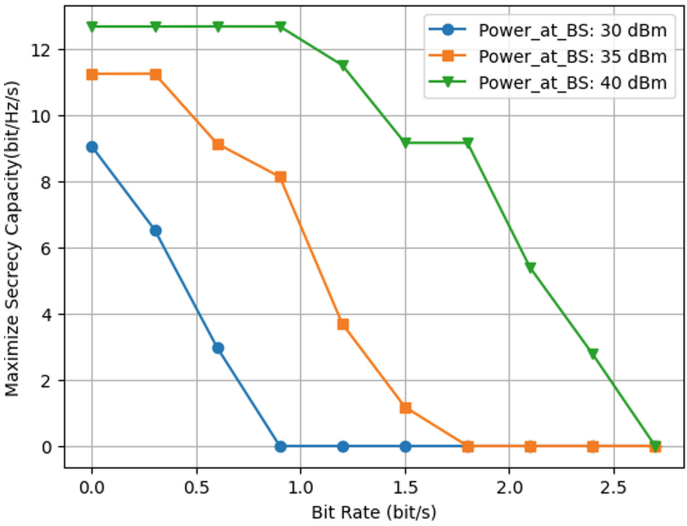

Fig. 4. Sum Secrecy Capacity with different BS's Transmit Powers

three cases of particle size (40,50,60) and two considered-functions for NSGA-II in which all the cases of particle size, the convergence algorithm is archived around iteration 30^{th}. Thus, the convergence of the NSGA-II algorithm in this model system is satisfied.

Then, we investigate the secrecy capacity of the whole proposed system with different BS's transmit power levels and the simulation result in Fig. 4. It is detailed that the increasing value of power level at BS enhances the SSC of the system. In particular, at $P_S = 40dBm$ SSC is better than that of $P_S = 30dBm$.

In Fig. 5, the SSCs are examined with the changes of the heights of UAV (40, 50, 60) m versus the threshold value of users' decoded-signal (γ_0 in the range $[0, 4]$ dB). It can be seen that from Fig. 5, the trends of SSC curves are alike in that SSC descends to zero at around $\gamma_0 = 4dB$ means that if the data rate at users increases the SSC also decreases. Moreover, the SSC of the proposed system model is decreased when the height of the UAV rises.

Figure 6 presents the effect of the strength of the jamming signal from the jammer on the user's data rate at Eavesdropper. Three power levels of Jammer are $P_J = (0,\ 0.5\ {}^*P_S,\ P_S)$ and $P_S = 40dBm$. As shown in Fig. 6, when P_J increases, the user's data rate at E declines. It means that the information of legal users is more secure.

Finally, Fig. 7 investigates the influence of weights of making decisions with data rate minima function at illegal users. The parameters in these simulations are set up as data rate is in the range [0,3.5] bit/s, the transmit power at BS $P_S = 40dBm$, weights for data rate minima function (0.2, 0.6, 0.8). Overall,

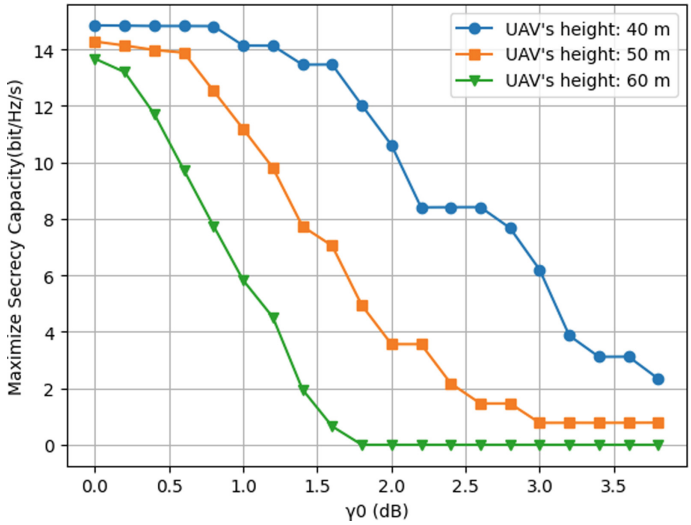

Fig. 5. The height of UAV effect on Sum Secrecy capacity

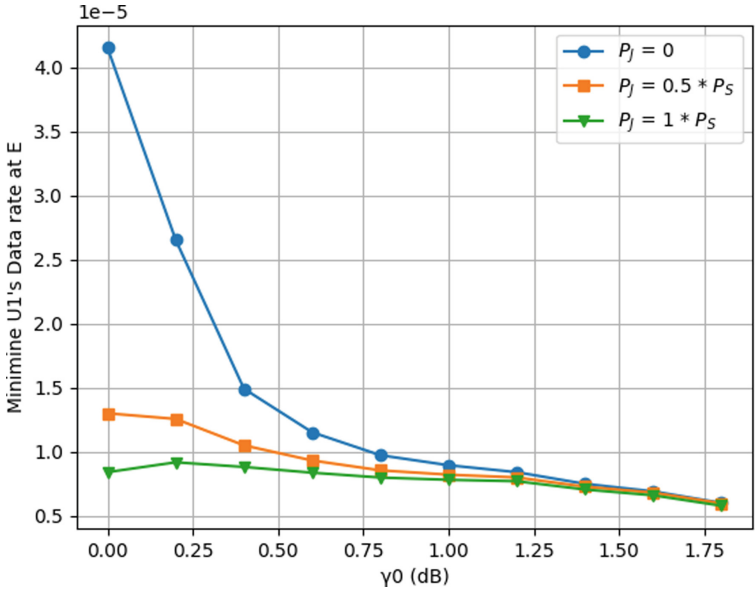

Fig. 6. Effect of Power levels at Jammer on data rate minima function at E

Fig. 6 shows that the trends of SSC lines for all cases are similar. Specifically, It can be seen that the weights of that function slightly increase users' data rate at eavesdroppers.

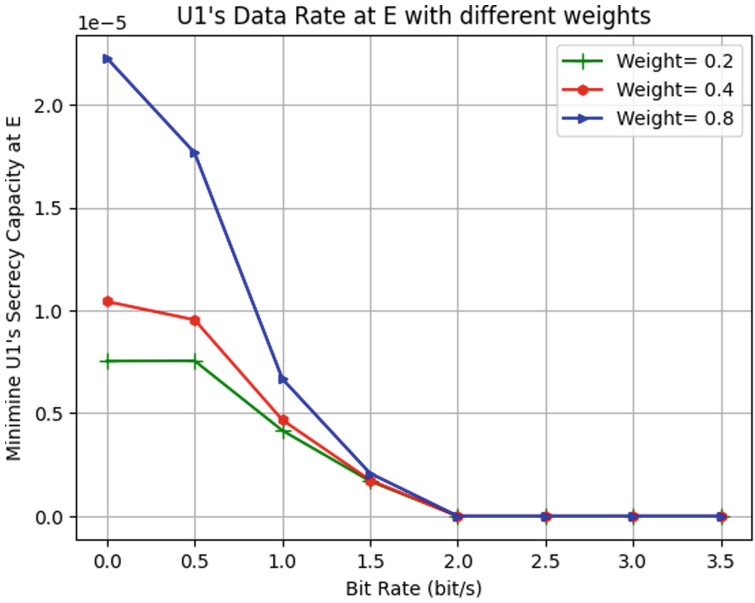

Fig. 7. Weights of Making Decision with data rate minima function at E

5 Conclusion

In this paper, we examined the secrecy capacity sum of the PD-NOMA model system in the UAV-relaying network in the Eavesdropper's occurrence and the assistance of a friendly jammer. In this proposed system design, BTS communicates to multi-NOMA users via the help of a UAV intermediate node. Then, ground-air and air-ground links undergo Rice channels. A friendly jammer broadcasts the jamming signals to interfere with transmitting the Eavesdropper - UAV link. Additionally, to increase the secrecy capacity of our proposed system and decrease the signal at the Eavesdropper, a multi-objective optimization technique - NSGA-II is applied. Finally, the effects of essential system parameters on secrecy capacity are investigated including the transmitted power level, the height of the UAV, the strength of the jamming signal, and the weights of making decisions.

Acknowledgment. This work was supported by Hanoi University of Industry, Hanoi.

References

1. Merwaday, A., Guvenc, I.: UAV-assisted heterogeneous networks for public safety communications. In: 2015 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 329–334 (2015)
2. Li, T., Sheng, M., Lyu, R., Liu, J., Li, J.: UAV assisted heterogeneous wireless networks: potentials and challenges. ZTE Commun. **16** (2018)

3. Ghafoor, U., Ali, M., Khan, H.Z., Siddiqui, A.M., Naeem, M.: NOMA and future 5G and B5G wireless networks: a paradigm. J. Netw. Comput. Appl. 103413 (2022)
4. Le, T.A., Kong, H.Y.: Evaluating the performance of cooperative NOMA with energy harvesting under physical layer security. Wirel. Pers. Commun. **108**, 1037–1054 (2019)
5. Chaudhary, B.P., Shankar, R., Mishra, R.K.: A tutorial on cooperative non-orthogonal multiple access networks. J. Defense Model. Simul. **19**(4), 563–573 (2022)
6. Azam, I., Shahab, M.B., Shin, S.Y.: Energy-efficient pairing and power allocation for NOMA UAV network under QoS constraints. IEEE Internet Things J. **9**(24), 25011–25026 (2022)
7. Huang, Q., Wang, W., Weidang, L., Zhao, N., Nallanathan, A., Wang, X.: Resource allocation for multi-cluster NOMA-UAV networks. IEEE Trans. Commun. **70**(12), 8448–8459 (2022)
8. Li, Y., Wang, W., Liu, M., Nan Zhao, X., Jiang, Y.C., Wang, X.: Joint trajectory and power optimization for jamming-aided NOMA-UAV secure networks. IEEE Syst. J. **17**(1), 732–743 (2022)
9. Chen, B., Li, R., Ning, Q., Lin, K., Han, C., Leung, V.C.: Security at physical layer in NOMA relaying networks with cooperative jamming. IEEE Trans. Veh. Technol. **71**(4), 3883–3888 (2022)
10. Le, T.A., Kong, H.Y.: Secrecy analysis of a cooperative NOMA network using an EH untrusted relay. Int. J. Electron. **106**(6), 799–815 (2019)
11. Wang, J., Zhang, J., Han, M., Pan, G.: Secrecy outage analysis for UAV assisted satellite-terrestrial SWIPT systems with NOMA. Digit. Sign. Process. **123** (2022)
12. Diao, D., Wang, B., Cao, K., Dong, R., Cheng, T.: Enhancing reliability and security of UAV-enabled NOMA communications with power allocation and aerial jamming. IEEE Trans. Veh. Technol. **71**(8), 8662–8674 (2022)
13. Diao, D., Wang, B., Cao, K., Weng, J., Dong, R., Cheng, T.: Secure wireless-powered NOMA communications in multi-UAV systems. IEEE Trans. Green Commun. Networking (2023)
14. Ma, H., Zhang, Y., Sun, S., Liu, T., Shan, Y.: A comprehensive survey on NSGA-II for multi-objective optimization and applications. Artif. Intell. Rev. 1–54 (2023)
15. Deb, K., Pratap, A., Agarwal, S., Meyarivan, T.: A fast and elitist multiobjective genetic algorithm: NSGA-II. IEEE Trans. Evol. Comput. **6**(2), 182–197 (2002). https://doi.org/10.1109/4235.996017