UAV-Assisted Physical Layer Security for Space–Air–Ground Integrated Networks (SAGIN) with Multiple Eavesdroppers

Tinh T. Bui, *Graduate Student Member, IEEE,* Dang Van Huynh, *Member, IEEE,*
Vishal Sharma, *Senior Member, IEEE,* Keshav Singh, *Member, IEEE,* Octavia A. Dobre, *Fellow, IEEE,*
Hyundong Shin, *Fellow, IEEE,* and Trung Q. Duong, *Fellow, IEEE*

***Abstract*—This paper investigates a drone (aka UAV)-assisted physical layer security framework for space–air–ground integrated networks (SAGINs) in the presence of multiple eavesdroppers. A single full-duplex UAV is deployed to support satellite-to-ground communications by simultaneously relaying desired signals to legitimate users and transmitting artificial noise to degrade the reception quality of eavesdroppers. To enhance secure connectivity, we formulate a max–min secrecy rate optimization problem that jointly considers sub-channel allocation and power distribution. The sub-channel allocation is optimized using a constrained genetic algorithm, which efficiently handles the combinatorial nature of the problem. Additionally, power allocation is optimized through a nested-loop approach, in which the outer loop employs Bayesian optimization to address complex objective functions, while the inner loop makes the allocation tractable using variable substitutions and approximation methods to overcome non-convexity. The simulation results demonstrate that the proposed method outperforms the benchmark schemes in terms of secrecy performance, particularly under stringent resource and security constraints in SAGINs.**

***Index Terms*—Space–air–ground integrated networks (SAGINs), physical layer security, max-min optimization, constrained genetic algorithm, approximation optimization**

T. T. Bui, D. V. Huynh, O. A. Dobre are with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1B 3X5, Canada (e-mails: {ttbui, vdhuynh, odobre}@mun.ca).

V. Sharma is with the School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast, BT7 1NN Belfast, UK, (e-mail: v.sharma@qub.ac.uk)

K. Singh is with the Institute of Communications Engineering, National Sun Yat-sen University, Kaohsiung 804, Taiwan (e-mail: keshav.singh@mail.nsysu.edu.tw).

H. Shin is with the Department of Electronics Engineering, Kyung Hee University, Yongin-si, 17104, Korea (e-mail: hshin@khu.ac.kr)

T. Q. Duong is with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1C 5S7, Canada, and with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, BT7 1NN Belfast, U.K., and also with the Department of Electronic Engineering, Kyung Hee University, Yongin-si, Gyeonggi-do 17104, South Korea (e-mail: tduong@mun.ca).

This work was supported in part by the Canada Excellence Research Chair (CERC) Program CERC-2022-00109, in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant Program RGPIN-2025-04941, and in part by NSERC CGV-198798. The work of V. Sharma was supported in part by UKRI in the UKRI-Horizon Europe program with the UKRI reference number 10061165 under MISO project "Autonomous Multi-Format In-Situ Observation Platform for Atmospheric Carbon Dioxide and Methane Monitoring in Permafrost & Wetlands. The work of O. A. Dobre was supported in part by the Canada Research Chair Program CRC-2022-00187. The work of H. Shin was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) under RS-2025-00556064 and RS-2025-25442355.

Corresponding authors are Trung Q. Duong and Hyundong Shin.

I. Introduction

With the progression towards the sixth generation (6G) of wireless networks, physical layer security (PLS) is emerging as a foundational mechanism for protecting data confidentiality in increasingly heterogeneous and ubiquitous communication environments. As communication becomes pervasive across terrestrial, aerial, and space domains, traditional cryptographic protocols face limitations in responsiveness, scalability, and overhead. PLS leverages the intrinsic randomness of wireless channels, such as fading, path loss, and interference, to ensure security at the signal level, independent of computational assumptions. In 6G networks supporting ultra-reliable and low-latency communication (URLLC), the role of massive multiple-input multiple-output (MIMO) and secrecy guard zones has been investigated to mitigate information leakage through analytical derivations of outage metrics and adaptive zone control [1]. Additionally, drone (aka UAV) swarms and distributed systems have introduced group secret key generation protocols using pairwise channel randomness, enhancing multicast and broadcast security [2]. Modern deployments also consider simultaneous wireless information and power transfer (SWIPT) and jamming-enabled secrecy rate maximization, as seen in the integration of intelligent omni-surfaces (IOS) and UAV relays in internet-of-thing (IoT) systems [3].

The role of UAVs in secure wireless networks has drawn significant attention due to their high mobility, favorable line-of-sight (LoS) conditions, and deployment flexibility. UAVs have been used as mobile relays and full-duplex jammers, injecting artificial noise (AN) while forwarding legitimate signals to enhance secrecy rates [4], [5]. Recent efforts incorporate deep learning and dynamic Bayesian inference to enable self-aware UAV radios capable of characterizing jammers and responding proactively to adversarial attacks [6]. Meanwhile, full-duplex millimeter wave (mmWave) orthogonal frequency division multiplexing (OFDM) systems combined with encryption and precoding techniques have been designed for secure color image transmission using UAVs as airborne relays [7]. To meet the confidentiality requirements of cellular-connected UAVs, secure precoding and authentication frameworks based on fingerprint embedding in massive MIMO links have been proposed, which optimize the power split between data and AN [8]. Cooperative rate-splitting (CRS) and robust resource allocation strategies have also been used to address imperfect channel state information (CSI) in UAV-BS networks, ensuring worst-case secrecy fairness among users [9].

Space–air–ground integrated networks (SAGIN) form the core of envisioned 6G architectures, enabling resilient connectivity over diverse devices and terrains. However, integrating heterogeneous links and shared spectrum access introduces significant challenges for secure transmissions. To mitigate these, signal spreading and waveform design strategies such as WFRFT-based complex-valued parallel spreading have been developed to enhance robustness against Doppler distortions and provide PLS in intelligent transportation systems [10]. In addition, generative artificial intelligence (AI)-driven deep reinforcement learning (DRL) has recently been used to jointly optimize trajectory, beamforming, and user association in high-altitude platform (HAP)-aided LEO satellite systems for improving secrecy energy efficiency [11]. Resource slicing and load balancing for SAGIN have also been addressed using multi-agent DRL frameworks that dynamically allocate resources across terrestrial and non-terrestrial layers [12], while label-free deep learning has been explored to optimize secure access point selection under co-channel interference [13]. In [14], [15], generative AI was proposed to be applied in SAGINs with the support of large language model (LLM) and proximal policy optimization (PPO) to build large-scale modeling and optimize the efficiency of resource utilization. A multi-objective reinforcement learning (RL) was applied in large-scale satellite constellations to address conflicts in routing design due to different applications in [16]. Hybrid radio frequency and free-space optical (RF/FSO) relaying, digital twin (DT)-enabled symbiotic security, and hierarchical game models for satellite-terrestrial resource cooperation continue to extend the design space for secure SAGIN deployments [17]–[19]. Regarding optimization, an optimal long-term data offloading scheme was proposed by allocating offloading data and power control in SAGINs, following by an online solution with 2% lower in computation cost compared to the optimal solution [20]. Additionally, in [21], a proposed hashing multi-arm beam training technique, which combines hash functions and antenna responses to build a codebook, achieved 96.4% accuracy and significantly reduced training overhead in SAGINs. In [22], uplink transmission with the combination of ground-air-space and ground-to-space in SAGINs was optimized to improve the network throughput.

A. Literature Review

PLS in SAGINs has received increasing attention since large coverage can expose communications to a higher risk of eavesdropping and interception, especially when satellites and UAVs broadcast signals over wide areas that may include unintended or adversarial receivers [23], [24]. Upper-layer cryptographic schemes in SAGINs face several practical drawbacks. They require frequent key distribution and rekeying, which is difficult over long-delay satellite links and interrupts UAV connections. The encryption and authentication processes require computational resources, which are particularly critical for battery-powered systems with limited onboard processing. In contrast, PLS leverages the physical characteristics of the wireless channel to provide low-complex, key-independent protection that complements upper-layer security [25], [26]. In the context of UAV-assisted communications, recent work has focused on leveraging the mobility and flexibility of UAVs for both signal forwarding and AN generation. A UAV-assisted backscatter communication system was studied in [27], where the UAV optimizes its hovering location, power allocation, and the reflection coefficient of the backscatter device to maximize secrecy rate under a single-eavesdropper scenario. To further enhance security, cooperative jamming strategies were incorporated in ambient backscatter setups, as shown in [28], where secrecy outage probabilities were derived using analytical quadrature methods.

For energy-constrained IoT applications, a double-cluster head model was introduced in [29], where inter-user interference in uplink non-orthogonal multiple access (NOMA) was exploited to obscure eavesdroppers. The study jointly optimized power, time scheduling, and UAV trajectory using alternating optimization with Dinkelbach's method. In another line of work, UAVs serving as decode-and-forward relays with RF energy harvesting capabilities were considered in [30]. Here, secrecy outage and effective secrecy throughput were derived under a composite fading model, and a hybrid particle swarm and genetic algorithm was used for optimization. More advanced secure transceiver designs have also emerged. In [31], a secure DFT-spread OFDM system with frequency-domain shaping and hyperchaotic encryption was proposed for reconfigurable intelligent surface- (RIS) and UAV-assisted terahertz (THz) links. To improve hardware efficiency, UAVs equipped with a one-bit analog-to-digital converter, a digital-to-analog converter, and massive MIMO arrays were analyzed in [32], where beamforming and maximum-ratio combining (MRC) were optimized for satellite-aerial-terrestrial relaying. Meanwhile, secure transmission of UAV control information over NOMA short-packet channels was investigated in [33], where analytical secrecy throughput expressions and block-length optimization were provided under fading environments.

In satellite-supported IoT uplinks, using UAVs to provide secure transmission between IoT devices and satellites was considered in [34]. A two-stage iterative framework combining joint beamforming and power allocation was proposed to maximize the minimum secrecy rate across users. Similarly, UAVs were deployed to assist satellite-to-vehicle communications in [4], where joint satellite beamforming and UAV power allocation were optimized through semi-definite relaxation and fractional programming to enhance secrecy while meeting quality of service (QoS) constraints. Robust secure communication under imperfect CSI was addressed using rate-splitting in [9], where the UAV base station splits messages into private and shared parts and forwards them to edge users, acting also as AN sources. In cellular-connected UAV scenarios, secure transmission and authentication were jointly considered in [8], which proposed a fingerprint-embedded linear precoder for massive MIMO systems, optimizing the power split between data and noise under Rician fading.

Further contributions have focused on encrypted UAV relaying for multimedia transmissions. A full-duplex mmWave OFDM system with joint peak to average power ratio (PAPR) reduction, channel coding, and encrypted precoding was introduced in [7] to enable secure color image transmission. To support low-power IoT devices, an IOS-UAV system was proposed in [3], in which the UAV acted simultaneously as a jammer and power supplier. A joint optimization of trajectory, phase shifts, and power was solved using successive convex approximation. Beyond physical-layer techniques, cognitive radio-inspired frameworks were proposed in [6], where a hierarchical dynamic Bayesian network was used to empower UAVs with self-awareness to detect and counteract jamming behavior. In [5], the dual-hop UAV relay network was analyzed under per-hop eavesdropping and imperfect CSI. Intercept probabilities were derived for both static and mobile nodes, revealing secrecy degradation due to channel estimation errors and Doppler effects. UAV swarms have also been considered for secure group communications. A sequential secret group key generation algorithm using network coding and partial pairwise key exchange was presented in [2], effectively balancing redundancy and overhead. In addition, the secrecy performance of UAV-enabled URLLC was studied in [1], where the introduction of a guard zone and massive MIMO reduced the connection and secrecy outage probabilities under LoS/non-line-of-sight (NLoS) channel models.

In parallel, PLS research in SAGIN environments has advanced considerably. For example, a complex-valued WFRFT-based spectrum spreading approach was proposed in [10] to address Doppler distortions and enable flexible signal shaping for ITS applications. To address dynamic SAGIN topologies, a generative AI-based DRL framework was introduced in [11]. The proposed Gen-DRL jointly optimizes UAV trajectory, user association, and beamforming to improve secrecy energy efficiency in downlink communications. Resource slicing and prioritized load balancing were studied in [12], where a multi-agent deep deterministic policy gradient (DDPG) framework was used to coordinate user-BS associations and UAV/satellite access under cross-layer priority constraints. For secure access point selection, a label-free deep learning model was proposed in [13], which employed Q-network approximation and unsupervised power optimization to improve secrecy rate under co-channel interference. Efficient latency-aware resource orchestration was addressed in [35], where DRL was applied to a multidomain virtual network embedding problem in SAGIN, considering traffic size and hop count.

More recently, DT-enabled symbiotic security was explored in [18]. A DT-controlled synergy precoding scheme was designed to recast co-channel interference into an asymmetric disturbance for eavesdroppers while maximizing minimum secrecy rates across the space, air, and ground segments. Hybrid RF/FSO relaying schemes were proposed in [17], where UAVs transmitted secure information to satellites over FSO links after injecting AN in RF uplinks. Trajectory and power allocation were jointly optimized via block coordinate descent and successive convex approximation. Resource fairness in cognitive satellite-terrestrial networks was studied in [19], which proposed a hierarchical game combining coalition formation and Stackelberg dynamics to ensure cooperation between satellite and terrestrial nodes while maintaining secrecy.

In summary, existing research has made substantial progress in enhancing PLS for UAV-assisted and SAGIN-based wireless networks through advanced signal processing, intelligent control, and optimization frameworks. However, most studies focus on single-domain scenarios, assume limited eavesdropper models, or overlook the joint design of sub-channel allocation, UAV cooperation, and power control in integrated satellite-terrestrial systems. This highlights the need for a more holistic and robust security framework capable of addressing multiple eavesdroppers in a fully integrated SAGIN environment.

B. Motivation and Contributions

Despite growing efforts to secure SAGINs, existing approaches often make simplifying assumptions that limit their practical applicability. Most notably, the majority of current works consider a single eavesdropper without fully capturing the complex integration of satellite, UAV, and terrestrial networks [4], [27]. For example, in [36], a system model was proposed in which a satellite serves multiple ground users and a UAV is used as an AN source to confuse an eavesdropper; however, this approach is inefficient in scenarios of multiple existing eavesdroppers. While important studies have explored advanced relay-jamming strategies [29], [30] or learning-based secure access in SAGINs [11], [13], they generally fall short of jointly optimizing limited resources such as sub-channel assignment and power allocation in the presence of multiple simultaneous eavesdroppers. Furthermore, the full-duplex capability of UAVs - an enabler for concurrent signal forwarding and AN injection - remains underexplored in the context of multi-user secrecy enhancement. These limitations create an urgent need for a more comprehensive security framework tailored to SAGINs. This work aims to bridge that gap by developing a UAV-assisted PLS scheme to support the main satellite communications for maximizing the minimum secrecy rate across all legitimate users while actively mitigating the threat of multiple eavesdroppers through optimal resource allocation.

In this paper, we investigate a UAV-assisted PLS framework for SAGINs under the presence of multiple eavesdroppers. A single UAV, operating in full-duplex mode, is deployed to assist communication from the satellite to ground users. The UAV simultaneously acts as a cooperative relay to improve legitimate users' signal quality and emits AN to degrade the eavesdroppers' channels. The main contributions of this paper are as follows:

- The proposed system model of SAGINs can be robust to the scenarios of the appearance of multiple eavesdroppers. The UAV operates in orthogonal sub-channels to improve the network secrecy rate by enhancing desired signals and reducing stolen data.
- A max-min secrecy rate optimization problem is formulated to focus on protecting the most at-risk user with the aim of secrecy fairness across users through joint optimization of sub-channel allocation and power allocation. The problem is built in a complex environment of interference between users, the UAV, and the satellite in multiple sub-channels. In addition, stringent constraints are added to guarantee the quality of services, including

security and satisfied data rate, with feasible transmit power values.

- A constrained genetic algorithm (GA) is designed to address the first sub-problem of sub-channel allocation, which is an integer programming. We propose encoding and decoding processes to avoid the inefficient evolution of the chromosome population. Four operations of evaluation, selection, crossover, and mutation are designed to find the optimal solution.
- Regarding power allocation, a nested-loop algorithm that consists of Bayesian optimization as outer loops and approximation methods as inner loops is proposed. Our method addresses the challenges of resource coupling, full-duplex operations, and the complex interference environment in SAGINs. Consequently, the efficiency of the proposed method is proven through the comparison with benchmark schemes to formulate secured SAGINs.

C. Paper Structure and Notations

The remainder of this study is arranged as follows: Section II presents the system model and transmission scheme, where we build the channel models and formulate the signal-to-interference-plus-noise ratios (SINRs) of users and eavesdroppers. The optimization problem to maximize the minimum secrecy rate is formulated in Section III. Additionally, Section IV describes the optimization methods, including the constrained GA and the nested-loop algorithm, while the simulation results are provided and analyzed in Section V. Finally, we summarize our findings, contributions, and suggest some potential directions to extend the study in Section VI.

The following notations are adopted throughout this paper. The Euclidean norm of a vector $\boldsymbol{x}$ is denoted by $\|\boldsymbol{x}\|$. The logarithm function with base two is written as $\log_2(\cdot)$, while $\log_{10}(\cdot)$ denotes the logarithm function with base ten. For a complex quantity, $\Re(\cdot)$ and $\Im(\cdot)$ denote its real and imaginary parts, respectively. The conjugate and Hermitian (conjugate transpose) of a matrix $\boldsymbol{X}$ are represented by $\boldsymbol{X}^*$ and $\boldsymbol{X}^\dagger$, respectively. Meanwhile, Null$\{\boldsymbol{X}\}$ denotes the null-space of matrix $\boldsymbol{X}$. Furthermore, max$(\boldsymbol{X})$ represents the maximum value of all elements in matrix or set $\boldsymbol{X}$, and $[x]^+$ is the maximum value of x and 0. $|\cdot|$ denotes either the absolute value (for scalars).

II. System Model and Transmission Scheme

In this paper, we propose a UAV-assisted PLS in a SAGIN depicted in Fig. 1. There is one satellite serving many ground users, including legitimate users (attacked) and normal users. In this scenario, the network is wiretapped by several eavesdroppers simultaneously. One UAV is used to support the network by acting as a full-duplex relay to enhance the signal quality of legitimate users and transmitting AN in order to confuse eavesdroppers.

The satellite is equipped with N_S antennas while the UAV has one omnidirectional antenna for receiving signals from the satellite and N_U antennas for transmitting signals and noise to users and eavesdroppers. The total bandwidth is divided into N parts, corresponding to N orthogonal sub-channels. The set of normal users that are not wiretapped by any eavesdropper is denoted by $\mathcal{K}_N = \{1, \dots, k_N, \dots, K_N\}$. Additionally, the set of legitimate users that eavesdroppers wiretap is given by $\mathcal{K}_W = \{1, \dots, k_W, \dots, K_W\}$ with $K_W \leq N$, and the set of eavesdroppers is $\mathcal{M} = \{1, \dots, m, \dots, M\}$ with the assumption of one legitimate users attacked by one eavesdropper. All users and eavesdroppers are equipped with one antenna. The locations of the satellite, the UAV, and the k-th ground user are denoted by $\boldsymbol{q}_s = [x_s, y_s, z_s]$, $\boldsymbol{q}_u = [x_u, y_u, z_u]$, and $\boldsymbol{q}_k = [x_k, y_k, 0]$, respectively.

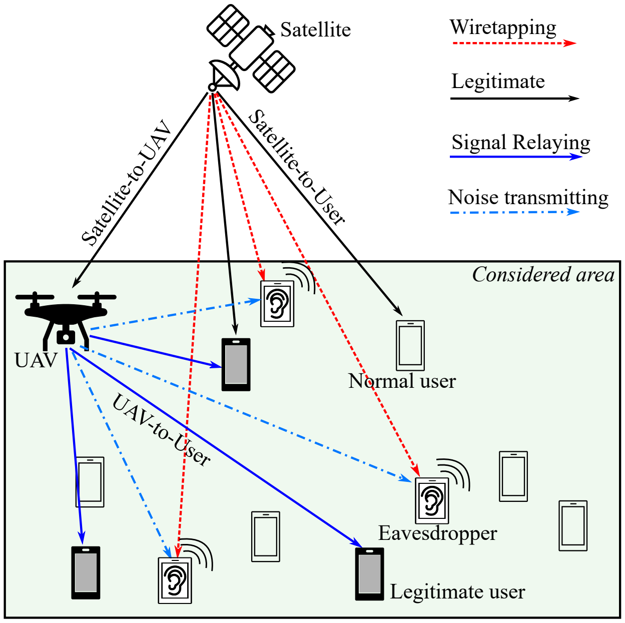

Fig. 1. A typical satellite-air-ground integrated networks.

A. Channel Model

1) Satellite-to-UAV Channel: The shadowed-Rician fading (SRF) model serves as an appropriate representation for the channel characteristics between low Earth orbit (LEO) satellites and UAVs [37]. The channel vector from the satellite to the UAV is expressed as

$$\boldsymbol{h}_{s,u}^{(n)} = [h_i^{(n)}]_{i=\overline{1,N_S}}, \tag{1}$$

where each element $h_i^{(n)}$ represents the channel coefficient from the i^{th} antenna of the satellite to the UAV and is defined by $h_i^{(n)} = \sqrt{g_i^{(n)} d_{s,u}^{-\alpha^{(1)}}}$. Here, $d_{s,u}$ denotes the distance between the satellite and UAV, while $\alpha^{(1)}$ is the associated path loss exponent. The term $g_i^{(n)}$ follows a shadowed-Rician distribution, denoted as SR$(\omega_i, \delta_i, \varepsilon_i)$, where ω_i indicates the mean power of the LoS component, δ_i is half the mean power of the scattered components, and ε_i characterises the Nakagami-m fading effect.

2) Satellite-to-User Channel: The channel between the UAV and ground users is modelled by incorporating both large-scale and small-scale fading effects. The large-scale fading is determined by a free-space path-loss model with a path-loss exponent of $\alpha^{(2)}$, and it accounts for the distance between the UAV and each user, as well as the carrier frequency f_c. The large-scale path loss in dB is calculated as

$$\mathrm{PL}_{s,k} = 10\alpha^{(2)} \log_{10}\left(\frac{4\pi f_c d_{s,k}}{c}\right), \tag{2}$$

where $d_{s,k}$ is the distance from the satellite to user k, c is the speed of light. The small-scale fading is modeled as Rayleigh fading, represented by a complex Gaussian random vector $\boldsymbol{g}_{s,k} \in \mathbb{C}^{1\times N_U}$ for user k on sub-channel n, where each element is drawn from $\mathcal{CN}(0,1)$. The channel vector between the satellite and the kth user can be given as

$$\boldsymbol{h}_{s,k}^{(n)} = \sqrt{10^{-\mathrm{PL}_{s,k}/10}}\boldsymbol{g}_{s,k}. \tag{3}$$

3) UAV-to-User Channel: The channel gain from the UAV to user k can be defined as

$$\boldsymbol{h}_{u,k}^{(n)} = \boldsymbol{g}_{u,k}\left(\frac{\lambda_c}{4\pi d_{u,k}}\right)^{\dfrac{\alpha^{(3)}}{2}} 10^{-\dfrac{c^{\mathrm{LoS}} Pr_{u,k}^{\mathrm{LoS}} + c^{\mathrm{NLoS}} Pr_{u,k}^{\mathrm{NLoS}}}{20}}, \tag{4}$$

where $\lambda_c = c/f_c$ is the wavelength, $\boldsymbol{g}_{u,k} \in \mathbb{C}^{N_U}$ denotes the small-scale fading vector corresponding to the channel between the UAV and user k. The parameter α represents the path loss exponent. The constants c^{LoS} and c^{NLoS} are weighting factors used to account for LoS and NLoS propagation conditions, respectively. Furthermore, $Pr_{u,k}^{\mathrm{LoS}}$ and $Pr_{u,k}^{\mathrm{NLoS}}$ denote the probabilities of LoS and NLoS links, with the constraint that $Pr_{u,k}^{\mathrm{LoS}} + Pr_{u,k}^{\mathrm{NLoS}} = 1$.

B. Transmission Model

Without loss of generality, we assume that there is only one eavesdropper m that illegally tries to eavesdrop on the data of a legitimate user k_W ($K_W \leq N$) in one sub-channel n. The satellite transmits the signal to all users using the maximum ratio transmission (MRT) precoding technique and simultaneously creates beams toward the UAV to emit the enhanced signal for legitimate users. Therefore, the transmitted signal at the satellite in the sub-channel n is expressed as

$$\begin{aligned}\boldsymbol{x}_s^{(n)} = &\textstyle\sum_{k_N\in\mathcal{K}_N} \varphi_{s,k_N}^{(n)} \boldsymbol{w}_{s,k_N}^{(n)} s_{s,k_N} \\ &+ \textstyle\sum_{k_W\in\mathcal{K}_W} \eta_{s,u,k_W}^{(n)} (\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)}) s_{s,k_W},\end{aligned} \tag{5}$$

where $\boldsymbol{w}_{s,k_N}^{(n)}$, $\boldsymbol{w}_{s,k_W}^{(n)}$, and $\boldsymbol{w}_{s,u}^{(n)}$ represent the precoding vectors at the satellite to generate a beam toward normal user k_N, legitimate user k_W, and the UAV, respectively ($\boldsymbol{w}_{s,k_N}^{(n)} = \sqrt{p_{s,k_N}^{(n)}}\boldsymbol{h}_{s,k_N}^{(n)}{}^{\dagger}/\|\boldsymbol{h}_{s,k_N}^{(n)}\|$, $\boldsymbol{w}_{s,k_W}^{(n)} = \sqrt{p_{s,k_W}^{(n)}}\boldsymbol{h}_{s,k_W}^{(n)}{}^{\dagger}/\|\boldsymbol{h}_{s,k_W}^{(n)}\|$, and $\boldsymbol{w}_{s,u}^{(n)} = \sqrt{p_{s,u}^{(n)}}\boldsymbol{h}_{s,u}^{(n)\dagger}/\|\boldsymbol{h}_{s,u}^{(n)}\|$); $s_{s,k}$ is the required signal of user k with the assumption of $\|s_{s,k}\|^2 = 1$. Binary variable $\varphi_{s,k_N}^{(n)} = 1$ when normal user k_N is served by the satellite in sub-channel n, and otherwise. Binary variable $\eta_{s,u,k_W}^{(n)} = 1$ when a legitimate user k_W, who is wiretapped in sub-channel n, receives the direct signal from the satellite and the relay signal from the UAV, and otherwise. The signal received at the UAV is given by

$$\begin{aligned}y_u^{(n)} = \boldsymbol{h}_{s,u}^{(n)}\boldsymbol{x}_s^{(n)} + \nu + n_u = \sum_{k_N\in\mathcal{K}_N} \varphi_{s,k_N}^{(n)} \boldsymbol{h}_{s,u}^{(n)} \boldsymbol{w}_{s,k_N}^{(n)} s_{s,k_N} \\ + \sum_{k_W\in\mathcal{K}_W} \eta_{s,u,k_W}^{(n)} \boldsymbol{h}_{s,u}^{(n)} (\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)}) s_{s,k_W} + \nu + n_u,\end{aligned} \tag{6}$$

where the residual self-interference in full-duplex mode after self-interference cancellation is represented by $\nu \sim CN(0,\sigma_\nu^2)$ [38], and $n_u \sim CN(0,\sigma_u^2)$ denotes the additive white Gaussian noise (AWGN) at the UAV. The transmitted signal at the UAV in sub-channel n is expressed as

$$\begin{aligned}\boldsymbol{x}_u^{(n)} &= \sum_{k_U\in\mathcal{K}_W} \eta_{s,u,k_U}^{(n)} (\boldsymbol{f}_{u,k_U}^{(n)} y_u^{(n)} + \boldsymbol{G}_{u,k_U}^{(n)} \boldsymbol{v}_u^{(n)}) \\ &= \sum_{\substack{k_U\in\mathcal{K}_W \\ k_N\in\mathcal{K}_N}} \eta_{s,u,k_U}^{(n)} \boldsymbol{f}_{u,k_U}^{(n)} \varphi_{s,k_N}^{(n)} \boldsymbol{h}_{s,u}^{(n)} \boldsymbol{w}_{s,k_N}^{(n)} s_{s,k_N} \\ &+ \sum_{k_U\in\mathcal{K}_W} \eta_{s,u,k_U}^{(n)} \boldsymbol{f}_{u,k_U}^{(n)} \boldsymbol{h}_{s,u}^{(n)} (\boldsymbol{w}_{s,k_U}^{(n)} + \boldsymbol{w}_{s,u}^{(n)}) s_{s,k_U} \\ &+ \sum_{k_U\in\mathcal{K}_W} \eta_{s,u,k_U}^{(n)} \boldsymbol{f}_{u,k_U}^{(n)} (\nu + n_u) + \sum_{k_U\in\mathcal{K}_W} \eta_{s,u,k_U}^{(n)} \boldsymbol{G}_{u,k_U}^{(n)} \boldsymbol{v}_u^{(n)},\end{aligned} \tag{7}$$

where $\boldsymbol{f}_{u,k_U}^{(n)} \in \mathbb{C}^{N_U\times 1}$ is the precoding vector of the UAV in sub-channel n referred to null-space precoding and is expressed as

$$\boldsymbol{f}_{u,k_U}^{(n)} = \beta_{u,1}^{(n)} \mathrm{Null}\{\boldsymbol{H}_{u,\mathcal{M}}^{(n)}\}, \tag{8}$$

where $\beta_{u,1}^{(n)}$ is the power scaling coefficient used at the UAV for relaying the received signal, $\boldsymbol{H}_{u,\mathcal{M}}$ is the channel matrix from the UAV to M eavesdroppers, $\boldsymbol{f}_{u,k_U}^{(n)}$ is designed to cancel all the desired information to eavesdroppers. $\boldsymbol{v}_u^{(n)} \in \mathbb{C}^{N_U\times 1}$ represents the vector of independent and identically distributed AN with the element $v_i \sim CN(0, 1/N_U)$; and

$$\boldsymbol{G}_{u,k_U}^{(n)} = \beta_{u,2}^{(n)} \mathrm{Null}\{\boldsymbol{H}_{u,\mathcal{K}_W}^{(n)}\} \boldsymbol{h}_{u,m\to k_U}^{(n)}{}^{\dagger} / \|\boldsymbol{h}_{u,m\to k_U}^{(n)}\|, \tag{9}$$

where $\boldsymbol{H}_{u,\mathcal{K}_W}$ is the channel matrix from the UAV to K_W legitimate users, $\boldsymbol{h}_{u,m\to k_U}^{(n)}$ being the channel vector from the UAV to eavesdropper m which tries to wiretap the legitimate user k_U. With the design of $\boldsymbol{G}_{u,k_U}^{(n)}$, the quality of the signal of legitimate users is guaranteed since the AN from the UAV is completely canceled in sub-channel n.

Following [4], we assume that the direct satellite signal and the relayed UAV signal arrive synchronously at both legitimate users and eavesdroppers. In addition, consistent with [1], [4], [8], the core network is assumed to have perfect CSI of all legitimate users and eavesdroppers. Under these assumptions, the received signal at user k_W is expressed in (10), while the received signal at eavesdropper m, which tries to wiretap the user k_W, is given in (11). The received signal at normal user k_N, which is not eavesdropped by any eavesdropper, is expressed in (12). The SINRs of legitimate user k_W, eavesdropper m, and normal user k_N are formulated as in (13), (14), and (15), respectively. In detail, the desired signal of legitimate user k_W is the combination of the signals from the satellite and the relay from the UAV. The eavesdropper

$$\begin{aligned}
y_{k_W}^{(n)} &= \boldsymbol{h}_{s,k_W}^{(n)}\boldsymbol{x}_s^{(n)} + \boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{x}_u^{(n)} + n_{k_W} \\
&= \sum_{k'_N\in\mathcal{K}_N} \boldsymbol{h}_{s,k_W}^{(n)}\varphi_{s,k'_N}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}s_{s,k'_N} + \boldsymbol{h}_{s,k_W}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})s_{s,k_W} + \sum_{k'_N\in\mathcal{K}_N} \boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}\varphi_{s,k'_N}^{(n)}\boldsymbol{h}_{s,u}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}s_{s,k'_N} \\
&+ \boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}\boldsymbol{h}_{s,u}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})s_{s,k_W} + \boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}(\nu + n_u) + n_{k_W}
\end{aligned} \tag{10}$$

$$\begin{aligned}
y_{m\to k_W}^{(n)} &= \boldsymbol{h}_{s,m}^{(n)}\boldsymbol{x}_s^{(n)} + \boldsymbol{h}_{u,m}^{(n)}\boldsymbol{x}_u^{(n)} + n_m \\
&= \sum_{k'_N\in\mathcal{K}_N} \boldsymbol{h}_{s,m}^{(n)}\varphi_{s,k'_N}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}s_{s,k'_N} + \boldsymbol{h}_{s,m}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})s_{s,k_W} + \boldsymbol{h}_{u,m}^{(n)}\boldsymbol{G}_{u,k_W}^{(n)}\boldsymbol{v}_u^{(n)} + n_m
\end{aligned} \tag{11}$$

$$\begin{aligned}
y_{k_N}^{(n)} &= \boldsymbol{h}_{s,k_N}^{(n)}\boldsymbol{x}_s^{(n)} + \boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{x}_u^{(n)} + n_{k_N} \\
&= \sum_{k'_N\in\mathcal{K}_N} \boldsymbol{h}_{s,k_N}^{(n)}\varphi_{s,k'_N}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}s_{s,k'_N} + \sum_{k'_W\in\mathcal{K}_W} \boldsymbol{h}_{s,k_N}^{(n)}\eta_{s,u,k'_W}^{(n)}(\boldsymbol{w}_{s,k'_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})s_{s,k'_W} \\
&+ \sum_{k'_U\in\mathcal{K}_W}^{k'_N\in\mathcal{K}_N} \boldsymbol{h}_{u,k_N}^{(n)}\eta_{s,u,k'_U}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}\varphi_{s,k'_N}^{(n)}\boldsymbol{h}_{s,u}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}s_{s,k'_N} + \sum_{k'_U\in\mathcal{K}_W} \boldsymbol{h}_{u,k_N}^{(n)}\eta_{s,u,k'_U}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}\boldsymbol{h}_{s,u}^{(n)}(\boldsymbol{w}_{s,k'_U}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})s_{s,k'_U} \\
&+ \sum_{k'_U\in\mathcal{K}_W} \boldsymbol{h}_{u,k_N}^{(n)}\eta_{s,u,k'_U}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}(\nu + n_u) + \sum_{k'_U\in\mathcal{K}_W} \boldsymbol{h}_{u,k_N}^{(n)}\eta_{s,u,k'_U}^{(n)}\boldsymbol{G}_{u,k'_U}^{(n)}\boldsymbol{v}_u^{(n)} + n_{k_N}
\end{aligned} \tag{12}$$

$$\gamma_{k_W} = \frac{|(\boldsymbol{h}_{s,k_W}^{(n)} + \boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}\boldsymbol{h}_{s,u}^{(n)})(\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})|^2}{\sum_{k'_N\in\mathcal{K}_N}\varphi_{s,k'_N}^{(n)}|(\boldsymbol{h}_{s,k_W}^{(n)} + \boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}\boldsymbol{h}_{s,u}^{(n)})\boldsymbol{w}_{s,k'_N}^{(n)}|^2 + |\boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}|^2(\sigma_\nu^2 + \sigma_u^2) + \sigma_{k_W}^2} \tag{13}$$

$$\gamma_{m\to k_W} = \frac{|\boldsymbol{h}_{s,m}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})|^2}{\sum_{k'_N\in\mathcal{K}_N}\varphi_{s,k'_N}^{(n)}|\boldsymbol{h}_{s,m}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}|^2 + |\boldsymbol{h}_{u,m}^{(n)}\boldsymbol{G}_{u,k_W}^{(n)}\boldsymbol{v}_u^{(n)}|^2 + \sigma_m^2} \tag{14}$$

$$\gamma_{k_N} = \frac{|(\boldsymbol{h}_{s,k_N}^{(n)} + \sum_{k'_U\in\mathcal{K}_W}\boldsymbol{h}_{u,k_N}^{(n)}\eta_{s,u,k'_U}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}\boldsymbol{h}_{s,u}^{(n)})\boldsymbol{w}_{s,k_N}^{(n)}|^2}{I_{s,k_N} + I_{u,k_N} + \sigma_{k_N}^2} \tag{15}$$

where the formulas I_{s,k_N} and I_{u,k_N}, denoting the interference received from the satellite and the UAV, are defined as follows

$$\begin{aligned}
I_{s,k_N} = &\sum_{k'_N\in\mathcal{K}_N\setminus k_N}\varphi_{s,k'_N}^{(n)}|(\boldsymbol{h}_{s,k_N}^{(n)} + \sum_{k'_U\in\mathcal{K}_W}\boldsymbol{h}_{u,k_N}^{(n)}\eta_{s,u,k'_U}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}\boldsymbol{h}_{s,u}^{(n)})\boldsymbol{w}_{s,k'_N}^{(n)}|^2 \\
&+ \sum_{k'_W\in\mathcal{K}_W}\eta_{s,u,k'_W}^{(n)}|(\boldsymbol{h}_{s,k_N}^{(n)} + \boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{f}_{u,k'_W}^{(n)}\boldsymbol{h}_{s,u}^{(n)})(\boldsymbol{w}_{s,k'_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})|^2
\end{aligned}$$

and $I_{u,k_N} = \sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}|\boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}|^2(\sigma_\nu^2 + \sigma_u^2) + \sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}|\boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{G}_{u,k'_U}^{(n)}\boldsymbol{v}_u^{(n)}|^2.$

m receives the high interference (i.e., AN) from the UAV, causing a decrease in illegal data received. Also, a normal user k_N receives the signals from both the satellite and the UAV, which consist of its desired data and interference. Therefore, the secrecy rate of user k_W is defined as

$$SR_{k_W} = B[\log_2(1+\gamma_{k_W}) - \log_2(1+\gamma_{m\to k_W})]^+, \tag{16}$$

where B is the bandwidth per sub-channel. Additionally, the data rate of normal user k_N is given as

$$R_{k_N} = B\log_2(1+\gamma_{k_N}). \tag{17}$$

III. Problem Formulation

In this paper, the objective is to maximize the minimum secrecy rate of all legitimate users under the constraints of sub-channel allocation, UAV association, and power allocation. The max-min secrecy rate formulation is adopted to guarantee fairness between legitimate users by maximizing the secrecy rate of the user with the lowest security. While this has a high probability of not maximizing the overall network throughput, it prevents situations where some legitimate users have very high secrecy rates, and the others are completely insecure. In detail, in the overall network throughput maximization problem, legitimate users with higher path-loss channels will be allocated minimum power from base stations, while our proposed max-min secrecy rate optimization will focus on the legitimate user with the minimum secrecy rate, resulting in improving the security of all legitimate users. The optimization problem is formulated as

$$\max_{\boldsymbol{P}_s,\boldsymbol{\beta}_u,\boldsymbol{\varphi},\boldsymbol{\eta}} \quad \min_{k_W\in\mathcal{K}_W} SR_{k_W} \tag{18a}$$

$$\text{s.t. } \Psi_s(\boldsymbol{P}_s,\boldsymbol{\beta}_u,\boldsymbol{\varphi},\boldsymbol{\eta}) \leq P_s^{(\max)}, \tag{18b}$$

$$\Psi_u(\boldsymbol{P}_s,\boldsymbol{\beta}_u,\boldsymbol{\varphi},\boldsymbol{\eta}) \leq P_u^{(\max)}, \tag{18c}$$

$$SR_{k_W} \geq SR_{min}, \forall k_W \in \mathcal{K}_W, \tag{18d}$$

$$R_{k_N} \geq R_{min}, \forall k_N \in \mathcal{K}_N, \tag{18e}$$

$$\sum\nolimits_{k_W\in\mathcal{K}_W} \eta_{s,u,k_W}^{(n)} \leq 1, \forall n, \tag{18f}$$

$$\sum\nolimits_{n=1}^{N} \eta_{s,u,k_W}^{(n)} = 1, \forall k_W \in \mathcal{K}_W, \tag{18g}$$

$$\sum\nolimits_{n=1}^{N} \varphi_{s,k_N}^{(n)} = 1, \forall k_N \in \mathcal{K}_N, \tag{18h}$$

$$\boldsymbol{P}_s, \boldsymbol{\beta}_u \geq 0, \boldsymbol{\varphi}, \boldsymbol{\eta} \in \{0,1\}, \tag{18i}$$

where $P_s^{(\max)}$ and $P_u^{(\max)}$ are the maximum transmit power of the satellite and the UAV, respectively, R_{min} is the minimum data rate required for all normal users, and SR_{min} is the minimum secrecy rate required by the networks. The sum of actual transmit power at the satellite and the UAV is expressed, respectively, as follows:

$$\Psi_s(\boldsymbol{P}_s,\boldsymbol{\beta}_u,\boldsymbol{\varphi},\boldsymbol{\eta}) = \sum_{n=1}^{N} \Bigg(\sum_{k_N\in\mathcal{K}_N} \varphi_{s,k_N}^{(n)} p_{s,k_N}^{(n)} + \sum_{k_W\in\mathcal{K}_W} \eta_{s,u,k_W}^{(n)} \|\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)}\|^2 \Bigg), \tag{19}$$

$$\begin{aligned}
&\Psi_u(\boldsymbol{P}_s,\boldsymbol{\beta}_u,\boldsymbol{\varphi},\boldsymbol{\eta}) \\
&= \sum_{n=1}^{N} \Bigg(\sum_{\substack{k_U\in\mathcal{K}_W \\ k_N\in\mathcal{K}_N}} \eta_{s,u,k_U}^{(n)} \varphi_{s,k_N}^{(n)} \|\boldsymbol{f}_{u,k_U}^{(n)} \boldsymbol{h}_{s,u}^{(n)} \boldsymbol{w}_{s,k_N}^{(n)}\|^2 \\
&+ \sum_{k_U\in\mathcal{K}_W} \eta_{s,u,k_U}^{(n)} \|\boldsymbol{f}_{u,k_U}^{(n)} \boldsymbol{h}_{s,u}^{(n)} (\boldsymbol{w}_{s,k_U}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})\|^2 \\
&+ \sum_{k_U\in\mathcal{K}_W} \eta_{s,u,k_U}^{(n)} (\|\boldsymbol{f}_{u,k_U}^{(n)}\|^2 (\sigma_\nu^2 + \sigma_u^2) + \|\boldsymbol{G}_{u,k_U}^{(n)} \boldsymbol{v}_u^{(n)}\|^2) \Bigg).
\end{aligned} \tag{20}$$

In the optimization problem (18), constraints (18b) and (18c) indicate the maximum sum of transmit power of the satellite and the UAV, respectively. The security performance of the network is guaranteed through constraints (18d) while constraints (18e) are the requirements for the quality of service of normal users. Constraints (18f), (18g), (18h), and (18i) require the feasibility of the optimal solution of problem (18). Problem (18) is a combinatorial optimization problem combining binary variables and real variables that formulate non-convex objective functions and constraints. To solve this problem, we propose a hybrid approach to separate the blocks of variables and optimize them efficiently in the next section.

IV. Optimization Methods

In this section, we propose the optimization strategies to address the joint design of sub-channel allocation and power allocation for enhancing PLS. Due to the mixed-integer and non-convex nature of the formulated problem, a hybrid approach is adopted. Specifically, a constrained genetic algorithm solves the sub-problem with binary variables, while a nested-loop algorithm is developed to optimize the real power variables. The details of each component are outlined in the following subsections. The variables are separated into two blocks including association $\boldsymbol{\varphi}, \boldsymbol{\eta}$ and power $\boldsymbol{P}_s, \boldsymbol{\beta}_u$.

A. Constrained Genetic Algorithm for Sub-Channel Allocation

By fixing trasmit power at the satellite and the UAV $\boldsymbol{P}_s, \boldsymbol{\beta}_u$, the optimization problem can be rewritten as follows

$$\max_{\boldsymbol{\varphi},\boldsymbol{\eta}} \quad \min_{k_W\in\mathcal{K}_W} SR_{k_W} \tag{21a}$$

$$\text{s.t. } (18b), (18c), (18d), (18e), (18f), (18g), (18h), (18i). \tag{21b}$$

In problem (21), the number of binary variables in (21) can be expressed as $N \times (K_W + K_N)$, causing $2^{N\times(K_W+K_N)}$ feasible cases which can be challenging to traditional search algorithms to find the optimal solution. GA offers several advantages to tackle NP-hard problems compared to other types of algorithms, such as high applicability and high flexibility. First, GA does not require an integral operation, while constraints can be easily integrated into the objective function as weighted values to encourage or punish good characteristics in the population. Second, the trade-off between complexity and accuracy can be controlled and adjusted to be more suitable for the requirements of problems by the number of chromosomes and the number of generations. Additionally, the trade-off between finding global and local optimums is controlled by the probability of mutation in the population. In more detail, the high mutation probability allows the algorithm to explore feasible points far from the current optimum, which is the best chromosome in the current generation; otherwise, the current optimum will be focused on optimizing with a lower mutation probability.

In the proposed GA shown in Fig. 2, a population consisting of many individuals denoted by pairs of binary chromosomes (i.e., one for $\boldsymbol{\varphi}$ and the other for $\boldsymbol{\eta}$) is created to search for the optimal solution. After population initialization, four operations, including evaluation, selection, crossover, and mutation, are used to guarantee the evolution of the population to better generations. Let $\boldsymbol{PO}_t$ denoting the population at time t, and each chromosome κ of an individual is equivalent to the combination $\boldsymbol{a}_t^{(\kappa)}$ of $\boldsymbol{\varphi}_t^{(\kappa)}$ and $\boldsymbol{\eta}_t^{(\kappa)}$. Due to strict constraints in (21), using binary encoding can cause the issue of a highly large search space and many illegal chromosomes in the next generations after crossover and mutation. Therefore, integer encoding and decoding methods are proposed. A compact integer-based encoding scheme represents sub-channel allocation decisions for legitimate and normal users. Each legitimate user or normal user is assigned exactly one sub-channel from a total of N available sub-channels.

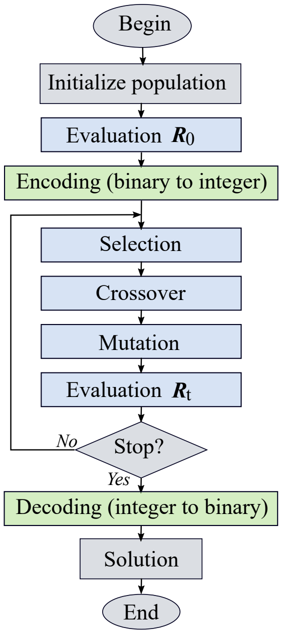
Begin
Initialize population
Evaluation $\boldsymbol{R}_0$
Encoding (binary to integer)
Selection
Crossover
Mutation
Evaluation $\boldsymbol{R}_t$
No
Stop?
Yes
Decoding (integer to binary)
Solution
End

Fig. 2. The constrained GA for optimizing sub-channel allocation.

- Encoding (binary to integer): The binary matrices $\boldsymbol{\eta} \in \{0,1\}^{K_W \times N}$ and $\boldsymbol{\varphi} \in \{0,1\}^{K_N \times N}$ indicate sub-channel assignments using one-hot vectors, where each row corresponds to a user and the column with value 1 indicates the selected sub-channel. These binary matrices are converted into integer vectors $\boldsymbol{\eta}_{\text{int}}$ and $\boldsymbol{\varphi}_{\text{int}}$ by identifying the index of the '1' in each row. This results in a compact representation where each element denotes the sub-channel index assigned to a user.
- Decoding (integer to binary): To evaluate chromosomes during the algorithm's execution, the integer vectors are decoded back to binary one-hot matrices. For each user, the sub-channel index indicated in the integer vector is set to 1 in its corresponding row, while all other entries remain 0. This reconstruction recovers the original binary allocation structure.

This encoding strategy significantly reduces the chromosome size and simplifies genetic operations such as crossover and mutation, while ensuring that the one-to-one sub-channel assignment constraints are maintained throughout the optimization process.

In addition, four operations used in GA to evolve the population through generations are described as follows

- Evaluation: To take into account the network security performance, we use the objective function r_t defined in (21). Each chromosome κ in the current population at time t is evaluated and denoted by a reward vector as
$$\boldsymbol{R}_t = \{r_t^{(\kappa)} | \kappa = \overline{1, K_\kappa}\}, \tag{22}$$
where κ represents for the current considered individual, K_κ is the number of individuals in the population, $r_t^{(\kappa)} = r_t(\boldsymbol{a}_t^{(\kappa)})$ is the evaluation value of individual κ.
- Selection: All chromosomes that do not obey the constraints are eliminated, and the fitness value is now turned into an objective function (21a). Depending on the fitness value, the probability of chromosome l chosen to be a parent for the next step is defined as
$$P_\kappa^{\text{sl}} = \frac{r_t^{(\kappa)} - \min(\boldsymbol{R}_t)}{\sum_{\kappa=1}^{K_\kappa} \left(r_t^{(\kappa)} - \min(\boldsymbol{R}_t) \right)}. \tag{23}$$
Since children can inherit good characteristics from their parents, the selection keeps chromosomes with high fitness value for the next step and eliminates the rest. This process is the same as natural selection in Biology.
- Crossover: A new generation of the population is created in this stage. Simple crossover methods, such as one-point or two-point crossover, can easily create invalid solutions that have a duplicating channel allocated to two different legitimate users, violating constraints (18f). Therefore, the uniform crossover method, which mixes genes independently across parents to create more diverse combinations, is chosen. The crossover probability P^{cr} denotes the chance of each parent being chosen for crossover.
- Mutation: While crossover tends to find the local optimum, mutation is the way to explore the feasible sets to increase the chance of finding a new better local optimum or global optimum in the best case. In the mutation step, each bit in any individual is flipped with the probability of P^{mt}. If the fitness value of mutated chromosomes is very low, they will have a low probability of being chosen at the selection step.

The improvement of generations is guaranteed by keeping some chromosomes with the highest fitness value. In detail, some chromosomes that have the highest value of the fitness function and that meet all the constraints are prioritized to pass to the next generation without any change in their genes. Two stopping conditions are used, including hard stopping and soft stopping conditions. Hard stopping condition indicates a maximum number of generations G_h, while soft stopping condition is set by G_s, the number of continuous times that the change of maximum fitness between the new generation and the old one is less than $\epsilon = 5\%$. The implementation of constrained GA remains feasible because parallel processing of the evaluation stage, frequency of the sub-channel allocation on a slow timescale, and flexibility in performance and execution time by adjusting the population size.

B. Power Allocation using Approximation Method

After allocating associations and sub-channels between the satellite, the UAV, and the users, we fix the values of $\boldsymbol{\varphi}$ and $\boldsymbol{\eta}$. The remaining optimization problem is expressed as follows

$$\max_{\boldsymbol{P}_s, \boldsymbol{\beta}_u} \quad \min_{k_W \in \mathcal{K}_W} SR_{k_W} \tag{24a}$$
$$\text{s.t.}\ (18\text{b}), (18\text{c}), (18\text{d}), (18\text{e}), (18\text{i}). \tag{24b}$$

First, we introduce K_W slack variables in the set $\boldsymbol{\zeta} = \{\zeta_k | k \in \mathcal{K}_W\}$ to reformulate problem (24) as [39]

$$\max_{\boldsymbol{P}_s, \boldsymbol{\beta}_u, \boldsymbol{\zeta}} \quad \min_{k_W \in \mathcal{K}_W} [\log_2(1+\gamma_{k_W}) - \log_2(1/\zeta_{k_W})]^+ \tag{25a}$$

$$\text{s.t. } \log_2(1+\gamma_{m\to k_W}) \le \log_2(1/\zeta_{k_W}), \forall k_W \in \mathcal{K}_W, \tag{25b}$$

$$\log_2(1+\gamma_{k_W}) - \log_2(1/\zeta_{k_W}) \ge SR_{min}/B, \forall k_W \in \mathcal{K}_W, \tag{25c}$$

$$(18b), (18c), (18d), (18e), (18i). \tag{25d}$$

To solve problem (25), we use a nested-loop algorithm which consists of an outer loop for solving the problem (25) with variables $\boldsymbol{\zeta}$ and an inner loop for solving the problem (25) with variables $\boldsymbol{P}_s$ and $\boldsymbol{\beta}_u$. By fixing $\boldsymbol{P}_s$ and $\boldsymbol{\beta}_u$, the outer problem can be formulated as

$$\max_{\boldsymbol{\zeta}} \quad \min_{k_W \in \mathcal{K}_W} [\log_2(\zeta_{k_W} + \psi_{k_W}(\zeta_{k_W}))]^+ \tag{26a}$$

$$\text{s.t. } \zeta_{k_W}^{min} \le \zeta_{k_W} \le \zeta_{k_W}^{max}, \forall k_W \in \mathcal{K}_W, \tag{26b}$$

where $\psi_{k_W}(\zeta_{k_W})$ is defined as a function of ζ_{k_W} in an inner problem. In problem (26), we want to maximize the minimum value of an increasing function (i.e., base-2 logarithm). Therefore, the inner problem can be expressed as

$$\psi_{k_W}(\zeta_{k_W}) \triangleq \max_{\boldsymbol{P}_s, \boldsymbol{\beta}_u} \quad \zeta_{k_W}\gamma_{k_W} \tag{27a}$$

$$\text{s.t. } \log_2(1+\gamma_{m\to k_W}) \le \log_2(1/\zeta_{k_W}), \forall k_W \in \mathcal{K}_W, \tag{27b}$$

$$\log_2(1+\gamma_{k_W}) - \log_2(1/\zeta_{k_W}) \ge SR_{min}/B, \forall k_W \in \mathcal{K}_W, \tag{27c}$$

$$(18b), (18c), (18e), (18i). \tag{27d}$$

According to (25a) and (25b), the lower bound and upper bound of ζ_{k_W} are defined as $\zeta_{k_W}^{min} = 0$ and $\zeta_{k_W}^{max} = 1$. To solve the outer problem (26), a multi-dimensional search method for finding the optimal value of $\boldsymbol{\zeta}$ in the feasible set is used. The functions $\psi_{k_W}(\zeta_{k_W})$ with all k_W are obtained by solving the inner problem (27). Therefore, evaluating the objective function in (26) is a computationally intensive task. Bayesian optimization, a powerful and efficient algorithm for optimizing problems with complex objective functions, is used to solve the outer problem. In problem (26), an element in the objective function $\psi_{k_W}(\zeta_{k_W})$ is defined by another optimization problem. Bayesian optimization leverages a surrogate model and acquisition function to efficiently explore the search space and optimize the highly computational function. Additionally, to solve the inner problem, we split the problem into two subproblems according to each variable type.

Problem 1: The sub-problem for optimizing power allocation in the satellite is formulated as

$$\max_{\boldsymbol{P}_s} \quad \zeta_{k_W}\gamma_{k_W} \tag{28a}$$

$$\text{s.t. } \log_2(1+\gamma_{m\to k_W}) \le \log_2(1/\zeta_{k_W}), \forall k_W \in \mathcal{K}_W, \tag{28b}$$

$$\log_2(1+\gamma_{k_W}) - \log_2(1/\zeta_{k_W}) \ge SR_{min}/B, \forall k_W \in \mathcal{K}_W, \tag{28c}$$

$$(18b), (18c), (18e), (18i). \tag{28d}$$

In problem (28), we change the variables of the satellite's power allocated to legitimate users and the UAV by their squares. To be more specifically, $\sqrt{p_{s,k_W}^{(n)}}$ and $\sqrt{p_{s,u}^{(n)}}$ are replaced by $p_{s,k_W}^{(n)}$ and $p_{s,u}^{(n)}$, respectively. According to [40], with $x \in \mathbb{C}$ and $y \in \mathbb{R}^+$, at the point $(x, y) = (\bar{x}, \bar{y})$, we have

$$\frac{|x|^2}{y} \ge \frac{2}{\bar{y}}\Re(\bar{x}^* x) - \frac{|\bar{x}|^2}{\bar{y}^2}y, \tag{29}$$

where $\Re(x)$ denotes the real value of the complex value x. The approaches to approximate the objective function and constraints with the aim of converting problem (28) to a convex problem are described as follows.

- Objective function: According to (29), let $\tau_{k_W}^{w1} = \boldsymbol{h}_{s,k_W}^{(n)} + \boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}\boldsymbol{h}_{s,u}^{(n)}$, $\tau_{k_W}^{w2} = |\boldsymbol{h}_{u,k_W}^{(n)}\boldsymbol{f}_{u,k_W}^{(n)}|^2(\sigma_\nu^2 + \sigma_u^2) + \sigma_{k_W}^2$, $x_{k_W} = \tau_{k_W}^{w1}(\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})$, $\overline{x}_{k_W} = \tau_{k_W}^{w1}(\overline{\boldsymbol{w}}_{s,k_W}^{(n)} + \overline{\boldsymbol{w}}_{s,u}^{(n)})$ $y_{k_W} = \sum_{k'_N \in \mathcal{K}_N} \varphi_{s,k'_N}^{(n)} |\tau_{k_W}^{w1}\boldsymbol{w}_{s,k'_N}^{(n)}|^2 + \tau_{k_W}^{w2}$, and $\overline{y}_{k_W} = \sum_{k'_N \in \mathcal{K}_N} \varphi_{s,k'_N}^{(n)} |\tau_{k_W}^{w1}\overline{\boldsymbol{w}}_{s,k'_N}^{(n)}|^2 + \tau_{k_W}^{w2}$, the objective (28a) can be approximated a concave function in an iteration as

$$\zeta_{k_W}\gamma_{k_W} \ge \frac{2\zeta_{k_W}}{\overline{y}_{k_W}}\Re\left(\overline{x}_{k_W}^* x_{k_W}\right) - \frac{\zeta_{k_W}|\overline{x}_{k_W}|^2}{\overline{y}_{k_W}^2}y_{k_W}. \tag{30}$$

- (28b): the constraint (28b) can be transformed as $\gamma_{m\to k_W} \le 1/\zeta_{k_W} - 1$ and then using Cauchy-Schwarz inequality. The approximately equivalent constraint can be expressed as

$$|\boldsymbol{h}_{s,m}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)})|^2 - \left(\sum_{k'_N \in \mathcal{K}_N} \varphi_{s,k'_N}^{(n)} |\boldsymbol{h}_{s,m}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}|^2 + |\boldsymbol{h}_{u,m}^{(n)}\boldsymbol{G}_{u,k_W}^{(n)}\boldsymbol{v}_u^{(n)}|^2 + \sigma_m^2\right)\left(\frac{1}{\zeta_{k_W}} - 1\right) \le 0. \tag{31}$$

- (28c): The constraint (28c) can be transformed as $\gamma_{k_W} \ge 2^{\log_2(\frac{1}{\zeta_{k_W}}) + \frac{SR_{min}}{B}} - 1$

$$\frac{2}{\overline{y}_{k_W}}\Re\left(\frac{|\overline{x}_{k_W}|^2}{\overline{x}_{k_W}}x_{k_W}\right) - \frac{|\overline{x}_{k_W}|^2}{\overline{y}_{k_W}}y_{k_W} \ge 2^{\log_2(\frac{1}{\zeta_{k_W}}) + \frac{SR_{min}}{B}} - 1, \forall k_W \in \mathcal{K}_W. \tag{32}$$

  The constraint (32) satisfies the disciplined convex programming (DCP) rule.
- (18b), (18c): Since each sub-channel is assigned at most one legitimate user and one legitimate user can own only one sub-channel, constraints (18b) and (18c) can be rewritten as second-order cone (SOC) constraints as

$$\sum_{n=1}^{N}\sum_{k_W \in \mathcal{K}_W} \eta_{s,u,k_W}^{(n)} \|\boldsymbol{w}_{s,k_W}^{(n)} + \boldsymbol{w}_{s,u}^{(n)}\|^2 \le P_s^{(\max)} - \sum_{n=1}^{N}\left(\sum_{k_N \in \mathcal{K}_N} \varphi_{s,k_N}^{(n)} p_{s,k_N}^{(n)}\right). \tag{33}$$

$$\sum_{n=1}^{N}\sum_{k_U\in\mathcal{K}_W}\eta_{s,u,k_U}^{(n)}\|\boldsymbol{f}_{u,k_U}^{(n)}\boldsymbol{h}_{s,u}^{(n)}(\boldsymbol{w}_{s,k_U}^{(n)}+\boldsymbol{w}_{s,u}^{(n)})\|^2$$
$$\leq -\sum_{n=1}^{N}\Bigg(\sum_{\substack{k_U\in\mathcal{K}_W\\k_N\in\mathcal{K}_N}}\eta_{s,u,k_U}^{(n)}\varphi_{s,k_N}^{(n)}\|\boldsymbol{f}_{u,k_U}^{(n)}\boldsymbol{h}_{s,u}^{(n)}\boldsymbol{w}_{s,k_N}^{(n)}\|^2$$
$$+\sum_{k_U\in\mathcal{K}_W}\eta_{s,u,k_U}^{(n)}\|\boldsymbol{f}_{u,k_U}^{(n)}\|^2(\sigma_\nu^2+\sigma_u^2)$$
$$+\sum_{k_U\in\mathcal{K}_W}\eta_{s,u,k_U}^{(n)}\|\boldsymbol{G}_{u,k_U}^{(n)}\boldsymbol{v}_u^{(n)}\|^2\Bigg)+P_u^{(\max)}. \quad (34)$$

- (18e): The constraint (18e) can be transformed as $\gamma_{k_N}\geq 2^{\frac{SR_{min}}{B}}-1$, and be rewritten as
$$\left(2^{\frac{SR_{min}}{B}}-1\right)y_{k_N}-x_{k_N}\leq 0,\forall k_N\in\mathcal{K}_N, \quad (35)$$
where $\tau_{k_N}^{n1}=\boldsymbol{h}_{s,k_N}^{(n)}+\sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}\boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}\boldsymbol{h}_{s,u}^{(n)}$, $\tau_{k_N,k'_W}^{n2}=\boldsymbol{h}_{s,k_N}^{(n)}+\boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{f}_{u,k'_W}^{(n)}\boldsymbol{h}_{s,u}^{(n)}$, $\tau_{k_N}^{n3}=\sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}|\boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{f}_{u,k'_U}^{(n)}|^2(\sigma_\nu^2+\sigma_u^2)+\sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}|\boldsymbol{h}_{u,k_N}^{(n)}\boldsymbol{G}_{u,k'_U}^{(n)}\boldsymbol{v}_u^{(n)}|^2+\sigma_{k_N}^2$, $x_{k_N}=|\tau_{k_N}^{n1}\boldsymbol{w}_{s,k_N}^{(n)}|^2$, $y_{k_N}=\sum_{k'_N\in\mathcal{K}_N\backslash k_N}\varphi_{s,k'_N}^{(n)}|\tau_{k_N}^{n1}\boldsymbol{w}_{s,k'_N}^{(n)}|^2+\sum_{k'_W\in\mathcal{K}_W}\eta_{s,u,k'_W}^{(n)}(|\tau_{k_N,k'_W}^{n2}(\boldsymbol{w}_{s,k'_W}^{(n)}+\boldsymbol{w}_{s,u}^{(n)})|^2+\tau_{k_N}^{n3}$. The left-hand expression of constraint (35) is approximated as the convex function, thereby satisfying the DCP rule.

Problem 2: The sub-problem for power allocation in the UAV by controlling the value of power scaling coefficients $\boldsymbol{\beta}$ is formulated as

$$\max_{\boldsymbol{\beta}_u}\quad \zeta_{k_W}\gamma_{k_W} \quad (36a)$$
$$\text{s.t. } \log_2(1+\gamma_{m\to k_W})\leq\log_2(1/\zeta_{k_W}),\forall k_W\in\mathcal{K}_W, \quad (36b)$$
$$\log_2(1+\gamma_{k_W})-\log_2(1/\zeta_{k_W})\geq SR_{min}/B,\forall k_W\in\mathcal{K}_W, \quad (36c)$$
$$(18c),(18e),(18i). \quad (36d)$$

The approaches to approximate the objective function and constraints with the aim of converting problem (36) to a convex problem are described as follows.

- Objective function: According to (29), let $\delta_{k_W}^{w1}=\boldsymbol{h}_{s,k_W}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)}+\boldsymbol{w}_{s,u}^{(n)})$, $\delta_{k_W,k'_N}^{w3}=\boldsymbol{h}_{s,k_W}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}$, $\delta_{k_W}^{w2}=\boldsymbol{h}_{u,k_W}^{(n)}\text{Null}\{\boldsymbol{H}_{u,\mathcal{M}}^{(n)}\}\boldsymbol{h}_{s,u}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)}+\boldsymbol{w}_{s,u}^{(n)})$, $\delta_{k_W,k'_N}^{w4}=\boldsymbol{h}_{u,k_W}^{(n)}\text{Null}\{\boldsymbol{H}_{u,\mathcal{M}}^{(n)}\}\boldsymbol{h}_{s,u}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}$, $\delta_{k_W}^{w5}=|\boldsymbol{h}_{u,k_W}^{(n)}\text{Null}\{\boldsymbol{H}_{u,\mathcal{M}}^{(n)}\}|^2(\sigma_\nu^2+\sigma_u^2)$, $x'_{k_W}(\boldsymbol{\beta}_u)=\delta_{k_W}^{w1}+\delta_{k_W}^{w2}\beta_{u,1}^{(n)}$, $\overline{x}'_{k_W}=x'_{k_W}(\bar{\boldsymbol{\beta}}_u)$, $y'_{k_W}(\boldsymbol{\beta}_u)=\sum_{k'_N\in\mathcal{K}_N}\varphi_{s,k'_N}^{(n)}|\delta_{k_W,k'_N}^{w3}+\delta_{k_W,k'_N}^{w4}\beta_{u,1}^{(n)}|^2+\delta_{k_W}^{w5}{\beta_{u,1}^{(n)}}^2+\sigma_{k_W}^2$, and $\overline{y}'_{k_W}=y'_{k_W}(\bar{\boldsymbol{\beta}}_u)$. The objective (36a) can be approximated a concave function in an iteration as
$$\zeta_{k_W}\gamma_{k_W}\geq\frac{2\zeta_{k_W}}{\overline{y}'_{k_W}}\Re\left(\overline{x}'^{*}_{k_W}x'_{k_W}\right)-\frac{|\overline{x}'_{k_W}|^2\zeta_{k_W}}{\overline{y}'^{2}_{k_W}}y'_{k_W}. \quad (37)$$
- (36b): The constraint (36b) can be transformed as $\gamma_{m\to k_W}\leq 1/\zeta_{k_W}-1$ or
$$\sum_{k'_N\in\mathcal{K}_N}\varphi_{s,k'_N}^{(n)}|\boldsymbol{h}_{s,m}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}|^2+|\boldsymbol{h}_{u,m}^{(n)}\boldsymbol{G}_{u,k_W}^{(n)}\boldsymbol{v}_u^{(n)}|^2+\sigma_m^2$$
$$\geq\frac{\zeta_{k_W}|\boldsymbol{h}_{s,m}^{(n)}(\boldsymbol{w}_{s,k_W}^{(n)}+\boldsymbol{w}_{s,u}^{(n)})|^2}{1-\zeta_{k_W}}. \quad (38)$$
- (36c): The constraint (36c) can be transformed as $\gamma_{k_W}\geq 2^{\log_2(\frac{1}{\zeta_{k_W}})+\frac{SR_{min}}{B}}-1$
$$\frac{2}{\overline{y}'_{k_W}}\Re\left(\overline{x}'^{*}_{k_W}x'_{k_W}\right)-\frac{|\overline{x}'_{k_W}|^2}{\overline{y}'^{2}_{k_W}}y'_{k_W}$$
$$\geq 2^{\log_2(\frac{1}{\zeta_{k_W}})+\frac{SR_{min}}{B}}-1,\forall k_W\in\mathcal{K}_W. \quad (39)$$
- (18c) and (18i) satisfy DCP rule.
- (18e): The constraint (18e) can be transformed as $\gamma_{k_N}\geq 2^{\frac{SR_{min}}{B}}-1$, and be rewritten as
$$\frac{2}{\bar{y}'_{k_N}}\Re\left(\bar{x}'^{*}_{k_N}x'_{k_N}\right)-\frac{|\bar{x}_{k_N}|^2}{\bar{y}'^{2}_{k_N}}y'_{k_N}\geq 2^{\frac{SR_{min}}{B}}-1, \quad (40)$$
where
$$\delta_{k'_N}^{n1}=\sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}\boldsymbol{h}_{u,k_N}^{(n)}\text{Null}\{\boldsymbol{H}_{u,\mathcal{M}}^{(n)}\}\boldsymbol{h}_{s,u}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)},$$
$x'_{k_N}(\boldsymbol{\beta}_u)=|\boldsymbol{h}_{s,k_N}^{(n)}\boldsymbol{w}_{s,k_N}^{(n)}+\delta_{k_N}^{n1}\beta_{u,1}^{(n)}|^2$, $\bar{x}'_{k_N}=x'_{k_N}(\bar{\boldsymbol{\beta}}_u)$, $\delta_{k_N,k'_W}^{n2}=\boldsymbol{h}_{s,k_N}^{(n)}(\boldsymbol{w}_{s,k'_W}^{(n)}+\boldsymbol{w}_{s,u}^{(n)})$, $\delta_{k_N,k'_W}^{n3}=\boldsymbol{h}_{u,k_N}^{(n)}\text{Null}\{\boldsymbol{H}_{u,\mathcal{M}}^{(n)}\}\boldsymbol{h}_{s,u}^{(n)}(\boldsymbol{w}_{s,k'_W}^{(n)}+\boldsymbol{w}_{s,u}^{(n)})$, $\delta_{k_N}^{n4}=\sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}|\boldsymbol{h}_{u,k_N}^{(n)}\text{Null}\{\boldsymbol{H}_{u,\mathcal{M}}^{(n)}\}|^2(\sigma_\nu^2+\sigma_u^2)$, $\delta_{k_N}^{n5}=\sum_{k'_U\in\mathcal{K}_W}\eta_{s,u,k'_U}^{(n)}|\boldsymbol{h}_{u,k_N}^{(n)}\text{Null}\{\boldsymbol{H}_{u,\mathcal{K}_W}^{(n)}\}\frac{\boldsymbol{h}_{u,m\to k'_U}^{(n)}}{\|\boldsymbol{h}_{u,m\to k'_U}^{(n)}\|}^{\dagger}\boldsymbol{v}_u^{(n)}|^2$, $y'_{k_N}(\boldsymbol{\beta}_u)=\sum_{k'_N\in\mathcal{K}_N\backslash k_N}\varphi_{s,k'_N}^{(n)}|\boldsymbol{h}_{s,k_N}^{(n)}\boldsymbol{w}_{s,k'_N}^{(n)}+\delta_{k'_N}^{n1}\beta_{u,1}^{(n)}|^2+\sum_{k'_W\in\mathcal{K}_W}\eta_{s,u,k'_W}^{(n)}|\delta_{k_N,k'_W}^{n2}+\delta_{k_N,k'_W}^{n3}\beta_{u,1}^{(n)}|^2+\delta_{k_N}^{n4}{\beta_{u,1}^{(n)}}^2+\delta_{k_N}^{n5}{\beta_{u,2}^{(n)}}^2+\sigma_{k_N}^2$, and $\bar{y}'_{k_N}=y'_{k_N}(\bar{\boldsymbol{\beta}}_u)$. The left-hand expression of constraint (40) is approximated as the concave function, thereby satisfying the DCP rule.

The algorithm combining the outer loops by the Bayesian optimization method and inner loops by the approximation method is described in Alg. 1. A Gaussian Process (GP) surrogate with a Matern kernel (equal to 2.5) is used to approximate the minimum secrecy rate objective. Expected improvement (EI) is used as the acquisition function, which combines the surrogate mean prediction and uncertainty to balance exploration of less-certain regions and exploitation of promising candidates. The search space is defined by bounded continuous intervals corresponding to the feasible ranges of the slack variables $\boldsymbol{\zeta}$ defined in (26b). Each evaluation involves inner solutions by solving the power allocation sub-problems in (28) and (36). The optimization proceeds for at most n_{calls} evaluations and terminates earlier if no further improvement in the acquisition function is observed.

Algorithm 1 Power Allocation Optimization Algorithm

```
Input: Bounds $\mathcal{X}$ combining $\zeta_{k_W}^{min}$ and $\zeta_{k_W}^{max}$, surrogate model $\mathcal{N}(\text{mean}(\boldsymbol{\zeta}), \text{std}^2(\boldsymbol{\zeta}))$, acquisition function $a(\boldsymbol{\zeta})$ as expected improvement, black-box function
    $\text{obj}(\boldsymbol{P}_s, \boldsymbol{\beta}_u, \boldsymbol{\zeta}) \triangleq \min_{k_W \in \mathcal{K}_W} \psi_{k_W}(\zeta_{k_W})$
Initialize dataset $\mathcal{D}_0 = \{(\boldsymbol{\zeta}^{(i)}, \text{obj}^{(i)})\}_{i=1}^{I}$
for $t = 1$ to $T$ do
    Fit/update surrogate model using $\mathcal{D}_{t-1}$
    Find next sample point: $\boldsymbol{\zeta}_t = \arg\max_{\boldsymbol{\zeta} \in \mathcal{X}} a(\boldsymbol{\zeta}|\mathcal{D}_{t-1})$
    Initialize $\psi_{k_W}^{(\min)} = \infty$
    for $k_W = 1$ to $K_W$ do
        $\psi_{k_W}^{(OLD)} = 0$ and $|\psi_{k_W}^{(CURRENT)} = \infty$
        while $|\psi_{k_W}^{(CURRENT)} - \psi_{k_W}^{(OLD)}| > \epsilon$ do
            Set $\psi_{k_W}^{(OLD)} = \psi_{k_W}^{(CURRENT)}$
            Optimize power $\boldsymbol{P}_s^*$ of (28) at the satellite
            Optimize power $\boldsymbol{\beta}_u^*$ of (36) at the UAV
            Update current best solution $\psi_{k_W}^{(CURRENT)} = \psi_{k_W}^*$
        end while
        if $\psi_{k_W}^{(CURRENT)} <= \psi_{k_W}^{(\min)}$ then
            $\psi_{k_W}^{(\min)} = \psi_{k_W}^{(CURRENT)}$
            $\boldsymbol{P}_s = \boldsymbol{P}_s^*$ and $\boldsymbol{\beta}_u = \boldsymbol{\beta}_u^*$
        end if
    end for
    Evaluate objective: $\text{obj}_t = \psi_{k_W}^{(\min)}$
    Update dataset: $\mathcal{D}_t = \mathcal{D}_{t-1} \cup \{(\boldsymbol{\zeta}_t, \text{obj}_t)\}$
end for
Output: Best observed input
    $\boldsymbol{P}_s^*, \boldsymbol{\beta}_u^*, \boldsymbol{\zeta}^* = \arg\max_{\boldsymbol{\zeta}^{(i)} \in \mathcal{D}_T} \text{obj}(\boldsymbol{P}_s, \boldsymbol{\beta}_u, \boldsymbol{\zeta})$
```

C. The Analysis of Computational Complexity

Decomposing the complex original problem into low-complex sub-problems helps to reduce the nature of high complexity and obtain at least a local optimal solution. Indeed, the original problem (18) has $(2K_N + 2K_W + 3)N$ variables (i.e. $(K_N + K_W + 3)N$ real positive variables and $(K_N + K_W)N$ binary variables) and $2 + 2(K_N + K_W)(N+1) + 4N$ constraints. Thus, the computational complexity of problem (18) can be approximated as $\mathcal{O}(((2K_N + 2K_W + 3)N)^2\sqrt{2 + 2(K_N + K_W)(N+1) + 4N})$ [41]. To address this, we decompose the original problem into three low-complexity sub-problems to reduce computational cost. Regarding the complexity of sub-channel allocation sub-problem (21), there are $K_N + K_W$ integer variables and $(K_N + K_W + 1)(N + 2)$ constraints after encoding. By applying precomputation and storing all sub-channel links, the fitness evaluation scales as $\mathcal{O}(K_N + K_W + N)$, following an overall complexity $\mathcal{O}(K_\kappa G_h(K_N + K_W + N)$, where G_h is the number of generations. Additionally, sub-problem (28) has $K_N + K_W + 1$ real positive variables and $2K_N + 3K_W + 3$ constraints while sub-problem (36) has $2K_W$ real positive variables and $K_N + 4K_W + 1$ constraints. Therefore, the computational complexity of sub-problem (28) and sub-problem (36) can be expressed $\mathcal{O}((K_N + K_W + 1)^2\sqrt{2K_N + 3K_W + 3})$ and $\mathcal{O}((2K_W)^2\sqrt{K_N + 4K_W + 1})$, respectively. Sub-problem (21) can be efficiently solved by constrained GA that employs the trade-off between complexity and optimal performance. Besides, sub-problem (28) and sub-problem (36) with significantly lower complexity are exploited in iterative Alg. 1 in order to find the optimal solution.

V. Simulation Results

In this section, we evaluate the performance of the proposed UAV-assisted PLS scheme in a SAGIN. The simulation system operates at a carrier frequency of 2 GHz, combining sub-channels of 0.5-1 MHz bandwidth. The altitude of the satellite on its orbit is 780 km with 128 transmit antennas and the maximum power in the range of 60-100 W. Meanwhile, the altitude of the UAV is in the range of 0.5-10 km with 1 received antenna and 64 transmit antennas and the maximum power in the range of 5-25 W. Simulations are conducted to assess the impact of various system parameters on the achievable minimum secrecy rate. The detailed simulation settings are summarized in Table I [42]. To demonstrate the effectiveness of the proposed joint sub-channel allocation and power allocation strategy, we compare it with baseline methods under different network conditions, such as varying number of eavesdroppers, the maximum transmit power of the satellite, the maximum transmit power of the UAV, and UAV altitude.

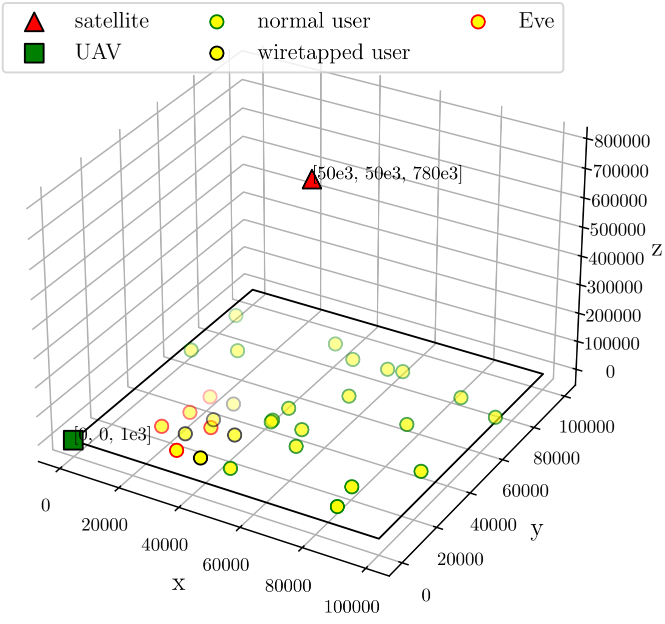

Fig. 3. An example of a system model where legitimate users and eavesdroppers are uniformly distributed in an area of 40 × 40 km^2 and normal users are in the remaining area.

A. Algorithm Convergence

The scenarios in this subsection combine 5 sub-channels, 5 legitimate users, 5 eavesdroppers, and 20 normal users as

TABLE I
SIMULATION PARAMETERS

Parameter	Description	Value
	Considered area	100×100 km^2
f_c	Carrier frequency	2 GHz
B	Bandwidth per sub-channel	0.5-1 MHz
z_s	Altitude of satellite	780 km
N_S	Number of satellite transmit antennas	128
$P_s^{\max}$	Maximum transmit power of satellite	60-100 W
z_u	Altitude of UAV	$0.5 - 10$ km
N_U	Number of UAV transmit antennas	64
$P_u^{\max}$	Maximum transmit power of UAV	5-25 W
K_N	Number of normal users	6
K_W	Number of legitimate users	4
M	Number of eavesdroppers	4
σ_u^2, σ_k^2	Noise power at UAV and users	-174 dBm/Hz
σ_ν^2	Self-interference noise at UAV	$2\sigma_u^2$
$(\omega_i, \delta_i, \varepsilon_i)$	SRF model	$(0.0005, 0.063, 2)$
$(\alpha^{(i)})$	The path loss exponents	$(2, 2, 2)$
P^{cr}, P^{mt}	The probability of crossover and mutation	$(0.9, 0.5)$

shown in Fig. 3. The maximum power of the satellite and the UAV are 100 W and 20 W, respectively. Additionally, the bandwidth of one sub-channel equals 0.5 MHz, and the minimum secrecy rate and minimum rate equal 10 kbps. The altitude of the UAV is 1 km above the ground.

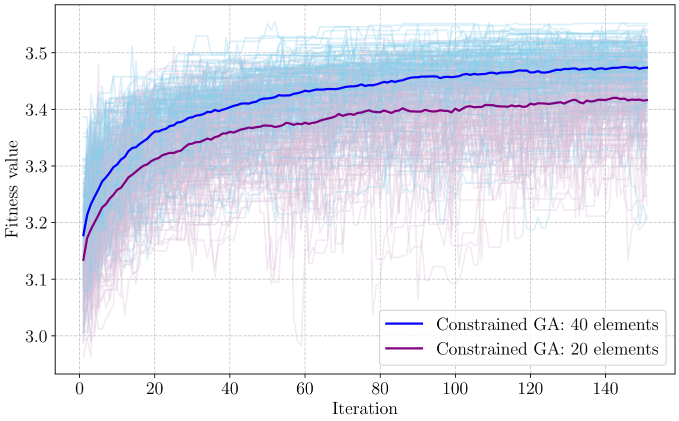

Fig. 4. Mean of fitness value in the constrained GA with the population of 20 elements and 40 elements ($P^{\mathrm{cr}} = 0.9$ and $P^{\mathrm{mt}} = 0.5$).

The comparison between the GAs using different numbers of elements demonstrates a clear performance advantage when increasing the population size. As shown in Fig. 4, we compare the mean convergence of 150 Monte Carlo iterations of GA with 20 and 40 elements through 150 evolution times. The mutation probability is set to $P^{mt} = 0.5$ to prevent premature convergence in our constrained GA. In our discrete sub-channel allocation problem, maintaining gene diversity is more important than preserving correlations, since the number of users per sub-channel is limited to avoid overhead. Consequently, chromosomes are optimized through diverse gene mixing rather than convergence on a few channels. Moreover, under the max–min objective, a low mutation probability increases the risk of premature convergence, as the best fitness value may remain unchanged and hinder further improvement.

The GA with 40 elements, with the mean denoted by the blue line, consistently achieves higher fitness values across iterations compared to the GA with 20 elements, denoted by the purple line. This suggests that a larger population provides greater genetic diversity, allowing the algorithm to explore the solution space more effectively and converge to better solutions. The convergence of the 40-element GA is also smoother and more stable, indicating improved optimization efficiency and robustness under the constrained scenario. However, the population size must be chosen carefully, as a larger population can lead to increased execution time. In the remaining simulations, we adopt the GA with 40 elements to generate the results, balancing performance and computational efficiency.

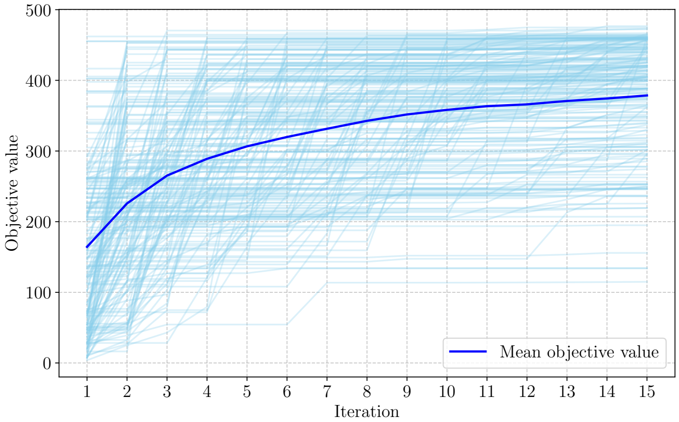

Fig. 5. Mean of objective value of power allocation optimization algorithm in 20 iterations ($SR_{\min} = 10$ kbps).

The convergence behavior of the outer loop for power allocation using Bayesian optimization is illustrated over 20 iterations in Fig. 5. As observed, the mean objective value improves steadily during the initial iterations and begins to plateau toward the later stages, indicating convergence. By the 10th iteration, the optimization process shows signs of stabilization, suggesting that the algorithm has effectively explored the solution space and is approaching a near-optimal power allocation. This demonstrates the efficiency of Bayesian optimization in navigating complex objective functions within a limited number of evaluations.

B. Impact of Satellite and UAV Transmit Power on Minimum Secrecy Rate

To evaluate the effectiveness, we introduce two benchmark schemes for comparison, including *RandomAll* and *OptAssocRandomPower*. In the *RandomAll* scheme, both the sub-channel allocation and power allocation are selected randomly. This serves as a lower-bound baseline, illustrating system performance without any optimization. In addition, the *OptAssocRandomPower* scheme employs optimal sub-channel allocation while assigning power values randomly, allowing us to isolate the impact of optimized power control. These benchmarks help highlight the performance gains achieved through the joint optimization of sub-channel allocation and power allocation in the proposed method.

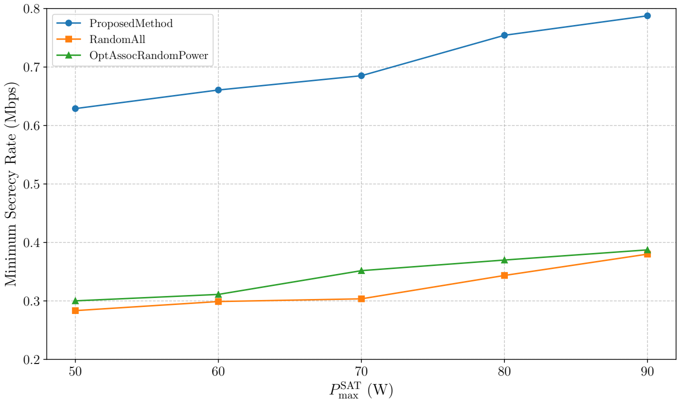

Fig. 6. The impact of maximum power of the satellite on the minimum secrecy rate ($B = 0.5$ MHz, $SR_{\min} = 100$ kbps, and $R_{\min} = 10$ kbps).

Fig. 6 illustrates the effect of the satellite's maximum transmit power, $P_{\max}^{\text{SAT}}$, on the achieved secrecy rate under different transmission strategies. As $P_{\max}^{\text{SAT}}$ increases from 50 W to 90 W, all schemes demonstrate an improvement in secrecy rate. The *Proposed Method* consistently outperforms both the *RandomAll* and *OptAssocRandomPower* baselines across the full power range. This performance gain validates the effectiveness of the proposed joint design that optimizes both sub-channel allocation and power allocation.

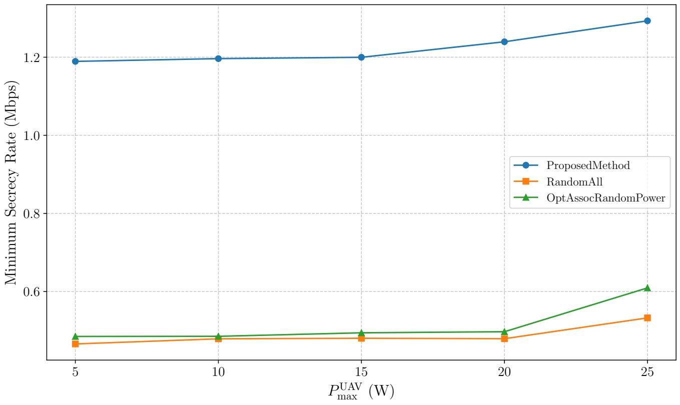

Fig. 7. The impact of maximum power of the UAV on the minimum secrecy rate ($B = 1$ MHz, $SR_{\min} = 50$ kbps, and $R_{\min} = 5$ kbps).

The impact of UAV transmit power on the minimum secrecy rate is illustrated in Fig. 7. As the UAV's maximum transmit power increases from 5 W to 25 W, the secrecy rate improves across all schemes, highlighting the importance of UAV transmission capability in enhancing secure communication. The secrecy rate saturates with the UAV's maximum transmit power from 5 W to 15 W because the effect of the UAV with low transmit power is limited. The minimum secrecy rate depends highly on the satellite power and the narrowness of the beams toward legitimate users. When the maximum transmit power is higher than 15 W, the minimum secrecy rate increases gradually from 1.2 Mbps at 15 W to 1.3 Mbps at 25 W. Additionally, the proposed method consistently achieves the highest secrecy rate compared to the *RandomAll* and *OptAssocRandomPower* benchmarks. This performance gain becomes more pronounced at higher power levels, indicating the effectiveness of jointly optimizing sub-channel allocation and power control in fully exploiting the available UAV transmit power to benefit legitimate users while disrupting eavesdroppers.

C. Impact of Distance to the UAV on Minimum Secrecy Rate

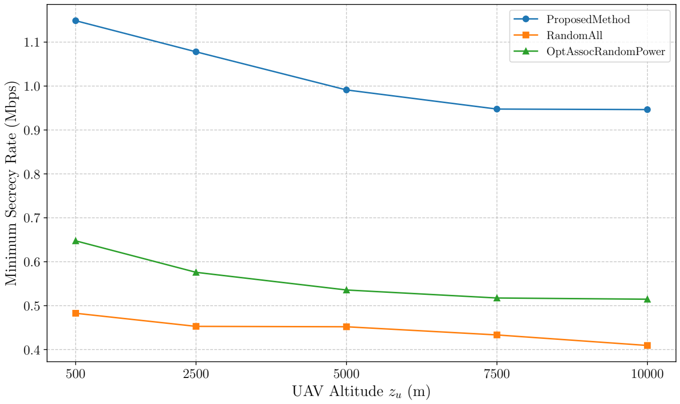

Fig. 8. The impact of distance to the UAV on the minimum secrecy rate ($B = 1$ MHz, $SR_{\min} = 50$ kbps, and $R_{\min} = 5$ kbps).

Fig. 8 illustrates the influence of the UAV altitude z_u on the system's secrecy rate performance. As altitude increases from 500 m to 10,000 m, the secrecy rate of all schemes gradually decreases. This trend reflects the trade-off between increased path loss at higher altitudes and the supportive capacity of the UAV on the minimum secrecy rate. In the first 5000 meters, the path loss of the channels from the UAV to the users and eavesdroppers is low. Therefore, the use of the UAV to enhance security is more effective by improving the legitimate signal and jamming eavesdroppers. When the altitude of the UAV is higher than 5000 meters, legitimate users and eavesdroppers receive low power of the relay signal and the AN from the UAV, respectively. Thus, the effect of the UAV on the network security is limited. The *Proposed Method* achieves the highest secrecy rate across all altitudes, demonstrating its robustness in adapting to different UAV placements. Compared to the *RandomAll* and *OptAssocRandomPower* benchmarks, the proposed approach significantly enhances performance, especially near the optimal UAV altitude, by effectively optimizing both sub-channel allocation and power allocation.

D. Impact of the Number of Eavesdroppers on Minimum Secrecy Rate

In this scenario, all eavesdroppers are randomly located within a 40×40 km^2 area, which is attacked. These nodes can be initially legitimate users, but the area is assumed to have fallen under the control of attackers, so the corresponding users act as eavesdroppers. This modeling choice reflects a realistic case where CSI of compromised users is available, while capturing the security threat of adversary-controlled regions. The legitimate users and normal users are distributed in the other area. Fig. 9 shows the impact of the number of eavesdroppers on the minimum secrecy rate. Overall, the

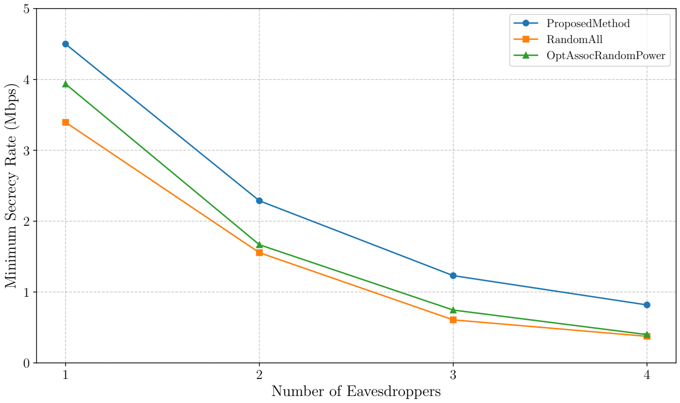

Fig. 9. The impact of the number of eavesdroppers (equal to the number of legitimate users) on the minimum secrecy rate ($B = 0.5$ MHz, $SR_{\min} = 100$ kbps, and $R_{\min} = 10$ kbps).

minimum secrecy rates of all methods decrease dramatically when the number of eavesdroppers increases from 1 to 4. In detail, our proposed method achieves around 4.5 Mbps of minimum secrecy rate with one eavesdropper, following a reduction to have the minimum secrecy rate of nearly 0.82 Mbps with four eavesdroppers. This trend shows that the appearance of multiple eavesdroppers requires the satellite and the UAV to spend more power to guarantee the secrecy rate of all legitimate users and the quality of service of normal users. Additionally, our proposed method outperforms the other by at least 0.42 Mbps higher in the case of 4 eavesdroppers.

VI. Conclusions and Future Work

This paper has presented a UAV-assisted PLS framework for SAGINs in the presence of multiple eavesdroppers. A full-duplex UAV had been deployed to simultaneously relay confidential signals and emit AN, improving the signal quality for legitimate users while disrupting eavesdroppers. The goal had been to maximize the minimum secrecy rate among all users. To achieve this, the framework had jointly optimized subchannel allocation and power control using a hybrid algorithm combining genetic optimization and nested-loop refinement. Simulation results have demonstrated that the proposed approach consistently outperformed benchmark strategies across various network conditions, achieving significantly higher secrecy rates. These results underline the effectiveness of the proposed framework and its potential application in secure communications for next-generation SAGINs, especially in scenarios requiring flexible and resilient security support.

The current study opens up several potential directions of PLS in SAGINs for further investigation. Firstly, the UAV, which is used as a full-duplex relay node, requires efficient self-interference cancellation techniques to ensure the quality enhancement and stable transmission. Additionally, instantaneous CSI requirement for the links such as satellite-UAV-user and satellite-UAV-eavesdropper can introduce channel estimation overhead to core networks due to the movable nature of satellites and UAVs. These highlight the importance of developing robust interference mitigation and low-complexity channel estimation techniques to enable practical deployment of our system model. In addition, learning-based techniques, such as reinforcement learning, could be explored to enable adaptive and real-time resource allocation in dynamic network environments. Lastly, incorporating practical system impairments—such as imperfect channel state information and hardware limitations—would increase the robustness of the model and facilitate its application in real-world scenarios.

References

[1] J. Yahui, Y. Kan, Q. Jing, and Y. Jiguo, “Massive MIMO and secrecy guard zone based improving physical layer security in UAV-enabled uRLLC networks,” *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 4553–4567, Apr. 2023.

[2] J. Sobia, A.-D. Arafat, I. Youssef, P. Anshul, and G. Jean-Pierre, “Group secret key generation using physical layer security for UAV swarm communications,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 6, pp. 8550–8564, Dec. 2023.

[3] A. M. Benaya, M. H. Ismail, A. S. Ibrahim, and A. A. Salem, “Physical layer security enhancement via intelligent omni-surfaces and UAV-friendly jamming,” *IEEE Access*, vol. 11, pp. 2531–2544, Jan. 2023.

[4] Z. Yin, M. Jia, N. Cheng, W. Wang, F. Lyu, Q. Guo, and X. Shen, “UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2739–2751, Mar. 2022.

[5] I. Elmehdi, Q. Marwa, B. F. El, and A.-K. Saif, “On the physical-layer security of a dual-hop UAV-based network in the presence of per-hop eavesdropping and imperfect CSI,” *IEEE Internet Things J.*, vol. 10, no. 9, pp. 7850–7867, May 2023.

[6] K. Ali, A. A. S., M. Lucio, N. Arumugam, and R. Carlo, “An emergent self-awareness module for physical layer security in cognitive UAV radios,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 888–906, Jun. 2022.

[7] S. J. Jafor, U. S. Enayet, I. M. Rabiul, R. Raad, K. A. Z., and M. M. A. Parvez, “Transceiver design for full-duplex UAV based zero-padded OFDM system with physical layer security,” *IEEE Access*, vol. 9, pp. 59 432–59 445, Apr. 2021.

[8] S. J. Maeng, Y. Yapıcı, İ. Güvenç, A. Bhuyan, and H. Dai, “Precoder design for physical-layer security and authentication in massive MIMO UAV communications,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2949–2964, Mar. 2022.

[9] B. Hamed, L. Mehdi, M. Majid, A. Ahmed, B. Hamid, and H. Lajos, “On the physical layer security of the cooperative rate-splitting-aided downlink in UAV networks,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5018–5033, Nov. 2021.

[10] F. Xiaojie, D. Zhaopeng, Y. Xinyu, L. Lei, S. Xuejun, and Z. Hongli, “Toward physical layer security and efficiency for SAGIN: A WFRFT-based parallel complex-valued spectrum spreading approach,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2819–2829, Mar. 2022.

[11] K. Amayika, L. Guoquan, M. D. Elhadj, C. K. Lilian, H. Nasir, and A. A. B. M., “Toward proactive, secure and efficient space-air-ground communications: Generative AI-based DRL framework,” *IEEE Open J. Commun. Soc.*, vol. 6, pp. 1284–1298, Feb. 2025.

[12] T. Haiyan, B. Paolo, Z. Liqiang, Z. Gan, L. Kai, and W. Kai-Kit, “Priority-based load balancing with multiagent deep reinforcement learning for space–air–ground integrated network slicing,” *IEEE Internet Things J.*, vol. 11, no. 19, pp. 30 690–30 703, Oct. 2024.

[13] W. Zhaowei, Y. Zhisheng, W. Xiucheng, C. Nan, Z. Yuan, and L. T. H., “Label-free deep learning driven secure access selection in space-air-ground integrated networks,” in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2023, pp. 958–963.

[14] R. Zhang, H. Du, Y. Liu, D. Niyato, J. Kang, Z. Xiong, A. Jamalipour, and D. I. Kim, “Generative AI agents with large language model for satellite networks via a mixture of experts transmission,” *IEEE J. Sel. Areas Commun.*, vol. 42, no. 12, pp. 3581–3596, Dec. 2024.

[15] R. Zhang, H. Du, D. Niyato, J. Kang, Z. Xiong, A. Jamalipour, P. Zhang, and D. I. Kim, “Generative AI for space-air-ground integrated networks,” *IEEE Wireless Commun.*, vol. 31, no. 6, pp. 10–20, Dec. 2024.

[16] B. Mao, X. Zhou, J. Liu, and N. Kato, “On an intelligent hierarchical routing strategy for ultra-dense free space optical low earth orbit satellite networks,” *IEEE J. Sel. Areas Commun.*, vol. 42, no. 5, pp. 1219–1230, May 2024.

[17] Z. Yalin, G. Xiaozheng, Y. Hang, Y. Kai, K. Jiawen, W. Ping, and N. Dusit, "Joint UAV trajectory and power allocation with hybrid FSO/RF for secure space–air–ground communications," *IEEE Internet Things J.*, vol. 11, no. 19, pp. 31 407–31 421, Oct. 2024.

[18] Y. Zhisheng, C. Nan, L. T. H., S. Yunchao, and W. Wei, "DT-assisted multi-point symbiotic security in space-air-ground integrated networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5721–5734, Sep. 2023.

[19] W. Xiting, R. Yuhan, L. Yongzhao, P. Cunhua, E. Maged, Z. Rui, and L. Tao, "A hierarchical game framework for win-win resource trading in cognitive satellite terrestrial networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 10, pp. 13 530–13 544, Oct. 2024.

[20] L. He, Z. Jia, K. Guo, H. Gan, Z. Han, and C. Yuen, "Online joint data offloading and power control for space-air-ground integrated networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 12, pp. 18 126–18 141, Dec. 2024.

[21] Y. Xu, C. Huang, L. Wei, Z. Yang, A. Al Hammadi, J. Yang, Z. Zhang, C. Yuen, and M. Debbah, "Hashing beam training for integrated ground-air-space wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 12, pp. 3477–3489, Dec. 2024.

[22] X. Cao, B. Yang, C. Yuen, and Z. Han, "HAP-reserved communications in space-air-ground integrated networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 8286–8291, Aug. 2021.

[23] T. V. Nguyen, T. D. Tran, N. S. Pham, V. T. Pham, and L. T. Tu, "Security-reliability analysis of NOMA-assisted hybrid satellite-terrestrial relay multi-cast transmission networks using fountain codes and partial relay selection with presence of multiple eavesdroppers," *EAI Endorsed Trans. Ind. Net. Intel. Syst.*, vol. 12, no. 3, Apr. 2025.

[24] Q. S. Nguyen, V. H. Nguyen, T. D. Tran, L. N. Nguyen, and L.-T. Tu, "On the security and reliability trade-off of the satellite terrestrial networks with fountain codes and friendly jamming," *EAI Endorsed Trans. Ind. Net. Intel. Syst.*, vol. 10, no. 4, p. e3, Dec. 2023.

[25] P. M. Nam, P. N. Dinh, N. L. Nhat, T. Lam-Thanh, and T. Le-Tien, "On the performance of the relay selection in multi-hop cluster-based wireless networks with multiple eavesdroppers under equally correlated rayleigh fading," *EAI Endorsed Trans. Ind. Net. Intel. Syst.*, vol. 11, no. 3, May 2024.

[26] H.-T. Duong, C. V. Phan, and Q.-T. Vien, "A secure cooperative image super-resolution transmission with decode-and-forward relaying over rayleigh fading channels," *EAI Endorsed Trans. Ind. Net. Intel. Syst.*, vol. 11, no. 4, Sep. 2024.

[27] R. Bin, H. Jie, A.-N. Azzam, Y. Kun, and J. Riku, "On the physical layer security of UAV-aided backscatter communications," *IEEE Wireless Commun. Lett.*, vol. 13, no. 2, pp. 274–278, Feb. 2024.

[28] J. Shaobo, W. Rong, L. Yi, W. Ning, Z. Di, S. Keshav, and M. Shahid, "Secrecy performance analysis of UAV-assisted ambient backscatter communications with jamming," *IEEE Trans. Wireless Commun.*, vol. 23, no. 12, pp. 18 111–18 125, Dec. 2024.

[29] M. Xiangyun, W. Xuanli, X. Ziyi, Z. Tingting, and X. Tao, "Secure resource allocation and trajectory design for UAV-assisted IoT with double cluster head," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 4, pp. 1661–1675, Dec. 2024.

[30] K. P. Gaurav, S. G. Devendra, Y. Suneel, K. Dragana, and J. Yuming, "Secrecy analysis and optimization of UAV-assisted IoT networks with RF-EH and imperfect hardware," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 8049–8063, Apr. 2025.

[31] H. M. Najmul, S. N. Kottakkaran, S. Tetsuya, I. M. Rakibul, K. S. Tamanna, and E. U. Shaikh, "Transceiver design of a secure multiuser FDSS-based DFT-spread OFDM system for RIS- and UAV-assisted THz communications," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 708–726, Jan. 2025.

[32] H. Dongxuan, S. Ziyuan, L. Han, M. Tianqi, and W. Zhaocheng, "UAV-assisted satellite-terrestrial secure communication using large-scale antenna array with one-bit ADCs/DACs," *IEEE Trans. Commun.*, vol. 71, no. 1, pp. 580–594, Jan. 2023.

[33] F. Zhaoxin, L. Huabing, Z. Nan, S. Zhaoyuan, C. Yunfei, and W. Xianbin, "Secure transmission of UAV control information via NOMA," *IEEE Trans. Commun.*, vol. 72, no. 8, pp. 4648–4660, Aug. 2024.

[34] Y. Zhisheng, C. Nan, S. Yunchao, H. Yilong, L. Yunhan, L. T. H., and Y. Shui, "UAV-assisted secure uplink communications in satellite-supported IoT: Secrecy fairness approach," *IEEE Internet Things J.*, vol. 11, no. 4, pp. 6904–6915, Feb. 2024.

[35] Z. Peiying, Z. Yi, K. Neeraj, and H. Ching-Hsien, "Deep reinforcement learning algorithm for latency-oriented IIoT resource orchestration," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 7153–7163, Apr. 2023.

[36] T. T. Bui, V. Sharma, A. Masaracchia, and T. Q. Duong, "UAV-aided optimal physical layer security in integrated satellite and terrestrial networks," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Cork, Ireland, 2025 (accepted).

[37] Y.-J. Chen, W. Chen, and M.-L. Ku, "Trajectory design and link selection in UAV-assisted hybrid satellite-terrestrial network," *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1643–1647, Jul. 2022.

[38] L. J. Rodriguez, N. H. Tran, and T. Le-Ngoc, "Performance of fullduplex AF relaying in the presence of residual self-interference," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1752–1764, Sep. 2014.

[39] 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 Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[40] Z. Zhang and Z. Zhao, "Rate maximizations for reconfigurable intelligent surface-aided wireless networks: A unified framework via block minorization-maximization," *arXiv preprint arXiv:2105.02395*, 2021.

[41] T. T. Bui, D. Van Huynh, L. D. Nguyen, H. Jung, and T. Q. Duong, "Joint phase-shift design and power control for near-and far-field communications in extremely large RIS-aided UAV networks," *IEEE Internet Things J.*, vol. 12, no. 13, pp. 22 658–22 668, Jul. 2025.

[42] M.-H. T. Nguyen, T. T. Bui, L. D. Nguyen, E. Garcia-Palacios, H.-J. Zepernick, H. Shin, and T. Q. Duong, "Real-time optimized clustering and caching for 6G satellite-UAV-terrestrial networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 3, pp. 3009–3019, Mar. 2024.